LEONAM DOS SANTOS GUIMARÃES

**SÍNTESE DE DOCTRINA DE SEGURANÇA
PARA PROJETO E OPERAÇÃO DE
SUBMARINOS NUCLEARES**

**TESE APRESENTADA À ESCOLA
POLITÉCNICA DA UNIVERSIDADE
DE SÃO PAULO PARA OBTENÇÃO
DO TÍTULO DE DOUTOR EM
ENGENHARIA**

SÃO PAULO

1999

LEONAM DOS SANTOS GUIMARÃES

BACHAREL EM CIÊNCIAS NAVAIS (ESCOLA NAVAL, RIO DE JANEIRO, BRASIL, 1980)

ENGENHEIRO NAVAL (ESCOLA POLITÉCNICA DA UNIVERSIDADE DE SÃO PAULO, BRASIL, 1986)

MESTRE EM ENGENHARIA NAVAL (ESCOLA POLITÉCNICA DA UNIVERSIDADE DE SÃO PAULO, BRASIL, 1991)

INGÉNIEUR ATOMIQUE (INSTITUT NATIONAL DES SCIENCES ET TECHNIQUES NUCLÉAIRES, SACLAY, FRANÇA, 1993)

MASTÈRE PROTECTION NUCLÉAIRE (CENTRE D'ÉTUDES SUR LA PROTECTION NUCLÉAIRE, FONTENAY, FRANÇA, 1995)

SÍNTESE DE DOCTRINA DE SEGURANÇA PARA PROJETO E OPERAÇÃO DE SUBMARINOS NUCLEARES

PROPOSTA DE UM CONJUNTO DE PRINCÍPIOS BÁSICOS, CRITÉRIOS GERAIS, REQUISITOS
ESPECÍFICOS E PROCEDIMENTOS DE VERIFICAÇÃO DO PROJETO E DE INSPEÇÃO DA
CONSTRUÇÃO E OPERAÇÃO PARA GARANTIA DA SEGURANÇA NUCLEAR E NAVAL DOS
REATORES PWR EMBARCADOS EM SUBMARINOS DE ATAQUE

**Tese apresentada à Escola
Politécnica da Universidade de
São Paulo para obtenção do título
de Doutor em Engenharia**

**Área de Concentração:
Engenharia Naval**

**Orientador:
Prof.Dr. Hernani Luis Brinati**

SÃO PAULO

1999

03/05/1913

À minha avó Noêmia Cortez
dos Santos ^{19/01/1999}, em
gratidão ao profundo e
incondicional amor que me
dedicou durante sua longa e
feliz vida. Tenho a certeza
que ela está agora, lá em
cima, compartilhando comigo
a enorme alegria que
representa ter vencido o
desafio de concluir este
trabalho.

A todos aqueles pioneiros que, nos idos de 1979, acreditaram que o sonho de projetar, construir e operar Submarinos Nucleares no Brasil poderia tornar-se uma realidade. Desejo que nós, seus sucessores, tenhamos a vontade e a competência suficientes para concluir a construção desta realidade, não deixando que as etapas já vencidas se percam no limbo dos sonhos perdidos.

A G R A D E C I M E N T O S

À MARINHA DO BRASIL, a quem devo integralmente toda minha formação profissional e grande parte de minha formação como pessoa, pelas inúmeras oportunidades proporcionadas, que permitiram obter os conhecimentos científicos e tecnológicos necessários para o desenvolvimento deste trabalho.

À MINHA FAMÍLIA, pela paciência e resignação com que suportou os incontáveis dias e noites nos quais não pude lhe dedicar toda a atenção requerida, ocupado que estava com a elaboração deste trabalho, como também pelo apoio e incentivo que, ao mesmo tempo, nunca me faltaram.

Ao PROF.DR. JORGE PINHEIRO DA COSTA VEIGA, meu mestre já há tantos anos, pelo incentivo, orientação e cobrança de resultados, sem os quais estou certo que não teria conseguido levar este trabalho ao seu termo final.

Guimarães, Leonam dos Santos

Síntese de Doutrina de Segurança para Projeto e Operação de Submarinos Nucleares. - São Paulo, 1999. 612f.

Tese (Doutorado) - Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia Naval.

1. Submarinos. 2. Propulsão Nuclear. 3. Segurança. I. Universidade de São Paulo. Escola Politécnica. Departamento de Engenharia Naval II. Título

EXTRATO

Considerando tanto os aspectos nucleares quanto os navais, esta tese propõe-se a organizar e sistematizar uma Doutrina de Segurança Global aplicável a futuros Submarinos Nucleares de Ataque (SNA) nacionais. Esta doutrina tem a forma de um conjunto de princípios básicos, critérios gerais, requisitos específicos e procedimentos de verificação do projeto e de inspeção da construção e operação, que garantam um alto padrão de segurança a esta classe de navio de guerra. Com ela, pretende-se constituir uma base consistente e coerente sobre a qual a Autoridade de Segurança Nuclear, considerando os Objetivos de Segurança propostos, possa avaliar a aceitabilidade dos riscos associados ao Ciclo de Vida do SNA, tomando assim suas competentes decisões quanto ao licenciamento do submarino.

RESUMO

Considerando tanto os aspectos nucleares quanto os navais, esta tese propõe-se a organizar e sistematizar uma Doutrina de Segurança Global aplicável a futuros Submarinos Nucleares de Ataque (SNA) nacionais. Esta doutrina tem a forma de um conjunto de princípios básicos, critérios gerais, requisitos específicos e procedimentos de verificação do projeto e de inspeção da construção e operação, que garantam um alto padrão de segurança a esta classe de navio de guerra. Com ela, pretende-se constituir uma base consistente e coerente sobre a qual a Autoridade de Segurança Nuclear, considerando os Objetivos de Segurança propostos, possa avaliar a aceitabilidade dos riscos associados ao Ciclo de Vida do SNA, tomando assim suas competentes decisões quanto ao licenciamento do submarino.

Entendendo-se segurança como percepção social de riscos, são discutidos o detalhamento, as interpretações, as derivações e as aplicações tecnológicas deste conceito básico em três contextos específicos: a disciplina de Segurança de Funcionamento de Sistemas Industriais (*Reliability-Availability-Maintanabilit-Safety*), de aplicação geral; a Segurança de Instalações Nucleares “Estacionárias”, em especial de reatores de potência eletronucleares; a Segurança Naval, que engloba tanto a Segurança Marítima (segurança da navegação, salvaguarda da vida humana no mar), típica de condições normais de paz, como a Capacidade de Sobrevivência (*Survivability*), típica das condições de guerra ou conflito. É feita, então, uma primeira abordagem global à Segurança da Propulsão Nuclear, que sintetiza as aplicações do conceito básico nestes três contextos e ressalta sua fundamentação na otimização do conjugado disponibilidade x segurança.

Os Princípios Básicos de Segurança são, a partir desta abordagem global, adaptados às particularidades da propulsão nuclear de SNA. Como “Princípios Básicos” entende-se os Objetivos Gerais de Segurança e uma série de diretrizes qualitativas que orientam como estes objetivos podem ser alcançados.

A seguir são propostos Critérios Gerais de Segurança para o projeto da Instalação Propulsora Nuclear (IPN) e de suas interfaces com a plataforma-navio do SNA. Como “Critérios Gerais” entende-se os Objetivos Detalhados de Segurança e uma série de diretrizes quantitativas que orientam o desenvolvimento do projeto integrado do conjunto de sistemas que compõem o SNA. São usados para garantir a adequação da segurança aos Princípios Básicos qualitativos.

Os requisitos específicos de segurança aplicáveis ao projeto de estruturas, componentes e sistemas da IPN e da plataforma-navio do SNA derivados dos Critérios Gerais são então desenvolvidos. Estes “Requisitos Específicos” são entendidos como regras quantitativas que determinam o projeto individual das partes integrantes do SNA. São usados para assegurar que os sistemas individuais do submarino, quando integrados, atendam aos Critérios Gerais.

São finalmente propostas diretrizes para o estabelecimento de uma regulamentação do processo de licenciamento dos SNA pela Autoridade de Segurança Nuclear e dos procedimentos de verificação da segurança do projeto e de fiscalização da operação associados. São ainda discutidos o conteúdo e a organização do Relatório de Análise de Segurança (RAS), documento básico deste processo, concluindo-se assim a estrutura da Doutrina de Segurança proposta.

A B S T R A C T

Considering both nuclear and naval aspects, this thesis intends to organize and to systematize a Global Safety Doctrine applicable to future national Nuclear Attack Submarines (SSN). This doctrine has the form of a set of basic principles, general criteria, specific requirements, design verification process and procedures for construction and operation inspection, aiming the assurance of a high level of safety pattern to these warships. Consequently, the doctrine would form a consistent and coherent basis for Nuclear Safety Authority (NSA) evaluate the social acceptability of SSN life cycle risks, considering the proposed Safety Objectives, in order to contribute to its competent decisions on submarine licensing.

Understanding safety as social perception of risks, detailing, interpretations, derivations and technological applications of this basic concept are discussed in three specific contexts: the Reliability-Availability-Maintainability-Safety (RAMS) discipline, of general application; the Safety of “Stationary” Nuclear Installations, specially power reactors; the Naval Safety, that includes both Marine Safety (navigation safety, safety of life in the sea), typical of normal conditions of peace, and Survivability, typical of the war or conflict conditions. A first global approach to the Safety of the Nuclear Propulsion, synthesizing the applications of the basic concept in these three contexts, and highlighting its foundation on a trade-off between availability and safety, is then developed.

Starting from this global approach, Safety Basic Principles are then adapted to the particularities of the SSN nuclear propulsion. As “Basic Principles” it is understood the Safety General Objectives and an associated series of qualitative guidelines for reaching these objectives.

Following, General Safety Criteria are proposed for the design of the Nuclear Propulsion Plant (NPP) and for its interfaces with SSN ship’s platform. As “General Criteria” it is understood the Safety Detailed Objectives and an associated series of quantitative guidelines to the development of the integrated design of SNA systems. They are considered to assure the SSN safety compliance to the qualitative Basic Principles.

Specific safety requirements applicable to NPP and ship’s platform structures, components and systems design, derived from General Criteria, are then developed. These “Specific Requirements” are understood as quantitative rules that determine the individual design of SNA main parts. They are used to assure that the individual systems of the submarine, when integrated, comply to the General Criteria.

Finally, they are proposed guidelines for the establishment of a regulatory process for SSN licensing by the Nuclear Safety Authority and for associated design safety verification procedures and operation safety enforcement. It is still discussed the Safety Analysis Report (SAR) content and organization, which constitutes the basic document for this process, concluding the structure of the Safety Doctrine proposal.

L I S T A D E T A B E L A S

TABELA 2.1:	OBJETIVOS DA SEGURIDADE NUCLEAR	46
TABELA 2.2:	NÍVEIS DE DEFESA EM PROFUNDIDADE.....	56
TABELA 2.3:	ACIDENTES MARÍTIMOS NA MARINHA MERCANTE.....	65
TABELA 2.4:	ACIDENTES MARÍTIMOS NA MARINHA MILITAR	67
TABELA 2.5:	ACIDENTES MARÍTIMOS COM SUBMARINOS MILITARES ...	70
TABELA 2.6:	INTERFACES ENTRE SISTEMAS DO AMBIENTE-NAVIO.....	87
TABELA 2.7:	INVENTÁRIO DE PRODUTOS DE FISSÃO DO U-235 PARA UM REATOR NAVAL DE 100 MWTH APÓS 600 DIAS DE OPERAÇÃO.....	95
TABELA 2.8:	NATUREZA FÍSICA DOS PRODUTOS DE FISSÃO DO U-235 ..	95
TABELA 2.9:	INVENTÁRIO RADIOATIVO DOS PRODUTOS DE ATIVAÇÃO DE UM REATOR NAVAL 1 ANO APÓS DESLIGAMENTO.....	96
TABELA 3.1:	PRINCÍPIOS BÁSICOS DE SEGURANÇA.....	107
TABELA 4.1:	CLASIFICAÇÃO DAS CLASSES DE CENÁRIOS OPERACIONAIS DO SNA CONFORME SUAS FREQUÊNCIAS ANUAIS DE OCORRÊNCIA	190
TABELA 4.2:	NÍVEIS DE CONSEQÜÊNCIAS PARA O SUBMARINO.....	191
TABELA 4.3:	NÍVEIS DE CONSEQÜÊNCIAS PARA O AMBIENTE.....	192
TABELA 4.4:	NÍVEIS DE CONSEQÜÊNCIAS PARA A TRIPULAÇÃO.....	193
TABELA 4.5:	NÍVEIS DE CONSEQÜÊNCIAS PARA PARA O PESSOAL DE APOIO EM TERRA.....	194
TABELA 4.6:	NÍVEIS DE CONSEQÜÊNCIAS PARA O PÚBLICO	195
TABELA 4.7:	OBJETIVOS DETALHADOS DE SEGURANÇA.....	196
TABELA 4.8:	DOSES EM CASO DE ACIDENTE BÁSICO DE PROJETO	217
TABELA 4.9:	DOSES EM CASO DE ACIDENTE SEVERO	217
TABELA 4.10:	ESTADOS DE MAR DE PROJETO	226
TABELA 5.1:	LIMITES DE TAXA DE DOSE EQUIVALENTE PARA ÁREAS LIVRES DO SNA.....	234
TABELA 5.2:	LIMITES DE DOSE PARA PARTES DO CORPO EM CONDIÇÕES DE IRRADIAÇÃO CONTROLADA.....	239
TABELA 5.3:	LIMITES PARA LIBERAÇÃO DE EFLUENTES	244
TABELA 5.4:	LIMITES DE CONCENTRAÇÃO DE POLUENTES NO AR.....	284

TABELA 7.1:	OBJETIVOS DE SEGURANÇA PARA SNA	352
TABELA B.1:	PERFIL DE VIDA ÚTIL DO SNA	364
TABELA B.2:	CICLO DE ATIVIDADES BÁSICO DO SNA.....	365
TABELA B.3:	CICLO DE ATIVIDADES INTERMEDIÁRIO DO SNA.....	365
TABELA B.4:	CICLO DE ATIVIDADES FINAL DO SNA.....	365
TABELA B.5:	TRANSIENTES NORMAIS DO SNA	366
TABELA B.6:	TRANSIENTES ANORMAIS DO SNA	369
TABELA B.7:	TEMPO MÁXIMO PARA O SNA SUSPENDER	373
TABELA E.1:	CLASSIFICAÇÃO DAS FALHAS EM FUNÇÃO DOS EFEITOS	400
TABELA E.2:	CLASSIFICAÇÃO DAS FALHAS EM FUNÇÃO DAS CAUSAS	401
TABELA E.3:	EXPRESSÕES PARA FALHA EM AVANÇO E FALHA EM ATRASSO DE REDUNDÂNCIAS SIMPLES.....	411
TABELA F.1:	COMPARAÇÃO DE LEIS DE PROBABILIDADES	434
TABELA F.2:	ESTATÍSTICAS DA LEI DE GUMBEL	439
TABELA F.3:	ESTATÍSTICAS DA LEI DE FRECHET	441
TABELA G.1:	CONFLITO ENTRE CONFIABILIDADE E SEGURIDADE.....	450
TABELA G.2:	COMPARAÇÃO ENTRE CONFIABILIDADE E SEGURIDADE	451
TABELA G.3:	FUNÇÕES SADT.....	464
TABELA G.4:	LEIS DE TRANSIÇÃO DAS REDES DE PETRI ESTOCÁSTICAS	468
TABELA G.5:	COMPARAÇÃO DE CARACTERÍSTICAS INTRÍNSECAS DOS MÉTODOS	473
TABELA G.6:	INTERESSE DOS MÉTODOS DE ANÁLISE PREVISIONAL PARA FALHAS DEPENDENTES	476
TABELA H.1:	EXEMPLO DE ALOCAÇÃO DE SEGURANÇA POR PONDERAÇÃO DE CONFIABILIDADE.....	489
TABELA J.1:	CONDIÇÕES DE PROCESSO DA INSTALAÇÃO NUCLEAR..	498
TABELA J.2:	SIMBOLOGIA DE SEQUÊNCIAS ACIDENTAIS EM PWR.....	515
TABELA J.3:	TERMOS-FONTE EM ACIDENTES SEVEROS.....	517
TABELA J.4:	EQUIPAMENTOS IMPORTANTES PARA A SEGURANÇA.....	518
TABELA P.1:	CLASSIFICAÇÃO DAS ATIVIDADES DE INSPEÇÃO, MANUTENÇÃO E REPARO DE UM SNA.....	560
TABELA P.2:	DIRETRIZES PARA JUSTIFICAÇÃO DE DOSES	562

L I S T A D E F I G U R A S

FIGURA 1.1:	DOUTRINA DE SEGURANÇA PARA SUBMARINOS NUCLEARES	1
FIGURA 1.2:	SUBMARINO NUCLEAR DE ATAQUE TÍPICO.....	4
FIGURA 1.3:	REATOR DE PROPULSÃO NAVAL PWR TÍPICO.....	5
FIGURA 1.4:	INSTALAÇÃO PROPULSORA NUCLEAR TÍPICA.....	6
FIGURA 1.5:	COMPARTIMENTO DE REATOR PWR TÍPICO	7
FIGURA 2.1:	SEGURANÇA DE FUNCIONAMENTO DE SISTEMAS	26
FIGURA 2.2:	DIAGRAMA DE FARMER	32
FIGURA 2.3:	AÇÃO DE PREVENÇÃO.....	37
FIGURA 2.4:	AÇÃO DE PROTEÇÃO.....	38
FIGURA 2.5:	AÇÃO DE SEGURO	38
FIGURA 2.6:	PROCEDIMENTO GERAL DE ANÁLISE DE SEGURANÇA	40
FIGURA 2.7:	PROCEDIMENTO DE ALOCAÇÕES DE SEGURANÇA.....	43
FIGURA 2.8:	CICLO DO COMBUSTÍVEL NUCLEAR.....	45
FIGURA 2.9:	COMPARAÇÃO DAS FRO DE ACIDENTES MARÍTIMOS PARASUBMARINOS E PARA NAVIOS DE GUERRA EM GERAL	69
FIGURA 2.10:	CORRELAÇÃO ENTRE PROFUNDIDADE E SEGURANÇA.....	76
FIGURA 2.11:	ENVELOPE DE SEGURANÇA DE SUBMARINOS.....	80
FIGURA 2.12:	INTERFACES ENTRE SISTEMAS DO AMBIENTE-NAVIO	86
FIGURA 3.1:	ROTAS PRINCIPAIS DE LIBERAÇÃO DE MATERIAIS RADIOATIVOS EM ACIDENTE GRAVE COM UM SNA.....	113
FIGURA 5.1:	ARRANJO ESTRUTURAL DO COMPARTIMENTO DO REATOR	278
FIGURA 5.2:	ARRANJO DE PASSAGEM PELO COMPARTIMENTO DO REATOR.....	279
FIGURA A.1:	REATORES A ÁGUA LEVE.....	358
FIGURA A.2:	ACIONAMENTO MECÂNICO DE SNA.....	361
FIGURA A.3:	ACIONAMENTO ELÉTRICO DE SNA.....	362
FIGURA A.4:	PROPULSÃO NUCLEAR DE NAVIOS-AERÓDROMOS.....	363
FIGURA E.1:	REPRESENTAÇÃO DE UM SISTEMA	394
FIGURA E.2:	INFORMAÇÕES NECESSÁRIAS À ANÁLISE DO SISTEMA ..	396
FIGURA E.3:	ETAPAS DO PROCESSO DE ANÁLISE.....	397

FIGURA E.4:	CURVA “BANHEIRA”	399
FIGURA E.5:	RELAÇÕES ENTRE DEFEITO, FALHA E PANE.....	403
FIGURA E.6:	CAUSAS, EFEITOS E MODOS DE FALHA.....	409
FIGURA E.7:	FALHA EM AVANÇO E FALHA EM ATRASO	410
FIGURA E.8:	ESQUEMA FUNCIONAL	410
FIGURA E.9:	FALHA EM ATRASO	410
FIGURA E.10:	FALHA EM AVANÇO.....	410
FIGURA E.11:	COMPARAÇÃO DE PROBABILIDADES PARA FALHA EM AVANÇO E FALHA EM ATRASO DE REDUNDÂNCIAS SIMPLES	412
FIGURA F.1:	DOMÍNIOS DE FUNCIONAMENTO DE UM SISTEMA.....	417
FIGURA F.2:	QUANTIL X_p DE UMA VARIÁVEL ALEATÓRIA X.....	424
FIGURA G.1:	CARACTERÍSTICAS DE SEGURANÇA DE FUNCIONAMENTO.....	444
FIGURA G.2:	ANÁLISE POR ZONAS	456
FIGURA G.3:	ANÁLISE TEMPORAL.....	457
FIGURA G.4:	ETAPAS DE UMA AMFE.....	460
FIGURA G.5:	ESTABELECIMENTO DE MODOS DE FALHA DE UM COMPONENTE E SUAS CAUSAS	460
FIGURA G.6:	ELABORAÇÃO DE UMA ÁRVORE DE CONSEQÜÊNCIAS....	463
FIGURA G.7:	EXEMPLO DE ÁRVORE DE CONSEQÜÊNCIAS	463
FIGURA G.8:	GRAFO DE ESTADO DE UM SISTEMA COM UM COMPONENTE.....	466
FIGURA G.9:	GRAFO DE ESTADOS PARA UM SISTEMA COM DOIS COMPONENTES.....	467
FIGURA G.10:	GRAFO DE ESTADOS PARA CONFIABILIDADE	467
FIGURA G.11:	REPRESENTAÇÃO ESQUEMÁTICA DO COMPORTAMENTO DO OPERADOR HUMANO.....	480
FIGURA G.12:	MÉTODO DA RESISTÊNCIA-CARREGAMENTO	481
FIGURA H.1:	RELAÇÕES ESTRUTURAIS	487
FIGURA J.1:	EVOLUÇÃO DE UM ACIDENTE SEVERO	517
FIGURA L.1:	BLOCO BÁSICO SADT.....	532
FIGURA L.2:	APLICAÇÃO DO SADT.....	533
FIGURA M.1:	ESQUEMA GERAL DE BLINDAGEM DE UM REATOR NAVAL.....	543

L I S T A D E A B R E V I A T U R A S

ABP:	ACIDENTES BÁSICOS DE PROJETO
ACP:	ACIDENTES COMPLEMENTARES DE PROJETO
AGPRP:	ACIDENTE DE GRANDE PERDA DE REFRIGERANTE PRIMÁRIO
AIEA:	AGÊNCIA INTERNACIONAL DE ENERGIA NUCLEAR
AL:	AUTORIZAÇÃO DE LOCAL
ALARA;	<i>AS LOW AS REASONABLE ACHIEVABLE</i>
AMFE:	ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS
AMFEC:	ANÁLISE DE MODOS DE FALHA, EFEITOS E CRITICIDADE
ANS:	<i>AMERICAN NUCLEAR SOCIETY</i> (EUA)
ANSI:	<i>AMERICAN NATIONAL STANDARDS INSTITUTE</i> (EUA)
AOI:	AUTORIZAÇÃO PARA OPERAÇÃO INICIAL
AOP:	AUTORIZAÇÃO PARA OPERAÇÃO PERMANENTE
APR:	ANÁLISE PRELIMINAR DE RISCOS
APRP:	ACIDENTE DE PERDA DE REFRIGERANTE PRIMÁRIO
APS:	ANÁLISE PROBABILÍSTICA DE SEGURANÇA
ARTGV:	ACIDENTE DE RUPTURA DE TUBOS DO GERADOR DE VAPOR
ASME:	<i>AMERICAN SOCIETY OF MECHANICAL ENGINEERS</i> (EUA)
ASN:	AUTORIDADE DE SEGURANÇA NUCLEAR
ASNM:	AUTORIDADE DE SEGURANÇA NUCLEAR MILITAR
ATWS:	ATICIPATED TRANSIENTS WITHOUT SCRAM
AU:	<i>ARRÊT D'URGENCE</i>
AUMN:	AUTORIZAÇÃO PARA UTILIZAÇÃO DE MATERIAIS RADIOATIVOS
BCP:	BOMBA DE CIRCULAÇÃO PRINCIPAL
BIBS:	<i>BUILT-IN BREATHING SYSTEM</i>
BNL	<i>BROOKENHAVEN NATIONAL LABORATORY</i> (EUA)
Bq:	BEQUEREL

BWR:	<i>BOILING WATER REACTOR</i>
CAB:	CICLO DE ATIVIDADES BÁSICO
CAF:	CICLO DE ATIVIDADES FINAL
CAI:	CICLO DE ATIVIDADES INTERMEDIÁRIO
CB:	CICLOS BÁSICO
CCPWR:	<i>CLOSED COUPLED PRESSURIZED WATER REACTOR</i>
CEI:	<i>COMMISSION ELECTROTECHNIQUE INTERNATIONAL</i>
CFU (CFS)	CRITÉRIO DE FALHA ÚNICA (SIMPLES)
CI:	COEFICIENTE DE INDISCRICÃO
Ci:	CURIE
CIPR	COMISSÃO INTERNACIONAL DE PROTEÇÃO RADIOLÓGICA
CN:	CRUZADOR NUCLEAR
CNEN:	COMISSÃO NACIONAL DE ENERGIA NUCLEAR
COC:	CENTRO DE OPERAÇÕES DE COMBATE
CP:	CLASSE DE PROJETO
CPIN:	CONDIÇÕES DE PROCESSO DA INSTALAÇÃO NUCLEAR
CS:	CLASSE DE SEGURANÇA
CV:	CICLO DE VIDA
DEPP:	DIAS EQUIVALENTES A PLENA POTÊNCIA
DGA:	DIESEL-GERADORES AUXILIARES
DGMM:	DIRETORIA GERAL DO MATERIAL DA MARINHA
DNB:	<i>DEPARTURE FROM NUCLEATE BOILING</i>
DNBR:	<i>DEPARTURE FROM NUCLEATE BOILING RATE</i>
DOD:	<i>DEPARTMENT OF DEFENCE</i>
DSIN:	<i>DIRECTORAT DE LA SÛRETÉ DES INSTALLATIONS NUCLÉAIRES</i>
ECM:	ESTAÇÃO DE CONTROLE DE MÁQUINAS
EHP:	<i>EFFECTIVE HORSE-POWER</i>
EIA:	ESTUDO DE IMPACTO AMBIENTAL
EIS:	EQUIPAMENTOS IMPORTANTES PARA A SEGURANÇA NUCLEAR

EIS:	EQUIPAMENTO IMPORTANTE PARA SEGURANÇA
EPI:	EQUIPAMENTO DE PROTEÇÃO INDIVIDUAL
EPRI:	<i>ELECTRIC POWER RESEARCH INSTITUTE</i> (EUA)
EUA:	ESTADOS UNIDOS DA AMÉRICA
FAO:	FREQÜÊNCIA ANUAL DE OCORRÊNCIA
FDP:	FUNÇÃO DENSIDADE DE PROBABILIDADE
FRO:	FREQÜÊNCIA RELATIVA DE OCORRÊNCIA
FRP:	FUNÇÃO REPARTIÇÃO DE PROBABILIDADE
FTA:	<i>FAULT TREE ANALYSIS</i>
GAS:	GUERRA ANTI-SUBMARINO
GNBQ:	GUERRA NUCLEAR-BIOLÓGICA-QUÍMICA
GQ:	GARANTIA DA QUALIDADE
GV:	GERADOR DE VAPOR
HAZOP:	<i>HAZARD AND OPERABILITY</i>
HSE:	<i>HEALTH AND SAFETY EXECUTIVE</i> (Grã-Bretanha)
IBAMA:	INSTITUTO BRASILEIRO DO MEIO AMBIENTE E RECURSOS NATURAIS RENOVÁVEIS
ICRP	<i>INTERNATIONAL COMMISSION OF RADIOLOGICAL PROTECTION</i>
IEEE:	<i>INSTITUTE OF ELECTRIC AND ELECTRONIC ENGINEERS</i> (EUA)
IEPWR:	<i>INTEGRATED EXTERNALLY PRESSURIZED WATER REACTOR</i>
IGP:	IMERSÃO A GRANDE PROFUNDIDADE
IMO:	<i>INTERNATIONAL MARITIME ORGANIZATION</i>
INB:	INSTALAÇÕES NUCLEARES DE BASE
INSAG:	<i>INTERNATIONAL NUCLEAR SAFETY ASSESSMENT GROUP</i>
IPN:	INSTALAÇÃO PROPULSORA NUCLEAR
IPSN:	<i>INSTITUT DE PROTECTION ET SÛRETÉ NUCLEAIRE</i> (França)
IPWR:	<i>INTEGRATED PRESSURIZED WATER REACTOR</i>
ISPWR:	<i>INTEGRATED SELF-PRESSURIZED WATER REACTOR</i>
LC:	LICENÇA DE CONSTRUÇÃO

LEU:	<i>LOW ENRICHED URANIUM</i>
LOCA:	<i>LOSS OF COOLANT ACCIDENT</i>
MAC:	MÉTODO DA ÁRVORE DE FALHAS
MACQ:	MÉTODO DA ÁRVORE DE CONSEQÜÊNCIAS
MARPOL:	<i>MARITIME POLLUTION</i>
MB:	MARINHA DO BRASIL
MCPR:	MÉTODO DA COMBINAÇÃO DE PANES RESUMIDAS
MDC:	MÉTODO DO DESCONTO DE COMPONENTES
MDCC:	MÉTODO DO DIAGRAMA CAUSAS-CONSEQÜÊNCIAS
MDS:	MÉTODO DO DIAGRAMA DE SUCESSO
MDT:	<i>MEAN DOWN TIME</i>
MEE:	MÉTODO DO ESPAÇO DE ESTADOS
MEP:	MOTOR ELÉTRICO DE PROPULSÃO
MNF:	<i>MARINE NATIONALE FRANÇAISE</i>
MPB:	MISSÃO DE PATRULHA BÁSICA
MRPE:	MÉTODO DA REDE DE PETRI ESTOCÁSTICA
MTBF:	<i>MEAN TIME BETWEEN FAILURES</i>
MTTF:	<i>MEAN TIME TO FAILURE</i>
MTTR:	<i>MEAN TIME TO REPAIR</i>
MTV:	MÉTODO DA TABELA DE VERDADE
MUT:	<i>MEAN UP TIME</i>
NAeN:	NAVIO-AERÓDROMO NUCLEAR
NE:	NORMA EXPERIMENTAL
NRC:	<i>NUCLEAR REGULATORY COMMISSION</i> (EUA)
ODS:	OBJETIVOS DETALHADOS DE SEGURANÇA
OGS:	OBJETIVOS GERAIS DE SEGURANÇA
ONG:	ORGANIZAÇÃO NÃO-GOVERNAMENTAL
OSTI:	ÓRGÃO DE SUPERVISÃO TÉCNICA INDEPENDENTE
OTAN:	ORGANIZAÇÃO DO TRATADO DO ATLÂNTICO NORTE

PAM:	PERÍODO DE ATUALIZAÇÃO E MODERNIZAÇÃO
PCCMN:	PLANO DE CONTABILIDADE E CONTROLE DE MATERIAIS NUCLEARES
PDCTPN:	PROGRAMA DE DESENVOLVIMENTO DE CAPACITAÇÃO TECNOLÓGICA EM PROPULSÃO NUCLEAR
PDF:	PERÍODO DE DOCAGEM FINAL
PDP:	PRINCÍPIO DE DEFESA EM PROFUNDIDADE
PDR:	PERÍODO DE DOCAGEM DE ROTINA
PEE:	PLANO DE EMERGÊNCIA EXTERNO
PEI:	PLANO DE EMERGÊNCIA INTERNO
PEL:	PLANO DE EMERGÊNCIA LOCAL
PGQ:	PROGRAMA DE GARANTIA DA QUALIDADE
PMG:	PERÍODO DE MANUTENÇÃO GERAL
PMR:	PERÍODO DE MANUTENÇÃO DE ROTINA
POB:	PERÍODO OPERATIVO BÁSICO
POF:	PERÍODO DE OPERAÇÃO FINAL
POI:	PERÍODO OPERATIVO INTERMEDIÁRIO
PROTER:	PROTÓTIPO EM TERRA
PWR:	PRESSURIZED WATER REACTORS
PZ:	PRESSURIZADOR
RAMS:	<i>RELIABILITY, AVAILABILITY, MANTENABILITY AND SAFETY</i>
RAS:	RELATÓRIO DE ANÁLISE DE SEGURANÇA
REM:	REQUISITOS DE ESTADO MAIOR
RF:	<i>REPUBLIQUE FRANÇAISE</i>
RFAS:	RELATÓRIO FINAL DE ANÁLISE DE SEGURANÇA
RIMA:	RELATÓRIO DE IMPACTO AMBIENTAL
RPAS:	RELATÓRIO PRELIMINAR DE ANÁLISE DE SEGURANÇA
SADT:	STRUCTURED ANALYSIS AND DESIGN TECHNIC
SCRAM:	<i>SAFETY CONTROL ROD AXE MAN</i>

SDFSI:	SEGURANÇA DE FUNCIONAMENTO DE SISTEMAS INDUSTRIAIS
SES:	SISTEMA ELÉTRICO DE SERVIÇO
SHARP:	<i>SYSTEMATIC HUMAN ACTION RELIABILITY PROCEDURE</i>
SNA:	SUBMARINO NUCLEAR DE ATAQUE
SOLAS:	<i>SAFETY OF LIFE AT SEA</i>
SOS:	SITUAÇÕES DE OPERAÇÃO DO SUBMARINO
SRE:	SISTEMA DE RESFRIAMENTO DE EMERGÊNCIA
Sv:	SIEVERT
TASD:	TRANSIENTES ANTECIPADOS SEM DESLIGAMENTO
TGP:	TURBO-GERADORES DE PROPULSÃO
TGS:	TURBO-GERADORES DE SERVIÇO
TNT:	TRINITROTOLUENO
TP:	TURBINAS DE PROPULSÃO
UF6:	HEXAFLUORETO DE URÂNIO
UO2:	DIÓXIDO DE URÂNIO
USFG:	<i>UNITED STATES FEDERAL GOVERNMENT</i>
VPR:	VASO DE PRESSÃO DO REATOR
ZTA:	ZONA TÉRMICAMENTE AFETADA

S U M Á R I O

LISTA DE TABELAS	vii
LISTA DE FIGURAS	lx
LISTA DE ABREVIATURAS	xi
RESUMO	xvii
ABSTRACT	xviii
1 INTRODUÇÃO	1
1.1 OBJETO	1
1.2 DEFINIÇÕES E CONCEITOS PRELIMINARES	2
1.3 NECESSIDADE GERADORA	8
1.4 ESCOPO	12
1.5 PROPÓSITO.....	13
1.6 ORGANIZAÇÃO	15
2 CONCEITOS E MÉTODOS	18
2.1 SEGURANÇA DE SISTEMAS INDUSTRIAIS	18
2.1.1 Contexto de Aplicação.....	19
2.1.2 Definição de Conceitos.....	20
2.1.3 Formulação de Parâmetros.....	27
2.1.4 Limites Superiores de Riscos	34
2.1.5 Gerenciamento de Riscos	36
2.2 SEGURANÇA NUCLEAR.....	43
2.2.1 Escopo	44
2.2.2 Objetivos.....	46
2.2.3 Riscos Potenciais e Funções Básicas.....	48
2.2.4 Defesa em Profundidade.....	52
2.2.5 Análise de Segurança Nuclear	57
2.3 SEGURANÇA NAVAL.....	61
2.3.1 Escopo	61
2.3.2 Objetivos.....	62
2.3.3 Riscos Potenciais e Funções Básicas.....	64
2.3.4 Análise da Segurança Marítima.....	71
2.3.5 Análise da Capacidade de Sobrevivência	81
2.4 SEGURANÇA NUCLEAR NAVAL.....	83
2.4.1 Identificação de Sistemas e Interfaces	84
2.4.2 Conjugado Disponibilidade x Seguridade	89
2.4.3 Inventário de Materiais Radioativos	94
2.4.4 Delineamento de Doutrina de Segurança	96
2.4.5 Análise de Segurança do Navio Nuclear	102

3	PRINCÍPIOS BÁSICOS	107
3.1	OBJETIVOS DE SEGURANÇA	108
3.1.1	Objetivo Geral	108
3.1.2	Objetivo de Proteção Radiológica	109
3.1.3	Objetivo de Segurança Nuclear (Confiabilidade e Seguridade)	109
3.1.4	Objetivo de Segurança Naval (Disponibilidade)	111
3.2	PRINCÍPIOS FUNDAMENTAIS	113
3.2.1	Responsabilidades pelo Gerenciamento do Ciclo de Vida	114
3.2.2	Estratégia de Defesa em Profundidade	117
3.2.3	Princípios Técnicos Gerais	121
3.3	PRINCÍPIOS ESPECÍFICOS	129
3.3.1	Áreas de Mobilidade e Localizações Fixas Pré-definidas	130
3.3.2	Projeto	137
3.3.3	Fabricação e Construção	163
3.3.4	Comissionamento	165
3.3.5	Operação	167
3.3.6	Gerenciamento de Acidentes	181
3.3.7	Planejamento de Emergência	185
4	CRITÉRIOS GERAIS	188
4.1	OBJETIVOS GERAIS DE SEGURANÇA	188
4.1.1	Critérios de Probabilidade	188
4.1.2	Critérios de Gravidade	190
4.1.3	Critérios de Risco	195
4.1.4	Critério de Falha Única	197
4.2	CONDIÇÕES DE PROCESSO E SITUAÇÕES DE OPERAÇÃO	198
4.2.1	Condições de Processo da Instalação Nuclear	198
4.2.2	Situações Operacionais do Submarino	203
4.2.3	Critérios Gerais de Análise	207
4.2.4	Análise das Condições de Processo da Instalação Nuclear	209
4.2.5	Análise das Situações Operativas do Submarino	213
4.3	CRITÉRIOS DE PROJETO	216
4.3.1	Áreas de Mobilidade e as Localizações Fixas Pré-definidas	216
4.3.2	Descomissionamento e Perda do Submarino	218
4.3.3	Classes de Segurança e Classes de Projeto	219
4.3.4	Condições Ambientais	225
4.3.5	Instalação Propulsora Nuclear	227
5	REQUISITOS ESPECÍFICOS	229
5.1	GARANTIA DA QUALIDADE	229
5.1.1	Estrutura organizacional	230
5.1.2	Documentação e registros	231
5.1.3	Procedimentos de Controle	231

5.1.4	Testes	232
5.2	PROTEÇÃO RADIOLÓGICA.....	233
5.2.1	Requisitos de Projeto	233
5.2.2	Proteção Individual.....	235
5.2.3	Proteção Ambiental.....	243
5.3	OPERAÇÃO.....	250
5.3.1	Documentação de Operação	252
5.3.2	Procedimentos Operacionais	256
5.3.3	Procedimentos de Emergência	258
5.3.4	Manutenção e Reparo	259
5.3.5	Treinamento, Qualificação e Adestramento da Tripulação.....	259
5.4	INSPEÇÕES E TESTES	262
5.4.1	Durante a Construção.....	265
5.4.2	Durante o Comissionamento	268
5.4.3	Durante a Operação.....	272
5.4.4	Durante Reparos, Modernização e Modificações	275
5.5	PLATAFORMA-NAVIO.....	277
5.5.1	Arranjo Geral.....	277
5.5.2	Ventilação e Condicionamento do Ar.....	283
5.5.3	Estrutura	285
5.5.4	Proteção contra Colisão e Quedas de Aeronaves.....	286
5.5.5	Proteção contra Incêndios	287
5.5.6	Segurança Física da IPN e do Material Físsil Especial	289
5.6	INSTALAÇÃO NUCLEAR.....	289
5.6.1	Requisitos de Projeto	289
5.6.2	Reator.....	292
5.6.3	Circuito Primário	398
5.6.4	Instrumentação.....	301
5.6.5	Dispositivos de Segurança.....	302
5.7	INSTALAÇÕES DE MÁQUINAS.....	306
5.7.1	Requisitos de Projeto	306
5.7.2	Máquinas Principais.....	308
5.7.3	Máquinas Auxiliares	310
5.7.4	Propulsão de Emergência	311
5.7.5	Sistemas Elétricos.....	312
6	PROCESSO DE LICENCIAMENTO.....	317
6.1	RESPONSABILIDADES E CONDIÇÕES	317
6.1.1	Organização Operadora	319
6.1.2	Autoridade de Segurança Nuclear	320
6.1.3	Condições de Aceitabilidade	321
6.1.4	Informações requeridas	322
6.2	RELATÓRIO DE ANÁLISE DE SEGURANÇA	326

6.2.1	Propósito e Escopo.....	326
6.2.2	Requisitos Específicos	327
6.2.3	Desenvolvimento da Análise	329
6.2.4	Conteúdo do Relatório	334
6.2.5	Revisão e Verificação.....	343
7	CONCLUSÕES	346
	ANEXOS.....	355
A	INSTALAÇÕES PROPULSORAS NUCLEARES	355
B	CICLO DE VIDA DE UM SUBMARINO NUCLEAR DE ATAQUE.....	364
B.1	Perfil de Vida Útil.....	364
B.2	Transientes Operacionais Normais	366
B.3	Transientes Operacionais Anormais	369
B.4	Condições de Prontidão.....	372
C	LICENCIAMENTO DE INSTALAÇÕES NUCLEARES	374
C.1	Aspectos Gerais	374
C.2	Licenciamento Nuclear.....	375
C.3	Licenciamento Ambiental	379
D	INCIDÊNCIA DE PERIGOS INDUSTRIAIS E RADIOLÓGICOS	380
D.1	Perigo e Risco	380
D.2	Segurança Absoluta e Risco Aceitável.....	385
D.3	Compromisso entre Riscos Locais e Riscos Globais	387
D.4	Aspectos Econômico-Financeiros	389
D.5	Riscos Radiológicos.....	390
E	ANÁLISE DE MODOS DE FALHA EM SISTEMAS.....	393
E.1	Sistema.....	393
E.2	Análise de um Sistema	395
E.3	Falha	397
E.4	Pane.....	400
E.5	Relações entre Defeito, Falha e Pane.....	402
E.6	Modos de Falha	403
E.7	Dependência entre Falhas	405
E.8	Falhas de Causa Comum e em Cascata.....	407
E.9	Classificação das Falhas de Causa Comum	408
E.10	Análise dos Modos de Falha	409
E.11	Falha em Atraso e Falha em Avanço de Elementos em Redundância Total.....	410
E.12	Falha em Atraso de Elementos em Redundância Parcial.....	412
E.13	Modos de Falha de Causa Comum	413
F	PROBABILIDADES EM SEGURANÇA DE SISTEMAS.....	415
F.1	Utilização das Probabilidades.....	417
F.2	Diferentes Definições de Probabilidades	421
F.3	Período de Retorno de um Evento	423

SÍNTESE DE DOCTRINA DE SEGURANÇA
PARA PROJETO E OPERAÇÃO DE SUBMARINOS NUCLEARES

F.4	Aproximações e Erros	425
F.5	Reflexões sobre a Fixação de Limites Mínimos de Probabilidade.....	427
F.6	Leis de Probabilidades.....	432
F.7	Leis de Valores Extremos	435
G	CONCEITOS E MÉTODOS DA SEGURANÇA DE FUNCIONAMENTO	443
G.1	Confiabilidade.....	445
G.2	Disponibilidade	446
G.3	Manutibilidade.....	447
G.4	Seguridade (ou Segurança)	448
G.5	Cindinística.....	448
G.6	Níveis de Segurança.....	449
G.7	Compromisso entre Confiabilidade e Segurança	449
G.8	Normas Clássicas de Segurança.....	451
G.9	Segurança como Qualidade.....	453
G.10	Segurança e Processo Decisório	454
G.11	“Leis” de Murphy.....	454
G.12	Métodos de Análise e Avaliação da Segurança de Sistemas.....	455
G.13	Tipos Gerais de Análises.....	456
G.14	Métodos Estáticos	457
G.15	Métodos Analíticos e de Simulação.....	464
G.16	Vantagens e Inconvenientes dos Diversos Métodos	468
G.17	Comparação dos Diversos Métodos	472
G.18	Critérios de Seleção de Métodos	475
G.19	Métodos Específicos	476
H	PROCEDIMENTOS DE ALOCAÇÕES DE SEGURANÇA	483
H.1	Conceito.....	483
H.2	Principais Métodos	484
I	PRINCÍPIO DE DEFESA EM PROFUNDIDADE.....	490
J	ANÁLISE DETERMINÍSTICA DE SEGURANÇA NUCLEAR.....	497
J.1	Classificação das Condições de Processo da Instalação	497
J.2	Definição das Categorias de Condições de Processo Básicas de Projeto	499
J.3	Seleção das Condições de Processo	500
J.4	Listagem e Subdivisões das Situações de Operação	503
J.5	Processo de Análise das Situações de Operação.....	508
J.6	Situações Acidentais Complementares.....	512
J.7	Determinação dos Equipamentos Importantes para a Segurança	517
J.8	Qualificação.....	519
J.9	Projeto das Barreiras	520
K	ANÁLISE PROBABILÍSTICA DE SEGURANÇA NUCLEAR.....	524
K.1	Quantificação de uma Análise Probabilística de Segurança.....	525
K.2	Métodos de Quantificação	527
K.3	Análise Probabilística de Segurança Global	529
L	ANÁLISE DE SEGURANÇA DO NAVIO NUCLEAR	530
L.1	Análise Funcional das Prestações	530

SÍNTESE DE DOCTRINA DE SEGURANÇA
PARA PROJETO E OPERAÇÃO DE SUBMARINOS NUCLEARES

L.2	Análise Preliminar de Riscos.....	533
L.3	Análise dos Modos de Falhas, Efeitos e Criticidade.....	536
L.4	Análise por Árvore de Causas	537
L.5	Modelagem por Grafos de Markov e por Redes de Petri.....	538
L.6	Métodos Específicos de Análise de Agressões	539
M	ORGANIZAÇÃO DA RADIOPROTEÇÃO À BORDO.....	541
M.1	Blindagens Radiológicas.....	542
M.2	Delimitação por Zonas	544
M.3	Objetivos Gerais por Categoria de Pessoal.....	545
M.4	Situações Radiológicas Consideradas.....	546
N	DETERMINAÇÃO DA VELOCIDADE DE AFUNDAMENTO DO SNA.....	547
O	ITEMIZAÇÃO DO RELATÓRIO DE ANÁLISE DE SEGURANÇA	548
P	JUSTIFICAÇÃO DE DOSES COM RESPEITO A REQUISITOS DE SEGURANÇA	557
P.1	Parâmetros	557
P.2	Quantificação de Parâmetros.....	558
P.3	Comparação Qualitativa de Parâmetros.....	559
P.4	Objetivos Detalhados.....	559
P.5	Análise Qualitativa de Doses Individuais	560
P.6	Implementação	561
	REFERÊNCIAS BIBLIOGRÁFICAS	563
	APÊNDICES	578
I	BIBLIOGRAFIA COMPLEMENTAR.....	578
II	DADOS GERAIS DOS SUBMARINOS NUCLEARES EXISTENTES NO MUNDO	592

1 INTRODUÇÃO

Neste capítulo inicial será feita uma apresentação global do conteúdo do trabalho, definindo-se o objeto da tese, sua necessidade e interesse ao nível nacional, seu propósito, as limitações do seu escopo e sua organização. O texto principal do Capítulo é complementado por 3 Anexos (A a C) que proporcionam suporte elucidativo aos temas abordados.

1.1 OBJETO

Doutrina. [do latim *doctrina*.] S. f. 1. Conjunto de princípios que servem de base a um sistema religioso, político, filosófico, científico, tecnológico, etc. 2. 3. 4 Opinião de autores. 5. 6. Regra, preceito, norma (HOLANDA, 1983).

A presente tese tem por objeto a síntese de uma Doutrina de Segurança Nuclear aplicável ao “Ciclo de Vida” de um “Submarino Nuclear de Ataque”. A Doutrina de Segurança proposta consiste num conjunto original, consistente e coerente de princípios básicos, critérios gerais de projeto, requisitos específicos para estruturas, componentes e sistemas, e procedimentos de verificação de projeto e de fiscalização da operação, cuja estrutura hierarquizada é representada pela Figura 1.1.

FIGURA 1.1: DOCTRINA DE SEGURANÇA PARA SUBMARINOS NUCLEARES

A doutrina proposta visa portanto permitir uma abordagem racional dos problemas tecnológicos decorrentes do emprego da energia nuclear especificamente na propulsão naval de “Submarinos Nucleares de Ataque”, englobando:

- a proteção da tripulação, do pessoal de apoio logístico em terra e do público em geral, tanto estando o submarino no mar como em porto ou base naval, contra riscos à saúde individual e danos ao meio ambiente decorrentes da emissão, intencional ou acidental, de substâncias radioativas e radiações ionizantes;
- a capacidade de sobrevivência do submarino, não somente com respeito aos riscos estritamente nucleares intrínsecos à “Instalação Propulsora Nuclear”, como também derivados das interações desta instalação com o restante da plataforma-navio e seus sistemas de combate (agressões internas), com o ambiente físico representado pelas áreas marítimas oceânicas e costeiras e as regiões terrestres litorâneas próximas (agressões externas), e com o ambiente tático-operativo naval (agressões de caráter militar).

A aplicação desta doutrina nas diferentes fases do “Ciclo de Vida” do “Submarino Nuclear de Ataque” deverá permitir o “Licenciamento” para operação de sua “Instalação Propulsora Nuclear” pela “Autoridade de Segurança Nuclear” e, dentro das restrições impostas por este processo de licenciamento, a otimização de sua eficiência operativa como meio naval de emprego militar.

1.2 DEFINIÇÕES E CONCEITOS PRELIMINARES

Para fins deste trabalho, considera-se as seguintes definições e conceitos:

“Submarino Nuclear de Ataque SNA” é um submarino de emprego militar dotado de um “Reator a Água Pressurizada” ou “Pressurized Water Reactor PWR”, fonte de energia de sua “Instalação Propulsora Nuclear” (Figura 1.2). Ressalta-se aqui que:

- o termo *nuclear* não possui relação com o sistema de armas do submarino, mas sim com seu sistema de geração de energia; o armamento destes navios é composto basicamente de torpedos lançados por tubos horizontais localizados na proa, podendo entretanto também

ser dotado de mísseis anti-superfície de curto ou médio alcance, lançados pelos próprios tubos de torpedo ou por tubos verticais específicos (CLANCY, 1993);

- a denominação *ataque* refere-se à sua capacidade de efetuar ataques torpédicos ou de mísseis a navios de superfície e a outros submarinos; esta capacidade, aliada à capacidade de operar por longos períodos em áreas oceânicas distantes das bases de apoio em terra (da ordem de 100 dias, autonomia limitada apenas pela capacidade de armazenamento de víveres e resistência psico-física da tripulação), à elevada velocidade (25-35 nós) e submerso a grandes profundidades (300-500m) torna o SNA particularmente bem adaptado à *defesa* das fronteiras marítimas nacionais, especialmente no cumprimento daquela tarefa básica do Poder Naval Brasileiro definida como “negação do uso do mar ao inimigo” (PEREIRA, 1997; SRPM, 1997, 1996, 1990; COSTA, 1997, 1985; FLORES, 1988);
- o reator PWR não é a única fonte de energia potencialmente aplicável à “Instalação Propulsora Nuclear” de um SNA; outros tipos de reatores têm sido propostos, porém o PWR é a opção de projeto largamente dominante nas realizações práticas estando presente em mais de 95% dos submarinos nucleares já construídos, que somam mais de 400 unidades (GUIMARÃES, 1996b; GUIMARÃES, 1991; CROUCH, 1960).

“Reator a Água Pressurizada” ou “Pressurized Water Reactor PWR” (GLASSTONE E SESSONSKE, 1994; DEVRON, 1983) é um reator nuclear que possui as seguintes características básicas (Figura 1.3):

- produção de energia por reações de fissão do núcleo do isótopo de Urânio U-235 por nêutrons térmicos (energia inferior a 0,025eV);
- termalização (moderação) dos nêutrons feita pela mesma água leve que também tem função de fluido de resfriamento (remoção de calor do combustível);
- núcleo combustível e fluido de resfriamento contidos no interior de um envelope estanque de alta integridade (barreira de pressão do “Circuito Primário”);
- barreira de pressão do “Circuito Primário” envolvida por um segundo envelope estanque de alta integridade (“Estrutura de Contenção”);

Além destas características básicas, o reator PWR de propulsão naval de SNA considerado dentro do escopo do presente trabalho possui as seguintes características adicionais:

- potência térmica da ordem de 50-100 MWth;
- combustível cerâmico sólido (UO_2) sob forma de pastilhas planas ou cilíndricas (ROSA DA SILVA, 1989), de baixo enriquecimento no isótopo U-235, i.e. *Low Enrichment Uranium* LEU, com menos de 20% de U-235 em peso do urânio total (LANNING e IPPOLITO, 1989), encamisado por revestimento metálico (aço inoxidável ou ligas de zircônio);
- núcleo combustível formado por elementos do tipo vareta ou do tipo placa (PERROTA, 1990);
- geometria fixa para o combustível e para o fluido de resfriamento, água leve, que também tem função de moderador;

FIGURA 1.2: (LANCY, 1993)

FIGURA 1.3: REATOR DE PROPULSÃO NAVAL PWR TÍPICO

“Instalação Propulsora Nuclear – IPN” baseada em reator PWR (GUIMARÃES, 1996b; DEBAENE, 1994; DE LADONCHAMPS E VERDEAU, 1972) consiste em dois circuitos termohidráulicos em ciclo fechado, utilizando água como fluido de trabalho: “Sistema de Resfriamento do Reator”, onde a água é mantida na fase líquida a temperatura elevada (250-300°C) devido à alta pressão do ciclo (120-160 bar), e “Sistema de Conversão de Energia”, onde a água sofre mudança de fase em um ciclo Rankine (Figura 1.4). Estes circuitos são fisicamente separados, porém acoplados por um trocador de calor do tipo casco-tubos, denominado Gerador de Vapor GV. O Anexo A apresenta e discute as características básicas das IPN navais.

“Sistema de Resfriamento do Reator” ou “Circuito Primário” inclui o Reator, componente mecânico que contém o combustível nuclear físsil, Bombas de Circulação Principais BCP de água de resfriamento, o lado dos tubos dos GV e um Pressurizador PZ. O calor gerado pelas reações nucleares de fissão em cadeia no combustível é transferido ao “Circuito Secundário” pelo Circuito Primário, por meio da circulação da água de resfriamento no interior dos tubos do GV. O ciclo é fechado pelas BCP que retornam a água resfriada no GV ao Reator para ser reaquecida. O circuito possui ainda um PZ que controla as variações de pressão no circuito devidas a desbalanceamentos transitórios entre a energia gerada no reator e a energia removida pelos GV. O conjunto formado pelo Reator, Circuito Primário e as blindagens radiológicas correspondentes é fisicamente arranjado no Compartimento do Reator, segregado do resto do submarino. Este compartimento constitui a “Estrutura de Contenção”, capaz de confinar no seu interior os materiais radioativos contidos no Reator e Circuito Primário mesmo nas mais graves condições acidentais postuladas (Figura 1.5).

CIRCUITO SECUNDÁRIO

CIRCUITO PRIMÁRIO

FIGURA 1.4: INSTALAÇÃO PROPULSORA NUCLEAR TÍPICA (REATOR PWR SEGREGADO, ACIONAMENTO ELÉTRICO DO PROPULSOR)

FIGURA 1.5: COMPARTIMENTO DE REATOR PWR NAVAL TÍPICO

“Circuito Secundário” converte a energia térmica removida do Circuito Primário pela vaporização da água contida no lado do casco dos GV num ciclo Rankine, sem superaquecimento. O vapor saturado produzido pelos GV irá acionar turbinas que convertem a energia térmica em energia mecânica. Esta energia mecânica será então convertida em energia elétrica por geradores acoplados às turbinas, ou será diretamente utilizada, caso as

turbinas sejam diretamente acopladas ao eixo propulsor do submarino, via uma engrenagem redutora. O resfriamento dos condensadores das turbinas é feito pela circulação de água do mar, em ciclo aberto.

“Ciclo de Vida” do submarino é definido como a seqüência de fases que se inicia com o estabelecimento das necessidades militares às quais deverá atender (Requisitos de Estado-Maior REM), seguindo-se com o projeto, fabricação de componentes, construção naval, montagem eletromecânica, comissionamento, períodos de operação, períodos de manutenção, eventuais obras de atualização e modernização, e descomissionamento, esta última marcando o fim de sua vida útil. Conclui-se este ciclo com o desmantelamento do submarino descomissionado e a disposição final de suas partes e do combustível irradiado ao longo de sua vida útil. O Anexo B apresenta e discute os períodos componentes do Ciclo de Vida de um SNA, o perfil de operação a ele associado e os tipos e frequências de transientes operacionais aos quais sua IPN é submetida.

“Autoridade de Segurança Nuclear ASN” é entendida como o organismo estatal que regulamenta e controla as atividades associadas a cada uma das fases do Ciclo de Vida do SNA importantes para a segurança nuclear, analisando e aprovando em diferentes etapas o relatório de análise de segurança da instalação nuclear embarcada, da plataforma-navio e das instalações de apoio logístico em terra, através de um processo técnico-administrativo denominado “Licenciamento de Instalações Nucleares”.

“Processo de Licenciamento” é a missão precípua da ASN. Tem por objetivo assegurar às demais autoridades governamentais que os níveis de segurança nuclear atingidos pelo SNA são socialmente aceitáveis. Essas últimas autoridades representam, em última instância, a própria sociedade. A ASN tem portanto como responsabilidade definir recomendações que especifiquem, a partir dos riscos específicos do SNA:

- modalidades pelas quais devem ser formulados os princípios, critérios e requisitos de segurança nuclear, já a partir da fase inicial do projeto de concepção;
- metodologia a ser seguida pelas organizações responsáveis pelo projeto, construção e operação, de forma que estas exigências sejam efetivamente atendidas.

1.3 NECESSIDADE GERADORA

O Poder Naval Brasileiro deve possuir meios para exercer a dissuasão naval clássica e executar suas quatro tarefas básicas (controlar áreas marítimas, negar o uso do mar ao inimigo, projetar poder sobre terra e contribuir para a dissuasão estratégica) em todos os oceanos em que existam interesses nacionais, de forma a respaldar a ação política externa quando esta assim o exigir (PEREIRA, 1997).

Os submarinos são navios com características especiais, que os distinguem das demais classes de navios de guerra. A principal delas é a ocultação: os inimigos aos quais ele pretende negar o uso ofensivo do mar podem saber que ele está numa determinada área marítima, mas não saberão exatamente onde. Diferentemente das forças de superfície, os submarinos são imunes à detecção por satélite, obrigando seus antagonistas a um esforço e dispêndio considerável de meios navais especializados na luta anti-submarino (navios de superfície e aeronaves) para encontrá-los. Seu emprego é portanto de capital importância numa concepção estratégica para a defesa das fronteiras marítimas brasileiras, próxima e distante (FLORES, 1988).

A incorporação da propulsão nuclear em submarinos de ataque proporciona àqueles meios navais características ímpares de mobilidade, discrição, permanência e poder de combate que confeririam uma capacidade às forças navais brasileiras compatível com as grandes distâncias envolvidas no Teatro de Operações Marítimas nacional. Tais meios navais dariam, portanto, uma fundamental contribuição para a credibilidade do efeito dissuasório e para o efetivo cumprimento das tarefas básicas do Poder Naval Brasileiro.

A aplicação da energia nuclear à propulsão de submarinos militares deve, entretanto, atender aos princípios básicos de proteção e recomendações estabelecidos pela Comissão Internacional de Proteção Radiológica CIPR (ICRP, 1991), que têm aceitação universal:

- I. Justificação: nenhuma prática deve ser adotada se o benefício a ser obtido não for suficientemente superior ao detrimento radiológico que poderia provocar;
- II. Limitação: a exposição de qualquer pessoa às radiações emitidas por fontes radiativas controladas associadas a uma prática justificada deve ser sujeita a limites máximos aceitáveis;

III. Otimização: as doses induzidas por quaisquer fontes radioativas associadas a uma prática justificada e limitada devem ser mantidas tão baixas quanto razoavelmente alcançável, levando-se em conta fatores econômicos e sociais (“*As Low As Reasonable Achievable*” ALARA).

Considerando-se esses princípios básicos de proteção, o SNA nacional deve possuir atributos de eficiência militar que tornem justificável, em termos de defesa nacional, a aplicação da energia nuclear para sua propulsão (Princípio da Justificação), simultaneamente a atributos de segurança nuclear que tornem as conseqüências decorrentes de sua operação limitadas (Princípio da Limitação), em termos de aceitabilidade de riscos sanitários e ambientais pela sociedade brasileira, e tão reduzidas quanto razoavelmente alcançável, levando-se em conta os fatores sociais e econômicos do País (Princípio da Otimização).

A diversidade e a complexidade das interfaces e dos efeitos de realimentação que podem ser identificados entre a IPN e o SNA propriamente dito, tornam necessário que, para garantir sua segurança, o submarino nuclear seja abordado como uma entidade única. Isto quer dizer que o conceito de instalação nuclear não fica restrito à propulsão, mas estende-se a todo o sistema-navio. Este sistema único incorpora os aspectos científicos e tecnológicos, bem como as metodologias e técnicas, ou seja, aquilo que poderia ser resumido como a “cultura”, tanto da engenharia naval, em especial seu ramo de aplicação militar, como da engenharia nuclear, em especial seu ramo de aplicação na geração de energia.

O reconhecimento do navio nuclear como um sistema único, resultado da combinação das “culturas” de dois grandes ramos da engenharia, implica na necessidade das regulamentações para sua segurança incorporarem e sintetizarem todos os aspectos relevantes, tanto para os submarinos militares como para os reatores nucleares de potência estacionários.

Para que o desenvolvimento autóctone de propulsão nuclear no Brasil seja coroado de êxito, torna-se necessário que os organismos responsáveis pelas diversas fases do Ciclo de Vida de um futuro SNA nacional demonstrem e garantam às autoridades navais competentes que seus atributos de eficiência militar tornam sua incorporação à Esquadra nacional justificável e, também à ASN, que seus atributos de segurança nuclear são aceitáveis, i.e. as

consequências de sua operação são limitadas e otimizadas. Estas demonstrações e garantias devem ser dadas antes de submeter o SNA nacional aos riscos externos específicos ao ambiente marítimo e aos riscos operacionais associados ao caráter militar de seu emprego.

Esta necessidade decorre de um imperativo associado à capacitação na obtenção e utilização da energia nuclear e visa minimizar os eventuais riscos tecnológicos, políticos, sociais e financeiros que poderiam acarretar um eventual insucesso no futuro, já durante a operação desta classe de navios de guerra. Para tal é de especial relevância o desenvolvimento prévio de um Protótipo em Terra PROTER para testes de validação e qualificação da IPN do SNA (GUIMARÃES, 1996a).

O Licenciamento de Instalações Nucleares no Brasil é de responsabilidade da Comissão Nacional de Energia Nuclear CNEN, e regulamentado pela Norma Experimental NE-1.04 (CNEN, 1984). Este documento possui um caráter estritamente administrativo-legal, não explicitando os princípios, critérios e requisitos de segurança adotados. De acordo com a norma, estes aspectos técnicos devem ser definidos, em sequência de prioridade, a partir de outras normas CNEN existentes, de normas e recomendações da Agência Internacional de Energia Nuclear AIEA e da base normativa adotada por países com “reconhecida competência técnica no setor nuclear”. As etapas e documentos associados ao processo de licenciamento de instalações nucleares no Brasil é apresentado e discutido pelo Anexo C.

Tendo em vista que o conjunto de normas técnicas da CNEN não é exaustivo e que as normas e recomendações da AIEA têm um caráter muitas vezes genérico, não entrando em detalhes necessários à efetiva verificação de projeto e fiscalização da operação, o licenciamento das instalações nucleares resulta sendo efetuado com base na regulamentação técnica dos EUA, como decorrência do fato da primeira usina nuclear implantada no País, ANGRA-I, ser de procedência americana. A segunda usina nuclear em implantação no País, ANGRA-II, de procedência alemã, tem requerido exceções a esta prática devido a incoerências entre as duas bases normativas estrangeiras. O escopo da norma CNEN de licenciamento de instalações nucleares, além disto, é limitado a instalações “estacionárias”, i.e. exclui as instalações “móveis”, dentre as quais se incluiria a IPN de um SNA.

O caráter “navio”, que impõe às suas IPN condições de funcionamento únicas, muito distintas daquelas impostas às instalações estacionárias, e o caráter “militar” da instalação, que conduz a dúvidas de ordem administrativa e legal sobre o organismo estatal ao qual caberia efetivamente as funções de ASN, justificam a exclusão das IPN de SNA da atual norma de licenciamento em vigor.

Considerando-se, entretanto, o caráter pioneiro do desenvolvimento de SNA no Brasil associado ao fato de uma regulamentação específica para esta aplicação nunca ter sido elaborada no País, certamente nenhuma organização nacional se encontra hoje tecnicamente preparada para cumprir a função de ASN para IPN. Além disto, não seria possível, considerando o caráter reservado das informações disponíveis sobre a propulsão nuclear naval de emprego militar nos poucos países onde ela foi desenvolvida e é atualmente utilizada (EUA, Rússia, França, Grã-Bretanha e China), adotar regulamentações estrangeiras ou internacionais, tal como vem sendo feito no País para as demais instalações nucleares estacionárias.

Conclui-se, portanto, que existe a necessidade, em especial para a ASN que terá jurisdição sobre as IPN de SNA, de desenvolvimento de estudos e de capacitação de pessoal para tratar dos diversos problemas científicos e tecnológicos associados à elaboração e à efetiva verificação do atendimento de regulamentações adaptadas à utilização eficiente e segura da energia nuclear para a propulsão de submarinos militares.

1.4 ESCOPO

O presente trabalho consiste na elaboração de uma proposta de Doutrina de Segurança Nuclear a ser aplicada ao desenvolvimento futuro de SNA no Brasil, como contribuição para o atendimento da necessidade identificada anteriormente. Aqueles aspectos de segurança não especificamente nucleares, ou seja, comuns aos submarinos militares dotados de propulsão convencional diesel-elétrica, não serão aqui abordados, já tendo sido tratados pela dissertação de mestrado em engenharia naval do autor (GUIMARÃES, 1991). Aqueles aspectos de projeto e operação da IPN que não são especificamente associados à segurança

também não serão aqui abordados, pois já foram tratados pelo *projet de fin d'études de ingénieur atomique* do autor (GUIMARÃES, 1993).

As estruturas, sistemas e componentes do submarino são abordados somente na medida em que tenham importância para a segurança nuclear. O trabalho visa, particularmente, a fase de projeto do Ciclo de Vida do SNA. Os princípios, critérios, requisitos e procedimentos desenvolvidos são também aplicáveis às demais fases que, entretanto, implicam requisitos específicos adicionais que não serão aqui abordados. Por esta limitação, os requisitos de operação, manutenção, inspeções e descomissionamento são tratados somente na medida que afetam direta ou indiretamente a fase de projeto. O gerenciamento a longo prazo do combustível irradiado ao longo da vida útil do submarino não é tratado por considerar-se que esta fase não é específica à propulsão nuclear, inserindo-se num contexto nacional mais amplo que engloba todos os reatores em operação no País.

Os princípios básicos, critérios gerais, requisitos funcionais e procedimentos de verificação de segurança são desenvolvidos considerando-se as condições normais de paz, pois somente nestas condições pode-se avaliar *a priori* o nível de demanda social por segurança (ou seu equivalente, o nível de aceitabilidade social de riscos). Tendo em vista a indeterminação das hipóteses de guerra ou conflito grave e a diversidade de variáveis psico-sociais que cada uma poderia implicar, este nível somente poderia ser avaliado *a posteriori*, i.e. após ou na iminência de ocorrência real de uma das condições hipotéticas. Estes fatos tornariam o desenvolvimento prévio de uma doutrina de segurança de pouca utilidade prática face a pouca duração e intensidade previstas para os conflitos plausíveis no atual quadro geopolítico mundial.

1.5 PROPÓSITO

A doutrina de segurança para submarinos nucleares proposta tem como propósito subsidiar a elaboração de uma estrutura de regulamentação que permita à ASN que tiver jurisdição sobre estas instalações examinar e julgar sobre a adequabilidade das disposições tomadas nas diferentes fases do seu ciclo de vida pelos organismos responsáveis, através de

um processo formal de licenciamento nuclear compatível com suas peculiaridades técnicas e operacionais.

O ponto focal destas peculiaridades, que constitui a base de desenvolvimento da doutrina proposta, reside na otimização do conjugado Disponibilidade x Seguridade. Com efeito, as bases normativas para projeto e operação de sistemas militares navais privilegiam a Disponibilidade como atributo fundamental para assegurar o sucesso da missão. Já as bases normativas para projeto e operação de sistemas nucleares dão prioridade a Seguridade.

Um SNA, que é um sistema militar e nuclear, deverá então possuir estes dois atributos de forma balanceada, o primeiro dentro da filosofia do Princípio da Justificação e o segundo dentro da filosofia do Princípio da Limitação. A filosofia do Princípio da Otimização deverá então ser aplicada considerando que a Segurança Nuclear não deverá comprometer a Segurança Naval. Isto decorre da constatação que, se esta última for comprometida, a primeira também fatalmente o será, e eventualmente de modo ainda mais grave, pois a segurança da instalação nuclear depende, em grande parte, da segurança do próprio submarino.

A doutrina proposta pretende portanto incorporar e sintetizar os aspectos relevantes, tanto da engenharia naval, como da engenharia nuclear, tendo como fundamento a teoria de Segurança de Funcionamento de Sistemas Industriais – SDFSI (VILLEMEUR, 1988) ou *Reliability, Availability, Maintainability and Safety - RAMS*, no jargão técnico anglo-saxão (VILLEMEUR, 1992). Ela é desenvolvida com base em princípios, critérios, requisitos e procedimentos, tanto de engenharia nuclear e como de engenharia naval, bem estabelecidos e universalmente aceitos.

O interesse da proposição desta doutrina está associado à adaptação, combinação e compatibilização dos conceitos, técnicas e práticas destas duas áreas da engenharia, gerando um conjunto que se pretende consistente e coerente e que se presume necessário, mas não disponível no País, como fundamento à implementação de uma futura regulamentação para licenciamento nuclear específica às IPN de SNA.

A doutrina de segurança proposta é marcadamente influenciada pelos “mandamentos” estabelecidos por Hyman George Rickover, Almirante-de-Esquadra engenheiro da marinha dos EUA (DUNCAN, 1990), pioneiro mundial não só da propulsão nuclear naval, como também da própria aplicação da energia nuclear para a produção de potência elétrica, os quais nos permitiremos aqui reproduzir:

- I. *“Não comissionar o navio enquanto houver equipamentos, sistemas ou procedimentos de operação classificados como "em desenvolvimento", ou seja, cujos critérios de projeto não tenham sido homologados experimentalmente, cujos protótipos não tenham sido testados em condições realísticas de serviço e com os quais a tripulação não esteja ainda plenamente familiarizada;*
- II. *Assegurar graus de redundância adequados ao projeto de sistemas, de forma que a instalação possa suportar, sem danos ao navio ou à tripulação, falhas de equipamentos e componentes, falhas estas que inevitavelmente irão ocorrer ao longo da vida operativa do navio;*
- III. *Minimizar a necessidade de ação dos operadores durante os transientes normais de operação. Se a instalação for inerentemente estável, o operador estará mais capacitado a responder satisfatoriamente aos transientes anormais e emergências;*
- IV. *Simplificar o projeto de sistemas de forma que, no caso de falha do controle automático, a atuação do operador em tempo adequado seja garantida;*
- V. *Selecionar somente materiais homologados experimentalmente para o tipo de aplicação desejada e, na medida do possível, aqueles que possuem as maiores margens de segurança com relação a eventuais deficiências passíveis de ocorrerem nas fases de aquisição, fabricação, instalação e manutenção;*
- VI. *Ao longo do processo de desenvolvimento, realizar extensivos testes de durabilidade (vida útil) para os componentes de sistemas críticos para a segurança do reator, de forma a garantir a adequação do projeto, em antecipação à fase operacional;*
- VII. *Quaisquer modificações na instalação devem ser implantadas usando protótipos em terra plenamente similares àqueles que serão utilizados nas instalações embarcadas. As instalações protótipo em terra devem ser submetidas aos mesmos transientes esperados para a instalação embarcada, de forma que os eventuais problemas possam ser identificados e resolvidos previamente à operação no mar;*
- VIII. *Treinar os operadores nos reatores protótipos em terra. Os simuladores não são aceitáveis como único meio de treinamento antes da operação no mar;*
- IX. *Verificar o projeto da instalação propulsora por meio de extensivas análises teóricas de confiabilidade e de acidentes, validação experimental obtida através de ensaios que busquem máxima similaridade com a operação real, e modelos*

físicos em escala reduzida ou, para as regiões mais críticas, modelos físicos (mockup) em escala natural 1:1;

- X. *Utilizar pessoal especialmente treinado para efetuar extensivas inspeções durante a construção. Só aceitar equipamentos que atendam rigorosamente aos requisitos das especificações; e*
- XI. *O projeto, construção e operação da instalação devem enfatizar a prevenção de acidentes e não somente garantir a segurança do navio e da tripulação após a ocorrência destes acidentes.”*

1.6 ORGANIZAÇÃO

Neste capítulo 1 foi feita uma apresentação global do conteúdo do trabalho, definindo-se o objeto da tese, sua necessidade e interesse ao nível nacional, seu propósito e as limitações do seu escopo.

A partir da noção fundamental de segurança como percepção social de riscos, no Capítulo 2 serão discutidos o detalhamento, as interpretações, as derivações e as aplicações tecnológicas deste conceito primário em três contextos específicos:

- a disciplina de SDFSI/RAMS, de aplicação geral aos sistemas industriais, dentro dos quais se incluem instalações nucleares, navios e submarinos;
- a Segurança de Instalações Nucleares “Estacionárias”, em especial de reatores de potência eletronucleares, segmento industrial que se notabiliza pelo desenvolvimento ao longo dos últimos 40 anos de uma doutrina de segurança específica a partir da qual a SDFSI/RAMS moderna tem suas origens (juntamente com a Segurança de Aviação, que não será aqui abordada) e que, com necessárias adaptações, é aplicável às IPN;
- a Segurança Naval, entendida aqui como a Segurança Marítima (segurança da navegação, salvaguarda da vida humana no mar), típica das condições normais de paz, e a Capacidade de Sobrevivência (*Survivability*), que é típica das condições de guerra ou conflito e integra os aspectos de suscetibilidade e de vulnerabilidade de um navio a ameaças externas, sendo diretamente aplicável, dentro de suas particularidades, aos SNA;

Conclui-se o Capítulo 2 com uma primeira abordagem global à Segurança da Propulsão Nuclear, sintetizando os conceitos e aplicações da segurança nos três contextos previamente discutidos. Com o objetivo de tornar o texto principal o mais fluente e conciso possível, este

capítulo é complementado por uma série de anexos que são suportes elucidativos considerados de relevância para a compreensão dos temas abordados.

Os Princípios Básicos de Segurança Nuclear são então adaptados às particularidades da propulsão naval de SNA no Capítulo 3. Como “Princípios” entende-se diretrizes qualitativas que orientam como os objetivos da segurança nuclear podem ser atingidos. Em cada caso, os princípios são enunciados curtos, seguidos de comentários sobre suas razões e sua importância.

No Capítulo 4 são propostos Critérios Gerais de Segurança para o projeto da IPN e de suas interfaces com a plataforma-navio do SNA. Como “Critérios Gerais” entende-se diretrizes quantitativas que orientam o desenvolvimento do projeto integrado do conjunto de sistemas que compõem o SNA. São usados para verificar sua adequação aos princípios qualitativos apresentados pelo Capítulo 3.

Os requisitos específicos de segurança aplicáveis ao projeto de estruturas, componentes e sistemas da IPN e da plataforma-navio do SNA derivados dos critérios gerais são então desenvolvidos no Capítulo 5. Estes “Requisitos Específicos” são entendidos como regras quantitativas que determinam o projeto individual de cada parte que compõe o SNA. São usados para garantir o atendimento aos critérios gerais aplicados ao conjunto dos sistemas do submarino, apresentados pelo Capítulo 4.

No Capítulo 6 são finalmente propostas diretrizes para o estabelecimento dos procedimentos de análise e verificação da segurança do projeto e da fiscalização da construção e operação associados à regulamentação do “Processo de Licenciamento” dos SNA. São ainda propostos e discutidos o conteúdo e a organização do Relatório de Análise de Segurança RAS, documento básico deste processo, concluindo assim a estrutura da Doutrina de Segurança proposta.

O Capítulo 7 apresenta as conclusões globais do trabalho, fundamentadas nas proposições e respectivas discussões feitas nos capítulos precedentes.

Seguem-se 16 anexos, referenciados ao longo dos capítulos, que têm como objetivo aprofundar alguns aspectos considerados particularmente relevantes para o entendimento do

texto e, concomitantemente, fundamentar os princípios, critérios, requisitos e procedimentos propostos, e as Referências Bibliográficas dos Capítulos e dos Anexos. Sob forma de apêndices, são ainda apresentadas: uma bibliografia complementar sobre os três contextos de aplicação da segurança discutidos no Capítulo 2, incluindo os artigos técnicos elaborados pelo autor ao longo do desenvolvimento da presente tese, publicados ou propostos para publicação em anais de congressos, simpósios, seminários e periódicos; e uma tabela de dados gerais sobre os submarinos nucleares existentes no mundo.

Apesar do autor ser oficial da Marinha do Brasil, cumpre ressaltar que a tese foi desenvolvida por moto próprio, sendo as opiniões nela expressas de caráter estritamente pessoal, não constituindo, sob nenhuma hipótese, uma posição institucional sobre os temas abordados.

2 CONCEITOS E MÉTODOS

A partir da noção fundamental de segurança como percepção social de riscos, no presente Capítulo serão discutidos o detalhamento, as interpretações, as derivações e as aplicações tecnológicas deste conceito básico em três contextos específicos:

- a disciplina de SDFSI/RAMS, de aplicação geral aos sistemas industriais, dentro dos quais se incluem instalações nucleares, navios e submarinos;
- a Segurança de Instalações Nucleares “Estacionárias”, em especial de reatores de potência eletronucleares, segmento industrial que se notabiliza pelo desenvolvimento ao longo dos últimos 40 anos de uma doutrina de segurança específica a partir da qual a SDFSI/RAMS moderna tem suas origens e que, com necessárias adaptações, é aplicável às IPN;
- a Segurança Naval, entendida aqui como a Segurança Marítima, típica das condições normais de paz, e a Capacidade de Sobrevivência (*Survivability*), que é típica das condições de guerra ou conflito e integra os aspectos de suscetibilidade e de vulnerabilidade de um navio a ameaças externas, sendo diretamente aplicável, dentro de suas particularidades, aos SNA;

Conclui-se este Capítulo com uma primeira abordagem global à Segurança da Propulsão Nuclear, sintetizando os conceitos e aplicações da segurança nos três contextos previamente discutidos. Os conceitos e métodos apresentados e discutidos ao longo das 4 seções que compõem o presente Capítulo constituirão a base sobre a qual serão desenvolvidos os Princípios, Critérios e Requisitos que formam o núcleo da Doutrina de Segurança que a presente tese se propõe a sintetizar

2.1 SEGURANÇA DE SISTEMAS INDUSTRIAIS

Nesta seção será discutido o contexto de aplicação da disciplina de SDFSI/RAMS como resposta técnica às demandas sociais por segurança, serão definidos e formulados matematicamente seus conceitos básicos e será finalmente discutida sua aplicação prática sob a forma do Gerenciamento de Riscos decorrentes de uma instalação industrial ao longo das fases de seu Ciclo de Vida. Este gerenciamento é baseado no estabelecimento prévio de

limites de riscos individuais e coletivos para o sistema e em procedimentos para análise do sistema e para alocação das ações de segurança a serem implementadas.

2.1.1 CONTEXTO DE APLICAÇÃO

O progresso material possibilitado pelo desenvolvimento da sociedade industrial, dita “de consumo”, nos últimos 20 anos tem conduzido a uma série de fenômenos sociais vulgarmente denominados em seu conjunto como “pós-modernidade”.

Um destes fenômenos é caracterizado por um aumento significativo das demandas sociais por segurança, numa busca de ideais utópicos de integridade física do homem e de seu meio ambiente. Estas demandas se agrupam em torno de bandeiras político-ideológicas como “consciência ecológica” e “direitos do consumidor”.

Em um tal ambiente psico-social, os sistemas industriais em geral são identificados como graves ameaças ao indivíduo, à sociedade e ao meio ambiente, sendo permanentemente assediados por grupos de pressão que requerem deles um nível de segurança de funcionamento indefinidamente crescente, esquecendo-se estes grupos muitas vezes de que são estes mesmos sistemas que provêem o conforto material que permite a própria colocação de suas reivindicações.

Os técnicos responsáveis pelo projeto, construção e operação dos sistemas industriais são freqüentemente surpreendidos pelos severos questionamentos que a sociedade faz de suas atividades, demonstrando-se muitas vezes incapazes de fornecer elementos racionais para uma negociação social do nível de segurança objetivo para suas instalações. Neste contexto, as instalações nucleares são particularmente percebidas pela sociedade “pós-moderna”, ecológica e higiênica, como verdadeiros “cavaleiros do apocalipse”, ocupando um lugar destacado no inconsciente individual e coletivo e tornando-se portanto alvos preferenciais de assédio por grupos de pressão política.

Estes fatos geram a necessidade de estabelecimento de doutrina de gerenciamento da segurança aplicável a todos os sistemas industriais, que tornem coerentes as abordagens particulares a cada setor. Na ausência desta doutrina, os diferentes técnicos tendem a abordar a segurança de suas instalações de maneiras contraditórias: “minimalista” ou

“maximalista”. A abordagem “minimalista” é evidentemente irresponsável pois os sistemas industriais implicam, em geral, riscos não desprezíveis. A abordagem “maximalista”, por outro lado, conduz a alocações irracionais e injustificadas de recursos, com prejuízo para própria sociedade, pois o custo das ações de segurança cresce desproporcionalmente às reduções de riscos obtidas, podendo vir a comprometer o atendimento aos próprios objetivos (ou “missão”) do sistema.

2.1.2 DEFINIÇÃO DE CONCEITOS

Identifica-se as seguintes definições vernáculas gerais para ‘Segurança’ e para os principais conceitos a ela associados (HOLANDA, 1983):

Segurança. *S. f. 1. ... 2. Estado, qualidade ou condição de **seguro**. 3. Condição daquilo ou daquele em que se pode confiar 4. ...*

Seguro. *[do latim securu] Adj. 1. Livre de **perigo** 2. Livre de **risco**; protegido, acautelado, garantido 3. ...*

Perigo *[do latim periculu] S.m. 1. Circunstância que prenuncia um mal para alguém ou para alguma coisa 2. Aquilo que provoca tal circunstância; **risco** 3. Estado ou situação que inspira cuidado; **gravidade** 4. Situação de fato da qual decorre o temor de uma lesão física ou moral a uma pessoa ou uma ofensa aos direitos dela.*

Risco *[do latim riscu] S. m. 1. Perigo ou possibilidade de **perigo** 2. Possibilidade de perda ou de responsabilidade por danos.*

Gravidade *[do latim gravitate] S. f. 1. Qualidade de **grave** 2. ... 3. Intensidade, profundidade 4. Circunstância perigosa 5. ...*

Grave *[do latim grave] 1. Sujeito à ação da **gravidade** 2. Importante, sério, ponderoso 3. ... 4. ... 5. Intenso, vivo, profundo 6. Doloroso, penoso 7. ... 8. Suscetível de conseqüências sérias, trágicas 9. ...*

Seguridade *[do fr. Sécurité ou do inglês Security] S. f. Conjunto de medidas, providências, normas e leis que visam proporcionar ao corpo social e a cada indivíduo o maior grau possível de garantia, sob os aspectos econômico, social, cultural, moral e sanitário.*

Com base nestes conceitos gerais, serão adotadas as seguintes definições vernáculas específicas ao objeto no presente trabalho, que serão em seguida transpostas para uma formulação matemática:

“Perigo”: circunstância ou situação determinada que potencialmente poderia ocorrer ao longo do Ciclo de Vida de um “Sistema Industrial” e da qual decorreriam conseqüências indesejáveis cuja “Gravidade” é considerada pelos grupos sociais afetados como intolerável.

“Gravidade”: intensidade do impacto social e econômico das consequências indesejáveis de um Perigo.

“Sistema Industrial” conjunto determinado de elementos discretos interrelacionados ou em interação com o objetivo de executar uma missão de natureza tecnológica; as partes de um sistema serão hierarquizadas no presente trabalho pelas seguintes relações inclusivas :
 $(\text{SISTEMA}) \subset (\text{SUB-SISTEMA}) \subset (\text{SISTEMA ELEMENTAR}) \subset (\text{COMPONENTE}) \subset (\text{ITEM})$

O impacto da Gravidade de um Perigo decorrente de um Sistema Industrial incide potencialmente sobre a saúde física e mental de seres humanos, tanto ao nível individual como ao coletivo, sobre a integridade de propriedades e bens públicos e privados, e sobre o equilíbrio dos eco-sistemas do meio ambiente local, regional, nacional e global. No Anexo D são apresentados os diferentes aspectos que caracterizam um Sistema Industrial e discutidas as incidências dos Perigos associados. O Anexo D discute ainda, em particular, os Perigos decorrentes dos efeitos biológicos das radiações ionizantes, de interesse específico para o presente trabalho.

“Evento Indesejado”: evento inicializador de um “Cenário Acidental”.

“Cenário Acidental”: sequência lógica de eventos que, a partir de um Evento Indesejado, conduz o Sistema Industrial a um estado de Perigo.

Os Eventos Indesejados e os Cenários Acidentais decorrentes estarão sempre diretamente associados à ocorrência de “Falhas” do sistema que implicam na interrupção de sua capacidade em atender funções que lhe são requisitadas. A ocorrência de uma Falha leva o sistema a um “Estado de Pane”. A “Causa de Falha” são circunstâncias ligadas ao projeto, fabricação ou emprego do sistema que implicam numa Falha. O “Modo de Falha” é constituído pelos efeitos pelo qual uma Falha é observada. Estes quatro conceitos são definidos e discutidos em maior profundidade pelo Anexo E.

“Risco”: possibilidade, dentro de um período de tempo determinado e sob condições iniciais pré-definidas, de ocorrência de um Cenário Acidental.

“Segurança”: possibilidade, dentro de um período de tempo determinado e sob condições iniciais pré-definidas, de não ocorrência de um Cenário Acidental.

A possibilidade de ocorrência de um Cenário Acidental é avaliada em termos objetivos por uma Probabilidade. A aplicação da Teoria das Probabilidades em SDFSI/RAMS inclui entretanto alguns aspectos específicos que são discutidos no Anexo F, em especial o conceito de “Probabilidade Subjetiva” ou “Verossimilhança”.

“Risco Objetivo”: valor esperado da Gravidade dos Perigos decorrentes do funcionamento de um Sistema Industrial (expectância ou esperança probabilística, i.e. produto da Probabilidade pela Gravidade), sob condições pré-definidas e durante um intervalo de tempo limitado; é determinado objetivamente pelas técnicas e métodos da SDFSI/RAMS.

“Risco Subjetivo”: expectativa de conseqüências indesejáveis decorrentes do funcionamento de um Sistema Industrial, determinada pela “Percepção de Riscos” subjetiva de indivíduos e coletividades acerca da Probabilidade e a Gravidade dos Perigos dele decorrentes.

“Percepção de Riscos”: conjunto de fenômenos de natureza sociológica e psicológica que criam uma hierarquia de Riscos Subjetivos, particular a cada indivíduo e a cada grupo social.

A hierarquia de Riscos Subjetivos (IPSN, 1994) não possui relação lógica com aquela derivada das formulações empregadas para determinação dos Riscos Objetivos.

A Percepção de Riscos coletiva (ou social) tende a avaliar os Riscos Subjetivos superestimando a Gravidade e subestimando as Probabilidades. Considerando-se dois Riscos Objetivos idênticos, a Percepção de Riscos coletiva tende portanto à aversão ao risco com maior Gravidade, ainda que tenha pequena probabilidade (acidentes em instalações nucleares, por exemplo), e ao conformismo ao risco com menor Gravidade, ainda que tenha alta probabilidade (acidentes rodoviários, por exemplo).

A percepção individual, por sua vez, é influenciada pela avaliação ao nível psicológico e nem sempre racional quanto aos benefícios e Riscos provenientes da atividade perigosa em questão. Deve aqui ser feita uma distinção entre dois tipos de riscos ao nível individual:

“Riscos Voluntários”: aqueles incorridos por livre e espontânea vontade de um indivíduo e dos quais ele julga auferir benefícios diretos tais que o impacto dos riscos associados são pouco considerados (atividades profissionais, uso de meios de transportes, prática de esportes e atividades de lazer, tratamentos médicos, tabagismo, por exemplo).

“Riscos Involuntários”: aqueles impostos a um indivíduo sem consulta prévia e dos quais ele julga auferir poucos ou mesmo nenhum benefício direto, nos quais o impacto dos riscos associados são considerados com maior intensidade (instalações industriais, alimentação, pesquisa científica e tecnológica, atividades militares, por exemplo).

A Percepção de Riscos individual avalia os Riscos Voluntários sob uma ótica totalmente distinta daquela usada para avaliar os Riscos Involuntários. Tal constatação, cuja explicação foge do escopo do presente trabalho, torna sem sentido qualquer hierarquização, ao nível individual, por exemplo, entre o risco do transporte rodoviário e o da produção de energia nuclear. O primeiro é objetivamente muito mais elevado do que o segundo, sendo porém tipicamente voluntário.

Cumpram ainda ressaltar que a hierarquia de Riscos derivada da Percepção Social e da Percepção Individual nem sempre são coerentes entre si. Isto deriva do fenômeno sociológico bem conhecido de que o homem tem um comportamento em coletividade diferente daquele que tem individualmente.

“Seguridade”: conjunto de ações técnicas tomadas ao longo do Ciclo de Vida de um Sistema Industrial, enquadradas dentro da disciplina de “SDFSI/RAMS”, que visam proporcionar à sociedade e a cada indivíduo um nível de Segurança tão elevado (ou um nível de Risco tão reduzido) quanto razoavelmente alcançável, levando-se em conta fatores sociais e econômicos.

“Risco Potencial”: Risco Objetivo determinado para um sistema industrial sem serem consideradas as ações técnicas de Seguridade efetivamente tomadas ao longo do seu Ciclo de Vida;

“Risco Residual”: Risco Objetivo determinado para um sistema industrial considerando-se as ações técnicas de Seguridade efetivamente tomadas ao longo do seu Ciclo de Vida.

“Risco Tolerável”: Risco Subjetivo determinado a priori com base na filosofia dos Princípios da Justificação e da Limitação da proteção radiológica (ICRP, 1991), independentemente das características específicas de um sistema industrial particular; a justificação e a limitação não

necessariamente restringem-se às conseqüências radiológicas, podendo ser estendida aos demais tipos de conseqüências.

“Risco Aceitável”: Risco Subjetivo determinado a posteriori com base na filosofia do Princípio da Otimização ou ALARA da proteção radiológica (ICRP, 1991), que depende das características específicas de um sistema industrial particular; a filosofia de otimização não necessariamente restringe-se às conseqüências radiológicas, podendo ser estendida aos demais tipos de conseqüências.

“Gerenciamento de Riscos”: aplicação prática da Seguridade que visa tornar os Riscos Objetivos Residuais de um Sistema Industrial em Riscos Subjetivos Aceitáveis ao nível social e individual.

A condição teórica de “Segurança Absoluta” ou de “Risco Zero” para sistemas industriais, i.e. a certeza da impossibilidade de um Perigo tornar-se real é uma utopia, pois ao desenvolvimento de todos os processos físicos, químicos e humanos atuantes nas fases do Ciclo de Vida das instalações estão associadas margens de incerteza decorrentes do caráter aleatório intrínseco tanto à natureza como ao próprio homem.

Tendo em vista esta realidade, o Gerenciamento de Riscos, dos quais a disciplina genérica de “SDFS/IRAMS” e a Doutrina de Segurança específica ao Sistema Industrial de interesse constituem as ferramentas básicas, deverá preconizar e garantir o cumprimento de ações de Seguridade que tornem, numa primeira instância, o Risco Objetivo Potencial de um Sistema Industrial inferior ao limite de Risco Subjetivo Tolerável. Numa segunda instância, as ações de Seguridade devem ser otimizadas no sentido de tornarem o Risco Objetivo Residual deste Sistema Industrial inferior ao limite de Risco Subjetivo Aceitável (HSE, 1988). Denomina-se a condição prática decorrente destas ações de “Segurança Objetiva”, i.e. aquela em que os riscos foram justificados (Princípio da Justificação), limitados (Princípio da Limitação) e otimizados (Princípio da Otimização).

“SDFS/IRAMS”: num sentido amplo, constitui a “Ciência das Falhas”, i.e. identificação, avaliação, previsão e controle de Falhas de um Sistema Industrial; num sentido estrito, é entendida como a capacidade de um sistema cumprir com sucesso seus objetivos precípuos

ou “missão”, sem que ocorram Eventos Indesejados; além do conceito de Seguridade, engloba os conceitos de Confiabilidade, Manutibilidade e Disponibilidade.

“Confiabilidade”: capacidade de um sistema cumprir uma função requerida, dentro de condições preestabelecidas, durante um período de tempo determinado; pode ser avaliada seja como “Confiabilidade Operacional”, resultante da observação e da análise estatística do comportamento de sistemas idênticos dentro de condições pré-definidas, ou como “Confiabilidade Extrapolada”, que resulta de uma extensão, feita com base em hipóteses de extrapolação ou interpolação, da Confiabilidade Operacional de uma entidade para intervalos de tempo ou condições diferentes, ou ainda como “Confiabilidade Previsional” (ou “Prevista”), que estima a confiabilidade futura de um sistema a partir de considerações sobre seu projeto e sobre a Confiabilidade Operacional e Extrapolada de seus componentes.

“Manutibilidade”: capacidade de um sistema ser mantido no, ou restabelecido ao estado de cumprir uma função requisitada, quando atividades de manutenção são realizadas dentro de condições preestabelecidas, seguindo um conjunto de procedimentos e meios previamente prescritos; estas atividades podem ser de “Manutenção Preventiva”, realizadas segundo um planejamento preestabelecido, baseado no histórico de operação do sistema, visando evitar a ocorrência de uma falha, de “Manutenção Preditiva”, realizadas no momento em que uma variável de processo do sistema monitorada atinge um valor crítico preestabelecido, visando restabelecer o funcionamento normal antes que o mesmo se degrade a um nível de Falha, e de “Manutenção Corretiva” (ou “Reparo”), realizadas após a ocorrência de uma Falha, visando restabelecer suas condições de funcionamento normal.

“Disponibilidade”: capacidade de um sistema estar, num instante determinado e dentro de condições preestabelecidas, em estado de cumprir uma função requisitada; pode ser avaliada como: “Disponibilidade Instantânea” (ou “Imediata”), que corresponde à definição propriamente dita, sendo condicionada pela Confiabilidade e permitindo a um sistema evitar um Perigo; “Disponibilidade Potencial” (“Prevista”, “Contínua” ou “Estatística”), que corresponde à capacidade do sistema funcionar de modo contínuo durante um intervalo de tempo determinado, considerando seu estado inicial, condicionada também pela Manutibilidade; e “Disponibilidade Pós-Acidental”, correspondendo à Capacidade de

Sobrevivência do sistema, i.e. à capacidade do sistema continuar a desempenhar suas funções, ainda que de forma degradada ou parcial, após uma Falha Grave que tenha afetado algumas de suas partes.

A relativamente recente estruturação da disciplina de SDFSIRAMS (VILLEMEUR, 1988, 1992) tem fornecido aos responsáveis pelas fases do Ciclo de Vida dos sistemas industriais uma base teórica para o desenvolvimento de doutrinas específicas de segurança e procedimentos práticos para um efetivo gerenciamento de riscos. Os objetivos da SDFSIRAMS podem ser representados graficamente pela Figura 2.1. O Anexo G apresenta e discute em maior profundidade os conceitos e métodos da SDFSIRAMS.

FIGURA 2.1: SEGURANÇA DE FUNCIONAMENTO DE SISTEMAS

Nas aplicações práticas da SDFSI/RAMS a sistemas industriais reais, podem ocorrer conflitos entre requisitos associados aos seus quatro conceitos básicos. O Anexo G discute exemplos destes conflitos. Eles deverão ser resolvidos pelo Gerenciamento de Riscos através de soluções de compromisso obtidas através de um processo de otimização. Para sistemas em que existam Cenários Acidentais associados ao seu funcionamento intempestivo, por exemplo, ocorrem conflitos entre a Confiabilidade e a Seguridade. Requisitos de Seguridade que impliquem em desligamento automático de um sistema quando forem atingidos valores limites para variáveis críticas de processo podem entrar em conflito com requisitos de Disponibilidade.

Uma discussão da otimização do conjugado Disponibilidade x Seguridade no caso da propulsão nuclear, ponto focal da aplicação do gerenciamento de riscos ao Ciclo de Vida de um SNA, é apresentada por (GUIMARÃES, 1997a).

2.1.3 FORMULAÇÃO DE PARÂMETROS

As definições previamente apresentadas devem ser formuladas em termos matemáticos para permitir a avaliação quantitativa dos parâmetros de segurança de um sistema, essencial para um efetivo gerenciamento de riscos.

Sejam:	Ω	Espaço de estados do Sistema Industrial
	$\Omega_i i=1, I$	Estados finais decorrentes dos Cenários Acidentais do Sistema Industrial, enumerados de $i=1$ a I , e onde $\Omega_i \supset \Omega$
	$C_j j=1, J$	Tipos de conseqüências indesejadas que estão associadas ao estado Ω_i , enumeradas de $j=1$ a J
	G_{ij}	Gravidade da conseqüência C_j para o estado Ω_i
	$\varepsilon_{in} n=1, N$	Eventos Indesejados que inicializam um Cenário Acidental do Sistema Industrial, enumerados de $n=1$ a N para cada estado Ω_i .

O Perigo Π decorrente do funcionamento do Sistema Industrial no seu espaço de estados Ω será formulado então pela expressão que se segue, como o somatório das

gravidades G_{ij} dos estados acidentais Ω_i , considerando todas os tipos de conseqüências C_j deles decorrente.

$$\Pi = [\sum_j (\sum_i G_{ij})] \quad [2.1]$$

O dimensional do Perigo Π é o mesmo das Gravidades G_{ij} que avaliam quantitativamente as conseqüências de diferentes naturezas $\{C_j\}$. Conclui-se então que, para medir-se Π é necessário normalizar-se as Gravidades numa mesma base dimensional. Conforme discutido no Anexo C, as potenciais conseqüências indesejáveis de um Sistema Industrial possuem diversas incidências sobre seres humanos, eco-sistemas, bens e propriedades, o que torna tal tarefa de normalização particularmente complexa, dificultando a avaliação de Π pela expressão [2.1].

O procedimento convencional para avaliação quantitativa de Π é reduzir-se cada uma das Gravidades a uma base monetária (DREICER, 1995; LEFAURE, 1994; JONES LEE, 1989; ICRP, 1983; SHRADER-FRECHETTE, 1985). Este procedimento, entretanto, é vulnerável a críticas de ordem ética e moral quando aplicado a valoração da saúde ou de perdas humanas.

Por outro lado, o conjunto $\{\Omega_i\}$ dos estados finais dos Cenário Acidentais verossímeis de um Sistema Industrial, apesar de ser finito, no caso geral é não-enumerável (vide Anexo E), o que constitui uma outra dificuldade para avaliação de Π pela expressão [2.1].

A quantificação de Π feita para um único Ω_i e para uma única classe de conseqüências C_j , seria dada pela expressão abaixo:

$$\Pi = G_{ij} \big|_{i=1, j=1} = g \quad [2.2]$$

A “Função Densidade de Probabilidade FDP” p do Evento Indesejado ε_{in} é determinada pela expressão a seguir, como o valor limite x_n da “Função Repartição (ou Distribuição) de Probabilidade FRP” P de uma variável aleatória X_n que caracteriza sua ocorrência durante um intervalo de tempo $t = \{0, T\}$. Note-se que a FRP de X_n

corresponde a integral da FDP de X_n . O Anexo F discute em maior profundidade as propriedades e relações entre estas funções.

$$p(\varepsilon_{in})|_{0,T} = p(X_n > x_n)|_{0,T} = P(x_n)|_T \quad [2.3]$$

No caso do evento ε_{in} representar uma falha durante o funcionamento (Falha em Atraso, vide Anexo E) no intervalo $t=\{0, T\}$, a Confiabilidade Previsional R do sistema com respeito a este evento é formulada pela expressão que se segue, como o complemento de sua probabilidade de ocorrência neste intervalo.

$$R = [1 - p(\varepsilon_{in})|_{t=0,T}] = [1 - p(X_n > x_n)|_{t=0,T}] = [1 - P(x_n)|_{t=T}] \quad [2.4]$$

No caso do evento ε_{in} representar uma indisponibilidade na partida ou funcionamento intempestivo (Falha em Avanço, vide Anexo E) no instante $t = T$, a Disponibilidade Instantânea A do sistema com respeito a este evento é formulada pela expressão abaixo como o complemento da sua probabilidade de ocorrência neste instante.

$$A = [1 - p(\varepsilon_{in})|_{t=T}] = [1 - p(X_n = x_n)|_{t=T}] \quad [2.5]$$

O Risco Objetivo $\mathfrak{R}$ decorrente do funcionamento do Sistema Industrial no seu espaço de estados Ω durante um intervalo de tempo T será formulado então pela expressão a seguir como o somatório, percorrendo todos os $i=1, I$ Estados Finais associados aos Cenários Acidentais, os $n=1, N$ Eventos Indesejados associados a cada Estado Final, e os $j=1, J$ Tipos de Conseqüências consideradas para cada Estado Final, do produto da Gravidade G_{ij} pela FRP de x_n . Esta modelagem do Risco como produto da Gravidade pela Probabilidade denomina-se Modelo da Expectância Linear das Conseqüências e é expresso por:.

$$\mathfrak{R} = \sum_j \{ \sum_i [\sum_n P(x_n)_T \cdot G_{ij}] \} \quad [2.6]$$

O dimensional de $\mathfrak{R}$ será então Gravidade por unidade de tempo. As dificuldades apontadas para avaliação de Π pela expressão [2.1] repetem-se para a avaliação de $\mathfrak{R}$ pela expressão [2.6], acrescida a uma nova: o caráter finito porém não enumerável de ε_{in} .

Pode-se quantificar $\Re$ para um único Estado Final $\Omega_{i=1} = \Omega$, um único Evento Indesejado $\varepsilon_{i=1,n=1} = \varepsilon$ e para uma única consequência $C_{j=1} = C$, como mostrado abaixo. Note-se que a FRP de x_n em $t=T$, neste caso, corresponde à FDP do Evento Indesejado ε em $t=\{0, T\}$, que por sua vez corresponde à FDP da Gravidade $G_{ij} = g$ no mesmo intervalo de tempo.

$$\Re = P(x_n)_{t=T} \cdot g = p(g)_{t=0,T} \cdot g. \quad [2.7]$$

Neste caso simplificado, a área sob a curva da FDP da Gravidade $G_{ij} = g$ em $t=\{0, T\}$, dada por $p(g)_{t=0,T}$, plotada num gráfico (Probabilidade x Gravidade) representa o Risco Objetivo de um Sistema Industrial. Este gráfico, $p = p(g)$, é utilizado para determinação de um indicador sintético (escalar) denominado “Gravidade Média μ_G ” das consequências do funcionamento de um Sistema Industrial, formulado pela expressão abaixo como o produto da Gravidade g pela sua FDP. Note-se que a gravidade é geralmente representada sob forma descontínua, i.e. como k níveis de gravidade.

$$\mu_G = \int g \cdot p(g) dg = \sum_k [g_k \cdot p(g_k)] \quad [2.8]$$

Ainda para este caso simplificado, a área sob a curva da FRP da Gravidade $G_{ij}=g$ em $t = T$, dada pela integral da FDP da Gravidade entre $t=\{0, T\}$, plotada num gráfico (Probabilidade x Gravidade) também representa o Risco Objetivo de um Sistema Industrial. Este gráfico, $P = P(g)$, denominado “Diagrama de Farmer” (FARMER, 1967), é utilizado para determinação de outro indicador sintético (escalar) denominado “Risco Médio μ_R ” das consequências do funcionamento de um Sistema Industrial, formulado a seguir como o produto da Gravidade g pela sua FRP, i.e. a área sob a curva $P = P(g)$. Note-se que neste gráfico a gravidade também é representada sob forma descontínua, i.e. como k níveis de gravidade.

$$\mu_R = \int g \cdot [\int p(g) dg] dg = \int g \cdot P(g) dg = \sum_k [g_k \cdot P(g_k)] \quad [2.9]$$

A Gravidade Média e o Risco Médio constituem figuras de mérito quantitativas que permitem a aplicação objetiva do Princípio da Otimização, estabelecendo parâmetros para comparações entre:

- (a) diferentes sistemas industriais existentes;
- (b) diferentes configurações possíveis para um sistema industrial em desenvolvimento ou em modificação;
- (c) um dado sistema industrial, existente ou em desenvolvimento/modificação, e o nível de Riscos Subjetivos Toleráveis determinado pela demanda social por Segurança.

A abordagem (a) constitui ferramenta básica para o Gerenciamento de Riscos de um conjunto de sistemas, permitindo determinar uma política de segurança a partir de priorização dos sistemas sobre os quais Ações de Segurança devem ser tomadas. A abordagem (b) constitui ferramenta básica para o gerenciamento de Riscos de um determinado sistema, permitindo avaliar a eficácia e eficiência das Ações de Segurança. A abordagem (c) permite verificar a aceitabilidade social da configuração atual de um sistema ou de um conjunto de sistemas.

Pode-se utilizar indiferentemente a Gravidade Média ou o Risco Médio como figuras de mérito, dado que existe uma relação direta entre os dois:

- A partir de um intervalo de definição dos níveis de Gravidade $[g_0, g_1, \dots, g_k]$, determina-se a gravidade média μ_G calculando-se o baricentro das Gravidades ponderadas pelos respectivos valores da FDP $[p_0, p_1, \dots, p_k]$.

$$\mu_G = \sum_k (g_k \cdot p_k) \quad [2.10]$$

- No cálculo do risco médio, a ponderação das Gravidades é feita pela FRP:

$$\mu_R = \sum_k (g_k \cdot \sum_{l=k,K} p_l) = \mu_G + (\sum_k g_k \cdot \sum_{l=k+1,K} p_l) \quad [2.11]$$

A Figura 2.2 apresenta um exemplo de Diagrama de Farmer, onde existem três níveis descontínuos de riscos. A Gravidade Média e o Risco Médio seriam então determinados por:

$$\mu_G = \sum_k \mu_{Gk} = \sum_k [g_k \cdot p(g=g_k)] = \sum_k (g_k \cdot p_k) \quad [2.12]$$

$$\mu_R = \sum_k \mu_{Rk} = \sum_k [g_k \cdot p(g \leq g_k)] = \sum_k (g_k \cdot P_k) \quad [2.13]$$

$$\mu_G = (g_1 \cdot p_1 + g_2 \cdot p_2 + g_3 \cdot p_3) = 3 \cdot 10^{-3} \quad [2.14]$$

$$\mu_R = [g_1 \cdot p_1 + (g_2 + g_1) \cdot p_2 + (g_3 + g_2 + g_1) \cdot p_3] = 3,21 \cdot 10^{-3} \quad [2.15]$$

FIGURA 2.2: DIAGRAMA DE FARMER

O Risco Médio dá um peso maior às gravidades mais severas do que a gravidade média. Com efeito, entre duas distribuições de mesma gravidade média, a diferença entre os respectivos riscos médios objetivos será tanto maior quanto maiores forem as probabilidades associadas às gravidades mais intensas. Este efeito é ainda mais notável quanto maior for a gravidade média. Sob este ponto de vista, o Risco Médio coincide melhor com a percepção social do Risco Subjetivo, decorrente de um maior peso dado aos eventos graves.

A formulação do Risco Subjetivo $\mathfrak{R}^*$ é baseada em Modelos de Expectância Não-Linear de Consequências (HANSEN, 1982), de natureza fundamentalmente empírica, pois envolvem fenômenos de origem social e psicológica (SLOVIC, 1980). Estes modelos podem ser expressos de forma genérica, sendo f uma função não linear, i.e. diversa do simples produto da Probabilidade pela Gravidade.

$$\mathfrak{R}^* = f [P(\epsilon), G] \quad [2.16]$$

A abordagem mais corrente para o desenvolvimento destes modelos são os estudos sociais de “disposição a pagar” (*willingness to pay*) desenvolvidos em alguns países

(STARR, 1973; SCHNEIDER, 1995). Deve-se ressaltar que os modelos derivados deste tipo de abordagem são restritos a um grupo social bem definido e a uma época determinada, não sendo válida, *a priori*, sua transposição para contextos diferentes do original.

A Segurança (ou Seguridade) Objetiva S do funcionamento do Sistema Industrial no seu espaço de estados Ω será formulado pela expressão a seguir como o inverso do Risco Objetivo, tendo a dimensão de Tempo por unidade de Gravidade.

$$S = 1 / \Re \quad [2.15]$$

Dentro deste formalismo, para um único Estado Final $\Omega_{i=1} = \Omega$ e uma única incidência de conseqüências $C_{j=1} = C$, S pode ser determinado pelo período de retorno Tr de um determinado valor limite x_n da FRP de uma variável aleatória X_n que caracteriza a ocorrência do evento ε_n .

$$S = Tr(x_n) = 1 / [1 - P(x_n)] \quad [2.16]$$

A partir de [2.5], pode-se deduzir $\Re$ como o valor da FDP p de observar no período de tempo $t = \{0, T\}$ um Evento Indesejado ε_{in} com período de retorno Tr .

$$\Re = p(X_n > x_n) = 1 - [p(X_n < x_n) |_{t=0,T}] = 1 - [P(x_n) |_{t=T}] = 1 - \{1 - [1/Tr(x_n)]\} \quad [2.17]$$

Para x_n suficientemente grande, determina-se $p(X_n > x_n)$ resolvendo-se a expressão [2.17], onde $P(x_n)$ é a FRP da variável aleatória X_n (vide desenvolvimento no Anexo F).

$$\Re = p(X_n > x_n) = 1 - [P(x_n)]^{1/T} \quad [2.18]$$

Para x_n e Tr suficientemente grandes, a expressão [2.17] se simplifica, chegando-se a (vide desenvolvimento no Anexo F):

$$\Re = p(X_n > x_n) = 1 - e^{-(T/Tr)} = T/Tr \quad [2.19]$$

A Disponibilidade Pós-Acidental A^* é formulada pela expressão [2.18] como a probabilidade do sistema, estando em um Estado Final Ω_i decorrente de um Cenário Acidental, retornar a um Estado Final Ω seguro devido a ocorrência de um Evento Desejado ε_{in}^* dentro do intervalo $t = \{T, T + \Delta t\}$. A probabilidade $p(\varepsilon_{in}^*)$ é determinada pelo valor

limite x_p^* da função repartição de probabilidade P de uma variável aleatória X_n^* que caracteriza sua ocorrência durante o intervalo $t = \{T, T+\Delta t\}$.

$$A^* = p(\varepsilon_{in}^*)_{T+\Delta t} = p(X_n^* > x_p^*)_{T+\Delta t} = P(x_p^*)_{T+\Delta t} \quad [2.20]$$

Note-se que, para um mesmo conjunto $\{\varepsilon_{in}\}$, S confunde-se com a Disponibilidade Potencial $\hat{A}$. Entretanto, $\hat{A}$ é em geral definida para um conjunto de eventos operacionais mais abrangente, nem todos conduzindo a uma situação de Perigo Ω_i . Da mesma forma, considerando-se um conjunto de Ω_i não necessariamente associados a situações de Perigo, para um mesmo $\{\varepsilon_{in}^*\}$, A^* confunde-se com a Manutibilidade Corretiva M .

2.1.4 LIMITES SUPERIORES DE RISCOS

A aceitabilidade social de uma instalação industrial perigosa depende da intensidade dos riscos para os trabalhadores, as populações vizinhas e o meio ambiente em geral. Admitindo-se que os riscos são quantificáveis de acordo com as formulações apresentadas, torna-se necessário fixar-se limites superiores a estes riscos com o objetivo de determinar-se a envergadura das ações de segurança requeridas para o seu efetivo gerenciamento.

A definição destes limites ao nível normativo e regulamentar é uma atividade que ultrapassa a área estritamente técnica, envolvendo uma série de considerações de ordem social e política. Apesar das dificuldades associadas a esta definição, alguns países têm determinado formalmente tais limites (HSE, 1989a; HSE, 1989b; HSE, 1988; NETHERLANDS, 1988). Analisando os estudos e práticas dos países europeus sobre o tema, (SMETS, 1992) propõe os seguintes limites:

- Limite superior para a probabilidade de ocorrência de um acidente que implique na morte de um trabalhador: 10^{-2} / ano / trabalhador
- Limite superior de risco coletivo ocupacional voluntário ao qual os trabalhadores da instalação são submetidos durante suas atividades profissionais: 10^{-2} mortes / ano
- Limite superior para a probabilidade de ocorrência de um acidente que implique na morte de um indivíduo na vizinhança da instalação: 10^{-3} / ano / indivíduo;
- Limite superior de risco coletivo involuntário ao qual as populações nas vizinhanças da instalação são submetidos: 10^{-3} mortes / ano

Adaptando-se estes limites às formulações anteriores teríamos, a partir de [2.10], para uma gravidade g_k igual ao número k de mortes:

risco individual ocupacional: $(g_1 \cdot p_1) \leq 10^{-2}$ mortes / ano

risco coletivo ocupacional: $\mu G = \sum k (g_k \cdot p_k) \leq 10^{-2}$ mortes / ano

risco individual público: $(g_1 \cdot p_1) \leq 10^{-3}$ mortes / ano

risco coletivo público: $\mu G = \sum k (g_k \cdot p_k) \leq 10^{-3}$ mortes / ano

Note-se que estes limites são estabelecidos para uma única classe de conseqüências, i.e. a probabilidade de morte de uma ou mais pessoas. Esta prática decorre das inerentes dificuldades de aceitação social de uma escala de Gravidade comum a diferentes classes de conseqüências. Estes limites não levam ainda em conta os aspectos do Risco Subjetivo associado à aversão às catástrofes. (SMETS, 1992) propõe, para consideração deste aspecto, o limite abaixo definido, no qual c é uma constante valendo entre (0,5; 1). Analisando a regulamentação de (NETHERLANDS, 1988), verifica que, implicitamente, considera-se $c = 0,67$. Teria-se então, a partir de [2.11]:

$$\mu R = \sum k (g_k^{1+c} \cdot \sum_{l=k,K} p_l) \leq 10^{-2} \cdot c \text{ mortes / ano}$$

A aplicação destes limites aos riscos de origem radiológica (vide Anexo D) não é imediata, à medida que, dentro da faixa de doses de radiação abaixo do limiar dos efeitos determinísticos (dose equivalente sobre o corpo inteiro inferior a 200 mSv), a eventual morte de um indivíduo ocorre de forma retardada, i.e. alguns anos após o evento que lhe deu origem, como um efeito estocástico.

Segundo (ICRP, 1991), uma dose de 1 Sv incidindo sobre uma população homogênea de indivíduos adultos representa um aumento de 5% na taxa de mortalidade natural por câncer deste grupo. Note-se que este indicador de risco representa uma aproximação: para maiores detalhes sobre a determinação do aumento da freqüência de ocorrência de mortes por câncer numa população irradiada, vide (ASQRAD, 1998). Note-se ainda que a taxa de mortalidade natural por câncer, significativamente variável conforme o grupo social amostrado, situa-se, em média, num patamar elevado, da ordem de 20-25%.

Isto implica que cada indivíduo, quando nasce, tem uma chance dentre 4 ou 5 de contrair um câncer mortal durante sua existência. As eventuais doses de irradiação que o indivíduo venha a receber irão aumentar essa probabilidade.

Considerando este fator de risco aproximado (5% / Sv), têm-se que o limite de dose individual ocupacional recomendado por (ICRP, 1991), i.e. 20 mSv / ano, corresponde um aumento da probabilidade de morte por câncer de 10^{-3} . Se considerarmos o limite de dose recomendado para um indivíduo do público (1 mSv / ano), têm-se $5 \cdot 10^{-5}$.

Conclui-se portanto que os limites de risco radiológico universalmente aceitos são, respectivamente, 1 e 2 ordens de grandeza inferiores aos limites gerais de riscos individuais para os trabalhadores e para o público. Note-se que a CIPR não recomenda limites de risco coletivo.

2.1.5 GERENCIAMENTO DE RISCOS

Em conformidade com sua definição, o Gerenciamento de Riscos consiste num conjunto de ações aplicadas aos diversos componentes de um Sistema Industrial, dentro de um procedimento lógico de análise, visando garantir sua Seguridade, ou seja, que seu Risco Objetivo Residual torne-se um Risco Subjetivo Aceitável. Nesta seção serão abordadas as ações de Prevenção, Proteção e Seguro que permitem esse gerenciamento. Serão ainda revistos o procedimento geral de análise do sistema dentro do qual estas ações são aplicadas e o procedimento de alocação destas ações às diversas partes do sistema.

2.1.5.1 Ações de Segurança

Uma Ação de Prevenção corresponde a uma medida prática de redução do Risco pela diminuição da probabilidade de ocorrência de um Evento Indesejado, sem diminuir a Gravidade do estado final do Cenário Acidental correspondente. Esta definição corresponde ao senso comum associado à prevenção, que consiste em impedir que um evento ocorra, sem sistematicamente considerar suas conseqüências.

A partir de um Risco Inaceitável identificado como A num gráfico de Farmer (Figura 2.3), a Ação de Prevenção consiste em passar a um Risco Aceitável B por deslocamento paralelo ao eixo das probabilidades. A margem de segurança teórica é então definida pela

distância entre a probabilidade B resultante após a Ação de Prevenção e o objetivo em probabilidade que pertence, por definição, ao limite de Riscos Aceitáveis.

FIGURA 2.3: AÇÃO DE PREVENÇÃO

Uma Ação de Proteção é uma medida de redução do risco baseada na redução da Gravidade do estado final de um Cenário Acidental após sua ocorrência, sem diminuir a probabilidade de ocorrência dos Eventos Indesejados correspondentes. Esta definição corresponde ao senso comum associado à proteção que consiste em limitar as consequências de um evento, sem considerar *a priori* sua probabilidade, eventualmente próxima de 1.

A partir de um Risco Inaceitável identificado como A num gráfico de Farmer (Figura 2.4), a Ação de Proteção consiste em passar a um Risco Aceitável B por deslocamento paralelo ao eixo das Gravidades. A margem de segurança teórica é então definida pela distância entre a Gravidade resultante após a Ação de Proteção e o objetivo em probabilidade que pertence, por definição, ao limite de Riscos Aceitáveis.

FIGURA 2.4: AÇÃO DE PROTEÇÃO

A Ação de Seguro, contrariamente à prevenção e à proteção, não tem por objetivo nem reduzir a probabilidade nem a gravidade de um evento indesejado. Seu objetivo é transferir para um terceiro (o segurador) total ou parcialmente as consequências financeiras do risco.

FIGURA 2.5: AÇÃO DE SEGURO

A partir do limite de Risco Inaceitável identificado num diagrama de Farmer (curva pontilhada da Figura 2.5), a Ação de Seguro consiste em deslocar este limite até uma posição em que o ponto A encontre-se no domínio aceitável. O deslocamento virtual do limite de aceitabilidade tem como contrapartida o pagamento de um prêmio ao segurador, cujo valor é diretamente proporcional ao número de “clientes” que são assegurados contra este risco, à Probabilidade de ocorrência e à Gravidade das consequências do Evento Indesejado, estimado a partir de bases de dados estatísticos, assim como de Ações de Proteção e Prevenção compulsórias impostas ao cliente para reduzir o nível de Risco Segurado.

2.1.5.2 Procedimento Geral de Análise de Segurança

As ações de Gerenciamento de Riscos são implementadas através de um Procedimento Geral de Análise de Segurança. O objetivo deste procedimento é otimizar as ações feitas a título exclusivo da segurança com aquelas feitas a título do sucesso técnico da missão. O procedimento aplica-se à determinação do nível de segurança de um novo sistema

em fase de projeto e desenvolvimento. As medidas tomadas, entretanto, estendem-se à fase de operação do sistema.

As informações iniciais requeridas são o conjunto de Cenários Acidentais, com seus estados finais $\{\Omega_i\}$, as classes de conseqüências indesejadas $\{C_j\}$, as Gravidades $\{G_{ij}\}$ e as probabilidades dos Eventos Indesejados $\{\epsilon_{in}\}$. Os resultados esperados correspondem a um programa de ações de segurança relativas a cada uma das etapas do procedimento e à avaliação do Risco Residual associado a cada uma delas.

O Procedimento de Análise de Segurança (Figura 2.6) se decompõe em quatro etapas correspondendo cada uma a um conjunto de ações específicas de identificação e de redução de risco com respeito ao cenário acidental considerado. Este por sua vez se decompõe em uma seqüência de eventos que se inicia em $\epsilon_{in} (E_0)$, encadeia-se logicamente com um série de eventos intermediários componentes do Cenário Acidental (E_1) e conclui-se no estado acidental $\Omega_i (E_A)$.

A posição no tempo das quatro etapas do procedimento com respeito ao instante de ocorrência dos três eventos correspondem a ações de prevenção (segurança intrínseca ou integrada E_1 e segurança implantada E_2) e de proteção (salvaguarda E_3 e emergência E_4). A probabilidade do acidente será então definida por:

$$P(E_I) = P(E_0) * P(\text{falha } E_1 | E_0) \quad [2.21]$$

$$P(E_A) = P(E_I) * P(\text{falha } E_2 | E_I) * P(\text{falha } E_3 | \text{falha } E_2) * P(\text{falha } E_4 | \text{falha } E_3) \quad [2.22]$$

A natureza destas ações pode ser ilustrada por um caso típico de projeto: seja um local fechado no qual são realizadas operações periódicas sobre um reservatório contendo um gás a alta pressão, o acidente postulado E_a correspondendo à explosão do reservatório seguida da morte de pelo menos um operador devido aos fragmentos gerados. As ações correspondentes às quatro etapas do procedimento de segurança seriam:

- E_1 : projetar, fabricar, montar, comissionar e inspecionar em serviço periodicamente o reservatório segundo normas e procedimentos de garantia da qualidade adaptados;

- E2: instalar um sistema de monitoração e controle de sobrepressão para alertar os operadores em caso de risco iminente de explosão definido pela ultrapassagem de um limite crítico de pressão;
- E3: instalar válvulas de alívio de pressão e instalar barreiras físicas em torno do reservatório;
- E4: prever saídas de emergência do local, disponibilidade de uma equipe de resgate e primeiros socorros e de assistência médica hospitalar próxima.

FIGURA 2.6: PROCEDIMENTO GERAL DE ANÁLISE DE SEGURANÇA

A Etapa 1, Segurança Intrínseca ou Integrada, está relacionada a um “projeto de risco mínimo”. Nesta etapa o projetista se esforça em conceber e implementar uma configuração para o sistema que possibilite o sucesso de sua missão. Este objetivo é visado, entretanto, com uma constante preocupação em eliminar ou diminuir *a priori*, através de uma concepção adaptada, as ações de prevenção identificadas como necessárias durante a vida operacional do sistema. Isto quer dizer que, nesta etapa, nenhum meio material, lógico ou humano, com fins exclusivamente de segurança, deve ser adicionado. Somente as projeções materiais ou

lógicas das funções necessárias ao cumprimento técnico da missão devem ser projetadas de modo mais seguro possível com respeito ao risco identificado. Dois tipos de ações possíveis respondem a este requisito, não devendo, entretanto, ter um impacto negativo sobre a probabilidade de sucesso da missão, pois nesta etapa não deve haver compromisso entre o sucesso da missão e a segurança do sistema: melhorias na configuração global do sistema ou de um sistema elementar ou sub-sistema associado; e melhorias de componentes ou itens do sistema através de sua seleção.

Na Etapa 2, Segurança Implantada, são implementados no sistema elementos de segurança não necessários ao sucesso técnico da missão, que implicam, em certos casos, em um compromisso entre o sucesso da missão (confiabilidade e disponibilidade) e a seguridade. Estes elementos integrados à configuração do sistema para eliminar ou reduzir o risco potencial constituem "barreiras de segurança ou de defesa em profundidade". São artifícios materiais, lógicos ou de procedimentos que impedem ou retardam a evolução de um cenário, com o objetivo de se contrapor à ocorrência do evento indesejado. Para justificar sua implantação no sistema, as barreiras devem atender a três princípios básicos:

- as barreiras devem ser confiáveis, robustas e duráveis, i.e. as barreiras devem ser efetivamente adaptadas à cobertura do evento indesejado que se deseja evitar, suficientemente dimensionadas com respeito ao evento indesejado de forma a prevenir falhas nelas próprias, e eficazes ao longo do tempo;
- se várias barreiras de mesma confiabilidade são implantadas em redundância, elas devem ser: testáveis em separado; independentes com respeito aos modos de falha de causa comum; e impermeáveis a todos os processos de propagação de falha ou de seus efeitos, i.e. a falha de uma das barreiras não deve implicar em falha de barreiras subsequentes;
- a eficácia ou a credibilidade das barreiras propostas deve ser sistematicamente justificada pela análise de segurança e validada por experimentos adaptados.

A Etapa 3, Salvaguarda, corresponde à implementação de um conjunto de ações de proteção que se seguem a um ou vários alarmes confirmados, que anunciam a ocorrência do evento indesejado e cujas causas diretas deverão ser controladas, isto é neutralizadas definitivamente ou retardadas para permitir que o sistema seja reconduzido a um estado

seguro. Esta etapa implica na necessidade de se prever, ainda na fase de projeto, testes e alarmes associados aos elementos cuja falha é crítica, i.e. implantação de sensores e canais de monitoração cobrindo perfeitamente o fenômeno sob vigilância, e uma estratégia eficaz de condução do sistema ou de seu ambiente a um estado seguro.

A Etapa 4, Emergência, corresponde a um conjunto de ações de proteção cujo objetivo é mitigar as consequências do acidente, isto é, minimizar a gravidade dos efeitos potenciais do evento indesejado, após sua ocorrência.

A lógica de projeto do sistema para cada uma destas fases operacionais, e para cada evento indesejado identificado, consiste então em prever um conjunto de ações específicas e eficazes que diminuam tanto a probabilidade de sua ocorrência como a gravidade das consequências diretas e indiretas de cada um destes eventos indesejados.

2.1.5.3 Procedimento de Alocações de Segurança

O Procedimento de Alocações de Segurança (Figura 2.7) tem por objetivo repartir as Ações de Segurança pelas partes do sistema, através de sua modelagem funcional, material e operacional (LECOQ, 1989; DESROCHES, 1986). Este procedimento deve dar às diferentes equipes participantes do desenvolvimento de um sistema, um conjunto de requisitos de projeto, construção e operação definidos ao seu nível de responsabilidade.

Para um objetivo missão de classe k, o procedimento de alocação consiste em repartir as Ações de Segurança sobre as partes conforme a importância que cada uma tem na totalização do Risco Objetivo do sistema. O Anexo H discute diferentes métodos de Alocações de Segurança.

FIGURA 2.7: PROCEDIMENTO DE ALOCAÇÕES DE SEGURANÇA

2.2 SEGURANÇA NUCLEAR

Nesta seção será discutida a Segurança de Instalações Nucleares “Estacionárias”, em especial de reatores de potência eletronucleares, segmento industrial que se notabiliza pelo desenvolvimento, ao longo dos últimos 40 anos, de uma doutrina de segurança específica, a partir da qual a SDFSI/RAMS moderna tem suas origens, e que, com necessárias adaptações, é aplicável às IPN.

Serão definidos o escopo e os objetivos gerais da Segurança Nuclear, os riscos potenciais dos reatores de potência e as funções básicas de segurança que fazem face a estes riscos. O princípio fundamental de Defesa em Profundidade será discutido, associando-o às barreiras físicas de contenção e confinamento de materiais radioativos requeridas para o cumprimento das funções básicas da Segurança Nuclear. Será finalmente discutido o procedimento de análise de segurança nuclear, associando-o ao procedimento geral proposto pela seção anterior

2.2.1 ESCOPO

“Seguridade Nuclear” (*Nuclear Security*) consiste em todas as ações empreendidas para proteção global das pessoas, das propriedades e do meio ambiente contra Perigos que possam resultar da construção, operação e descomissionamento das instalações nucleares, assim como da armazenagem, transporte, uso ou transformação de substâncias radioativas naturais e artificiais. É um conceito abrangente que envolve várias técnicas e análises, incluindo Proteção Radiológica, “Segurança Nuclear”, Segurança Física das instalações nucleares

contra agressões premeditadas (atos de sabotagem) e Gerenciamento de Crise no caso de ocorrência de acidentes severos (DSIN, 1998).

“Segurança Nuclear” (*Nuclear Safety*) é uma das partes componentes da Seguridade Nuclear, que consiste nas ações tomadas ao longo de todo o Ciclo de Vida de uma “Instalação Nuclear de Base”, visando a prevenção de acidentes e a mitigação de suas conseqüências. Engloba também as ações tomadas para limitar e otimizar tanto a exposição dos trabalhadores às radiações ionizantes durante a operação normal das “Instalações Nucleares de Base”, incluídas as atividades de manutenção, como a produção e disposição dos rejeitos radioativos e efluentes (DSIN, 1998).

A Segurança Nuclear está centrada no Gerenciamento de Riscos induzidos pelas radiações ionizantes provenientes dos materiais radioativos contidos nas “Instalações Nucleares de Base”. A natureza e incidência destes riscos, denominados Riscos Radiológicos são discutidas pelo Anexo D. O gerenciamento destes riscos é feito fundamentalmente através de Ações de Prevenção de acidentes e, secundariamente, através de Ações de Proteção dos trabalhadores e do público em geral, no caso destes acidentes virem a ocorrer. Ações de Proteção do meio ambiente são também tomadas à medida que tenham um impacto direto ou indireto sobre o público.

“Instalações Nucleares de Base INB” incluem os reatores nucleares e as instalações diretamente ligadas ao “Ciclo do Combustível Nuclear” (GUIMARÃES, 1998), ilustrado pela Figura 2.8, correspondendo às etapas:

- mineração de urânio;
- beneficiamento do minério (produção de *yellow cake*);
- conversão de *yellow cake* em hexafluoreto de urânio (UF₆);
- enriquecimento do UF₆;
- reconversão do UF₆ e fabricação de pastilhas de UO₂;
- fabricação de elementos combustíveis;
- carregamento e “queima” dos elementos combustíveis em reatores;
- descarregamento e armazenagem de elementos combustíveis usados;
- reprocessamento de elementos combustíveis usados; e

- reaproveitamento do urânio e plutônio recuperados pelo reprocessamento

FIGURA 2.8: CICLO DO COMBUSTÍVEL NUCLEAR

2.2.2 OBJETIVOS

O objetivo fundamental da segurança de instalações nucleares é proteger o público e os trabalhadores das consequências de liberações de produtos radioativos decorrentes de sua operação normal e de acidentes, conforme Tabela 2.1 (IAEA, 1993).

TABELA 2.1: OBJETIVOS DA SEGURIDADE NUCLEAR (IAEA, 1993)

SÍNTESE DE DOCTRINA DE SEGURANÇA
PARA PROJETO E OPERAÇÃO DE SUBMARINOS NUCLEARES

OBJETIVO GLOBAL	
"proteger os indivíduos, a sociedade e o meio ambiente de efeitos indesejáveis pelo estabelecimento e manutenção nas instalações nucleares de defesas efetivas contra riscos radiológicos"	
OBJETIVO DE PROTEÇÃO	OBJETIVO DE SEGURANÇA
"garantir que, em toda a situação de operação, a exposição à radiação dentro da instalação, ou devida a toda descarga planejada de material radioativo proveniente da instalação, seja mantida abaixo dos limites prescritos e tão reduzidos quanto razoavelmente praticável, e garantir que as consequências radiológicas de qualquer acidente possam ser mitigadas"	"tomar todas as medidas praticáveis para prevenir acidentes em instalações nucleares e mitigar suas consequências caso eles ocorram; garantir, com alto nível de confiança que, para todos os acidentes possíveis previstos pelo projeto da instalação, incluindo aqueles de probabilidade muito pequena, toda consequência radiológica será mínima e abaixo dos limites prescritos; e garantir que a possibilidade de acidentes que causem consequências severas é extremamente pequena"

Para o atendimento destes objetivos, uma série de princípios básicos é preconizada, cobrindo a estrutura legal de regulamentação, o gerenciamento da segurança, aspectos técnicos gerais e específicos, bem como as atividades de verificação da segurança (IAEA-INSAG, 1992; IAEA-INSAG, 1988). Estes princípios básicos são então desenvolvidos em critérios de projeto gerais e específicos (IAEA, 1978; IAEA, 1986; USFG, 1977; ANSI/ANS, 1983; BNL, 1978; RF, 1995; HSE, 1992; AFCEN, 1993). Esta doutrina estabelece portanto as diretrizes para o Gerenciamento de Riscos das instalações nucleares, que compreende:

- planejamento e execução sistemática de atividades de projeto, construção e operação que minimizem a possibilidade de ocorrência de acidentes, incluindo requisitos operacionais que garantam a operação da instalação dentro dos limites de projeto especificados; e
- planejamento e execução sistemática de atividades de projeto, construção e operação que minimizem as consequências dos acidentes, caso eles ocorram.

A responsabilidade pelo Gerenciamento de Riscos e consequente atendimento aos Objetivos da Segurança Nuclear é outorgada ao Operador da INB, que deverá ser

previamente licenciado pela ASN. Esta responsabilidade não é de nenhuma maneira diluída pela separação de atividades e responsabilidades de projetistas, fornecedores, construtores, prestadores de serviços de manutenção e ASN.

O estabelecimento do Processo de Licenciamento das instalações nucleares é prerrogativa de cada país, que estabelece suas próprias normas e procedimentos administrativos. O desenvolvimento histórico deste processo nos EUA, que constitui um paradigma internacional, é apresentado por (OKRENT, 1991).

Neste contexto, a ASN pode ser entendida como o representante do governo nacional que irá garantir à sociedade que os Riscos Objetivos Residuais de uma INB são Riscos Subjetivos Aceitáveis, i.e. justificados, limitados e otimizados. Tendo em vista que Risco Zero é uma utopia, o fato da ASN emitir uma licença, i.e. considerar os riscos envolvidos como aceitáveis, não implica que ela assuma responsabilidade pelas consequências indesejadas no caso da real ocorrência de um acidente. Esta responsabilidade recai integralmente sobre o Operador, o que o torna o maior interessado pela segurança de sua instalação.

Sob este aspecto, cabe ressaltar o preceito constitucional brasileiro que impõe: “A responsabilidade civil por danos nucleares independe de culpa”, i.e. não importando porquê e como ocorreu um acidente, o operador responderá integralmente pelos danos dele decorrentes.

As funções da ASN e do operador são então desta forma estruturados:

- A ASN define os Objetivos Gerais de Segurança – OGS;
- O Operador propõe soluções técnicas, justificando que os objetivos podem ser alcançados;
- A ASN analisa a eficácia das soluções propostas;
- O Operador implementa as soluções aprovadas;
- A ASN verifica durante inspeções que as soluções aprovadas foram corretamente implementadas e emite as autorizações administrativas e legais correspondentes às diferentes etapas do Processo de Licenciamento.

A esfera de atuação da ASN compreende:

- Análise da Segurança Nuclear da instalação;
- Análise da Proteção Radiológica da instalação;
- Gerenciamento dos rejeitos radioativos da instalação;
- Monitoração de efluentes radioativos da instalação e proteção ambiental; e
- Supervisão do transporte e armazenagem de materiais radioativos e físséis.

A eficácia do Gerenciamento de Riscos de instalações nucleares está fortemente associada ao estabelecimento de uma “Cultura de Segurança” (IAEA-INSAG, 1991) e de uma “Estratégia de Defesa em Profundidade” (IAEA-INSAG, 1997).

“Cultura de Segurança” representa o conjunto de características e atitudes nas organizações e nos indivíduos que garante, com uma máxima prioridade, que os aspectos importantes para a segurança nuclear recebem a atenção requerida pela sua significância. A Cultura de Segurança deve governar as ações e interações de todos os envolvidos nas atividades relacionadas com a energia nuclear.

“Estratégia de Defesa em Profundidade” deve ser implementada de forma a compensar potenciais falhas humanas e materiais, baseada em vários níveis de proteção que incluam sucessivas barreiras físicas e em procedimentos que impeçam a liberação incontrolada de matérias radioativas no meio ambiente. A estratégia inclui não só a proteção da instalação através de barreiras como a proteção das próprias barreiras. Ela também inclui medidas posteriores para proteger o público e o meio ambiente das eventuais conseqüências no caso em que as barreiras não se mostrem totalmente efetivas.

2.2.3 RISCOS POTENCIAIS E FUNÇÕES BÁSICAS

Dentre as INB, aquelas que apresentam os maiores Perigos devido à quantidade e toxicidade do inventário de materiais radioativos nelas contidas são os reatores de potência, os reatores de pesquisa e as usinas de reprocessamento de combustíveis usados. Note-se aqui que a distinção feita entre os dois tipos de reatores está ligada à sua utilização:

- reatores de potência são aqueles cuja missão é produzir energia térmica para geração de eletricidade (reatores eletronucleares), para geração direta de calor (reatores calogêneos)

ou para acionamento do eixo propulsor de um navio ou submarino (reatores de propulsão naval); e

- reatores de pesquisa são aqueles cuja missão é produzir fluxo de nêutrons para irradiação de materiais diversos (produção de radioisótopos, “dopagem” de semicondutores, materiais a serem usados em reatores de potência ou outras aplicações nucleares).

No que tange à Gravidade dos Perigos potenciais de reatores, o fator mais relevante não é propriamente sua utilização, mas sua potência térmica, que é diretamente proporcional ao inventário de produtos radioativos contidos na instalação:

- para reatores de propulsão naval, a potência térmica é da ordem de 50-100 MWth;
- para reatores eletronucleares, de 1.000-3.800 MWth (CEA, 1998); e
- para reatores de pesquisa o espectro é muito variado, indo de potências térmicas praticamente nulas (unidades críticas) até 800MWt (IAEA, 1998).

Os reatores nucleares possuem duas características específicas que os diferenciam das outras instalações de produção de energia:

- i) durante o seu funcionamento normal acumulam uma grande quantidade de materiais radioativos, dos quais os operadores e o público em geral devem ser permanentemente protegidos e que podem provocar um acidente de significativas proporções caso sejam dispersos em grande escala no meio ambiente;
- ii) uma significativa quantidade de energia continua sendo produzida pelo decaimento radioativo dos produtos de fissão contidos na matriz do combustível nuclear por longo período mesmo após o reator ter sido desligado.

O Risco Potencial dos reatores decorre principalmente da possibilidade de dispersão dos materiais radioativos para fora dos locais previstos. As possíveis causas desta dispersão devem então ser objeto da Análise de Segurança. Os materiais radioativos são, em sua maior parte, produzidos no interior do material combustível físsil e é necessário que eles aí permaneçam até que o combustível usado seja descarregado do reator. O resfriamento adequado do combustível e de seu encamisamento é portanto essencial. Deve-se ainda ressaltar que:

- de modo a possibilitar a operação normal do reator por períodos longos, da ordem de alguns anos, sem necessidade de recarregá-lo de combustível, e para contrabalançar diversos efeitos relativos ao nível de potência em que ele opera, o núcleo deve conter uma quantidade de material físsil que excede em muito a massa crítica para a condição de desligamento a frio; o nível de potência produzido por este material consequentemente resulta da combinação de uma série de parâmetros que devem ser controlados externamente, ou seja, o reator não possui um nível de potência naturalmente intrínseco, determinado exclusivamente por parâmetros internos;
- sob condições de operação anormais, a energia liberada pelo reator pode aumentar de forma extremamente rápida e descontrolada, somente podendo ser limitada pelos efeitos de realimentação da reação em cadeia relacionados com a temperatura ou pela dispersão do combustível, desfazendo a massa crítica;
- a energia liberada pelo combustível não pode ser imediatamente anulada, mesmo que a reação nuclear de fissão em cadeia seja interrompida; isto decorre da desintegração dos produtos radioativamente instáveis derivados da fissão nuclear liberar uma certa quantidade de energia até ser atingida uma condição estável; o tempo de decaimento necessário para que cada um destes produtos atinja a estabilidade varia enormemente: de menos de 1 segundo até milhares de anos; apesar de exponencialmente decrescente, a potência produzida pode permanecer em níveis significativos por longos períodos, requerendo resfriamento contínuo.

As ações de Gerenciamento de Riscos irão então reduzir o Risco Potencial de dispersão de materiais radioativos ao nível de Risco Residual Aceitável, por meio do cumprimento de três funções básicas da Segurança Nuclear de reatores (LEWIS, 1977; PERSHAGEN, 1989; LILLINGTON, 1995; LIBMANN, 1996):

- I) Controle eficaz da reação nuclear de fissão em cadeia e, consequentemente, da potência produzida;
- II) Resfriamento adequado do combustível, de modo a manter as condições termohidráulicas mínimas para que seja mantida a integridade mecânica do seu encamisamento; e

III) Contenção dos materiais radioativos não só na própria matriz do combustível e seu encamisamento (Primeira Barreira), como também no envelope estanque do Circuito Primário (Segunda Barreira), e no envelope estanque do compartimento onde se localiza o reator (Terceira Barreira). Esta função de contenção aplica-se não só ao reator propriamente dito como também às outras partes da instalação nuclear que venham a conter materiais radioativos.

Os Riscos Potenciais de reatores nucleares são caracterizados pelas Falhas que conduzem à perda de uma ou mais das três funções básicas de segurança. Identificam-se então três grandes “famílias” de Cenários Acidentais:

- a) Acidentes de Reatividade (ou de Criticalidade): aqueles que envolvem a perda do controle externo dos parâmetros que determinam o fator de multiplicação do fluxo neutrônico gerado pela reação de fissão nuclear em cadeia no interior do combustível, fazendo com que ocorra uma “excursão” de potência, i.e. um aumento excessivamente rápido na energia gerada pelo núcleo do reator;
- b) Acidentes de Perda de Resfriamento: aqueles que envolvem um grande desequilíbrio entre a potência térmica gerada pelo núcleo do Reator e a potência removida pelo seu sistema de resfriamento. Os cenários mais graves desta família conduzem a um estado final de fusão do núcleo;
- c) Acidentes de Perda de Estanqueidade: aqueles que envolvem vazamentos de uma ou mais barreiras de contenção. Os cenários mais graves desta família conduzem a um estado final em que há liberação de parcelas significativas do inventário de produtos radioativos (Termos-Fonte Acidental) para o meio ambiente.

Estas três grandes famílias de acidentes estão intimamente interligadas: um acidente de reatividade pode levar a um acidente de perda de resfriamento, que por sua vez pode levar a um acidente de perda de estanqueidade. Caso os acidentes da primeira e segunda família não se propaguem para a terceira, suas consequências são limitadas ao interior da instalação, i.e. podem implicar em danos somente a seus operadores e materiais componentes. Os acidentes da terceira família são aqueles de onde podem decorrer consequências para o público em geral e o meio ambiente.

2.2.4 DEFESA EM PROFUNDIDADE

2.2.4.1 Barreiras Físicas de CONTENÇÃO

A proteção do público contra as conseqüências de uma liberação acidental de materiais radioativos para o meio ambiente repousa, em última instância, sobre a interposição de uma série de barreiras estanques. A análise de segurança nuclear consiste portanto, primeiramente, em garantir a eficácia destas barreiras e sua correta operação sob Condições de Processo da Instalação Nuclear CPIN normais e acidentais. Este tipo de análise enfatiza a natureza progressiva da segurança, distinguindo três sucessivos, porém interrelacionados, estágios:

- a) Prevenção: a eficácia de cada barreira deve ser demonstrada para os materiais selecionados, sua adaptação às CPIN e manutenção de suas características especificadas ao longo do tempo. É essencial que os limites tecnológicos sejam explicitados de forma que uma margem de segurança real entre estes limites e as CPIN possam ser definidos com razoável grau de confiança;
- b) Vigilância e Proteção: os sistemas de monitoração, controle e proteção devem ser projetados de forma a detectar qualquer deriva dos parâmetros críticos de operação em direção aos limites tecnológicos pré-definidos, permitindo assim a atuação, caso necessário, de ações corretivas manuais ou automáticas em tempo hábil para que a instalação retorne às condições normais de operação;
- c) Mitigação de Conseqüências: no evento de uma CPIN acidental em que os limites tecnológicos sejam excedidos, ações de proteção devem ser executadas de modo a evitar ou reduzir a escala de liberação de materiais radioativos para o meio ambiente.

Para os reatores PWR em regime de potência, as barreiras que permitem reter os materiais radioativos são:

- 1) Matriz do Combustível, onde ficam retidos os produtos de fissão e de ativação de natureza não volátil, assim como o próprio urânio;
- 2) Encamisamento da Matriz do Combustível, onde ficam retidos os produtos de fissão e de ativação de natureza volátil;

- 3) Envelope Estanque do Circuito Primário (barreira de pressão), onde ficam retidos os produtos que venham a transpor as duas primeiras barreiras e outros produtos diluídos ou em suspensão na água de resfriamento (produtos de corrosão, impurezas, resíduos de tratamento químico, o próprio oxigênio componente da água) ativados durante sua passagem pelo interior do núcleo;
- 4) Envelope Estanque de CONTENÇÃO, definida pelo compartimento que contém o Reator e Circuito Primário, resistente à pressão decorrente de uma ruptura total da tubulação principal de resfriamento do Reator, onde ficam retidos todos os produtos anteriormente citados no caso de falha concomitante das barreiras anteriores.

O desempenho destas barreiras sob as diversas CPIN deve ser analisado de forma determinística, i.e. postula-se a ocorrência um determinado Cenário Acidental e verifica-se analiticamente o desempenho da cada barreira. As CPIN postuladas deverão então cobrir quatro domínios de operação:

- a) Normal: inclui CPIN em regime permanente e transitório para as quais as margens de segurança com respeito aos limites tecnológicos das barreiras são tais que não implicam em atuação de nenhuma ação corretiva manual ou automática;
- b) Anormal: inclui CPIN em regime permanente e transitório para as quais as margens de segurança com respeito aos limites tecnológicos das barreiras são tais que implicam em atuação de ações corretivas manuais ou automáticas, que entretanto são reversíveis, permitindo que a instalação volte, em relativamente curto espaço de tempo, ao Domínio Normal de operação, ou que permaneça em operação num modo degradado, eventualmente a potência reduzida;
- c) Incidental: inclui CPIN em regime transitório para as quais as margens de segurança com respeito aos limites tecnológicos das barreiras são tais que implicam em atuação de ações corretivas manuais ou automáticas irreversíveis, não permitindo que a instalação volte, em relativamente curto espaço de tempo, ao Domínio Normal de operação. O objetivo nestas condições é evoluir para uma CPIN em regime permanente do Domínio Anormal, i.e. operação num modo degradado, até serem realizadas ações de manutenção que permitam retornar ao Domínio Normal, e proteger os operadores, já que as primeiras três barreiras

de contenção poderão perder total ou parcialmente sua capacidade de retenção dos materiais radioativos;

- d) Acidental: inclui CPIN em regime permanente e transitório para as quais as margens de segurança com respeito aos limites tecnológicos das barreiras são excedidas, implicando em atuação de ações corretivas manuais ou automáticas irreversíveis tais que a instalação torna-se impossibilitada de retornar ao Domínio Normal de operação. O objetivo nestas condições é garantir a máxima integridade da última barreira de contenção, de forma a evitar a liberação de materiais radioativos para o meio ambiente, dado que a capacidade de retenção dos materiais radioativos pelas barreiras precedentes pode ser gravemente comprometida.

De forma a sintetizar a análise determinística do desempenho das barreiras e, especialmente, determinar a independência entre elas, o que é essencial à análise de segurança nuclear, deve ainda ser realizada a verificação da evolução de acidentes graves, onde a integridade da última barreira é severamente comprometida. Este processo final de análise tem um caráter formal, já que, em certos casos, envolve eventos postulados cuja identificação não é precisa, trazendo, entretanto, a vantagem de permitir a análise da transferência dos produtos radioativos do núcleo para o exterior da instalação e avaliar a ordem de grandeza das consequências radiológicas no caso de perda de integridade de todas as barreiras.

A definição das duas primeiras barreiras é simples, apesar de sua extensão, i.e. o combustível e todo seu revestimento. Não ocorre o mesmo para as outras duas barreiras:

- O envelope estanque do Circuito Primário, apesar de bem definido no interior do compartimento do Reator, ramifica-se para o exterior deste de maneira esparsa. Além disto, o compartimento do Reator não é o único da instalação que contém materiais radioativos. Por estas razões, a delimitação desta barreira não é tão simples e direta como poderia se pensar numa primeira abordagem;
- A sucessão de barreiras possui uma importante descontinuidade nos GV: seus tubos, de espessura pequena e que representam uma área significativa do Envelope Estanque do Circuito Primário, desempenham, para certas CPIN do Domínio Normal, Anormal e Incidental, simultaneamente às funções de Envelope Estanque de Contenção.

O Circuito Secundário, cuja pressão de projeto é inferior à do Circuito Primário, deve ser protegido de eventual sobrepressão por válvulas de alívio. Ele não pode portanto ser considerado como estanque no caso de vazamento de tubos do GV, dado que tal vazamento fará com que sua pressão aumente. Além disto, a manutenção do vácuo nos condensadores requer purgas periódicas de gases incondensáveis que nele se acumulam, dentre os quais poderão ser encontrados produtos radioativos transferidos por eventuais vazamentos nos GV, ainda que em pequenas quantidades que não tragam influências significativas para a pressão do Circuito Secundário. Esta característica peculiar aos Reatores PWR é bem conhecida e constitui uma dificuldade ao princípio de segurança nuclear de interposição de barreiras sucessivas entre os produtos radioativos e o meio ambiente.

Estas reflexões tiveram uma significativa contribuição para evolução deste princípio original para o mais abrangente Princípio de Defesa em Profundidade PDP. Este último inclui o Princípio das Barreiras, mas requer uma análise da instalação mais abrangente e detalhada do que a Análise Determinística das CPIN. A aplicação do PDP irá então conduzir a uma evolução da Análise de Segurança Nuclear constituída pela Análise Probabilística de Segurança APS, que complementa a análise determinística.

2.2.4.2 Princípio de Defesa em Profundidade

A garantia da segurança das instalações nucleares repousa fundamentalmente sobre o Princípio de Defesa em Profundidade PDP:

“Para compensar potenciais falhas humanas e do material, um conceito de defesa em profundidade deve ser implementado, baseado em vários níveis de proteção que incluam sucessivas barreiras físicas e de procedimentos que impeçam a liberação de materiais radioativos para o meio ambiente”
(IAEA-INSAG, 1997).

Ainda que as medidas adotadas para prevenir as falhas ou acidentes procurem evitá-los, postula-se que eles ocorram e, através de sua análise, adota-se meios adequados para enfrentá-los, de forma a garantir que suas conseqüências se encontrem a níveis julgados socialmente aceitáveis. Isso, entretanto, não dispensa a análise de situações ainda mais graves,

que podem resultar de falhas múltiplas ou severas, e que sejam previstos meios para enfrentá-las nas melhores condições possíveis. Seus objetivos são:

- a) compensar as eventuais falhas humanas e técnicas;
- b) manter a eficácia das barreiras, impedindo que ocorram danos ao navio e às próprias barreiras;
- c) proteger o público e o meio ambiente de danos que decorreriam caso as barreiras não fossem plenamente eficazes.

A defesa em profundidade é organizada segundo cinco níveis, apresentados pela Tabela 2.2. As medidas específicas a cada nível são apresentadas pelo Anexo I. Uma falha única, técnica ou humana, ocorrida a um dado nível de defesa, e mesmo combinações de falhas afetando vários níveis, não deverão se propagar, de forma a não comprometer a defesa nos níveis seguintes. A independência dos diferentes níveis é portanto um requisito fundamental.

TABELA 2.2: NÍVEIS DE DEFESA EM PROFUNDIDADE

NÍVEL	OBJETIVO	MEIOS
1	Prevenção das condições de falha ou de funcionamento anormal	Dimensionamento prudente e alto nível de qualidade na construção e operação
2	Controle das condições de funcionamento anormais e detecção das falhas	Sistemas de regulação, limitadores e protetores, e outros dispositivos de vigilância e monitoração
3	Controle das situações acidentais dentro dos limites básicos de projeto	Dispositivos específicos de segurança e procedimentos de operação acidental
4	Controle das situações graves no interior da instalação, compreendendo medidas para impedir a progressão do acidente e para atenuar suas conseqüências	Dispositivos e procedimentos complementares para gerenciamento de situações acidentais
5	Atenuação das conseqüências radiológicas no exterior da instalação decorrentes de liberações de produtos radioativos	Procedimentos de emergência, com intervenção externa à instalação

Ocorrendo uma falha em um nível, o seguinte deverá consequentemente atuar. O objetivo no primeiro nível é impedir a ocorrência de todo funcionamento anormal, assim como

de falhas de sistemas. Ocorrendo uma falha no primeiro nível, o funcionamento anormal deverá ser controlado, ou as falhas detectadas, pelo segundo nível de proteção. Em caso de falha do segundo nível, o terceiro assegura a manutenção das funções de segurança ativando sistemas e dispositivos específicos. Ocorrendo uma falha no terceiro nível, o quarto limita a progressão do acidente por meio de medidas de gerenciamento da situação acidental, de modo a impedir ou atenuar uma situação grave, com liberação de materiais radioativos para o exterior do navio. O último objetivo (quinto nível) é atenuar as consequências radiológicas de liberações significativas ao exterior, por meio de intervenções de emergência nas áreas externas afetadas.

Os operadores, o público e o meio ambiente são protegidos, em última instância, pela sucessão de barreiras físicas, que podem servir tanto a fins de funcionamento e segurança, como somente de segurança. O PDP se aplica à proteção da integridade destas barreiras contra todas as ameaças internas e externas. Nas situações normais de operação em que uma ou várias barreiras são violadas, por exemplo durante a carga de combustível do reator, são requeridos dispositivos especiais temporários para garantir a continuidade do confinamento dos materiais radioativos.

A aplicação do PDP se apoia na análise determinística de um número suficiente de CPIN (sucessão lógica de eventos de origens internas, externas ou combinadas), postuladas como as mais críticas que poderiam ocorrer na instalação, evidentemente dentre aquelas que possuam alguma verossimilhança.

Esta análise determinística deve ser complementada por uma análise probabilística que permita comprovar o atendimento aos objetivos de segurança face aos estados finais das CPIN analisadas. A seleção das CPIN é então uma etapa fundamental que deve ser implementada desde o início do estudo do projeto.

2.2.5 ANÁLISE DE SEGURANÇA NUCLEAR

O procedimento convencional de análise de segurança é baseado na análise determinística de um conjunto de CPIN estabelecido *a priori* ao qual a instalação deverá funcionar sem implicar em Riscos Subjetivos Intoleráveis para os trabalhadores, o público e o

meio ambiente. Estas CPIN abrangem os Domínios de Operação Normal, Anormal, Incidental e Acidental. A análise é ainda complementada pela verificação das consequências radiológicas de acidentes graves hipotéticos, com consequências severas, para os quais os Riscos Objetivos devem ser mitigados através de procedimentos de emergência adaptados. Estes últimos acidentes, entretanto, não constituem CPIN.

As primeiras CPIN acidentais consideradas são aquelas devidas aos potenciais “pontos fracos” da própria instalação. Os riscos derivados da interação entre os diversos sistemas componentes são progressivamente identificados e incorporados ao escopo da análise. De modo similar, as potenciais agressões externas são identificadas e os resultados de estudos sobre a possibilidade de ocorrência destas agressões passam a ser considerados para determinar os requisitos de projeto e operação.

A análise determinística de segurança consiste portanto na análise das condições de operação, através do estudo dos cenários típicos associados a cada uma delas, em especial aqueles considerados *a priori* como "envelopes", sob o ponto de vista de solicitações à instalação. Compreende as seguintes atividades, cujos resultados são consolidados por um RAS (LIBMANN, 1996; NRC, 1978, 1989, 1996; BNL, 1978; IAEA, 1994):

- a) análise sistemática das CPIN em situação incidental e acidental a partir de hipóteses “envelope”;
- b) análise das agressões de origem interna e externa na instalação nuclear;
- c) avaliação das consequências radiológicas para os trabalhadores, o público e o meio ambiente para as CPIN analisadas;
- d) identificação das funções importantes para a segurança, levando à classificação de segurança dos equipamentos, componentes e estruturas da instalação;
- e) qualificação dos códigos de cálculo utilizados para as análises;
- f) qualificação dos equipamentos, componentes e estruturas classificados como importantes para a segurança (Equipamentos Importantes para a Segurança Nuclear -EIS).

O Anexo J apresenta os princípios e procedimentos básicos da abordagem de análise determinística de segurança das instalações nucleares, em especial daquelas baseadas em reatores de potência do tipo PWR.

Verifica-se que o procedimento geral de análise determinística de segurança nuclear é baseado num processo Identificação Análise Controle. Este procedimento aplicado aos sistemas componentes das instalações nucleares leva à redundância, segregação, garantia de qualidade e restrições operacionais, que visam evitar os acidentes e manter a integridade das barreiras.

Neste aspecto, entretanto, o procedimento de segurança tende a centrar-se fortemente no reator: por exemplo, uma ênfase relativamente menor é dada à área de proteção contra incêndios como sendo uma parte global do sistema. Isto é demonstrado pela ocorrência do incêndio na Central Nuclear de Brown Ferry, nos EUA, e os esforços posteriores para desenvolver as necessárias normas regulatórias (IAEA, 1996). Acredita-se entretanto que, devido à implementação e aceitação geral da abordagem de SDFSI/RAMS na engenharia nuclear desde o seu nascimento, existem poucas áreas que possam ter sido subestimadas nesta extensão.

As restrições operacionais desempenham um importante papel na segurança dos reatores nucleares. Através do procedimento Identificação Análise Controle, as especificações técnicas da instalação nuclear são determinadas e não deverão ser ultrapassadas durante a operação. Os procedimentos operacionais irão então requerer que o reator seja desligado no caso em que uma variável de processo atinja um valor limite de segurança, previsto nas especificações. As especificações técnicas estabelecem ainda as condições mínimas para operação da instalação (por exemplo, a disponibilidade de sistemas, condições ambientais). Caso não sejam atendidas, isto implicará em desligamento do reator ou em ações corretivas permitidas pelas especificações técnicas (IAEA, 1979). Tais ações corretivas podem ser uma redução de potência ou uma limitação do tempo de operação.

Essencialmente, considera-se que o desligamento do reator sempre resultará num estado final mais seguro, ou seja, em um incidente ou acidente menos severo. Tal abordagem enfatiza, portanto, a estabilidade e integridade do reator como a principal preocupação de segurança. Tal abordagem implica que os requisitos de segurança têm sempre prioridade com respeito aos requisitos de disponibilidade.

O procedimento convencional de análise determinística possui um aspecto probabilístico, à medida que é baseado, implícita ou explicitamente, em critérios qualitativos para avaliar a verossimilhança de eventos indesejados e para avaliar a gravidade de suas consequências. Estes critérios qualitativos são representados por expressões subjetivas da probabilidade de ocorrência (tais como: freqüente, ocasional, provável, improvável, raro, hipotético) e da gravidade das consequências representadas por expressões subjetivas da probabilidade de ocorrência das CPIN (tais como: desprezível, marginal, crítica, catastrófica).

Com efeito, a análise determinística requer análises probabilísticas parciais e limitadas a sistemas, sub-sistemas e componentes para justificar hipóteses e premissas assumidas. A demanda social por segurança associada à consolidação dos métodos de análise da SDFSI/RAMS e ao estabelecimento de bases de dados de funcionamento específicas conduziram, entretanto, a uma evolução no sentido de buscar-se a efetiva quantificação dos riscos residuais, verificando-se assim os objetivos gerais de segurança assumidos para a instalação, ensejando o desenvolvimento de um procedimento de análise probabilística global.

Nos EUA, em 1975, foi apresentado o primeiro estudo global de risco de fusão de núcleo (NRC, 1975) de reatores de potência. A tendência atual é de generalizar a abordagem probabilística, buscando determinar globalmente o nível de risco efetivamente incorrido pelo público como consequência da operação da instalação nuclear. Os níveis assim determinados podem ser comparados a objetivos preestabelecidos, permitindo um efetivo Gerenciamento de Riscos.

O interesse de análise probabilística global reside sobretudo na análise de todos os fatores em jogo e na evidência dos pontos relativamente fracos da instalação. Este tipo de análise terá um papel fundamental na segurança do projeto e operação dos reatores do futuro. O objetivo probabilístico estabelecido para os futuros reatores europeus prevê a ocorrência de menos de um acidente com consequências graves para o público a cada um milhão de anos (LIBMANN, 1996). Isto corresponderia a um período de retorno de vinte mil anos de funcionamento, considerando-se um parque eletronuclear composto por cinquenta reatores.

O Anexo K apresenta e discute os princípios e procedimentos básicos da abordagem probabilística de análise de segurança. O método probabilístico básico utilizado para esta

análise é o Método da Árvore de Consequências, sendo as probabilidades de transição entre eventos avaliadas por Análise de Modos de Falha, Efeitos e Criticidade, Método da Árvore de Falhas e Método do Espaço de Estados. O emprego destes métodos é discutido pelo Anexo G.

2.3 SEGURANÇA NAVAL

Nesta seção será discutida a Segurança Naval, entendida aqui como a “Segurança Marítima”, típica das condições normais de paz, e a “Capacidade de Sobrevivência” (*Survivability*), típica das condições de guerra ou conflito e que integra os aspectos de “Suscetibilidade” e de “Vulnerabilidade” de um navio a ameaças externas, sendo diretamente aplicável, dentro de suas particularidades, aos SNA.

Serão definidos o escopo e os objetivos gerais da Segurança Naval, os riscos potenciais dos submarinos e as funções básicas de segurança que fazem face a estes riscos. Estas funções de segurança serão então analisadas sob o ponto de vista da Segurança Marítima e da *Survivability*.

2.3.1 ESCOPO

A engenharia naval dos submarinos militares é apresentada e discutida de forma abrangente por (GABLER, 1986; BURCHER e RYDILL, 1994; GUIMARÃES, 1991; JACKSON, 1992). A história de seu desenvolvimento técnico e de seu emprego militar é apresentada por (VAN DER VAT, 1994; HARRIS, 1997). Seu interesse para o Poder Naval Nacional é discutido por (SRPM, 1996; FLORES, 1988; COSTA, 1997).

A segurança naval dos navios de guerra em geral, e dos submarinos militares em particular, envolve dois aspectos complementares, destacados a seguir.

- a) “Segurança Marítima” ou “Segurança de Navegação”, típica de condições normais de paz (PINIELLA, 1996) e cujos fundamentos são estabelecidos pela International Maritime Organization IMO e pelas normas das sociedades classificadoras. A abordagem tradicional tem sido essencialmente atender aos objetivos de proteger a tripulação de eventos que possam causar morte ou injúrias pessoais (SOLAS, 1992); proteger as populações de eventos ocorridos em navios ou instalações portuárias, que possam causar

morte ou injúrias pessoais, proteger as zonas oceânica, costeira e portuária de eventos ocorridos em navios ou instalações portuárias que possam causar danos ambientais (MARPOL, 1978); e proteger a integridade física dos navios e instalações portuárias de modo a evitar perdas de propriedades. São reconhecidos três princípios básicos para o cumprimento destes objetivos:

- minimizar as possibilidades de ocorrência de acidentes;
- minimizar as consequências de um acidente e as possibilidades de perda do navio;
- maximizar as possibilidades de sobrevivência, socorro e resgate da tripulação em caso de perda ou abandono do navio.

b) “Capacidade de Sobrevivência” ou “*Survivability*”, típica de condições de guerra ou conflito grave (GERALD, 1994), que integra dois aspectos complementares:

- “Suscetibilidade”: possibilidade de insucesso na missão face as ameaças de caráter militar (sistemas de armas operados pelo inimigo); sua análise permite avaliar a ameaça militar num sentido amplo, fornecendo uma avaliação probabilística de ser detectado pelo inimigo (“assinaturas” eletromagnética, acústica, térmica), de ser afetado pelo seu armamento (“superfície de alvo” visual, térmica, radar, sonar) e de resistir aos efeitos destas armas (choques, incêndios, alagamentos, perturbações eletromagnéticas, agentes nucleares, químicos e biológicos); e
- “Vulnerabilidade”: gravidade das consequências para o navio e sua tripulação decorrente de agressões e acidentes; sua análise considera a evolução de cenários derivados de um evento inicializador indesejado de origem interna ou externa ao navio, identificado pela análise de suscetibilidade, fornecendo uma avaliação probabilística do estado final do sistema-navio.

2.3.2 OBJETIVOS

Historicamente, a ênfase da Segurança Marítima tem sido colocada sobre o próprio navio como meio de atingir o objetivo de segurança da vida humana no mar. Mais recentemente, a mesma abordagem tem sido aplicada para a proteção do meio ambiente, ou seja, proteger o navio de falhas catastróficas sob condições acidentais implica em proteger também o meio ambiente.

Esta doutrina é implementada pela combinação de diversas ações exercidas ao longo de toda a vida útil do navio, desde sua concepção até seu descomissionamento. Estas ações incluem o desenvolvimento de normas e regulamentos, revisão e aprovação do projeto, inspeção e re-inspeção para certificação, requisitos mínimos de tripulação, e licenciamento de operadores.

Uma característica fundamental da Segurança Marítima é o seu caráter global. Seus objetivos devem, portanto, ser perseguidos em três áreas de atuação distintas:

- desenvolvimento de normas e padrões de segurança a nível internacional, com base na colaboração e intercâmbio de informações técnicas estabelecida através da IMO;
- implementação e imposição, a nível nacional, das normas e padrões internacionais globalmente acordadas; e
- desenvolvimento, implementação e imposição de normas e padrões a nível nacional para aqueles aspectos que ainda não foram suficientemente bem definidos internacionalmente ou que envolvam peculiaridades locais.

Observa-se que, apesar de ao longo dos últimos 150 anos a necessidade de normas regulamentadoras da Segurança Marítima ter sido crescentemente reconhecida, a segurança propriamente dita tem sido derivada de uma abordagem “após os fatos”, ou seja, através de um procedimento de “reação ao desastre” do tipo Acidente Investigação Correção. Neste processo, as atividades de correção, na grande maioria das vezes têm reforçado a sobrevivência do navio como meio primordial de proteção da vida humana no mar.

Felizmente tem se observado uma notável mudança de ênfase na regulamentação da Segurança Marítima, que vem cada vez mais adotando uma abordagem racional, baseada na disciplina de SDFS/RAMS, utilizando-se dos seus métodos para acompanhar os avanços da inovação tecnológica no setor naval, levando à abordagem da Capacidade de Sobrevivência (ALDWINCKLE e POMEROY, 1982; ATMA, 1994; HARRINGTON, 1970; ZHAREN e DUNCAN, 1994; SNAME, 1994). Apesar destes métodos não serem ainda universalmente adotados nas aplicações navais, nota-se a influência da abordagem de segurança no desenvolvimento relativamente recente dos códigos da IMO aplicáveis a navios para

transporte de gás, navios para transporte de produtos químicos, navios petroleiros e navios baseados em efeitos de suportação dinâmica.

A análise de Capacidade de Sobrevivência de sistemas foi também utilizada para a revisão da Convenção Internacional para a Segurança da Vida Humana no Mar *Safety-Of-Life-At-Seas SOLAS*, particularmente naqueles capítulos relacionados com a proteção contra incêndios e aplicações de salvatagem de pessoal embarcado (SOLAS, 1992).

Considerando os aspectos operacionais da segurança dos navios, a mesma tradição histórica de “navio em primeiro lugar” geralmente permanece verdadeira. Devido ao alto valor de um grande navio e de sua carga útil, é normal que o comandante tome todas as decisões necessárias para assegurar sua sobrevivência, incluindo forçar a operação de sua instalação de máquinas até os limites de sua resistência, e até mesmo encalhar voluntariamente o navio antes que ele afunde, de modo a facilitar o socorro à tripulação e o salvamento do navio e de sua carga.

Em resumo, pode-se concluir que, tanto tradicionalmente como em termos dos novos métodos de SDFSI/RAMS aplicados à melhoria da segurança dos navios, a própria sobrevivência do navio é a principal preocupação, o que resulta, via de regra, na segurança da tripulação, do público e do meio ambiente.

2.3.3 RISCOS POTENCIAIS E FUNÇÕES BÁSICAS

O Riscos Potenciais específicos à segurança naval em condições normais de paz são basicamente os acidentes marítimos, especialmente aqueles denominados de “fortunas do mar” (naufrágio, encalhe, colisão), incêndios, explosões e eventos envolvendo manipulação de cargas, que para os navios de guerra poderão ser armas e munições. De maneira similar à Segurança Nuclear, a Segurança Naval irá requerer o atendimento, pelo navio, de funções básicas de segurança.

Diferentemente da Segurança Nuclear, não identifica-se no caso da Segurança Naval um conjunto convencional de CPIN classificadas segundo sua Frequência Anual de Ocorrência FAO estimada *a priori*, conforme apresentado pelo Anexo J. Será portanto

desenvolvida, a seguir, uma identificação de situações operativas que representem riscos potenciais específicos aos submarinos, categorizados de acordo com sua FAO estimada.

A base de dados de incidentes e acidentes marítimos desenvolvida pelo Lloyd Register of Shipping, cobrindo navios mercantes por classificados por esta sociedade, ordena estes eventos em nove categorias e estabelece as FAO para cada uma delas, apresentadas pela Tabela 2.3 (LMIS, 1994). Note-se que as quatro primeiras categorias se referem às chamadas “fortunas do mar”.

TABELA 2.3: ACIDENTES MARÍTIMOS NA MARINHA MERCANTE
(frequência em eventos / 1.000 navios mercantes - ano)

CAT	DESCRIÇÃO	FAO
1	NAUFRÁGIO: inclui navios que afundaram como resultado de mau tempo, alagamento, emborcamento, ruptura generalizada do casco, etc., e não como consequência das categorias 2-7 e 9	1,0
2	ENCALHE: inclui navios que sofreram choque com o fundo do mar ou com restos de naufrágios, independente do tempo que permaneceram retidos	4,7
3	ABALROAMENTO: inclui navios que atingiram ou foram atingidos por elementos externos que não outros navios ou o fundo do mar (categorias 2 e 4), tais como plataformas de petróleo fixas ou quando rebocadas	1,8
4	COLISÃO: inclui navios que atingiram ou foram atingidos por outros navios estando no mar, atracados ou fundeados, não incluindo restos de naufrágios (categoria 2)	3,2
5	INCÊNDIO E EXPLOSÃO: quando o incêndio é o primeiro evento reportado, exceto se for uma consequência de falha do casco ou de máquinas (categoria 8)	3,8
6	DESAPARECIMENTO: quando após um período de tempo razoável não são recebidas notícias do navio ou quando seu destino final é indeterminado	0,2
7	PERDA OU DANO EM GUERRA: inclui navios avariados ou afundados quando operando em teatros de operações militares ou por atos hostis	0,3
8	AVARIAS DE CASCO E MÁQUINAS: inclui navios perdidos ou avariados como resultado de avaria ou falha que não atribuída às categorias 1-7 ou 9	10,2
9	DIVERSOS: inclui navios que foram perdidos ou avariados por causas desconhecidas ou por outras razões não classificadas	0,1
TOTAL		25,3

Verifica-se então que a FAO total, incluindo todas as categorias de eventos para navios mercantes, é de 25,3 eventos / 1.000 navios.ano. Analisando-se as condições

particulares em que estes eventos ocorreram (STANSFELD, 1994) pode-se concluir que, considerando os tempos passados pelos navios em mar aberto e em áreas portuárias ou de águas restritas, uma alta proporção de eventos indesejados ocorre nestas últimas regiões, o que reforça a importância do desenvolvimento de procedimentos operacionais abrangentes e do treinamento das tripulações para reduzir a probabilidade deste tipo de situações.

A única base de dados de incidentes e acidentes marítimos envolvendo navios de guerra em condições normais de paz disponível na literatura aberta, não classificada por razões de sigilo militar, foi desenvolvida pela Organização Não-Governamental ONG *Greenpeace* (HANDLER, 1990). Nela são identificados 1.554 eventos no período de 1945-1989, classificados em 12 categorias, não permitindo, entretanto, a determinação direta das FAO já que não existem registros do volume total de operações, em termos de navios-ano no período, durante o qual estes eventos ocorreram.

Esta base de dados, entretanto, permite determinar as Frequências Relativas de Ocorrência FRO de cada uma das 12 categoria de eventos. Conhecidas as FRO e fazendo-se a hipótese de que a FAO total de eventos nas marinhas de guerra em situações de paz é igual à FAO total de eventos nas marinhas mercantes apresentada pela Tabela 2.3, pode-se determinar as FAO referentes às categorias de eventos em navios militares considerando-se que a FAO de cada categoria é igual a sua FRO multiplicada pela FAO total. Os valores obtidos por esta relação são apresentados na Tabela 2.4.

$$\text{FAO categoria} = (\text{FRO categoria}) \cdot (\text{FAO total}) \quad [2.23]$$

Cumprе ressaltar que esta hipótese possui um caráter fortemente estimativo. Para estabelecer uma aproximação mais precisa, seria necessário levantar-se ano a ano, durante todo o período coberto pela base de dados, o número total de navios existentes nas marinhas de guerra do mundo e o número de dias de mar que cada um destes navios efetivamente realizou. As grandes margens de incerteza associadas a um tal levantamento faria com que o valor assim determinado não fosse significativamente mais preciso do que aquele derivado da hipótese adotada. Note-se ainda que dois fatores contribuem para considerar que,

qualitativamente, a FAO de eventos nas marinhas mercantes é similar a FAO de eventos nas marinhas de guerra:

- Os navios de guerra praticam, em condições normais de paz, operações militares que potencialmente envolvem maiores riscos do que as operações de navios mercantes;
- Por outro lado, os navios de guerra, via de regra, operam com tripulações mais numerosas e melhor treinadas, além de serem projetados, construídos, operados e mantidos com o objetivo de suportarem solicitações mais graves do que os navios mercantes.

TABELA 2.4: ACIDENTES MARÍTIMOS NA MARINHA MILITAR
(frequência em eventos / 1.000 navios de guerra - ano)

CATEGORIA	DESCRIÇÃO	FRO	FAO
A	COLISÃO	31,25%	7,9
B	INCÊNDIO	18,30%	4,6
C	ENCALHE	8,91%	2,3
D	EXPLOSÃO	7,81%	2,0
E	FALHA DE EQUIPAMENTO	6,72%	1,7
F	NAUFRÁGIO	5,14%	1,3
G	MAU TEMPO	4,46%	1,1
H	PROPULSÃO	4,04%	1,0
I	ARMAS E MUNIÇÕES (sem explosão)	3,70%	0,9
J	QUEDA DE AERONAVES	2,33%	0,6
K	ALAGAMENTOS	1,85%	0,5
L	DIVERSOS	5,48%	1,4
TOTAL		100%	25,3

A base de dados da ONG Greenpeace permite ainda determinar as FRO dos eventos com respeito à classe de navio de guerra afetado. Verifica-se que a FRO referente aos

submarinos corresponde a cerca de 25% do número total de eventos identificados considerando-se todas as classes de navios de guerra afetados. Mais uma vez aqui não é possível determinar-se diretamente a FAO correspondente, tendo vista a não disponibilidade dos (submarinos . ano) no período.

Verificando-se, entretanto, a composição das marinhas de guerra mundiais nos últimos 10 anos (SHARPE, 1998), observa-se que os submarinos contribuem com cerca de 15% do número total de unidades navais operativas. Faz-se então as seguintes hipóteses, que permitem determinar a razão existente entre a FAO de eventos envolvendo submarinos FAO_{sub} e a FAO de eventos envolvendo navios de guerra em geral FAO_{ng} :

- a relação entre o número de submarinos e o número total de navios de guerra (incluindo os submarinos) nas marinhas de guerra do mundo manteve-se constante ao longo de todo o período abrangido pela base de dados; e
- os submarinos, em média, perfazem um número de dias de mar por ano igual àquele correspondente à média de todos os navios de guerra (incluindo os próprios submarinos).

$$(\text{Submarinos.Ano}) / (\text{Navios de guerra.Ano}) = Sa / Na = 15\% \quad [2.24]$$

$$(\text{Eventos Submarinos}) / (\text{Eventos Navios de guerra}) = Es / En = 25\% \quad [2.25]$$

$$Es / Sa = FAO_{sub} = (25\% / 15\%) \cdot (En / Na) = 167\% FAO_{ng} \quad [2.26]$$

Com base na hipótese já feita de que a FAO de eventos para navios de guerra é igual a FAO de eventos para navios mercantes, pode-se então determinar a FAO de eventos em submarinos, que corresponderá a 42,3 eventos / 1.000 submarinos-ano.

A base de dados da ONG Greenpeace permite ainda determinar as FRO das diversas categorias considerando-se apenas os eventos envolvendo submarinos. Verifica-se que a distribuição das FRO por categoria de acidente para os submarinos tem uma distribuição diferente daquela observada para o conjunto dos navios de guerra. Esta constatação estatística poderia ser atribuída às peculiaridades do projeto e operação desta classe de navio de guerra. Uma comparação entre as FRO das diversas categorias para os

acidentes envolvendo submarinos e navios de guerra em geral são apresentadas pela Figura 2.9.

Observa-se pela Figura 2.9 que a importância relativa dos eventos de colisão e encalhe são menores no caso de submarinos. Por outro lado, nota-se a significativamente maior importância de eventos de falhas de equipamentos, de incêndios e de acidentes não explosivos ligados ao manuseio de armas e munições, que no caso de submarinos envolvem basicamente os torpedos e, em menor escala os mísseis.

É interessante ressaltar que não existem registros de acidentes de quedas de aeronaves em submarinos. Tais acidentes, entretanto, são verossímeis, dado que existem condições tático-operativas em que a transferência de carga ou pessoal entre helicópteros e submarinos operando na superfície pode tornar-se necessária. Uma falha crítica na aeronave durante uma tal manobra poderia levar a sua queda sobre o submarino, que entretanto se daria a partir de uma altura relativamente baixa, até 2-3 vezes a altura total do submarino acima de sua linha d'água na superfície.

**FIGURA 2.9: COMPARAÇÃO DAS FRO DE ACIDENTES MARÍTIMOS PARA
SUBMARINOS E PARA NAVIOS DE GUERRA EM GERAL**

Com base nas hipóteses feitas para determinação da FAO e nos valores observados das FRO, pode-se elaborar uma categorização de acidentes marítimos envolvendo submarinos militares usando-se a relação [2.23]. Os valores obtidos são apresentados pela Tabela 2.5, constituindo uma identificação e classificação das Situações Operacionais do Submarino SOS a serem analisadas, sob o ponto de vista de segurança, em conjunto com as CPIN de sua IPN.

TABELA 2.5: ACIDENTES MARÍTIMOS COM SUBMARINOS MILITARES
(frequência em eventos / 1.000 navios de guerra - ano)

CATEGORIA	DESCRIÇÃO	FRO	FAO
A	COLISÃO	11,99%	5,1
B	INCÊNDIO	27,10%	11,5
C	ENCALHE	2,88%	1,2
D	EXPLOSÃO	3,36%	1,4
E	FALHA DE EQUIPAMENTO	12,23%	5,2
F	NAUFRÁGIO	0,48%	0,2
G	MAU TEMPO	3,36%	1,4
H	PROPULSÃO	7,43%	3,2
I	ARMAS E MUNIÇÕES (sem explosão)	14,63%	6,1
J	QUEDA DE AERONAVES	0,00%	0,0

SÍNTESE DE DOCTRINA DE SEGURANÇA
PARA PROJETO E OPERAÇÃO DE SUBMARINOS NUCLEARES

K	ALAGAMENTOS	9,11%	3,8
L	DIVERSOS	7,43%	3,1
TOTAL		100%	42,3

Para o atendimento dos objetivos da Segurança Marítima, fazendo face aos Riscos Potenciais acima identificados, o projeto, a construção e a operação dos navios (não serão aqui abordadas as instalações portuárias) deverão garantir o cumprimento de sete funções básicas:

- I) Disponibilidade de Energia, que garante o funcionamento do sistema de acionamento do eixo propulsor e dos demais sistemas internos indispensáveis ao cumprimento das demais funções;
- II) Navegabilidade, incluindo auxílios à navegação, comunicações externas e informações meteorológicas, que garantem que o navio não opere involuntariamente em condições ambientais adversas e são de vital importância para evitar colisões e encalhes;
- III) Integridade Estrutural do envelope estanque, que garante a flutuabilidade do navio;
- IV) Estabilidade Estática transversal e longitudinal, que garante critérios limitantes para as atitudes do navio (trim, banda e calado), obtida pelo equilíbrio na distribuição de pesos a bordo;
- V) Manobrabilidade, que garante a navegação dentro dos critérios limitantes de estabilidade dinâmica;
- VI) Habitabilidade, que garante condições ambientais no interior do navio adequadas à vida humana e ao funcionamento de componentes necessários ao cumprimento das demais funções (temperatura, pressão, umidade relativa, composição da atmosfera interna);
- VII) Socorro e Salvamento, que garante o escape da tripulação no caso de perda inevitável do navio e a possibilidade do navio receber auxílio externo.

2.3.4 ANÁLISE DAS FUNÇÕES DE SEGURANÇA MARÍTIMA

Os submarinos militares operam em três condições distintas: superfície, submerso e semi-submerso (submersão à cota periscópica). As sete funções básicas da segurança

marítima então ser atendidas nestas três condições e também nos períodos de transição entre elas.

2.3.4.1 Disponibilidade de Energia

A disponibilidade de energia, função básica necessária ao cumprimento das demais está intimamente associada à continuidade de sua produção. Esta continuidade deve ser garantida tanto em modo de operação normal, na capacidade nominal de produção, como em modo de operação degradado, em capacidade reduzida. A garantia de continuidade da produção de energia é uma decorrência da confiabilidade global do sistema de geração e de sua manutibilidade e reparabilidade.

A confiabilidade global da instalação de geração de energia é obtida através de:

- confiabilidade individual dos componentes e sistemas associados;
- redundâncias de componentes e sistemas críticos para a continuidade da produção; e
- diversidade dos princípios de funcionamento e segregação física dos componentes e sistemas redundantes.

A confiabilidade individual dos componentes e sistemas associados à instalação de geração de energia é obtida através de:

- aplicação de normas e guias de projeto adaptados à utilização em submarinos;
- aplicação de um sistema de garantia da qualidade ao projeto e fabricação que assegure o fiel cumprimento das especificações técnicas elaboradas;
- execução de testes de desempenho e análises de confiabilidade que confirmem o cumprimento e validem a aplicação das especificações técnicas elaboradas; e
- aplicação de um sistema de manutenção preventiva planejada que assegure a continuidade no tempo do cumprimento das especificações técnicas elaboradas.

A redundância de sistemas críticos para a continuidade de produção de energia deve atender ao critério de falha única, que consiste em garantir que sua função deve poder ser cumprida de maneira satisfatória mesmo em caso de falha de qualquer um de seus componentes. A aplicação deste critério pode implicar na divisão da instalação de geração de energia em sub-unidades que gozem de um certo grau de independência funcional.

A diversidade dos princípios de funcionamento e segregação física dos componentes e sistemas redundantes, bem como das sub-unidades independentes, têm como objetivo limitar as consequências das falhas em modo comum. Estas falhas têm origem em deficiências de projeto, de fabricação e de manutenção, que podem ser reproduzidas em diversos componentes de mesmas características, ou em agressões de origem interna ou externa (incêndios, alagamentos, efeitos dinâmicos de ruptura de tubulações, explosões) que atingem uma mesma região do navio.

A manutibilidade e reparabilidade da instalação de geração de energia é obtida através de:

- acessibilidade dos componentes e sistemas críticos para a continuidade da produção de energia;
- aplicação de um sistema de manutenção preventiva, preditiva e corretiva;
- disponibilidade de sobressalentes e ferramentas especiais para manutenção destes componentes e sistemas;
- disponibilidade de pessoal técnico qualificado para execução destas atividades de manutenção.

A acessibilidade implica num projeto de arranjo físico que possibilite rotas de acesso de pessoal, rotas de remoção de equipamentos e espaços livres em torno dos componentes e sistemas críticos para a continuidade da produção de energia.

A aplicação de um sistema de manutenção preditiva implica na implementação de equipamentos e sistemas de monitoração de variáveis de operação significativas dos equipamentos críticos, tais como vibração, ruído, temperaturas, composição físico-química de fluidos de processo, que permitam a diagnose e antecipem atividades de manutenção. Um sistema de manutenção corretiva implica numa coletânea de procedimentos que identifiquem, para cada falha ou avaria, as ações a serem tomadas e o material necessário a estas ações. Para que o sistema de manutenção planejada, preditiva e corretiva possa ser operacionalizado, a disponibilidade de sobressalentes, materiais de manutenção de uso comum ou especial, ferramentas de uso comum e especial e, eventualmente, facilidades de oficina devem ser previstos. Finalmente, a manutibilidade e reparabilidade da instalação só

pode ser obtida por pessoal qualificado e submetido a treinamento continuado a bordo e em terra.

Pelo fato de operarem em três condições diferentes, os submarinos militares têm mais de um sistema de geração de energia. No caso de submarinos convencionais, tem-se diesel-geradores para operação na superfície e na cota periscópica e bancos de baterias para operação submerso. No caso de submarinos nucleares, estes dois sistemas convencionais são mantidos, os bancos de baterias por requisitos de segurança da própria instalação nuclear e para operação submerso ultra-silenciosa (com o reator voluntariamente desligado), e pelo menos um diesel-gerador, também por requisitos de segurança nuclear e como último recurso para retornar à base após um desligamento involuntário do reator sem possibilidade de recuperação no mar.

2.3.4.2 Navegabilidade

Quando navegando na superfície o submarino é especialmente vulnerável devido à suas reduzidas silhuetas visual e de reflexão radar. Suas características geométricas limitam também o alcance de suas luzes de navegação. Por outro lado, quando navegando submerso, é praticamente imune a colisões (excetuando-se quando em manobras táticas envolvendo outras unidades navais) e aos efeitos de mau tempo. Suas comunicações nesta condição submersa são, entretanto muito limitadas (PAIVA, 1988). Durante a transição da condição submerso para superfície o submarino é particularmente vulnerável, pois durante um certo período de tempo perde totalmente seus referenciais de navegação, podendo vir a colidir com alvos na superfície que não foram identificados ao início da manobra.

2.3.4.3 Integridade Estrutural

A Integridade Estrutural do envelope estanque do casco dos submarinos se reveste de uma importância crucial quando opera na condição submerso, não só pelo fato da pressão externa devido à profundidade implicar em grande volumes d'água serem embarcados por pequenas aberturas, rapidamente inviabilizando qualquer tentativa de esgoto por bombas (HELLER, 1972), como também pelo fato de, na condição submerso, o submarino não possuir praticamente nenhuma reserva de flutuabilidade.

O projeto de submarinos considera as seguintes profundidades típicas, em ordem crescente, que implicam em carregamentos estáticos distribuídos de pressão da água do mar sobre o seu envelope estanque:

- i) calado de operação normal na superfície, na qual a velocidade é limitada pelo grande aumento da resistência ao avanço do navio;
- ii) profundidade de operação normal à cota periscópica, na qual a velocidade é limitada pelos efeitos de arrasto hidrodinâmico e vibrações induzidas nos mastros;
- iii) profundidade mínima de operação na máxima velocidade, limitada pelo risco de emersão involuntária;
- iv) profundidade máxima de “hovering” (velocidade nula), limitada pelos procedimentos de recuperação;
- v) profundidade máxima de operação na máxima velocidade, limitada pelos procedimentos de recuperação;
- vi) profundidade máxima de operação, limitada pelos procedimentos de recuperação;
- vii) profundidade de teste de imersão profunda, realizado após períodos de reparos;
- viii) profundidade máxima de recuperação (“overshooting”) após o mais grave acidente postulado de travamento de hidroplanos na posição de mergulho;
- ix) profundidade máxima de recuperação após o mais grave acidente postulado de água aberta;
- x) profundidade máxima para salvamento da tripulação;
- xi) profundidade mínima de colapso (limite inferior do intervalo de confiança da profundidade de cálculo);
- xii) profundidade de cálculo estrutural do casco resistente; e
- xiii) profundidade máxima de colapso (limite superior do intervalo de confiança da profundidade de cálculo).

As profundidades iii) a vi) são determinadas pelo envelope de segurança. As profundidades vii) e ix) são determinadas pela análise de vulnerabilidade. A profundidade x) é determinada pela características de desempenho dos veículos de salvamento a grande profundidade disponíveis. As profundidades xi) a xiii) são determinadas pela aplicação do

método da resistência-carregamento ao projeto estrutural do casco resistente (FAULKNER e DAS, 1990).

O projeto estrutural de submarinos considera ainda os seguintes carregamentos sobre o seu envelope estanque:

- i) carregamentos dinâmicos provenientes da propagação de ondas de choque na água do mar originadas por explosões submarinas;
- ii) carregamentos dinâmicos provenientes de colisões com outros navios, submarinos ou outras estruturas marítimas ou portuárias, pouso ou choque com o fundo e encalhe na superfície;
- iii) carregamentos dinâmicos provenientes da queda de helicópteros durante manobras militares;
- iv) carregamentos estáticos devidos a manobras normais de esgoto dos tanques de lastro com ar comprimido de baixa pressão à cota periscópica;
- v) carregamentos dinâmicos devidos a manobras de esgoto dos tanques de lastro em emergência com ar comprimido de alta pressão à cota máxima de operação; e
- vi) carregamentos estáticos em anteparas devidos a alagamento de uma subdivisão estanque do casco resistente à cota máxima de salvamento da tripulação.

As diversas profundidades associadas aos carregamentos considerados impõem requisitos de projeto e/ou restrições operacionais a cada um dos componentes do envelope estanque. As profundidades de projeto são interrelacionadas através de coeficientes ou margens de segurança que são esquematizadas pela Figura 2.11. Os carregamentos dinâmicos máximos admissíveis são definidos pela resistência residual do envelope estanque, determinada pela margem de segurança instantânea existente entre a profundidade de operação onde este carregamento ocorre e a profundidade de cálculo.

FIGURA 2.10: CORRELAÇÃO ENTRE PROFUNDIDADE E SEGURANÇA

O envelope estanque resistente à pressão exercida pela água do mar de um submarino pode ser dividido nas seguintes partes distintas:

- i) estrutura do casco resistente à pressão resultante da profundidade de cálculo;
- ii) penetrações no casco resistente à pressão resultante da profundidade de cálculo;
- iii) tanques de lastro externos, resistentes ao diferencial de pressão entre o ar comprimido injetado no seu interior para emersão do submarino e a pressão resultante da cota onde é feita esta injeção;
- iv) anteparas de subdivisão de compartimentos estanques, resistentes à pressão resultante de alagamento na profundidade máxima de salvamento da tripulação;

As penetrações no casco resistente constituem os itens mais vulneráveis com respeito à integridade da estanqueidade do submarino, especialmente com respeito aos carregamentos dinâmicos. Elas incluem uma miscelânea de itens que, por esta razão, tornam-se importantes para a segurança do navio:

- peças de passagem pelo casco resistente;
- válvulas de casco fixadas diretamente sobre as peças de passagem pelo casco resistente;
- tubulações de água do mar e seus acessórios (válvulas, instrumentos, filtros) que alimentam equipamentos internos ao casco resistente;

- equipamentos internos ao casco resistente (basicamente trocadores de calor) alimentados com água do mar;
- equipamentos internos ejetores ao casco resistente (tubos de torpedos, ejetores de sinais, ejetores de lixo);
- tubulações hidráulicas ou pneumáticas e seus acessórios (válvulas, instrumentos, filtros) que alimentam equipamentos externos ao casco resistente a partir de acumuladores internos ao casco resistente ou que alimentam equipamentos internos ao casco resistente a partir de acumuladores externos ao casco resistente;
- acumuladores hidráulicos ou pneumáticos externos ao casco resistente que alimentam utilizadores internos ao casco resistente;
- utilizadores hidráulicos e pneumáticos externos ao casco resistente alimentados por acumuladores internos ao casco resistente;
- acumuladores hidráulicos ou pneumáticos internos ao casco resistente que alimentam utilizadores externos ao casco resistente;
- utilizadores hidráulicos e pneumáticos internos ao casco resistente alimentados por acumuladores externos ao casco resistente;
- câmaras para escape e trânsito de pessoal do ou para o casco resistente;
- câmaras para embarque e remoção de componentes e/ou armamento (torpedos e mísseis) do ou para o casco resistente;
- câmaras para recolhimento de mastros retráteis (periscópios, antenas); e
- tubo telescópico do eixo propulsor.

A selagem do tubo telescópico é um ponto particularmente vulnerável pois sua falha acarretaria na perda simultânea de estanqueidade e de propulsão (NATACCI, 1997). Para limitar as consequências desta falha do ponto de vista da estanqueidade adota-se dispositivos especiais de vedação, tais como selos infláveis.

Outro ponto particularmente vulnerável são as tubulações de água do mar de pequeno diâmetro, tais como linhas de instrumentação, cuja ruptura, provável quando submetida a carregamentos dinâmicos intensos, pode dispersar no ambiente interno do submarino uma neblina salina podendo causar falhas em equipamentos elétricos que podem conduzir a

cenários acidentais severos, dependendo das condições em que ocorrem e da importância para segurança dos equipamentos atingidos (BENTLEY, 1975).

2.3.4.4 Estabilidade Estática

A Estabilidade Estática é necessária a verificação dos critérios mínimos para os braços BG entre os centros de empuxo e de gravidade nos planos transversal e longitudinal e que o adequado balanceamento entre os pesos no interior do casco resistente e o empuxo total gerado (estado de flutuabilidade neutra) sejam atendidos para todas as condições operacionais submerso.

Deve ainda ser verificado que, em qualquer condição operacional submerso, os tanques de lastro possam ser esgotados de modo a estabelecer um estado de flutuabilidade positiva. Neste estado, levando em conta o empuxo gerado pelo ar nos tanques (nova posição do centro de empuxo B'), os critérios de BG mínimo devem também ser atendidos.

Por outro lado, nas condições operacionais na superfície, os tanques de lastro devem poder ser alagados, de modo a estabelecer-se um estado de flutuabilidade neutra, que permita o mergulho, devendo a ligeira flutuabilidade negativa necessária para efetivar o mergulho ser fornecida pelo alagamento de tanques de compensação internos. Nas condições operacionais na superfície, critérios de estabilidade transversal e longitudinal específicos (comuns a navios de superfície) devem também ser atendidos.

Estas verificações são feitas através do Polígono de Equilíbrio (JACKSON, 1992). Os critérios de BG mínimo devem atender não só aos requisitos estáticos como também aos requisitos dinâmicos e àqueles associados à transição da condição submerso para superfície (BUCHER e RYDILL, 1994);

2.3.4.5 Manobrabilidade e Estabilidade Dinâmica

Apesar de aparentemente o submarino possuir uma grande liberdade de manobra nas três direções quando submerso em águas profundas, na realidade ele opera numa lâmina d'água relativamente fina, pois sua profundidade máxima de mergulho é apenas de 3 a 5 vezes o seu comprimento, ou seja, em velocidades e ângulos de trim elevados, o submarino pode atravessar esta lâmina de segurança com respeito a integridade estrutural em muito pouco

tempo, da ordem de minutos, efeito especialmente relevante no caso de emperramento de hidroplanos. Por outro lado, os efeitos de alagamentos podem conduzir rapidamente a um estado de fluviabilidade muito negativa, o que também pode levar a ultrapassagem da profundidade de segurança. Estes efeitos conduzem a restrições operacionais representadas como áreas limitadas sobre um gráfico velocidade x profundidade denominado Envelope de Segurança (Figura 2.10) e ao desenvolvimento de meios e procedimentos de recuperação em emergência específicos (BROWN e CHALMERS, 1989);

2.3.4.6 Habitabilidade

O fato da atmosfera interna do submarino ser um sistema fechado quando em operação submerso requer uma série de sistemas dedicados à purificação (eliminação de componentes nocivos ao homem e aos materiais), regeneração (eliminação do gás carbônico produzido pela respiração biológica e recomposição do teor adequado de oxigênio) e condicionamento (manutenção de níveis de temperatura e umidade adequados) do ar interno.

Considerando a importância desta função, os submarinos são dotados de sistemas de segurança para garantir a respiração dos tripulantes em situações de emergência chamados Built-in Breathing Systems BIBS (GABLER, 1986). A atmosfera fechada, somada aos requisitos de fluviabilidade que limitam o embarque de água, meio convencional de extinção de fogo, coloca também problemas particulares no que tange ao combate a incêndios.

FIGURA 2.11: ENVELOPE DE SEGURANÇA TÍPICO

2.3.4.7 Socorro e Salvamento

O escape da tripulação de submarinos naufragados só pode ser efetuado, evidentemente, se a profundidade é inferior à cota de colapso do casco resistente. Os meios requeridos para o escape dependem da profundidade dentro da qual será realizado: até 80m é possível o escape livre, através das ante-câmaras de acesso ao submarino; até 200m é possível a subida livre, para a qual é necessário equipamento individual de salvamento; para profundidades maiores torna-se necessário o auxílio externo, através de sinos de mergulho ou de veículos submarinos especialmente projetados para esta função (ADAMS, 1988).

2.3.5 ANÁLISE DA CAPACIDADE DE SOBREVIVÊNCIA

A análise da capacidade de sobrevivência (*survivability*) do navio de guerra dentro do contexto de uma dada missão, e face a uma ameaça postulada, cobre simultaneamente a avaliação do estado de disponibilidade dos meios que devem permitir ao navio o cumprimento desta missão e dos meios que devem permitir enfrentar esta ameaça, e uma estima da possibilidade do navio sobreviver aos efeitos desta ameaça dentro de condições pré-definidas.

Pela análise de cada uma das ameaças ou combinações de ameaças que o navio de guerra poderá ter que enfrentar durante o cumprimento de suas missões é possível, em princípio, estimar o estado de disponibilidade global do sistema-navio em operação e otimizar sua capacidade de resistir aos efeitos destas ameaças.

Com efeito, esta abordagem permite avaliar, separadamente, para cada tipo de agressão potencial em relação com as missões, os danos causados ao navio, i.e. à sua estrutura e aos seus equipamentos, e deduzir seu estado de capacidade operacional dentro

das funções básicas vitais que são a mobilidade e a tripulação, assim como dentro das funções básicas de combate. Os resultados da análise podem se revestir de diferentes formas, indo de um simples inventário, por domínio, das avarias provocadas até uma estima do estado de disponibilidade do sistema-navio no seu conjunto, a partir de avaliações de seu estado de disponibilidade dentro de cada uma das funções básicas em questão.

Com o objetivo de atender aos seus objetivo, a análise de *survivability* deve refletir os diferentes estados de disponibilidade do sistema-navio, respectivamente por função básica e no seu conjunto. Isto requer a definição a priori de critérios específicos de avaliação do estado de disponibilidade dentro de cada função básica e de um critério de avaliação do estado de disponibilidade global do sistema navio, incluída a tripulação.

Dentro da Organização do Tratado do Atlântico Norte OTAN, tais critérios de avaliação do estado de disponibilidade dos navios de guerra têm sido objeto de propostas de normalização (GERALD, 1994). São preconizados quatro estados de referência: disponível, ligeiramente degradado, severamente degradado e indisponível. A partir destes critérios, dentro do contexto de uma dada missão, é possível, inicialmente, avaliar separadamente o estado de disponibilidade do navio dentro de cada função básica associada à missão: mobilidade, comando e controle, guerra anti-aérea, guerra anti-superfície, guerra anti-submarino. Em seguida, é possível estimar a disponibilidade global do sistema-navio por uma combinação ponderada dos estados obtidos precedentemente dentro de cada função básica.

Os dados necessários à análise são aqueles relativos à descrição do navio, cujo estado inicial poderá ser normal ou degradado, e às agressões postuladas. O nível de detalhamento dos dados dependerá, evidentemente, do propósito da análise: validação ou comparação de alternativas de projeto de sistemas, de arranjo físico e de critérios de resistência adotados; identificação de avarias tais como perda de fluabilidade, de mobilidade e de capacidade de combate.

No que concerne o navio, são requeridos elementos de informação referentes ao arranjo geral, às dimensões e escantilhões estruturais, à identificação de sistemas vitais e sua descrição funcional, e à resistência aos efeitos de armas (choque, sopro, fragmentos) e à tripulação. Para as agressões, são requeridas informações referentes à identificação da

ameaça (convencional, nuclear, química, biológica), as condições da explosão (intensidade, distância, local, marcação, profundidade ou altura), a definição da carga de combate e seus efeitos sobre o pessoal e o material (choque submarino, sopro, explosão ao contato ou a distância, fragmentação, incêndio). Para análise, todas estas informações são evidentemente traduzidas em parâmetros técnicos que poderão ser definidos em termos probabilísticos.

A garantia da *survivability*, ou seja, a segurança de funcionamento do sistema-navio, repousa sobre o mesmo PDP definido para a segurança das instalações nucleares. A análise de suscetibilidade e da análise de vulnerabilidade irá empregar aqueles conceitos fundamentais da SDFSI discutidos nos itens anteriores.

A avaliação da ameaça num sentido amplo, i.e. ser detectado e, em seguida, ser atingido, é o objeto da análise de suscetibilidade, que pode ser entendida como uma Análise Probabilística de Segurança de nível 1. A redução da suscetibilidade cobre o conjunto de medidas tomadas para minimizar a probabilidade de ocorrência do evento indesejado, i.e. ser atingido. Isto implica em detetar sem ser detectado, escapando dos sensores do inimigo pelo aumento da discrição, da furtividade, da capacidade dos próprios sensores, das contra-medidas disponíveis. Estas ações de prevenção compreendem uma primeira linha de defesa.

A análise de vulnerabilidade considera a evolução subsequente à ocorrência do evento indesejado, podendo ser entendida como uma Análise Probabilística de Segurança de nível 2. Ela fornece uma descrição das conseqüências, i.e. das avarias e perdas humanas possíveis. A redução da vulnerabilidade tem como objetivo, inicialmente, assegurar uma resistência intrínseca com respeito às agressões postuladas, minimizando as avarias a níveis aceitáveis. Estas ações de proteção compreendem uma segunda linha de defesa.

Reduzir a vulnerabilidade é também empreender ações para limitar o impacto das agressões sobre a disponibilidade operacional do sistema-navio. É desenvolver arranjos físicos de modo a garantir aos sub-sistemas a máxima probabilidade de integridade, concentrando seus componentes, reduzindo as zonas expostas e segregando sistemas redundantes. É ainda conferir ao sistema-navio capacidades de reconfiguração ou de reparo as mais rápidas possíveis e ao mais alto nível de funcionalidade, prevendo redundâncias funcionais e sobressalentes apropriados, integrando meios e procedimentos de controle de

avarias. O tempo e os custos necessários à restauração das funções representam também um aspecto da disponibilidade do sistema-navio de guerra. Estas ações constituem a terceira linha de defesa.

2.4 SEGURANÇA NUCLEAR NAVAL

Nesta seção será feita uma primeira abordagem global da Segurança da Propulsão Nuclear, sintetizando os conceitos e aplicações da segurança nos três contextos discutidos pelas seções anteriores.

Será feita inicialmente uma identificação de sistemas componentes e das respectivas ações de interface que caracterizam os problemas de segurança específicos à Propulsão Nuclear Naval. A seguir será discutido o aspecto central associado a estes problemas, constituído pelo compromisso entre a Disponibilidade e a Seguridade, que foi tratado de forma genérica pela seção 2.1. O inventário de materiais radioativos contido no núcleo e Circuito Primário de um reator PWR de propulsão naval, fator determinante dos riscos potenciais de uma IPN, será avaliado. Será então feito um delineamento da Doutrina de Segurança proposta caracterizando o processo de otimização do conjugado Disponibilidade x Seguridade. Finalmente, será discutida a aplicação dos métodos de análise da SDFSI/RAMS à análise de segurança de um navio nuclear.

2.4.1 IDENTIFICAÇÃO DE SISTEMAS E INTERFACES

Os navios dotados de uma IPN são analisados como um conjunto composto por quatro “Macro-sistemas”, identificados a seguir, que interagem entre si. A segurança do conjunto resulta, por um lado, da segurança intrínseca de cada um dos Macro-sistemas, e por outro, do controle das conseqüências decorrentes das suas interações.

- I Instalação Nuclear;
- II Navio;
- III Apoio Logístico; e
- IV Ambiente.

A Instalação Nuclear é entendida como aquela parte do navio cuja função é fornecer o vapor necessário à propulsão e à produção de energia elétrica para consumo interno. Ela compreende, para instalações baseadas em reatores PWR (vide Anexo A):

- i. Reator e Circuito Primário;
- ii. Sistemas auxiliares associados ao Circuito Primário;
- iii. Dispositivos Especiais de Segurança;
- iv. Dispositivos Especiais de Blindagem;

O Navio propriamente dito, i.e. excluída a Instalação Nuclear, compreende:

- i. Instalação de Máquinas (vide Anexo A):
 - Circuito Secundário;
 - Sistemas auxiliares associados ao Circuito Secundário;
 - Sistema de Resfriamento dos Condensadores Principais do Circuito Secundário;
 - Sistema de Acionamento do Eixo Propulsor;
 - Eixo Propulsor e Hélice;
 - Sistema Elétrico de Serviço;
 - Sistema Hidráulico de Serviço;
 - Sistema Pneumático de Serviço;
 - Sistema de Ventilação e Condicionamento de Ar.
- ii. Plataforma-Navio:
 - estrutura do casco;
 - sistemas de governo e manobra;
 - sistemas de navegação;
 - sistemas de comunicações internas e externas;
 - sistemas de controle de avarias;
 - tripulação;
 - sistemas associados à habitabilidade do navio e suporte à tripulação; e
 - sistemas associados ao socorro da tripulação e salvamento do navio,
- iii. Carga Útil:
 - sistemas de combate (deteção, contra-medidas, direção de tiro);

- armas e munições; e
- outros sistemas específicos à missão do navio.

O Apoio Logístico é entendido como todas as instalações fixas em terra e móveis no mar (navios, submarinos, aeronaves) que venham a prestar serviços ao Navio e à Instalação Nuclear, compreendendo:

- i. estaleiro de construção;
- ii. bases navais de manutenção e reparo;
- iii. navios tênder, oficina e de socorro e salvamento específicos;
- iv. veículos submarinos de resgate, socorro e salvamento;
- v. outros navios ou aeronaves que possam eventualmente prestar apoio ou operar em conjunto com o navio nuclear.

O Ambiente é entendido como o universo dentro do qual o navio opera, excluídos os 3 Macro-sistemas precedentes, compreendendo:

- i. Ambiente Físico, imposto pelo:
 - mar (o elemento líquido natural e os fundos marinhos);
 - atmosfera;
 - zona costeira próxima, com sua população e seu ambiente industrial;
 - eco-sistemas circundantes;
- ii. Ambiente Operativo, imposto por:
 - emprego do navio;
 - procedimentos táticos; e
 - ameaças de caráter militar, i.e. os meios navais e aeronavais dos inimigos.

Distingue-se dois tipos de ações de interface entre os macro-sistemas:

- I Carregamentos que um Macro-sistema A impõe sobre um Macro-sistema B, que são as ações inevitáveis e restritivas impostas por A em B devido ao funcionamento ou à própria natureza de A;
- II Necessidades expressas por um Macro-sistema A a um Macro-sistema B, que são os requisitos que implicam em uma ação de B em benefício do funcionamento ou da própria natureza de A.

A Figura 2.12 esquematiza estas interfaces e a Tabela 2.6 apresenta os Carregamentos e Necessidades nas interfaces de interesse para a segurança entre os macro-sistemas.

FIGURA 2.12: INTERFACES ENTRE SISTEMAS DO AMBIENTE-NAVIO

TABELA 2.6: INTERFACES ENTRE SISTEMAS DO AMBIENTE-NAVIO

CARREGAMENTOS	NECESSIDADES
INSTALAÇÃO NUCLEAR	NAVIO
<ol style="list-style-type: none"> 1. Suportação e arranjo 2. Radiações Ionizantes 3. Descomissionamento 4. Limitações ao sistema de propulsão 5. Acidentes nucleares nas condições de reator ligado e desligado 6. Liberação de materiais radioativos (normal e acidental) 7. Vibrações e ruídos 	<ol style="list-style-type: none"> 1. Fornecimento contínuo de energia, fluidos diversos, ventilação e água de resfriamento 2. Blindagem radiológica 3. Pessoal especializado para operação 4. Serviço de radioproteção 5. Sobressalentes e ferramentas especiais 6. Oficinas 7. Laboratório de análises radio-químicas
INSTALAÇÃO NUCLEAR	APOIO LOGÍSTICO
<ol style="list-style-type: none"> 1. Acidentes nucleares na condição de reator desligado 2. Liberação (ou transferência) de materiais radioativos (normal ou acidental) 3. Período entre recargas de combustível 4. Armazenagem de combustível irradiado e de combustível novo 5. Radiações 6. Descomissionamento 	<ol style="list-style-type: none"> 1. Fornecimento contínuo de energia, fluidos diversos, ventilação e água de resfriamento no cais e em dique seco 2. Instalações especializadas para troca de combustível, processamento de rejeitos e efluentes e descontaminação de componentes 3. Blindagem e confinamento no cais e em dique seco 4. Pessoal especializado de manutenção e reparo 5. Sobressalentes, ferramentas especiais e oficina "quente"
INSTALAÇÃO NUCLEAR	AMBIENTE
<ol style="list-style-type: none"> 1. Liberação de materiais radioativos (normal e acidental) 	<ol style="list-style-type: none"> 1. Água de resfriamento nas condições de operação normais e acidentais

SÍNTESE DE DOCTRINA DE SEGURANÇA
PARA PROJETO E OPERAÇÃO DE SUBMARINOS NUCLEARES

<ul style="list-style-type: none"> 2. Acidentes nucleares nas condições de reator ligado e desligado 3. Descarga de água de resfriamento aquecida (“assinatura” térmica) 4. Descarga de produtos químicos diversos não-radioativos 	<ul style="list-style-type: none"> 2. Qualidade adequada da água de resfriamento (partículas em suspensão, poluentes diversos, organismos vivos, temperatura) 3. Blindagem radiológica exterior ao casco do navio 4. Procedimentos de operação 5. Formação e treinamento de operadores
NAVIO	INSTALAÇÃO NUCLEAR
<ul style="list-style-type: none"> 1. Perfil de missão 2. Ciclos de operação 3. Transmissão dos movimentos do mar 4. Transmissão de choques e vibrações 5. Transmissão de agressões externas 6. Transmissão de agressões internas 7. Presença de tripulantes 8. Ausência de apoio externo (quando no mar) 9. “Fortunas do mar” 10. Perturbações eletro-magnéticas 	<ul style="list-style-type: none"> 1. disponibilidade da geração de energia 2. flexibilidade de operação (modos alternativos degradados) 3. manobrabilidade (transitórios bruscos), em especial a chamada “manobra de crash” (passagem de toda força a vante a toda força a ré em curto espaço de tempo)
NAVIO	APOIO LOGÍSTICO
<ul style="list-style-type: none"> 1. Ciclos de Operação (períodos de manutenção) 	<ul style="list-style-type: none"> 1. Fornecimento contínuo de energia, fluidos diversos, ventilação e água de resfriamento 2. Cais de atracação 3. Dique seco 4. Sobressalentes e ferramentas especiais 5. Oficinas 6. Pessoal especializado em manutenção e reparo

SÍNTESE DE DOCTRINA DE SEGURANÇA
PARA PROJETO E OPERAÇÃO DE SUBMARINOS NUCLEARES

TABELA 2.6: INTERFACES ENTRE SISTEMAS DO AMBIENTE-NAVIO (cont.)

CARREGAMENTOS	NECESSIDADES
NAVIO	AMBIENTE
<ol style="list-style-type: none"> 1. Descarga de produtos químicos diversos não-radioativos 2. Fortunas do mar 	<ol style="list-style-type: none"> 1. Condições aceitáveis de navegação 2. Socorro e salvamento 3. Procedimentos de operação 4. Formação e treinamento de operadores
CARREGAMENTOS	NECESSIDADES
AMBIENTE	INSTALAÇÃO NUCLEAR
<ol style="list-style-type: none"> 1. Movimentos do mar 2. Fortunas do mar 3. Agressões externas naturais 4. Agressões externas operacionais 5. Atos de sabotagem 6. Grupo crítico (público afetado) 7. Corrosão 8. Alagamento 9. Borrifos 10. Resfriamento e diluição de boro incontrolados em caso de naufrágio 	<ol style="list-style-type: none"> 1. Avaliação das conseqüências das condições de operação normais e acidentais 2. Procedimentos de emergência
AMBIENTE	NAVIO
<ol style="list-style-type: none"> 1. Movimentos do mar 2. Fortunas do mar 3. Perturbações eletromagnéticas 4. Agressões externas naturais 5. Agressões externas operacionais 6. Atos de sabotagem 7. Grupo crítico (público afetado) 	<ol style="list-style-type: none"> 1. Avaliação das conseqüências das condições de operação normais e acidentais 2. Procedimentos de emergência
AMBIENTE	APOIO LOGÍSTICO
<ol style="list-style-type: none"> 1. Agressões externas naturais 2. Atos de sabotagem 3. Grupo crítico 	<ol style="list-style-type: none"> 1. Avaliação das conseqüências das condições de operação normais e acidentais 2. Procedimentos de emergência
APOIO LOGÍSTICO	INSTALAÇÃO NUCLEAR
<ol style="list-style-type: none"> 1. Agressões externas naturais 2. Agressões externas originadas pelas atividades de manutenção e reparo 3. Atos de sabotagem 4. Grupo crítico 	<ol style="list-style-type: none"> 1. Avaliação das conseqüências das condições de operação normais e acidentais 2. Exige procedimentos de emergência 3. Segurança física
APOIO LOGÍSTICO	NAVIO
<ol style="list-style-type: none"> 1. Agressões externas naturais 2. Agressões externas originadas pelas atividades de manutenção e reparo 3. Atos de sabotagem 	<ol style="list-style-type: none"> 1. Facilidades de base naval 2. Segurança física
APOIO LOGÍSTICO	AMBIENTE
<ol style="list-style-type: none"> 1. Liberação de materiais radioativos (normal e acidental) 2. Acidentes nas instalações nucleares de apoio 3. Descarga de água de resfriamento aquecida (poluição térmica) 4. Descarga de produtos químicos diversos não-radioativos 	<ol style="list-style-type: none"> 1. Avaliação das conseqüências das condições de operação normais e acidentais 2. Procedimentos de emergência

2.4.2 CONJUGADO DISPONIBILIDADE X SEGURIDADE

O caráter “navio” e o caráter “militar” impõem às instalações nucleares embarcadas condições extremamente particulares, muito distintas daquelas impostas às instalações em terra. São aqui consideradas somente as exigências de segurança nuclear dentro de “condições normais de paz”. É evidente que em “condições de conflito grave” ou “condições de guerra declarada” os níveis de riscos considerados socialmente aceitáveis não possuiriam mais os mesmos valores, alterando os conceitos fundamentais de segurança nuclear .

A segurança da instalação nuclear embarcada está intimamente ligada à segurança do navio, que por sua vez depende da disponibilidade da propulsão e da produção de energia elétrica. A confiabilidade e segurança da IPN embarcada constitui assim uma parte integrante e indissociável da segurança global do navio. A instalação nuclear embarcada deve, portanto, ser capaz de:

- a) suportar sem falha variações de potência bruscas, a partir de diversas condições iniciais;
- b) se a segurança do navio exigir, continuar operando excepcionalmente em um modo degradado, dentro de condições menos restritivas do que aquelas correspondentes ao nível de segurança habitualmente requerido.

Um navio militar é um sistema altamente complexo. A instalação nuclear deve assim coexistir com numerosas outras instalações embarcadas suscetíveis de agravar certas solicitações ou de induzir agressões. Os requisitos de arquitetura naval irão, inevitavelmente, limitar as soluções de projeto possíveis. Por exemplo, estes requisitos irão impor:

- ritmos de utilização previstos para o navio e a rotação de tripulações;
- conceitos gerais de manutenção do navio tais como porto-base e frequência de paradas periódicas;
- requisitos de variação de potência em situação normal e em emergência;
- movimentos (jogo, caturro, arfagem) e atitudes (trim, banda, calado) da plataforma;
- características físicas das agressões a serem consideradas;
- conseqüências das "fortunas do mar" (encalhe, colisão, naufrágio).

A peculiaridade dos reatores de propulsão nuclear naval em comparação com os outros tipos de reatores (geração de eletricidade, pesquisa, geração de calor) se prende às seguintes características:

- I. Não-Singularidade e Imbricação com o navio;
- II. Integrabilidade e Adaptabilidade ao navio;
- III. Flexibilidade e Disponibilidade para o navio;
- IV. Segurança Global reator + navio; e

A principal peculiaridade de uma instalação nuclear de propulsão naval está associada à sua própria vocação: comparado com uma central núcleo-elétrica (o mesmo se aplica aos reatores para geração de calor e aos reatores de pesquisa), que representa uma entidade em si mesma (ainda que ligada a uma rede de distribuição de energia elétrica que ela alimenta; já que esta ligação é bastante “fraca” e geralmente não-vital), o reator de propulsão naval é “apenas” um componente de um conjunto mais vasto e mais complexo - o navio - do qual ele faz parte e constitui um componente vital.

Este fato é ainda mais marcante no caso de submarinos, onde a imbricação da instalação nuclear com as demais instalações é muito forte e onde a propulsão deve ter um nível de confiabilidade e disponibilidade ao menos igual àquele dos dispositivos associados à segurança de mergulho. Deve-se ressaltar que a segurança de submarino ou navio de superfície sem propulsão é extremamente vulnerável à menor avaria ou dificuldade de navegação.

O reator de propulsão naval constitui, deste modo, um componente vital de um conjunto complexo, imbricado e integrado: “o navio”, cuja finalidade não depende da tecnologia de propulsão adotada.

Uma outra característica essencial do reator de propulsão naval é sua capacidade de integrar-se a bordo do navio. Esta noção de integrabilidade recobre diversos aspectos. Os mais evidentes são os imperativos de peso e volume, sobretudo no caso de submarinos, cujas margens de projeto e construção para equilíbrio de pesos e momentos são sempre muito limitadas, e para o qual a redução das dimensões das aberturas de acesso é um objetivo importante, mas igualmente no caso de navios de superfície, para os quais a presença de um

componente tão pesado e volumoso tal como a contenção de um reator perturba a harmonia do projeto dos conveses e a resistência mecânica da “viga-navio”, tendo em conta, aqui também as aberturas de acesso geralmente de grandes dimensões.

Estas limitações, que nas origens da propulsão nuclear naval constituíram as causas principais de fracasso de alguns projetos, tais como a tentativa francesa de desenvolvimento de um sistema baseado em reator de urânio natural/água pesada (MNF, 1992), continuam essenciais: as técnicas pelas quais elas são contornadas medem o desempenho comparado das instalações de propulsão naval (relações peso/potência, volume/potência).

Na prática, os requisitos de minimização do peso concernem sobretudo o projeto da proteção biológica (blindagens) do reator. Com efeito, se definirmos o peso desta proteção como sendo o peso adicional necessário ao sistema para atender as normas de radioproteção que são impostas sobre o projeto, este peso adicional pode representar, a grosso modo, até metade do peso total do sistema, no caso extremo de um reator embarcado em um submarino de pequeno deslocamento (JAEGER, 1975).

Se as limitações de volume e de peso (principalmente da proteção biológica) são importantes, elas não são, entretanto, as únicas a caracterizar a integrabilidade e a adaptabilidade ao navio.

De uma maneira geral, o ambiente-navio (definido como o conjunto de condições particulares impostas ao reator pelo fato dele estar embarcado) constitui uma fonte de requisitos para o projetista da instalação nuclear, muito distintos daqueles impostos às instalações em terra.

- a) os movimentos de plataforma e em particular as inclinações, que constituem um elemento de complexidade suplementar onde existe uma superfície livre líquida (GV, PZ) e sobre o projeto mecânico de sistemas (suportação, resistência mecânica aos choques);
- b) as acelerações de plataforma e os choques resultantes de explosões submarinas próximas ao casco.

O ambiente-navio é hostil à instalação nuclear, que por outro lado vê-se obrigada a contar exclusivamente com os recursos embarcados no navio em caso de dificuldade.

Simultaneamente, a instalação nuclear deve ser projetada, em todos os seus aspectos, de modo a minimizar os requisitos que ela impõe ao projeto e à operação do navio. Isto pode conduzir, em alguns casos, à renúncia a certas soluções usuais em instalações nucleares terrestres (GLASSTONE e SESONSKE, 1994) como, por exemplo:

- a) o controle de reatividade de reatores PWR por veneno solúvel (ácido bórico), que conduz a grandes quantidades de efluentes não rejeitáveis diretamente para o mar, o que complicaria sobremaneira os circuitos auxiliares da instalação;
- b) o controle químico da composição da água do Circuito Secundário por tratamento envolvendo processos de volatilização, impraticável dentro do espaço confinado que representa um submarino.

A instalação nuclear de propulsão naval é um componente vital de um conjunto mais vasto e complexo. Isto implica que uma de suas qualidades essenciais reside na sua Disponibilidade Instantânea, que deverá ser máxima. Esta noção de disponibilidade total ao “chamado da função”, não deve ser confundida com a Disponibilidade Potencial das centrais eletronucleares, definida como a razão entre a energia efetivamente produzida e a energia que potencialmente poderia ter sido produzida.

A continuidade da produção de energia deve ser garantida, notadamente durante os transitórios bruscos e freqüentes que caracterizam o operação do navio. Isto conduz na prática a buscar a máxima flexibilidade de utilização para a instalação nuclear. O requisito de tornar crítico o reator mesmo durante o pico de envenenamento por Xenônio (DE LADONCHAMPS e VERDEAU, 1972) após um desligamento, sem paralelo em reatores “estacionários”, constitui uma das principais características do grau de flexibilidade operacional exigido da IPN. O aumento da disponibilidade decorrente da flexibilidade operacional constitui, por sinal, uma das principais razões para a adoção quase universal do reator PWR para propulsão naval, pois este tipo de reator apresenta características próprias que a favorecem significativamente.

A busca da disponibilidade máxima conduz o projetista do reator a conceber o controle da instalação de maneira tal que a continuidade da produção de energia (eventualmente reduzida) seja a máxima possível e que, em nenhum caso, uma primeira avaria menor da IPN

ou do navio cause sua interrupção. Como regra geral, a busca da melhor disponibilidade conduz ao que poderia ser qualificado como um “superdimensionamento” da IPN em comparação com uma instalação nuclear estacionária, pois as margens de projeto e de operação são muito maiores do que as requeridas exclusivamente para o funcionamento normal.

Em paralelo com os requisitos de disponibilidade, os requisitos de segurança se exprimem para as instalações propulsoras nucleares de um modo diferente dos outros tipos de reator. Pelo fato da não-singularidade e imbricação com o navio, os objetivos gerais de segurança são enunciados para o conjunto reator + navio, e não para a instalação nuclear isoladamente. A maximização da segurança do conjunto reator + navio conduz o projetista a conceber a IPN com uma série de disposições construtivas e também de regras de operação e de lógicas de controle que visam garantir a continuidade da produção de energia, em nível sem paralelo com as instalações terrestres.

Obviamente, esta abordagem é limitada sempre que o aumento da disponibilidade possa representar um risco inaceitável de acidentes com possibilidades de contaminação e irradiação de populações ou do meio ambiente. Este compromisso é caracterizado pelo poder de decisão concedido ao comandante do navio de inibir deliberadamente certas ações de proteção do reator caso julgue que a segurança do navio estaria ameaçada em caso de perda da propulsão. Isto só é aceitável devido ao fato que, mesmo navegando próximo de costa, as consequências de um acidente só incidiriam sobre a tripulação do navio, sobre a qual ele é totalmente responsável.

Ressalta-se que um navio militar só se encontra em efetiva segurança com respeito aos diversos riscos operativos e de navegação a que está submetido se ele puder dispor rapidamente da energia fornecida pela instalação nuclear. Assim, se o fornecimento de vapor nuclear não é assegurado, em particular por razões ligadas à segurança nuclear, a manobrabilidade do navio, e portanto sua própria segurança podem ser gravemente afetadas. Deve-se distinguir, nestes casos, o que constitui um Risco Presente (ou imediato) e um Risco Potencial: quando um navio é confrontado com um alagamento ou colisão iminente, o que constitui um Risco Presente, a disponibilidade total da energia nuclear será requerida, mesmo

que o fato de operar a IPN em condições acima dos limites de projeto aumente, temporariamente, a probabilidade de ocorrência de um acidente na IPN, o que constitui um Risco Potencial.

2.4.3 INVENTÁRIO DE PRODUTOS RADIOATIVOS

Os Riscos Potenciais de origem radiológica associados à propulsão nuclear naval são qualitativamente os mesmos decorrentes dos reatores nucleares, abordados anteriormente, dado que o inventário de produtos radioativos existentes no núcleo de um reator de propulsão naval não difere qualitativamente daquele correspondente aos reatores de potência eletronucleares. Quantitativamente, entretanto, ele é de 10 a 100 vezes menor, i.e. implica em Gravidade de Perigos potenciais de 1 a 2 ordens de grandeza inferiores, dependendo dos reatores específicos comparados (se comparamos um reator naval de 50 MWth com a Central Nuclear de Angra-II, teremos um fator da ordem de 70).

Este inventário inclui cerca de 180 diferentes radionuclídeos, dos quais 100 têm meia-vida inferior a hora, 34 têm meia-vida entre 1 hora e 1 dia. Cerca de 40 possuem, entretanto, meia-vida mais longa, de meses a anos, incluindo os transurânicos, de meia-vida extremamente longa, mas que representam um fração muito reduzida do inventário total (GUIMARÃES, 1997b). A atividade total e composição deste inventário depende do enriquecimento inicial do combustível (quanto maior o enriquecimento, menor formação de transurânicos, tais como o Plutônio) e do histórico de funcionamento do reator até o momento do seu desligamento (maior queima ou *burn-up*, implicando em maior atividade).

A Tabela 2.7 apresenta o inventário de produtos de fissão do U-235 para um reator de propulsão naval de 100 MWth, operado a plena potência durante 600 dias. Os inventários são dados para o momento de desligamento e para 3, 100 e 1000 dias de "resfriamento". Note-se que, após o desligamento, o decaimento radioativo faz com que a atividade seja reduzida a cerca de, respectivamente, 65%, 18% e 3%.

Este inventário estará contido no interior da primeira barreira de contenção, composta pelo encamisamento do combustível. Se fizermos a hipótese que o encamisamento falhe, as liberações potenciais para o circuito primário dependerão da natureza física de cada

radionuclídeo: aqueles que são gasosos ou voláteis serão transferidos praticamente a 100% para o circuito primário. Aqueles que são de natureza não volátil tenderão a ficar retidos no interior da matriz do combustível. A tabela 2.8 identifica a natureza física dos produtos de fissão.

TABELA 2.7: INVENTÁRIO DE PRODUTOS DE FISSÃO DO U-235 PARA UM REATOR NAVAL DE 100 MWth APÓS 600 DIAS DE OPERAÇÃO (GUIMARÃES, 1997b)

	desligamento (1000 TBq)	3 dias (1000 TBq)	100 dias (1000 TBq)	1000 dias (1000 TBq)
Xe, Kr	216,6	9,5	9,4	8
I, Br	654	174	0	0
Cs, Rb	118,44	118,41	108,2	50,8
Te, Se, Sb	196,84	28,35	5,03	0,26
Ba, Sr	393,94	364,04	53,27	12,9
Ru, Rh, Pd, Mo, Tc	394,2	284,6	48	2,4
Y, Zr, Nb, La, Ce, Pr, Nd, Pm, Sm, Eu	1906,05	1534,9	479,88	46,4
TOTAL	3880,07	2513,80	703,78	120,76

obs: 1 TBq = 10^{12} Bq

TABELA 2.8: NATUREZA FÍSICA DOS PRODUTOS DE FISSÃO DO U-235

PRODUTO DE FISSÃO	FAMÍLIA	GRUPO
Xe, Kr	1 - gases nobres	gases inertes
I, Br	2 - halogêneos	voláteis
Cs, Rb	3 - álcalis metálicos	voláteis
Te, Se, Sb	4 - calogêneos	voláteis
Ba, Sr	5 - terras alcalinas	não-voláteis
Ru, Rh, Pd, Mo, Tc	6 - metais nobres	não-voláteis
Y, Zr, Nb, La, Ce, Pr, Nd, Pm, Sm, Eu	7 - terras raras	não-voláteis

Devido ao fluxo neutrônico gerado no núcleo, determinados nuclídeos componentes dos materiais estruturais do Reator, assim como os produtos de corrosão do Circuito Primário e da superfície do encamisamento do combustível tornam-se radioativos por ativação. Os produtos de corrosão se depositam nas superfícies interiores das tubulações, válvulas, PZ, GV e BCP. O nível de atividade total destes componentes entretanto é modesto em comparação com o núcleo. A tabela 2.9 apresenta o inventário destes produtos para um reator naval típico, um ano após o desligamento. A meia-vida dos radionuclídeos envolvidos é relativamente longa.

TABELA 2.9: INVENTÁRIO RADIOATIVO DOS PRODUTOS DE ATIVAÇÃO DE UM REATOR NAVAL 1 ANO APÓS DESLIGAMENTO (GUIMARÃES, 1997b)

RADIO-NUCLÍDEO	MEIA-VIDA (anos)	COMPONENTES SÓLIDOS (TBq)	DEPÓSITOS (<i>crud</i>) (TBq)
Carbono-14	5.730	0,423	5,8e-7
Ferro-55	2,73	2,26e3	7,16e-2
Cobalto-60	5,27	4,71e2	4,02
Níquel-59	7,5E4	1,73	5,07e-5
Níquel-63	100,1	1,93e2	9,64e-3
TOTAL		2,93e3	4,10

2.4.4 DELINEAMENTO DE DOCTRINA DE SEGURANÇA

Estabelecida uma doutrina que maximiza a segurança da tripulação, do público e do ambiente, reconhecendo a capacidade de sobrevivência do navio como a preocupação primária de segurança, torna-se necessário estabelecer uma metodologia geral e desenvolver ou adaptar métodos e modelos requeridos para sua aplicação ao projeto, construção e operação dos navios nucleares.

Para atingir estes objetivos, é necessário recorrer à teoria de SDFSI/RAMS, que enfatiza o desenvolvimento de um programa de análise preditiva de segurança, que pode ser sintetizada pelo trinômio Identificação Análise Controle.

Este programa deve necessariamente estabelecer uma abordagem disciplinada para identificar metodicamente aqueles perigos que devem ser eliminados ou controlados, avaliar o projeto do sistema, prever ações corretivas ao longo de todas as fases do ciclo de vida do sistema envolvido, e prover o retorno da experiência operacional para assegurar que os objetivos de projeto foram atingidos (DOD, 1969). O desenvolvimento de um programa de segurança requer o conhecimento aprofundado, consubstanciado por modelos físicos e métodos matemáticos de análise de:

- i. sistema propriamente dito;
- ii. ambiente onde o sistema opera;
- iii. riscos potenciais ao ambiente induzidos pela operação do sistema;
- iv. riscos potenciais ao sistema induzidos pelo ambiente onde ele opera;
- v. consequências para o ambiente das agressões induzidas pelo sistema; e
- vi. consequências para o sistema das agressões induzidas pelo ambiente.

Estes conhecimentos não são, entretanto, por si só suficientes: é necessário ainda a capacidade de combiná-los analiticamente. Considerando-se esta base de conhecimentos e os requisitos para o navio nuclear, o primeiro passo será identificar todos os perigos associados ao sistema (navio) ou sub-sistemas (instalação nuclear, etc.). A inclusão dos cenários identificados no campo de análise deve ter a exaustividade como objetivo, sendo o critério do possível, e não somente o de provável, utilizado. Devem ser simultaneamente considerados três parâmetros para qualquer risco:

- a) Gravidade: consequências associadas a um perigo particular, em termos de liberação de radioatividade e operação do navio;
- b) Probabilidade: a verossimilhança de ocorrência de um evento inicializador e das várias consequências dele resultantes;
- c) Controle: a quantidade e tipo de recursos ou ações disponíveis para eliminar ou mitigar as consequências resultantes do perigo.

O uso fundamentado do *engineering judgement*, baseado no conhecimento e nas informações disponíveis, para aferir a cada perigo/evento uma classificação em termos de severidade, probabilidade e controle permitirá uma imagem clara do nível de segurança

atingido, o nível de risco aceitável, dos meios disponíveis para controlar os Perigos e suas consequências, e o custo associado aos vários níveis de controle.

Existem quatro métodos para tratar os Perigos identificados:

- a) eliminar o Perigo pelo projeto;
- b) evitar o Perigo, prevendo-se dispositivos de segurança cuja atuação não dependa de ação dos operadores;
- c) evitar o Perigo, empregando dispositivos de alarme que determinem ações específicas dos operadores;
- d) desenvolver e exigir rígido cumprimento de procedimentos operacionais que evitem os Perigos ou mitiguem suas consequências.

Evidentemente, a linha de ação mais desejável seria eliminar todos os perigos através do projeto de engenharia. Entretanto, esta tarefa é inviável, tornando-se obrigatório recorrer a um dos três outros métodos para evitar ou reduzir as consequências da ocorrência de um perigo.

Tendo projetado um sistema considerando a segurança, torna-se em seguida necessário analisá-lo para garantir que ele realmente atende os requisitos operacionais, reduzir a probabilidade de ocorrência de perigos e reduzir as consequências destes perigos, caso eles venham a se concretizar, a um nível aceitável. Esta análise deve ser feita de modo contínuo ao longo da vida do sistema e deve ser periodicamente atualizada com base em dados históricos de segurança gerados pela operação do sistema ou de sistemas similares.

Considere-se o caso de um submarino nuclear que se encontra navegando próximo a superfície (cota periscópica) e detecta uma ameaça operativa que o obriga a mergulhar rápido (grande ângulo de ponta para baixo) para sua cota máxima de operação. Durante o mergulho, ocorre um evento que conduz o reator a operar acima de um limite máximo definido por uma especificação técnica, o que pode vir a causar dano ao núcleo ou a algum sistema importante para a segurança nuclear se o reator continuar a operar:

- A doutrina de segurança para reatores em terra requereria que o reator fosse desligado imediatamente, possivelmente de modo automático, até que reparos fossem feitos.

- O desligamento do reator do submarino nesta situação hipotética poderia levar o navio, devido a sua própria inércia, a ultrapassar sua cota máxima de mergulho, podendo atingir a cota de colapso (falha mecânica da estrutura resistente e perda da estanqueidade) e em seguida naufragar, colocando assim a tripulação em grave perigo e também perdendo-se totalmente o controle sobre o reator, pois o navio será perdido.
- A doutrina de segurança proposta indica que o reator deve continuar a ser operado ao nível de potência necessário para uma manobra de recuperação e deveria ser desligado somente se:
 - o evento de falha conduzir à completa destruição do reator, a propulsão sendo perdida de toda forma; ou
 - a situação for tal que o navio seria perdido mesmo que a potência do reator fosse mantida.

Ressalte-se que a doutrina de segurança proposta não aprova ou recomenda a operação do reator além dos limites das especificações técnicas nem em qualquer outro modo perigoso, quando a segurança e sobrevivência do navio e de sua tripulação não se encontram seriamente ameaçadas.

Tendo identificado um Evento Indesejado (Especificação Técnica X foi excedida) e avaliado um determinado nível de risco para as diferentes possíveis conseqüências (naufrágio ou operação além das especificações técnicas por um período T de tempo com um nível conhecido e aceitável de dano ao reator) às quais estão associadas uma probabilidade de ocorrência dependente do projeto do sistema adotado, uma decisão deve ser tomada em termos de qual das quatro ações devem ser consideradas para mitigar o problema:

- a) a probabilidade de ocorrência do evento é alta o suficiente para requerer o reprojetado do sistema e eliminar sua possibilidade de ocorrência?
- b) as conseqüências são tão rápidas e/ou desastrosas de forma a requerer o desligamento automático (SCRAM na terminologia anglo-saxônica, RESA na alemã, AU na francesa) do reator e partida dos sistemas de segurança?
- c) o perigo deve ser alarmado, com a possibilidade da operação além das especificações técnicas ser continuada, conforme decisão do operador, em situações de emergência?

d) devem ser desenvolvidos procedimentos especiais que permitam a operação nesta condição de falha por um determinado período de tempo, mesmo quando não existe situação de emergência?

A resposta a estas perguntas forma a base da doutrina preconizada, que consiste em prover o máximo de proteção para o conjunto navio/reator como um sistema integrado.

Conforme citado anteriormente, existem quatro métodos para tratar os perigos identificados: eliminação, dispositivos automáticos de segurança, dispositivos de alarme e procedimentos especiais. Existem entretanto várias opções de projeto específicas, incluídas dentro destas quatro categorias que atenderiam os requisitos. Algumas destas opções serão discutidas.

A opção de projeto de eliminar ou controlar um perigo parece ser, tecnologicamente falando, o melhor método, apesar de não ser necessariamente o mais econômico. Este método, quando usado em conjunto com os outros três é extremamente útil. Em particular, o aumento das margens de segurança entre o projeto e os limites de operação permite uma maior flexibilidade para a continuidade da operação, tempo para efetuar de modo ordenado e racional diagnósticos precisos e implementação de procedimentos especiais, em lugar do que seria um desligamento automático mandatório ou uma drástica redução de potência num reator em terra. Isto pode ser muito útil no projeto do combustível e na definição dos parâmetros operacionais de pressão, temperatura e vazão dos sistemas.

No projeto de sistemas de segurança onde são implementados diversos níveis de redundância, a autoridade de segurança pode exigir redução de potência ou desligamento da instalação em caso de perda de um ou mais “trens” redundantes. Eventualmente, a operação pode ser permitida por um determinado intervalo de tempo, de modo a possibilitar a correção do problema. Se os reparos não são efetivados neste período, exige-se o desligamento a quente até que a instalação possa voltar a operar dentro das especificações técnicas.

No caso da propulsão naval, a duração deste intervalo de tempo no qual a instalação nuclear pode operar com um “trem” redundante fora de funcionamento deve ser muito maior do que aquele permitido a um reator em terra, devido à eventual indisponibilidade de

sobressalentes e à necessidade, em termos de segurança, de completar a missão no mar. Nestes casos, as lógicas de funcionamento dos sistemas de segurança do tipo 2 em 3 devem poder ser reajustadas para 1 em 2, colocando-se pessoal adicional para monitorar continuamente o parâmetro afetado ou para executar controle manual local sobre o sistema. A segurança neste caso é melhor garantida permanecendo a instalação em operação.

Um evento plausível deste tipo de controle é a perda de um mecanismo de acionamento de barras de controle. Esta perda da função de acionamento pode resultar de uma falha local, afetando um elemento individual ou de uma falha mais generalizada, afetando um banco ou grupo de elementos. Este evento indesejado possivelmente não afetará a função de SCRAM, não ocasionando nenhum efeito imediato, assumindo-se a operação do reator em regime permanente. Potencialmente, a longo termo, poderá ocorrer alguma distorção na forma do fluxo neutrônico ou instabilidades de potência locais. Se a perda ocorrer num grupo de elementos de segurança, ela pode afetar a margem de excesso de reatividade, mas sem nenhum efeito catastrófico resultante do evento.

- Um reator estacionário seria desligado compulsoriamente num caso como este.
- Num navio, tal ação seria indesejável, mesmo em situações normais, pois, no mínimo, conduziria à perda da manobrabilidade do navio. Como não existiriam efeitos imediatos sobre a segurança, seria recomendável que o navio continuasse sua singradura até um porto onde fosse possível efetuar-se os reparos necessários ou, no mínimo, até um fundeadouro onde o reator pudesse ser desligado sem implicar em perigos para o navio enquanto os reparos pudessem ser efetuados.

A definição dos sinais de segurança que produzem o desligamento automático do reator, no caso da propulsão naval, conduz a uma análise de vantagens, desvantagens e condições nas quais o contorno (*by-pass*) ou invalidação de alguns ou todos os sinais de SCRAM podem ser realizados de forma a garantir a continuidade da operação em situações de emergência.

A análise de segurança deve então limitar a um mínimo indispensável os eventos que possam gerar um sinal de SCRAM. Para aqueles eventos que requerem o desligamento de urgência, o sistema de proteção deve ter interfaces com alarmes e com um sistema automático

de limitação que reduza a potência quando os parâmetros de operação do reator se aproximam das margens mínimas de operação. A redução automática de potência poderá em seguida ser invalidada por ação do operador, de modo a manter o reator dentro dos limites de segurança. No caso do reator não poder ser mantido dentro dos limites de segurança, a função de SCRAM permanece ainda disponível para proteger a tripulação, o público e o meio ambiente.

Neste contexto, pode ser desejável projetar o ponto de operação e o limite de segurança onde o desligamento automático ocorrerá com uma margem mais ampla e ajustar o ponto de SCRAM próximo ao limite máximo do sistema, de modo que a perda de potência ocorra somente como último recurso para evitar danos severos ao reator. Exatamente onde este ponto ocorre somente pode ser verificado para cada projeto específico, e deve ser amplamente justificado e documentado pela análise de segurança.

Através da correta aplicação da doutrina discutida, fica evidenciado que a função de SCRAM deve representar o limite máximo de operação, e não deverá nunca ser invalidado ou contornado (*by-pass*).

Os procedimentos operacionais que permitem a continuidade do funcionamento do reator em caso de falha mecânica, de monitoração, de controle ou de segurança de sistemas são de extrema importância. É necessário que, a bordo de um navio, a decisão final de operar o reator além de suas especificações técnicas seja exclusiva do comandante do navio. Deste modo, o comandante deve ser capaz de tomar decisões fundamentadas em seus próprios conhecimentos de engenharia nuclear e na avaliação da assessoria técnica fornecida pelo chefe de máquinas, e nos seus conhecimentos navais e experiência de mar. Estas decisões baseiam-se no pleno entendimento das consequências de cada linha de ação possível, ou seja, de continuar a geração de potência nuclear em face dos danos que sofrerá o reator, ou desligar o reator em face dos riscos de perda do navio e de sua tripulação (e, em última instância, do próprio reator).

2.4.5 ANÁLISE DE SEGURANÇA DO NAVIO

A diversidade e a complexidade das interfaces e efeitos de realimentação que podem ser identificados entre a instalação propulsora nuclear e o navio propriamente dito, tornam necessário que, para garantir sua segurança, o navio nuclear seja abordado como uma entidade única. Isto quer dizer que o conceito de Instalação Nuclear não está limitado aos sistemas de geração e utilização de energia a bordo, mas estende-se a todo o Sistema-Navio. Este sistema único incorpora os aspectos científicos e tecnológicos, bem como as metodologias e técnicas, ou seja, aquilo que poderia ser resumido como a “cultura”, tanto da engenharia naval, em especial seu ramo de aplicação militar, como da engenharia nuclear, em especial seu ramo de aplicação na geração de energia elétrica.

O reconhecimento do navio nuclear como um sistema único, resultado da combinação de “culturas” de dois grandes ramos da engenharia, implica na necessidade das regulamentações para sua segurança incorporarem e sintetizarem todos os aspectos relevantes tanto para os navios militares como para as usinas núcleo-elétricas estacionárias.

Conforme apresentado na subseção 2.3.1, a influência da plataforma-navio pode ser expressa em termos de necessidades e carregamentos. O navio deve assegurar, em diversos níveis de continuidade, o fornecimento de serviços à instalação nuclear, que devem ser garantidos não só durante os períodos de operação como também durante os períodos de indisponibilidade do navio para a manutenção e reparo:

- a) alimentação de energia elétrica, hidráulica, pneumática;
- b) água de resfriamento para condensadores principais e auxiliares e trocadores de calor de resfriamento de diversos sistemas;
- c) ventilação e condicionamento de ar;
- d) contenção estanque para o compartimento do reator;
- e) armazenagem, tratamento e descarga de rejeitos;
- f) proteção contra agressões externas provenientes do meio ambiente;
- g) operação, inspeção, manutenção e reparo, incluindo armazenagem de sobressalentes, ferramentas comuns e especiais, instrumentos para medições, análises e testes.

A Segurança de Funcionamento dos sistemas, componentes e materiais do navio que prestam serviços que interferem diretamente na segurança da instalação nuclear é avaliada por

métodos de análise análogos àqueles empregados para as instalações nucleares. Essa análise estende-se às conseqüências de acidentes provocados por eventos inicializadores externos à instalação nuclear que podem atingir determinadas áreas físicas do navio onde encontram-se instalados esses sistemas, tais como incêndios, explosões, alagamentos.

A Análise de Segurança do Navio Nuclear, discutida em maior profundidade pelo Anexo L, deve tratar dos problemas apresentados pela integração das instalações nucleares a bordo, devendo ser complementar e coerente com a análise de segurança da instalação nuclear:

- o navio apresenta-se como um “prestador de serviços” no que se refere às necessidades da instalação; a segurança de funcionamento dos dispositivos que garantem esses fornecimentos deve ser analisada em todas as configurações de operação;
- as instalações e o navio induzem riscos de avarias recíprocas que devem ser analisados e minimizados.

A instalação nuclear pode implicar em dois tipos de riscos para o navio:

- a) riscos radiológicos (irradiação, contaminação), mesmo em situação de desligamento do reator;
- b) riscos não nucleares, devidos às condições de pressão e de temperatura e à presença de hidrogênio em certos circuitos.

Para limitar esses riscos radiológicos em situação normal, aplicam-se os seguintes princípios:

- a) organização do navio em zonas de ventilação;
- b) limitação e controle administrativo do tempo de permanência nas zonas de risco;
- c) instalação de meios de controle e de vigilância radiológica do pessoal;
- d) existência de um compartimento de contenção com acesso por antecâmara;
- e) limitação do número de penetrações (cabeamento, tubulações, dutos) na contenção.

O Anexo M discute a organização da radioproteção a bordo dos navios dotados de propulsão nuclear

Em Condições de Processo da Instalação Nuclear acidentais CPIN4 (vide Anexo L), deve ser possível:

- a) garantir a resistência do compartimento de contenção à pressão máxima pós-acidental;
- b) extinguir a reação de fissão nuclear em cadeia, garantindo o confinamento e o resfriamento do núcleo,
- c) isolar (fluidos e ventilação) as zonas do navio implicadas,
- d) medir os fluxos de equivalentes de dose ambientes e monitorar a contaminação do ar e dos fluidos em todos os lugares em que o pessoal permanece ou entra.

A política de manutenção tem significativa influência sobre o projeto do navio (SEVESTRE, 1991). De um modo geral, distingue-se três níveis de manutenção da IPN:

- a) manutenção de 3^o escalão, que é a situação normal de parada a quente, onde a manutenção é limitada a rondas e testes;
- b) manutenção de 2^o escalão, com trabalhos na instalação nuclear, que podem requerer sua parada a frio, porém para intervenções limitadas;
- c) manutenção de 1^o escalão, necessitando a abertura do reator para inspeção ou intervenção sobre o núcleo, o vaso de pressão e seus internos;

Estes níveis de manutenção são associados a três tipos de instalações de apoio em terra:

- a) porto de escala, onde o navio permanece autônomo;
- b) estação naval, limitada ao fornecimento de fluidos ou energia e, eventualmente, coleta de efluentes radioativos;
- c) base naval, dotada de instalações especializadas para a manutenção da instalação nuclear (sala limpa, oficina mecânica quente, células quentes, piscina de armazenagem de elementos combustíveis).

A segurança das instalações de apoio em terra que participam da segurança nuclear do reator em manutenção é objeto de uma análise complementar ao estudo de segurança do navio.

A movimentação de combustíveis nucleares constitui um aspecto muito importante desta análise, pois o projeto do navio e das instalações em terra deverá garantir que, durante as operações de recarga do núcleo (SCHAFSTALL, 1977):

- a) os riscos de queda de cargas pesadas dentro do vaso do reator sejam limitados;
- b) o resfriamento do combustível irradiado seja mantido;
- c) não haja descontinuidade no confinamento.

As solicitações do navio com respeito ao ambiente são destinadas a garantir a segurança da instalação nuclear dentro das diversas Condições de Processo da Instalação Nuclear, de CPIN1 a CPIN4 (vide Anexo L). As agressões geradas pelo ambiente sobre o navio, são transmitidas à instalação nuclear com um fator de amplificação ou atenuação, segundo o caso.

Excluídas as condições acidentais, o navio nuclear pode realizar liberações de efluentes radioativos, gasosos ou líquidos, diretamente no meio ambiente ou por intermédio de instalações de tratamento em terra, sob a condição de não ultrapassar os limites autorizados, estabelecidos numa base anual.

3 PRINCÍPIOS BÁSICOS

Neste capítulo serão desenvolvidos os Princípios Básicos de Segurança para Submarinos Nucleares de Ataque, primeiro nível (vide Figura 1.1) da Doutrina de Segurança proposta. Como “Princípios Básicos” entende-se diretrizes qualitativas que orientam como os objetivos da segurança nuclear podem ser atingidos. Estes princípios são estruturados na forma preconizada pela (IAEA-INSAG, 1988) para Instalações Nucleares de Potência INP, mantendo-se sua filosofia geral, porém reavaliando-os e adaptando-os, sempre que necessário, às particularidades de uma IPN (Tabela 3.1):

- I. Objetivos
- II. Princípios Fundamentais de Gerenciamento
- III. Princípios de Defesa em Profundidade
- IV. Princípios Técnicos Gerais
- V. Princípios Específicos

TABELA 3.1: PRINCÍPIOS BÁSICOS DE SEGURANÇA

Objetivos	GERAL		Proteção Radiológica	Confiabilidade e Seguridade	Disponibilidade		
Princípios Fundamentais de Gerenciamento	CULTURA DE SEGURANÇA		Responsabilidade da Organização Operadora		Controle Regulamentar e Supervisão Independente		
Princípios de Defesa em Profundidade	DEFESA EM PROFUNDIDADE		Prevenção de Acidentes		Mitigação de Consequências		
Princípios Técnicos Gerais	Validação	Garantia da Qualidade	Fatores Humanos	Análise de Segurança	Proteção Radiológica	Experiência Operacional e Pesquisa de Segurança	
Princípios Técnicos Específicos	Mobilidade	Projeto	Fabricação e Construção	Comsio-namento	Operação	Gerenciame-nto de Acidentes	Planejamento de Emergências

Para cada área identificada pela Figura 3.1, os princípios são apresentados sob a forma de enunciados curtos, seguidos de uma discussão sobre sua necessidade e relevância.

3.1 OBJETIVOS DE SEGURANÇA

São definidos quatro objetivos de segurança para as IPN de SNA. O primeiro é um objetivo de natureza genérica. Os outros três são objetivos complementares que interpretam o objetivo geral, tratando, respectivamente, da Proteção Radiológica, da Confiabilidade e Seguridade (Segurança Nuclear), e da Disponibilidade (Segurança Naval).

Os objetivos de segurança não são independentes: sua superposição visa garantir o caráter global do objetivo geral, enfatizando os aspectos complementares da segurança.

3.1.1 OBJETIVO GERAL

Objetivo: Estabelecimento e manutenção de uma defesa efetiva dos indivíduos (tripulantes e pessoal de apoio em terra), da sociedade (público em geral) e do meio ambiente contra perigos de origem radiológica decorrentes da operação de SNA.

No estabelecimento do objetivo de segurança geral, “perigos de origem radiológica” significam efeitos adversos sobre a saúde, tanto dos tripulantes do SNA como do pessoal de apoio em terra e do público, assim como efeitos adversos sobre o meio ambiente, tais como a contaminação por produtos radioativos do mar, litoral, atmosfera ou produtos alimentícios. Não inclui outros tipos mais convencionais de perigos que possam decorrer da operação do SNA.

A defesa será efetiva se ela evitar que a operação do SNA implique num aumento significativo do nível de riscos aos quais os indivíduos, a sociedade e o ambiente já estão normalmente expostos como consequência de outras atividades de caráter industrial socialmente aceitas.

Note-se entretanto que a implementação desta defesa não só reduzirá os riscos de origem radiológica mas também os riscos derivados da existência de fontes de energia concentradas, tais como fluidos a altas pressões e temperatura, na IPN.

Deve ser reconhecido que, embora os interesses de sociedade requeiram proteção contra os efeitos prejudiciais da radiação, eles não incluem somente a proteção radiológica das pessoas e do meio ambiente. A proteção dos investimentos feitos para obtenção do SNA, assim como do patrimônio material e cultural geral da sociedade é de relevante importância para a sociedade e demanda atenção para todos os aspectos de

segurança abordados pelo presente trabalho. Entretanto, o enfoque principal será o da segurança radiológica dos indivíduos, sendo os princípios básicos expressos exclusivamente nestes termos, o que porém não significa que os outros fatores não devam ser considerados.

3.1.2 OBJETIVO DE PROTEÇÃO RADIOLÓGICA

Objetivo: Em operação normal, garantir que as doses de radiação recebidas pela tripulação, pessoal de apoio em terra e público externo, devidas à exposição direta e à liberação controlada para o ambiente de material radioativo proveniente da IPN, sejam mantidas tão reduzidas quanto razoavelmente realizável e abaixo de limites prescritos. Em operação anormal e acidental, garantir meios para mitigar a extensão das exposições à radiação devido a eventos indesejados.

A proteção radiológica nos SNA é executada numa base rotineira em condições normais, sendo previstas ações específicas para condições anormais e acidentais. Para condições operacionais planejadas da IPN e para ocorrências anormais previstas, o atendimento a padrões baseados nas recomendações da ICRP assegura proteção radiológica apropriada. Isto é, o princípio de limitação de doses da ICRP provê proteção apropriada para situações planejadas, para as quais é prevista a ocorrência pelo menos uma vez ao longo do ciclo de vida do SNA.

Os padrões de proteção radiológica acima mencionados foram desenvolvidos para prevenir efeitos prejudiciais das radiações ionizantes, mantendo as exposições suficientemente reduzidas de modo a excluir a possibilidade de ocorrência de efeitos determinísticos e a limitar a probabilidade de ocorrência de efeitos estocásticos a níveis julgados socialmente toleráveis. Eles se aplicam a circunstâncias controladas. No evento de um acidente que poderia causar uma fonte de exposições que não estaria completamente sob controle, são planejadas ações de proteção internas ao SNA e, eventualmente, contramedidas externas, para mitigar os efeitos sobre os tripulantes, o público e o meio ambiente.

3.1.3 OBJETIVO DE CONFIABILIDADE E SEGURIDADE (SEGURANÇA NUCLEAR)

Objetivo: Garantir um alto grau de confiabilidade à IPN, prevenindo a ocorrência de acidentes. Considerando a ocorrência de um espectro de acidentes determinado a priori, garantir que as conseqüências radiológicas, se existirem, sejam mínimas, provendo a IPN de dispositivos especiais de segurança que assegurem a continuidade do atendimento das

funções básicas de segurança nuclear. Garantir ainda que a probabilidade de acidentes severos, fora do espectro pré-determinado e com consequências radiológicas significativas, seja extremamente pequena, provendo o SNA de meios e procedimentos para execução de planos de emergência interno e externo que mitiguem estas consequências.

A prevenção de acidentes é a primeira prioridade de segurança tanto para projetistas e construtores como para operadores. Este objetivo é alcançado pelo uso de estruturas, componentes, sistemas e procedimentos de operação altamente confiáveis em uma IPN operada por pessoal imbuído de uma forte cultura de segurança.

Entretanto, em nenhum sistema desenvolvido pelo homem pode-se garantir que a prevenção de acidentes terá pleno êxito. Os projetistas de IPN assumem então que estruturas, componentes e sistemas possam falhar e que erros humanos são possíveis, podendo conduzir a ocorrências anormais, que podem ser desde pequenas perturbações no seu funcionamento até seqüências acidentais altamente improváveis. A necessária proteção adicional é alcançada pela incorporação de dispositivos especiais de segurança na instalação.

Estes dispositivos são implementados para deter o progresso de um acidente dentro do espectro de ocorrências considerado no projeto e, quando necessário, mitigar suas consequências. Os parâmetros de projeto de cada dispositivo especial de segurança são definidos por uma análise determinística de sua efetividade contra os acidentes aos quais pretende-se controlar. O acidente que requer os parâmetros de projeto mais extremos para uma determinada função de segurança é denominado Acidente Básico de Projeto ABP para esta função.

Leva-se também em consideração acidentes de muito baixa probabilidade, com consequências mais severas do que aqueles considerados explicitamente no projeto, denominados Acidentes Complementares de Projeto ACP. Alguns destes acidentes severos poderiam causar tal deterioração nas condições da IPN que o resfriamento adequado do núcleo do reator não poderia ser mantido, ou que danos ao combustível aconteceriam por outras razões. Estes acidentes teriam um potencial para consequências de ordem radiológica significativas se os materiais radioativos liberados pelo combustível não forem adequadamente confinados.

Considerando que estes acidentes pudessem todavia acontecer, são implementados procedimentos para gerenciar sua evolução e mitigar suas consequências. Estes procedimentos complementares são definidos com base na experiência operacional, na análise de segurança e nos resultados de experimentos específicos. O projeto, áreas de operação, procedimentos operacionais e treinamento de operadores consideram as ações requeridas para controlar a progressão e as consequências destes acidentes. A limitação de consequências requer ações que assegurem a continuidade do resfriamento do núcleo, a integridade do confinamento dos materiais radioativos, e um plano de emergência externo adequado. Os acidentes de consequências severas são extremamente improváveis porque são efetivamente evitados pelo projeto e pela operação ou são mitigados pela defesa em profundidade.

O objetivo de confiabilidade e seguridade é aplicado à prevenção de acidentes, mitigação de consequências e gerenciamento de situações de emergência de tal modo que o Risco Objetivo Residual total seja muito baixo e que nenhum cenário acidental particular, seja de baixa ou de alta probabilidade, contribua para o risco total de maneira excessiva quando comparado aos demais cenários.

3.1.4 OBJETIVO DE DISPONIBILIDADE (SEGURANÇA NAVAL)

Objetivo: Garantir um alto grau de disponibilidade à IPN, assegurando que a probabilidade de ocorrência de um acidente naval envolvendo o SNA provocado pelo desligamento compulsório do reator seja muito baixa e, nos casos em que ocorra este desligamento, prover dispositivos especiais de segurança que garantam a continuidade da produção de energia para o atendimento das funções básicas de segurança naval.

A segurança global do SNA é um objetivo primário. A segurança da IPN é uma parte integrante desta segurança global. Poderia ser necessário, porém, para a segurança global do submarino, requerer a continuidade da operação da IPN em situações onde a potência seria reduzida, ou mesmo o reator desligado, caso a segurança nuclear fosse a única consideração. A operação em tais condições só deverá, entretanto, ser efetivada após a devida consideração dos Riscos Potenciais radiológicos para a tripulação, o público em geral e o meio ambiente.

Este objetivo deriva da constatação que um submarino operando em modo degradado, com o reator tendo sofrido alguns danos, pode ser intrinsecamente mais

seguro do que um submarino com reator íntegro, porém desligado, i.e. sem governo nem propulsão, podendo tal situação pode rapidamente degenerar-se em um acidente naval e mesmo nuclear severo, resultante de possível colisão, encalhe ou afundamento.

Entretanto, o Objetivo de Segurança Naval não implica, sob nenhuma hipótese, em negligência no cumprimento do Objetivo de Segurança Nuclear, pois existem situações onde os riscos à integridade do reator seriam tão severos que o seu desligamento seria incontornável, pois um submarino em situações extremas, encalhado ou mesmo afundado, com um reator desligado em estado seguro, é uma situação mais favorável em termos de exposições e liberação de produtos radioativos do que um submarino nas mesmas condições com as funções básicas de segurança nuclear comprometidas. Se o funcionamento do reator além dos limites normais previstos em suas especificações técnicas não garantir o salvamento do submarino, e portanto também do próprio reator, então o reator deve ser compulsoriamente desligado.

A Figura 3.1 apresenta uma árvore de conseqüências preliminar que considera a IPN num estado inicial de plena potência (ou seja, com o SNA nas suas áreas de mobilidade) com o objetivo de avaliar a ordem de grandeza da probabilidade de ocorrência de acidentes com significativas liberações de produtos de fissão para o ambiente. A análise desta árvore mostra:

- a grande importância relativa dos eventos inicializadores de origem naval, externa à IPN (erros de navegação, eventos externos, “fortunas do mar” em conseqüência da perda da propulsão);
- a pequena importância relativa dos eventos inicializadores de origem nuclear, interna à IPN (perda de integridade do envelope estanque do circuito primário, seguida de perda de refrigerante);
- o efeito negativo sobre a segurança do SNA que pode ter o desligamento automático do reator exclusivamente por razões de segurança da IPN (desligamento automático seguido de “fortunas do mar”);
- o efeito negativo sobre a segurança da IPN que pode se seguir a um transiente anormal sem desligamento automático do reator, exclusivamente por razões de segurança do SNA.

ROTAS PRINCIPAIS DE LIBERAÇÃO

FIGURA 3.1: ROTAS PRINCIPAIS DE LIBERAÇÃO DE MATERIAIS
RADIOATIVOS EM CASO DE ACIDENTE GRAVE COM UM SNA

3.2 PRINCÍPIOS FUNDAMENTAIS

Determinados conceitos são gerais em aplicação, referindo-se à maneira de implementação dos princípios de segurança específicos que serão posteriormente enunciados. Estes conceitos são chamados aqui princípios fundamentais de segurança e

e são de três tipos, relacionando-se ao gerenciamento do ciclo de vida do SNA, à defesa em profundidade e a aspectos técnicos particulares, de emprego generalizado.

3.2.1 RESPONSABILIDADES PELO GERENCIAMENTO DO CICLO DE VIDA

São identificados três princípios fundamentais de gerenciamento. Eles são ligados ao estabelecimento de uma cultura de segurança, à responsabilidade da organização operadora, e à regulamentação legal do controle e verificação de segurança das atividades associadas.

3.2.1.1 Cultura de Segurança

Princípio: Uma cultura de segurança estabelecida governa as ações e interações de todos os indivíduos e organizações engajadas nas atividades relacionadas com a propulsão nuclear.

A expressão “cultura de segurança” refere-se a um tema de caráter geral: a dedicação pessoal e responsabilidade de todos os indivíduos engajados em todas atividades importantes para a segurança das IPN . O ponto de partida para que seja dada a atenção necessária aos assuntos de segurança está no gerenciamento de mais alto nível de todas as organizações envolvidas. Devem ser estabelecidas e implementadas estratégias gerenciais que assegurem a execução das atividades dentro das melhores práticas, reconhecendo que sua importância está não só nas práticas propriamente ditas mas também no ambiente de conscientização da segurança que elas criam, incluindo:

- Cadeias de responsabilidade e de comunicação explícitas
- Procedimentos claros, sem margens para interpretações ambíguas
- Exigência de uma rígida aderência a estes procedimentos;
- Revisões internas de atividades relacionadas à segurança; e, acima de tudo,
- Treinamento e educação do pessoal envolvido que enfatize as razões que estão por trás das práticas de segurança estabelecidas, juntamente com as conseqüências de deficiências do desempenho individual para a segurança.

Estes aspectos são especialmente importantes para organizações responsáveis pela operação e para o pessoal diretamente envolvido na operação da IPN . Para estes últimos, a todos os níveis, o treinamento deve enfatizar o significado de suas tarefas individuais do ponto de vista de compreensão básica do funcionamento, do conhecimento da instalação e seus componentes, e das ações de comando e controle

sobre ela, com ênfase especial nas razões subjacentes aos limites de segurança e às conseqüências de violações destes limites.

Para garantir que as informações relevantes à segurança sejam transmitidas livremente, um ambiente de trabalho franco e aberto deve ser estabelecido; a comunicação de ocorrência de erros de procedimento deve ser particularmente encorajada pelo gerenciamento. Por estes meios deverá ser alcançada uma mentalidade de segurança que permita uma atitude inerentemente interrogativa, a prevenção do laxismo, um compromisso individual com a qualidade, e o desenvolvimento tanto da responsabilidade individual como da auto-regulação organizacional com respeito aos aspectos de segurança.

3.2.1.2 Responsabilidade da Organização Operadora

Princípio: A responsabilidade final pela segurança da IPN repousa sobre a organização que a opera. Esta responsabilidade global não é diluída de nenhuma maneira pelas responsabilidades parciais por atividades específicas de projeto, fabricação de componentes, montagem, comissionamento e licenciamento.

Uma vez que a organização operadora aceita a IPN, ela assume integralmente a responsabilidade pelo seu funcionamento. A organização operadora deverá então estabelecer uma estratégia gerencial para garantir o cumprimento dos requisitos de segurança, definir procedimentos para controle seguro da instalação sob todas as condições normais e anormais, inclusive as de manutenção, e manter um grupo de operação plenamente capacitado. A organização operadora deverá assegurar que as responsabilidades estejam bem definidas e documentadas e que os recursos necessários para execução das tarefas do grupo de operação estejam disponíveis.

A organização operadora também tem responsabilidades em certas áreas onde seu controle é menos direto. Usando seu próprio pessoal e recursos, ou por ação de organizações externas qualificadas, a organização operadora executa revisões e auditorias rigorosas e, caso necessário, aprova processos para garantir que os fatores que determinam a segurança da IPN foram devidamente considerados.

Este princípio da responsabilidade da organização operadora pela segurança é de importância fundamental. As responsabilidades de outras organizações envolvidas são também importantes para a segurança, revestindo-se entretanto de um aspecto

financeiro e legal. A definição das responsabilidades formais destas outras organizações é um tema jurídico que não será abordado, mas evidentemente é requerido dos projetistas, fabricantes e construtores, como mínimo, garantir um projeto adequado e equipamentos que atendam às especificações em termos tanto de detalhes de engenharia como de desempenho funcional, respeitando padrões de qualidade proporcionais à importância para a segurança dos componentes ou sistemas.

3.2.1.3 Controle Regulamentar e Supervisão Independente

Princípio: O governo nacional estabelece a estrutura legal para o desenvolvimento da propulsão nuclear e para atuação da Autoridade de Segurança Nuclear independente que é responsável pela autorização e controle das IPN e pelo cumprimento da regulamentação pertinente. A separação de responsabilidades entre a ASN e as outras organizações envolvidas é clara, de modo a garantir sua independência com respeito a pressões externas impróprias.

Uma ASN legalmente garante controle ao nível governamental, licenciando, regulamentando e acompanhando a operação de IPN, no que tange à sua segurança. As atividades da ASN cobrem as seguintes áreas funcionais:

- especificação e desenvolvimento de normas e regulamentações para a segurança;
- emissão de licença para a organização operadora, com base na análise de segurança da IPN ;
- inspeção, monitoramento e revisão do desempenho de segurança da IPN e organização operadora;
- exigência de ações corretivas à organização operadora quando necessário, retirando a licença de operação, se não forem alcançados níveis de segurança aceitáveis;
- promoção da pesquisa científica e tecnológica relevante para a segurança; e
- disseminação de informações técnicas relevantes para a segurança.

A ASN age independentemente de projetistas, fabricantes, construtores e operadores no sentido de assegurar que a segurança seja a única missão do seu pessoal. Os recursos da ASN deverão ser suficientes para realizar suas funções sem afetar adversamente os cronogramas de obtenção ou de operação da IPN, exceto quando indispensável para a garantia de segurança. A ASN deve possuir competência técnica em todo o espectro da tecnologia nuclear.

Para exercer suas funções efetivamente, a ASN deve ter autoridade legal necessária que lhe proporcione acesso livre à IPN e às informações técnicas pertinentes existentes na organização operadora.

3.2.2 ESTRATÉGIA DE DEFESA EM PROFUNDIDADE

A defesa em profundidade destaca-se dentre os princípios fundamentais por permear todos os aspectos de segurança da tecnologia de propulsão nuclear. Todas as atividades de segurança, sejam organizacionais, comportamentais ou técnicas, estão sujeitas a barreiras sobrepostas, de forma que se houver uma falha, esta será compensada ou corrigida sem que sejam causados danos ao nível individual (tripulantes e pessoal de apoio em terra) ou coletivo (público em geral). Esta idéia de níveis múltiplos de proteção é a característica central da defesa em profundidade e é repetidamente usado nos princípios de segurança específicos que seguem.

3.2.2.1 Defesa em Profundidade

Princípio: Para compensar potenciais falhas humanas e materiais, o conceito de defesa em profundidade é implementado, centrado em vários níveis de proteção que incluem barreiras sucessivas que previnem a liberação de material radioativo para o ambiente. O conceito inclui a proteção das barreiras evitando danos à IPN e às próprias barreiras. Inclui ainda ações de proteção complementares para proteger o público e o ambiente de danos no caso das barreiras não serem completamente efetivas.

A defesa em profundidade proporciona uma estratégia global para ações e dispositivos de segurança das IPN. Quando corretamente aplicado, assegura que nenhuma falha conduziria a dano ao público, e que combinações de falhas que só são remotamente possíveis conduziriam a pequeno dano. A defesa em profundidade auxilia na garantia de que as três funções básicas de segurança são preservadas, e que os materiais radioativos não alcancem nem os indivíduos nem o ambiente.

O princípio de defesa em profundidade é implementado principalmente por meio de uma série de barreiras que nunca devem ser, *a priori*, contornadas. Danos atingindo os indivíduos ou o ambiente somente viriam a ocorrer caso estas barreiras fossem previamente violadas. Estas barreiras são físicas e proporcionam o confinamento do material radioativo em localizações sucessivas determinadas. As barreiras podem ter função operacional ou somente de segurança. O funcionamento da IPN só é permitido

se este sistema de barreiras múltiplas estiver íntacto e capaz de funcionar conforme suas especificações.

A confiabilidade das barreiras físicas é aumentada aplicando o conceito de defesa em profundidade a cada uma delas, protegendo-as por uma série de ações e dispositivos de segurança. Cada barreira física é projetada de modo conservador, sendo sua qualidade verificada para assegurar que existam margens suficientes contra eventuais falhas. Seu estado é monitorado, e todo processo da instalação capaz de afetar seu estado é controlado em operação.

Diversos aspectos humanos da defesa em profundidade atuam no sentido de proteger a integridade das barreiras, tais como garantia de qualidade, controles administrativos, revisões de segurança, regulamentação independente, limites operacionais, qualificação e treinamento de pessoal, e cultura de segurança.

Disposições de projeto que incluem tanto os sistemas envolvidos na operação normal da instalação como os dispositivos especiais de segurança auxiliam a prevenir carregamentos que ameacem a integridade das barreiras físicas, a prevenir a falha de uma barreira caso ela seja ameaçada, e a prevenir danos a mais de uma barreira em série. O projeto dos dispositivos especiais de segurança que protegem as barreiras físicas devem ser funcionalmente independentes sob as condições de acidente.

Todos os dispositivos de segurança componentes da defesa em profundidade deverão estar disponíveis quando a IPN estiver em operação normal em potência. Dispositivos apropriados específicos deverão estar disponíveis em outros modos de operação. A existência de vários componentes de defesa em profundidade nunca deverá servir de justificativa para operação na ausência de um deles.

O projeto de sistemas de acordo com a defesa em profundidade inclui controles de processo que usam realimentação para proporcionar uma tolerância a falhas que poderiam de outra forma levar a IPN a condições anormais ou acidentais de operação. Estes controles protegem as barreiras físicas mantendo a instalação em uma região de parâmetros operacionais autorizada onde as barreiras não serão ameaçadas. O cuidado no projeto de sistemas previne efeitos de transientes bruscos que poderiam fazer com que pequenos desvios operacionais degenerassem em condições anormais ou acidentais.

O projeto adequado das barreiras e as medidas para sua proteção associadas à realimentação para manter a operação em uma região segura leva a IPN a um desempenho otimizado. O mais importante indicador do sucesso da defesa em profundidade é a operação com pouca ou nenhuma necessidade de funcionamento dos sistemas de segurança.

Apesar do sistema de barreiras múltiplas proteger os indivíduos e o ambiente de um amplo espectro de condições anormais de operação, os Planos de Emergência interno e externo são ainda desenvolvidos como um componente adicional da defesa em profundidade, contra a possibilidade de material radioativo, ainda assim, poder ser liberado de forma descontrolada, atenuando danos aos indivíduos e ambiente em tais condições acidentais severas.

São definidos dois corolários do Princípio de Defesa em Profundidade: prevenção de acidentes e mitigação de consequências. Estes corolários são apresentados a seguir.

3.2.2.2 Prevenção da Ocorrência de Acidentes

Princípio: A prevenção de acidentes, particularmente aqueles que possam causar dano severo ao núcleo do reator, levando à perda da IPN, é a principal ênfase da segurança dos SNA.

O projeto, construção, operação e manutenção de IPN têm como seu objetivo primário a geração de energia para o SNA de forma contínua e confiável. Conforme o princípio geral de gerenciamento com base em uma cultura de segurança, suas implicações devem ser consideradas nas decisões tomadas em todas as situações de operação do SNA.

O primeiro meio de prevenção de acidentes é garantir uma qualidade do projeto, fabricação, construção e operação da IPN tal que desvios das condições operacionais normais sejam pouco frequentes.

Os sistemas de segurança são usados como um apoio à realimentação do controle de processos que visam impedir que tais desvios evoluam para acidentes. Os sistemas de segurança fazem uso de redundância e diversidade de projeto e a segregação física de componentes em paralelo, quando apropriado, para reduzir a probabilidade da perda de uma função básica de segurança. Os sistemas e componentes de segurança são inspecionados e testados regularmente para revelar qualquer degradação que poderia

conduzir a condições operacionais anormais ou a um desempenho de segurança inadequado.

As condições anormais que poderiam afetar a segurança nuclear devem ser prontamente identificadas pela monitoração e alarmes das variáveis críticas dos sistemas e, em muitos casos, iniciando ações corretivas automaticamente. Os operadores devem ser treinados para reconhecer em tempo hábil os eventos inicializadores de um acidente e responder corretamente e de uma maneira oportuna a tais condições anormais. Eles também devem ser exaustivamente treinados em procedimentos operacionais apropriados, de forma a tornarem-se totalmente familiarizados com seu emprego.

Deste modo, a prevenção de acidentes dependerá de equipamentos projetados de modo conservador e de boas práticas operacionais para prevenir falhas, garantia de qualidade para verificar a rígida aderência às especificações de projeto, vigilância para identificar precocemente degradações no desempenho ou falhas durante operação, e ações planejadas para assegurar que pequenas falhas ou desvios não se propaguem no sentido uma situação mais grave.

A Análise Probabilística de Segurança deve orientar o projeto e operação, identificando potenciais cenários acidentais que possam contribuir de modo significativo para o Risco Objetivo total da instalação. Os resultados desta análise devem implicar em ações de segurança para reduzir esta contribuição.

3.2.2.3 Mitigação das Conseqüências de Acidentes

Princípio: Os Planos de Emergência interno e externo que efetivamente reduzem as conseqüências de um acidente, minimizando as conseqüências de eventuais liberações de material radioativo, são desenvolvidos e efetivamente implementados e periodicamente exercitados.

A mitigação das conseqüências de acidentes estendem o conceito de defesa em profundidade para além da prevenção de acidente. As ações de proteção que conduzem à mitigação de acidente são de três tipos: gerenciamento de acidentes, dispositivos especiais de segurança e contramedidas externas à IPN .

O gerenciamento de acidente inclui procedimentos operacionais previamente definidos que, em circunstâncias nas quais são excedidas as especificações de projeto da instalação, faria uso ótimo dos equipamentos existentes, eventualmente de modo

incomum, para restabelecer o controle sobre a evolução do acidente. Esta fase de gerenciamento do acidente teria o objetivo de restabelecer um estado seguro na instalação, com o reator desligado, o combustível continuamente resfriado, o material radioativo confinado e a função de confinamento garantida.

Em tais circunstâncias, os dispositivos especiais de segurança atuariam de forma a confinar o material radioativo liberado pelo núcleo, fazendo com que as eventuais liberações para o ambiente fossem mínimas. Estes dispositivos especiais de segurança incluem barreiras físicas, algumas das quais tendo como único propósito conter o material radioativo.

As contramedidas externas incluídas nos Planos de Emergência vão além das ações de proteção internas, compensando a remota possibilidade de falha. Em tal caso, os efeitos sobre a população circunvizinha ou o ambiente seriam mitigados por ações tais como abrigo ou evacuação, controle de acesso e descontaminação, e pela prevenção da transferência do material radioativo para as cadeias alimentares e outros caminhos de irradiação de seres humanos.

3.2.3 PRINCÍPIOS TÉCNICOS GERAIS

Identifica-se uma série de princípios técnicos gerais subjacentes à aplicação efetiva da tecnologia de segurança às IPN visando o atendimento dos Objetivos acima apresentados.

3.2.3.1 Emprego de Técnicas de Engenharia Validadas

Princípio: A tecnologia de propulsão nuclear está baseada em práticas de engenharia validadas através de experimentos, ensaios, testes e realimentação de experiência operacional, consolidadas em códigos e normas aprovadas e adequadamente documentadas.

Os sistemas e componentes são projetados de modo conservador, sendo fabricados e testados dentro de padrões de qualidade proporcionais a suas funções de segurança. São utilizados códigos e normas aprovados cuja adequação e aplicabilidade às condições de operação foram devidamente avaliadas e completados ou modificados se necessário. Caso sejam identificadas oportunidades para aperfeiçoamento das práticas existentes, estas deverão ser cautelosamente aplicadas.

Os códigos e normas para uso nuclear são adotados após sua formulação pela comunidade científica e tecnológica e sua aprovação pela ASN. Alguns códigos e normas existentes foram modificados a partir de sua forma original para considerar as características específicas e a elevada importância atribuída à segurança para seu emprego na área nuclear. Estes códigos e normas aprovados têm os objetivos simultâneos de confiabilidade e seguridade, sendo baseados em princípios comprovados pela pesquisa, experimentos e ensaios, e experiência operacional. Os códigos e normas de uso naval têm características semelhantes, porém com um caráter não tão formal no que tange à aprovação pela ASN. Eles têm como objetivo principal a busca de uma máxima disponibilidade e capacidade de sobrevivência para o submarino.

Os métodos de fabricação e construção são igualmente desenvolvidos a partir de uma base experimental de validação. Fornecedores aprovados e com significativa experiência acumulada contribuem de forma decisiva para a confiabilidade de componentes importantes para a segurança. Os desvios das práticas de fabricação e construção que previamente demonstraram sua adequabilidade são aceitos somente após demonstração cabal de que as alternativas satisfazem as especificações nucleares. A qualidade é garantida pelo uso de normas apropriadas e pela seleção, treinamento e qualificação do pessoal de fabricação e construção. O emprego de técnicas de engenharia validadas continua ao longo de todo o ciclo de vida da instalação. Quando reparos e modificações são feitos, uma análise e revisão de projeto deve ser executada para assegurar que o sistema retornou a uma configuração coberta pela análise de segurança e especificações técnicas. Quando questões de segurança novas e não revistas são colocadas, a análise de segurança deve ser refeita.

O projeto e construção de tipos novos de IPN são baseadas até onde possível na experiência operacional obtida em instalações similares ou em resultados de programas de pesquisa e de operação de protótipos.

3.2.3.2 Garantia da Qualidade

Princípio: As atividades de garantia de qualidade são exercidas ao longo do ciclo de vida de um SNA como parte de um sistema abrangente que proporciona, com alta confiabilidade, que todos os componentes fabricados, assim como todos os serviços e tarefas executados atendam os requisitos especificados.

O sistema de garantia de qualidade abrangente referido no princípio acima começa com a execução do projeto e análises conforme o princípio precedente, i.e. com o emprego de técnicas de engenharia validadas, e continua com o uso dos métodos de garantia de qualidade. Os outros princípios técnicos fundamentais de segurança também são importantes no desenvolvimento e implementação deste sistema, particularmente o princípio de análise e verificação da segurança e o princípio da experiência operacional e da pesquisa de segurança, tratados mais adiante.

O alto padrão de qualidade tanto dos componentes como do elemento humano constitui o cerne da segurança de uma IPN . A meta do sistema da qualidade é assegurar que os equipamentos funcionarão e os indivíduos executarão suas tarefas de modo satisfatório. Ao longo do ciclo de vida da instalação, estas técnicas são aplicadas a todo o espectro de atividades de projeto, obtenção de componentes, montagem, comissionamento, manutenção, inspeções e testes.

Todos os componentes, estruturas e sistemas são classificados com base na importância de suas funções para a segurança, sendo desta forma projetados, fabricados e montados dentro de padrões de qualidade proporcionais àquela classificação.

As técnicas de garantia de qualidade compõem um gerenciamento adequado e são essenciais para atingir e demonstrar o atendimento de um alto padrão de qualidade dos produtos e da operação. Uma estrutura organizacional adaptada às técnicas de garantia de qualidade é necessária a todas as organizações envolvidas, devendo prover uma definição clara das responsabilidades dos diversos grupos componentes e canais de comunicação e coordenação entre eles.

Esta estrutura é fundamentada no princípio de que a responsabilidade por alcançar qualidade em uma tarefa está em quem a executa, com outros verificando que a tarefa foi executada corretamente, e ainda outros auditando o processo como um todo. A autoridade do pessoal de garantia de qualidade é estabelecida de modo explícito dentro da organização de forma a permitir identificar problemas de qualidade inadequada e os resolver. A seleção e treinamento de pessoal para atividades de garantia de qualidade, adaptado às normas técnicas aplicáveis e à cultura institucional das organizações envolvidas deve receber atenção especial.

O Programa de Garantia de Qualidade PGQ proporciona a base para a análise de tarefas, desenvolvimento de métodos, estabelecimento de padrões e identificação dos equipamentos e qualificações necessárias. Dentro da base estabelecida pelo PGQ está a definição dos itens e atividades para as quais aplica-se a garantia de qualidade e as normas ou outros requisitos que devem ser implementado por instruções, cálculos, especificações, desenhos e outros documentos de engenharia.

As técnicas de garantia de qualidade cobrem a validação de projeto, o fornecimento e emprego de materiais, os métodos de fabricação, inspeção e testes, e os procedimentos para assegurar que as especificações são atendidas. Os documentos associados estão sujeitos a procedimentos estritos para verificação, emissão, alteração e cancelamento. Os procedimentos formais para tratar não-conformidades são um aspecto importante do PGQ.

Um componente essencial de garantia de qualidade é a verificação documentada de que as tarefas foram executadas como requerido, as não-conformidades foram identificadas e corrigidas, e que foram tomadas ações para evitar a repetição de erros. Os meios necessários para atingir este objetivo incluem uma hierarquia de documentação, procedimentos de controle de qualidade que possibilitem a amostragem dos produtos, acompanhamento das práticas adotadas e testemunho de testes e inspeções, e pessoal suficiente em número e qualificação.

3.2.3.3 Fatores Humanos

Princípio: O pessoal envolvido nas atividades que afetam segurança da IPN é treinado e qualificado para executar suas tarefas. A possibilidade de erro humano na operação da IPN é considerada facilitando as decisões corretas e inibindo as decisões erradas tomadas pelos operadores, e implementando meios para detectar e corrigir ou compensar erros.

Um das lições mais importantes depreendidas da análise dos eventos anormais reais, desde os incidentes menores até acidentes graves, é o fato de serem, frequentemente, resultado de ações humanas incorretas. Tais eventos ocorrem quando os operadores não reconhecem a importância para a segurança de suas ações, quando violam procedimentos, quando não foram alertados para condições particulares da instalação, são confundidos por dados incompletos, ou não entendem completamente o comportamento da instalação. A organização operadora deve reconhecer o alto nível

tecnológico da IPN e, portanto, assegurar que seu pessoal possa operá-la de modo satisfatório.

O componente de erro humano de eventos indesejados e acidentes foi muito grande no passado. A solução para este problema deve ser alcançada em duas frentes: no projeto, através da automação, e pelo uso otimizado das capacidades humanas em circunstâncias não usuais.

Os dispositivos de engenharia e controles administrativos devem proteger a instalação contra violações da segurança. Além disso, a atenção aos fatores humanos na fase de projeto deve assegurar que a instalação seja tolerante ao erro humano, por exemplo, pela atuação automática de sistemas de controle ou de proteção, caso uma ação do operador implique num parâmetro da instalação exceder limites operacionais normais ou limites de desligamento. O projeto de sistemas de proteção deve assegurar que a intervenção do operador para corrigir falhas só é requerida em casos onde há tempo suficiente para diagnose e ação de corretiva.

O arranjo físico da Estação de Controle de Máquinas ECM deve permitir a localização e concentração de indicadores e atuadores usados em operações relacionadas à segurança e gerenciamento de acidentes, e ferramentas informatizadas para auxílio ao diagnóstico, de forma a permitir uma rápida resolução das questões de segurança. Os dados disponíveis na ECM devem ser suficientes para a diagnose de qualquer falha que possa se desenvolver e para avaliar os efeitos de qualquer ação executada.

Devem existir meios de comunicação confiáveis entre a ECM e os operadores que se encontram em outros locais e possam ter que tomar ações que afetem o estado da instalação. Os procedimentos administrativos devem assegurar que tais ações sejam autorizadas previamente pelos operadores da ECM. O arranjo e identificação dos atuadores localizados fora da ECM devem prevenir erros na sua seleção.

Para manter a instalação dentro dos limites do domínio de operação seguro, são seguidos somente procedimentos operacionais aprovados. Para garantir que isto efetivamente seja respeitado, o treinamento e retreinamento dos operadores em sala de aula, em simuladores e na própria instalação, além do estudo aprofundado dos sistemas componentes da Instalação, devem receber alta prioridade. Ferramentas de auxílio à

operação, manutenção e inspeção devem ser desenvolvidas levando em conta os pontos fortes e os pontos fracos do desempenho humano.

A discussão precedente enfatiza o fator humano na operação, o que é particularmente importante, mas a atenção a este aspecto não deve negligenciar o fator humano na manutenção e inspeções. Os erros nessas atividades foram causas importantes de falhas de componentes e sistemas no passado. Por isso, o pessoal de manutenção, da mesma maneira que o pessoal de operação, também deve seguir procedimentos operacionais aprovados que assegurem a excelência no desempenho de suas tarefas.

3.2.3.4 Análise e Verificação de Segurança

Princípio: A análise de segurança é feita antes que a construção e operação da IPN se inicie. A análise é suficientemente documentada e independentemente revisada, sendo atualizada à luz de novas informações de segurança significativas surgidas ao longo do ciclo de vida do SNA.

A análise de segurança inclui uma revisão crítica sistemática dos modos pelos quais estruturas, sistemas e componentes poderiam falhar, e identifica as consequências de tais falhas. A análise é empreendida expressamente para revelar qualquer deficiência subjacente ao projeto. Os resultados são documentados em detalhes para permitir auditoria independente do escopo, profundidade e conclusões da revisão crítica.

O Relatório de Análise de Segurança RAS preparado para o licenciamento contém uma descrição da instalação suficientemente detalhada para permitir a análise independente de suas características de segurança.

O RAS inclui informações técnicas sobre as áreas marítimas de operação do SNA e áreas onde se localizam as instalações de apoio à sua operação em terra, sobre as características principais de sistemas, especialmente aqueles com função de controle e desligamento do reator, resfriamento do combustível e contenção do material radioativo e dos dispositivos especiais de segurança. O RAS descreve a ainda a análise feita para os ABP e apresenta os resultados obtidos.

A elaboração do RAS pela organização operadora e sua revisão pela ASN constituem a base para a aprovação da construção e operação da IPN, demonstrando que

todas as questões de segurança foram adequadamente resolvidas ou são passíveis de resolução.

Devem ser desenvolvidos métodos para avaliar o atendimento aos objetivos de segurança. Estes métodos são aplicados inicialmente na fase de projeto, e posteriormente, ao longo das demais etapas da vida útil da instalação, se forem planejadas alterações na configuração inicial, e na avaliação de experiência operacional para verificar se a segurança vem sendo mantida. Dois métodos de análise complementares, determinístico e probabilístico, são empregados. Estes métodos são conjuntamente usados para avaliar e melhorar a segurança no projeto e na operação.

No método de análise determinístico, seleciona-se um conjunto de ABP que engloba um largo espectro de eventos indesejados que poderiam ameaçar a segurança da instalação. A análise dos cenários acidentais decorrentes destes eventos é utilizada para demonstrar que a resposta da instalação e de seus sistemas de segurança satisfaz as especificações predeterminadas tanto em termos de desempenho da própria instalação como em termos de atendimento aos objetivos de segurança. O método determinístico emprega modelos físicos e matemáticos de análise validados e aceitos pela ASN para prever a evolução dos eventos e suas consequências.

O método probabilístico é usado para avaliar a probabilidade de estados finais da instalação decorrentes de cenários acidentais inicializados por um conjunto pré-definido de eventos indesejados. Esta avaliação pode levar em conta os efeitos de ações de proteção e mitigação de consequências tomadas dentro e fora da instalação. A análise probabilística é usada para calcular o Risco Objetivo Residual da instalação e, especialmente, identificar possíveis deficiências no projeto ou nos procedimentos de operação que poderiam causar aumento excessivo no risco.

O método probabilístico deve ainda ser usado para estimar a frequência de ocorrência dos diversos cenários operacionais identificados qualitativamente, auxiliando na seleção dos ABP que requerem uma análise determinística.

O processo é repetido no seu todo ou em partes ao longo do ciclo de vida da instalação se novos resultados da pesquisa de segurança ou da análise da experiência operacional demonstrarem esta necessidade.

3.2.3.5 Proteção Radiológica

Princípio: Um sistema de práticas de proteção radiológica, consistente com as recomendações da ICRP, da IAEA, e da ASN, é adotado no projeto, no comissionamento e nas fases operacionais do SNA.

São tomadas medidas para proteger a tripulação, o pessoal de apoio em terra e o público em geral contra os efeitos prejudiciais da radiação proveniente da IPN em operação normal, em condições operacionais anormais e em acidentes. Estas medidas tem como objetivo o controle das fontes de radiação, a implementação e garantia de contínua efetividade das barreiras de blindagem e contenção e dos Equipamentos de Proteção Individual EPI, e o efetivo cumprimento de procedimentos administrativos para controlar as exposições individuais.

A Proteção Radiológica é considerada no projeto prevendo-se blindagens biológicas da fontes de radiação externa, confinando-se as fontes que possam causar contaminação ambiental e otimizando-se o arranjo físico da instalação para minimizar os tempos de execução de atividades de operação e manutenção em zonas de radiação.

Para o controle, orientação e proteção do pessoal, são desenvolvidos procedimentos que definem as práticas seguras, os meios físicos de proteção e os procedimentos administrativos necessários para cada tarefa que poderia conduzir à exposição à radiação. Cuidados especiais devem ser tomados para as tarefas realizadas em ambientes particularmente severos do ponto de vista de doses individuais.

Estas são as características principais que tornam possível atender ao objetivo de proteção radiológica. Assegurar que ele é atingido requer vigilância e monitoramento contínuo das condições da instalação e sua manutenção num nível máximo de limpeza com respeito ao acúmulo localizado de contaminação.

3.2.3.6 Experiência Operacional e Pesquisa de Segurança

Princípio: As organizações envolvidas na propulsão nuclear asseguram que a experiência operacional acumulada e os resultados da pesquisa científica e tecnológica pertinente à segurança sejam coletados, divulgados, revisados e analisados, e que os ensinamentos retirados destas informações sejam efetivamente aprendidos pelo pessoal envolvido e que ações sejam tomadas para corrigir eventuais deficiências.

A organização que opera uma IPN mantém um sistema efetivo para coleta e interpretação de experiência operacional, e dissemina prontamente as informações importantes para a segurança entre seu próprio pessoal e para outras organizações pertinentes. As causas primárias dos acidentes são analisadas. São identificados eventos que podem ser considerados como precursores de acidentes e são tomadas ações para prevenir sua repetição. Cada organização operadora busca aprender da experiência das outras organizações, coordenando-se o compartilhamento de dados operacionais.

O objetivo primário é que nenhum evento relacionado com a segurança passe despercebido e que sejam feitas correções para prevenir sua recorrência, seja na mesma instalação ou em outra semelhante. Mais importante ainda, este princípio reflete o fato de que um potencial acidente seria provavelmente identificado através da ocorrência de eventos precursores, e desta forma tornando-se previsível e portanto evitável. O retorno da experiência operacional também aumenta a base de conhecimentos sobre características funcionais dos equipamentos e as tendências de variação de seu desempenho, e ainda facilita dados quantitativos para a análise de segurança.

A pesquisa científica e tecnológica para aumentar a base de conhecimentos sobre o desempenho da IPN, sobre sua resposta a ocorrências anormais e sobre possíveis sucessões de eventos em acidentes severos leva à melhoria da interpretação do retorno da experiência e a uma melhor definição de medidas corretivas que poderiam ser necessárias. Vantagens adicionais podem ser obtidas pelo uso dos resultados da pesquisa para melhorar o desempenho da IPN, mantendo margens de segurança aceitáveis. Os resultados da pesquisa podem ainda ser incorporados ao projeto da IPN, tornando-a mais segura. De uma maneira geral, a pesquisa e desenvolvimento propiciam a manutenção da competência técnica dentro de organizações envolvidas na propulsão nuclear.

3.3 PRINCÍPIOS ESPECÍFICOS

A estrutura de princípios de segurança é complementada pelos princípios específicos apresentados a seguir. Identifica-se sete categorias destes princípios, as cinco primeiras organizadas na ordem de progressão do ciclo de vida do SNA: áreas de mobilidade e localizações fixas pré-definidas, projeto, fabricação e construção, comissionamento e operação. Somam-se duas categorias adicionais de princípios

cobrindo o gerenciamento e mitigação dos efeitos de acidentes severos, embora estes sejam improváveis. Os objetivos de segurança e os princípios fundamentais apresentados anteriormente constituem uma estrutura conceitual onde repousam os princípios de específicos segurança, com ampla aplicação nas suas sete categorias.

3.3.1 ÁREAS DE MOBILIDADE E LOCALIZAÇÕES FIXAS PRÉ-DEFINIDAS

O conceito de emprego de um SNA nacional consideraria, a princípio, uma área de mobilidade operativa localizada no Oceano Atlântico, entre os paralelos de 25° N e 65° S. A área principal de emprego estaria situada entre os paralelos de 15° N e 60° S, englobando águas tropicais, subtropicais e temperadas. Uma área secundária Norte incluiria o Mar do Caribe, com águas tropicais, entre os paralelos de 15° N e 25° N e outra área Secundária Sul, entre os paralelos de 60° S e 65° S, abrangendo parte do Oceano Polar Antártico.

Dentro desta área de mobilidade, pode-se identificar localizações costeiras fixas onde o SNA estacionará durante seus períodos de reparo e manutenção e durante escalas feitas ao longo de suas missões operativas. Estas localizações incluem a Base Naval Principal à qual o SNA está subordinado de modo permanente, o estaleiro de construção, bases navais secundárias às quais o SNA poderá ser destacado em caráter temporário, portos civis no qual o SNA poderá atracar ou fundear por períodos curtos de escala e outros fundeadouros onde poderá permanecer por razões operativas.

A seleção das localizações fixas é um processo com significativa importância à medida que as circunstâncias locais podem afetar a segurança do SNA e das instalações nucleares de apoio em terra. Esta seleção é realizada buscando-se um equilíbrio entre fatores concorrentes, que incluem aspectos estratégicos, econômicos, técnicos, de relações públicas e de segurança. Consequentemente, embora a implementação de um dos princípios fundamentais de segurança a seguir apresentados pudesse conduzir eventualmente à rejeição de um local proposto por razões puramente ligadas à segurança, este não seria o único fator considerado.

Os princípios constituem portanto uma orientação sobre os aspectos de segurança a serem considerados quando da seleção de localizações fixas para o SNA. As modificações das características do local cuja ocorrência pode ser prevista ao longo do ciclo de vida do SNA devem ser consideradas no processo de seleção.

Serão então apresentados e discutidos a seguir princípios para operação do SNA nas áreas de mobilidade e localizações fixas, com o propósito de estabelecer:

- padrões para a análise preliminar e final de segurança realizadas antes do SNA obter autorização para operação;
- fundamento para a regulamentação e diretivas administrativas estabelecidas por autoridades portuárias quando o SNA encontra-se em um porto civil; e
- fundamento para o estabelecimento de procedimentos operacionais do navio.

3.3.1.1 Condições Gerais para Operação do SNA

Princípio: O público circundante não deverá ser afetado por riscos radiológicos mesmo que um acidente grave ocorra. O público circundante não deverá sofrer danos à saúde devido às radiações mesmo que um acidente severo ocorra, sendo a dose coletiva, neste caso, tão reduzida quanto razoavelmente praticável. Em ambas as situações, a localização do navio nuclear deve ser tal que ele possa ser evacuado para um fundeadouro seguro e que medidas adequadas para proteção do público possam ser tomadas.

Como acidente grave entende-se o pior acidente possível do ponto de vista técnico, utilizado como referência para a análise da segurança do navio. O Acidente de Grande Perda de Refrigerante Primário AGPRP é convencionalmente considerado como Acidente Básico de Projeto ABP de referência.

Como acidente severo entende-se acidentes que excedam a gravidade do ABP, mas cuja ocorrência é considerada inverossímil do ponto de vista técnico. Um tal acidente decorreria do estabelecimento de hipóteses de falha em dispositivos especiais de segurança que atuam durante a evolução do ABP, conduzindo à liberação de quantidades significativas de materiais radioativos para o exterior do SNA. Neste caso, superpõe-se ao ABP convencional uma falha do sistema de contenção, com liberação para o ambiente de uma fração do inventário de materiais radioativos que se encontrariam retidos dentro do compartimento do reator (termo-fonte acidental).

3.3.1.2 Condições para Atracação, Fundeio e Navegação em Zonas Portuárias Civas

Princípio: Toda a área dentro de uma curta distância do SNA deve ser considerada como zona restrita e toda área dentro de uma longa distância do reator do navio nuclear deve ser uma zona não-residencial.

Entende-se como “curta distância” a zona dentro da qual o público pode ser “afetado pela radiação” por exposição externa ou por inalação de material radioativo durante “período de tempo de exposição contínua”, se nenhuma medida é tomada para o público em caso de “acidente grave”. Zona restrita é a área onde, a princípio, nenhuma pessoa reside de modo permanente e que se encontra sob controle administrativo das autoridades portuárias.

O “período de tempo de exposição contínua:” é tal que, após decorrido, a exposição do público em uma posição específica é desprezível devido a, por exemplo, evacuação do navio avariado. Considera-se que o público não foi “afetado pela radiação” quando as doses máximas para a glândula tireóide (consequência da inalação de iodo radioativo liberado pelo reator acidentado) e para o corpo inteiro (consequência da radiação γ emitida pela nuvem formada pelos gases inertes radioativos liberados e pela radiação γ direta emitida pelos demais materiais radioativos contidos no interior do compartimento de contenção do reator acidentado) do indivíduo mais exposto forem inferiores aos limites quantitativos estabelecidos pelos Critérios Gerais apresentados pelo Capítulo 4. Para considerar-se que o público não foi “seriamente afetado pela radiação”, estas doses máximas não deverão exceder o dobro dos limites anteriormente estabelecidos.

Como “longa distância” entende-se a zona dentro da qual o público pode ser “seriamente afetado pela radiação” por exposição externa ou por inalação de material radioativo durante um “período de tempo de exposição contínua”, se nenhuma medida é tomada para o público em caso de “acidente severo”. Zona não-residencial é uma área onde a princípio nenhuma pessoa reside de modo permanente.

3.3.1.3 Condições para Atracação e Fundeio em Local Protegido

Princípio: O navio nuclear quando atracado, fundeado ou navegando em zonas portuárias deve possuir, previamente designado, um ponto de atracação ou fundeio em local protegido para onde possa ser prontamente evacuado no caso de um acidente. Este local deve atender às seguintes condições: toda área dentro de uma “distância de exclusão” deve ser “zona não-residencial”; a área fora da “distância de exclusão” do local protegido e dentro da “distância de evacuação” deve ser “zona de baixa população”.

Como “distância de exclusão” entende-se a zona dentro da qual o público pode ser afetado pela radiação por exposição externa ou por inalação de material radioativo em caso de “acidente grave”, não sendo considerado neste caso nenhuma movimentação posterior do SNA.

Como “distância de evacuação” entende-se a zona dentro da qual o público pode ser “seriamente afetado pela radiação” por exposição externa ou por inalação de material radioativo em caso de acidente severo, não sendo considerada neste caso nenhuma movimentação posterior do SNA.

Como zona de baixa população entende-se aquela onde medidas apropriadas podem ser tomadas para proteger o público de riscos radiológicos sérios, i.e. uma zona de baixa densidade demográfica, dotada de um sistema de comunicações e transportes adaptado à situação de evacuação rápida..

3.3.1.4 Condições para Navegação em Águas Costeiras

Princípio: O SNA deve navegar a uma distância de segurança da costa

Como “distância de segurança” entende-se aquela abaixo da qual um indivíduo do público poderia ser “seriamente afetado pela radiação” no caso de ocorrência de um “acidente severo”.

3.3.1.5 Fatores Ambientais Externos

Princípio: Os fatores ambientais locais das áreas de mobilidade que poderiam afetar adversamente a segurança do SNA devem ser considerados nos critérios de projeto da IPN. Os fatores ambientais locais devem ser considerados como figuras de mérito para a seleção das localizações fixas. Os fatores ambientais locais das localizações fixas selecionadas que poderiam afetar adversamente a segurança tanto do SNA como das Instalações Nucleares de apoio em terra devem ser considerados nos critérios de projeto da IPN.

Os fatores ambientais locais incluem fatores naturais e riscos associados às atividades humanas circundantes. Os fatores ambientais locais naturais a serem considerados para as áreas de mobilidade incluem estados de mar, batimetria (perfis de profundidade), propriedades físico-químicas da água do mar (temperaturas, salinidades) e ocorrência de fenômenos oceanológicos e meteorológicos severos.

Para os fatores ambientais locais naturais a serem considerado para as localizações fixas costeiras somam-se as características geológicas e sismológicas, os regimes de correntes e de marés e o potencial de perturbações hidrológicas e meteorológicas.

Os fatores ambientais locais associados às atividades humanas em condições normais de paz nas áreas de mobilidade e nas proximidades das localizações fixas costeiras incluem riscos de agressões decorrentes do tráfego marítimo civil e de manobras navais.

Nas localizações fixas costeiras, incluem riscos de explosões, incêndios decorrentes de instalações portuárias e retro-portuárias, assim como do tráfego rodoviário e ferroviário circundante, e riscos de quedas de aeronaves devidas ao tráfego aéreo local. Os riscos de intrusão, roubo de materiais nucleares, sabotagem e ações terroristas devem também ser considerados para elaboração do Plano de Proteção Física da Instalação.

Os fatores ambientais locais associados às atividades humanas nas áreas de mobilidade em condições de guerra ou conflito grave incluem riscos de agressões decorrentes do armamento empregado pelo inimigo nas suas ações de Guerra Anti-Submarino GAS (torpedos, cargas de profundidade, minas) e nas suas ações de Guerra Nuclear-Química-Biológica GNBQ. Nas localizações fixas costeiras, adicionam-se os riscos de agressões decorrentes de ações de comandos e de bombardeios aéreos, navais e terrestres.

A análise de fatores ambientais deverá determinar a probabilidade de ocorrência de eventos externos que possam afetar adversamente a segurança do SNA e de sua IPN, assim como das instalações nucleares de apoio em terra. A análise de agressões deverá determinar os possíveis efeitos dos eventos externos cuja probabilidade de ocorrência é significativa sobre estas instalações.

A gravidade destes efeitos determinará o risco correspondente e, conseqüentemente, a necessidade de implementação de ações de prevenção e de proteção no projeto e operação das instalações. Os potenciais eventos externos extremos que possam conduzir a IPN a condições acidentais severas têm particular relevância, devendo ser verificada a viabilidade de implementação de ações de mitigação de conseqüências.

3.3.1.6 Impacto Radiológico sobre o Público e o Ambiente

Princípio: O impacto radiológico do SNA e das Instalações Nucleares de apoio em terra sobre o público e ambiente é avaliado tanto para condições de operação normal como para condições acidentais.

Os materiais radioativos podem causar detrimento à saúde do homem e das demais espécies vivas diretamente, através de sua liberação para o mar, rios e lagoas, ar e solo. Estes materiais dispersos poderão ainda ser incorporados indiretamente através de transferências físicas entre os diversos compartimentos (do ar para o solo, do ar para o mar, rios e lagos, do mar para o solo, do solo para aquíferos subterrâneos) e ao longo das cadeias alimentares (do mar para os produtos da pesca, do solo para produtos agrícolas e pecuários).

As transferências ao longo das cadeias alimentares são particularmente complexas, à medida que envolvem fenômenos físicos e químicos (características dos radionuclídeos envolvidos), oceanográficos (circulação geral e local dos mares), geomorfológicos (estrutura dos solos), hidrológicos (estruturas das bacias hidrográficas superficiais e aquíferos subterrâneos), meteorológicos (circulação geral e local da atmosfera), biológicos (características de incorporação dos radionuclídeos às espécies vivas, hábitos alimentares dos diferentes elos da cadeia alimentar), sociais (hábitos alimentares locais das populações) e econômicos (fluxos de comércio de alimentos nas regiões potencialmente impactáveis). Este último aspecto é de particular relevância à medida que pode promover transferências a longas distâncias, em escala até mesmo global.

As características oceanográficas das áreas de mobilidade, assim como as características físicas das localizações fixas, tais como topografia, geologia e hidrologia devem ser suficientemente conhecidas de forma a poder-se avaliar impactos de potenciais acidentes. As características ambientais das áreas de mobilidade (distribuição de espécies marinhas, usos do mar, distribuição das populações litorâneas) assim como as características ambientais das localizações fixas (distribuição de espécies terrestres, uso da terra e dos recursos hídricos, distribuição das populações circundantes) devem igualmente serem conhecidas.

Os resultados dos estudos ambientais são usados para demonstrar que os objetivos de segurança são cumpridos, tanto em operação normal, para a qual são estabelecidos limites apropriados para descargas rotineiras de efluentes, como em liberações acidentais de materiais radioativos, caso em que são consideradas contramedidas previstas pelos Planos de Emergência Externos.

3.3.1.7 Viabilidade dos Planos de Emergência

Princípio: As áreas de mobilidade e as localizações fixas pré-definidas para o SNA são compatíveis com contramedidas externas que podem ser necessárias para limitar os efeitos de liberações acidentais de materiais radioativo. Esta compatibilidade deve ser mantida ao longo de todo ciclo de vida do SNA.

Considerando o atendimento ao princípio que estabelece condições para operação em águas costeiras, previamente apresentado, acidentes com o SNA nas áreas de mobilidade não implicarão, *a priori*, em implementação de Planos de Emergência Externos. No que tange a acidentes nas localizações fixas pré-definidas, a viabilidade dos Planos de Emergência Externos pode ser afetada por características físicas e ambientais, e isto deverá ser levado em conta na seleção inicial destes locais.

3.3.1.8 Garantia de Continuidade da Fonte Fria

Princípio: Nas localizações fixas pré-definidas do SNA é disponível uma fonte fria confiável capaz de remover a energia gerada pela IPN após o desligamento do reator, tanto a curto como a longo prazo.

A fonte fria para remoção de calor da IPN de um SNA em operação nas suas áreas de mobilidade é evidentemente o próprio mar. Neste caso, a confiabilidade e capacidade da fonte fria é praticamente infinita. Entretanto, o problema da continuidade da fonte fria coloca-se em situações operacionais especiais, tais como pouso no fundo, e em situações acidentais, tais como encalhe e naufrágio. No caso de pouso no fundo e encalhe, as caixas de mar podem ser bloqueadas devido a posição do SNA e as características (tença) do fundo. No caso de naufrágio, tornam-se indisponíveis as fontes de energia que garantem a alimentação das bombas de circulação de água do mar, o resfriamento somente podendo ser continuado através de processos de circulação natural.

Para o SNA atracado ou fundeado nas localizações fixas pré-definidas, o problema coloca-se de maneira semelhante às condições de operação na área de mobilidade, sendo a fonte fria garantida pela desobstrução das caixas de mar e continuidade de fornecimento de energia para as bombas de circulação.

Para o SNA docado nas localizações fixas pré-definidas devem ser previstos meios externos para garantir a continuidade da remoção do calor residual do núcleo do reator. Neste caso, condições ambientais externas adversas poderiam ameaçar a disponibilidade destes meios externos, a menos que sejam tomadas precauções adequadas no projeto e operação tanto do SNA como das instalações de apoio em terra.

3.3.2 PROJETO

O objetivo primário dos projetistas de IPN é garantir o sucesso da missão do SNA. Deve ser garantido que os componentes, sistemas e estruturas da IPN tenham características, especificações e materiais apropriados, e que sua integração funcional seja tal que as especificações de desempenho global da IPN são atendidas. As especificações da IPN são consistentes com a missão, em termos de geração de energia, vida útil, manobrabilidade, necessárias para atender as demandas do SNA e, além disto, atender aos objetivos de segurança identificados na seção 3.1 e os princípios gerais de segurança identificados pelas seções 3.2 e 3.3. Os projetistas também mantêm um sistema de controle de configuração para registrar a base de projeto de segurança da Instalação, garantindo que alterações realizadas ao longo das etapas de construção, comissionamento e operação mantenham a conformidade com esta base de projeto.

Na fase de projeto, são consideradas as necessidades e capacidades de desempenho do pessoal que operará a Instalação, e definidas informações e recomendações práticas para incorporação nos procedimentos operacionais. As opções de projeto são selecionadas de modo a facilitar o atendimento da primeira prioridade de segurança, que é a prevenção de acidentes. Também são consideradas as opções de projeto que facilitem a prevenção e mitigação das conseqüências de acidentes que poderiam conduzir a uma liberação significativa de materiais radioativos para fora da Instalação.

A segurança no projeto da IPN se preocupa basicamente em controlar a localização, a movimentação e as condições dos materiais radioativos dentro da

Instalação, de forma que eles estejam permanentemente confinados em um estado seguro dentro das barreiras físicas previstas para isto.

A análise de segurança deverá verificar o comportamento da Instalação sob um amplo espectro de condições, incluindo operação normal em regime permanente e condições transientes durante manobras do SNA. Inclui também ocorrências anormais antecipadas e ocorrências hipotéticas nas quais a Instalação deverá resistir sem dano inaceitável em virtude de suas características funcionais e das características de segurança implantadas. O projeto deverá tirar o máximo proveito de processos com características de segurança intrínseca. São também considerados acidentes além da base de projeto, assegurando-se que suas conseqüências podem ser efetivamente mitigadas por meio do gerenciamento de acidente e de contramedidas estabelecidas pelo planejamento de emergências.

Os aspectos de segurança no projeto da IPN estão associados às quatro funções que previnem a liberação e dispersão de materiais radioativos para fora da instalação:

- continuidade na geração de energia;
- controle da reatividade do núcleo;
- resfriamento do combustível; e
- contenção de materiais radioativos dentro das barreiras físicas apropriadas.

Os princípios específicos de segurança aplicados ao projeto são divididos em três grupos:

- procedimentos gerais: gerenciamento do projeto, tecnologia validada e base geral de projeto;
- segurança de sistemas funcionais: controle de processos, sistemas de segurança automáticos, objetivos de confiabilidade, falhas dependentes, qualificação de equipamentos, inspeção de equipamentos de segurança, proteção radiológica no projeto; e
- sistemas específicos de segurança: proteção contra transientes de potência, integridade do núcleo do reator, sistemas de desligamento automático, remoção de calor normal, remoção de calor em emergência, integridade do sistema de resfriamento do reator, contenção de materiais radioativos, proteção das estruturas de contenção, monitoramento das condições de segurança, preservação da capacidade

de controle, perda das alimentações elétricas normais e controle dos acidentes dentro da base de projeto.

3.3.2.1 Gerenciamento do Projeto

Princípio: A designação e subdivisão de responsabilidades pela segurança são bem definidas ao longo da fase de projeto da IPN e, posteriormente para alterações de projeto durante as fases operacionais.

O projeto de uma IPN segura é conduzido sob a autoridade de um gerente de engenharia suficientemente qualificado, cujas atitudes e ações refletem uma cultura de segurança e que assegura o atendimento de todos os requisitos de segurança regulamentares. Aspectos segregados do projeto podem ser desenvolvidos por diferentes seções de um grupo de projeto central e por outros grupos subcontratados a partes específicas do projeto. Um número adequado de pessoal qualificado é essencial em cada atividade. O gerente de engenharia estabelece um conjunto bem definido de interfaces entre os grupos encarregados das diversas partes do projeto, e entre os projetistas, fornecedores e construtores.

A equipe de projeto é comprometida na preparação do RAS e de outros documentos importantes para a segurança. Esta equipe também deve incluir um grupo de coordenação que tem a responsabilidade de assegurar que todas as exigências de segurança são cumpridas.

Este grupo está permanentemente familiarizado com as características e limitações dos componentes incluídos no projeto. Ele comunica-se com os futuros operadores para assegurar que suas necessidades são consideradas no projeto e que há um fluxo apropriado de informações de projeto para a elaboração dos procedimentos operacionais conforme os mesmos são desenvolvidos e para o planejamento e execução do treinamento de operadores. O grupo de coordenação tem acesso direto ao gerente de projeto mas não necessariamente é a ele subordinado.

Conforme o princípio fundamental apresentado na seção 3.2, a garantia da qualidade é aplicada a todas as atividades de projeto importantes para a segurança. Um componente essencial desta atividade é o controle de configuração, assegurando que a base de projeto de segurança é efetivamente registrada e mantida atualizada quando mudanças de projeto acontecem.

3.3.2.2 Tecnologia Validada

Princípio: As tecnologias incorporadas ao projeto são demonstradas por experimentos e testes de desempenho. Inovações tecnológicas somente são introduzidas no projeto após pesquisa e desenvolvimento com validação experimental em protótipos, tanto ao nível de componente, como de sistema ou Instalação completa, conforme apropriado.

Este princípio é uma aplicação específica do princípio fundamental apresentado na seção 3.2 sobre emprego de técnicas de engenharia validadas. O desenvolvimento tecnológico seguro requer um equilíbrio entre inovações e práticas consagradas. O projeto deverá ser executado conforme normas e regulamentações nacionais e internacionais aplicáveis, particularmente aquelas especificamente desenvolvidas para emprego nuclear, aceitas pelos órgão de regulamentação profissional da engenharia e reconhecidas pela ASN. Estas normas e regulamentações refletem procedimentos de projeto demonstrados por aplicações práticas anteriores. Devem, entretanto, ser consideradas melhorias nas práticas estabelecidas, que, para ascenderem ao nível de técnicas validadas deverão passar pelas etapas de experimentos, testes e avaliação de protótipos, eventualmente em escala.

A maioria das aplicações da tecnologia em engenharia requer o uso de métodos analíticos. Os modelos físicos e matemáticos usados em projeto são validados por meio de demonstração experimental ou operacional e análise de dados. Os resultados de análises mais complexas são verificados através de cálculos de *benchmarks* baseados em experimentos pertinentes, testes padronizados e “revisão pelos pares” (*peer review*). Sempre que possível devem ser usados dados e modelos realistas (*best estimate*) para estimar o desempenho de Instalação, definir as margens de segurança e determinar a evolução de condições acidentais. Onde a modelagem realista não é possível, modelos conservadores são empregados.

3.3.2.3 Base Geral de Projeto

Princípio: Uma IPN é projetada para atender a um conjunto de eventos incluindo condições normais, ocorrências operacionais antecipadas, eventos externos extremos e condições acidentais. Para este propósito, regras e critérios conservadores, que incorporam significativas margens de segurança, são usados para estabelecer os requisitos de projeto. Análises abrangentes são desenvolvidas para avaliar o desempenho de segurança e capacidades dos vários componentes e sistemas da Instalação.

Os vários eventos que a Instalação terá que enfrentar são classificados de acordo com suas probabilidades de ocorrência. O projeto deverá assegurar que não haverá nenhum dano à Instalação como resultado daqueles eventos classificados como operacionais normais, ou daqueles para os quais associa-se uma significativa probabilidade de ocorrência durante o ciclo de vida do SNA. A um nível de probabilidade muito mais baixo encontram-se combinações de falhas de componentes, sistemas e estruturas e erros humanos que poderiam ameaçar a proteção proporcionada pelas características de segurança inerentes aos sistemas ligados à operação normal da Instalação.

Dentro do princípio de defesa em profundidade, são então incluídos dispositivos e sistemas de segurança no projeto de Instalação, de forma a protegê-la contra a possibilidade de ocorrência de determinadas classes de acidentes e para mitigar as correspondentes conseqüências que contribuiriam significativamente para o Risco Objetivo Residual.

Os dispositivos especiais de segurança são, portanto, projetados para prevenir ou mitigar um espectro específico de acidentes. O acidente incluído neste espectro que impõe as características de um dispositivo especial de segurança é denominado o ABP para este dispositivo. Os dispositivos especiais de segurança são então projetados de forma que nenhum destes acidentes ou sucessões de acidentes seja predominante na composição do Risco Objetivo Residual da Instalação. O projeto considera ainda os requisitos para atividades de manutenção e inspeções periódicas, planejadas para assegurar a continuidade, ao longo de todo o ciclo de vida do SNA, da conformidade com a base geral de projeto.

3.3.2.4 Sistemas de Controle de Processos

Princípio: A operação normal e as ocorrências operacionais antecipadas são controladas de forma que as variáveis da Instalação e dos sistemas componentes permaneçam dentro de seus limites operacionais, reduzindo assim a frequência com que os sistemas de segurança são acionados.

São atribuídos às variáveis neutrônicas e termohidráulicas importantes para a segurança da Instalação faixas de operação, limites de proteção e limites de segurança. Os limites de segurança são valores extremos das variáveis para os quais uma análise conservativa acrescida de margens de segurança indica a possibilidade de inicialização

de danos indesejáveis ou inaceitáveis para a Instalação. Os limites de proteção são valores das variáveis inferiores aos limites de segurança que, se atingidos devido a ocorrências operacionais antecipadas ou a falhas ou mau funcionamento de equipamento, poderiam conduzir a Instalação a uma condição insegura, requerendo uma ação protetora automática, tal como uma redução de potência programada ou desligamento. Os limites de proteção são definidos de modo que as variáveis críticas da Instalação não atinjam os limites de segurança. A faixa de operação é o domínio de funcionamento normal da Instalação, definido por valores das variáveis inferiores aos limites de proteção.

É de fundamental importância para uma IPN que as ações automáticas não sejam muito freqüentemente induzidas, especialmente quando elas não são estritamente indispensáveis para proteção da Instalação, da tripulação ou do público. Uma elevada freqüência destas ações não só iria interferir adversamente com o sucesso da missão do SNA, como também poderia comprometer a segurança do submarino pela redução da disponibilidade da geração de energia e pelos efeitos de desgaste decorrentes de uma freqüência relativamente elevada de transientes bruscos, prejudicando a confiabilidade dos sistemas de segurança.

Entretanto, as variáveis neutrônicas e termohidráulicas mais significativas para a segurança são mantidas automaticamente dentro da faixa de operação. Isto é obtido por sistemas de controle com realimentação que acionam atuadores elétricos e mecânicos quando as variáveis evoluem para os limites da faixa de operação, restabelecendo o estado operacional normal. Os limites para a faixa de operação normal são escolhidos de forma que as ações de realimentação impeçam as variáveis de alcançar os limites de proteção em operação normal.

3.3.2.5 Sistemas de Segurança Automáticos

Princípio: Os sistemas de segurança automáticos garantem que o reator seja desligado de forma segura, que o resfriamento do combustível seja mantido e que as eventuais liberações de produtos de fissão através das barreiras sejam controladas, caso os limites de segurança sejam excedidos.

Apesar da alta qualidade do projeto e construção da IPN, postula-se que sucessões de eventos originando-se dentro ou fora da Instalação ocorrerão

ocasionalmente, excedendo as características de proteção dos sistemas de controle normais.

Estas falhas hipotéticas constituem um amplo espectro de inicializadores de acidentes com respeito aos quais o projeto é avaliado. Os dispositivos especiais de segurança são então incorporados para assegurar a integridade da Instalação, especialmente garantindo que os danos ao núcleo do reator seja limitado até mesmo no mais severo dos ABP. Em tais circunstâncias, seria controlada a potência do reator, seria mantido o resfriamento do núcleo e os materiais radioativos liberados da matriz do combustível permaneceriam contidos pelas barreiras físicas sucessivas.

A partida e continuidade da operação dos dispositivos especiais de segurança são garantidas por:

- projeto dentro do princípio de falha segura (*fail-safe*);
- proteção contra falhas em modo comum; e
- independência entre os dispositivos especiais de segurança e os sistemas de processo.

A aplicação do critério de falha única (ou simples) ao projeto dos dispositivos especiais de segurança garante que a falha de um componente não cause a perda da função a ser cumprida. Quando um sistema executa funções de processo e de segurança, seu projeto deve ser tal que a função de segurança não seja afetada por demandas inadvertidas do controle de processo.

As práticas de engenharia validadas, a experiência operacional e a análise de segurança requerem alta confiabilidade para os sistemas elétricos e a instrumentação que dão suporte aos sistemas de segurança. Os sistemas mecânicos e de processo que garantem o cumprimento das funções básicas de segurança dependem de eletricidade para alimentar seus componentes ativos, indicar seu estado e controlar sua operação. Deste modo, a confiabilidade de sistemas de segurança é determinada pela confiabilidade dos sistemas que lhe dão suporte, i.e. a segurança da IPN é intimamente dependente da continuidade da prestação de serviços proporcionada pelos sistemas da plataforma-navio do SNA.

O projeto da IPN deve incluir a capacidade para testar os sistemas de segurança automáticos ao longo do ciclo de vida do SNA, com auto-testes automáticos onde possível. As condições de teste devem buscar reproduzir as condições operacionais.

3.3.2.6 Objetivos de Confiabilidade

Princípio: Objetivos de confiabilidade são atribuídos a sistemas e funções de segurança. Estes objetivos são estabelecidos com base nos objetivos gerais de segurança e são consistentes com a atuação dos sistemas ou funções em diferentes cenários acidentais. Os componentes e sistemas para os quais são definidos objetivos de confiabilidade devem ser dotados de meios para testes e inspeções periódicas.

Os requisitos de projeto aplicáveis a sistemas e funções de segurança de alta confiabilidade devem ser expressos sob a forma de objetivos de confiabilidade específicos. A confiabilidade dos sistemas que dão suporte ao funcionamento dos sistemas e funções de segurança, tais como alimentação em energia para componentes e fornecimento de água de resfriamento deve ser considerada na formulação de objetivos de confiabilidade. Os objetivos são fixados para assegurar disponibilidade instantânea na partida e desempenho adequado ao longo do período de tempo de funcionamento exigido.

A confiabilidade requerida de sistemas e funções de segurança é baseada em análises de engenharia desenvolvidas através da combinação de métodos probabilísticos indutivos, dedutivos e de simulação. Independentemente dos métodos pelos quais os objetivos de confiabilidade são estabelecidos, a análise de confiabilidade é executada durante todo o processo de projeto para assegurar que os sistemas e funções de segurança satisfaçam efetivamente a estes objetivos. Testes funcionais e modelagem dos sistemas são empregados para demonstrar que os objetivos de confiabilidade são atendidos não somente no início da operação do SNA como ao longo de todo o seu ciclo de vida. A garantia da manutenção dos objetivos de confiabilidade durante a vida útil do SNA requer que o projeto desenvolva sistemas capazes de serem testados e inspecionados em serviço, sempre que possível sob condições de funcionamento reais.

Para alguns sistemas, os objetivos de confiabilidade podem ser definidos em valores que estão além das possibilidades de demonstração experimental. Neste caso, torna-se necessário assegurar esta maior confiabilidade funcional através de sistemas independentes adicionais cada um dos quais capaz de executar a função de segurança determinada. A diversidade e separação física destes sistemas reduzem a possibilidade de falhas em modo comum.

3.3.2.7 Falhas Dependentes

Princípio: As alternativas de projeto são selecionadas com o objetivo de prevenir a perda de funções de segurança devido a falhas simultâneas de vários componentes, sistemas ou estruturas resultantes de uma causa comum.

Os métodos de projeto apropriados para prevenir falhas simultâneas em dois ou mais sistemas são definidos para cada circunstância específica. Dentre os métodos usuais destacam-se a segregação física através da simples distancia ou de barreiras protetoras, redundância associada à diversidade e qualificação para resistir a agressões.

Alguns eventos de causa comuns que devem ser considerados teriam suas origens em ocorrências internas à IPN. Estes eventos incluem a perda de fontes de alimentação elétrica comuns, falta de combustível para geradores diesel de emergência, perda de prestações de serviço comuns (alimentações hidráulica e pneumática, condicionamento de ar, instrumentação, resfriamento), incêndios, explosões, projetis ejetados por falhas em componentes rotativos ou pressurizados, interação de sistemas, ou erros no projeto, operação, manutenção ou testes. Devem ser ainda consideradas falhas decorrentes de defeitos de fabricação e construção não detectadas.

Eventos de causa comum externa à IPN incluem agressões provenientes do próprio SNA, similares aqueles de causa interna, e provenientes do ambiente externo ao SNA, tanto de origem natural como derivados de atividades humanas circundantes. Estes últimos foram abordados no princípio que trata dos Fatores Ambientais Externos (subseção 3.3.1). Para uma IPN dotada de mais de um reator, os eventos que poderiam originar-se numa unidade são considerados como eventos inicializadores externos adicionais para as outras unidades.

Devido à importância do fogo como causa comum de falha simultânea de vários componentes, a implementação de sistemas de prevenção e combate a incêndios em SNA reveste-se de excepcional relevância para a segurança. As especificações de projeto devem considerar o emprego extensivo de materiais resistentes ao fogo. Os sistemas hidráulicos e de lubrificação devem usar fluidos não inflamáveis ou serem efetivamente protegidos contra a deflagração de incêndios e protegidos dos efeitos do fogo. A prevenção e combate a incêndios deve empregar os métodos identificados para evitar falhas de causa comum.

Dentre as potenciais agressões de origem externa ao SNA em operação nas áreas de mobilidade e atracado ou fundeado nas localizações fixas pré-definidas, aquela derivada de carregamentos mecânicos impulsivos (choques) sobre o submarino como efeito de explosões submarinas, colisões, encalhes e choque com o fundo requerem particular atenção. A IPN é protegida destes carregamentos através da definição de critérios de projeto mecânico das estruturas compatíveis com a intensidade máxima prevista deste carregamentos para a qual a capacidade de sobrevivência do SNA deve ser garantida e através de calçamento resiliente de componentes e equipamentos internos que amortecia a intensidade destes carregamentos.

Para o SNA em dique seco nas localizações fixas pré-definidas, devem ainda ser considerados efeitos de abalos sísmicos e potenciais problemas ligados a liquefação de solos e deslizamentos de terra. Cuidados especiais devem então ser tomados na seleção da localização do dique seco e no esquema de suporte do SNA quando docado (distribuição e características dos picadeiros). Note-se que os carregamentos mecânicos derivados deste tipo de agressão externa tendem a ser significativamente inferiores àqueles produzidos pelos choques. Ainda para o SNA docado ou atracado em cais para atividades de manutenção, devem ser consideradas no projeto agressões externas decorrentes da queda de cargas pesadas de guindastes sobre o submarino.

3.3.2.8 Qualificação de Equipamentos

Princípio: Os componentes e sistemas de segurança são selecionados dentre aqueles que estão qualificados para as condições que prevaleceriam no ambiente pós-acidental no qual seu funcionamento é requerido. Os efeitos de envelhecimento em funcionamento normal e anormal são considerados no projeto e procedimentos de qualificação.

As condições sob as quais é exigido que um equipamento execute uma função de segurança podem diferir significativamente daquelas para as quais ele está normalmente exposto. Seu desempenho pode ainda ser afetado pelos fenômenos associados ao seu “envelhecimento” (*ageing*) ou pelas condições particulares de serviço requeridas pela operação da Instalação. A identificação das condições ambientais sob as quais equipamento deverá funcionar é parte integrante do desenvolvimento do projeto. Entre estas estão as condições pós-acidentais decorrentes do espectro de acidentes que compõem a base de projeto, incluindo condições extremas de temperatura, pressão,

radiação, vibração, umidade e impactos de jatos fluidos, sendo ainda também considerados os efeitos de agressões externas.

A disponibilidade e confiabilidade exigida deverá ser mantida ao longo de todo o ciclo de vida da Instalação. Cuidados especiais devem ser tomados durante o projeto para identificar e prevenir, através de manutenção planejada, os efeitos de falhas de causa comum e de perda da capacidade de resistir as condições ambientais pós-acidentais adversas decorrentes de fenômenos de envelhecimento. O envelhecimento é considerado no projeto pela definição apropriada de condições ambientais, condições de processo, ciclos de funcionamento, programas de inspeção e testes em serviço, vida útil e substituição programada de componentes críticos.

A qualificação deve ser preferencialmente obtida através de testes de desempenho de protótipos. Isto nem sempre é completamente exequível, particularmente no que tange à resistência à vibração de equipamentos de grande porte e aos efeitos de envelhecimento. Em tais casos, a qualificação deve ser feita com base em análises de engenharia, eventualmente acompanhadas por testes parciais.

3.3.2.9 Inspeção em Serviço dos Equipamento de Segurança

Princípio: As estruturas, componentes, e sistemas importantes para a segurança são projetados e construídos de modo que possam ser inspecionados e testados ao longo de sua vida útil para verificar a continuidade do atendimento de suas especificações.

A demonstração de que as características de segurança de componentes e equipamentos são preservadas ao longo do ciclo de vida da IPN é obtida através das inspeções em serviço. Na fase de projeto devem ser tomadas medidas que permitam um acesso adequado, compatível com a frequência prevista de inspeções em serviço destes componentes e equipamentos, e de ferramentas especiais que facilitem estas atividades. A inspeção em serviço do envelope estanque (barreira de pressão) do Circuito Primário recebe atenção especial devido a sua fundamental importância para a contenção dos materiais radioativos e as severas condições ambientais sob as quais está submetida durante longos períodos de tempo.

A proteção radiológica dos operadores deve também ser cuidadosamente considerada no projeto dos dispositivos especiais e procedimentos para execução das inspeções em serviço dos equipamentos de segurança. Outros sistemas de segurança que

recebem particular atenção no projeto para que sejam asseguradas as possibilidades de sua inspeção em serviço dentro das melhores condições para os operadores incluem caminhos físicos da cabeaço elétrica e de instrumentação, caixas de junção de cabos, penetrações no envelope estanque de contenção, sistemas de resfriamento e lubrificação, e componentes que contêm materiais orgânicos e outros que possam degradar-se com o tempo ou como resultado de sua exposição às radiações ionizantes.

3.3.2.10 Proteção Radiológica no Projeto

Princípio: São incorporados no projeto dispositivos especiais de proteção para reduzir a exposição da tripulação do SNA às radiações ionizantes e para manter as emissões de efluentes radioativos dentro de limites prescritos.

O projeto deverá proporcionar proteção para o pessoal de operação e manutenção contra a radiação direta e a contaminação por materiais radioativos. Cuidados especiais devem ser tomados no projeto de sistemas de processamento de rejeitos radioativos de forma a garantir conservativamente o atendimento aos limites máximos autorizados para liberação de efluentes. O projeto deve garantir que todos os componentes da Instalação que contêm materiais radioativos sejam adequadamente blindados e que estes materiais sejam efetivamente contidos nos envelopes preestabelecidos.

Esta proteção deve ser eficaz tanto em operações rotineiras, como também em circunstâncias menos freqüentes, tais como durante manutenção, reparos e modificações, quando os tipos de atividades são mais variados. O projeto de arranjo físico da Instalação deve considerar os requisitos de proteção radiológica, especialmente no que tange à localização apropriada de componentes e sistemas de Instalação, aproveitando-se ao máximo os efeitos de auto-blindagem, contenção e confinamento de materiais radioativos, acessibilidade, controle de acesso, necessidades por monitoramento e controle dos ambiente acessíveis durante o funcionamento e descontaminação.

Uma atenção especial deve ser dada à seleção de materiais que não se tornem excepcionalmente ativos, com meias-vidas longas, quando submetidos à irradiação por nêutrons, para evitar detalhes de projeto que favoreçam a retenção de materiais ativados em localizações das quais só poderiam ser removidos com dificuldade, e para o uso de

acabamentos superficiais que facilitem a descontaminação. O projeto deve ainda prever facilidades para monitoramento e descontaminação do pessoal e de áreas físicas da Instalação.

Durante a fase de projeto devem ainda ser considerados os aspectos de proteção radiológica aplicados à fase de descomissionamento. Após o fim da vida operacional da Instalação, e da remoção de todo combustível nuclear, quantidades significativas de materiais radioativos permanecerão retidos em componentes, equipamentos e estruturas. Este fato deve ser considerado na seleção de materiais, buscando-se empregar aqueles que terão baixa radioatividade residual na escala de tempo representativa para o descomissionamento e na definição dos acessos, quando devem ser levadas em conta as necessidades do futuro desmantelamento da Instalação.

3.3.2.11 Proteção contra Transientes de Reatividade

Princípio: O reator é projetado com uma margem conservadora de segurança, de forma que eventuais variações bruscas na reatividade do núcleo não induzam acidentes com conseqüências graves.

Um acidente de reatividade seria aquele no qual ocorre, global ou localmente, um aumento brusco na reatividade do núcleo, fazendo com que a potência gerada exceda instantaneamente a capacidade de remoção de calor do Circuito Primário, danificando assim o combustível. Dois tipos de efeitos atuam de forma a contrabalançar um tal aumento na reatividade: o primeiro é a realimentação de reatividade negativa intrínseca aos reatores PWR e o outro é a introdução no núcleo de elementos absorvedores de nêutrons. Ambos tendem a reduzir a reatividade e, conseqüentemente, a geração de potência, sendo entretanto influenciados pela opções de projeto.

Somente os coeficientes de realimentação de reatividade negativos não podem, entretanto, prevenir a ocorrência de todo o espectro de acidentes de reatividade possíveis, mas eles podem ser efetivos em muitos deles, especialmente pelos efeitos de estabilização que produzem. Portanto, o projeto do núcleo do reator normalmente baseia-se nestas características inerentes para auxiliar na prevenção de acidentes de reatividade. Nos casos em que somente as características inerentes não são suficientes, os sistemas de controle e de proteção são projetados para assegurar a máxima confiabilidade no controle da reatividade sob todas as condições operacionais. O

sistema de proteção, que atua através de ações de desligamento automático do reator, é projetado para ter a efetividade e confiabilidade necessárias para a redução instantânea dos aumentos de reatividade induzidas por transientes de potência, prevenindo assim a ocorrência de danos ao núcleo do reator.

A combinação dos efeitos de realimentação intrínsecos, dos sistemas de controle de reatividade e dos sistemas de desligamento automático garantem portanto a proteção do reator com uma margem de segurança satisfatória. Esta garantia da confiabilidade do sistema de desligamento automático deve ser demonstrada analítica e experimentalmente, verificando-se ainda que os efeitos de transientes bruscos de reatividade sejam toleráveis.

Deverá ser ainda verificado que eventos externos, falhas de equipamento ou erros de humano não conduzam, por sua vez, a este tipo de transiente. Adicionalmente, ações de prevenção devem ser tomadas de forma a reduzir a probabilidade de que estes transientes possam ocorrer como resultado de eventos que se originam em outras condições de operação que não a operação normal da Instalação. As ações mais significativas a serem tomadas são aquelas que combinam:

- limitar as taxas de retirada de barras de controle e de segurança, associando estratégias de gerenciamento das barras e sistemas automáticos de controle e de proteção;
- assegurar que a remoção ou inserção de uma única barra de combustível não apresentaria transiente que cause dano significativo ao núcleo do reator
- assegurar que durante o processo de carregamento do núcleo do reator não é possível que a criticalidade seja atingida
- assegurar que a retirada de uma única barra de controle ou segurança qualquer quando o reator encontra-se desligado não tornará o núcleo crítico.

3.3.2.12 Integridade do Núcleo do Reator

Princípio: O núcleo é projetado para ter estabilidade mecânica. Ele é projetado para tolerar variações nos parâmetros operacionais previstos pela base de projeto. O projeto é tal que uma distorção ou movimento do núcleo possível de ocorrer durante um ABP não prejudiquem a efetividade do controle de reatividade ou dos sistemas de desligamento de segurança nem comprometam o resfriamento adequado do combustível.

As varetas de combustível tendem a ser distorcidas e deslocadas em caso de ocorrência de um acentuado gradiente radial de aquecimento ao longo do núcleo de um reator. Se este efeito não é contrabalançado, a distorção do núcleo pode induzir mudanças na reatividade ou inibir a inserção de elementos de controle ou segurança. Em alguns casos, a distorção poderia afetar os diâmetros hidráulicos de canais de escoamento de refrigerante específicos e, conseqüentemente, comprometer o resfriamento do combustível. Desta forma, devem ser tomadas precauções particulares para prevenir efeitos indesejáveis de distorção do núcleo induzidos por carregamentos térmicos, mecânicos e radiação.

As vibrações das varetas de combustível induzidas por efeitos termohidráulicos devem ser evitadas através de restrições mecânicas. Isto previne a flutuação do fluxo neutrônico associado e um excessivo desgaste do encamisamento. Os elementos combustível e outros componentes do núcleo são contidos de forma que mudanças abruptas de posição não podem causar transientes bruscos de reatividade. Deve-se entretanto ter o cuidado de que os vínculos introduzidos não introduzam, por sua parte, novos problemas de segurança.

A análise apoiada por experimentos adequadamente delineados deve verificar que o núcleo é geometricamente estável contra choques, transientes de sistemas e outros carregamentos dinâmicos aos quais poderia ser submetido.

Uma elevada qualidade das varetas de combustível é um requisito de segurança importante. Uma vareta combustível danificada ou distorcida pode potencialmente comprometer o resfriamento e o controle de reatividade.

Além disso, uma falha no encamisamento representa a perda de uma barreira de contenção dos materiais radioativos, comprometendo o princípio de defesa em profundidade. Danos menos severos podem reduzir a capacidade do combustível de resistir a condições acidentais.

Por estas razões, procedimentos especiais de garantia de qualidade no projeto e fabricação do combustível são indispensáveis. A manutenção da integridade do combustível é verificada através do monitoramento do nível de atividade no refrigerante durante a operação.

3.3.2.13 Sistemas de Desligamento Automático

Princípio: Os sistemas que permitem o desligamento automático do reator são projetados para serem independentes dos equipamentos e processos empregados para o controle de potência. Estes sistemas possibilitam uma redução da reatividade rápida e altamente confiável, exclusivamente usada para fins de segurança. A ação de desligamento de segurança está permanentemente disponível sempre que os procedimentos para atingir a criticalidade estejam sendo seguidos intencionalmente e sempre que o reator estiver numa condição em que a criticalidade possa ser atingida acidentalmente.

Os sistemas de desligamento automático de segurança devem ser funcionalmente independentes dos sistemas de controle de reatividade usados para operação normal do reator. Só podem ser usados sensores ou dispositivos comuns se a análise de confiabilidade demonstrar cabalmente que tal procedimento é aceitável. Sob todas as condições consideradas no projeto em que o núcleo está crítico ou poderia ficar crítico, os sistemas de desligamento automático deverão estar ativos, garantindo uma reatividade negativa suficiente para o desligamento seguro, caso este for requerido. A análise da inserção de reatividade é um parâmetro importante em algumas sucessões de acidente, e são exigidas ações de projeto para manter este parâmetro dentro de limites apropriados, definidos pela base de projeto.

Os barramentos elétricos e os circuitos lógicos de atuação dos sistemas de desligamento automático deverão estar segregados dos equipamentos usados para controle de potência normal, de forma que nenhuma interferência entre as demandas do controle e do desligamento automático seja possível. Somente quando o reator encontrar-se em estados de desligamento seguro garantidos, i.e. estados onde existe uma margem excepcionalmente grande de subcriticalidade que são definidos previamente pelo projeto, os sistemas de desligamento automático de segurança poderiam ser temporariamente inabilitados.

Um evento de baixa probabilidade que deve ser analisado é a recusa de um sistema de desligamento automático atuar quando for solicitado. Um tal cenário dependerá fortemente das características particulares de cada instalação e das circunstâncias específicas que conduzem ao sinal de desligamento automático. Suas consequências poderiam ser um aumento excessivo na reatividade, na pressão do Circuito Primário, nas temperaturas do combustível ou em alguma outra causa potencial

de dano à Instalação. O projeto deve portanto garantir que estes cenários, denominados Transientes Antecipados Sem Desligamento TASD (*Anticipated Transients Without Scram* ATWS), não contribuam de modo excessivo para o Risco Objetivo Residual da Instalação. Isto é obtido fazendo-se com que a probabilidade de ocorrência de tais acidentes seja suficientemente baixa ou garantindo que eles não conduzirão a danos severos ao núcleo. A prevenção destes acidentes ou a limitação dos seus efeitos assegura que o objetivo de segurança é atingido mesmo no caso de falha do sistema de proteção do reator.

A análise dos TASD é de particular relevância para as IPN. Eles estão associados a eventuais conflitos entre o Objetivo de Seguridade e o Objetivo de Disponibilidade apresentados pela seção 3.1. Durante a operação de um SNA, podem ocorrer situações em que seja requerido à IPN transientes bruscos de potência com o objetivo de evitar situações de elevado risco iminente, tais como colisão, encalhe, naufrágio, ataques por armamento inimigo. Nestas situações, o desligamento automático da IPN poderá conduzir a consequências mais severas para o submarino, sua tripulação, o ambiente e o público do que aquelas que seriam incorridas, em termos de danos ao reator, caso o mesmo continuasse operando. A análise detalhada dos TASD permitirá conhecer os limites últimos da IPN, permitindo ao Comandante do submarino tomar as necessárias decisões de compromisso em tempo real, considerando as reais gravidades dos riscos envolvidos.

3.3.2.14 Remoção de Calor Normal

Princípio: Os sistemas de resfriamento do reator são projetados com alta confiabilidade para remover o calor gerado pelo núcleo durante a operação em potência e em condições de desligamento normal. Eles também proporcionam meios para a remoção de calor do núcleo do reator durante ocorrências operacionais antecipadas e durante os acidentes nos quais a integridade do Circuito Primário é mantida.

O Sistema de Resfriamento do Reator (Circuito Primário) é o meio principal de remoção de calor do núcleo em condições normais de operação. É também o meio preferencial para remoção de calor residual após o desligamento voluntário ou após o desligamento devido a uma ocorrência anormal e em acidentes onde o envelope estanque do Circuito Primário permanece intacto.

Para a remoção de calor residual a longo prazo, quando a potência gerada pelo decaimento radioativo dos materiais do núcleo atinge valores pequenos, podem ser considerados outros sistemas específicos para esta condição, não necessariamente relacionado com a segurança, mas usados em operações normais de reator, que podem alternativamente executar a função importante para a segurança de remoção de calor residual. Sua disponibilidade para emprego neste caso reforça o princípio de defesa em profundidade.

3.3.2.15 Remoção de Calor em Emergência

Princípio: O projeto prevê meios alternativos para restabelecer e manter o resfriamento do combustível sob condições de acidente nas quais os sistemas de remoção de calor normal falhem ou que a integridade do envelope estanque do Circuito primário seja perdida.

Certas condições anormais poderiam prejudicar a capacidade de remoção de calor de todos os sistemas ativos de resfriamento do reator empregados em condições normais. Nos reatores PWR de propulsão naval, devido ao seu arranjo compacto, a circulação natural é em geral suficiente para garantir a continuidade da remoção de calor de decaimento nestas circunstâncias, contanto que o envelope estanque do circuito primário permaneça intacto e que seja mantida, pelo menos em parte, a capacidade para remoção de calor do Circuito Secundário. Para os casos em que estas duas condições não são atendidas, torna-se necessário sistemas de resfriamento do reator em emergência para evitar danos severos ao núcleo. Este sistemas incluem sistemas de injeção de refrigerante, nos casos em que haja perda de água de resfriamento, i.e. Acidentes de Perda de Refrigerante Primário APRP (*Loss of Coolant Accidents* LOCA), sistemas para remoção do calor residual independentes daqueles existentes para condições normais, e sistemas de água de alimentação de emergência dos GV, para assegurar a capacidade de remoção de calor no Circuito Secundário.

O projeto de reatores PWR, desde suas origens, sempre deu uma relevante importância à obtenção da máxima confiabilidade no desempenho da função de segurança de remoção do calor residual do núcleo após desligamento, pois considera-se que a perda desta função tem uma contribuição significativa para o Risco Objetivo Residual destas instalações. A busca desta máxima confiabilidade tem levado ao desenvolvimento de sistemas injeção passivos, baseados em diferenciais de pressão

estabelecidos naturalmente, e de resfriamento também passivo, baseados nos fenômenos de circulação natural, considerados *a priori* como mais seguros do que os sistemas ativos, baseados na injeção a partir de reservatórios pressurizados externamente e de circulação forçada através de bombas, também alimentadas externamente. O pequeno porte dos reatores de propulsão naval (comparado com os reatores para geração de energia elétrica) facilita a implementação destes sistemas passivos e estas possibilidades devem ser exploradas para aperfeiçoar a segurança das IPN.

3.3.2.16 Integridade do Sistema de Resfriamento do Reator

Princípio: Os códigos e normas para projeto e fabricação de vasos de pressão e tubulações industriais são complementados para emprego nuclear por margens de segurança, procedimentos de Garantia da Qualidade e inspeções em serviço adicionais, com o objetivo de prevenir, com alta confiabilidade, a ocorrência de condições que possam conduzir a rupturas do envelope estanque do Circuito Primário durante a vida operacional da IPN.

A integridade da barreira de pressão do envelope estanque do Circuito Primário é uma função de segurança crítica, pois sua falha pode conduzir, simultaneamente, à perda da função básica de resfriamento adequado do combustível e, em casos extremos, à perda da função básica de contenção de materiais radioativo. Esta integridade é particularmente importante para os grandes componentes, tais como o VPR, GV, PZ e BCR, onde uma falha catastrófica provocaria um acidente cujas conseqüências severas seriam praticamente impossíveis de controlar.

Para todos os componentes que formam parte da barreira de pressão do Circuito primário, particularmente o VPR, uma cuidadosa atenção deve ser dada ao projeto, seleção de materiais, fabricação, instalação, inspeção e testes, com ênfase particular no emprego de normas bem estabelecidas e fornecedores experientes, e procedimentos detalhados para obtenção da máxima qualidade. A análise de tensões deve demonstrar que as estruturas podem resistir aos carregamento mais extremos que possam vir a ser impostos em condições normais e acidentais.

As matérias-primas devem ser devidamente certificadas e os procedimentos de fabricação devidamente qualificados antes do início da construção. Múltiplas inspeções devem ser realizadas durante e após a construção e montagem dos componentes da barreira de pressão, usando-se métodos não-destrutivos e ensaios destrutivos em

amostras de produção, feitas com os mesmos materiais e procedimentos de soldagem empregados na fabricação. O teste hidrostático a pressões significativamente superiores às condições operacionais normais, anormais e acidentais confirma a resistência do sistema montado antes do carregamento do combustível nuclear.

A análise de resistência das partes metálicas da barreira de pressão está baseada na hipótese que, durante a construção e montagem, podem ter sido introduzidos pequenos defeitos que permanecem não detectados pelas inspeções devido ao seu tamanho. Tal análise mostra que o projeto, as limitações operacionais e as inspeções periódicas proporcionam uma garantia, com ampla margem de segurança ao longo de todo o ciclo de vida da Instalação, que os defeitos não detectados não se desenvolveriam até um tamanho que seria crítico sob as máximas tensões que poderiam ocorrer em condições normais e acidentais.

Os riscos à integridade do envelope estanque do Circuito Primário devem ser prevenidos assegurando-se uma adequada proteção contra sobrepressão, através de sistemas de alívio. Para os vasos de pressão em materiais ferríticos, qualquer combinação de pressão e baixa temperatura que poderiam causar uma ruptura frágil (inclusive combinações que poderiam ser encontradas em ABP) deve ser evitada. Devem ainda ser levados em consideração os mecanismos de deterioração da integridade da barreira de pressão no projeto da Instalação, incluindo fadiga, corrosão sob tensão e efeitos de fragilização pela irradiação e pelo hidrogênio.

Durante a vida útil da Instalação, a continuidade da integridade da barreira de pressão é verificada por inspeções, análises, e ensaios de amostras expostas às radiações de material testemunho dos processos de fabricação, pelo monitoramento de vazamentos com sistemas especialmente projetados para este propósito, e fazendo-se qualquer reparo ou substituições que se demonstrarem necessários. Acessos fáceis, que permitam inspeções freqüentes, devem ser previstos pelo projeto.

Devem ser evitadas soldas em regiões nas quais o nível do fluxo de nêutrons é muito elevado. Os aços e consumíveis de soldagem (eletrodos, fluxos, gases) devem ter um conteúdo muito baixo de elementos que acelerem os efeitos de deterioração induzido pela radiação, especialmente cobre e fósforo. Os aços empregados devem ter alta soldabilidade e, juntamente com suas soldas, ter uma baixa suscetibilidade a

fraturas sob todas as temperaturas na região operacional. O VPR deverá ter diâmetro suficientemente grande para assegurar uma significativa atenuação do fluxo de nêutrons entre o núcleo e sua superfície interna.

3.3.2.17 Contenção e Confinamento de Materiais Radioativos

Princípio: A IPN é projetada para ser capaz de conter e confinar os materiais radioativos que poderiam ser liberados pelo combustível em todo o espectro de acidentes considerados pela base de projeto.

São requeridos dispositivos especiais para conter e confinar os materiais radioativos que poderiam ser liberados como resultado de um acidente, a menos que seja demonstrado que uma proteção adequada contra tal liberação é garantida por outros meios. Deve-se notar que, considerando-se o grande inventário de gases nobres radioativos, nenhum sistema disponível atualmente poderia confinar todos os materiais radioativos passíveis de serem liberados pelos ABP. Os sistemas especiais têm porém a função de prevenir vazamentos dos materiais radioativos mais significativos sob o ponto de vista do impacto radiológico. Estes sistemas que proporcionam a função de contenção têm as características comuns identificadas a seguir:

- Uma estrutura estanque envolve a região dentro da qual os materiais radioativos, principalmente os produtos de fissão, poderiam ser liberados no caso de perda de integridade do combustível.
- O confinamento pode ser obtido fazendo uma estrutura suficientemente resistente para que, quando hermeticamente isolada, possa resistir à pressão interna máxima decorrente dos ABP. Uma tal estrutura é chamada então de Contenção. A estrutura de Contenção normalmente possui um subsistema que garante seu isolamento, assim como outros subsistemas que monitoram suas condições e proporcionam proteção contra fenômenos que possam ameaçar sua integridade. Juntamente com a estrutura propriamente dita, estes subsistemas constituem o sistema de contenção.
- O confinamento pode ser obtido dotando a estrutura com dispositivos que permitam que a pressão decorrente de um acidente seja aliviada para o exterior, assegurando entretanto que a maior parte dos materiais radioativos liberados pelo combustível seja contida.
- A estrutura mantém sua integridade tanto no curto como no longo prazo sob as condições de pressão e temperatura que poderiam prevalecer durante os ABP.

- Aberturas e penetrações, quando fechadas, assim como outros pontos singulares na estrutura, são projetados para atender aos mesmos requisitos da estrutura de forma que não constituam pontos vulneráveis e, conseqüentemente, rotas potenciais para a liberação de materiais radioativos.
- Se a análise demonstrar que o calor residual do reator poderia conduzir a um aumento de temperatura interna da contenção, podendo assim gerar uma pressão que poderia ameaçar a integridade da estrutura, devem ser previstos meios para sua remoção.

Deve ser demonstrado que a capacidade de confinamento é tal que os objetivos da base de projeto quanto à limitação de vazamentos de materiais radioativos são atingidos. O projeto deverá então prever meios de testes para demonstração funcional dos objetivos de projeto.

O projeto deve identificar as potenciais rotas de contorno do confinamento em caso de acidentes e tomar medidas eficazes de forma a prevenir a liberação direta para o ambiente de materiais radioativos através destas rotas alternativas.

3.3.2.18 Proteção da Estrutura de Contenção

Princípio: Se não pode ser garantido que a estrutura de contenção mantém sua integridade no caso de acidentes severos além dos ABP, dispositivos especiais de mitigação de conseqüências contra os efeitos de tais acidentes são implementados para atender ao objetivo geral de segurança.

Este princípio refere-se particularmente a uma estrutura de confinamento concebida como uma estrutura de contenção, conforme discutido no princípio anterior. Uma estrutura de contenção é projetada para resistir a pressão interna máxima esperada como resultado do ABP para esta estrutura, usando-se fatores de segurança significativos. Análises complementares indicam que, em casos extremos, acidentes severos além da base de projeto poderiam gerar pressões superiores à pressão de projeto para a estrutura de contenção. Entretanto, estes valores mais altos são, na maioria dos casos, inferiores aos limites máximos de resistência da estrutura, excluindo-se as margens de projeto.

Se cenários acidentais severos puderem conduzir a pressões que causam tensões que excedam os limites máximos de resistência calculados para a estrutura de

contenção, esta poderá falhar. Em caso de falha catastrófica precoce, uma liberação significativa de materiais radioativos poderia acontecer, requerendo medidas emergenciais externas de proteção. Tais circunstâncias poderiam gerar uma contribuição apreciável para o Risco Objetivo Residual da Instalação.

Se esta contribuição para o Risco Objetivo Residual for tão grande que gere um conflito com os objetivos gerais de segurança, devem ser tomadas medidas especiais para proteger a estrutura de contenção. Algumas soluções de engenharia têm sido propostas e aplicadas em casos específicos, tais como queimadores do hidrogênio contido na atmosfera interna da Contenção, sistemas de alívio de pressão da Contenção através de filtros, sistemas de aspersão de refrigerante no interior da Contenção e recuperadores resfriadores do *corium*.

Considerações similares são aplicáveis a estruturas de confinamento não projetadas para suportar altas pressões internas.

3.3.2.19 Monitoramento do Estado da Instalação

Princípio: Os parâmetros importantes para a segurança a serem monitorados na Estação de Controle de Máquinas são selecionados, e sua apresentação é organizada de forma a assegurar que os operadores tenham indicações claras e sem ambigüidades do estado da IPN, especialmente com a finalidade de identificar e diagnosticar as ações automáticas, a operação dos sistemas de segurança e degradações na defesa em profundidade.

O contínuo conhecimento e entendimento do estado da Instalação por parte dos operadores é um componente vital da defesa em profundidade. A Estação de Controle de Máquinas ECM do SNA deve ser provida de informações logicamente organizadas sobre as variáveis de processo da Instalação para averiguar seu estado de funcionamento normal, identificar e diagnosticar condições anormais, e observar o efeito de resposta das ações corretivas de controle e dos sistemas de segurança. As informações sobre eventos inicializadores internos e externos devem ser também apresentadas na ECM. O alarme antecipado de potenciais problemas em desenvolvimento deve ser garantido e incluído o monitoramento de sistemas individuais, monitoramento de vibrações ou ruídos incomuns e excessivos, e sistemas para detecção de vazamentos ou de níveis incomuns de radiação, temperatura ou umidade.

Os recursos para transmissão e exibição das informações incluem medidores, indicadores de estado, indicadores de tendências de parâmetros, alarmes priorizados e diversos auxílios informatizados ao diagnóstico, assim como também canais de comunicações interiores confiáveis entre os operadores da ECM e eventuais operadores locais ou pessoal de manutenção. Um cuidado especial deve ser tomado pelo projeto no sentido de assegurar que os operadores têm os meios necessários para monitorar a informação mais útil e importante, e evitando distrações que podem advir de informações periféricas. Operadores experimentados, assim como especialistas em fatores humanos constituem precioso auxílio aos projetistas para identificação, apresentação e organização apropriada dos dados necessários a uma operação segura.

3.3.2.20 Preservação da Capacidade de Controle

Princípio: A Estação de Controle de Máquinas é projetada para permanecer habitável sob as condições operacionais normais, ocorrências anormais antecipadas e acidentes considerados na base de projeto. Uma Estação de Controle de Máquinas alternativa é disponível, dotada de monitoramento independente e capacidades essenciais de controle necessárias para resfriar o núcleo, desligar o reator e isolar a contenção em condições acidentais nas quais a estação principal for avariada, tornar-se inabitável ou inacessível.

O ambiente da ECM deve ser protegido contra condições anormais que poderiam comprometer a efetividade dos operadores ou poderiam afetar sua saúde. Tais condições poderiam decorrer de eventos internos ou externos à IPN. No caso em que o ambiente da ECM for degradado por qualquer razão, os operadores devem ser alertados imediatamente por um sistema específico de monitoramento e devem estar disponíveis equipamentos de proteção individual adequados.

Podem ainda ocorrer situações, particularmente decorrentes de eventos externos à IPN, nas quais a ECM principal poderia ficar inabitável ou poderia ser avariada num tal nível em que se tornaria inutilizável. Devem então ser providos meios alternativos para assegurar a continuidade da operação segura da IPN nestas situações. Pelo menos uma ECM secundária deve então ser prevista pelo projeto, equipada com os controles necessários que permitam aos operadores dar continuidade à operação da IPN de forma a assegurar no mínimo o atendimento às funções básicas de segurança: controle de

reatividade e desligamento de reator, remoção de calor residual e contenção dos materiais radioativos até o SNA retornar a uma localização fixa segura.

O operação da IPN pode requerer eventualmente ações de controle e monitoramento locais que alteram as características de desempenho de sistemas, tais como fechamento e abertura de válvulas. Onde ações de controle e monitoramento local associadas são previstas em localizações diferentes, um sistema de comunicações interna confiável entre estes pontos deve estar disponível.

3.3.2.21 Perda Total das Alimentações Elétricas

Princípio: A IPN é projetada de forma que a perda total das alimentações elétricas normal e de emergência não implique, a curto prazo, em danos ao combustível. A IPN é ainda dotada de sistemas alternativos de alimentação elétrica de forma que, em caso de avarias graves no SNA, a alimentação dos equipamentos vitais às funções básicas de segurança seja restabelecida em tempos razoáveis, evitando danos ao combustível a médio e longo prazo.

A continuidade nas alimentações elétricas é vital para a segurança da IPN. Sua confiabilidade e disponibilidade é diretamente proporcional à segurança da Instalação. Os sistemas elétricos de serviço normais e de emergência são projetados com redundâncias de modo a garantir uma alta disponibilidade. As potenciais falhas em modo comum destas redundâncias devem ser cuidadosamente identificadas, e medidas para sua prevenção devem ser implementadas, tanto no projeto, por meio da diversidade e segregação dos componentes destes sistemas (turbo-geradores, moto-geradores, diesel-geradores, baterias de acumuladores), como nos procedimentos operacionais e de manutenção.

Em particular, a IPN deve ser projetada para resistir, simultaneamente e sem comprometimento das funções de segurança, à perda total das alimentações elétricas normais e à indisponibilidade temporária das alimentações de emergência por um período especificado de tempo. A duração mínima deste período de tempo é função do projeto de cada Instalação em particular, devendo entretanto ser significativamente maior que os tempos máximos estimados para o restabelecimento de pelo menos um dos sistemas de alimentação de emergência.

As características de resfriamento normal e de emergência do reator por circulação natural, intrínsecas ao projeto da IPN desempenham um papel fundamental

na duração deste período de tempo. Procedimentos operacionais especialmente adaptados a esta condição devem ser desenvolvidos e testados para maximização desta capacidade.

3.3.2.22 Controle dos Acidentes Básicos de Projeto

Princípio: Durante a fase de projeto são implementados meios para o controle dos acidentes dentro da base de projeto, incluindo a especificação da instrumentação associada, necessária para que os operadores da IPN acompanhem a evolução dos cenários acidentais e possam intervir para preservação das funções de segurança nuclear.

Os operadores da IPN são auxiliados por equipamentos de segurança, instrumentação e procedimentos operacionais apropriados para terem uma resposta adequada durante a ocorrência de cenários acidentais dentro da base de projeto, de forma a exercer sobre eles um controle eficaz. O projeto deve garantir primeiramente que eventuais evoluções anormais sejam reconhecidas em modo automático, e que a restauração das condições normais seja obtida por meio das características de realimentação neutrônicas intrínsecas e pelos controles de processo. Estes controles são secundados pelas capacidades normais de desligamento, resfriamento contínuo do combustível e contenção de materiais radioativos. A proteção adicional é garantida pelos sistemas de segurança implantados, que devem estar disponíveis para atuação automática.

Por meio destes dois níveis de defesa, qualquer evolução anormal do comportamento da Instalação seria interrompida automaticamente através de sistemas adequadamente projetados, pelo menos por um período de tempo razoável, estabelecido *a priori*, durante o qual os operadores poderiam avaliar os sistemas, analisar linhas de ação alternativas e decidir corretamente pelas ações subseqüentes, para as condições nas quais as ações automáticas não tenham respondido da melhor maneira possível. Neste sentido, o operador funciona como um nível de defesa adicional. Para maximizar a probabilidade de acerto nas decisões dos operadores, o projeto deve prever auxílios informatizados ao diagnóstico e procedimentos de emergência baseados no estado atual da Instalação para uso nestas circunstâncias. Os intervalos de decisão típicos para que o operador tome uma decisão e execute uma ação positiva é de 10 a 30 minutos ou, dependendo da situação, períodos ainda maiores.

O papel do operador nestas circunstâncias seria de assegurar que todos os sistemas responderam corretamente à situação anormal, diagnosticar o evento inicializador desta situação em tempo hábil e intervir, se for preciso, para restabelecer as funções básicas de segurança. Uma instrumentação adequada e meios de apresentação clara das variáveis monitoradas constituem auxílios fundamentais para o eficaz desempenho destas tarefas, explicitando os parâmetros críticos para a segurança e simulando os resultados das diversas alternativas de ação passíveis de serem tomadas.

3.3.3 FABRICAÇÃO E CONSTRUÇÃO

A primeira exigência de segurança é que componentes, sistemas e estruturas sejam fabricados e que a IPN seja construída de acordo com as especificações de projeto. Esta exigência é atendida mantendo-se rígida supervisão sobre um amplo espectro de atividades, desde a responsabilidade das organizações envolvidas até a motivação e competência técnico-profissional dos executores individuais.

3.3.3.1 Avaliação da Segurança do Projeto

Princípio: A construção de uma IPN somente é iniciada após tanto a organização operadora como a ASN estarem plenamente convencidas, por meio de análises apropriadas, de que os problemas principais de segurança da instalação foram satisfatoriamente resolvidos e que a solução dos eventuais problemas remanescentes é viável de ser obtida antes da operação inicial, tendo as atividades requeridas para isto sido planejadas e efetivamente iniciadas.

As opções disponíveis aos projetistas para modificar características de segurança da Instalação vão rapidamente sendo restringidas conforme a fabricação e a construção evoluem. Por isto torna-se necessário coordenar a avaliação de segurança com a fabricação e a construção de modo a assegurar que as opções de projeto mais significativas para a segurança foram otimizadas e que as decisões de licenciamento sejam tomadas oportunamente.

De uma maneira geral, ao final de cada fase de projeto da IPN (estudos de exeqüibilidade, projeto de concepção, projeto básico ou preliminar, projeto de detalhamento para construção) deverá ser executada uma análise de segurança com grau de detalhamento compatível com o desenvolvimento do processo de obtenção do SNA. Esta análise global é revisada pela ASN para assegurar que as exigências da regulamentação foram ou serão atendidas, e que o Risco Objetivo Residual da

Instalação encontra-se a um nível socialmente aceitável. As licenças e autorizações administrativas emitidas pela ASN com base nesta revisão poderão ser condicionadas à solução de problemas específicos durante a construção, porém antes do início da operação. Controles adicionais podem ainda ser estabelecidos durante a construção, de forma que o projeto final, a instalação e a verificação da adequação dos equipamentos importantes para a segurança possa ser revisada de modo satisfatório.

3.3.3.2 Obtenção da Qualidade

Princípio: Os fabricantes de componentes, sistemas e estruturas e os construtores da Instalação assumem a responsabilidade pela alta qualidade de seus produtos usando técnicas bem estabelecidas e procedimentos executivos validados, apoiados por um Sistema de Garantia da Qualidade eficaz.

A fabricação de componentes, sistemas e estruturas, assim como a construção da Instalação de acordo com as especificações é uma responsabilidade imediata dos fornecedores contratados pela organização operadora da IPN. O sucesso nestas atividades dependerá da efetividade das técnicas e procedimentos adotados e a maneira pela qual eles são efetivamente praticados. A fabricação e a construção são feitas com base em especificações detalhadas para materiais, processos, produtos, e métodos de testes e inspeções. Os fabricantes de componentes, sistemas e estruturas devem ser escolhidos dentre aqueles que demonstraram previamente suas capacidades em satisfazer as exigências especiais e precisas de uma IPN, que são frequentemente específicos à indústria nuclear e que estão baseados em códigos e normas que contêm critérios de aceitação para os produtos finais. Os fornecedores de componentes, sistemas e estruturas importantes para a segurança tem frequentemente sua competência verificada e certificada por Órgãos de Supervisão Técnica Independente OSTI, reconhecidos pela ASN.

O fabricante estabelece procedimentos para controle de processos e de documentação, identificação e controle de materiais e componentes, planejamento de inspeções e testes, manutenção de registros, pontos intermediários de verificação de processos e procedimentos corretivo para não-conformidades, todos sujeitos a uma hierarquia de práticas de Garantia da Qualidade. O fabricante é o responsável pelo desenvolvimento e validação de suas técnicas e procedimentos de fabricação, assim

como de seus métodos de controle de qualidade, treinamento de pessoal e por prover condições de trabalho satisfatórias.

Embora o fabricante tenha a responsabilidade imediata pela qualidade de seus produtos, é sob a organização operadora que recai a responsabilidade geral pela segurança da Instalação. Esta responsabilidade é exercida através de auditorias e inspeções nos fornecedores com o objetivo de verificar suas técnicas, procedimentos, documentação e práticas efetivas, incluindo a Garantia da Qualidade e a organização gerencial, realizadas pela própria organização operadora ou por outras organizações que agem como seus prepostos. Para os itens importantes para a segurança, os procedimentos e resultados destas auditorias e inspeções devem estar disponíveis para revisão pela ASN.

3.3.4 COMISSIONAMENTO

É necessário demonstrar que a IPN foi satisfatoriamente construída e montada, estando efetiva e seguramente pronta para serviço antes de sua operação inicial. Para este propósito, um programa de comissionamento corretamente planejado e documentado deve ser elaborado e executado. Os futuros operadores participam ativamente desta fase. Os sistemas da Instalação são progressivamente entregues aos operadores conforme as montagens e testes vão sendo concluídos.

Até que o programa de comissionamento atinja a fase de carregamento do combustível, todos os itens importantes para a segurança devem ter sido entregues aos operadores. Em alguns casos este processo pode ter uma fase intermediária na qual outra organização administra as operações de comissionamento, atuando efetivamente como um agente do futuro operador da Instalação.

3.3.4.1 Verificação da Segurança do Projeto e da Construção

Princípio: O programa de comissionamento é estabelecido e seguido para demonstrar que a Instalação integrada, especialmente os itens importantes para a segurança e proteção radiológica, foi construída e encontra-se funcionando de acordo com as especificações de projeto, assegurando que eventuais desvios são identificados e corrigidos.

Para assegurar que as especificações de projeto foram atendidas, o programa de comissionamento inclui verificações funcionais dos itens de segurança e dos dispositivos para proteção radiológica. O programa de comissionamento e seus

resultados estão sujeitos a acompanhamento e revisão pela ASN. Algumas fases do comissionamento têm lugar ainda durante a construção e montagem. São testados componentes de sistemas; assim como os sistemas completos. São avaliadas eventuais não-conformidades com as especificações de projeto identificadas durante estas verificações, que são corrigidas e documentadas à organização operadora de forma que qualquer efeito que possam vir a ter sobre a operação de Instalação seja considerado. Onde não podem ser realizados testes completos de componentes e sistemas sob condições de operação realistas, são executados testes combinados sob condições tão realistas quanto possível.

O comissionamento continua com o carregamento do combustível, primeira criticalidade e subida de potência. Os resultados do comissionamento estão sujeitos a revisão final pela ASN. Eles também devem ser empregados pelos projetistas para aperfeiçoar o projeto de instalações futuras.

3.3.4.2 Testes Funcionais e Validação de Procedimentos Operacionais

Princípio: Os procedimentos para operação normal da IPN e de seus sistemas individuais e para os testes funcionais a serem executados durante a fase operacional são validados como parte do programa de comissionamento.

Os procedimentos a serem seguidos durante a fase operacional são elaborados antes e durante o comissionamento com base nas informações fornecidas pelos projetistas e fabricantes. A fase de comissionamento deve portanto ser aproveitada para testar e atualizar estes procedimentos operacionais para a Instalação e seus sistemas, confirmando os métodos que serão usados depois para os testes funcionais dos equipamentos, em especial aqueles importantes para a segurança. Esta atividade também proporciona aos operadores formação básica e treinamento, familiarizando-os com as localizações, respostas, peculiaridades e interações dos sistemas. Esta é uma das principais razões do envolvimento dos futuros operadores da Instalação já na fase inicial do comissionamento.

3.3.4.3 Coleta de Dados Básicos

Princípio: Durante os testes de comissionamento são coletados e registrados dados detalhados de componentes importantes para a segurança e parâmetros operacionais iniciais dos sistemas.

Durante o comissionamento e operação inicial são coletados e registrados dados básicos sobre o funcionamento de componentes e sistemas que serão utilizados como referência para o monitoramento futuro permitir a detecção de degradações incipientes. Incluídas neste processo, encontram-se as inspeções e testes do VPR e demais componentes da barreira de pressão do Circuito Primário. Como regra geral, durante o comissionamento são coletados dados básico sobre todos os parâmetros relacionados à segurança que serão monitorados rotineiramente durante a operação.

3.3.4.4 Ajustes Pré-Operacionais da Instalação

Princípio: Durante o programa de comissionamento, as características operacionais de sistemas de segurança e processo “tais como construídos”(as built) são determinadas e documentadas. Os pontos operacionais são ajustados nos valores de projeto utilizados para as análises de segurança. Os procedimentos de treinamento e as condições limitantes para a operação são modificados para refletir precisamente as características operacionais reais dos sistemas.

Os sistemas de segurança e de processo são testados e calibrados durante o período pré-operacional de comissionamento. As informações obtidas indicam onde são necessários ajustes para assegurar que a Instalação, a análise de segurança, o treinamento de operadores e os procedimentos operacionais estão coerentes, i.e. estabelecidos numa base única. Deste modo, a Instalação irá funcionar conforme desejado quando for iniciada sua operação permanente.

3.3.5 OPERAÇÃO

A organização operadora é responsável pelo fornecimento de todo o equipamento, pessoal, procedimentos e meios de gerenciamento necessários para a operação segura da IPN, inclusive a desenvolvimento de um ambiente de trabalho no qual a segurança é percebida como um fator vital, sendo um tema de responsabilidade individual do pessoal envolvido.

Pode parecer à primeira vista, que esta ênfase na segurança poderia entrar em conflito com as exigências funcionais de garantia do sucesso da missão do SNA, entendida aqui no seu sentido mais amplo. Este conflito é, entretanto, mais aparente do que real, à medida em que os fatores de projeto, construção e gerenciamento operacional que promovem a seguridade coincidem com aqueles que contribuem para a disponibilidade e confiabilidade no cumprimento da missão. A disponibilidade e

confiabilidade a longo prazo não poderá nunca ser obtida através de comprometimentos da seguridade a curto prazo.

3.3.5.1 Organização e Responsabilidades

Princípio: A organização operadora assume plena responsabilidade pela operação segura da IPN através de uma estrutura organizacional adaptada às especificidades da propulsão nuclear, sob a autoridade do Comandante do SNA. O Comandante assegura que todos os meios necessários à operação segura da IPN estão disponíveis, inclusive um número adequado de operadores qualificados e experientes.

A responsabilidade cotidiana pela segurança de IPN reside no Comandante do SNA, que assegura que os meios necessários para alcançá-la estão disponíveis e que as necessidades de segurança determinam as operações na Instalação. Ele é apoiado pela estrutura administrativa e pelo mais alto nível da organização operadora, que proporciona adequado suporte financeiro, técnico, material e de pessoal para a operação. As responsabilidades para com a segurança de todos os níveis hierárquicos e funções administrativas, gerenciais e executivas envolvidos são claramente definidas pelos procedimentos e instruções normativas da organização operadora.

Um número suficiente de operadores qualificados deve ser empregado para o desempenho de todas as atividades normais de operação da IPN, sem tensões ou atrasos impróprios, inclusive a supervisão das atividades executadas por contratados externos durante períodos de carga de trabalho excepcional, tais como os períodos de manutenção e reparos. Os procedimentos e especificações de tarefas devem considerar o pessoal necessário para sua execução, definindo claramente as qualificações requeridas e a linha sucessória para as posições-chave, levando-se em consideração as dificuldades e o tempo requerido para retreinamento.

Os requisitos de pessoal para ocorrências operacionais anormais são analisados de forma a assegurar a capacidade de desempenhar qualquer tarefa especializada necessária, tais como gerenciamento de acidentes, análise e controle de avarias, combate a incêndios, busca e salvamento, primeiros socorros, monitoramento externo e comunicações. Estes requisitos de pessoal levam em conta os dispositivos de emergência disponíveis no SNA.

3.3.5.2 Procedimentos de Revisão de Segurança

Princípio: A organização operadora mantém procedimentos de revisão de segurança para garantir a vigilância e auditoria contínua da segurança operacional da IPN, dando suporte ao Comandante do SNA no exercício de suas responsabilidades pela segurança global do submarino.

Os procedimentos de gerenciamento da segurança devem cobrir todos os aspectos rotineiros da operação do SNA. Sob a forma de relatórios padronizados, os resultados da execução destes procedimentos devem ser sistematicamente apresentados ao Comandante do SNA, à sua cadeia de comando e às organizações de apoio em terra. Além disto, a organização operadora deve dispor de meios para revisão independente da segurança, por meios próprios ou através de OSTI devidamente certificado pela ASN.

O objetivo principal destas revisões de segurança é assegurar que, nos aspectos de operação importantes para a segurança, o Comandante do SNA terá apoio técnico de organismos independentes de eventuais pressões externas pela continuidade da operação do submarino, que muito provavelmente advirão da cadeia de comando. As atividades de revisão independente são executadas de forma separada da operação da IPN, sendo realizadas de uma forma contínua para verificar que o gerenciamento da Instalação é realizado corretamente de acordo com as especificações. Os relatórios destas atividades são formais e são transmitidos diretamente à administração superior da organização operadora. Uma particular atenção deve ser dada neste processo ao retorno da experiência operacional, incluindo:

- análise de eventos anormais e deficiências da Instalação identificadas tanto localmente como em Instalações semelhantes;
- revisões de eficiência e eventuais modificações dos procedimentos operacionais;
- modificações da Instalação que afetem a segurança;
- adequação da qualificação e treinamento dos operadores;
- efetivo atendimento dos requisitos regulamentares da ASN;
- atitudes gerais do gerenciamento da operação e dos operadores com respeito à segurança da Instalação.

Particularmente, em assuntos específicos de especial relevância para a segurança da Instalação, tais como manobras intencionais não usuais, testes ou experimentos não rotineiros, alterações nas condições ou limites de segurança, devem ser formulados

procedimentos especiais pelos operadores, que deverão então sofrer uma revisão independente. Somente após esta revisão a ASN aprovará sua execução.

3.3.5.3 Condução da Operação

Princípio: A operação da IPN é conduzida por pessoal devidamente autorizado, de acordo com controles administrativos rígidos e observando-se rigorosa disciplina no cumprimento dos procedimentos operacionais aprovados.

A Instalação só é operada adequadamente por pessoal qualificado e treinado, que permanentemente demonstra nas suas atividades a incorporação de uma verdadeira Cultura de Segurança. Tais operadores devem ter plena ciência do significado de suas atividades para a segurança e das conseqüências de eventuais erros. A operação da Instalação será feita em um ambiente condizente com a segurança, com alto nível de disciplina dos operadores, a inexistência de padrões de conduta impróprios e máxima concentração nas tarefas realizadas.

Os operadores de serviço devem monitorar continuamente o estado da Instalação para confirmar que componentes e sistemas estão executando satisfatoriamente suas funções ou estão em um apropriado estado de disponibilidade para o funcionamento. Eles devem assegurar que eventuais deficiências de Instalação e desvios das condições ou configurações da Instalação exigidas pelos procedimentos são identificados em tempo hábil para implementação de ações corretivas convenientes. Os alarmes de advertência devem ser investigados e as ações corretivas tomadas nos tempos prescritos. Eventuais fenômenos incomum, tais como ruídos ou mudanças aparentes nos processos ou no desempenho de sistemas devem ser investigados e ações apropriadas devem ser tomadas se houver risco para componentes vitais ou uma resposta indevida dos controles de processo ou sistemas de segurança.

A rotina da ECM inclui o permanente acompanhamento de listas de verificação e registro de dados pertinentes da Instalação, mantendo-se estes registros atualizados para serem formalmente passados durante a rendição dos quartos de serviço, e inspeções visuais regulares pela Instalação. O monitoramento é particularmente importante quando ocorrem alterações no estado de Instalação.

A Instalação deve ser operada com base em uma hierarquia de procedimentos aprovados, sujeitos a um rígido controle de documentação que garanta sua correta

atualização. Eventuais desvios destes procedimentos somente poderão ser feitos após aprovação a um nível hierárquico apropriado, proporcional à sua relevância para a segurança. A manutenção e vigilância dos componentes e sistemas da Instalação devem estar sujeitos a um rigoroso controle, sendo as atividades de manutenção executadas pelo pessoal autorizado e somente após aprovação formal pela hierarquia.

Modificações na Instalação relevantes para a segurança somente devem ser realizadas por meio de procedimentos aprovados. A configuração da Instalação deve ser mantida dentro das especificações de projeto e da análise de segurança pelo cumprimento estrito de procedimentos que incluem esquemas formais de aprovação de modificações e revisões periódicas dos documentos afetados. Devem ainda ser mantidos no SNA desenhos e descrições atualizadas da IPN.

Uma cadeia de comunicação formal deve existir para a transmissão de ordens e para a transmissão de informações relacionadas à operação segura da Instalação, incluindo registros confiáveis e rapidamente recuperáveis das ordens, instruções e informações de potencial importância para a segurança, e confirmação de seu recebimento e correto entendimento.

Uma atenção especial deve ser dada a implementação de dispositivos físicos e de procedimentos administrativos que efetivamente previnam a possibilidade de execução de ações não autorizadas pelos operadores da IPN e demais tripulantes do SNA, sejam intencionais ou não, que poderiam ameaçar a segurança.

Os operadores da IPN devem ser objeto de um acompanhamento específico na área de assistência social de modo a prevenir condições pessoais particulares que possam vir a afetar seu desempenho no serviço, tais como problemas familiares, afetivos, financeiros, de saúde, etc. Eventuais condutas impróprias fora do serviço devem ser investigadas e severamente punidas, sendo a reincidência causa de retirada da licença de operador. Condutas impróprias durante o serviço devem ser causa de imediata retirada da licença. Tal rigor disciplinar visa garantir a total confiança que os operadores da IPN devem necessariamente inspirar à tripulação do SNA.

3.3.5.4 Treinamento

Princípio: São estabelecidos programas de treinamento e retreinamento para o pessoal de operação e manutenção que garantam a execução das suas tarefas segura e eficazmente. O treinamento é particularmente intensivo para pessoal de quarto na ECM, incluindo o emprego de simuladores.

O programa de treinamento inclui a identificação de requisitos, o desenvolvimento de especificações e materiais, execução e avaliação das atividades de ensino. O treinamento formal dos operadores cobre as áreas chaves de tecnologia como neutrônica, termohidráulica e proteção radiológica, a um nível compatível com as tarefas a serem executadas.

O treinamento dos operadores deve desenvolver conhecimentos teóricos e práticos da Instalação e de seu funcionamento. Inclui o conhecimento completo do arranjo físico, as localizações de componentes e sistemas importantes, as localizações, funções e efeitos dos seus controles, e o alinhamento normal dos sistemas da Instalação, com ênfase particular sobre os sistemas que têm importância para a segurança. Os operadores em formação aprendem as rotinas para operação normal da Instalação, e sua resposta a falhas que poderiam causar acidentes caso não haja uma ação efetiva. Este aspecto do treinamento tem como objetivo melhorar as capacidades de diagnóstico.

O treinamento deve cobrir o retorno da experiência operacional da IPN e de instalações semelhantes. Os operadores são treinados tanto nos procedimentos operacionais normais como nos de emergência. O programa de treinamento inclui aulas e estudo convencionais, emprego de simuladores, operação de protótipos e estágios de familiarização com a Instalação real. A aprovação dos alunos no programa conduzirá ao seu licenciamento formal pela ASN, que aplicará uma avaliação individual independente da organização operadora.

Através dos programas de treinamento, os operadores tomam conhecimento dos principais resultados das análises probabilísticas de segurança da Instalação identificando a importância dos sistemas na prevenção de danos à Instalação ou de acidentes severos. Eles são alertados para as localizações e quantidades de materiais radioativos na Instalação, conhecendo as medidas a serem tomadas para prevenir sua dispersão. O treinamento de operadores deve enfatizar a importância de manter a

Instalação dentro de suas condições e limites operacionais, considerando detalhadamente as consequências que adviriam de sua violação.

Deve ser ressaltada a importância de manter a subcriticalidade quando a Instalação não está operando, do contínuo resfriamento do núcleo, e do controle e confinamento de todos os materiais radioativos. O retreinamento é promovido a intervalos que assegurem a manutenção dos conhecimentos essenciais para uma operação segura e eficiente de Instalação, em particular para as condições anormais e acidentais. O treinamento inicial e os retreinamentos planejados são desenvolvidos simuladores representativos e em protótipos operacionais. O trabalho de equipe deve ser enfatizado pelo treinamento, particularmente em exercícios de incidentes e acidentes em simulador.

Um treinamento complementar é requerido para preparar os operadores para as tarefas específicas a serem desempenhadas no caso de acidentes. Deve ainda ser promovido treinamento específico para todo pessoal envolvido em tarefas associadas aos planos de emergência interno e externo.

O treinamento do pessoal de manutenção vai além do ensino das suas tarefas básicas, enfatizando as consequências para a segurança de eventuais erros técnicos ou não observância de procedimentos. O treinamento e qualificação de pessoal de manutenção reflete a experiência operacional acumulada da Instalação sobre indisponibilidades e funcionamento inadvertido ou deficiente de sistemas de segurança, que freqüentemente são causados por erros nos procedimentos e práticas de manutenção. O treinamento do pessoal de manutenção analisar tais incidentes. A avaliação do pessoal de manutenção deve verificar seu conhecimento destes incidentes.

O treinamento da tripulação do SNA não envolvida diretamente com a operação da IPN deve enfatizar os problemas particulares da operação da Instalação, considerando os excepcionais requisitos para a segurança, e familiarização com procedimentos de emergência.

3.3.5.5 Condições e Limites Operacionais

Princípio: Um conjunto de condições e limites operacionais é definido para identificar o domínio para operação segura da IPN. São ainda fixados requisitos mínimos para a disponibilidade de equipamentos e pessoal.

Como discutido anteriormente, um conjunto de limites e condições de segurança invioláveis define os valores extremos das variáveis operacionais dentro dos quais análises conservativas demonstraram que a Instalação não sofrerá efeitos indesejáveis ou danos inaceitáveis.

Os limites operacionais para operação normal são fixados para as variáveis críticas da Instalação, que são controladas por sistemas automáticos. Os limites operacionais e de proteção são estabelecidos de modo conservador, com base em métodos de análise validados e asseguram que os transientes antecipados não conduzem a ultrapassagem dos limites de segurança.

As condições e limites operacionais são definidos para todas as etapas do comissionamento, operação em potência, desligamento, partida, manutenção, testes e recarregamento de combustível. São executados testes e inspeções periódicos para calibração de instrumentos de medida e de apresentação dos valores das variáveis que têm limites de segurança, verificando-se os pontos de atuação.

Condições adicionais asseguram que os sistemas de segurança estão ou em operação ou prontos para uso. Estas condições são definidas de acordo com a confiabilidade e a resposta esperada dos sistemas. Requisitos mínimos de pessoal também são definidos, particularmente sobre os operadores da ECM. Estas condições somente podem ser contornadas temporariamente para testes específicos ou outros propósitos especiais, com base em medidas compensatórias e em análise de segurança prévia, devendo ser aprovado a um nível hierárquico compatível com a importância para a segurança envolvida.

O conjunto original de condições ou limites operacionais, assim como qualquer mudança subsequente, está sujeito a revisão e aprovação pela organização operadora e a ASN, de acordo com sua importância para a segurança. Como uma parte vital da cultura de segurança, é essencial que pessoal da Instalação entenda as bases teóricas e práticas usadas para o estabelecimento dos limites de operação e as consequências de sua violação.

Os limites operacionais não podem ser infringidos exceto quando previsto em procedimentos formais que assegurem tanto o pleno reconhecimento das implicações para a segurança e a implementação de eventuais fatores compensatórios.

3.3.5.6 Procedimentos Operacionais Normais

Princípio: A operação normal da IPN é controlada por procedimentos detalhados, validados e formalmente aprovados.

Os procedimentos operacionais da Instalação estão baseados no projeto e na análise de segurança e são validados através de simulações, experimentos, testes em protótipos, comissionamento e retorno da experiência operacional. Eles são apresentados em detalhe suficiente para permitir que os operadores executem suas tarefas sem análises adicionais. Do ponto de vista de segurança, os procedimentos, se corretamente seguidos, asseguram que não são excedidos as condições e os limites operacionais da Instalação, e que os componentes, sistemas e estruturas importantes para a segurança estão disponíveis. As especificações técnicas incluídas nos procedimentos cobrem testes de calibração e inspeções periódicos dos sistemas de segurança.

Uma atenção particular é dada pelos procedimentos para mudanças de estados operacionais, operação a baixa potência, condições de teste e situações em que partes de sistemas de segurança encontram-se voluntariamente indisponíveis (para manutenção, por exemplo). Nos procedimentos para carregamento e descarregamento do núcleo é dada ênfase aos riscos de criticalidade ou outros eventos indesejáveis que poderiam acontecer, tal como a queda de objetos pesados dentro do VPR.

Os procedimentos operacionais somente são revisados após aprovação formal, conforme procedimentos administrativos estabelecidos, e os documentos que definem os procedimentos operacionais estão sujeitos a controle conforme procedimentos de garantia de qualidade. Os operadores são treinados para as revisões principais dos procedimentos operacionais antes que estas sejam implementadas.

3.3.5.7 Procedimentos Operacionais de Emergência

Princípio: Os procedimentos operacionais de emergência são estabelecidos, documentados e aprovados para garantir uma resposta satisfatória dos operadores a eventos anormais.

Os dispositivos especiais de segurança são instalados para salvaguardar a Instalação dos acidentes dentro da base de projeto, sendo acionados automaticamente na ocorrência dos eventos inicializadores antecipados.

Os operadores são treinados para utilizar o período de tempo, previsto pelo projeto, durante o qual não é deles requerida nenhuma ação, para investigar e identificar as causas do acionamento automático destes sistemas. As informações adicionais fornecidas aos operadores pelo monitoramento dos sistemas lhes auxilia então a decidir as ações a serem tomadas para prevenir ou mitigar as conseqüências para a Instalação. Adicionalmente, procedimentos operacionais de emergência específicos devem estar disponíveis para responder aos ABP e aos acidentes além da base de projeto que contribuem significativamente para o Risco Objetivo Residual da IPN.

Estes procedimentos geralmente incorporam respostas baseadas na correta diagnose do eventos inicializadores. Se estes não podem ser identificados a tempo, ou se uma avaliação posterior faz com que o diagnóstico inicial seja descartado, os procedimentos operacionais de emergência definem respostas a partir do estado atual da Instalação, deduzido a partir dos sintomas observados. A exata determinação das causas que levaram a Instalação ao estado deixa de ser relevante nestes casos, sendo tais procedimentos orientados para o restabelecimento das funções básicas de segurança.

Os procedimentos operacionais de emergência também facilitam a recuperação a longo prazo de um acidente e a limitação de suas conseqüências radiológicas para a tripulação do SNA, para o público e o ambiente. Estes procedimentos fazem parte do programa de treinamento de operadores e do pessoal de proteção radiológica. Eles incluem os planos de emergência interno e externos que permitem o gerenciamento de acidentes severos que poderiam conduzir à liberação de quantidades significativas de materiais radioativos.

3.3.5.8 Procedimentos de Proteção Radiológica

Princípio: O pessoal de proteção radiológica da organização operadora estabelece procedimentos formais para o controle, orientação e proteção da tripulação, executando rotinas de monitoramento radiológico do ambiente interno do SNA, da exposição individual dos tripulantes, e das liberações controladas e autorizadas de efluentes radioativos.

Um serviço de proteção radiológica, formado por pessoal especializado, responde diretamente ao Comandante do SNA. Este serviço inclui o pessoal que monitora e registra as doses individuais, os níveis de radiação das áreas significativas, os efluentes radioativos, as ações de descontaminação e a preparação para

armazenamento e disposição de rejeitos radioativos, e supervisiona e controla o acesso de pessoal em áreas de radiação. O serviço de proteção radiológica tem responsabilidades específicas no caso de emergências. O pessoal de operação pode assumir algumas destas tarefas de proteção radiológica. Procedimentos específicos são elaborados para regulamentar as funções de proteção radiológica.

O pessoal de proteção radiológica deve ter acesso direto ao Comando do SNA sempre que for necessário garantir a observância dos procedimentos de proteção radiológica. Os tripulantes devem ser individualmente motivados pelo Comando e pelo pessoal de proteção radiológica para manter as próprias exposições rotineiras à radiação tão reduzidas quanto praticável.

O serviço de proteção radiológica mantém equipamentos de proteção individual especiais para realização de atividades de manutenção e de vigilância em áreas de radiação do SNA. Isto é particularmente relevante para os sistemas importantes para a segurança: os problemas de proteção radiológica não devem implicar em reduções nas atividades de inspeções, testes e manutenções programadas, nem impedir a realização de reparos que forem necessários. Os operadores que executam tarefas sob condições de altas taxas de dose, com usos de equipamentos especiais de proteção, devem ter treinamento específico em modelos em escala natural dos locais onde fará a intervenção, com o objetivo de minimizar os tempos de exposição.

3.3.5.9 Apoio Técnico à Operação

Princípio: Estão disponíveis ao longo de todo o ciclo de vida do SNA grupos externos de apoio técnico de engenharia à operação da IPN, com competência em todas as disciplinas importantes para a segurança,.

A continuidade da operação segura de uma IPN requer o apoio em terra de organizações de engenharia que podem ser convocadas para assessorar na especificação e execução de modificações, reparos e testes especiais na Instalação, proporcionando suporte analítico conforme necessário à segurança. Este recursos podem ser providos pela própria organização operadora ou pode estar disponível através de fornecedores e consultores externos. É de responsabilidade da organização operadora garantir que os recursos estarão permanentemente disponíveis.

Um fator importante para assegurar este apoio é propiciado pela manutenção, dentro da organização operadora ou em outras instituições no País, de programas de Pesquisa e Desenvolvimento relacionados com a segurança da propulsão nuclear.

3.3.5.10 Retorno da Experiência Operacional

Princípio: A organização operadora institui medidas para assegurar que os eventos significativos para a segurança sejam identificados e avaliados em profundidade, e que as medidas corretivas necessárias sejam implementadas prontamente, sendo as informações sobre elas amplamente disseminadas. O pessoal responsável pela operação da IPN tem acesso à experiência operacional pertinente a instalações semelhantes.

A importância para a segurança de um programa efetivo para o retorno da experiência operacional é apresentada no princípio fundamental Experiência Operacional e Pesquisa de Segurança. O Comandante do SNA informa prontamente aos setores competentes da organização operadora e da ASN qualquer ocorrência anormal de relevância para a segurança, de forma que suas implicações possam ser corretamente analisadas, a causa básica identificada e a informação comunicada a instalações similares. As boas práticas operacionais, quando julgado que poderão trazer potenciais benefícios para a segurança, também devem ser informadas.

Independentemente das análises genéricas que podem se seguir a uma ocorrência anormal e potencialmente prejudicial, o Comandante deverá implementar medidas específicas necessárias à prevenção da repetição de eventos semelhantes na IPN, ou pelo menos para assegurar que sua repetição não conduzirá a um acidente. Qualquer modificação correspondente, seja de material ou de procedimentos, só deverá ser implementada após a demonstração, pela análise de segurança, que a mudança não compromete a segurança de Instalação e depois que sejam tomadas medidas para garantir a qualidade de sua execução, proporcionais à sua importância para a segurança.

O pessoal responsável pela operação da IPN deve utilizar as informações obtida pelo retorno da experiência operacional de outras instalações semelhantes como uma fonte de ensinamentos aplicáveis à melhoria da segurança de sua próprias Instalação.

A vigilância e manutenção regular pelos operadores da IPN ou por congêneres em outras instalações semelhantes constituem uma valiosa fonte de informação sobre componentes e sistemas relacionados à segurança. Agrupamento de informação em

bancos de dados acessíveis aos responsáveis pela operação destas instalações é, deste modo, muito útil. A informação deve ser compilada e processada, e submetida a uma análise de tendências da Instalação, eventualmente em cooperação com outras instalações semelhantes, para identificar falhas ou degradação incipientes, como aquelas devidas ao envelhecimento. Devem então serem implementadas medidas para prevenir estas falhas ou inverter tendências adversas reveladas pelo processamento dessa informação.

O gerenciamento da operação deverá estar atento quanto à relevância das análises de risco para a segurança da Instalação, devendo cooperar na execução destas análises através da coleta e transferência dos dados necessários que estiverem disponíveis.

3.3.5.11 Manutenção, Inspeções e Testes

Princípio: As estruturas, componentes e sistemas importantes para a segurança são objeto de manutenção preventiva, inspeções, testes e reparos planejados, assegurando-se assim que permanecerão capazes de atender às especificações de projeto ao longo de todo o ciclo de vida do SNA. Estas atividades são realizadas conforme procedimentos escritos, apoiados por ações de garantia de qualidade.

Quando uma IPN entra em operação, seu programa de manutenção preventiva e vigilância é posto em prática para que estruturas, componentes e sistemas continuem operando como especificado, não sendo reduzida por fenômenos de envelhecimento, desgaste ou outros processos de deterioração funcional a sua capacidade de atender plenamente aos objetivos do projeto.

A análise de tendências feita, por exemplo, por monitoramento de vibrações, deve ser empregada para melhorar a efetividade do programa. Estas atividades representam um papel essencial prevenindo falhas em operação, sendo então corrigidas a tempo as deficiências assim descobertas. A conformidade com procedimentos escritos e aprovados deve sempre ser requerida e verificada onde sistemas importantes para a segurança estão envolvidos. Os procedimentos asseguram que os operadores da ECM permanecem informados da evolução de qualquer atividade em andamento.

Uma programação aprovada de inspeções deve ser seguida, baseada em análises realizadas na fase de projeto e de testes de comissionamento, sendo alterada de acordo com a experiência operacional.

Deve ser dedicada atenção especial à vigilância do estado das barreiras físicas de retenção de materiais radioativos, em particular das regiões do envelope estanque do Circuito Primário sujeitas a irradiação por nêutrons térmicos e a ciclos de pressão e envelhecimento como uma consequência do funcionamento normal. Onde possível, devem ser feitos testes em amostras removíveis que foram expostas a condições similares ou aceleradas durante os mesmos ciclos de funcionamento. As atividades de manutenção planejadas são executadas com base na importância para a segurança dos sistemas, e tendo em mente a possibilidade de práticas imprudentes reduzirem os benefícios potenciais da defesa em profundidade.

Um componente principal da disponibilidade instantânea das funções de segurança essenciais são os testes funcionais periódicos dos sistemas de segurança. A frequência, extensão e natureza destes testes são determinados pela disponibilidade requerida, e pela capacidade prática de simular o funcionamento. Em circunstâncias onde a demonstração plena não é possível por testes periódicos do sistema, testes de componentes individuais e de sistemas parciais devem ser executados para demonstrar a disponibilidade da função de segurança.

Sabendo-se que a execução incorreta de atividades de manutenção e testes podem causar graves problemas, deve ser considerada a otimização das características destas atividades, tais como frequência e escopo de manutenção preventiva, com base em instruções dos fabricantes de equipamentos, retorno da experiência operacional e análise de tendências, treinamento e procedimentos.

A exposição à radiação do pessoal durante manutenção deve ser controlada e limitada por meio de planos de trabalho para controle radiológico, ensaios e monitoramento.

Os elevados padrões de segurança a serem alcançados pela manutenção requerem que o pessoal envolvido esteja atento aos aspectos de segurança das tarefas que estão executando. Os trabalhadores de manutenção devem então ser treinados cuidadosamente para suas tarefas, de forma a reduzir a possibilidade de erro humano na

execução de suas tarefas. As atividades de manutenção requerem eventualmente a indisponibilidade temporária de sistemas de segurança específicos.

Isto só deve ser permitido em cumprimento a procedimentos escritos, testados e aprovados, e tendo sido implementadas medidas compensatórias durante o período de indisponibilidade. O pessoal de manutenção deve ser treinado nos equipamentos específicos nos quais intervém. Quando o trabalho é executado em equipamentos por indivíduos que não fazem parte do pessoal treinado e qualificado para a Instalação, ele deve ser supervisionado e verificado por um indivíduo qualificado, treinado no desempenho da tarefa e no seu significado para a segurança.

3.3.5.12 Garantia da Qualidade na Operação

Princípio: Um Programa de Garantia de Qualidade para operação é estabelecido pela organização operadora com o objetivo de assegurar um desempenho satisfatório em todas as atividades importantes para a segurança da IPN.

Este princípio específico complementa o princípio fundamental em garantia de qualidade, considerando a fase de operação do ciclo de vida do SNA. Este Programa de Garantia de Qualidade dá suporte aos responsáveis pela operação, incluindo o próprio Comandante, no sentido de assegurar uma correta execução de suas atividades.

3.3.6 GERENCIAMENTO DE ACIDENTES

Entre os acidentes de probabilidade muito baixa, não considerados pela base de projeto, encontram-se alguns que poderiam conduzir a circunstâncias nas quais não poderia ser mantido um adequado resfriamento do núcleo, ou nas quais uma degradação significativa do combustível poderia efetivamente ocorrer ou pelo menos tornar-se iminente.

Devem, então, ser tomadas providências para gerenciar tais circunstâncias ainda que elas sejam de muito baixa probabilidade. O gerenciamento de acidentes como um componente de proteção inclui as ações a ser conduzidas pelos operadores durante a evolução de um cenário acidental, após serem excedidas as condições limite previstas pela base de projeto da Instalação, mas antes de que um acidente severo de fato desenvolva.

Tais ações dos operadores poderiam alterar ou inverter o curso de um cenário acidental. O gerenciamento de acidentes atua em seguida como um componente de mitigação de conseqüências, incluindo ações positivas dos operadores no caso de real ocorrência de um acidente severo, dirigidas a prevenir propagações adicionais de um tal acidente e aliviando seus efeitos. O gerenciamento de acidentes inclui ações que poderiam ser tomadas para proteger a função de confinamento ou, caso esta esteja irremediavelmente comprometida, limitar as potenciais liberações de materiais radioativos para o ambiente.

Os princípios de segurança previamente discutidos que tratam da análise da experiência operacional, monitoramento do estado da Instalação e controle de acidentes dentro da base de projeto, contribuem significativamente para a capacidade de gerenciamento de acidentes. Além destes, entretanto, são previstos dispositivos e procedimentos adicionais específicos.

A meta do gerenciamento de um acidente não considerado pela base de projeto seria devolver a Instalação a um estado controlado, no qual a reação nuclear de fissão em cadeia é essencialmente extinta, o combustível é resfriado continuamente e os materiais radioativos são confinados.

O gerenciamento de acidentes deverá aproveitar ao máximo as capacidades remanescentes da Instalação, se necessário indo além das funções originalmente previstas para alguns sistemas e usando sistemas “de fortuna” para alcançar esta meta. O gerenciamento de acidentes deverá responder às circunstâncias específicas do evento, mesmo sabendo-se que elas não podem ser previstas com antecedência, devendo as decisões tomadas considerar o tempo que estaria disponível entre a diagnose correta dos sintomas e o lançamento iminente de produtos de fissão para o ambiente.

Para a diagnose de eventos além da base de projeto e a execução de atividades de gerenciamento de acidentes, o tempo disponível para tomada de decisões pelos operadores tende a ser um pouco mais longo que aqueles para ABP, pois neste caso a Instalação já estaria irreversivelmente perdida.

Um gerenciamento de acidentes efetivo requer o treinamento dos operadores e a disponibilidade de informações e capacidade de controle na ECM principal ou secundária. Isto aumentaria significativamente a probabilidade dos operadores terem

uma indicação suficiente das condições adversas e da disponibilidade de equipamentos necessários às eventuais ações corretivas e de proteção.

3.3.6.1 Estratégia para Gerenciamento de Acidentes

Princípio: Os resultados de simulações da resposta da IPN a potenciais acidentes além da base de projeto são usados na definição de orientações para elaboração de uma estratégia para o gerenciamento de acidentes.

A análise dos acidentes além da base de projeto que têm potencial para degradação severa do núcleo e perda das barreiras que previnem o lançamento de materiais radioativos deve ser executada pelos melhores meios analíticos e de simulação disponíveis. Devem ser identificados os sintomas dos acidentes específicos analisados para uso na diagnose e medidas a serem tomadas para reduzir significativamente a extensão dos danos à Instalação e dos efeitos da radiação sobre a tripulação, o público e o ambiente. Estas medidas podem considerar o emprego de sistemas normais da Instalação ou modos não originalmente previstos ou dispositivos especiais especificamente implementados para o gerenciamento de acidentes.

3.3.6.2 Treinamento e Procedimentos para Gerenciamento de Acidentes

Princípio: Os operadores da IPN e os demais tripulantes do SNA são treinados e retreinados nos procedimentos a serem seguidos no caso de ocorrência de um acidente severo além da base de projeto.

Toda a tripulação do SNA deverá ser familiarizada com as características das análises descritas no princípio anterior, como parte do seu programa de treinamento. Os procedimentos empregados no gerenciamento de acidentes são os procedimentos operacionais de emergência da IPN, que devem incluir as providências a serem tomadas nestas situações severas.

Os procedimentos de emergência para estas situações limite são de natureza geral e servem para indicar aos operadores as capacidades da Instalação para deter o curso e mitigar as consequências de acidentes severos. Estes procedimentos são flexíveis, de forma que possam ser ajustados às incertezas associadas a sua potencial evolução.

O treinamento dos operadores da Instalação deve assegurar sua familiaridade com os sintomas de acidentes além da base de projeto e os procedimentos para

gerenciamento de acidentes. Os simuladores são ferramentas de treinamento indispensáveis para este treinamento, que devem poder representar corretamente o modo pelo qual um acidente evoluiria, pelo menos até a ocorrência de dano extenso ao combustível.

Quando o tempo e as comunicações permitirem, uma equipe de especialistas deve ser formada para aconselhar o Comandante do SNA no caso de ocorrência um acidente que exceda a base de projeto. Esta equipe deve incluir técnicos familiarizados com as análises de acidentes severos previamente realizadas para a Instalação.

3.3.6.3 Dispositivos de Engenharia para Gerenciamento de Acidentes

Princípio: Equipamentos, instrumentação e ferramentas de auxílio ao diagnóstico estão disponíveis aos operadores para controlar a evolução e as consequências de acidentes severos além da base de projeto.

O desenvolvimento de um comportamento anormal da Instalação em consequência de falha de equipamentos ou erros do operador poderiam ser rápidos em algumas circunstâncias. O quarto de serviço na ECM teria então que diagnosticar a causa e iniciar um plano de ações corretivas apropriado rapidamente, devendo portanto ser previstos meios para auxiliar nestas tarefas particularmente complexas.

Estes meios devem incluir instrumentação externa à ECM, qualificada para ambientes severos e capaz de prover a informação necessária à identificação de condições anormais, correção de falhas e determinação dos efeitos das ações corretivas. Exemplos de instrumentação especificamente implementada para gerenciamento de acidentes são os sistemas para análise de tendências para o inventário de refrigerante primário (medidores de nível de líquido no VPR), medidores de altas pressões e de concentração de hidrogênio na contenção e medidores de radioatividade no refrigerante primário.

A capacidade para mitigação de acidente sempre foi considerada importante no projeto de instalações nucleares. O emprego de estruturas de confinamento e sistemas de contenção constitui uma evidência deste objetivo. Estes equipamentos tornam-se úteis em circunstâncias mais extremas que aquelas originalmente previstas nas especificações devido às margens de segurança consideradas pelo projeto.

Certas evoluções de projeto tem sido implementadas recentemente para mitigar os efeitos de acidentes severos, concentrando-se no restabelecimento e manutenção do resfriamento do núcleo e das funções de confinamento. Estas evoluções incluem a instalação de sistemas de alívio de pressão com filtros e de queimadores de hidrogênio na Contenção.

3.3.7 PLANEJAMENTO DE EMERGÊNCIA

O planejamento e a preparação para emergência devem incluir as atividades necessárias para assegurar que, no caso de um acidente, todas as ações para a proteção da tripulação, do público e do ambiente poderiam ser executadas, e que a efetiva decisão pelo uso dos serviços disponíveis seria disciplinada.

Um aspecto fundamental do planejamento de emergência é o cumprimento das determinações da Lei de Responsabilidade Civil por Danos Nucleares, em vigor no País.

3.3.7.1 Planos de Emergência

Princípio: Os planos de emergência interno e externo são elaborados pela organização operadora e aprovados pela ASN antes do início da operação do SNA, sendo exercitados periodicamente para assegurar a efetiva funcionalidade das medidas previstas no caso de um acidente potencial que resultaria em liberações significativas de materiais radioativos no interior e no exterior do SNA. O plano de emergência externo define zonas geográficas ao redor do SNA, permitindo planejamento de respostas proporcionais aos potenciais impactos.

Os planos de emergência são constituídos por ações internas e externas ao SNA a serem tomadas para proteger respectivamente a tripulação e o público de qualquer lançamento significativo de materiais radioativos pela IPN para o interior do próprio submarino, para as instalações de apoio em terra ou para o ambiente de uma forma geral. O Plano de Emergência Interno é de integral responsabilidade da organização operadora. O Plano de Emergência Externo é de responsabilidade de outra autoridade a nível nacional, tendo entretanto participação significativa da organização operadora.

Os planos são testados periodicamente, exercitando-se seus canais de comunicação e meios logísticos. Os planos de emergência definem arranjos organizacionais e uma divisão de responsabilidades pela execução das ações de emergência, sendo flexíveis o suficiente para serem adaptados às circunstâncias particulares em que seriam efetivamente empregados.

Os planos de emergência definem as ações que seriam tomadas no caso de um acidente severo para restabelecer o controle sobre a Instalação, para proteger a tripulação, o público e o ambiente, e para proporcionar rapidamente a informação necessária para a ASN e outras autoridades. O planejamento de emergência define zonas ao redor do SNA que determina uma base geográfica sobre a qual são implementadas medidas protetoras como parte de uma resposta proporcional aos efeitos esperados. Estas medidas incluem a notificação das organizações envolvidas, a abrigagem e evacuação do pessoal circundante, profilaxia de radioproteção e fornecimento de equipamento de proteção individual, monitoramento da radiação, controle de acesso às zonas afetadas, descontaminação, assistência médica, fornecimento de alimentos e água, controle de produtos agrícolas e comunicação social.

Considerando-se os princípios fundamentais que tratam das áreas de mobilidade e localizações fixas do SNA, pode-se considerar que para um submarino em operação no mar não seria necessário um Plano de Emergência Externo. Para um SNA em localização fixa atracado ou fundeado em Base Naval, as ações do Plano de Emergência Externo seriam restritas, *a priori*, à zona sob controle administrativo da organização operadora. Para um SNA em localização fixa atracado ou fundeado em porto civil, as ações do Plano de Emergência Externo seriam restritas, *a priori*, à zona sob controle administrativo da autoridade portuária.

3.3.7.2 Execução dos Planos de Emergência

Princípio: Um centro de coordenação de emergência permanentemente equipado está disponível fora das zonas de atuação dos planos de emergência. No local, um centro semelhante coordena as atividades de emergência interna e comunica-se com o centro de emergência externo.

O centro de emergência externo é onde toda a ação de emergência é determinada e iniciada, aparte das medidas internas ao SNA para manter a IPN sob controle e proteger a tripulação.

Este centro deve ter canais de comunicação confiáveis com o SNA e com todas as demais organizações envolvidas na execução do plano de emergência, como autoridades civis locais e nacionais. Dados meteorológicos, hidrográficos e oceanográficos locais, particularmente sobre os níveis de radiação natural, se disponíveis, devem ser transmitidos aos centros de emergência. Mapas da área local

devem estar disponíveis, indicando as zonas de planejamento de emergência e suas características. Registros de informações importante recebidas e enviadas deverão estar permanentemente disponíveis

O centro de emergência interno é um local ao qual todas as contramedidas podem ser determinadas e iniciadas, aparte do controle da IPN. Deve ser equipado com instrumentação que retransmita as condições mais significativas da Instalação. Este centro, que poderia ser instalado a bordo de outro navio, seria o local onde seriam compilados dados sobre as condições de Instalação para transmissão ao centro de emergência externo, devendo ser provido de equipamento de proteção individual para o pessoal que o garante.

3.3.7.3 Análise de Consequências de Acidentes e Monitoramento Radiológico

Princípio: Estão disponíveis meios para previsão, em tempo real, da extensão e impacto de qualquer liberação de materiais radioativos no caso de ocorrência de um acidente, possibilitando uma análise rápida e contínua da situação radiológica, e determinação da necessidade de implementação de medidas de proteção.

Métodos e modelos de análise devem estar disponíveis para a organização operadora que permitam predição da exposição potencial de uma potencial ou real liberação de materiais radioativos. O monitoramento local é usado para caracterizar o termo-fonte e taxas de liberação. Para os dados externos à área sob controle da organização operadora, devem ser previstas equipes móveis de monitoramento radiológico e para certas localizações fixas pré-definidas, de redes de estações de monitoramento fixas. Recursos laboratoriais deverão também estar disponíveis para análise rápida e interpretação dos níveis e da natureza da radioatividade em números significativos de amostras.

As decisões sobre necessidade, natureza e extensão das contramedidas protetoras devem ser tomadas com base em recomendações definidas pela organização operadora e em níveis de intervenção ou diretrizes fixados pela ASN, que deverá receber as informações pertinentes rapidamente e deve ter competência técnica específica para fazer as avaliações e autoridade administrativa para tomar as decisões que podem se tornar necessárias.

4 CRITÉRIOS GERAIS

Neste Capítulo serão propostos Critérios Gerais de Segurança para o projeto da IPN e de suas interfaces com a plataforma-navio do SNA. Como “Critérios Gerais” entende-se o detalhamento dos Objetivos e Princípios de Segurança numa série de diretrizes quantitativas que orientam o desenvolvimento do projeto integrado do conjunto de sistemas que compõem o SNA.

São inicialmente desenvolvidos critérios para a Probabilidade de ocorrência e para a Gravidade de conseqüências das diferentes Condições de Processo da Instalação Nuclear CPIN e Situações de Operação do Submarino SOS. Estes critérios são então combinados sob forma de critérios para o Risco residual aceitável, compondo assim os Objetivos Detalhados de Segurança ODS. É apresentado o Critério de Falha Única, de natureza determinística, e discutida sua aplicação aos sistemas do SNA.

Em seguida são desenvolvidos os critérios de projeto para definição de áreas de mobilidade e de localizações fixas do submarino, e para o descomissionamento e perda do navio. São estabelecidas as bases para determinação das classes de segurança e das condições ambientais a serem consideradas para os componentes, estruturas, equipamentos e sistemas do SNA.

São finalmente definidas as CPIN e SOS a serem submetidas à análise quanto ao atendimento dos OGS e desenvolvidos critérios gerais para execução destas análise critérios particulares à análise das CPIN e das SOS.

4.1 OBJETIVOS DETALHADOS DE SEGURANÇA

4.1.1 CRITÉRIO DE PROBABILIDADE

Em nenhuma atividade humana a segurança pode ser absoluta e portanto nenhum critério pode ser desenvolvido garantindo a ausência de riscos. No caso de submarinos convencionais, é normalmente possível estabelecer critérios gerais e requisitos específicos de projeto, construção e operação sobre uma base empírica, fundada na aceitabilidade da experiência operacional prévia.

O Risco Objetivo Residual resultante do atendimento destes critérios e requisitos é então considerado consuetudinariamente como aceitável, não sendo quantitativamente explicitado nem verificado em relação a parâmetros objetivos. No caso de submarinos nucleares em geral e dos SNA em particular, onde os problemas de segurança específicos envolvem Perigos de origem radiológica para o público e o ambiente aos quais está associada uma percepção social dos riscos extremamente sensível, uma abordagem mais sistemática torna-se essencial.

Tal abordagem requer uma quantificação do nível de Risco Objetivo Residual alcançado pela aplicação dos critérios e requisitos estabelecidos e a verificação de sua aceitabilidade com base em critérios objetivos pela ASN.

A primeira etapa desta abordagem é a hierarquização dos cenários operacionais do SNA de acordo com a suas Frequências Anuais de Ocorrência FAO estimadas e dos níveis de conseqüências máximas. Estes dois conceitos são introduzidos como se segue:

- Os cenários operacionais são classificados de acordo com a sua probabilidade de ocorrência, que pode variar desde contínua (probabilidade igual a 1) até extremamente remota (probabilidade considerada mínima);
- Para cada classe, é estabelecido um nível máximo de conseqüências. Considerando-se o conceito de risco, que conjuga probabilidade e gravidade, estes níveis são definidos de forma inversamente proporcional à magnitude da FAO respectiva.

Os cenários operacionais do SNA são definidos como Condições de Processo da Instalação Nuclear CPIN e Situações Operativas do Submarino SOS, notando-se que uma CPIN pode levar a diferentes SOS e vice-versa. Estes cenários são hierarquizados em 5 classes, definidas conforme faixas de FAO, determinadas qualitativa ou quantitativamente conforme a Tabela 4.1.

As quatro primeiras classes constituem a base de projeto, onde se encontram incluídos os cenários operacionais dentro dos quais os sistemas de processo e de segurança da IPN são especificados e dimensionados. Na última classe, complementar, são incluídos cenários acidentais fora da base de projeto. O desempenho dos sistemas de processo e de segurança da IPN são verificados para estes cenários e os resultados desta análise são

utilizados para determinar ações de gerenciamento de emergências e os Planos de Emergência Interno e Externo.

A cada classe de cenário operacional são associados diferentes níveis de consequências máximas aceitáveis incidindo sobre o próprio SNA (critério Disponibilidade) e o ambiente circundante (critério Liberação), assim como sobre os diferentes grupos humanos afetados, que são a tripulação (critério Tripulação), o pessoal de apoio logístico em terra (critério Apoio) e o público em geral (critério Público). Estes níveis constituem escalas de gravidade que, conjugadas com a escala de probabilidade estabelecida pelas classes de FAO, determinam o Risco Objetivo Residual da IPN

TABELA 4.1: CLASIFICAÇÃO DE CENÁRIOS OPERACIONAIS DO SNA
CONFORME SUAS FREQUÊNCIAS ANUAIS DE OCORRÊNCIA

CLASSE	VEROSSIMILHANÇA	FAO
1	contínuo ou freqüente: ocorre continuamente ou é provável ocorrer diversas vezes durante o ciclo de vida do SNA	> 1
2	infreqüente: não ocorre freqüentemente mas é provável que ocorra pelo menos uma vez durante o ciclo de vida do SNA	$1 > \text{FAO} > 10^{-2}$
3	possível: a princípio, não deve ocorrer durante o ciclo de vida de um único SNA, mas poderia ocorrer quando considera-se o ciclo de vida de um esquadrão composto por mais de uma unidade	$10^{-2} > \text{FAO} > 10^{-4}$
4	improvável: a princípio, não deve ocorrer durante o ciclo de vida de um esquadrão de SNA composto por mais de uma unidade, sendo porém possível	$10^{-4} > \text{FAO} > 10^{-6}$
Comple- mentar	hipotético: a princípio, não ocorrerá durante o ciclo de vida de um esquadrão de SNA composto por mais de uma unidade, sendo sua remota possibilidade de ocorrência associada à perda total de sistemas e funções de segurança atuantes em cenários de classe 4	$10^{-6} > \text{FAO}$

4.1.2 CRITÉRIO DE GRAVIDADE

Os níveis de consequências máximas aceitáveis consideradas pelo critério D (Disponibilidade) referem-se ao estado final do SNA decorrente do cenário operacional considerado, conforme Tabela 4.2.

TABELA 4.2: NÍVEIS DE CONSEQUÊNCIAS PARA O SUBMARINO

NÍVEL	CONSEQUÊNCIAS PARA O SUBMARINO
1	OPERAÇÃO NORMAL <ul style="list-style-type: none">• Submarino disponível imediatamente com plena capacidade operacional;• Situações de operação normais sob propulsão nuclear.
2	OPERAÇÃO DEGRADADA <ul style="list-style-type: none">• Submarino disponível com capacidades operacionais reduzidas (redução de potência) imediatamente ou após uma intervenção de reparo passível de ser realizada pela própria tripulação;• Situações de operação degradadas sob propulsão nuclear.
3	ACIDENTES COM RECUPERAÇÃO DA OPERAÇÃO <ul style="list-style-type: none">• Capacidades operacionais seriamente comprometidas, podendo ir até perda total da potência nuclear ou incapacidade de navegar submerso, implicando retorno prematuro à base sob propulsão auxiliar convencional;• Situações de operação incidentais sérias sob propulsão auxiliar convencional (reator desligado com remoção de calor residual).
4A	ACIDENTES SEM RECUPERAÇÃO DA OPERAÇÃO, COM SALVAMENTO DO SUBMARINO <ul style="list-style-type: none">• Degradações materiais importantes, podendo ir até a incapacidade de mover-se por seus próprios meios (necessidade de reboque para retorno à base), mantida, entretanto, uma mínima disponibilidade de fontes de energia internas;• Situações de operação acidentais com perda total da propulsão (reator desligado com resfriamento de emergência).
4B	ACIDENTES SEM RECUPERAÇÃO DA OPERAÇÃO, COM PERDA DO SUBMARINO <ul style="list-style-type: none">• Degradações materiais importantes, podendo ir até a perda de todas as fontes de energia internas (necessidade de fornecimento externo de energia ou meios passivos para manutenção das funções de segurança);• Situações de operação acidentais com perda total do submarino por naufrágio ou encalhe (reator desligado com resfriamento passivo ou provido por meios externos).
Comple-	ACIDENTES SEVEROS

SÍNTESE DE DOUTRINA DE SEGURANÇA
PARA PROJETO E OPERAÇÃO DE SUBMARINOS NUCLEARES

mentar	<ul style="list-style-type: none"> • Perda do submarino e das funções básicas de segurança (resfriamento do núcleo e contenção); • Situações de operação acidentais complementares.
--------	---

Os níveis de conseqüências máximas aceitáveis considerados pelo critério L (Liberações) referem-se à atividade total e de radionuclídeos de particular interesse sob o ponto de vista de impacto ambiental dos materiais radioativos liberados da IPN para o interior do submarino e para o ambiente externo decorrente do estado final do SNA para o cenário operacional considerado, conforme Tabela 4.3.

TABELA 4.3: NÍVEIS DE CONSEQÜÊNCIAS PARA O AMBIENTE

NÍVEL	CONSEQÜÊNCIAS PARA O AMBIENTE
1	<ul style="list-style-type: none"> • Observância dos limites anuais para liberação de efluentes autorizados pela ASN • Classificação das áreas internas do submarino por zonas de radiação conforme condições normais de projeto
2	<ul style="list-style-type: none"> • Observância dos limites anuais para liberação de efluentes autorizados pela ASN • Possibilidade de reclassificação temporária das áreas internas do submarino por zonas de radiação, retornando-se às condições normais após intervenção da tripulação
3	<ul style="list-style-type: none"> • Observância, por incidente, dos limites anuais de liberação de efluentes autorizados pela ASN • Possibilidade de reclassificação permanente das áreas internas do submarino por zonas de radiação, o retorno às condições normais requerendo intervenção do apoio em terra
4	<ul style="list-style-type: none"> • Termo-fonte liberado (relativo ao inventário de produtos radioativos): <ul style="list-style-type: none"> ✓ 2% dos gases raros ✓ 1% do iodo • Taxa máxima de vazamento da Contenção: <ul style="list-style-type: none"> ✓ 0,4%/dia no primeiro dia após o acidente ✓ 0,2%/dia nos 29 dias subsequentes
Comple- mentar	<ul style="list-style-type: none"> • Termo-fonte liberado (relativo ao inventário de produtos radioativos): <ul style="list-style-type: none"> ✓ 80% dos gases raros ✓ 0,6% do iodo orgânico ✓ 60% do iodo inorgânico ✓ 40% do céσιο

	✓ 5% do estrôncio
--	-------------------

Os níveis de consequências máximas aceitáveis considerados pelo critério T (Tripulação) referem-se ao detrimento à saúde e integridade física dos tripulantes decorrentes da evolução do cenário acidental considerado, conforme a Tabela 4.4.

Este detrimento é derivado não só dos efeitos determinísticos e estocásticos das radiações ionizantes provenientes dos materiais radioativos contidos na IPN, como também de outros efeitos não radiológicos. Os níveis máximos são definidos para os operadores da IPN e para os demais tripulantes do submarinos não afetos a tarefas em zona controlada.

TABELA 4.4: NÍVEIS DE CONSEQUÊNCIAS PARA A TRIPULAÇÃO

NÍVEL	CONSEQUÊNCIAS PARA A TRIPULAÇÃO
1	<ul style="list-style-type: none"> Situação com riscos ocupacionais normais; Doses efetivas (corpo inteiro) para os operadores da IPN dentro do limite anual de 20 mSv e tão reduzidas quanto razoavelmente realizável. Doses efetivas (corpo inteiro) para os demais tripulantes dentro do limite anual de 5 mSv e tão reduzidas quanto razoavelmente realizável.
2	<ul style="list-style-type: none"> Risco de danos imediatos leves para a tripulação, não associados a causas radiológicas; Doses efetivas (corpo inteiro) para os operadores da IPN dentro do limite anual de 50 mSv; Doses efetivas (corpo inteiro) para os demais tripulantes dentro do limite anual de 20 mSv.
3	<ul style="list-style-type: none"> Risco de danos imediatos graves com uma pequena probabilidade de morte de um membro da tripulação; Dose efetiva (corpo inteiro) sobre tripulante mais afetado inferior a 100mSv.
4	<ul style="list-style-type: none"> Risco de vida elevado para um ou vários membros da tripulação; Abandono do submarino dos tripulantes não envolvidos nas ações do Plano de Emergência Interno
Comple- mentar	<ul style="list-style-type: none"> Abandono de toda tripulação do submarino; Perda da tripulação.

Os níveis de consequências máximas aceitáveis considerados pelo critério A (Apoio) referem-se ao detrimento à saúde e integridade física pessoal em terra envolvido em atividades de apoio ao SNA decorrentes da evolução do cenário acidental considerado, conforme a Tabela 4.5. Este detrimento é derivado não só dos efeitos determinísticos e estocásticos das radiações ionizantes provenientes dos materiais radioativos contidos na IPN e nas instalações nucleares de apoio em terra, como também de outros efeitos não radiológicos.

Os níveis de consequências máximas aceitáveis considerados pelo critério P (Público) referem-se ao detrimento à saúde de indivíduos do público diretamente afetados pela evolução do cenário acidental considerado (membro do grupo crítico mais exposto), conforme a Tabela 4.6. O detrimento considerado é derivado exclusivamente dos efeitos estocásticos das radiações ionizantes provenientes dos materiais radioativos contidos na IPN e nas instalações nucleares de apoio em terra.

TABELA 4.5: NÍVEIS DE CONSEQUÊNCIAS PARA PARA O PESSOAL DE APOIO
EM TERRA

NÍVEL	CONSEQUÊNCIAS PARA O PESSOAL DE APOIO EM TERRA
1	<ul style="list-style-type: none">• Situação com riscos ocupacionais normais;• Doses efetivas (corpo inteiro) dentro do limite anual de 20 mSv e tão reduzidas quanto razoavelmente realizável.
2	<ul style="list-style-type: none">• Risco de danos imediatos leves, não associados a causas radiológicas;• Doses efetivas (corpo inteiro) dentro do limite anual de 50 mSv;
3	<ul style="list-style-type: none">• Risco de danos imediatos graves com uma pequena probabilidade de morte de um indivíduo;• Dose efetiva (corpo inteiro) sobre indivíduo mais afetado inferior a 100mSv.
4	<ul style="list-style-type: none">• Risco de vida elevado para um ou vários indivíduo;• Dose efetiva (corpo inteiro) sobre tripulante mais afetado inferior a 250mSv• Dose efetiva (tireóide) sobre indivíduo mais afetado inferior a 1.500mSv• Abandono do local do pessoal não envolvido nas ações do Plano de Emergência Interno
Comple-	<ul style="list-style-type: none">• Dose efetiva (corpo inteiro) sobre indivíduo mais afetado inferior a 250mSv

mentar	<ul style="list-style-type: none"> • Dose efetiva (tireóide) sobre indivíduo mais afetado inferior a 3.000mSv • Abandono do local do pessoal não envolvido nas ações do Plano de Emergência Externo
--------	---

O critério geral para aceitabilidade do Risco Objetivo Residual associado à operação da IPN ao longo do ciclo de vida do SNA será então determinado verificando-se que todos os cenários operacionais verossímeis classificados conforme sua FAO implicam em impactos inferiores às máximas conseqüências definidas *a priori*. Cada cenário será assim classificado conforme sua FAO e o critério de aceitabilidade para cada classe é definido com base em níveis de conseqüências máximas. O Risco Residual Aceitável é então definido sob a forma de Objetivos Detalhados de Segurança ODS

TABELA 4.6: NÍVEIS DE CONSEQÜÊNCIAS PARA O PÚBLICO

NÍVEL	CONSEQÜÊNCIAS PARA O PÚBLICO
1	<ul style="list-style-type: none"> • Dose efetiva (corpo inteiro) sobre o membro do público mais afetado inferior a 100 μSv
2	<ul style="list-style-type: none"> • Dose efetiva (corpo inteiro) sobre o membro do público mais afetado inferior a 1 mSv
3	<ul style="list-style-type: none"> • Dose efetiva (corpo inteiro) sobre o membro do público mais afetado inferior a 5 mSv • Dose efetiva (tireóide) sobre o membro do público mais afetado inferior a 15 mSv
4	<ul style="list-style-type: none"> • Dose efetiva (corpo inteiro) sobre o membro do público mais afetado inferior a 50 mSv • Dose efetiva (tireóide) sobre o membro do público mais afetado inferior a 250 mSv
Comple- mentar	<ul style="list-style-type: none"> • Dose efetiva (corpo inteiro) sobre o membro do público mais afetado inferior a 100 mSv • Dose efetiva (tireóide) sobre o membro do público mais afetado inferior a 450 mSv

4.1.3 CRITÉRIOS DE RISCO

Deverão ser estabelecidos, ao início de cada projeto de SNA, os Objetivos Detalhados de Segurança ODS para a IPN e para as instalações nucleares de apoio ao SNA em terra. Os ODS são diferenciados em função da gravidade das consequências de um cenário operacional, e quantificados com o objetivo de fixar os conjugados FAO x consequências máximas aceitáveis, sendo definidos com relação a posições geográficas típicas:

- I. submarino atracado ou fundeado em porto civil (próximo a aglomerações humanas);
- II. submarino atracado ou fundeado em base naval (distante de aglomerações humanas);
- III. submarino operando em águas costeiras; e
- IV. submarino operando em águas oceânicas.

A análise de segurança da plataforma-navio do SNA e da IPN deve definir os cenários operacionais e respectivas FAO considerados na base de projeto e para gerenciamento e planejamento de emergências (critérios de probabilidade), que vão ser associados aos critérios de gravidade D, L, T, A e P, compondo assim os critérios de risco, denominados Objetivos Detalhados de Segurança (ODS).

Para situações normais de paz e posições geográficas I, II e III, os ODS são definidos conforme a Tabela 4.7. Para cenários operacionais cuja ocorrência é restrita à posição geográfica IV, as consequências máximas definidas pelo Critérios L, T, A e P poderão ser elevadas de um nível. Para situações de guerra ou conflito grave, além dos cenários operacionais considerados para as situações normais de paz, deverão ser estabelecidos cenários decorrentes de agressões provenientes dos efeitos do armamento dos potenciais inimigos e suas respectivas FAO. As consequências máximas aceitáveis para estes cenários específicos definidas pelos critérios poderão ser, a princípio, elevadas de um nível. Ressalta-se a aceitação do aumento do nível de riscos nas condições de guerra e posição geográfica IV são apenas indicativas. Sua aplicação ao projeto somente poderia ser feita após aprovação prévia da ASN.

TABELA 4.7: OBJETIVOS DETALHADOS DE SEGURANÇA

CLASSE	CRITÉRIO D	CRITÉRIO L	CRITÉRIO T	CRITÉRIO A	CRITÉRIO P
--------	------------	------------	------------	------------	------------

SÍNTESE DE DOCTRINA DE SEGURANÇA
PARA PROJETO E OPERAÇÃO DE SUBMARINOS NUCLEARES

	Paz I-II-III	Guerra IV.	Paz I-II-III	Guerra IV.	Paz I-II-III	Guerra IV.	Paz I-II-III	Guerra IV.	Paz I-II-III	Guerra IV.
1	1		1		1		1		1	
2	2		2	3	2	3	2	3	2	3
3	3	2	3	4	3	4	3	4	3	4
4	4	3	4	C	4	C	4	C	4	C
Comple- mentar	Comple- mentar		Comple- mentar		Comple- mentar		Comple- mentar		Comple- mentar	

4.1.4 CRITÉRIO DE FALHA ÚNICA

O Critério de Falha Única (ou Simples) CFU (ou CFS) afirma que o desempenho necessário de uma sistema de segurança deverá ser obtido apesar da falha eventual de um único componente qualquer do sistema. Supõe-se que uma única falha ocorra nos sistemas de segurança projetados para mitigar os efeitos de um evento indesejável inicializador. Deve-se analisar o acidente supondo não somente uma combinação de um evento inicializador com quaisquer outras falhas que possam ocorrer como resultado direto de um evento inicializador, como também uma falha eventual de um único componente que é necessário para o desempenho de uma função de segurança que presumivelmente mitigue os efeitos de um evento inicializador.

- O conceito é aplicado aos sistemas importantes para a segurança da IPN, entendendo-se sistema como o conjunto constituído por todos os componentes através dos quais uma determinada função é realizada.
- O conceito refere-se à capacidade de um sistema de segurança como um todo, após a falha de um componente qualquer, e não a cada um dos sub-sistemas necessários ao desempenho da função do sistema.
- O critério de falha única aplica-se ao sistema de segurança e não a cada um dos sub-sistemas, mesmo se cada um desses sub-sistemas for capaz por si só de realizar a função do sistema.

Os sistemas aos quais deve ser aplicado o CFU são aqueles necessários para garantir o funcionamento seguro do reator na partida, operação em potência, desligamento e a manutenção das condições de desligamento sob todas as CPIN. Exemplos de sistemas aos

quais é aplicado o critério são: o sistema de proteção, o sistema de remoção de calor residual, o sistema de resfriamento de emergência, o sistema de remoção de calor da contenção, o sistema de isolamento da contenção, o sistema de controle da atmosfera interna da contenção e o sistema de água de resfriamento.

- O CFU não é aplicável aos sistemas cujo funcionamento é requerido somente em condições operacionais da IPN (CPIN-1 e CPIN-2).
- Para os sistemas cujo funcionamento deve ser garantido em condições acidentais (CPIN-3 e CPIN-4), o CFU deve ser incorporado no projeto pelo uso de redundância, diversidade, independência, segregação física ou, quando for necessário, através do fornecimento de sistemas de segurança específicos.
- O CFU não é aplicável às CPIN com nível de conseqüência 4b pelo critério D.
- O CFU não é aplicável aos sistemas cujo funcionamento é requerido somente em condições acidentais complementares (CPIN-complementar).
- O CFU é aplicado de forma determinística, devendo ser usado na projeto de sistemas em associação aos demais critérios de segurança.

As falhas únicas devem ser postuladas para os componentes ativos e passivos que atuam durante a evolução dos ABP. Ao realizar a análise de falha única, a falha de um componente passivo, projetado, produzido, inspecionado e mantido em serviço em um nível de qualidade extremamente elevado, poderá não ser considerada. Entretanto, quando se supõe que um componente passivo não falha, essa abordagem analítica deve ser justificada, levando-se em conta o período total de tempo, após o evento inicializador, em que o componente é necessário.

O CFU é aplicado não só ao componente do sistema de segurança, como também às alimentações deste componente, tais como energia elétrica, hidráulica, pneumática, água de resfriamento. Nos casos em que um sistema de segurança não tem uma fonte de alimentação específica, ou quando uma determinada fonte supre mais do que um sistema de segurança, estas fontes devem ser consideradas como um sistema de segurança em separado, devendo o CFU ser a ele aplicado.

4.2 CONDIÇÕES DE PROCESSO E SITUAÇÕES DE OPERAÇÃO

4.2.1 CONDIÇÕES DE PROCESSO DA INSTALAÇÃO NUCLEAR

Entende-se como CPIN os cenários operacionais inicializados ou cujo estado final é determinado pela IPN. Como apresentado em 4.1, são designadas CPIN às 4 classes de situações operativas, conforme suas FAO e níveis de consequências. Esta classificação de ocorrências deve ser considerada como um critério de projeto.

A Análise de Segurança deve então demonstrar, através de evidências objetivas, que a frequência e as consequências de qualquer ocorrência não são maiores do que aquelas que correspondem à classe dentro da qual está designada. As particularidades do projeto de uma IPN específica podem indicar a necessidade de alterações, tanto em frequência como em consequências, dos critérios de classificação apresentados.

4.2.1.1 Condições de Processo Classe 1

Os cenários CPIN-1 são aqueles cuja ocorrência é freqüente ou regular durante a operação normal da Instalação, recarga de combustível e manutenção. Deste modo, as situações CPIN-1 são acomodadas dentro das margens entre os parâmetros de funcionamento e o valor limite para estes parâmetros que implicam ações automáticas ou manuais de proteção.

Como estas situações são freqüentes ou regulares, elas devem ser consideradas do ponto de vista de sua influência sobre as consequências das situações incidentais e acidentais (CPIN-2, CPIN-3 e CPIN-4). Sob este aspecto, a análise destas últimas situações deve ser baseada em condições iniciais correspondendo às condições mais adversas que podem ocorrer durante a operação em situações CPIN-1.

São apresentadas a seguir as CPIN-1 definidas *a priori*:

- a) Regime Estacionário e Condições de Partida e Parada
 - i. Operação em potência sob controle automático, entre 20% e 100% da potência térmica nominal, com temperatura média entre a entrada e saída do reator constante;
 - ii. Operação em potência sob controle manual, entre 0% e 20% da potência térmica nominal, com temperatura média entre a entrada e saída do reator proporcional ao nível de potência e $k_{ef} > 0,99$;
 - iii. Parada a quente, com o reator subcrítico ($k_{ef} < 0,99$), temperatura média correspondente ao nível de potência 0% e sistema de remoção de calor residual isolado;

- iv. Desligamento a quente, com o reator subcrítico ($k_{ef} < 0,99$), temperatura média inferior àquela correspondente ao nível de potência 0% e sistema de remoção de calor residual em operação;
- v. Desligamento a frio, com o reator subcrítico ($k_{ef} < 0,99$), com pressão e temperatura mínima;
- vi. Recarga, com o reator subcrítico ($k_{ef} < 0,95$), tempo do reator removido, sistema na pressão atmosférica e carga de combustível no interior do vaso

b) Operações com desvios permitidos

Alguns desvios autorizados pelas especificações técnicas da Instalação podem ocorrer durante a operação continuada e são considerados em conjunção com as demais situações de operação. Estes desvios incluem:

- i. Operação com componentes ou sistemas fora de serviço, tal como uma das bombas de circulação de água de resfriamento do circuito primário;
- ii. Pequenas falhas no encamisamento do combustível;
- iii. Presença de radioatividade na água de resfriamento:
 - Produtos de fissão;
 - Produtos de corrosão ativados;
 - Trítio.
- iv. Operação com pequenos vazamentos pelos tubos dos geradores de vapor
- v. Testes específicos

c) Transientes operacionais

- i. Aquecimento e resfriamento;
- ii. Variação de carga em degraus;
- iii. Variação de carga em rampa;
- iv. Rejeição total de carga na potência máxima nominal;

4.2.1.2 Condições de Processo Classe 2

No pior caso, as situações de operação CPIN-2 devem resultar no desligamento automático do reator, com a Instalação sendo capaz de retornar à operação num intervalo de tempo relativamente curto. Por definição, estas situações não deverão se propagar de modo a conduzir a Instalação a uma situação de categoria superior (CPIN-3 ou CPIN-4). Adicionalmente, as situações CPIN-2 não deverão resultar em falhas no encamisamento do combustível nem em sobrepressão no circuito primário e no circuito secundário. São apresentadas a seguir situações de operação CPIN-2 definidas *a priori*:

- a) mau funcionamento do sub-sistema de água de alimentação dos geradores de vapor do circuito secundário causando redução da sua temperatura;

- b) mau funcionamento do sub-sistema de água de alimentação dos geradores de vapor do circuito secundário causando aumento da sua temperatura;
- c) aumento excessivo na vazão de vapor no sub-sistema de vapor vivo do circuito secundário;
- d) abertura inadvertida de uma válvula de alívio e segurança de um gerador de vapor causando a despressurização do sub-sistema de vapor vivo do circuito secundário;
- e) redução total da demanda de carga externa;
- f) desligamento automático (*trip*) de uma ou mais turbinas;
- g) fechamento inadvertido de uma válvula principal de bloqueio de vapor no sub-sistema de vapor vivo do circuito secundário;
- h) queda de vácuo nos condensadores principais do circuito secundário;
- i) perda de alimentação elétrica normal;
- j) perda da vazão normal de água de alimentação dos geradores de vapor;
- k) perda parcial da vazão de água de resfriamento do circuito primário;
- l) retirada descontrolada de um banco de elementos de controle na condição do reator subcrítico ou a baixa potência (partida/parada);
- m) retirada descontrolada de um banco de elementos de controle na condição do reator em potência;
- n) desalinhamento de um elemento ou todo um banco de controle, considerando sua queda total ou parcial até a base do núcleo;
- o) partida de bombas de um “loop” inativo do circuito primário a uma temperatura incorreta;
- p) mau funcionamento de sistemas conduzindo a uma redução na concentração de veneno solúvel (ácido bórico) diluído na água de resfriamento do circuito primário;
- q) operação inadvertida do sistema de resfriamento de emergência do reator durante funcionamento em potência;
- r) mau funcionamento de sistemas conduzindo a injeção de refrigerante no circuito primário, aumentando o inventário de água de resfriamento;
- s) abertura inadvertida de uma válvula de alívio e segurança do pressurizador;
- t) falha em tubulações de pequeno diâmetro transportando água de resfriamento do circuito primário para fora da contenção.

4.2.1.3 Condições de Processo Classe 3

Por definição, as situações CPIN-3 decorrem de falhas cuja probabilidade de ocorrência ao longo da vida útil da Instalação é muito pequena e que podem resultar em danos no encamisamento do combustível. Neste caso, a Instalação somente poderá voltar a operar após intervalo de tempo relativamente longo, requerido para os necessário reparos. A liberação de radioatividade nestas situações não deverá ser suficiente para interromper ou restringir o uso público de áreas além da área de exclusão em torno da Instalação. Uma situação CPIN-3 não deverá propagar-se de modo a conduzir a Instalação a uma situação CPIN-4, nem conduzir à perda das funções básicas de segurança de resfriamento do combustível e de contenção. São apresentadas a seguir situações de operação CPIN-3 definidas *a priori*:

- a) pequenas falhas em tubulações de vapor do circuito secundário;
- b) perda total da vazão de água de resfriamento do circuito primário;
- c) desalinhamento de um elemento ou todo um banco de controle, considerando sua retirada total ou parcial até o topo do núcleo com o reator na potência máxima nominal;
- d) carregamento e operação inadvertida de um elemento combustível numa posição imprópria;
- e) perda de água de resfriamento primário devido a ruptura de tubulações de pequeno diâmetro ou a trincas em tubulações de grande diâmetro, com atuação do sistema de resfriamento de emergência;
- f) falha ou vazamentos em vasos de pressão contendo rejeitos gasosos;
- g) falha ou vazamentos em vasos de pressão contendo rejeitos líquidos.

4.2.1.4 Condições de Processo Classe 4

As situações de categoria CPIN-4 decorrem de falhas extremamente improváveis de ocorrerem durante a vida útil da Instalação, mas que são postuladas devido ao fato de suas consequências poderem incluir liberações de materiais radioativos potencialmente significativas. O projeto da Instalação deverá então limitar estas liberações para o meio-ambiente a valores que não provoquem um aumento inaceitável nos riscos sanitários incorridos pelo público. Uma falha simples que conduza a Instalação a uma situação CPIN-4

não deve ter como consequência a perda das funções de sistemas necessários à mitigação das consequências do acidente, incluindo o resfriamento de emergência e a contenção. São apresentadas a seguir situações de operação CPIN-4 definidas *a priori*:

- a) ruptura total na tubulação principal de vapor do circuito secundário;
- b) ruptura total na tubulação principal de água de alimentação de um gerador de vapor;
- c) travamento do rotor de uma bomba de circulação de água de resfriamento do circuito primário;
- d) espectro de acidentes de ejeção total de um elemento de controle;
- e) ruptura de tubos dos geradores de vapor;
- f) acidentes de perda de água de resfriamento do circuito primário resultantes do espectro de rupturas postuladas para o envelope estanque do circuito primário;
- g) acidentes de manuseio de combustível irradiado.

4.2.1.5 Condições de Processo Complementares

As situações de categoria CPIN-Complementar decorrem de falhas adicionais àquelas consideradas pelo critério de falha simples, tendo como consequência a perda das funções de sistemas necessários ao controle das CPIN-4. Nestas condições, a função básica de segurança de Contenção pode ser comprometida em diferentes graus, dependendo da sequência particular de eventos considerada. São apresentadas a seguir CPIN-Complementares típicas, para as quais devem ser desenvolvidos procedimentos operacionais especiais e Planos de Emergência:

- a) transiente operacional CPIN-1 ou CPIN-2 seguido de perda total do Circuito Secundário, perda total de água de alimentação de emergência e das válvulas de alívio de pressão dos geradores de vapor;
- b) perda total de energia elétrica após um acidente de grande perda de refrigerante primário;
- c) perda do subsistema de injeção de emergência durante o período de resfriamento a longo prazo após um acidente de pequena perda de refrigerante primário;
- d) ocorrência simultânea de um grande APRP e de ruptura total na tubulação principal de vapor do circuito secundário no interior da Contenção

4.2.2 SITUAÇÕES OPERACIONAIS DO SUBMARINO

Entende-se como SOS os cenários operacionais inicializados ou cujo estado final é determinado pelo submarino. De modo similar às CPIN, são designadas SOS às 4 classes de situações operativas, conforme suas FAO e níveis de consequências. Esta classificação de ocorrências deve ser considerada como um critério de projeto. A Análise de Segurança deve então demonstrar, através de evidências objetivas, que a frequência e as consequências de qualquer ocorrência não são maiores do que aquelas que correspondem à classe dentro da qual está designada. Especificidades do projeto do submarino podem indicar a necessidade de alterações, tanto em frequência como em consequências, dos critérios de classificação apresentados.

4.2.2.1 Situações Operacionais do Submarino Classe 1

As SOS-1 incluem situações de ocorrência freqüente, planejadas ou não, como:

- a) Operação submerso, sob propulsão nuclear;
- b) operação submerso, sob propulsão auxiliar (baterias);
- c) operação na superfície, sob propulsão nuclear;
- d) operação na cota periscópica, sob propulsão nuclear;
- e) operação em *hovering* (velocidade nula), sob propulsão nuclear ou auxiliar (baterias)
- f) operação na superfície, sob propulsão auxiliar diesel-elétrica (esnorquel);
- g) operação na cota periscópica, sob propulsão auxiliar diesel-elétrica (esnorquel);
- h) operação atracado;
- i) operação fundeado;
- j) manobras táticas;
- k) parada brusca (manobra de *crash*)
- l) provas de Cais e de Mar;
- m) teste de Imersão a Grande Profundidade IGP;
- n) embarque e desembarque de armas, munição e combustível ;
- o) manobras com aeronaves de asa móvel (helicópteros);
- p) estados de mar extremos (base probabilística anual).

4.2.2.2 Situações Operacionais do Submarino Classe 2

As SOS-2 incluem situações pouco frequentes não planejadas que ocorrem durante operação normal, ou procedimentos especiais planejados executados durante operação anormal, como:

- a) perda total de um dos bordos do Circuito Secundário;
- b) perda temporária do sistema elétrico de serviço principal;
- c) perda temporária do sistema de governo ou do aparelho de suspender;
- d) alagamentos, dentro da capacidade de bombeamento do sistema de esgoto;
- e) fechamento inadvertido das válvulas de casco das tubulações do sistema de resfriamento principal dos condensadores do Circuito Secundário;
- f) fechamento inadvertido das válvulas de casco da tubulação de resfriamento do sistema de circulação de água do mar para resfriamento de outros componentes que não os condensadores principais;
- g) abertura inadvertida das válvulas do sistema de desvio de vapor para os condensadores principais
- h) falha do sistema de vácuo dos condensadores principais
- i) falha de um componente de controle do Circuito Secundário, como reguladores das turbina ou controladores de água de alimentação ou de vazão de vapor;
- j) fechamento inadvertido das válvulas de bloqueio de vapor;
- k) fechamento inadvertido das válvulas de bloqueio de água de alimentação dos geradores de vapor;
- l) travamento na posição aberta das válvulas garganta de alimentação das turbinas de propulsão;
- m) falhas no sistema de lubrificação ou nos mancais das turbinas;
- n) falhas no sistema de selagem das turbinas;
- o) falha do pré-aquecimento da água de alimentação;
- q) estados de mar extremos (base probabilística decenal);

4.2.2.3 Situações Operacionais do Submarino Classe 3

As SOS-3 incluem situações acidentais cuja verossimilhança é remota, como:

- a) encalhe ou pouso no fundo sem perda da fonte fria (água do mar), assumindo que o submarino permanece intato, com banda e trim de respectivamente 30^0 e 10^0 ;
- b) alagamento acima da capacidade de bombeamento do sistema de esgoto;
- c) colisão fora da região do compartimento do reator;
- d) incêndio ou explosão que não afetem diretamente o compartimento de reator;
- e) estados de mar extremos (base probabilística secular);
- f) perda total da linha de eixo;
- g) travamento dos hidroplanos;
- h) choque com o fundo a baixa velocidade.
- i) falha do sistema de remoção de calor residual externo durante docagem;
- j) perda total da alimentação elétrica externa quando atracado ou docado;
- k) detonação da carga explosiva mínima para ocorrência de um modo de falha da estrutura do casco resistente a 50m do submarino operando em sua profundidade máxima de operação (vide item 4.2.3).

4.2.2.4 Situações Operacionais do Submarino Classe 4

As SOS-4a cobrem situações cuja probabilidade é extremamente remota e nas quais algumas fontes de energia estão disponíveis no submarino, como:

- a) encalhe ou pouso no fundo com perda intermitente da fonte fria (água do mar), assumindo que o submarino permanece intato, com banda e trim de respectivamente 45^0 e 15^0 ;
- b) estados de mar extremos (base probabilística milenar);
- c) queda de aeronave de asa móvel (helicóptero) de baixa altura (duas vezes a altura da vela), fora da área do compartimento do reator;
- d) colisão seguida de incêndio ou explosão a bordo do submarino, no outro navio envolvido ou nas proximidades, sem falha da Contenção;
- e) movimentação do núcleo do reator;
- l) choque com o fundo a velocidade elevada;
- m) alagamento do compartimento do reator;

- n) detonação da carga explosiva mínima para ocorrência de um modo de falha da estrutura do casco resistente a 50m do submarino operando a 50% de sua profundidade máxima de operação (vide item 4.3.3).

As SOS 4b incluem situações cuja probabilidade é extremamente remota mas que seriam acompanhadas por uma perda total de todas as fontes de energia, como:

- a) afundamento em águas profundas fora da plataforma continental, sem falha imediata da contenção;
- b) afundamento em águas rasas, dentro da plataforma continental, porém a distância de segurança do litoral, sem falha imediata da contenção;
- c) encalhe com perda intermitente da fonte fria (água do mar), assumindo que o submarino permanece intato, com banda e trim de respectivamente 45^0 e 15^0 ;
- d) incêndio descontrolado, obrigando ao abandono do submarino.

4.2.2.5 Situações Operacionais do Submarino Complementares

As situações de categoria SOS-Complementar decorrem de acidentes de origem naval tendo como consequência a perda de funções básicas de segurança. Nestas condições, a Contenção pode ser comprometida em diferentes graus, dependendo da seqüência particular de eventos considerada. São apresentadas a seguir SOS-Complementares típicas, para as quais devem ser desenvolvidos procedimentos operacionais especiais e Planos de Emergência:

- a) afundamento em águas profundas fora da plataforma continental, com falha imediata da contenção;
- b) afundamento em águas rasas, dentro da plataforma continental, a distância superior à distância de segurança do litoral, com falha imediata da contenção;
- c) afundamento em águas rasas, dentro da plataforma continental, a distância inferior à distância de segurança do litoral, sem falha imediata da contenção;
- d) colisão na região do compartimento do reator, a distância superior à distância de segurança do litoral, com falha imediata da Contenção, ;

- e) queda de aeronave de asa móvel (helicóptero) de baixa altura (duas vezes a altura da vela), sobre o compartimento do reator, a distância superior à distância de segurança do litoral;
- f) emborcamento ou banda superior a 45°;
- g) perda total da fonte fria (água do mar);

4.2.3 CRITÉRIOS GERAIS DE ANÁLISE

As CPIN e SOS devem ser inicialmente submetidas a avaliações probabilísticas, de modo a verificar o atendimento às faixas de FAO definidas *a priori*, confirmando assim sua classificação para um projeto de SNA específico. Confirmadas as classificações, as CPIN e SOS devem ser submetidas a uma análise determinística de modo a demonstrar que suas consequências máximas estão dentro do critério geral de aceitabilidade. As hipóteses principais feitas para as avaliações probabilísticas e para a análise determinística, assim como os resultados obtidos, devem ser apresentados na Análise de Segurança e devem ser refletidos no projeto do submarino e de sua IPN.

A análise das CPIN e SOS deve ser aprovada pela ASN e deve incluir, pelo menos:

- Hipóteses feitas com relação aos eventos inicializadores, condições iniciais e ações corretivas consideradas como não sendo efetivas, se houverem;
- Descrição das contramedidas efetivas, incluindo detalhes de sistemas e componentes cujo funcionamento é inicializado pelo sistema de proteção e outras ações tomadas pelos operadores;
- Descrição resumida dos métodos de análise empregados, incluindo dados experimentais, testes de modelos e protótipos, modelos físicos e matemáticos, e códigos computacionais utilizados;
- Hipóteses e bases teóricas para o cálculo de consequências radiológicas (por exemplo atividade liberada dos elementos de combustível, atividade específica do refrigerante primário, fatores de deposição, eficiência de filtragem, taxas de vazamento, fatores de dispersão e fatores de dose);
- Parâmetros para o cálculo dos fatores de dispersão (por exemplo altura da fonte e condições meteorológicas prevaletentes);

- Descrição da sequência de eventos do cenário operacional postulado, incluindo uma apresentação analítica de suas consequências;
- Medidas adotadas para prevenir falhas em modo comuns de sistemas de segurança.

As hipóteses para inicialização dos cenário e sucessão de eventos devem estar baseadas nos seguintes princípios:

- Os sistemas de remoção de calor residual para ocorrências operacionais antecipadas e após acidentes de perda de refrigerante, o sistema de remoção de calor da contenção, a alimentação do sistema de resfriamento em emergência, o sistema de proteção do reator, e qualquer outro sistema de segurança de reator, assim como seus sistemas de suporte, devem executar suas funções dentro do Critério de Falha Única;
- Analisando um determinado sistema de segurança, a falha única de cada componente deve ser assumida em associação com o evento inicializador. Erros de operador que causem falhas de um componente ou sistema também devem ser considerados, tanto como evento inicializador ou como causa de uma falha postulada;
- Os subsistema de segurança redundantes que não satisfazem o critério de falha única não devem ser considerados como disponíveis, mesmo que o reparo de uma de suas partes durante operação de reator seja prevista pelos Procedimentos Operacionais;
- Os dispositivos automáticos de proteção do reator devem atuar na ocorrência de um evento inicializador de CPIN/SOS-3/4. Onde a ação do operador for necessária, deve ser assumido que não será executada até 30 minutos após o evento inicializador e não deve contornar a atuação dos sistemas de proteção. Deve ainda ser demonstrado que, até onde praticável, a IPN permanece segura no caso de indisponibilidade da tripulação; e
- A análise de acidentes deve considerar uma margem adequada de segurança onde os resultados de eventos estudados não podem ser previstos com certeza.

Na avaliação das consequências de acidentes, os aspectos a longo prazo também devem ser considerados, e refletidos no projeto. Estes aspectos devem incluir:

- continuidade das funções básicas de segurança;
- danos progressivos;
- capacidade dos bancos de baterias para geração de energia em emergência;

- disponibilidade de combustível fóssil para geração de energia em emergência.

4.2.4 ANÁLISE DAS CONDIÇÕES DE PROCESSO DA INSTALAÇÃO NUCLEAR

As condições de processo da IPN que criam riscos para o pessoal a bordo do submarino, o público ou o ambiente devem ser classificadas sob uma CPIN apropriada. Os principais ABP devido aos quais é provável que ocorra liberação de materiais radioativos para o interior do submarino e ambiente são, *a priori*:

- Acidentes de Ruptura dos Tubos dos Geradores de Vapor ARTGV, com o potencial de liberarem materiais radioativos para o interior do submarino, através do vazamento de fluido refrigerante do Circuito Primário para o Circuito Secundário e deste para o ambiente interno do submarino, e para o ambiente, através do alívio de pressão dos GV para o mar;
- Acidentes de Perda de Refrigerante Primário APRP, com o potencial de liberarem materiais para o interior do submarino e ambiente, através de pequenos vazamentos de fluido refrigerante da Contenção intacta e de eventuais operações de alívio de pressão e recirculação de água de resfriamento de emergência.

Os materiais radioativos liberados pelos ARTGV para o ambiente tendem a ser inferiores, a princípio, àqueles potencialmente liberados pelos APRP. Os materiais radioativos liberados pelos APRP para o interior do submarino tendem a ser inferiores, a princípio, àqueles potencialmente liberados pelos ARTGV.

As falhas do reator, máquinas ou equipamentos que podem causar uma CPIN-2, CPIN-3 ou CPIN-4 devem ser analisadas conforme as condições gerais apresentadas em 4.2.3. Os seguintes eventos em particular devem ser analisados e os resultados apresentados na Análise de Segurança:

- retirada de uma única barra de controle ou de um qualquer grupo de barras de controle movidas por um acionamento ou controle comum, começando a partir de qualquer posição, incluindo condições a quente e a frio, com o núcleo do reator crítico ou subcrítico, independente de seu nível de potência;
- vazamento de refrigerante primário por tubos defeituosos nos geradores de vapor para o Circuito Secundário, considerando o fechamento das linhas de vapor e de água de alimentação após transferência de atividade; as taxas de dose no compartimento de

máquinas devem ser avaliadas e apresentadas na Análise de Segurança e no Manual de Operação;

- ejeção de uma única barra de controle ou de um grupo qualquer de barras de controle movidas por um acionamento ou controle comum, considerando a condição inicial mais desfavorável de potência ou distribuição de potência, e de inserção de reatividade;
- travamento de uma única barra de controle ou de um grupo qualquer de barras de controle movidas por um acionamento ou controle comum, em qualquer localização no núcleo no mais desfavorável estado de queima do combustível;
- falha no acionamento ou controle de uma única barra de controle ou grupo de barras de controle qualquer;
- partida inadvertida de uma única bomba de circulação de refrigerante primário qualquer, ou de mais que uma, se isto é possível, devido à ocorrência de uma falha;
- injeção de água fria no Circuito Primário na vazão máxima possível, a partir de sistemas de controle volumétrico, purificação, resfriamento de emergência, ou outra fonte existente;
- elevação súbita de pressão no Circuito Primário resultante de eventos como fechamento de válvulas de bloqueio de vapor, rejeição de carga de uma ou mais turbinas, manobras ou outras causas;
- redução não intencional da concentração de veneno solúvel no núcleo, caso este seja empregado na IPN;
- falha dos controladores de potência do reator;
- perda da fonte fria;
- acidentes de perda de refrigerante;
- vazamento de refrigerante primário de um tanque de armazenamento, ou por gaxetas, válvulas ou selos nas tubulações associadas;
- transientes operacionais antecipados sem desligamento automático do reator.

Os eventos de perda da fonte fria devem incluir:

- rejeição total de carga de todas as turbinas;
- falhas do condensador principal, sem recurso de condensadores auxiliares;

- falha de uma bomba de alimentação, fechamento de uma linha de alimentação ou outro evento de falha dentro do sistema de alimentação dos geradores de vapor;
- falha de uma rota de transmissão de calor quando o submarino está atracado ou docado, sem turbinas em operação.

Os APRP devem ser analisados conforme as seguintes condições:

- uma ruptura deve ser assumida em qualquer parte da tubulação que forma parte da barreira de pressão primário, até aquela de maior diâmetro, mas não incluindo os bocais do vaso de pressão do reator;
- a vazão de perda de refrigerante pela ruptura postulada deve ser consistente com uma ruptura instantânea em guilhotina, exceto quando pode ser mostrado, à critério da ASN, que existem restrições físicas suficientes para limitar o movimento das extremidades rompidas, ou são implementados outros meios para prevenir tal tipo de ruptura;
- o APRP é considerado, *a priori*, como o pior ABP, que define envelope de conseqüências da Base de Projeto, devendo incluir as seguintes providências:
 - os limites de projeto da estrutura e dos sistemas da Contenção do compartimento do reator não devem ser excedidos e a pressão de projeto deve considerar uma margem suficiente com respeito à pressão calculada;
 - as conseqüências radiológicas devem estar conforme os ODS;
 - o núcleo deve ser mantido dentro de uma geometria que possibilite seu resfriamento;
 - os elementos de combustível devem poder resistir às cargas térmicas e mecânicas a eles impostas, assegurando seu resfriamento e que o número de falhas do encamisamento do combustível é aceitável com respeito aos ODS;
 - caso sejam implementados sistemas passivos de redução de pressão, injeção de refrigerante ou resfriamento de emergência, sua operação não deve ser prejudicada por qualquer atitude de submarino resultante dos estados de mar assumida no projeto do submarino para SOS-1 e SOS-2.
- uma análise específica deve ser realizada para determinar o número de falhas de tubos dos geradores de vapor que reduziriam significativamente a vazão de injeção de refrigerante, avaliando seu efeito sobre o desempenho do resfriamento em emergência do núcleo

- As seguintes condições iniciais ou de contorno adicionais devem ser consideradas em análises de APRP:
 - um subsistema resfriamento de emergência do núcleo falha, assumindo-se que não poderá voltar a operar;
 - um segundo subsistema resfriamento de emergência do núcleo está ligado ao trecho de tubulação rompido, não injetando refrigerante no vaso de pressão do reator;
 - reparos, manutenção ou testes em serviço de um terceiro subsistema resfriamento de emergência do núcleo devem também ser considerados, caso estas atividades sejam previstas e autorizadas pela ASN;
 - a atuação automática dos sistemas de segurança do reator deve ser capaz de desligar o reator e mantê-lo num estado seguro durante pelo menos 30 minutos após um evento inicializador;
 - o projeto deve ser tal que um operador pode ativar os sistemas de proteção e de segurança mas não pode contornar a ação dos sistemas automáticos;
 - somente os sistemas que são especialmente projetados para as condições de APRP continuam operando.

A perda de vapor secundário ou água de alimentação como consequência de uma ruptura em guilhotina postulada da linha a vapor principal ou linha de alimentação principal dos geradores de vapor fora ou dentro da Contenção deve ser tratada como um ABP, se necessário. Em todo caso, o efeito sobre o reator deve ser avaliado e descrito na Análise de Segurança.

A falha de um componente ativo ou erro de operação deve ser considerado para os sistemas de processamento de rejeitos radioativos e não deve prejudicar a função de segurança do sistema, mesmo no caso de ocorrência de CPIN-3 ou CPIN-4.

O efeito de uma falha que envolve qualquer componente essencial dos sistemas de geração e distribuição de potência elétrica deve ser analisado. A perda total da alimentação elétrica principal deve ser considerada um ABP.

4.2.5 ANÁLISE DAS SITUAÇÕES OPERATIVAS DO SUBMARINO

Apesar das proteções implantadas contra efeitos de colisão, os seguintes princípios devem ser adotados para analisar os acidentes navais do submarino:

- O submarino suporta a máxima extensão dos danos de colisão e encalhe postulados pelo capítulo 5. Todos os equipamentos sujeitos a danos de penetração e localizados em compartimentos alagados são considerados como inoperantes. Os equipamentos projetados e qualificados para operação sob condições de alagamento podem ser considerados como operantes, contanto que possa ser demonstrado a continuidade de suas alimentações de energia;
- Para cenários de afundamento em águas rasas, é assumido que o submarino encontra-se com o reator desligado, em uma profundidade igual ao diâmetro máximo de seu casco. A estrutura de contenção não se encontra alagada, exceto se forem implementados dispositivos especiais para inundação nesta profundidade. Os dispositivos de equalização das pressões hidrostáticas da estrutura de Contenção podem não operar e o submarino pode repousar em ângulos determinados por uma análise específica aprovada pela ASN, ou nos ângulos máximos postulados;
- O afundamento em águas profundas deve ser considerado um ABP e, como um mínimo, os critérios básicos de segurança I e III, apresentados pela subseção 4.3.3 devem ser satisfeitos. A contenção dos materiais radioativos deve ser efetivamente mantida durante um período de tempo suficientemente longo para assegurar que não ocorrerá nenhuma liberação significativa por:
 - manutenção de pelo menos uma significativa barreira estrutural ao redor das fontes altamente radioativas, com suficiente estanqueidade e resistência à corrosão;
 - manutenção de uma geometria de núcleo passível de resfriamento por meios passivos, mesmo se o núcleo for danificado.
- As fases transientes do afundamento de submarino devem considerar os seguintes aspectos
 - As hipóteses de comportamento durante o afundamento devem ser fisicamente realistas e uma margem razoável para erro deve ser aplicada aos cálculos da velocidade vertical (vide modelo sugerido pelo Anexo N);
 - pode ser assumido que o reator é desligado antes do naufrágio do submarino, mas não completamente despressurizado;

- a atividade liberada pelo submarino naufragado deve ser avaliada assumindo que o fechamento dos dispositivos de equalização de pressão da estrutura de Contenção têm falhas de isolamento após sua operação, permanecendo neste estado indefinidamente; e
- cargas de choque horizontais que são o resultado de colisões e encalhes devem ser determinadas por análises específicas e as conclusões refletidas pelo projeto.

Os potenciais efeitos do emborcamento do submarino devem ser analisados, verificando-se o atendimento dos critérios básicos de segurança, particularmente a garantia de manutenção do núcleo num estado subcrítico e da transmissão do calor residual para o mar, sendo os resultados apresentados na Análise de Segurança.

As situações de encalhe e pouso no fundo do submarino devem ser analisadas, considerando:

- perda de circulação de água do mar por bloqueio das caixas de mar localizadas no fundo e nas laterais do casco;
- encalhe em localização sensível aos movimentos de marés, com perda total intermitente de circulação de água do mar;
- determinação das inclinações máximas do submarino encalhado ou pousado no fundo.

A análise de incêndios e explosões a bordo deve ser realizada conforme as seguintes condições:

- o incêndio se origina de uma única fonte e ocorre em qualquer compartimento que contenha substâncias inflamáveis;
- a análise deve mostrar que existem proteções estruturais e sistema de detecção e combate a incêndios suficientes para assegurar que os sistemas e equipamento de segurança do reator são protegidos adequadamente;
- devem ser considerados os efeitos de deflagração ou explosão de materiais embarcados no submarino não associados à IPN e a análise destes eventos postulados deve demonstrar que a segurança do reator não será prejudicada;
- eventos de colisão seguidos de explosão ou incêndio devem ser analisados e os efeitos sobre a segurança da IPN de incêndios de longa duração devem ser considerados.

Os efeitos de mísseis gerados por falhas estruturais de válvulas e acessórios de tubulações pressurizadas, de máquinas rotativas ou de outras fontes, assim como de efeitos de chicoteamento e de jatos fluidos decorrentes de rompimento de tubulações pressurizadas devem ser analisados com respeito à segurança da IPN, considerando particularmente falhas em modo comum devidas a estes efeitos.

Até onde praticável, os efeitos de ondas de pressão decorrentes de explosões, dentro e nas proximidades do submarino, deve ser analisado em detalhes para mostrar que a estrutura de Contenção protege fontes radioativas adequadamente. A avaliação deve considerar a reação hidroelástica do submarino submetido a tais ondas de pressão. Os cenários típicos de explosão submarina devem ser postulados e seu efeitos analisados em relação à segurança da IPN. Para definição destes cenários, deve ser considerado que:

- fixada uma distância padrão D do casco resistente do submarino ao ponto da detonação (*a priori* 50m), a carga explosiva mínima M_r (definida em termos de kg de TNT) capaz de provocar um modo de falha da estrutura do casco é uma função da resistência residual P_r , definida pela diferença entre a profundidade na qual ocorre a explosão e a profundidade de cálculo do colapso do casco, segundo o seguinte modelo genérico (vide Figura 2.11):

$$M_r = D / (c \cdot P_r^k) \quad [4.1]$$

onde c e k são constantes experimentais

- os carregamentos sobre os itens internos ao casco resistente devidos à explosão de M_r são tanto mais severos quanto é maior P_r , i.e. quanto menor a profundidade em que ocorre a explosão;
- devem então ser postulados no mínimo dois cenários: explosão de M_r na profundidade máxima de operação, que corresponde, em geral, a 50% de P_r , e explosão de M_r à profundidade na qual, de acordo com o conceito de emprego do SNA, ele operará a maior parte de seu tempo no mar, que corresponde, em geral, a 25% de P_r , i.e. 50% da profundidade máxima de operação.

Uma proteção específica contra choque de aeronave não deve ser considerada no projeto do submarino, exceto se for pretendido que ele opere com helicópteros. A análise de quedas de aeronave sobre o submarino deve assegurar que o choque resultante e o eventual incêndio subsequente não comprometam as funções básicas de segurança da IPN.

Os efeitos de fumaça e gases tóxicos originados por fontes internas ao SNA devem ser analisados, demonstrando-se a continuidade da operação segura do submarino e da IPN. Devem ser implementados meios para impedir que a fumaça e os gases tóxicos penetrem a ECM e demais estações de controle no submarino.

As conseqüências prováveis de condições ambientais extremas para a operação segura do submarino e da IPN devem ser avaliadas.

O projeto deverá considerar dispositivos e procedimentos de segurança física adequados à proteção do submarino contra ações de sabotagem, desvio de materiais radioativos, ou outros atos criminosos que possam prejudicar a segurança da IPN.

4.3 CRITÉRIOS DE PROJETO

4.3.1 ÁREAS DE MOBILIDADE E AS LOCALIZAÇÕES FIXAS PRÉ-DEFINIDAS

Com referência às condições fundamentais para operação do SNA, para atracação, fundeio e navegação em zonas portuárias civis, atracação e fundeio em local protegido, navegação em águas costeiras, definidas pelos princípios específicos apresentados pelo item 3.3.1, os seguintes valores de referência devem ser considerados:

- I. “período de tempo de exposição contínua”: pela própria propulsão de emergência ou com auxílio de rebocadores do porto, 2 horas deverão ser suficientes para evacuação do submarino acidentado para “local protegido”; no caso de condições desfavoráveis de navegação (mau tempo, congestionamento do porto), 6 horas deverão ser suficientes;
- II. “curta distância”: 50 m
- III. “longa distância”: 250 m
- IV. “distância de exclusão”: 250 m
- V. “distância de evacuação”: 750 m
- VI. “distância de segurança”: 12 milhas náuticas

As doses de radiação incidentes sobre um indivíduo posicionado nestes limites devem ser inferiores aos valores apresentados pela Tabela 4.8, no caso de ABP, e pela tabela 4.9, no caso de acidente severo.

TABELA 4.8: DOSES EM CASO DE ACIDENTE BÁSICO DE PROJETO

Ponto e Tempo de Exposição	Dose sobre a Tireóide	Dose Corpo Inteiro	
		γ_{nuvem}	γ_{direto}
50 metros 6 horas	100 mSv	0,02 mSv	0,1 mSv
250 metros 6 horas	10 mSv	0,04 mSv	0,06 mSv
250 metros 30 dias	100 mSv	0,008 mSv	0,01 mSv

TABELA 4.9: DOSES EM CASO DE ACIDENTE SEVERO

Ponto e Tempo de Exposição	Dose sobre a Tireóide	Dose Corpo Inteiro	
		γ_{nuvem}	γ_{direto}
250 metros 24 horas	250 mSv	1 mSv	0,4 mSv
750 metros 24 horas	250 mSv	0,8 mSv	0,01 mSv
750 metros 30 dias	450 mSv	0,8 mSv	0,8 mSv

4.3.2 DESCOMISSIONAMENTO E PERDA DO SUBMARINO

O descomissionamento do SNA pode ser intencional ou não intencional, temporário ou final. O descomissionamento intencional se refere a situações onde a organização operadora ou a ASN considera que, por segurança ou qualquer outra razão, o submarino não deve ser mantido em serviço. O descomissionamento não intencional acontece quando uma fortuna do mar ou outra causa fortuita torna o submarino ou sua IPN imprópria para serviço.

No caso de descomissionamento temporário, ou durante a fase inicial do descomissionamento final, a organização operadora deve tomar medidas de monitoramento e de segurança adaptadas à redução dos riscos potenciais, tanto de origem nuclear como de outras origens, específicos ao estado atual do submarino e de sua IPN. O pessoal de apoio em terra responsável pelo monitoramento e segurança deve ter a autoridade e materiais

necessários para controlar qualquer incidente de origem interna ou externa que envolva o submarino ou sua IPN.

As operações diretamente ou indiretamente associadas com o descomissionamento intencional ou planejado do SNA devem satisfazer os princípios, critérios e requisitos de segurança para proteger o pessoal de apoio em terra, o público e o ambiente de riscos inaceitáveis que podem ser causados pelo submarino após sua IPN estar desligada em caráter definitivo.

A possibilidade de descomissionamento não intencional, devido a fortunas do mar, incidentes de origem interna ou externa, atos de sabotagem, operações de guerra ou qualquer outra causa não intencional, deve ser considerada durante o projeto do submarino. Onde apropriado, devem ser implementadas medidas para prevenir sua ocorrência ou limitar suas consequências.

Em cenários operacionais onde a segurança naval do submarino é gravemente comprometida, a segurança nuclear passa a constituir o objetivo principal tanto a curto como a longo prazo. As possíveis consequências radiológicas do afundamento do submarino dependerão do nível de potência no qual a IPN esteve operando anteriormente, da sequência particular de eventos que conduz ao naufrágio, e da posição final do casco naufragado, devendo ser limitadas pelos ODS. O afundamento também afeta:

- a continuidade das alimentações de energia e de refrigerante da IPN; e
- a possibilidade de controle operacional dos dispositivos de segurança.

A viabilidade de recuperar o casco naufragado ou partes dele deve ser considerada no projeto onde isto for tecnicamente possível. A identificação e a vigilância do naufrágio deve ser garantida, até onde praticável, por tempo indefinido.

4.3.3 CLASSES DE SEGURANÇA E CLASSES DE PROJETO

Para assegurar uma segurança adequada durante todas as CPIN e SOS, devem ser observados três critérios básicos de segurança:

- I. Devem ser providos meios adequados para proteger fontes radioativas e minimizar o potencial para liberação de materiais radioativos, de forma que as exposições a bordo, do público e do ambiente sejam mantidos tão reduzidas quanto razoavelmente praticável.
- II. Devem ser providos meios para remover seguramente calor residual do núcleo do reator.
- III. Devem ser providos meios para controlar e desligar o reator seguramente, mantendo-o neste estado o tempo que for necessário.

As seguintes funções de segurança são geralmente necessárias para satisfazer os critérios acima, podendo porém ser necessário complementar estas funções em casos de projetos particulares.

As funções de segurança necessárias ao atendimento do critério I são:

- Manter, como a primeira barreira, uma integridade aceitável do encamisamento do combustível no núcleo de reator;
- Manter, como a segunda barreira, a integridade do envelope estanque do Circuito Primário;
- Prevenir e limitar uma liberação não intencional de material radioativo da estrutura de contenção, como a terceira barreira;
- Prevenir e limitar uma liberação não intencional de material radioativo da estrutura do submarino, como a quarta barreira.

As funções de segurança necessárias ao atendimento do critério II são:

- Transferir o calor residual do núcleo do reator para uma última fonte de resfriamento;
- Manter um inventário suficiente de água de resfriamento para o núcleo; e
- Prover as alimentações e serviços de apoio necessários ao funcionamento dos sistemas de segurança.

As funções de segurança necessárias ao atendimento do critério III são:

- Controlar adequadamente a reatividade do núcleo;
- Tornar o reator subcrítico, sem exceder as limites de projeto do combustível especificados; e
- Prover as alimentações e serviços de apoio necessários ao funcionamento dos sistemas de segurança.

Deve ser definida para cada item uma classe de segurança, fundada na importância das conseqüências da perda da função executada. Os requisitos para materiais, projeto, construção, testes, inspeções e operação devem refletir a classificação de segurança determinada. A distribuição típica de classes de segurança é apresentada a seguir como uma orientação geral e não constituindo-se num critério propriamente dito.

A Classe de Segurança 1 (CS-1) aplica-se aos seguintes itens:

- Sistema de Proteção e Desligamento do reator;
- O vaso de pressão do reator e componentes da (ou dentro da) barreira de pressão do Circuito Primário e estruturas de suporte do núcleo cujo falha poderia causar uma CPIN 3 ou 4. Os componentes conectados ao sistema de resfriamento do reator e formando parte da barreira de pressão podem não ser designados como CS-1, contanto que:
 - Para as falhas postuladas do componente durante operação normal, o reator possa ser desligado e resfriado adequadamente, considerando-se que a água de resfriamento perdida é repostada exclusivamente pelo sistema de controle volumétrico empregado na operação normal da Instalação; ou
 - O componente é, ou pode ser, isolado do sistema de resfriamento de reator através de duas válvulas. Cada válvula aberta deve ter fechamento automático. O tempo de fechamento deve ser tal que, no caso da falha do componente postulada durante operação normal, cada válvula permanece operável e o reator pode ser desligado e resfriado adequadamente; e
- O casco do gerador de vapor e tubulações principais, incluindo as válvulas de isolamento das linhas de vapor e água de alimentação.

A Classe de Segurança 2 (CS-2) aplica-se aos seguintes itens:

- Componentes da barreira de pressão não cobertos pela CS-1;
- Estrutura de Contenção e seus sistemas de segurança,
- Componentes, sistemas ou subsistemas necessários para:
 - Remover o calor residual do núcleo na ocorrência de CPIN 2, 3 ou 4;
 - Controlar a radioatividade liberada dentro da estrutura de Contenção;
 - Controlar o teor de hidrogênio na atmosfera interna da Contenção após um acidente de perda de refrigerante;
 - Resfriar o núcleo em emergência (Sistema de Resfriamento em Emergência SRE, incluindo alimentação elétrica em emergência, acumuladores, tanques de água de resfriamento, etc.);

- Resfriar a contenção ou reduzir a pressão no seu interior após um acidente de perda de refrigerante;
- Repor o inventário de água de resfriamento do reator, como uma função de segurança; e
- Assegurar qualquer outra função que pode resultar de importância semelhante para segurança;
- Alimentação de energia do sistema de proteção de reator;
- Acionamento das barras de controle e sistemas de alimentação e apoio associados;
- Sistema de purificação da atmosfera interna da estrutura de Contenção, incluindo as partes deste sistema externas à estrutura de contenção, que atuam como uma extensão do seu envelope estanque durante recirculação do ar;
- Proteção contra sobrepressão do Circuito Primário e sistemas de alívio, não cobertos pela CS-1; e
- Como determinado pela ASN e registrado na Análise de Segurança, outros equipamentos do submarino que afetam a IPN e cuja falha poderia causar diretamente uma CPIN-3.

A Classe de Segurança 3 (CS-3) aplica-se aos seguintes itens:

- Qualquer sistema, componente ou estrutura de segurança da IPN não coberto pelas CS-1 ou CS-2;
- .Sistemas auxiliares que dão suporte ao funcionamento de sistemas de segurança, tais como: sistemas de óleo lubrificante, sistemas hidráulicos, circuitos de resfriamento de água do mar, sistemas de ar comprimido, e sistemas de óleo combustível para geradores elétricos de emergência;
- Circuitos de resfriamento de água do mar cumprindo funções de segurança exigidas para satisfazer o critério II; e
- Sistemas que não são de segurança mas cuja falha resultaria em um liberação inaceitável para o interior do submarino ou para o ambiente de material radioativo gasoso que normalmente seria retido para decaimento, tais como sistemas de processamento de rejeitos e circuitos de purificação de água de resfriamento do Circuito Primário.

A Classe de Segurança 4 (CS-4) aplica-se aos seguintes itens:

- Vapor secundário e sistemas de água de alimentação que formam parte do sistema de remoção de calor e são localizados fora da estrutura de Contenção, além da segunda

válvula de isolamento, contanto que um sistema alternativo redundante e independente seja disponível para remover o calor residual;

- Turbinas e condensadores, incluindo turbo-geradores alimentados pela IPN não cobertos por CS-1, 2, ou 3, quando possuem funções de remoção de calor;
- Estruturas do submarino não cobertas por CS-2 ou CS-3;
- Outros equipamentos do submarino cuja falha poderia causar uma CPIN-2 diretamente;
- Outros componentes de IPN não cobertos por CS-1, 2 ou 3.

A classe de segurança deve ser definida através de avaliação caso a caso de cada sistema, componente e estrutura, explicitamente determinada na Análise de Segurança, e devidamente aprovada pela ASN.

Dentro de cada classe de segurança, a todo sistema ou componente deve ser atribuída uma classe de projeto apropriada e variando de CP-1 a CP-4. Cada classe de projeto define padrões específicos de projeto, fabricação e garantia de qualidade que é proporcional aos efeitos da falha do sistema ou componente na segurança do submarino.

As Classes de Projeto não necessariamente correspondem numericamente às Classes de Segurança.

A Classe de Projeto 1 (CP-1) requer aplicação dos padrões mais altos de projeto e garantia de qualidade, e incluindo os seguintes critérios:

- Para componentes pressurizados, os requisitos de projeto devem ser baseados nas seguintes considerações:
 - Condições de carregamento, incluindo,:
 - . Carregamentos de pressão permanentes;
 - . Carregamentos de pressão transitórios durante manobras, desligamento ou partida;
 - . Flutuações de pressão devido a forças inerciais causadas pelos movimentos extremos de plataforma do submarino para todos os estados de mar considerados pela base de projeto;
 - . Cargas térmicas permanentes e transitórias;
 - . Forças dinâmicas que surgem de acidentes de perda de refrigerante, agindo na barreira de pressão de Circuito Primário, suas estrutura internas e estruturas de suportes;

- . Forças dinâmicas causadas pelo chicoteamento de tubulações numa ruptura em guilhotina;
- . Forças dinâmicas que surgem de qualquer outro acidente postulado pelas CPIN-3 e CPIN-4, assim como pelas SOS-3 e SOS-4;
- . Efeitos de vibração induzida pelo submarino;
- . Forças inerciais devidas aos movimentos de submarino no mar.;
- . Operação permanente do submarino com uma banda de até 30°, jogo de até 45°, trim e caturro de até 10°, assim como em qualquer combinação de ângulos dentro desses limites. Estes ângulos podem ser reduzidos se for demonstrado que o submarino não passa por tais atitudes extremas, caso em que a redução deve ser aprovada pela ASN;
- . Assegurar sua integridade em todos os ângulos de inclinação;
- Análise de tensões detalhada, identificando flexões e tensões locais máximas sob as condições de carregamento acima definidas;
- Análises de resposta, com respeito aos carregamentos dinâmicos de movimentos no mar, acidentes de ruptura de tubulações, ação de válvulas de fechamento rápido, e vibrações forçadas induzidas por fontes do submarino;
 - . Fatores de amortecimento relativamente baixo devem ser assumidos;
 - . Onde puder ser demonstrado que nenhum efeito de ressonância significativo é possível, a análise de resposta para vibrações do submarino pode ser dispensada, com aprovação da ASN;
- Análises detalhadas do comportamento com respeito à fratura frágil e dúctil, análise de fadiga e propagação de trincas e avaliação de margens para falhas aceitáveis, incluindo os efeitos da radiação;
- Na seleção de materiais;
 - . suficientemente alta resistência e ductilidade;
 - . valores demonstrados de mecânica da fratura;
 - . conhecimento das taxas de crescimento de trincas;
- Ensaios extensivos dos materiais para demonstrar as propriedades referidas acima com supervisão do OSTI;
- Estruturas e componentes de bombas e motores pressurizados que são altamente solicitados, i.e. cujas tensões principais tendem ao valor máximo admissível, devem permitir ensaios não destrutivos irrestritos, durante inspeções periódicas, para detectar e monitorar falhas e trincas na sua superfície e volume;
- As estruturas pressurizadas devem;
 - Ser soldadas com penetração total;
 - Ter estruturas de suportes, bocais e tubulações integrados com o casco;
 - Ter reforços adequados nas aberturas e flanges para manter as tensões de projeto;

- Ser, de forma geral, projetadas e construídas conforme procedimentos bem estabelecidos e possuírem a mais alta qualidade.
- Outros componentes CP-1 não pressurizados devem ser projetados e construídos dentro de especificações proporcionais a sua importância para segurança, aprovadas pela ASN.

A Classe de Projeto 2 (CP-2) requer um alto padrão de projeto e de garantia de qualidade, incluindo:

- Os carregamentos aplicados a estruturas pressurizadas e sua suportaço, e para componentes de mquinas cuja tenso principal tende ao valor mximo de tenso admissvel, deve incluir a soma das influncias estticas e dinmicas devido a variveis de processo e aos movimentos do submarino no mar. Como um requisito mnimo, as aceleraes normais devem ser complementadas por fatores de carga para cobrir outros efeitos dinmicos;
- A anlise de tenses, onde necessrio, deve seguir normas e critrios pertinentes. Normalmente, os escantilhes devem seguir requisitos especficos da ASN, ou de organizaes devidamente reconhecidas pela ASN. As tubulaes devem ser analisadas para carregamentos trmicos onde as temperaturas excedem 120C e para reaes estticas presso, aplicando fatores dinmicos quando considerados carregamentos de inrcia como peso prprio e movimentos do submarino no mar.;
- Anlise de resposta para tubulaes somente precisa ser realizada onde limites de temperatura fixados por normas e critrios pertinentes so excedidos, ou naqueles casos que envolvem condies acidentais particulares que requerem a demonstrao da confiabilidade de componentes;
- A seleo, testes e inspees de materiais devem seguir os requisitos para caldeiras e vasos de presso que so estabelecidos pela ASN ou por organizaes devidamente reconhecidas pela ASN;
- O projeto e procedimentos de construo devem seguir a experincia geral em projeto de vasos de presso e tubulaes para submarinos, seguindo as exigncias para vapor a alta temperatura estabelecidos pela ASN ou por organizaes devidamente reconhecidas pela ASN; e
- A estrutura de conteno deve ser projetada para resistir:

- pressão e variações de temperatura que surgem de um acidente de perda de refrigerante, combinadas com tensões devidas a movimentos de submarino no mar;
- diferenças de pressão que ocorrem durante o afundamento do submarino e diferenças de pressão devido à subsequente inundação da estrutura de contenção a uma temperatura de 4°C.

A Classe de Projeto 3 (CP-3) deve corresponder aos mesmos padrões de projeto aplicados a caldeiras e tubulações de vapor de emprego naval, devendo seguir critérios estabelecidos pela ASN ou por organizações devidamente reconhecidas pela ASN.

A Classe de Projeto 4 (CP-4) deve seguir padrões internacionais e nacionais para projeto, construção e testes, considerando as forças inerciais que agem nos componentes.

4.3.4 CONDIÇÕES AMBIENTAIS

As condições meteorológicas, a densidade de população e o uso de terra locais, devem ser considerados na análise de consequências da operação do SNA nas localizações fixas pré-determinadas. Os resultados obtidos devem ser apresentados na Análise de Segurança.

Como requerido pelas várias CPIN e SOS, o projeto do SNA e de sua IPN deve considerar os efeitos de eventos naturais extremos, como estados de mar, tornados, tsunamis, furacões, ventos, neve e gelo, aplicáveis às áreas de mobilidade e localizações fixas pré-determinadas.

As forças inerciais que agem no submarino nos diferentes estados de mar aplicáveis às áreas de mobilidade devem ser analisadas com respeito às classes de segurança. Esta análise deve examinar o movimento do submarino nos seis graus de liberdade e deve utilizar o espectro de ondas para as áreas principais e secundárias de operação.

Os componentes e estruturas devem ser capazes de resistir às forças inerciais calculadas para características de estado de mar determinadas nas bases probabilísticas apresentadas pela Tabela 4.10.

TABELA 4.10: ESTADOS DE MAR DE PROJETO

Classe de Segurança	Base Probabilística
---------------------	---------------------

CS-1	Secular
CS-2 CS-3	Decenal
CS-4 Casco e equipamentos e máquinas não cobertos por normas internacionais e nacionais	Anual

Os carregamentos impulsivos decorrentes de fortunas do mar (colisão, encalhe, choque com o fundo), de explosões submarinas e de queda de aeronaves de asa móvel ou outros objetos pesados manipulados durante operações de manutenção sobre os componentes da IPN devem ser considerados no projeto.

Devem ser considerados os movimentos do submarino no mar para avaliação da estabilidade do controle do reator e para avaliação do seu comportamento dinâmico, assumindo-se as características de estado de mar decorrentes da Tabela 4.10.

Os sistemas de segurança e suas fontes de energia devem ser projetados para operar sem continuamente quando o submarino está experimentando uma banda estática de até 30° ou ângulos de jogo e de caturro de até, respectivamente, 45° e 10° , assim como qualquer combinação de ângulos dentro desses limites. Um único movimento não excedendo 45° para um bordo não deve causar um mau funcionamento ou sobrecarga mesmo se ele ocorre durante uma ação de desligamento de emergência. Estes ângulos podem ser reduzidos se puder ser demonstrado que o submarino não experimenta tais atitudes extremas, caso em que a redução deve ser justificada na Análise de Segurança aprovada pela ASN.

Para projeto de sistemas de condicionamento de ar para áreas controladas e equipamentos eletrônicos de sistemas de segurança, devem ser assumidos valores extremos de umidade relativa.

Os efeitos de vapores de óleo de máquinas, poeira, fumaça e gases tóxicos no caso de incêndio originado pelos sistemas do SNA externos à IPN ou do ambiente devem ser considerados no projeto.

Os efeitos de vibrações induzidas pelo propulsor e máquinas devem ser considerados e, onde necessário, refletidos no projeto e testes de dispositivos de monitoramento, sistemas e componentes de controle.

4.3.5 INSTALAÇÃO PROPULSORA NUCLEAR

A IPN deve ser projetada para operar satisfatoriamente sob as condições navais, considerando-se as condições ambientais apresentadas no item 4.3.4. A IPN deve ser projetada para limitar os carregamentos mecânicos cíclicos decorrentes de efeitos de vibração, choque e condições acidentais.

Os seguintes critérios governam a operação da IPN durante as diversas condições de processo (CPIN):

- O reator deve ser plenamente operável e nenhum sinal de desligamento automático deve ocorrer como resultado de uma CPIN 1;
- As ocorrências CPIN-2 devem permitir reiniciar a operação do reator, eventualmente a potência reduzida, dentro de um intervalo de tempo razoável, sem redução da segurança;
- As ocorrências CPIN-3 podem requerer o desligamento do reator;
- As ocorrências CPIN-4, como condições limitantes, não devem resultar em riscos inaceitáveis para o público ou o ambiente, nem exceder os limites de liberação de materiais radioativos estabelecidos no item 4.1.2;
- As doses de radiação para a tripulação, pessoal de apoio em terra e público em geral decorrentes de ocorrências CPIN-1, 2 ou 3 devem ser mantidas tão baixas quanto razoavelmente praticável e dentro dos limites apropriados estabelecidos no item 4.1.2.

A IPN deve ser capaz de responder às demandas de potência pelo menos tão rapidamente quanto uma instalação de turbina a vapor convencional de porte e potência semelhantes. Deve também ser capaz de ser ligada sem ajuda externa a partir de uma condição de desligamento.

A potência máxima desenvolvida no regime de marcha a ré e taxa de variação de carga dos geradores de vapor e das turbinas devem ser analisadas para demonstrar que o

submarino tem uma razoável capacidade de parada em emergência, i.e. a distância percorrida da condição toda força a vante até a condição de velocidade nula é relativamente pequena.

Os sistemas, componentes e estruturas da IPN, de CS-1 a CS-4 devem ser projetados e construídos de forma a permitir testes adequados de suas condições e funções. Onde estão sujeitos a carregamentos mecânicos, térmicos ou de pressão, sua resistência também deve ser testada.

Deve ser possível realizar testes da capacidade funcional dos sistemas de resfriamento do reator em emergência e de remoção de calor residual, e do sistema de proteção de reator. Os testes realizados com o reator em operação e com o Circuito Primário pressurizado não devem interromper o desempenho de funções de segurança, reduzir o nível de redundância de qualquer sistema abaixo do mínimo exigido, ou prejudicar uma eventual operação do sistema necessária durante sua execução.

5 REQUISITOS ESPECÍFICOS

Neste capítulo serão formulados os requisitos específicos de segurança aplicáveis ao projeto de estruturas, componentes e sistemas da IPN e da plataforma-navio do SNA. Estes “Requisitos Específicos” são entendidos como regras quantitativas que determinam o projeto individual de cada parte que compõe o SNA. Devem ser considerados de forma a garantir o atendimento aos Critérios Gerais, estes últimos aplicados ao conjunto dos sistemas.

Os Requisitos Específicos são propostos a partir da análise crítica dos requisitos de projeto empregados para reatores eletrônicos e para submarinos convencionais, ampliada e sintetizada pela experiência já acumulada no País ao longo do desenvolvimento do projeto de um SNA nacional.

Serão inicialmente abordados aspectos “integrais” (Garantia da Qualidade, Proteção Radiológica, Operação, Inspeções e Testes) e em seguida são tratados os aspectos de projeto particulares aos sistemas da Plataforma-Navio do SNA, de sua IPN propriamente dita (Reator e Circuito Primário), de suas máquinas principais e auxiliares, e de suas instalações elétricas.

5.1 GARANTIA DA QUALIDADE

Como uma pré-condição, necessária para aprovação da construção de um submarino nuclear pela ASN, um Programa de Garantia da Qualidade PGQ, cobrindo todo o ciclo de vida do submarino deve ser desenvolvido, documentado e implementado de forma a assegurar o atendimento aos princípios básicos, critérios gerais e requisitos específicos de segurança.

O PGQ deverá detectar não-conformidades e cobrir todas as atividades desde a concepção até a disposição final, incluindo as fases de projeto, desenvolvimento, obtenção, transporte, armazenagem e testes de componentes, construção, comissionamento, condução da operação, procedimentos operacionais, manutenção, reparos e inspeções, e descomissionamento.

A implementação do PGQ deverá assegurar que todas as atividades e materiais obedecem os documentos de projeto, procedimentos escritos e instruções e que a efetividade

do próprio PGQ é auditada. Uma descrição completa do PGQ deve ser incluída na Análise de Segurança para aprovação da ASN antes do efetivo início do processo de obtenção do SNA. Os requisitos específicos do PGQ devem assegurar que:

- uma estrutura organizacional encontra-se claramente estabelecida, identificando as responsabilidades pelo programa ao longo do ciclo de vida do SNA;
- o controle de toda a documentação é mantido ao longo do ciclo de vida do SNA;
- todos os requisitos especificados são efetivamente implementados;
- os materiais e procedimentos são compatíveis com o nível de qualidade requerido, que corresponde às classes de segurança e de projeto atribuídas ao componente ou sistema;
- as propriedades dos materiais empregados são demonstradas antes e durante a fabricação, satisfazendo as exigências das especificações aprovadas;
- o projeto, a obtenção, a fabricação, o transporte e manuseio, o armazenamento, a instalação, a manutenção, os testes e os procedimentos operacionais são compatíveis com o nível de qualidade requerido, que corresponde às classes de segurança e de projeto atribuídas ao componente ou sistema;
- os componentes e sistemas são fabricados, instalados e mantidos conforme planos, desenhos e especificações aprovadas pela ASN;
- a operação de sistemas e componentes obedece às funções a eles especificadas, particularmente com respeito às suas funções de segurança;
- todos os princípios básicos, critérios gerais e requisitos específicos, além de outras exigências da ASN são completamente satisfeitas; e
- são mantidos registros de todos os procedimentos de garantia da qualidade, planos de fabricações, inspeções e testes e decisões tomadas em casos de não-conformidade.

5.1.1 ESTRUTURA ORGANIZACIONAL

A estrutura organizacional do PGQ deve definir claramente as responsabilidades funcionais, os níveis de autoridade, as linhas de comunicação e as interfaces, onde são envolvidos arranjos organizacionais múltiplos. As responsabilidades funcionais dentro do PGQ devem incluir:

- o atendimento aos objetivos de qualidade por aqueles diretamente envolvidos na execução das atividades; e
- quando é necessária a verificação de conformidade com as especificações estabelecidas, esta é realizada por quem não têm responsabilidade na execução da atividade.

Em todas as fases do ciclo de vida do submarino, deve haver uma única autoridade identificada como responsável pela ASN global e controle do PGQ. Onde atividades são subcontratadas ou onde acontece uma transferência de responsabilidade primária, deve ser exercido efetivo controle para assegurar integração e continuidade das ações de garantia da qualidade.

5.1.2 DOCUMENTAÇÃO E REGISTROS

Devem ser estabelecidos e documentados procedimentos para controlar a preparação, revisão, aprovação, emissão, verificação e cancelamento de todos os documentos essenciais às atividades que afetam a qualidade.

Medidas de controle devem ser estabelecidas e documentadas de forma a assegurar que todas as exigências regulamentares da ASN são identificadas e corretamente aplicadas.

Devem ser mantidos registros de garantia da qualidade para todos os aspectos do PGQ. Os registros devem apresentar evidência objetiva de controle da qualidade e devem incluir dados sobre revisões, inspeções, testes, auditorias, monitoramento do desempenho das atividades, análises de materiais, monitoramento das variáveis de operação, falhas e deficiências, reparos e outros dados apropriados. Os registros de garantia da qualidade devem ser coletados, armazenados e mantidos para futuras referências.

5.1.3 PROCEDIMENTOS DE CONTROLE

Os procedimentos de controle de projeto devem verificar sua adequação pelo uso de revisões independentes, métodos alternativos de cálculo, análise crítica das hipóteses e premissas assumidas e pelo desempenho satisfatório em testes. As alterações de projeto devem estar sujeitas ao mesmo nível de controle aplicado ao projeto original.

Devem ser estabelecidos procedimentos bem documentados que assegurem terem sido incluídas ou referenciadas nos documentos de obtenção de componentes e serviços

todas as exigências regulamentares aplicáveis, as bases de projeto, normas e especificações, critérios de desempenho e outros dados necessários. Materiais, equipamentos e serviços comprados devem estar sujeitos a controle para assegurar sua conformidade com as especificações de obtenção.

Uma consideração básica na avaliação e seleção de fornecedores deve ser sua capacidade para prover materiais, equipamentos e serviços que obedeçam plenamente às exigências dos documentos de obtenção.

Devem ser estabelecidas medidas para controle de materiais e equipamentos, inclusive subconjuntos pré-montados, de forma que eles possam ser identificados prontamente durante instalação e operação. Um controle de documentação associado deve estar disponível para estes itens, adaptado às fases sequenciais do processo de obtenção.

Os processos e procedimentos empregados na fabricação, manuseio, armazenagem, instalação, testes e operação de sistemas e componentes devem ser continuamente monitorados para assegurar que a qualidade originalmente verificada não é degradada.

O PGQ deve prescrever as ações requeridas para detectar, identificar e retificar quaisquer desvios que possam prejudicar o funcionamento correto de qualquer equipamento ou sistema para os quais o PGQ se aplica. Falhas, funcionamento incorreto, deficiências, desvios, materiais e equipamento defeituosos ou impróprios ou qualquer outra não-conformidade pertinente devem ser revisados e ações corretivas aprovadas devem ser implementadas.

5.1.4 TESTES

Um programa de testes aprovado deve ser estabelecido, contendo o planejamento, identificação, padrões de desempenho, procedimentos e documentação de todos os testes requeridos para garantir o atendimento das exigências do PGQ. O programa de testes deve incluir testes de qualificação de procedimentos e de equipamento, testes de qualificação de protótipos, testes prévios à montagem, testes pré-operacionais e de comissionamento, e testes em serviço. Os dispositivos de testes e de medidas usados devem ser controlados e freqüentemente calibrados para manter sua precisão dentro dos limites especificados.

O escopo dos testes de garantia da qualidade deve ser especificado, conforme necessário, para os documentos pertinentes, materiais, estruturas, componentes ou sistemas envolvidos, incluindo a qualificação do pessoal que deverá executá-los.

5.2 PROTEÇÃO RADIOLÓGICA

5.2.1 PROTEÇÃO RADIOLÓGICA NO PROJETO

A IPN e outras fontes de radiação no SNA devem ser projetadas e blindadas de forma que durante as CPIN e SOS 1, 2 e 3 todas as exposições são mantidas ALARA e, em todo caso, dentro do limite dose-equivalente pertinente. A distância e o tempo de ocupação, como também a blindagem radiológica, devem ser considerados para o controle das exposições individuais.

O projeto deve assegurar que, quando o reator está funcionando normalmente ou está desligado, nenhuma pessoa a bordo ou nas proximidades do submarino pode, como resultado da operação do submarino, estar sujeita a níveis de irradiação externa ou contaminação que excedam os limites de dose-equivalente especificados. Onde apropriado, devem ser adotados fatores de segurança na fase de projeto que propiciem margens adequadas em contingências imprevistas.

O projeto do submarino e de sua IPN deve ser tal que não há nenhum aumento significativo no nível de radiação de fundo nas áreas de mobilidade, devido à operação em CPIN e SOS 1 e 2.

O submarino deve ser dividido em áreas designadas de acordo com a magnitude real ou potencial do risco radiológico envolvido (vide Anexo M). Levando em conta a natureza do risco radiológico nas áreas controladas e supervisionadas, barreiras de acesso, equipamentos de proteção e monitoramento individual, chuveiros e vestiários devem ser localizados, conforme necessário, entre áreas controladas ou supervisionadas e áreas livres adjacentes, prevenindo a transferência de contaminação de uma área para outra. Sinais de advertência devem ser colocados à entrada para uma área controlada ou supervisionada para indicar os riscos. O acesso a uma área controlada deve ser limitado às pessoas autorizadas e as entradas e saídas devem ser registradas.

Os arranjos de proteção radiológica devem ser tais que, sob condições operacionais normal, nenhuma restrição é necessária na operação e manutenção da parte convencional do submarino. Enquanto o submarino estiver em dique seco, o acesso ao fundo do submarino deve ser limitado administrativamente.

Dentro das áreas livres deve ser esperado que, até onde seja razoavelmente exequível, as taxas de dose com o reator em potência nas CPIN 1 e 2 não excedam os valores estabelecidos pela Tabela 5.1.

TABELA 5.1: LIMITES DE TAXA DE DOSE EQUIVALENTE PARA ÁREAS LIVRES
DO SNA

ÁREA OU ESPAÇO	TAXA DE DOSE EQUIVALENTE
CENTRO DE OPERAÇÕES DE COMBATE E OUTROS COMPARTIMENTOS OPERATIVOS A VANTE DO REATOR	0,75 $\mu\text{Sv} / \text{h}$
ACOMODAÇÕES (COBERTAS, CAMAROTES, RANCHO, SANITÁRIOS)	0,15 $\mu\text{Sv} / \text{h}$
VELA E SUPERESTRUTURA	0,50 $\mu\text{Sv} / \text{h}$
COSTADO ACIMA DA LINHA D'ÁGUA	0,50 $\mu\text{Sv} / \text{h}$
FUNDO, EM FLUTUAÇÃO, COM O REATOR A BAIXA POTÊNCIA (condições de manutenção e inspeção atracado ou fundeado)	7,50 $\mu\text{Sv} / \text{h}$

O projeto deve minimizar, até onde razoavelmente exequível, a dispersão de radioatividade. Todas as partes do submarino nas quais materiais radioativos ou contaminação possam existir devem ser identificadas e medidas de projeto apropriadas devem ser tomadas para assegurar que a dispersão de materiais radioativos no ambiente ou contaminação de outras partes do submarino será minimizada e que os necessários procedimentos de descontaminação podem ser executados de forma segura, dentro dos limites de dose-equivalente pertinentes.

Particular atenção deve ser dada aos riscos potenciais de contaminação de superfícies e equipamentos. Devem ser incorporadas medidas de projeto apropriadas para minimizar as dificuldades de execução dos procedimentos de descontaminação e para permitir controle adequado dos rejeitos radioativos gerados. Irregularidades estruturais e superficiais devem ser evitadas em todos os sistemas e equipamento que contêm materiais radioativos.

O projeto da IPN e instalações associadas (inclusive a instalação de processamento de rejeitos), sua blindagem e contenção, e sua localização no submarino deve ser tal que qualquer liberação de radioatividade que surja das CPIN e SOS 1, 2 e 3 não impeça a manobra do submarino.

A dose equivalente de irradiação externa, juntamente com a dose equivalente decorrente da incorporação de radioatividade que poderia ser recebida na superfície externa do casco deve estar dentro das exigências de limite de dose para qualquer condição acidental CPIN e SOS 4.

As partes do submarino que seriam ocupadas pela tripulação durante qualquer CPIN e SOS 4 devem ser localizadas e blindadas de forma a garantir que as doses individuais do pessoal que ocupa estes espaços estaria dentro dos limites de dose, considerando toda a evolução temporal do cenário acidental.

5.2.2 PROTEÇÃO INDIVIDUAL

As doses de radiação recebidas pela tripulação, pessoal de apoio logístico em terra e membros do público em geral como resultado da operação do SNA nas CPIN-1, CPIN-2 e CPIN-3, assim como nas SOS-1, SOS-2 e SOS-3 deve ser mantidas abaixo dos limites dose-equivalente apropriados, recomendados por (ICRP, 1991), e ALARA.

A contaminação de superfícies e do ar como resultado CPIN-1, CPIN-2 e CPIN-3, assim como nas SOS-1, SOS-2 e SOS-3 deve ser mantida abaixo de limites derivados dos limites dose-equivalente pertinentes.

A base de projeto para limitação de doses recebidas pela tripulação, pessoal de apoio logístico em terra e membros do público em geral como resultado da operação do SNA nas

CPIN-4 e SOS-4 não deve exceder duas vezes o limite anual de dose-equivalente ocupacional pertinente.

A menos que explicitamente designado como “trabalhador afeto às radiações” (vide Anexo M), nenhum membro da tripulação ou qualquer outra pessoa a bordo ou que venha a permanecer nas proximidades do submarino deve ser exposto, como resultado da operação do SNA, a doses de radiação que excedam o limite dose-equivalente pertinente para membros do público em geral.

Somente os indivíduos da tripulação e do pessoal de apoio logístico em terra que normalmente trabalham dentro de áreas controladas ou supervisionadas do submarino (vide Anexo M) serão consideradas como “trabalhador afeto às radiações”.

O submarino deve ser equipado com meios suficientes de proteção individual, inclusive respiradores com filtros e dispositivos para respiração independente da atmosfera local, para lidar com as condições ambientais previstas para as CPIN-1, CPIN-2 e CPIN-3, assim como para as SOS-1, SOS-2 e SOS-3.

Devem ser estabelecidos procedimentos documentados que deverão garantir uma proteção radiológica adequada para os membros da tripulação sob todas as CPIN e SOS, incluindo:

- mapeamento sistemático e completo das áreas de trabalho antes que estes sejam efetivamente iniciados;
- planejamento das atividades e dos tempo de ocupação das áreas de radiação, assegurando que as exposições individuais à radiação são mantidas ALARA e dentro dos limites estabelecidos;
- previsão das doses individuais durante as atividades planejadas;
- seleção dos necessários dosímetros pessoais, roupas protetoras, aparelhos de respiração, e equipamento de comunicação para cada indivíduo;
- controles administrativos que evitem exposições inadvertidas a níveis de radiação elevados, tanto durante a operação como em períodos de manutenção e inspeções;
- medidas profiláticas e de descontaminação de indivíduos e de superfícies não blindadas contaminados; e

- exercício periódico regular de todos os procedimentos operacionais para controlar emergências radiológicas a bordo do submarino, incluindo as interfaces com os planos de emergência locais das instalações de apoio logístico em terra.

Nenhuma alteração em procedimentos de proteção radiológica poderá ser implementada por outro indivíduo que não o responsável especificamente designado, sendo ainda explicitamente aprovada pelo comandante do SNA.

Deve ser mantido um registro detalhado das doses individuais recebidas por cada membro da tripulação afeto a atividades em áreas de radiação. A entrada de outros indivíduos em áreas controladas e supervisionadas deverá ser feita com uso de dosímetros pessoais aprovados, devendo ser mantido também o registro destas doses.

Todo tripulante deverá ser submetido a um exame médico antes de assumir funções à bordo que envolvam exposição à radiação. Além do exame médico prévio, os tripulantes devem ser submetidos a exames médicos periódicos anuais. Deverá ser verificada a sua aptidão física aos tipos de tarefas que desempenhará, dando atenção especial aos aspectos que evidenciem radio-sensibilidades específicas. O exame médico deve incluir um registro pessoal abrangendo o histórico de exposição à radiação, antecedentes médicos de família etc. Neste exame médico, deve ser reservada uma atenção especial às evidências de câncer e catarata nos olhos. Exames laboratoriais devem incluir a análise da urina, análise do sangue e uma comparação dos constituintes sanguíneos com padrões médicos para indivíduos não expostos às radiações.

A tripulação do SNA deverá incluir pelo menos um oficial médico especializado na área de proteção radiológica / radiologia, o qual deverá ser capaz de diagnosticar e socorrer qualquer tripulante que sofra exposições acidentais à radiação.

Serão mantidos os assentamentos resultantes de levantamentos e monitoramentos radiológicos nas áreas sujeitas à radiação, bem como os assentamentos individuais, para cada tripulante. Nos assentamentos deverá constar uma série de informações, que deverão ser mantidas pelo menos por 30 anos, dentre as quais:

- dados relevantes e informações sobre a natureza geral do trabalho sujeito à radiação e o tipo da mesma;
- nível de radiação ao qual o tripulante tenha sido submetido ou presuma-se que tenha sido exposto;
- método de monitoramento utilizado (se individual ou de área);e
- resultados dos exames médicos e de monitoramento individual.

As áreas sujeitas à radiação serão monitoradas, controladas e sinalizadas. Cada acesso a essas áreas deverá ser equipado com um mecanismo de controle que faça funcionar um alarme visível ou audível, de forma que um indivíduo entrando nessas áreas tenha consciência do fato, além de dar conhecimento ao responsável pela proteção radiológica do SNA. Áreas com alto nível de radiação devem ser mantidas trancadas, existindo um controle individual de acesso a elas.

Quando o submarino nuclear é descomissionado, devem ser tomadas precauções específicas para proteger os trabalhadores, o público e o ambiente de riscos de irradiação e contaminação originados principalmente de:

- elementos de combustível e efluentes altamente radioativos;
- água de resfriamento e componentes do Circuito Primário da IPN, assim como outros circuitos de mais baixo nível de radioatividade; e
- qualquer outro rejeito radioativo que seja produzido durante o descomissionamento.

5.2.2.1 Limites de Dose

Serão considerados limites e condições diferenciados para as situações de: irradiação controlada, doses planejadas, condições de emergência e condição de acidente. Ainda dentro desta abrangência, são diferenciadas a exposição interna e a exposição externa.

Os limites estabelecidos para irradiação controlada são referentes às doses máximas permissíveis em condições normais de trabalho.

- A dose máxima permissível para o corpo inteiro, gônadas ou órgãos hematopoéticos é de 20mSv em qualquer período de 12 meses;

- Em um trimestre, a dose máxima permissível é de 10 mSv, desde que a dose total acumulada nos últimos 12 meses não tenha ultrapassado 20mSv.
- Se não for conhecida a dose previamente acumulada, admitir-se-á que o indivíduo tenha recebido, em cada ano anterior, a dose máxima permissível.
- A dose recebida pelos órgãos, excluídas as gônadas, o corpo inteiro e a medula óssea, não deverá exceder os limites apresentados pela Tabela 5.2.

TABELA 5.2: LIMITES DE DOSE PARA PARTES DO CORPO EM CONDIÇÕES DE
IRRADIAÇÃO CONTROLADA

Órgãos	Limite Trimestral (mSv)	Limite Anual (mSv)
Mãos, Antebraço, Pés e Tornozelo	400	750
Osso, Tireóide, Pele do Corpo Inteiro excluindo-se as Mãos, Antebraço, Pés e Tornozelos	150	300
Qualquer órgão isolado, excluindo-se as gônadas e os órgãos hematopoéticos	80	150

Para irradiação planejada, existirão situações nas quais serão admitidas doses acima dos limites normais, desde que de maneira planejada segundo o estipulado a seguir.

- No caso de irradiação externa planejada, as doses máximas permissíveis não poderão ultrapassar o limite anual de 50 mSv nem o limite de 100 mSv para a dose acumulada nos últimos cinco anos.
- Após uma irradiação externa planejada, o indivíduo não deverá receber doses superiores a 20 mSv por ano, de forma que a dose acumulada nos cinco anos subsequentes não ultrapasse o limite de 100 mSv.
- Um indivíduo não deverá participar de uma irradiação planejada se previamente tiver recebido, nos últimos 12 meses, uma irradiação única ou incorporação de material radioativo, com uma dose superior ao limite trimestral para irradiação controlada.

As tentativas imediatas de salvamento de vidas humanas, de evitar a exposição do público à radioatividade e de preservar a integridade do SNA são justificativas suficientes

para se tolerar uma exposição à irradiação acima dos limites em condições controladas e planejadas, denominadas irradiações de emergência. Os limites quantitativos nestes casos não podem ser especificados, mas as doses individuais devem ser compatíveis com a relevância do evento particular em questão, tornando-se necessário o treinamento específico do pessoal potencialmente envolvido em tais situações, os quais devem ter plena consciência das consequências das exposições a que podem vir a estar submetidos. Os seguintes limites devem ser considerados nestes casos:

- Doses individuais em condições de emergência, não devem exceder 100 mSv para o corpo inteiro.
- Para exposição de mãos, antebraços, pés e tornozelos em condições de emergência, um indivíduo poderá receber uma dose de 1500 mSv.
- Exposições ao nível das mencionadas acima devem ser limitadas a apenas uma vez em toda a vida.
- Em casos de ações menos urgentes, tais como combate a incêndios e alagamentos, as doses não deverão ultrapassar 50 mSv para o corpo inteiro e 750 mSv para mãos, antebraços, pés e tornozelos.

5.2.2.2 Dosimetria e Monitoramento

Sistemas de monitoramento de radiações, incorporando equipamentos fixos ou portáteis, conforme apropriado, devem estar disponíveis no submarino, indicando e registrando, onde necessário, os níveis de radiação nos ambientes interno e externo, os níveis de contaminação de superfícies e da atmosfera internas, e as concentrações e vazões de processos envolvendo materiais radioativos, devendo incluir:

- alarmes e, onde necessário, ações automáticas, se níveis predeterminados de irradiação, contaminação, concentrações ou fluxos radioativos são excedidos;
- equipamento para indicar e registrar níveis de irradiação e concentrações de atividade no Circuito Primário e Circuito Secundário, em todos os demais sistemas de bordo contendo materiais radioativos, e todas os potenciais pontos de descarga de efluentes radioativos do submarino;

- equipamentos para indicar a concentração de atividade nos fluidos de resfriamento dos componentes da IPN que estão em contato com refrigerante primário pressurizado; e
- provisão adequada de instrumentação de monitoramento reservas e instalações satisfatórias para a manutenção e calibração destes equipamentos a bordo.

A faixa de medida dos instrumentos fixos e portáteis deve permitir o monitoramento da radiação tanto durante operação normal como durante condições de acidente.

As indicações de níveis de radiação e de níveis de contaminação atmosférica nas áreas controladas devem ser transmitidas permanentemente para a ECM. O Circuito Secundário, a atmosfera no interior da estrutura de Contenção e nos compartimentos a ela adjacentes devem ser monitorados continuamente por sistemas separados, que transmitirão as respectivas indicações à ECM, alarmando qualquer aumento significativo em relação aos níveis normais.

Os dados obtidos por meio de equipamentos fixos de monitoramento devem ser complementados por dados coletados durante inspeções regulares feitas com monitores portáteis. O pessoal envolvido em tais inspeções deve ser especificamente treinado no uso dos instrumentos empregados.

Devem ser estabelecidos pontos fixos de monitoramento da radiação de forma a permitir a comparação dos níveis medidos com aqueles originalmente verificados durante o comissionamento, permitindo assim acompanhar sua evolução ao longo do ciclo de vida do submarino. Um número adequado de pontos fixos deve ser selecionado, principalmente no interior dos compartimentos da IPN, mas também fora deles, tanto no interior do submarino como em sua superfície exterior.

Os níveis de radiação devem ser verificados periodicamente a plena potência, em potências parciais e durante desligamento a frio e a quente (particularmente nas condições de atracação e fundeio), e em condições de vaso do reator aberto, com e sem combustível (particularmente nas condições de docagem). O mapeamento de fluxos de dose devem ser consequentemente revistos, sempre que necessário. Adicionalmente, as áreas normalmente

acessíveis do submarino devem ser periodicamente verificadas quanto aos níveis de contaminação.

O submarino deve ser equipado com monitores portáteis de radiação suficientes para execução das inspeções de rotina e de emergência. Este equipamento deve incluir detetores de radiação beta, gama e de nêutrons, coletores de amostras de ar, e monitores de contaminação de alfa/beta. A quantidade de dosímetros pessoais levada a bordo deve satisfazer às necessidades de serviço normal e deve ser suficiente para todo o pessoal embarcado em caso de um acidente. Além dos instrumentos mencionados, o submarino deve ser dotado de equipamento laboratorial apropriado para a análise de amostras radioativas.

Os sistemas de monitoramento e registro devem incluir:

- equipamento fixo e portátil para avaliar as concentrações e quantidades de materiais radioativos gasosos e particulados em suspensão na atmosfera interna do submarino, que potencialmente poderiam ser liberados para o meio ambiente;
- equipamento para identificar potenciais falhas nos elementos combustíveis e nos tubos dos geradores de vapor, pela conseqüente presença de materiais radioativos na água de resfriamento do Circuito Primário e no vapor/água de alimentação do Circuito Secundário;
- equipamento para monitorar e alarmar a taxa de liberação e a atividade total das linhas de descargas gasosas, particularmente as linhas de purga de incondensáveis dos condensadores principais do Circuito Secundário;
- equipamento para avaliar com uma precisão satisfatória a concentração de atividade e quantidade total de rejeitos líquidos nos respectivos sistemas de coleta, processamento e armazenamento;
- equipamento para medir e registrar as concentrações de atividade dos radioisótopos significativos contidos nos efluentes líquidos, associado a alarmes adequados e tendo a capacidade de isolamento automático das linhas de descarga para o ambiente marinho;
- equipamento para avaliar os níveis e tipos de radiação emitidos por rejeitos radioativos sólidos, previamente à sua segregação e tratamento; e

- procedimentos e equipamentos de testes e monitoramento adequados à verificação da condição operacional correta dos sistemas de processamento e armazenagem de rejeitos efluentes.

Um registro detalhado, abrangente e permanente deve ser mantido para:

- doses ocupacionais dos indivíduos expostos a radiação a bordo;
- níveis de radiação nos compartimentos internos e no exterior do submarino;
- níveis de contaminação nas áreas acessíveis do submarino;
- inventário de rejeitos radioativos gerados pela operação do submarino (sólidos, líquidos e gasosos), os tipos de processamento aplicados e as quantidades e localizações das armazenagens a bordo;
- quantidades e atividades dos efluentes radioativos descarregados pelo submarino, sua localização geográfica e data de liberação;
- estimativas da composição isotópica das descargas de efluentes, incluindo as quantidades e atividades associadas a cada um dos principais componentes;
- taxas de dose em áreas de armazenamento de rejeitos; e
- atividade da água de resfriamento do Circuito Primário e do vapor/água de alimentação do Circuito Secundário.

Procedimentos operacionais específicos devem ser implementados para garantir pronta informação à ASN no caso de lançamento accidental de substâncias radioativas no ambiente marinho acima dos limites recomendados.

5.2.3 PROTEÇÃO AMBIENTAL

5.2.3.1 Limites para Liberação de Efluentes

Os níveis de atividade dos efluentes radioativos produzidos pela operação do submarino e liberados para o ambiente em CPIN-1 e CPIN-2 devem ser tão reduzidos quanto razoavelmente praticável e dentro dos limites apresentados pela Tabela 5.3.

Note-se que estes limites restritivos são um reflexo do fato de que as necessidades operacionais de liberação são muito reduzidas e que normalmente não haverá nenhuma dificuldade em armazenar os rejeitos a bordo e descarregá-los em instalações de apoio em

terra, onde melhores meios de gerenciamento poderão ser aplicados. Os limites não devem ser interpretados como uma indicação de que descargas maiores necessariamente representariam um risco inaceitável.

O projeto deverá eliminar, sempre que praticável, eventuais necessidades de liberação de efluentes radioativos para o ambiente quando o submarino encontrar-se em porto ou base naval, atracado ou fundeado. Se tais liberações forem estritamente necessárias, elas devem ser restritas pelo limites derivados do limite anual de dose equivalente para o público estabelecidos por (ICRP, 1991).

A descarga de rejeitos sólidos e de efluentes líquidos para instalações de apoio logístico em terra deve estar conforme as condições estabelecidas pela ASN para licenciamento destas instalações e os princípios, critérios e requisitos estabelecidos pela respectiva Análise de Segurança.

TABELA 5.3: LIMITES PARA LIBERAÇÃO DE EFLUENTES NO AMBIENTE

FORMA	PORTO	ÁGUAS COSTEIRAS	ÁGUAS OCEÂNICAS
SÓLIDO	Nenhuma liberação	Nenhuma liberação	Nenhuma liberação
LÍQUIDO	Nenhuma liberação	<ul style="list-style-type: none">• Liberações anuais de atividade total inferiores a $7,4 \cdot 10^{10}$ Bq, considerando-se que estas liberações são feitas em uma única localização geográfica• Liberações anuais de atividade total inferiores a $8,9 \cdot 10^{11}$ Bq, considerando-se que estas liberações são feitas em pelo menos 12 localizações geográficas diferentes• Concentração de atividade volumétrica inferior a $3,7 \cdot 10^6$ Bq / m³, em ambos os casos	
GASOSO	Nenhuma liberação	Dentro de limites derivados do limite anual de dose equivalente para o público	

5.2.3.2 Gerenciamento de Rejeitos

O projeto da IPN e da plataforma-navio do submarino deve, até onde razoavelmente praticável, minimizar a produção durante as CPIN-1 e CPIN-2 de rejeitos e efluentes radioativos. Deve ainda possibilitar seu gerenciamento seguro, seja por armazenamento dos

rejeitos e sua disposição posterior em terra, seja por processamento dos rejeitos e liberações controladas dos efluentes decorrentes para o ambiente marinho, dentro das limitações impostas pela ASN, de forma a assegurar que o impacto ambiental da operação do SNA seja socialmente aceitável.

O projeto e a operação das instalações de armazenamento e processamento devem considerar:

- as quantidades potenciais da radioatividade gerada;
- requisitos de resfriamento e blindagem;
- possíveis efeitos corrosivos de certos líquidos e gases radioativos;
- detecção de vazamentos;
- presença e detecção de gases combustíveis, como hidrogênio; e
- providências para prevenir a explosão de gases ou líquidos combustíveis e mitigar suas consequências, caso esta venha a ocorrer.

A capacidade mínima de armazenamento de rejeitos radioativos sólidos, líquidos e gasosos deve ser compatível com o perfil de operação do submarino, devendo incluir uma margem apropriada para contingências. Esta capacidade deve considerar tanto o espectro de CPIN operacionais prováveis como também os períodos entre descargas dos rejeitos para as instalações de apoio logístico em terra.

As instalações de armazenamento e processamento de rejeitos do SNA devem ser projetadas de forma a prevenir eventuais liberações descontroladas para o ambiente marinho.

As instalações de armazenamento, processamento a bordo, descarga e transporte de materiais radioativos devem ser projetadas, construídas, operadas, mantidas e inspecionadas segundo um alto padrão, proporcional a suas implicações de segurança, de tal modo que os riscos de uma liberação descontrolada para o ambiente ou para outros compartimentos do submarino sejam aceitáveis.

Deverá ser considerada a possível necessidade de segregação de rejeitos devido a suas diferentes propriedades químicas e características radioativas, tais como atividade

específica ou conteúdo isotópico, bem como a proteção contra incêndios, no caso de rejeitos combustíveis.

5.2.3.3 Rejeitos Sólidos

As fontes típicas de rejeitos radioativos sólidos a serem consideradas são aquelas contendo radioatividade gerada pelo Reator e Circuito Primário da IPN e incluem:

- resinas de troca iônica;
- filtros; e
- itens diversos, associados a execução de atividades em áreas controladas, incluindo vestimentas de proteção e ferramentas, assim como materiais e consumíveis das análises laboratoriais de amostras.

Os rejeitos radioativos sólidos somente devem ser descarregados em instalações de apoio logístico em terra devidamente equipadas para recebê-los e nunca para o ambiente. A transferência destes rejeitos do submarino para as instalações em terra deve ser realizada conforme procedimentos de proteção radiológica específicos, assegurando que a exposição à radiação direta é minimizada e que eventuais contaminações superficiais ou do ar são evitadas.

Antes de seu armazenamento, os rejeitos radioativos sólidos devem ser segregados apropriadamente de acordo com sua atividade, tipos de radiação emitida, atividade química, combustibilidade, etc. Sistemas específicos para a redução de volume destes rejeitos poderão ser incorporados ao projeto do SNA, desde que satisfaçam os princípios básicos, critérios gerais e requisitos específicos de segurança.

As instalações de armazenamento de rejeitos radioativos sólidos devem levar em conta a possibilidade de tais rejeitos poderem conter ou poderem gerar gases ou líquidos. Onde esta possibilidade existe, os rejeitos devem ser mantidos em recipientes fechados, estanques a gases ou em tanques que podem requerer suspiros para alívio de pressão. Tais recipientes devem ser submetidos a inspeções e manutenções periódicas e equipamentos de testes adequados devem estar disponíveis para verificar sua integridade e estanqueidade. Onde um suspiro é necessário, o mesmo deve ser conectado a um sistema de armazenamento ou a uma rota de descarga aprovada pela ASN.

5.2.3.4 Rejeitos Líquidos

As instalações de coleta, processamento e armazenamento de rejeitos líquidos devem ser projetadas para atender ao volume gerado pela operação de IPN nas CPIN-1 e CPIN-2. Como exemplo de fontes geradoras, têm-se:

- aumento do volume de refrigerante primário como resultado da expansão térmica derivada das temperaturas operacionais do reator;
- vazamentos operacionais e rejeitos que se originam do Circuitos Primários e de seus sistemas auxiliares, de atividades de descontaminação de equipamentos e pessoal, lavagem de vestimentas de proteção, amostragens e outras fontes diversas; e
- atividades de inspeção, manutenção e reparo.

A descarga de grandes quantidades de rejeitos quimicamente tóxicos e radioativos que podem resultar de procedimentos de descontaminação que requerem a drenagem de sistemas contendo fluidos radioativos deve somente ocorrer junto a instalações especiais de apoio em terra que obedecem a requisitos específicos da ASN. Estas instalações devem possibilitar a transferência de rejeitos radioativos líquidos do submarino para a terra, ou para instalações flutuantes especiais, através de dois sistemas segregados, um para rejeitos de atividade mais alta e o outro para rejeitos de baixa atividade.

Os líquidos radioativos devem ser coletados e armazenados a bordo do submarino em recipientes fechados ou tanques, caso sua liberação para o ambiente exceda os limites anteriormente estabelecidos.

Os seguintes requisitos devem ser atendidos pelo projeto das instalações de processamento e armazenamento de rejeitos radioativos líquidos:

- os rejeitos devem ser segregados com base na sua natureza físico-química e características radioativas, tais como atividade específica e conteúdo de isotópico;
- devem ser previstos meios para remover resíduos sólidos (borras e incrustações) acumulados durante a operação normal dos sistemas;
- devem ser previstos equipamentos para monitoramento e tanques de decaimento, com arranjos adequados à determinação tanto do volume e atividade do seu conteúdo como também da vazão na qual este conteúdo é liberado para o ambiente ou para as instalações

de apoio em terra, cujo projeto deve permitir processamento adicional deste conteúdo, se for necessário;

- as linhas de descarga e transferência dos rejeitos e efluentes radioativos líquidos devem ser dotadas de dispositivos de isolamento automáticos, de forma a prevenir liberações inadvertidas ou descontroladas;
- a capacidade dos tanques de armazenamento deve ser suficiente para reter todos os drenos localizados em outras áreas controladas, sob as condições CPIN-1 e CPIN-2; e
- arranjos adequados de resfriamento e blindagem devem ser previstos para as instalações de processamento e armazenamento de rejeitos líquidos.

5.2.3.5 Rejeitos Gasosos

Os rejeitos radioativos gasosos gerados pela IPN que requerem gerenciamento são os seguintes:

- ativação pelo fluxo neutrônico do refrigerante primário e de suas impurezas e aditivos químicos;
- escape de produtos de fissão gasosos e voláteis de elementos combustíveis defeituosos; e
- ativação direta por nêutrons da atmosfera interna da estrutura de Contenção.

Devem ser previstos meios para controlar todas eventuais rotas de descarga pelas quais os rejeitos radioativos gasosos poderiam alcançar os compartimentos do submarino e ambiente. As fontes de descarga típicas incluem:

- vazamentos de refrigerante primário;
- desaeração do Circuito Primário;
- desaeração do Circuito Secundário, particularmente a descarga de incondensáveis dos condensadores principais;
- suspiro de tanques contendo materiais radioativos;
- alívio de pressão dos geradores de vapor; e
- alívio de pressão do volume de estrutura de Contenção.

As liberações para o ambiente devem satisfazer os limites anteriormente apresentados. Quando isto não puder ser alcançado inicialmente, os rejeitos gasosos devem ser processados

para atender aos limites de liberação ou devem ser armazenados a bordo em instalações específicas.

A compressão de rejeitos radioativos gasosos e o seu armazenamento sob pressão pode ser permitida, contanto que o projeto, construção, operação e inspeções em serviço dos vasos de armazenamento e tubulações associadas satisfaçam os requisitos anteriormente especificados. Para isto, deve ser demonstrado por análise que a falha de um vaso de armazenamento não conduziria a uma condição inaceitável. Os possíveis riscos decorrentes do armazenamento e compressão de gases combustíveis também devem ser analisados.

A concentração de atividade dos efluentes gasosos liberados para o ambiente deve ser controlada e, se necessário, devem sofrer diluição de forma que a concentração de atividade máxima permissível não seja excedida. As linhas de descarga devem ser dotadas de capacidade de isolamento automático para prevenir liberações inadvertidas ou descontroladas.

Deve ser possível a monitoração da atividade ou do nível de radiação, conforme apropriado, nas áreas de armazenamento.

5.2.3.6 Ventilação e Filtração

Uma combinação eficiente de arranjos de ventilação e de filtração deve ser prevista para:

- manter a concentração de atividade no ar interno aos espaços habitáveis dentro dos limites derivados;
- permitir a capacidade de purga do ar interno à estrutura de Contenção; e
- prevenir a disseminação descontrolada de contaminação pelos compartimentos do submarino.

A exaustão do ar interno da estrutura de Contenção e a ventilação dos compartimentos adjacentes deve ser devidamente monitorada, alarmada e filtrada, levando a um ponto de descarga, projetado de forma a evitar a contaminação de normalmente áreas habitadas e a acumulação de materiais radioativos nas linhas de descarga.

A ventilação e a filtração do ar interno à estrutura de Contenção deve ser completamente independente dos sistemas que servem os compartimentos habitados do submarino.

As exaustões de áreas controladas e supervisionadas devem ser monitoradas continuamente e os respectivos fluxos de ar devem passar por filtros de alta eficiência, com elevada capacidade de separação, testados para remover, no mínimo, 99,95 % de partículas de tamanho semelhante ao existente na fumaça de cigarros. Além disso, deverão ser empregados filtros de carvão ativado de alta eficiência na remoção de radioisótopos.

5.3 OPERAÇÃO

Os seguintes requisitos específicos aplicam-se à operação do SNA:

- O fato de sua propulsão ser nuclear não implicará em nenhuma prioridade particular com respeito às regras gerais de navegação na superfície, i.e. serão aplicáveis ao SNA as mesmas regras aplicáveis a submarinos convencionais;
- Sempre que houver combustível nuclear carregado no núcleo do reator, a IPN deverá ser supervisionada por pessoal qualificado, mantendo um serviço de quarto contínuo na ECM;
- Todo o trabalho requerido a bordo do submarino que envolva a manipulação e disposição de materiais radioativos gasosos, líquidos ou sólidos, ou ainda qualquer outra possibilidade de ocorrência de contaminação imprevista, só deverá ser realizado de acordo com procedimentos operacionais específicos, que deverão estabelecer os locais e equipamentos apropriados e assegurar um controle adequado das exposições à radiação decorrentes;
- Além do combustível nuclear carregado no núcleo do reator, nenhum material físsil, deverá ser embarcado no submarino;
- Sob condições operacionais normais (CPIN-1), a IPN deve poder ser ligada rapidamente, elevando-se prontamente seu nível de potência a um nível mínimo capaz de assegurar uma navegação segura. O sistema de propulsão convencional em emergência, deve estar pronto para uso quando o submarino encontra-se em portos ou águas costeiras;
- A IPN somente poderá funcionar em modos operacionais previstos no Manual de Operação aprovado pela ASN; e

- O efetivo de lotação, o treinamento, as qualificações e a formalização da certificação de oficiais e tripulantes devem ser aprovados pela ASN e deverá ser suficiente para a operação segura do submarino em todas as CPIN e SOS.

A organização operadora sendo responsável pela operação segura do SNA e de sua IPN, deve assegurar que:

- A operação é conduzida estritamente dentro das condições autorizadas pela Análise de Segurança e pelo Manual de Operação;
- A operação é conduzida por pessoal qualificado, devidamente certificado conforme as normas estabelecidas pela ASN;
- Os oficiais e a tripulação são permanentemente treinados e adestrados para a correta aplicação e execução dos procedimentos operacionais;
- O submarino deverá estar disponível para receber inspetores da ASN sempre que encontrar-se em porto ou base naval; e
- As atividades de manutenção e reparo são realizadas por pessoal especificamente treinado para sua execução.

O comandante, oficiais e demais membros da tripulação devem ser submetidos a processos formais de certificação de suas qualificações e serem permanentemente submetidos a treinamento apropriado às suas responsabilidades e deveres, conforme normas específicas da ASN.

A estrutura organizacional do SNA deverá incluir uma divisão especificamente responsável pela proteção radiológica a bordo. Esta divisão deverá ser composta por um número adequado de membros da tripulação devidamente qualificados e certificados para execução das atividades de proteção radiológica previstas pelos procedimentos operacionais, que incluem monitoração de áreas e de pessoal, fornecimento e controle do uso de equipamentos de proteção individual.

A estrutura organizacional do SNA deverá incluir ainda um oficial médico e pelo menos um praça com especialização em enfermagem com função de seu auxiliar, ambos com formação específica em proteção radiológica. Este oficial médico deverá reportar-se

diretamente ao comandante do SNA e ser o responsável pelo controle das doses individuais, supervisionando a correta execução das atividades da divisão de proteção radiológica.

5.3.1 DOCUMENTAÇÃO DE OPERAÇÃO

A documentação de operação que estabelece as características específicas da construção e da operação do submarino deve ser mantida atualizada e estar permanentemente disponível à bordo do SNA para inspeção pela ASN. Ela é constituída por:

- Relatório de Análise de Segurança RAS e documentos de engenharia associados;
- Licença de Operação emitida pela ASN e detalhes dos limites e restrições operacionais por ela impostos;
- Manual de Operação;
- Certificados individuais que atestem a qualificação e o treinamento nuclear dos tripulantes;
- Planos de emergência locais;
- Registros de inspeções, testes funcionais, atividades de manutenção e reparos da IPN realizados pela tripulação desde o último período de manutenção programada; e
- Registros de proteção radiológica (controle individual de doses, monitoração de áreas), inventário de rejeitos armazenados e em processamento, inventário de efluentes liberados e inventário de material físsil embarcado.

O Manual de Operação do SNA deve apresentar todos os procedimentos necessários para o pessoal qualificado operar o submarino e sua IPN de forma segura, sob todas as condições operacionais normais e anormais (CPIN-1, CPIN-2, SOS-1 e SOS2), assim como sob as condições incidentais e acidentais (CPIN-3, CPIN-4, SOS-3 e SOS-4). Deverá também apresentar instruções para a operacionalização dos planos de emergência previstos para as CPIN e SOS complementares especificadas. São apresentados a seguir alguns dos dados que deverão ser incluídos no Manual de Operação do SNA:

- Descrição da IPN, com diagramas de sistemas e outros dados pertinentes à monitoração da radiação, equipamento de proteção radiológica, meios de prevenção e combate a incêndios, equipamentos reserva e partes sobressalentes;
- Valores nominais, valores limites e desvios autorizados das variáveis de processo para operação normal da IPN e dos sistemas associados, incluindo:
 - Tempos de permanência de pessoal em áreas de radiação;
 - Níveis de radiação em áreas críticas pré-selecionadas; e
 - Níveis de atividade nos fluidos de resfriamento do Circuito Primário e Circuito Secundário e nos rejeitos gasosos, líquidos, sólidos;
- Procedimentos operacionais para as condições normais de operação da IPN, tais como partida, transientes de potência e desligamento, incluindo dados sobre:
 - Verificação funcional dos sistemas de controle e de proteção da IPN antes da partida e durante a operação em potência;
 - Determinação da posição crítica dos elementos de controle de reator e sua reatividade integral e diferencial, assim como também o balanço de reatividade do núcleo e suas variações durante o tempo de queima; e
 - Grau de redundância mínima permissível para os sistemas de segurança da IPN e os sistemas de alimentação elétrica associados, assegurar partida e operação segura do reator. Os equipamento que estejam eventualmente sendo testados ou reparados não devem ser considerados operacionais para o propósito de determinação do grau de redundância, exceto quando o teste é realizado em um modo operacional;
- Procedimentos operacionais para as condições anormais de operação da IPN, descrevendo as ações a serem tomadas para passagem para os modos degradados de operação, sem perda de continuidade na geração de potência;
- Procedimentos operacionais para as condições incidentais de operação da IPN, descrevendo os cenários típicos de eventos e as ações de proteção e posterior recuperação da operação em modo degradado, com uma mínima perda de continuidade na geração de potência;
- Procedimentos operacionais para as condições acidentais de operação da IPN, descrevendo não somente os cenários típicos de eventos e as ações de proteção a serem tomadas, como também os meios de diagnóstico do estado atual do reator e as ações de mitigação de consequências a serem tomadas para conduzi-lo a um estado seguro;
- Planos de emergência locais para mitigar as consequências dos acidentes além da base de projeto postulados;

- Estrutura organizacional da operação do submarino, incluindo:
 - Efetivos mínimos e responsabilidades individuais sobre a proteção radiológica e segurança nuclear da IPN;
 - Norma de condução da operação pelo quarto de serviço tanto no mar como em porto;
 - Procedimentos de acesso às áreas controlada e supervisionadas, incluindo particularmente o acesso a interior do Compartimento do Reator (estrutura de Contenção);
 - Programa de exercícios e adestramentos periódicos para o pessoal envolvido na operação da IPN; e
 - Instruções para a manutenção de registros de operação da IPN, de monitoramento das condições radiológicas a bordo e para elaboração de relatórios a serem submetido à ASN em caso de eventos de falha e de ocorrência de incidentes e acidentes;
- Instruções para execução de inspeções periódicas da IPN, da estrutura de Contenção e da estrutura do casco, incluindo dados como frequência, extensão e métodos;
- Instruções adicionais para assegurar a segurança do submarino e do meio ambiente, incluindo:
 - docagem e inspeções com submarino flutuando, relativas à segurança nuclear e proteção ambiental;
 - segurança radiológica;
 - processamento e armazenamento de rejeitos radioativos sólidos, líquidos e gasosos e descargas de efluentes;
 - prevenção e combate a incêndios e controle de materiais combustíveis dentro dos compartimentos da IPN;
 - requisitos específicos relativos às interfaces da IPN com sistemas e dispositivos para manuseio de armas e munições embarcadas;
 - procedimentos administrativos que previnam a ocorrência de atividades de manutenção em componentes de segurança e proteção do reator durante testes de sistemas a eles direta ou indiretamente relacionados.

Toda a informação técnica que envolve a operação da IPN deve ser devidamente registrada nos livros de quarto apropriados do SNA, i.e. livro de quarto de operação da IPN, livro de quarto da proteção radiológica, livro de inventário de rejeitos e livro de inventário de materiais físeis, e em outro documento especificado no Manual de Operação. As seguintes informação devem ser permanentemente registradas:

- modo de carregamento do núcleo do reator e seu parâmetros principais de funcionamento;
- lista de equipamentos operacionais da IPN e o seu respectivo tempo de operação;

- verificações funcionais e ajustes dos sistemas de monitoração, controle e proteção, calibração de instrumentos e inspeções de equipamentos;
- operações envolvendo recarga do núcleo, manutenção, reparo e substituição de equipamentos, e ações de descontaminação associadas;
- ocorrência de eventos indesejados, com detalhes das ações corretivas tomadas e dos conseqüentes resultados obtidos;
- falhas e desvios do desempenho operacional normal de componentes e sistemas;
- alterações das condições operacionais e instruções dadas aos operadores autorizados para implementar mudanças nas condições de funcionamento de equipamentos;
- a condição das blindagens e outros arranjos de proteção radiológica do submarino e dados referentes à medida de níveis de radiação a bordo e nos fluidos de resfriamento do Circuito Primário e Circuito Secundário, assim como registros de qualquer contaminação identificada e das medidas de descontaminação tomadas;
- doses de radiação individuais;
- quantidade, tipo e nível de atividade dos rejeitos radioativos a bordo e dos efluentes descarregados do submarino, com dados sobre sua localização e hora/local das eventuais descargas;
- exercícios e adestramentos realizados, com informação sobre emergências radiológicas assumidas e os equipamentos utilizados; e
- qualquer desvio dos procedimentos operacionais preconizados pelo Manual de Operação.

Os planos de emergência devem estar preparados para limitar as conseqüências dos acidentes postulados para o submarino e meio ambiente. Estes planos devem considerar a ocorrência destes acidentes no mar (Plano de Emergência Interno PEI) e em porto (Plano de Emergência Local PEL).

- O PEI deverá prever, além dos procedimentos gerais aplicáveis ao caso do submarino encontrar-se em águas oceânicas, procedimentos especiais para o caso do submarino encontrar-se em águas costeiras.
- O PEL deverá prever, além dos procedimentos gerais aplicáveis ao caso do submarino encontrar-se em qualquer porto ou base naval, procedimentos especiais para cada

localização fixa prevista pela base de projeto do SNA, considerando suas peculiaridades físicas e demográficas.

Os planos de emergência devem descrever as ações técnicas e administrativas a serem executadas, devendo estabelecer:

- Meios de diagnóstico e sinais de alarme para cada tipo de acidente;
- Grupos de emergência, suas responsabilidades, equipamento e pontos de reunião;
- Tabela-mestra para condições de emergência, definindo os deveres e responsabilidades individuais do pessoal de serviço de quarto na ECM, do pessoal que guarnece estações de controle de emergência e dos demais membros da tripulação;
- Locais de reunião para os membros da tripulação não essenciais para a execução do PEI no mar, assim como procedimentos e rotas de evacuação do submarino para os membros da tripulação não essenciais para a execução do PEL em porto;
- Planejamento de exercícios periódicos para o pessoal diretamente envolvido na sua execução e para os demais tripulantes e pessoal de apoio logístico em terra;
- Listagem de responsáveis em terra que deverão ser informados das condições a bordo e os meios de comunicação que deverão estar disponíveis;
- Modos de operação dos equipamentos e sistemas da IPN e do submarino relacionados com a segurança; e
- Listagem sequencial de ações requeridas para prevenir, conter e limitar potenciais liberações de materiais radioativos para o submarino e o meio ambiente, e as responsabilidades específicas de cada membro da tripulação na sua execução.

Um planejamento de inspeções, testes funcionais, manutenção e reparos de equipamento da IPN deve estipular a frequência e datas das atividades prescritas pelo Manual de Operação. As datas de efetiva execução destas atividades devem ser registradas para demonstrar que as determinações da ASN são cumpridas estritamente e que a condição técnica dos equipamentos é apropriadamente controlada e mantida.

5.3.2 PROCEDIMENTOS OPERACIONAIS

A operação do submarino e sua IPN deve seguir os procedimentos constantes do Manual de Operação. Durante operação normal, os procedimentos a serem seguidos devem incluir:

- Testes funcionais dos sistemas de monitoramento, controle, e proteção da IPN, calibração de instrumentos e equipamentos de monitoração da radiação, e inspeção dos equipamentos relacionados com a segurança, em intervalos especificados;
- Manutenção, reparo e substituição de componentes de equipamentos relacionados com a segurança;
- Atendimento às normas e regulamentos da organização operadora e da ASN para o armazenamento e disposição de rejeitos radioativos e para contabilidade e controle de materiais físeis;
- Supervisão da IPN, incluindo o controle da qualidade dos fluidos de resfriamento do Circuito Primário e do Circuito Secundário;
- Registro, nos livros de quarto do submarino apropriados, de todos os incidentes e informações relativas à operação da IPN e à manutenção e verificação de equipamentos;
- Teste de estanqueidade da estrutura de Contenção, da eficiência dos sistemas de purificação do ar interno e do controle dos níveis de radiação a bordo;
- Verificação da disponibilidade imediata e confiabilidade em serviço dos componentes redundantes de reserva da IPN e das fontes de alimentação elétrica em emergência, dos sistemas de remoção de calor da estrutura de Contenção, e dos sistemas de resfriamento e remoção de calor residual do núcleo normais e de emergência;
- Verificação dos tempos de queda e das velocidades movimentação dos elementos de controle do reator no núcleo;
- Prontidão contínua de sistemas de comunicação redundantes entre o comando do submarino, os compartimento de máquinas, a ECM e as posições de controle em emergência;
- Planejamento do treinamento e adestramento do pessoal de bordo e da realização de exercícios realistas; e
- Controle de materiais inflamáveis e explosivos a bordo, minimizando a possibilidade de agressões externas à IPN.

As inspeções em serviço e manutenção periódica de equipamentos não devem prejudicar a capacidade dos sistemas relacionados à segurança de executar suas funções, implicando em níveis de redundância abaixo dos requisitos mínimos.

A ASN deve assegurar que estão sendo observados os requisitos para operação segura do SNA, particularmente com respeito a:

- Efetivo da tripulação com um número adequado de pessoal qualificado;
- Condução e condições técnicas do submarino e de sua IPN compatível com a Análise de Segurança e o Manual de Operação;
- Práticas adotadas pelo quarto de serviço e para supervisão da operação da IPN;
- Efetiva verificação e registro pela tripulação das condições técnicas do submarino e de sua IPN; e
- Validade da documentação de operação, manutenção dos registros de operação da IPN, das condições radiológicas e dos incidentes ocorridos, assim como a oportuna submissão à ASN de relatórios de análise dos eventos operacionais relevantes para a segurança.

5.3.3 PROCEDIMENTOS DE EMERGÊNCIA

Se uma situação de emergência ocorrer, um sinal de alarme apropriado deve ser acionado, o caráter da emergência identificado, e a extensão dos danos determinada. Ações devem ser executadas para controlar a situação de emergência e minimizar seus efeitos, conforme os procedimentos do plano de emergência aplicável.

No caso de uma emergência que ameace a segurança do submarino ou que poderia resultar na liberação descontrolada de radioatividade para o meio ambiente, o comandante deve notificar imediatamente a organização operadora e a ASN.

No caso de um lançamento descontrolado de materiais radioativos excedendo os valores previstos pela Análise de Segurança em portos ou águas costeiras, o submarino deve içar o sinal de emergência internacional apropriado:

- “AK”: “eu tive um acidente nuclear a bordo” ou
- “AJ” : “eu tive um acidente nuclear severo e você deve aproximar-se com precaução”.

Quando houver um risco de exposição da tripulação a doses de radiação que exceda os limites dose-equivalente anuais para exposição profissional recomendadas pela ICRP, o comandante deve tomar as ações necessárias para minimizar as exposições individuais, promovendo o abandono do navio.

5.3.4 MANUTENÇÃO E REPARO

As atividades de manutenção e reparo de sistemas e componentes de CS-1 a CS-4, devem ser planejadas e executadas de acordo com procedimentos previamente aprovados pela ASN.

A manutenção e reparo de equipamento dentro de áreas controladas, o manuseio e transporte de equipamentos contaminados, e locais e equipamentos adequados para descontaminação de equipamento devem ser planejados e executados de modo a otimizar as doses incorridas pelo pessoal envolvido, i.e. reduzi-las a níveis ALARA.

Devem ser previstos arranjos que assegurem que as atividades de manutenção e reparo possam ser executadas de modo seguro, sem exposições à radiação excessivas do pessoal envolvido e sem liberação descontrolada de materiais radioativos para fora das áreas pré-determinadas para a sua execução. Sempre deverá haver pelo menos uma barreira física significativa entre os materiais radioativos manipulados durante estas atividades e o exterior das áreas em que são executadas.

Deverá ser permitido somente ao pessoal especialmente treinado na execução correta dos procedimentos operacionais e em proteção radiológica realizar atividades de manutenção e reparo que envolvam altos níveis de radiação. Os procedimentos operacionais respectivos devem estar elaborados e aprovados pela ASN antes que tais atividades sejam iniciadas.

Os dispositivos, ferramentas e sobressalentes usados pelo pessoal de manutenção e de reparo para substituir componentes de sistemas devem obedecer os mesmos requisitos de qualidade do item reparado.

5.3.5 TREINAMENTO, QUALIFICAÇÃO E ADESTRAMENTO DA TRIPULAÇÃO

O número mínimo de tripulantes do SNA, assim como suas respectivas qualificações, devem obedecer os requisitos do Manual de Operação aprovados pela ASN e devem garantir que o submarino e sua IPN possam ser operados e mantidos de modo seguro. A ASN deve aprovar especialmente o número mínimo de tripulantes designados para a operação da IPN.

Os requisitos a seguir aplicam-se aos oficiais não pertencentes ao Departamento de Máquinas do submarino:

- Devem ter completado com sucesso um curso de treinamento especial aprovado pelo ASN, cujo currículo deve incluir como um mínimo:
 - princípios básicos de efeitos biológicos da radiações ionizantes e de proteção radiológica; e
 - os princípios básicos da energia nuclear e de sua aplicação à propulsão naval de submarinos;
 - as características particulares da estrutura e desempenho de um submarino nuclear;
 - conhecimento das potenciais conseqüências de acidentes de navegação para o submarino e para o meio ambiente;
 - ações a serem tomadas para prevenir ou mitigar as situações de emergência postuladas (execução dos planos de emergência);
- A conclusão do curso e a aprovação no respectivo exame deve ser refletida através de certificados de qualificação emitidos pela ASN; e
- Estes oficiais não envolvidos diretamente com a operação da IPN devem possuir certificados de qualificação nuclear proporcionais aos seus efetivos deveres e responsabilidades.

Os requisitos a seguir aplicam-se aos oficiais pertencentes ao Departamento de Máquinas do submarino:

- Devem ter completado com sucesso um curso de treinamento especial e o respectivo exame de certificação aplicado pela ASN. O currículo deste curso deve incluir, como um mínimo:
 - princípios de engenharia nuclear e teoria dos reatores nucleares;
 - física das radiações, incluindo efeitos biológicos e ambientais das radiações ionizantes, princípios de proteção radiológica e monitoração da radiação;

- princípios de projeto operacionais da IPN, seus sistemas de monitoração, de controle e de proteção; dispositivos especiais de segurança da IPN e do submarino e características particulares da estrutura do casco do submarino;
 - estudo detalhado da IPN do submarino para o qual o oficial está sendo treinado com base nos respectivos Relatório de Análise de Segurança e Manual de Operação e nos manuais de operação e manutenção individuais de seus sistemas, equipamento e componentes;
 - treinamento prático, primeiramente em simulador e em protótipo em terra da IPN e em seguida no próprio SNA, na execução dos procedimentos operacionais normais, anormais, incidentais, acidentais e complementares;
 - treinamento prático em modelos parciais representativos (*mock-up*), em protótipo em terra da IPN e no próprio SNA na execução de procedimentos de manutenção, de inspeções e testes, de recarga do núcleo do reator e de gerenciamento de rejeitos;
 - estudo das normas nacionais e internacionais de segurança aplicáveis ao submarino e a sua IPN;
- a certificação deve registrar a conclusão do curso de treinamento especial, explicitando as qualificações obtidas; e
 - o Chefe de Máquinas e os demais oficiais do Departamento de Máquinas devem possuir certificados de qualificação adequados aos deveres e responsabilidades individuais, estando sujeitos a re-treinamento e re-certificação periódicos
 - a certificação está associada a uma determinada classe de SNA, a operação de uma unidade de outra classe requerendo nova certificação específica.

Todo membro da tripulação do submarino que executa tarefas específicas ou gerais no caso de um evento indesejado de origem radiológica, independentemente de pertencer ou não ao Departamento de Máquinas, deve ter treinamento em proteção radiológica a um nível proporcional com seus deveres particulares. Este treinamento deve ser atualizado periodicamente e deve ser repetido a uma frequência suficiente para assegurar uma continuidade da conscientização e entendimento dos requisitos de proteção radiológica.

O pessoal diretamente responsável pela proteção radiológica deve ter:

- sido treinado nas atividades de proteção e de dosimetria a um nível adequado às suas funções; e
- completado com sucesso um curso de treinamento detalhado e possuir um certificado de qualificação emitido pela ASN que indica os tipos de IPN e de equipamento de proteção radiológica para os quais foram treinados.

O oficial-médico e praças enfermeiros do submarino devem receber treinamento adequado no tratamento terapêutico dos efeitos deterministas das radiações.

Os demais membros de tripulação devem concluir cursos teóricos e treinamento prático em proteção radiológica proporcional aos seus deveres, como também instruções no uso de equipamento de proteção individual. Este treinamento pode ser dado em um centro de treinamento específico ou a bordo do submarino, através de oficiais qualificados do Departamento de Máquinas. Este pessoal deve ser familiarizado com os procedimentos estabelecidos para entrada em áreas controladas do submarino e com a execução das ações dos planos de emergência.

Todo o pessoal a bordo não membro da tripulação, deve ter recebido instrução prévia em procedimentos de proteção radiológica e ações dos planos de emergência, antes de embarcar no submarino.

As qualificações e desempenho de membros de tripulação na execução de suas tarefas específicas e gerais devem ser permanentemente verificados e aperfeiçoados através da simulação, o mais realista possível, da ocorrência de eventos indesejados. Estes exercícios devem simular os danos prováveis e as consequências das CPIN e SOS postuladas que envolvem direta ou indiretamente a IPN, sua realização sendo determinada por um planejamento prévio e por decisão inopinada do Comandante. À ASN é reservado o direito de, durante inspeções e auditorias de segurança, deflagrar um exercício inopinado.

5.4 INSPEÇÕES E TESTES

Os requisitos específicos de inspeções e testes são descritos neste Capítulo sob o título das três fases principais do ciclo de vida do submarino, que são as seguintes:

- fase de construção, que abrange o período de projeto, seleção e aquisição de materiais, componentes e sistemas, fabricação, teste de desempenho realizados pelo fabricante, transporte e armazenamento, pré-montagens em oficina e montagem de campo;
- fase de comissionamento, que abrange o período de testes pré-operacionais, criticalidade inicial após o primeiro carregamento do núcleo, ensaios de física do núcleo, operação inicial em potência e provas de mar; e

- fase de operação, que abrange o período da certificação e da entrada em serviço inicial (após testes de mar), a vida útil do submarino até o seu descomissionamento e a preparação para sua disposição final.

Durante o desenvolvimento das fases citadas acima, a ASN deve verificar a segurança nuclear do SNA através de auditorias e inspeções, conforme o caso, para verificar se as atividades da organização operadora relativas à construção, comissionamento e operação do submarino estão de acordo com os princípios básicos, critérios gerais e requisitos específicos estabelecidos. As inspeções devem garantir que:

- os materiais e procedimentos usados são compatíveis com o nível de qualidade necessário conforme a classe de projeto do componente;
- os resultados das características dos materiais antes e durante a fabricação são compatíveis com as especificações aprovadas pela ASN;
- os processos de fabricação são compatíveis com procedimentos de garantia da qualidade necessários para assegurar o desempenho desejado e a confiabilidade dos componentes e sistemas inspecionados;
- os componentes e os sistemas são fabricados e testados de acordo com os desenhos e as especificações aprovadas pela ASN; e
- o funcionamento dos componentes e dos sistemas é compatível com as suas funções específicas, particularmente as funções de segurança;
- a IPN e todos os sistemas de segurança associados satisfazem princípios básicos, critérios gerais e requisitos específicos estabelecidos, assim como outras exigências de segurança relevantes aprovadas pela ASN; e
- o submarino e todos os sistemas essenciais para a segurança serão mantidos e continuarão a funcionar adequadamente durante toda a vida útil do submarino.

Os períodos de inspeção e os métodos a serem usados devem ser detalhadamente especificados e aprovados pela ASN. Essas inspeções devem ser descritas na Análise de Segurança e no Manual de Operação, conforme o caso.

As inspeções, os testes e revisões dos sistemas, componentes, estruturas e desenhos devem ser especificados de acordo com a relevância da classe de segurança e de projeto do

item em questão. A Análise de Segurança ou o Manual de Operação, conforme o caso, devem descrever detalhes tais como:

- métodos a serem usados;
- intervalos entre as inspeções;
- a autoridade de inspeção adequada;
- a abrangência das inspeções; e
- procedimentos para eventuais ações corretivas.

Caso seja necessário do ponto de vista de proteção radiológica, blindagens adicionais, procedimentos de testes especiais e medidas de descontaminação adequadas devem ser utilizadas durante as atividades de manutenção, inspeções e testes.

Ao longo da vida útil do SNA podem ocorrer situações em que o detrimento radiológico, em termos de doses individuais e doses coletivas, para execução de certas atividades específicas de manutenção, inspeção e testes torna-se particularmente elevado. Tais situações devem ser analisadas sob o ponto de vista do Princípio da Justificação da proteção radiológica, visando obter-se soluções de compromisso aceitáveis entre os ganhos em termos de segurança nuclear e o detrimento radiológico decorrente. Uma orientação quantitativa para este tipo de análise é apresentada pelo Anexo P.

Os resultados das inspeções e dos testes devem ser registrados e as cópias de todos os relatórios devem ser mantidas pela organização operadora para verificação da ASN. Os relatórios de inspeções e de testes devem conter os seguintes dados:

- o nome do submarino, números ou letras identificadores, o nome da organização operadora, a data e o local da inspeção;
- os sistemas, os sub-sistemas e os componentes inspecionados;
- as condições de funcionamento do reator;
- as funções de segurança testadas, incluindo uma descrição dos procedimentos e métodos usados;
- os resultados dos testes, incluindo as disfunções observadas antes e durante o teste, como também uma descrição da condição observada dos componentes ou dos sistemas;

- o tempo sob carregamento e o tempo de disponibilidade e informações equivalentes, se assim for necessário conforme as especificações da inspeção;
- condições de irradiação e de contaminação, se houver, incluindo dispositivos especiais de proteção providenciados ou as medidas de descontaminação tomadas;
- requisitos para a repetição da inspeção, caso for necessário;
- condições especiais de operação, manutenção ou reparo decorrentes da inspeção ou impostas pela ASN; e
- nomes daqueles que realizam os testes e o nome do supervisor técnico independente e do representante da ASN que testemunhou as atividades.

5.4.1 DURANTE A CONSTRUÇÃO

As atividades de inspeção durante a fase de construção devem incluir uma verificação completa da estrutura do casco, máquinas e equipamentos, dos componentes principais da barreira de pressão, e dos componentes dos sistemas de segurança.

As inspeções a seguir referidas devem assegurar que todas as máquinas e os sistemas elétrico, estrutural, de comunicação, de proteção radiológica assim como os outros sistemas e equipamentos sejam compatíveis com os princípios básicos, critérios gerais e requisitos específicos de segurança estabelecidos.

A estrutura de contenção, seus sistemas de segurança e demais sistemas a ela associados devem ser testados de acordo com as suas funções de segurança tal como foram projetados, conforme os procedimentos apresentados anteriormente e segundo testes de pressão e testes de vazamento realizados da seguinte forma:

- Após o término da construção, um teste de pressão deve ser aplicado à estrutura de contenção de acordo com procedimentos adequados, até que se possa alcançar uma pressão de 110% da pressão de projeto. O teste hidrostático deve ser usado, a não ser que isso possa danificar a estrutura de contenção, sua suportação ou equipamentos nela contidos, caso em que dispositivos pneumáticos de teste devem ser utilizados. Quando a temperatura de teste for inferior à temperatura projetada, a pressão de teste P_T deve ser determinada de acordo com a seguinte fórmula:

$$P_T = 1,1 * \underline{Y_T} * P$$

Y_t

onde: Y_T é a resistência ao escoamento do material da estrutura de contenção na temperatura do teste;

Y_t é a resistência ao escoamento do material da estrutura de contenção na temperatura de projeto;

P é a pressão de projeto;

A tensão geral da membrana não deve ultrapassar $0,90 Y_T$ nos testes hidrostáticos e $0,75 Y_T$ nos testes pneumáticos.

- O teste deve ser observado por um supervisor técnico independente certificado pela ASN e precauções especiais devem ser tomadas para proteger os operadores quando ar ou gás sob pressão for usado como meio de teste;
- Após o teste de pressão, a estrutura de contenção deve ser inspecionada visualmente e por ensaios não-destrutivos para se detectar defeitos, imperfeições ou trincas superficiais, na extensão definida e aprovada pela ASN. Os dados obtidos a partir desta inspeção inicial devem servir de base de referência para verificações futuras;
- Antes dos primeiros testes de comissionamento a quente da IPN, a estanqueidade integral da estrutura de contenção deve ser testada. A taxa de vazamento integral deve ser determinada através de métodos aprovados pela ASN e deve ser realizada após o teste de pressão descrito acima, e depois que todas as penetrações da estrutura da contenção forem instaladas; e
- Os resultados do teste de taxa de vazamento inicial devem ser usados para estabelecer métodos e procedimentos necessários para extrapolar, a partir dos resultados dos testes feitos com pressões de teste mais baixas, as taxas de vazamento em situações pós-acidentais e aquela corresponde à pressão de projeto P .

Os compartimentos de confinamento adjacentes ao compartimento de contenção devem ser testados quanto a sua estanqueidade. Se a prevenção vazamentos destes compartimentos for baseada no estabelecimento de uma depressão de pelo menos 100 Pa com relação aos demais compartimentos do submarino, a ASN pode dispensar o teste de estanqueidade por pressão.

Os componentes submetidos a alta pressão devem ser testados de acordo com os seguintes requisitos:

- Os componentes de CS-1 ou CS-2 (exceto a estrutura de contenção) devem ser testados a uma pressão excedendo as suas pressões de projeto de forma a corresponder às normas aprovadas sob as quais os componentes foram projetados. Deve-se levar em consideração as características do material e a temperatura de funcionamento ao determinar as pressões de teste;
- Os componentes de CS-3 ou CS-4 devem ser testados a uma pressão adequada, excedendo a pressão de projeto;
- Sujeitos aos requisitos acima, os componentes e sistemas que contêm líquidos ou gases radioativos devem ser testados com um excesso de pressão não inferior a 1 bar e deve-se verificar também sua estanqueidade nesta condição. A sensibilidade dos métodos de detecção de vazamento usados deve ser compatível com o nível de radioatividade a ser contido;
- Após a instalação a bordo, todos os componentes da IPN, que não foram testados de acordo com os requisitos acima, devem ser testados em relação à pressão de teste máxima dos sistemas a eles interligados, para garantir o teste das soldas de fechamento;
- Vasos de pressão e rotores de bombas e motores de CP-1 altamente solicitados devem ser 100% inspecionados por métodos não-destrutivos para identificar falhas e trincas na sua superfície e no interior de seu corpo. Métodos de ensaios não-destrutivos devem ser capazes de detectar o mínimo defeito significativo e os resultados devem oferecer uma base comparativa para testes semelhantes realizados durante inspeções periódicas;
- Medidas iniciais de espessura de vasos de pressão devem ser documentadas para futura referência comparativa;
- Os vasos de pressão e carcaças de máquinas ou equipamentos de CP-1 e CP-2 devem ser feitos em material aprovado pela ASN. Os ensaios destes materiais devem obedecer a procedimentos aprovados pela ASN e devem ser testemunhados por um supervisor técnico independente;
- As características mecânicas do material do Vaso de Pressão do Reator VPR devem ser monitoradas em relação a alterações induzidas pela radiação na ductilidade e mecânica da

fratura ao longo de toda sua vida útil. As amostras de teste, montadas em cápsulas de irradiação, são introduzidas no interior do VPR para que a fluência de nêutrons, a temperatura e os transientes reflitam as condições reais que o afetam, devendo serem dispostas de forma a permitir sua remoção periódica para ensaios; e

- Eixos, pás, parafusos e outros elementos de máquinas componentes de equipamentos do CP-1 submetidos a carregamentos elevados devem ser testados sob requisitos semelhantes àqueles exigidos para o VPR, e o desempenho das partes rotativas deve ser verificado por ensaios de sobrevelocidade.

Sensores, instrumentos e outros componentes que devem funcionar de forma confiável em condições acidentais devem ser submetidos a testes de qualificação conforme os seguintes requisitos:

- Protótipos e amostras de produção de tais equipamentos devem ser ensaiados sob condições equivalentes de temperatura, pressão, umidade, vibração e radiação às condições acidentais.
- Após término da instalação a bordo do submarino e antes do reator atingir a sua criticalidade inicial, os sistemas de segurança e de proteção do reator, incluindo a instrumentação nuclear, os chaveamentos, os controles e os monitores, devem ser testados quanto ao seu funcionamento satisfatório e quanto a sua precisão. Tanto quanto praticável, o funcionamento dos sensores também deve ser verificado.

O equipamento elétrico e eletrônico, instrumentação, controles e chaveamentos CS-1, CS-2 e CS-3 dos sistemas de segurança do reator e devem ser testados em protótipos e serem compatíveis com os seguintes requisitos:

- A precisão especificada dos sensores e unidades de processamento de sinais deve ser demonstrada pelo fabricante. A calibragem dos canais de medida neutrônicos dos sistemas de segurança deve ser demonstrada.
- Devem ser demonstradas a qualidade e características dos materiais dos componentes de instrumentação pressurizados de CS-1 e CS-2. Esses componentes devem ser submetidos a testes de pressão.

5.4.2 DURANTE O COMISSIONAMENTO

As inspeções durante a fase de comissionamento devem abranger os testes de todos os sistemas do submarino, inclusive um teste pré-operacional completo da IPN, carregamento do núcleo, operação inicial em potência e provas de mar. O programa geral dos testes deve ser aprovado pela ASN e os testes devem ser executados progressivamente, de forma metódica, garantindo que todos os requisitos de segurança sejam satisfeitos.

Antes do carregamento do núcleo, o Circuito Primário e os sistemas auxiliares a ele interligados devem ser cuidadosamente verificados em relação à limpeza, para evitar eventuais bloqueios nos canais de resfriamento e indevida ativação de quantidades significativas de impurezas. Além disso, verificações devem ser realizadas para garantir:

- Estanqueidade dos circuitos sob pressão nominal;
- Funcionamento adequado da instrumentação de pressão, temperatura, vazão e níveis de líquido dos sistemas;
- Funcionamento adequado das válvulas de alívio e de segurança no Circuito Primário e Circuito Secundário.

Após o carregamento do núcleo, porém antes do aquecimento do Circuito Primário, estes requisitos devem ser mais uma vez verificados, assim como:

- A composição e as propriedades físico-químicas da água de resfriamento do Circuito Primário e Circuito Secundário, para garantir que se encontram dentro dos parâmetros aceitáveis; e
- Funcionamento adequado dos sistemas elétricos principais e de emergência.

Durante a fase de comissionamento que antecede a criticalidade, verificações devem ser feitas para garantir:

- Funcionamento adequado dos sistemas de controle de reatividade, incluindo ensaios de tempos de queda dos elementos de controle e segurança (SCRAM);
- Funcionamento adequado dos sistemas de detecção nuclear interna e externa ao VPR e as características de segurança associadas;
- Funcionamento adequado de monitoração da radiação para efeitos de proteção radiológica;

- Funcionamento adequado dos circuitos auxiliares e de emergência para o resfriamento do núcleo, inclusive as seqüências de partida automática de equipamentos redundantes;
- Estanqueidade a vazamentos da estrutura de contenção e o funcionamento adequado dos dispositivos automáticos de isolamento;
- Não ocorrência de desligamento automático do reator como resultado de sinais de SCRAM não válidos;
- Funcionamento adequado dos sistemas de proteção do reator;
- Precisão da instrumentação relacionada com a segurança do núcleo;
- Chaveamento adequado de unidades de reserva em sistemas redundantes; e
- Desempenho adequado de intertravamentos e alarmes.

Durante a criticalidade inicial e os testes de física do núcleo, porém antes da subida de potência, deve-se ter certeza de que a IPN, e de uma forma mais geral, de que todos os equipamentos do submarino tenham a disponibilidade exigida pela Análise de Segurança. Entre outras coisas, os seguintes itens devem ser verificados:

- Ativação apropriada do sistema de resfriamento de emergência do reator, inclusive os arranjos de chaveamento entre seus trens redundantes;
- Funcionamento adequado das válvulas de bloqueio de vapor; e
- Valores de parâmetros de reatividade e as margens de sub-criticalidade, em todas as condições apropriadas, para verificar os valores exigidos na Análise de Segurança.

Durante a operação inicial em potência antes das provas de mar, os seguintes itens devem ser verificados através de testes a carga reduzida:

- Funcionamento adequado das alimentações de energia elétrica e continuidade de funcionamento durante transientes de chaveamentos entre as diferentes configurações operacionais;
- Funcionamento adequado do sistema de propulsão;
- Efetividade das blindagens radiológicas do Compartimentos do Reator e das eventuais blindagens existentes em outros compartimentos do submarino;
- Funcionamento adequado do equipamento para a medida da radioatividade nos Circuito Primário, Circuito Secundário e demais sistemas auxiliares;

- Funcionamento preciso e adequado dos instrumentos de medida da potência do reator;
- Eventual contaminação de circuitos não radioativos;
- Medida de parâmetros de reatividade e a margem de sub-criticalidade disponível em todas as condições, verificando os valores exigidos na Avaliação de Segurança;
- Chaveamento adequada entre os meios normais de remoção do calor residual e sistemas alternativos;
- Meios efetivos de controle da reatividade e da potência, suficientes para atender a respectiva função básica de segurança;
- Funcionamento adequado do sistema de remoção do calor residual em emergência; e
- Meios de controle e registro de doses individuais e equipamentos de detecção de radiação suficientes para satisfazer aos critérios de proteção radiológica.

Durante a fase de provas de mar, as inspeções e testes devem ser realizados conforme os seguintes itens:

- Os sistemas da IPN e do submarino devem ser verificados quanto ao funcionamento satisfatório e seguro em condições normais no mar. Os tópicos a serem verificados incluem:
 - Funcionamento adequado da IPN em operação prolongada a plena potência e em transientes de potência durante manobras, especialmente em condição de emergência típica da chamada “manobra de colisão” (*crash*), com variação brusca da potência do eixo propulsor da situação “tudo a vante” à situação “tudo a ré”, até o submarino atingir velocidade nula.
 - Efetividade da IPN em superar os efeitos de envenenamento por Xenônio (tempos para nova partida do reator após desligamento por SCRAM);
 - Valores adequados dos parâmetros físicos fundamentais relativos à segurança do reator;
 - Funcionamento adequado das alimentações de energia elétrica, usando a energia principal gerada pela IPN, e continuidade de funcionamento durante transientes de chaveamento entre configurações alternativas dos sistemas elétricos;
 - Funcionamento adequado dos instrumentos de medida de radioatividade nos processos do Circuito Primário, Secundário e auxiliares;
 - Precisão e funcionamento adequado de instrumentos de medida de potência do reator;
 - Eventual contaminação de circuitos não radioativos;
 - Partida do reator imediatamente após um desligamento automático aleatório e depois de um período de funcionamento a baixa potência; e
 - Capacidade para desempenhar testes em serviço no sistema de proteção do reator, sem perda das funções de segurança.

- A IPN também deve passar por provas de mar para demonstrar sua operação de acordo com os requisitos de projeto, tal como está estabelecido na Análise de Segurança, durante quaisquer situações CPIN-1, CPIN-1, SOS-1 e SOS-2, como as que envolvem:
 - falha simples de qualquer componente ativo da IPN e do sistema de propulsão;
 - rejeição de carga de uma turbina qualquer durante funcionamento a plena potência; e
 - falha de uma alimentação elétrica, hidráulica ou pneumática durante chaveamento para o sistema de reserva.

Após término das provas de mar, deve ficar demonstrado que:

- a radioatividade está contida dentro dos especificações de projeto e, através do balanço de massa do refrigerante primário ou outros métodos apropriados, não existem vazamentos não intencionais para o vapor secundário ou qualquer outro sistema ou compartimento não radioativo; e
- as liberações intencionais de efluentes radioativos líquidos ou gasosos podem ser controlados aos níveis permitidos e, quando no meio ambiente, estes não retornam ao submarino pelas suas tomadas de ar e de água do mar.

5.4.3 DURANTE A OPERAÇÃO

Para os propósitos desta seção, a fase operacional é definida como o período entre o comissionamento e o descomissionamento. Os requisitos apresentados complementam os requisitos que estão ligados aos componentes não nucleares do casco, das máquinas e dos equipamentos.

A IPN e a estrutura do casco, particularmente na região do compartimento do reator, devem ser periodicamente inspecionados da seguinte forma:

- anualmente, durante os Períodos de Manutenção de Rotina PMR (duração de um mês após cada Missão de Patrulha Básica MPB, vide Anexo B) e os Períodos de Docagem de Rotina PDR (duração de 4 meses após cada 23 meses de cumprimento de Missões Básicas de Patrulha, vide Anexo B), de acordo com os requisitos a seguir especificados;
- quadrienalmente, durante os Períodos de Manutenção Geral PMG (duração de 13 meses após 50 meses de operação, vide Anexo B) de acordo com os requisitos a seguir especificados;

- durante os períodos de parada para recarga do combustível, que a princípio devem coincidir com os PMG;
- mediante determinação da ASN, inspeções contínuas podem ser realizadas em complemento às inspeções periódicas; os ciclos de inspeções contínuas devem durar um período que não ultrapasse aquele prescrito entre inspeções periódicas relevantes e cada parte sujeita à inspeção contínua deve ser inspecionada pelo menos uma vez durante esse período; se for considerado como necessário pela ASN, partes separadas devem ser inspecionadas mais de uma vez durante o ciclo;
- as inspeções periódicas e contínuas não devem ser indevidamente limitadas pela radiação e os vasos de pressão e tubulações a elas submetidos devem, sempre que praticável, terem fácil acesso.

A estrutura do casco na região do compartimento do reator e as estruturas de proteção contra colisão devem ser inspecionadas anualmente, durante os PMR. A cada dois anos, durante os PDR, a inspeção deve incluir verificação de deformações e reduções na espessura do chapeamento e dos membros estruturais principais.

As inspeções anuais devem garantir que os sistemas da IPN satisfaçam as funções de segurança especificadas e devem incluir as seguintes disposições:

- Os registros de bordo das instalações de máquinas relativos ao funcionamento do reator, os relatórios de operação, e os dados referentes a inspeções e testes periódicos e em serviço devem ser examinados em caso de ocorrências anormais;
- A efetividade das seguintes funções de segurança devem ser demonstradas pelas inspeções:
 - proteção do reator;
 - resfriamento de emergência do reator, incluindo os sistemas de alimentação de energia associados;
 - remoção de calor residual através de outros meios que não os geradores de vapor;
 - integridade dos circuitos radioativos;
 - controle da reatividade;
 - sistema elétrico de emergência sob plena carga;
 - gerenciamento de rejeitos e controle de liberação de efluentes;
 - funções de contenção, exceto medidas de índice de vazamento da estrutura de contenção (fechamento, isolamento, controle atmosférico, alívio de pressão); e

- ventilação da áreas controladas;
- durante a demonstração destas funções de segurança, devem ser verificados os sistemas auxiliares que dão suporte aos sistemas que diretamente desempenham estas funções, tais como alimentação elétrica, hidráulica, pneumática, instrumentação e controle.

Cada inspeção quadrienal da IPN deve incluir, além dos requisitos das inspeções anuais, as seguintes disposições:

- as estruturas componentes da barreira de pressão do Circuito Primário, dos vasos de pressão do sistema secundário e as tubulações de vapor e água de alimentação, assim como as máquinas e equipamentos associados devem ser submetidos a um extensivo programa de ensaios não destrutivos;
- a taxa de vazamento integral da estrutura de contenção deve ser medida;
- todos os sistemas do CS-1, CS-2 e CS-3 devem ser inspecionados em relação a capacidades específicas; os sistemas CS-4 devem ser inspecionados segundo os procedimentos gerais aplicáveis a equipamentos navais;
- as partes altamente carregadas e as soldas da barreira de pressão do Circuito Primário, incluindo as Zonas Termicamente Afetadas ZTA destas soldas, devem ser submetidas a ensaios não destrutivos superficiais e volumétricos para avaliar quantitativamente quaisquer falhas ou trincas que podem ter se desenvolvido ou propagado;
- o VPR deve ser examinado com respeito a falhas e trincas por métodos ultra-sônicos, de forma a comparar seu estado atual com as avaliações realizadas anteriormente; essas verificações devem, na medida do possível, englobar toda a área superficial e todo o volume do corpo do VPR nas regiões de máxima fluência da radiação; sua extensão, procedimentos e frequência devem satisfazer a ASN, considerando que todo o recipiente de pressão do reator deve ser completamente examinado durante o período de 12 anos de funcionamento do reator; considerando as recargas de combustível do reator, cada período quadrienal pode prolongar-se no máximo por um ano, dependendo das condições de queima reais do núcleo;
- os geradores de vapor, as carcaças das bombas e os corpos das válvulas, o vaso de pressão de pressurizador e os demais vasos de pressão do Circuito Primário, devem ser

testados por métodos cuja extensão, frequência e procedimentos devem ser previamente aprovados pela ASN;

- todos os componentes pressurizados, além daqueles componentes da barreira de pressão do Circuito Primário, devem ser testados a um nível adequadamente superior às pressões de projeto, de forma a adaptar-se às normas segundo as quais cada componente foi construído; em geral, os seguintes sistemas devem ser testados à pressão e inspecionados se a sua pressão projetada for superior a 2 bar:
 - componentes CS-1 e CS-2;
 - sistemas de desmineralização,
 - sistemas de purificação e controle volumétrico;
 - sistemas de selagem;
 - sistemas de resfriamento de emergência e os sistemas de suporte ao seu funcionamento;
 - sistemas de remoção de calor residual do núcleo do reator, excetuando-se os condensadores principais;
 - sistemas de manuseio e disposição de rejeitos;
 - sistemas de remoção de calor e alívio de pressão da estrutura de contenção;
 - sistemas hidráulicos de controle, se houver;
 - sistemas hidráulicos de desligamento automático do reator (acionamento de elementos de controle), se houver;
 - sistemas de drenagem da estrutura de contenção, se houver;
 - sistemas de resfriamento de componentes;
 - sistemas de resfriamento por água do mar associados à IPN;
 - sistema de vapor vivo (do gerador de vapor até as válvulas garganta das turbinas);
 - sistema de água de alimentação dos geradores de vapor, incluindo as bombas de alimentação e pré-aquecedores.

A partir da segunda inspeção quadrienal, além destes requisitos devem ser incluídas as seguintes disposições:

- todos os vasos de pressão e tubulações, exceto a estrutura de contenção, devem ser testados a uma pressão superior às suas respectivas pressões de projeto de forma a adaptar-se às normas aprovadas sob as quais foram construídos; se os ensaios não destrutivos do VPR comprovarem que a integridade da barreira de pressão permanece intacta, seus testes de pressão periódicos podem ser dispensados;
- testes de pressão ou qualquer outro método de detecção de vazamento adequado devem ser conduzidos em todos os componentes que contêm gases ou líquidos radioativos, além

daqueles do CP-1; os vasos de armazenagem também devem ser limpos e inspecionados interna e externamente para detectar falhas; e

- as soldas, aberturas, conexões e suportes dos componentes do CP-2, CP-3 e CP-4 que são fabricados a partir de material que tenha uma tensão superior a 450 N/mm^2 quando submetidos à pressão de teste à temperatura ambiente devem ser submetidos a ensaios não destrutivos.

5.4.4 DURANTE REPAROS, MODERNIZAÇÃO E MODIFICAÇÕES

Durante os períodos de recarga do núcleo e em todas as ocasiões possíveis durante atividades de reparo, quando a IPN não estiver em funcionamento, as seguintes inspeções devem ser realizadas:

- inspeções de todo o fundo, tanques, vasos de pressão, tubos e conexões, estruturas e fundações no compartimento do reator;
- inspeções das blindagens biológicas;
- inspeções da barreira de pressão do Circuito Primário e verificação funcional dos sistemas de remoção do calor residual do núcleo;
- verificação funcional de todos os sistemas de segurança, especialmente aqueles que sofreram intervenções, e verificação do tempo necessário para desligamento automático do reator (tempo de queda de elementos de controle no núcleo);
- inspeções das partes internas do reator (com o combustível removido);
- limpeza de todos os tanques, vasos de pressão, tubulações e espaços internos do compartimento do reator para eliminar corrosão, sedimentos e outras contaminações;
- teste de vazamento da estrutura de contenção.

De acordo com os procedimentos e intervalos propostos no Manual de Operação e quaisquer outras instruções pertinentes aprovadas pela ASN, uma equipe treinada deve verificar as funções de segurança durante os períodos de operação entre as inspeções periódicas. Os testes devem cobrir pelo menos os sistemas do CS-1 e CS-2 e devem ser supervisionados pelo chefe de máquinas do submarino e devidamente registrados.

Se for requisitado pela ASN, deve ser feita uma inspeção, geral ou parcial, cada vez que ocorrer um evento operacional indesejado ou se uma falha for detectada, afetando ou

podendo afetar a segurança do submarino, a eficiência e integridade de sua proteção radiológica ou de qualquer equipamento, ou ainda sempre que quaisquer reparos ou modificações forem feitos.

A inspeção deve ser feita de forma a assegurar que os reparos e modificações necessários foram feitos de forma eficaz e que os materiais e o trabalho de tais reparos se adaptam aos requisitos de qualidade e são compatíveis em todos níveis com os princípios básicos, critérios gerais e requisitos específicos de segurança.

Se um componente da IPN for substituído, adicionado ou alterado durante o ciclo de vida do submarino, as inspeções e testes pré-operacionais das partes afetadas devem ser realizados antes do teste de vazamento do conjunto do sistema.

5.5 PLATAFORMA-NAVIO

5.5.1 ARRANJO GERAL

Serão aqui estabelecidos requisitos referentes ao arranjo físico dos espaços internos e sistemas componentes da plataforma-navio do SNA, bem como para acesso e isolamento destes espaços nas diferentes CPIN e SOS. O arranjo deve obedecer aos seguintes requisitos básicos:

- Minimizar o volume e o peso dos sistemas e seus componentes, sem detrimento da eficiência, confiabilidade e segurança da instalação.
- Otimizar a distribuição de pesos no submarino.
- Atender os demais requisitos específicos estabelecidos, em especial àqueles de proteção radiológica, habitabilidade, manutenção e reparo, e inspeção em serviço.
- Agrupar os sistemas em compartimentos de forma a permitir o controle de acesso nas diferentes CPIN e SOS.
- Agrupar os sistemas em compartimentos de forma a viabilizar seu isolamento em caso de alagamento, incêndio ou liberação de radioatividade.
- Garantir o acesso da tripulação a todos os serviços essenciais mesmo em condições acidentais.

- Dispor os sistemas e seus componentes de forma a atender aos critérios de confiabilidade, especialmente no que diz respeito à prevenção de falhas de causa comum.

O submarino deve ser dividido em áreas classificadas com base nos riscos radiológicos a elas associados. Os riscos radiológicos associados à classificação das áreas levarão em conta as CPIN e SOS operacionais (CPIN-1, CPIN-2, SOS-1 e SOS-2).

O casco resistente do submarino deverá ser subdividido em no mínimo três (3) compartimentos estanques, com o compartimento do reator localizado na posição intermediária.

O casco resistente poderá ser total ou parcialmente envolvido por tanques de lastro, guardando-se, preferencialmente, um arranjo do tipo “casco duplo”, pelo menos para o compartimento do reator

O compartimento de reator deve ser localizado de forma a atender aos seguintes requisitos (Figura 5.1):

- Minimização de danos decorrentes das SOS de colisão, encalhe, choque com o fundo, quedas de aeronaves, e riscos externos associados a armas, munições, assim como outras fontes identificadas por análise de segurança específica, através de limitação radial por tanques de lastro (arranjo de casco duplo) ou somente pela estrutura do casco resistente (arranjo de casco simples), desde que demonstrado que esta última pode suportar, sem perda de estanqueidade as SOS postuladas;
- Ser limitado longitudinalmente por *cofferdams* ou anteparas estendendo-se por toda seção transversal do submarino, projetados para prover proteção adequada contra incêndios ou explosões externos ao compartimento, assim como blindagem radiológica.

FIGURA 5.1: ARRANJO ESTRUTURAL DO COMPARTIMENTO DO REATOR

Os *cofferdams* e tanques que fazem parte dos limites estruturais do compartimento de reator devem se restringir ao transporte de água de lastro e óleo combustível para propulsão em emergência.

O compartimento de reator deve ser projetado de forma a facilitar o salvamento do reator ou a recuperação de suas partes essenciais no caso de naufrágio do submarino, sem que, entretanto, as soluções adotadas para atender este requisito venham a implicar em riscos adicionais à IPN em operação normal.

O compartimento do reator pode ser dotado de uma passagem que permita o trânsito de pessoal de vante para ré do submarino. Esta passagem deve possuir blindagens radiológicas adequadas que permitam que um indivíduo possa atravessá-la pelo menos quatro vezes por dia de operação normal, mantendo-se sua dose-equivalente dentro dos limites máximos prescritos e ALARA. Esta passagem, entretanto, não necessita ser dimensionada para resistir à máxima pressão pós-acidental, assumindo-se que, em caso de um grande Acidente de Perda de Refrigerante Primário APRP, as pressões do volume livre do compartimento do reator e da passagem sejam equalizadas através de dispositivos específicos. Para esta passagem são adotadas três configurações típicas, apresentadas pela Figura 5.2.

FIGURA 5.2: ARRANJO DE PASSAGEM PELO COMPARTIMENTO DO REATOR

A estrutura de CONTENÇÃO do compartimento do reator deve ser projetada de forma a limitar liberações de materiais radioativos para o interior do submarino e para o meio ambiente nas CPIN e SOS postuladas. Os requisitos de projeto devem incluir os seguintes aspectos:

- a estrutura de CONTENÇÃO deve estar circundada por compartimentos de confinamento;
- a barreira de pressão do Circuito Primário deve estar localizada dentro da estrutura de CONTENÇÃO;
- a estrutura de CONTENÇÃO e suas penetrações devem ser projetadas para resistir às condições pós-acidentais internas após a ocorrência de todas as CPIN;
- as linhas que penetram os limites de estrutura de CONTENÇÃO devem ser dotadas de válvulas de isolamento, que por sua vez devem ser localizadas tão próximas quanto praticável destes limite, remotamente controladas e automaticamente atuadas;
- exceto durante a recarga de combustível, o acesso de pessoal e equipamentos ao interior da estrutura de CONTENÇÃO deve ser feito via antecâmaras que deverão garantir a integridade e estanqueidade da estrutura sob todas as CPIN. As necessidades de acesso com o Circuito Primário pressurizado devem ser reduzidas ao mínimo indispensável;
- um sistema de condicionamento de ar em circuito fechado, independente e segregado do sistema equivalente para o submarino deverá garantir a purificação e resfriamento da atmosfera interior da estrutura de CONTENÇÃO, mantendo a umidade e temperatura nos valores de projeto para todas as CPIN operacionais (CPIN-1 e CPIN-2);
- sendo o sistema de condicionamento de ar em circuito fechado, devem ser previstos dispositivos para renovar o ar interior à estrutura de CONTENÇÃO com ar fresco antes da eventual entrada de pessoal, assegurando uma qualidade do ar satisfatória com respeito aos padrões sanitários aceitáveis. Os dispositivos de purga do ar interno devem ser projetados de forma que sua operação seja feita por períodos curtos;

- o eventual alívio da pressão no interior da estrutura de Contenção, após qualquer CPIN postulada, deve ser controlado, monitorando-se os materiais radioativos e o hidrogênio liberado, através do uso de filtros de alta eficiência, de forma a garantir que os limites de dose não sejam excedidos; a operação destes dispositivos, entretanto, não deverá ser considerada para supressão de pressão no curto prazo após a ocorrência das CPIN postuladas; a eficiência do projeto de filtros deve ser determinada na análise de segurança, devendo estar disponíveis equipamentos e dispositivos para verificar periodicamente o real atendimento aos valores de eficiência assumidos;
- devem ser previstos sistemas para controlar e monitorar os níveis de atividade e de concentração de hidrogênio no interior da estrutura de Contenção submetida às CPIN postuladas; e
- a deformação das estruturas do casco do submarino e dos compartimentos de confinamento quando submetidos às CPIN e SOS postulados pela base de projeto não deve afetar a integridade estrutural e a estanqueidade da estrutura de Contenção, nem causar flambagem ou instabilidade plástica.

Os compartimentos do submarino imediatamente adjacentes ao compartimento do reator deverão ter características de confinamento dinâmico, i.e. ser mantidos sob uma depressão mínima de 75 Pa, formando assim uma barreira adicional entre os materiais radioativos e os demais compartimentos do submarino e o meio ambiente. Estes compartimentos de confinamento deverão:

- controlar eventuais vazamentos de materiais radioativos da estrutura de Contenção intacta para o submarino e para o ambiente em toda as CPIN;
- prevenir e controlar (incluindo: monitoramento, retenção temporária e processamento) as liberações de material radioativo para as outras partes do submarino e para o ambiente de todas as outras fontes de radioatividade que poderão estar neles contidas; e
- assegurar, quando são simultaneamente violadas a segunda e a terceira barreiras para fins de manutenção e reparo postulados, que permaneça pelo menos uma barreira física entre o combustível irradiado e o ambiente interno e externo ao submarino, com os requisitos de estanqueidade aos gases e à água requeridos pela segurança nuclear.

- confinar, para tratamento e controle de liberação para o ambiente pelo sistema de ventilação:
 - material radioativo que pode vazar da barreira de pressão do Circuito Primário, ou de ruptura de tubulações de pequeno diâmetro fora da estrutura de Contenção;
 - material radioativo que pode vazar de uma penetração da estrutura de Contenção, ou de vasos de armazenamento de rejeitos.

Todas as anteparas ou outros limites estruturais que formam os compartimentos de confinamento deverão ser estanques a gases e a incêndios e de construção integralmente soldada. As penetrações elétricas e de tubulações deverão possuir características de estanqueidade e integridade estrutural idênticas às daquelas das estruturas que limitam os compartimentos de confinamento.

Os compartimentos de confinamento deverão envolver completamente o compartimento do reator, e seus limites estruturais deverão ser projetados para protegê-lo das agressões externas postuladas. Suas penetrações e aberturas para acesso de pessoal devem ser capazes de manter a estanqueidade aos gases requerida. Os limites dos compartimentos de confinamento devem ser estruturalmente integrados aos cofferdams, anteparas e outras estruturas que formam o compartimento de reator. As penetrações nos limites da estrutura de Contenção e dos compartimentos de confinamento devem ser mantidas em um número mínimo indispensável.

A localização de equipamentos importantes para a segurança do submarino e de sua IPN deve ser escolhida levando-se em conta:

- as características de arranjo devem incluir segregação física adequada de sistemas redundantes e de componentes importante para a operação segura do submarino e de sua IPN;
- o arranjo deve assegurar, do melhor modo possível, a imunidade a danos na ocorrência de acidentes internos ou externos; estruturas, componentes e sistemas CS-1 e outros que contenham materiais radioativos, incluindo rejeitos radioativos de alto nível, devem ser localizados dentro de estruturas resistentes à colisão;

- máquinas que tem um potencial para geração de mísseis (projeção de partes internas em caso de falhas) devem ser orientadas ou protegidas para minimizar os eventuais efeitos sobre o submarino e equipamentos importantes para a segurança da IPN;
- a Estação de Controle de Máquinas ECM deve ser localizada numa posição pouco vulnerável com respeito a incêndios, mísseis internos resultantes de explosões, substâncias tóxicas e radioatividade, mas suficientemente próxima da IPN para minimizar o comprimento das linhas de serviço;
- os sistemas essenciais à garantia das funções de segurança da IPN, especialmente a alimentação elétrica, no caso de falha no sistema principal, devem ser funcionalmente independentes e fisicamente segregados do sistema principal; onde praticável, a segregação deve ser feita através de barreiras resistentes a incêndios e de estruturas estanques à água;
- deve ser prevista uma estação de controle em emergência separada e distante da ECM; desta posição, deve ser possível a um operador conduzir com segurança o reator à condição de desligado a quente e a frio, mantê-lo no estado de subcrítico, e garantir a continuidade da remoção de calor residual;
- a estação de controle em emergência deve estar conectada funcionalmente com o comando do submarino, de forma que os procedimentos de desligamento possam ser executados sob controle direto do comandante; e
- as blindagens e sistemas ambientais devem garantir que posições de controle essenciais possam ser guarnecidas durante períodos razoáveis de tempo após a ocorrência das CPIN postuladas.

As aberturas para acesso de pessoal e material nos limites do compartimento de reator ou nos limites de espaços dentro do compartimento de reator estanques à água, ao ar ou proteção contra fogo, devem ser dotadas de fechamentos que mantenham a integridade da barreira da qual fazem parte. Onde necessário para segurança nuclear ou segurança física, devem ser providos arranjos apropriados para operação local e remota. Devem ser também implementados arranjos especiais, antecâmaras se for necessário, para que os diferenciais de

pressão de ar entre compartimentos adjacentes requeridos pela segurança não se tornem ineficazes durante operação das aberturas de acesso.

5.5.2 VENTILAÇÃO E CONDICIONAMENTO DO AR

As seguintes condições ambientais devem ser mantidas na atmosfera interna dos compartimentos habitáveis do submarino:

- A pressão ambiente deve ser mantida próxima à pressão atmosférica.
- A temperatura dos compartimentos habitáveis deve ser:
 - máxima de 32⁰, sem restrições de umidade relativa do ar e considerando-se o não funcionamento das unidades de condicionamento de ar;
 - mínima de 19⁰, com umidade relativa do ar entre 40% e 60%;
 - de projeto em 22⁰, com umidade relativa do ar entre 40% e 60%.
- A temperatura na praça de máquinas não deve exceder a 50⁰, não havendo limites para a umidade relativa do ar, considerando-se o não funcionamento das unidades de condicionamento de ar. Para o projeto, deve-se considerar 38⁰, sem restrições da umidade relativa do ar.
- A temperatura do compartimento do reator pode atingir até 57⁰, sem limites para a umidade relativa do ar.
- As condições acima estabelecidas devem ser mantidas para temperaturas do mar (fonte fria) encontradas em serviço compreendidas entre -2⁰ e +29⁰.
- Deve ser previsto isolamento térmico na superfície interna do casco resistente na Estação de Controle de Máquinas.
- Deve-se manter a quantidade adequada de oxigênio no ar ambiental, para qual são recomendados os índices compreendidos entre 18 e 22 %, à pressão atmosférica e à temperatura de 22⁰.
- Deve-se controlar a concentração de gases tóxicos ou inflamáveis, de vapores e de poeira no ar ambiental, dentro de valores máximos admissíveis dos principais agentes poluidores apresentados na Tabela 5.4

TABELA 5.4: LIMITES DE CONCENTRAÇÃO DE POLUENTES DO AR

Componentes	Principais Fontes	Concentração Máxima no Ar
-------------	-------------------	---------------------------

Dióxido de Carbono	Respiração	1 %
Monóxido de Carbono	Cozinha	25 ppm
Hidrogênio	Baterias	2 %
Freon - 12	Refrigeração	500 ppm
Hidrocarbonetos	Pinturas, solventes, graxas	25 ppm

Os sistemas de ventilação que servem espaços que contêm ou podem conter material radioativo devem ser segregados dos demais sistemas de ventilação do submarino, devendo também ser segregados dos espaços fora da área controlada, exceto onde os dutos possam ser adequadamente blindados, protegidos contra agressões externas e estanques ao ar.

Os sistemas de exaustão que servem espaços que contêm ou podem conter material radioativo devem ser monitorados e controlados para uma eventual presença de radioatividade. A localização das descargas de exaustão devem ser selecionadas cuidadosamente para evitar potencial contaminação de áreas do submarino.

Devem ser implementados dispositivos para prevenir e combater a presença de fumaça densa e materiais tóxicos provenientes de fontes internas e externas, que poderiam conduzir a perda de visibilidade, asfixia ou outros efeitos indesejados sobre os operadores da ECM, da estação de controle de emergência e do comando do navio.

As localizações das tomadas de ar de insuflamento devem ser selecionadas cuidadosamente para evitar a possibilidade de reentrada de materiais radioativos descarregados pelas exaustões.

Devem ser previstas redundâncias para os componentes ativos de ventilação e exaustão essenciais, com ventiladores auxiliares que sejam acionados automaticamente em caso de falha dos ventiladores principais.

Se o ar de ventilação flui de um espaço para outro, o fluxo deve ser no sentido das áreas com menor potencial de contaminação para áreas com potencial de contaminação mais elevado.

Os arranjos de ventilação e filtração para os compartimentos de confinamento devem manter permanentemente uma condição de depressão (pressão subatmosférica), mesmo quando uma via de acesso encontra-se aberta.

5.5.3 ESTRUTURA

Considerando-se o peso e a rigidez do compartimento do reator, uma análise da resistência longitudinal do casco do submarino deve ser feita, particularmente para as SOS de encaixe, de pouso no fundo a grandes profundidades e de docagem.

O módulo da seção transversal nas extremidades do compartimento do reator não deve variar bruscamente, devendo a estrutura ser integrada suavemente ao restante do casco resistente do submarino. Os membros estruturais de transição devem ser adequadamente projetados e dimensionados para transferir o peso e as cargas geradas pelo compartimento de reator ao restante da estrutura do submarino, devendo estender-se até onde necessário a vante e a ré do compartimento de reator, de forma a garantir a continuidade estrutural do casco. Esta continuidade estrutural tem significativa importância nas SOS que envolvam choques e colisões oblíquas.

O casco resistente na região do compartimento do reator deverá ser projetado para resistir à pressão hidrostática externa máxima postulada para o submarino, sendo ainda verificada a sua resistência à pressão interna máxima postulada pelas CPIN, em especial à CPIN-4 de acidente de grande perda de refrigerante primário.

As anteparas e *cofferdams* que limitam longitudinalmente o compartimento do reator deverão ser projetados para resistir à pressão interna máxima postulada pelas CPIN, sendo ainda verificada a sua resistência à pressão hidrostática externa máxima postulada pelas SOS de alagamento de um compartimento. Este último carregamento deve considerar os perfis de profundidade das áreas de operação do submarino, sendo compatível com a cota máxima da plataforma continental nestas áreas. As estruturas que limitam longitudinalmente os compartimentos de confinamento devem resistir às máximas condições de depressão estabelecidas no seu interior.

As fundações devem ser projetadas adequadamente de forma a garantir a suportaço dos componentes sob todas as CPIN e SOS. Elas devem garantir o posicionamento correto do reator e dos componentes da barreira de presso do Circuito Primrio sob qualquer ngulo de inclinao do submarino. Os suportes devem acomodar as tenses trmicas derivadas de todas as CPIN. Devem ser previstos acessos para inspeo e manuteno da estrutura de Conteno. Onde possvel, as fundações devem ser integradas com a estrutura do casco resistente.

O projeto das fundações dos compartimentos de confinamento e da estrutura de Conteno deve permitir sua interao com a estrutura do casco resistente e considerar as foras inerciais de acordo com sua classe de segurana.

As estruturas de suporte de blindagens devem ser projetadas para resistir aos carregamentos inerciais conforme prescrito para as classes de segurana CS-2 e CS-3 e s deformaes do casco resistente do submarino.

5.5.4 PROTEO CONTRA COLISO E QUEDAS DE AERONAVES

Os tanques de lastro que envolvem radialmente o compartimento do reator devem proporcionar proteo estrutura de Conteno contra as SOS de coliso e queda de aeronaves postuladas. Estes tanques de lastro podero estender-se para alm do comprimento do compartimento do reator, proporcionando proteo tmm aos compartimentos de confinamento.

A proteo contra coliso e choque de aeronaves deve ser analisada, sendo os resultados da anlise apresentados na Anlise de Segurana do submarino. As SOS postuladas devem considerar a possibilidade de eventos cuja probabilidade remota com respeito ao tipo de navio ou objeto abalroado e incluindo situaes de navegao ocenica, costeira e em zonas porturias. Devem tmm incluir e considerar:

- demonstrao atravs de cculos e ensaios em modelos da eficcia da proteo contra coliso;
- localizao de compartimento de reator;
- compartimentagem de submarino;

- estabilidade em avaria
- resistência das estruturas avariadas,
- deslocamento, velocidade e forma da proa do navio abalroador, que pode ser, por exemplo:
 - de mesmo porte do submarino, navegando à mesma velocidade;
 - de grande porte, com proa bulbosa;
 - de alta velocidade, com proa fina;
 - o submarino colidindo com um objeto fixo de massa infinita;
- risco de incêndios e explosões;
- perda de manobrabilidade; e
- efeitos sobre as armas e munições embarcadas no submarino.

5.5.5 PROTEÇÃO CONTRA INCÊNDIOS

Consistentemente com os demais requisitos, os sistemas de segurança devem ser projetados e localizados de forma a minimizar a probabilidade de ocorrência e a gravidade das conseqüências de incêndios e explosões. Onde o atendimento às funções de segurança possa ser ameaçado em caso de incêndio, devem ser instaladas estruturas resistentes ao fogo para segregar as partes redundantes do sistema ou seus subsistemas.

Estruturas de proteção contra fogo, equipamento e sistemas adicionais podem ser requeridos para assegurar a integridade das blindagens, da estrutura de Contenção, dos compartimentos de confinamento, e dos sistemas essenciais à segurança do reator, de modo que um incêndio de origem única não comprometa o desligamento do reator nem sua subsequente manutenção num estado seguro.

Todos os espaços contendo sistemas e equipamentos essenciais à segurança da IPN e dos tripulantes devem ser providos com sistemas de detecção e alarme contra incêndios e com um sistema de combate a incêndios remoto que use um agente extintor não corrosivo. Deve ainda ser considerado:

- uso de agentes extintores que permitam fácil descontaminação;
- uso limitado de detetores de ionização em espaços que possam ter níveis altos de radiação; e

- limitação e controle do hidrogênio liberado pelo processo de radiólise, ou de reações subsequentes a um acidente de perda de refrigerante primário.

O projeto adequado, o emprego de barreiras estruturais resistentes ao fogo, e a correta localização e operação de sistemas de detecção e combate a incêndios devem minimizar a probabilidade de ocorrência de avarias à IPN e seus sistemas de controle e proteção decorrentes de incêndios em compartimentos “não nucleares” do submarino.

Devem existir pelo menos duas rotas de fuga alternativas da ECM principal e do compartimento onde o posto de controle da IPN em emergência está localizado. Cada rota de fuga deve permitir uma efetiva proteção contra o fogo desde estes compartimentos até as escotilhas de escape do submarino.

Dentro de espaços tais como o compartimento de reator e os compartimentos de confinamento, que contêm equipamentos essenciais à operação segura da IPN, deve ser evitado sempre que possível o uso de substâncias combustíveis e sistemas que requerem substâncias combustíveis para o seu funcionamento. Onde o uso de tais substâncias não puder ser evitado, devem ser elaborados procedimentos operacionais e implementadas medidas de proteção específicas.

Os sistemas para a segurança da IPN, e em particular aqueles para geração de energia em emergência após o desligamento do reator, devem ser segregados e fisicamente separados através de barreiras estruturais de proteção contra fogo e providos com equipamentos individuais de combate a incêndios..

A existência de uma posição de controle de emergência deverá possibilitar os operadores a conduzir o reator até uma condição de desligamento a frio e mantê-lo nesta condição de subcrítica com remoção contínua do calor residual, no caso de um incêndio na ECM. Reciprocamente, um incêndio na posição de controle de emergência não deve afetar a habilidade e funcionamento da ECM.

Os riscos de incêndio ou explosão originados nos sistemas de armas do submarino ou em fontes externas devem ser analisados. Onde a análise evidenciar a necessidade, devem ser

implementados sistemas e arranjos de proteção contra incêndios específicos, ou outros dispositivos e procedimentos especiais aceitáveis pela ASN,.

5.5.6 SEGURANÇA FÍSICA DA IPN E DO MATERIAL FÍSSIL ESPECIAL

Procedimentos e sistemas de segurança física contra sabotagem e atos de terrorismo devem ser levados em consideração no projeto e na operação do submarino nuclear, de forma a proteger a IPN e o material físsil especial existente a bordo. Estes procedimentos e sistemas de segurança física devem, entretanto, ser consistentes e harmonizados com os princípios, critérios e requisitos da segurança nuclear.

Nenhum procedimento ou sistema de segurança física deve impedir o acesso imediato e seguro de um tripulante a qualquer compartimento do submarino, no caso de um incêndio ou outra situação emergencial, nem impedir a entrada em um compartimento se este acesso é requerido para o desempenho de funções de segurança.

5.6 INSTALAÇÃO NUCLEAR

5.6.1 REQUISITOS DE PROJETO

A configuração dos sistemas deve permitir inspeção em serviço e testes, sem degradação do nível de segurança da instalação. Os componentes pressurizados devem obedecer os critérios correspondentes a sua classe de projeto, sendo previstos:

- Teste de pressão inicial;
- Inspeções e testes de pressão periódicos;
- Testes periódicos de estanqueidade a vazamentos das penetrações;
- Isolamento de sistema;
- Programas de vigilância (*surveillance*);
- Lavagem (*flushing*) dos sistemas após sua montagem inicial, reparos ou modificações;
- Proteção contra sobrepressão.

Todos os sistemas essenciais à operação ou segurança da IPN devem ser capazes de ser controlados manualmente, além de qualquer automação prevista. O acionamento automático dos sistemas de segurança deve ser previsto para todos os eventos inicializadores que requeiram ação rápida. Em geral, tal ação automática deve ser prevista onde a ação do

sistema segurança seja requerida dentro de menos de 15 minutos para prevenir consequências inaceitáveis. Os sistemas automaticamente iniciados devem poder levar a IPN a uma condição segura em pelo menos 30 minutos, sem ajuda da tripulação. O projeto deve assegurar que um operador possa retomar controle das funções dos sistemas de segurança mas não pode inibir sua ação automática.

Os sistemas de segurança para os quais o critério de falha única se aplica incluem:

- Desligamento de reator;
- Proteção de reator;
- Remoção de calor residual do núcleo;
- Resfriamento de emergência do núcleo;
- Isolamento de Contenção;
- Remoção de calor da Contenção; e
- Controle das condições ambientais da Contenção.

Particular atenção deve ser prestada às interfaces entre a IPN e a plataforma-navio do submarino, visando assegurar a manutenção da segurança nuclear e da segurança naval:

- As tubulações que se estendem fora da estrutura de Contenção e que contêm ou podem conter material radioativo devem ser dotadas de válvulas de isolamento duplas e meios de detecção de vazamento. Onde as tubulações têm diâmetro interno maior que 15 mm, uma das válvulas de isolamento deve ser controlada remotamente e deve ser operada automaticamente;
- Interligações entre as tubulações normais do submarino e aquelas que contêm ou podem conter materiais radioativos deve ser minimizado. Onde estas interligações são inevitáveis, as conexões devem ser providas de válvulas de isolamento duplas e devem ser previstos meios para garantir que a tubulação entre estas válvulas é mantida vazia. Em nenhum caso devem existir interligações entre sistemas que circulam fluidos radioativos e sistemas de aguada do submarino;
- Os suportes de tubulações da IPN devem ser adequadamente projetados para todas as condições de operação do submarino, inclusive condições de emergência envolvendo rupturas de tubulações e subsequente chicoteamento.

A resistência das estruturas internas de reator, elementos de combustível e equipamentos classes CS-1 e CS-2 deve considerar os carregamentos resultantes das condições apresentadas pelo Capítulo 4. Os efeitos de tais carregamentos não devem impedir o desligamento do reator e nem devem afetar a geometria do núcleo, comprometendo seu resfriamento. Estes carregamentos devem incluir:

- Movimentos do submarino no mar;
- Acidentes Básicos de projeto da IPN e do submarino; e
- Vibrações induzidas pelo propulsor, por movimentos de culapadas (*slamming*) e choque com o fundo, pelas máquinas principais e auxiliares e por outras fontes de vibração a bordo;
- Carregamentos inerciais e flutuações de fluxo causadas pelos efeitos de redistribuição de vazão devido aos movimentos do submarino.

A resistência estrutural dos internos de reator, elementos de combustível e equipamentos classes CS-1 e CS-2 deve ainda considerar os requisitos de inspeções inicial e em serviço, buscando facilitar, ao máximo praticável, sua execução, bem como margens de segurança adequadas para o estabelecimento de:

- Número de carregamentos cíclicos decorrentes das CPIN e SOS postuladas ao longo da vida útil do SNA (vide Anexo B); e
- Características destes carregamentos cíclicos decorrentes das CPIN e SOS adotados pelo projeto mecânico.

Os efeitos de cada condição real de carregamento ocorrida durante a vida útil da IPN deverão ser determinados *a posteriori* de forma a, permanentemente, ter-se disponível uma estima da vida útil segura remanescente dos componentes do reator e Circuito Primário.

5.6.2 REATOR

5.6.2.1 Núcleo

A duração de vida útil do núcleo é definida, convencionalmente, como a energia, expressa em Dias Equivalentes a Plena Potência DEPP, produzida pelo reator entre sua primeira criticalidade e um estado de queima tal que não seria mais possível atingir a criticalidade no momento de ocorrência do valor máximo (pico) de concentração de Xenônio após um desligamento automático subsequente a um período de operação a plena potência. Para um SNA, a vida útil típica do núcleo é da ordem de 50-100 DEPP.

Note-se que o requisito de vida útil do núcleo constitui mais um objetivo que uma real restrição operacional do SNA: mesmo após o fim da vida útil convencional, o reator pode voltar a ser criticalizado após determinado período de tempo (da ordem de dezenas de minutos) após a ocorrência do pico de Xenônio, a baixa potência, com a temperatura do Circuito Primário podendo então ser reduzida até um valor mínimo suficiente para alimentar o Circuito Secundário com uma pressão de vapor aceitável. Após certo tempo de operação nesta condição, o Xenônio desaparece e o reator poderá novamente atingir sua potência máxima. A vida útil convencional refere-se, portanto, ao período de operação do reator durante o qual não existe restrição ao religamento após um SCRAM.

Para as CPIN-1 e CPIN-2 não devem ocorrer condições termohidráulicas do núcleo críticas que possam acarretar danos ao combustível. A determinação das condições do núcleo deve incluir margens suficientes para cobrir incertezas nos cálculos e deve levar em conta os efeitos associados aos movimentos do submarino no mar. Estas margens termohidráulicas, particularmente a razão de afastamento do regime de troca de calor por ebulição nucleada (*Departure from Nucleate Boiling Rate* DNBR), devem ser estabelecida como limites operacionais e devidamente aprovadas pela ASN. Os cálculos associados devem estar baseados em correlações experimentais de fluxo crítico de calor, que consideram as mais extremas condições decorrentes das CPIN postuladas e dos movimentos do submarino no mar.

A distribuição da vazão de refrigerante pelos canais de combustível individuais do núcleo e as incertezas associadas devem ser levadas em conta, outorgando-se particular atenção à redistribuição de vazão e à influência dos movimentos do submarino no mar na transferência de calor e nas propriedades do refrigerante. Devem ser demonstradas margens

de segurança adequadas para condições anormais de vazão do refrigerante decorrentes de perturbações na potência de bombeamento ou outras causas. Análises ou ensaios devem demonstrar a ausência ou aceitabilidade de vibrações induzidas pela vazão de refrigerante no núcleo e suas estruturas de suportaço, assegurando que delas não decorre nenhum risco à segurança na operaço do reator.

O projeto, fabricaço, inspeço e operaço do combustível devem ser tais que as eventuais liberaçoes de produtos de fissão durante sua “queima” no reator sejam mantidas tão reduzidas quanto requerido pelos critérios de proteço radiológica e de segurança nuclear. Para todas as CPIN, o projeto do combustível deve levar em conta fatores tais como propriedades dos materiais, efeitos da radiaço, necessidade de manter o núcleo dentro de uma geometria passível de resfriamento, processos físicos e químicos, carregamentos estáticos e dinâmicos, tolerâncias de fabricaço e incertezas dos modelos de cálculo.

Na fase de projeto devem ser especificados padrões para o desempenho seguro do combustível sob todas as CPIN. O combustível deve ser avaliado por um programa de testes de irradiaço e ensaios pós-irradiaço, especificados para confirmar seus parâmetros de projeto sob todas as CPIN. Os métodos de fabricaço e os procedimentos de garantia de qualidade devem assegurar que o combustível alcança o alto nível de confiabilidade requerido. Programas de monitoraço devem ser estabelecidos para assegurar que o comportamento de combustível é mantido dentro dos limites especificados ao longo de toda vida útil do núcleo.

A água do Circuito Primário deve ser permanentemente monitorada para detecço de falhas do combustível. O combustível que não se encontra conforme com os padrões estabelecidos para seu desempenho sob todas as CPIN deve ser removido do núcleo na primeira oportunidade surgida após sua detecço.

5.6.2.2 Controle da Reatividade

A base de projeto para controle de reatividade deve incluir as seguintes considerações:

- A probabilidade de ocorrência de eventos que resultem em aumentos de reatividade não planejados deve ser remota e não deve conduzir a situações que possam apresentar riscos inaceitáveis para a tripulação, o público em geral e o meio ambiente, conforme definido pelo Capítulo 4;
- O efeito de acidentes de reatividade postulados não deve resultar em danos à barreira de pressão do Circuito Primário maiores que escoamento de materiais em pontos localizados, dentro dos limites da correspondente especificação de projeto mecânico, nem impedir o desligamento do reator;
- O efeito líquido das características de realimentação inerentes ao núcleo deve tender a compensar um aumento rápido de reatividade quando a IPN se encontrar na sua faixa de potência operacional, levando-se em conta as atitudes, os movimentos e as acelerações postuladas pelo projeto do submarino; e
- O desligamento rápido do reator (SCRAM) deve ser eficaz em ângulos de banda de até 90°, devendo o reator ter capacidade de ser mantido na condição de desligamento em todos os ângulos. Além disto, o sistema de desligamento rápido do reator (SCRAM) deve operar automaticamente em inclinações menores, por razões de segurança, sempre que:
 - a estrutura de Contenção é inundada;
 - o submarino supera em 50% sua profundidade máxima de operação;
 - o submarino joga ou assume um ângulo de banda maior que 45°;
 - o submarino caturra com uma amplitude maior que 10°;
 - o submarino assume um ângulo de trim maior que 30°.

Os dispositivos de controle de reatividade devem satisfazer os seguintes requisitos:

- Pelo menos dois sistemas de controle de reatividade mecânicos independentes, confiáveis e efetivos devem ser previstos. Cada um deles deve ser por si só capaz de desligar o reator e manter o núcleo na condição subcrítica a frio;
- Um terceiro sistema, baseado em princípios de engenharia diversos dos dois sistemas precedentes (por exemplo, injeção de boro a alta pressão), deve ser previsto para desempenhar a função de desligamento rápido (SCRAM), sem entretanto ter funções de controle operacional da reatividade.
- Os dois sistemas de controle de reatividade mecânicos devem:

- ser capazes, individualmente, de tornar automaticamente o núcleo subcrítico e de mantê-lo num estado subcrítico a frio em qualquer etapa de sua vida útil, sem recurso ao uso de veneno solúvel (ácido bórico, por exemplo), assumindo-se que o elemento absorvedor de controle mais reativo tenha sido retirado do núcleo e não possa ser re-inserido; na condição a frio ($\sim 20^0$), a sub-criticalidade deve ser de no mínimo 1.000 pcm;
- ser capazes, em conjunto, de manter o núcleo subcrítico a pelo menos 5.000 pcm, durante as operações de recarga de combustível, considerando que todos os elementos absorvedores encontram-se totalmente inseridos no núcleo;
- ser capazes, individualmente, de controlar as variações de reatividade do núcleo de forma confiável, assegurando que os limites de projeto especificados para o combustível não sejam excedidos em nenhuma CPIN;
- incorporar dispositivos e arranjos mecânicos específicos que minimizem a possibilidade de ocorrência de movimentação não intencional de um elemento de controle;
- operam corretamente, mesmo que ocorra uma falha no primeiro sinal inicializador de sua ativação;
- ao receber um sinal de qualquer parâmetro de desligamento automático, ser capazes de reduzir o potência de reator de forma rápida o suficiente para evitar que os limites de projeto de combustível sejam excedido;
- prever indicação individual da posição de cada elemento absorvedor de controle na ECM;
- ser projetados de forma a reduzir a um nível aceitável a probabilidade de retirada inadvertida contínua de um elemento de controle;
- ser projetados de forma a reduzir a probabilidade de erro do operador através de estabelecimento de seqüências de ativação dos elementos de controle pré-determinadas e incontornáveis, incorporando dispositivos e arranjos funcionais que impeçam a retirada de elementos de controle em agrupamentos ou sucessões não planejados;
- O sistema adicional de desligamento rápido do reator empregando princípios de engenharia diversos dos dois sistemas de controle de reatividade deve ser capaz de tornar o núcleo subcrítico e de mantê-lo num estado subcrítico a frio em qualquer etapa de sua vida útil, sem exceder os limites de projeto do combustível considerando-se a ocorrência de uma falha única;
- Individualmente, cada sistema de controle de reatividade deve ser completamente operável sob todas as atitudes de projeto do submarino e possibilitar:
 - testes funcionais periódicos;
 - calibração periódica dos instrumentos de detecção nuclear que cobrem toda a faixa de potência de reator (0-100%); e
 - verificação do funcionamento adequado da instrumentação;

- os meios de controle de reatividade devem ser capazes de tornar e manter a longo prazo, com uma margem suficiente, o núcleo subcrítico, tanto durante como após sua vida útil, incluindo os períodos de manutenção, recarga, condições acidentais da IPN e condições acidentais do submarino, particularmente as condições de emborcamento e naufrágio;
- considerando que o elemento de controle mais reativo seja totalmente inserido no núcleo e não seja possível retirá-lo, o reator deve ser capaz de atingir a criticalidade durante toda a vida útil do núcleo durante o pico de concentração de Xenônio que segue a um desligamento automático após longo período de operação a plena potência, à mínima temperatura possível, considerando-se as características particulares das turbinas do Circuito Secundário, que devem ser operáveis em um nível de potência suficiente para manter o governo e habitabilidade do submarino sob as CPIN-1 e CPIN-2; e
- os meios de controle de reatividade devem ser projetados para serem operados da ECM, mas devem também prever a capacidade de serem operados da estação de controle em emergência, externa à ECM.

Durante o processo de partida, para garantir a continuidade do funcionamento dos sistemas de controle de reatividade, de segurança e de proteção do reator, devem estar disponíveis pelo menos duas fontes independentes de alimentação elétrica até que o nível de potência seja alcançado.

Para evitar variações de reatividade não planejadas decorrentes de variações da densidade do moderador, devem ser previstos meios para detectar e controlar oscilações de potência do núcleo do reator involuntárias, a menos que possa ser demonstrado por análise que tais oscilações têm um efeito desprezível e não resultam em uma diminuição das margens aceitáveis com respeito aos limites de projeto do combustível.

5.6.2.3 Controle do Reator

Uma falha única de qualquer componente de controle não deve impedir o desligamento seguro do reator, devendo ser previstos meios para testar os sistemas de controle de reator durante a operação, detectando, e onde possível, reparando, falhas em componentes, sem reduzir a capacidade do sistema executar suas funções de uma maneira segura e estável.

Todo o controle da IPN deve ser passível de ser executado pelos operadores de serviço na ECM, a qual deve:

- Ser equipada para operar e monitorar todos os sistemas da IPN, particularmente os relacionados à segurança sob as CPIN e SOS de 1 a 4; e
- Ser projetada e construída de forma que suas condições de habitabilidade, particularmente os níveis de radiação, temperatura e composição da atmosfera interna, e proteção contra incêndios e alagamentos, sejam mantidas sob todas as CPIN e SOS, de forma a permitir sua permanente ocupação.

A estação de controle em emergência deve ser equipada com a instrumentação e os controles necessários para:

- inicialização independente do desligamento a quente do reator;
- capacidade independente para o subsequente desligamento a frio;
- monitoração das condições da IPN, mantendo o reator no estado de desligamento a quente ou a frio; e
- remoção do calor residual do reator.

Considerando a inerente estabilidade da própria IPN, o sistema de controle deve ser projetado para regular a potência do reator em resposta à demanda operacional das manobras e da missão do SNA, devendo ser projetado de forma que nenhuma restrição operacional adicional, i.e. que não fosse também aplicável a um hipotético submarino convencional de porte e potência semelhantes, seja imposta ao submarino.

Na determinação das variáveis de controle da IPN deve-se considerar que:

- Para aquelas variáveis importantes para a segurança nuclear do reator, devem ser previstos canais de medida múltiplos associados a uma lógica de votação compatível com a confiabilidade requerida para garantir a classificação das CPIN (critério de probabilidade) apresentada pelo Capítulo 4;
- O período do reator (tempo de duplicação do fluxo de nêutrons no núcleo em transientes de criticalidade positiva) pode ser usado como um indicador, mas não deve ser usado nas malhas de controle de potência quando o reator está ligado;

- As características de projeto dos sistemas de controle do reator deve minimizar respostas a eventuais sinais espúrios.

Intertravamentos devem ser previstos dentro dos sistemas de controle para impedir ações inadvertidas de um operador. Onde estes intertravamentos possam ser contornados, a efetiva execução desta ação deve ser proeminentemente alarmada na ECM. A necessidade destes *by-passes* deve, entretanto, ser minimizada.

5.6.3 CIRCUITO PRIMÁRIO

5.6.3.1 Barreira de Pressão

Os componentes que formam parte dos limites da barreira de pressão do Circuito Primário devem ser projetados, fabricados, montados e testados segundo os padrões da classe CP-1. Devem ser previstos meios para detecção de vazamentos de refrigerante para o interior do Compartimento do Reator e para o lado secundário dos geradores de vapor. Seu projeto deve considerar as forças estáticas e dinâmicas impostas ao longo de toda a vida útil do SNA e originadas por:

- carregamentos cíclicos induzidos por variações de pressão e de temperatura derivadas das CPIN postuladas;
- carregamentos inerciais impostos pelas CPIN e SOS postuladas; e
- vibrações induzidas por fontes internas e externas à IPN.

A barreira de pressão do Circuito Primário deve ser projetada com margens suficientes para que, quando submetida às condições operacionais, de manutenção e testes, e acidentais, seus materiais estruturais se comportem dentro do regime elástico. O projeto deve considerar as temperaturas de serviço e outras condições que afetam os limites do regime elástico para os materiais estruturais sob estas condições, como também as incertezas na determinação de:

- propriedades físicas dos materiais;
- efeitos da irradiação nestas propriedades;
- tensões residuais e tensões calculadas para as condições estacionárias e transientes; e

- sensibilidade dos equipamentos utilizados e frequência dos ensaios não-destrutivos realizados durante as inspeções em serviço.

Os materiais e métodos construtivos devem ser selecionados dando-se particular atenção aos seguintes aspectos:

- adaptabilidade ao emprego em ambientes nucleares e navais;
- corrosão e erosão pela água de resfriamento do reator;
- existência de traços de elementos nos materiais que possam ser suscetíveis à ativação sob radiação ao transporte ao longo dos circuitos; e
- efeitos da irradiação por nêutrons nas propriedades dos materiais.

A proteção contra sobrepressão do Circuito Primário deve obedecer aos seguintes requisitos:

- Devem ser previstas pelo menos duas válvulas de segurança, cuja descarga deve ser feita para o interior de um tanque específico localizado no interior da estrutura de Contenção. Este tanque deve possuir dispositivos automáticos para descarga segura, no caso de sua sobrepressão ou transbordamento;
- O emprego de discos de ruptura como substituto de válvulas de segurança não é aceitável;
- A capacidade das válvulas de segurança deve ser tal que, mesmo no evento de falha de uma válvula, a pressão no Circuito Primário durante qualquer CPIN não exceda a máxima pressão operacional permissível por mais que 10%;
- Não devem ser permitidos dispositivos de fechamento a montante e a jusante de uma válvula de segurança, a menos que:
 - um intertravamento positivo garanta que, automaticamente, se a linha de alívio é bloqueada, outra linha seja previamente conectada ao circuito, proporcionando capacidade de alívio adicional adequada; e
 - um sinal de desligamento automático do reator por sobrepressão seja incorporado ao sistema de proteção.
- O nível de qualidade e critérios de projeto mecânico para os componentes de proteção contra sobrepressão devem ser iguais àqueles requeridos para a barreira de pressão da qual eles fazem parte.

5.6.3.2 Geradores de Vapor

Para garantir o isolamento rápido da Contenção em condições acidentais, particularmente no caso de ruptura ou vazamentos dos tubos dos geradores de vapor, as tubulações de água de alimentação e vapor principal devem ser dotadas de válvulas de bloqueio posicionadas o mais próximo possível da estrutura do Compartimento do Reator. A atividade de Nitrogênio-16 nas linhas de vapor principal junto aos geradores de vapor deve ser permanentemente monitorada e alarmada para detecção de vazamentos provenientes do Circuito Primário.

O lado do casco (Secundário) dos geradores de vapor e as tubulações de vapor até a primeira válvula de bloqueio de vapor devem ser protegidos contra sobrepressão por pelo menos duas válvulas de segurança redundantes. Levando o critério de falha única em conta, o dimensionamento destas válvulas de segurança deve ser tal que, para quaisquer que sejam as condições consideradas, a pressão interna nunca excederá a pressão de projeto em mais que 10%.

Considerando que o alívio será feito diretamente para o mar, na ocorrência de travamento em aberto ou fechamento incompleto das válvula de alívio após descarga, estas válvulas devem estar associadas a válvulas de bloqueio de fechamento rápido, que impeçam o embarque de água do mar. Estas válvulas devem possuir intertravamentos que impeçam o seu fechamento inadvertido e seus modos de falha devem ser na posição fechada

O lado dos tubos (Primário) dos geradores de vapor faz parte da barreira de pressão do Circuito Primário. O lado secundário dos geradores a vapor e as linhas de vapor e de água de alimentação até a segunda válvula de isolamento da estrutura de Contenção devem ter os mesmos nível de qualidade, classe de projeto e programa de inspeção em serviço aplicados aos componentes da barreira de pressão do Circuito Primário.

O lado secundário dos geradores de vapor deve ser dotado de um sistema de purga e de detecção de vazamentos provenientes do Circuito Primário causados por defeitos ou falhas nos tubos de troca de calor.

5.6.3.3 Sistema de Remoção de Calor Residual

O sistema de remoção de calor residual do reator deve ser projetado para permitir operação contínua desassistida durante um período de tempo mínimo necessário, demonstrado pela análise de segurança, cobrindo toda a evolução dos cenários associados às CPIN e SOS postuladas, excluindo:

- Emborcamento na superfície; e
- Naufrágio a uma profundidade tal que seja demonstrado que a inundação da estrutura de Contenção promoverá o necessário resfriamento do núcleo a longo prazo.

Se o emborcamento na superfície constituir uma SOS postulada, deve ser demonstrado que o sistema de remoção de calor residual é capaz de operar por um período máximo de tempo até ocorrer o naufrágio.

O sistema de remoção de calor residual deve ser projetado com capacidade, confiabilidade e redundância suficientes para assegurar que:

- Sob as CPIN-1 e 2, são mantidas tanto a integridade do revestimento do combustível como uma geometria do núcleo passível de resfriamento; e
- Sob as CPIN-3 e 4, as falhas do revestimento de combustível são limitadas a um valor aceitável pela ASN e uma geometria do núcleo passível de resfriamento é mantida.

A remoção de calor residual do núcleo deve ser possível de ser realizada no caso de indisponibilidade total de fontes de alimentação de energia elétrica, i.e. o sistema deve ser capaz de operar em modo passivo, através de processos de circulação natural.

5.6.4 INSTRUMENTAÇÃO

Até onde seja razoavelmente praticável, os canais de instrumentação do sistema de proteção de reator devem ser redundantes e segregados dos canais de instrumentação dos sistemas de controle e monitoração da operação da IPN e devem ter sua continuidade de funcionamento assegurada para todas as condições ambientais previstas para as CPIN postuladas.

O arranjo físico e redundâncias de componentes, cabeamento e equipamentos devem ser tais que a instrumentação do sistema de proteção de reator permanecerá operável no caso de incêndio de origem única ou qualquer outra condição acidental do submarino e da IPN.

Em todos os instrumentos devem ser indicados os valores limite das variáveis medidas e as respectivas faixas de funcionamento normal. Os canais de instrumentação que monitoram parâmetros e equipamentos importantes para segurança devem, onde praticável, ser auto-testáveis e possuir modos de falha segura.

A ocorrência de falhas deve ser sinalizada por alarmes sonoros e visuais. As interfaces homem-máquina devem garantir uma avaliação rápida e não ambígua do estado de funcionamento da IPN, com toda a informação essencial referente ao desempenho da instalação ou necessária à interpretação de falhas e mau funcionamento sendo registrada automaticamente. Onde quer que útil para continuidade de operação, segurança ou manutenção, devem ser previstos indicadores na ECM, locais e, até onde necessário, na estação de controle de emergência.

5.6.5 DISPOSITIVOS DE SEGURANÇA

5.6.5.1 Sistema de Proteção do Reator

A IPN deve ser dotada de um sistema de proteção do reator com as seguintes funções:

- Monitorar continuamente as condições de operação do reator, verificando se estas estão dentro dos limites de segurança de projeto;
- Inicializar automaticamente a operação dos sistemas, tais como a função de desligamento rápido dos sistemas de controle da reatividade, que asseguram que os limites de projeto dos sistemas importantes para a segurança da IPN não são excedidos; e
- Diagnosticar a ocorrência de acidentes e inicializar ações dos sistemas que garantem a continuidade das funções básicas de segurança da IPN.

O sistema de proteção de reator deve ter um grau de redundância satisfatório, que assegure seu correto funcionamento quando ocorrer uma falha, devendo ser capaz de ser testado durante operação sem reduzir a proteção mínima estipulada na Análise de Segurança.

A instrumentação do sistema, para a qual se requer continuidade de funcionamento sob as CPIN-3 e 4, deve ser especificamente qualificada para as condições ambientais pós-

acidentais delas decorrentes. A falha ou mau funcionamento de um canal de instrumentação deve ser alarmada sonora e visualmente.

Pelo menos duas variáveis de processo distintas devem ser medidas para detectar qualquer falha, mau funcionamento ou acidente na IPN. Se isto não é razoavelmente praticável, devem ser incorporadas redundâncias adicionais no canal de medida da única variável disponível.

5.6.5.2 Contenção

O projeto dos sistemas da Contenção deve considerar os seguintes requisitos:

- A estrutura de Contenção e sistemas relacionados devem estabelecer uma barreira essencialmente estanque contra liberações inaceitáveis de materiais radioativo contidos no Circuito Primário, de forma que as conseqüências das eventuais liberações estejam dentro dos limites estabelecidos pelo Capítulo 4;
- Somente o Reator, o Circuito Primário e os sistemas auxiliares e de segurança a ele ligados devem estar localizados no interior da estrutura de Contenção;
- De acordo com o princípio de defesa em profundidade, os compartimentos de confinamento adjacentes ao Compartimento do Reator (vide Figura 5.1) devem prover, numa extensão razoavelmente praticável, uma barreira adicional contra eventuais vazamentos de materiais radioativos da estrutura de Contenção, que controle as liberações decorrentes. As partes estruturais comuns aos compartimentos de confinamento e à estrutura de Contenção devem ser reduzidas a um mínimo e devem ser projetadas para evitar uma falha simultânea de ambas as barreiras onde as CPIN e SOS postuladas possam conduzir a uma perda de estanqueidade à água ou a gases de uma das barreiras;
- A estanqueidade da estrutura de Contenção deve ser mantida na presença da pressão externa decorrente das SOS que impliquem em mergulho acima da profundidade máxima de operação, particularmente a SOS de naufrágio; neste caso devem ser previstos dispositivos de balanceamento entre a pressão externa e a pressão interna da estrutura da Contenção, de forma que seus limites de projeto mecânico não sejam excedidos; o projeto destes dispositivos deve garantir que após feita a compensação entre as pressões externa e interna, a estrutura da Contenção retorne a sua condição de estanqueidade;

- A estanqueidade da estrutura de CONTENÇÃO e dos compartimentos de confinamento a ela adjacentes deve ser preservada na ocorrência de uma ruptura da tubulação principal da linha de vapor vivo nestes últimos; neste caso, a estanqueidade dos compartimentos de confinamento deve também ser assegurada;
- O projeto de estrutura de CONTENÇÃO deve prever:
 - Teste inicial de pressão;
 - Inspeções periódicas;
 - Testes de estanqueidade a vazamentos; e
 - Isolamento dos sistemas que penetram seus limites físicos;
- Os componentes, equipamentos e sistemas relacionados à segurança localizados no interior da estrutura de CONTENÇÃO devem resistir às condições ambientais mais severas nas quais eles podem estar sujeitos durante as situações acidentais nas quais seu funcionamento é requerido, incluindo os efeitos de jatos de fluidos a alta pressão e temperatura, projetis gerados internamente e forças de chicoteamento de tubulações;
- A estrutura de CONTENÇÃO deve ser projetada com margens suficientes para assegurar que, sob todas as CPIN e SOS de 1 a 4:
 - Os materiais estruturais se comportam dentro do regime elástico; e
 - A probabilidade de propagação de uma fratura frágil é minimizada.
- O projeto deve considerar as temperaturas de serviço e outras condições para os materiais estruturais da CONTENÇÃO durante a operação, manutenção, testes, e condições acidentais postuladas. Deve também considerar as incertezas na determinação de:
 - propriedades físicas dos materiais;
 - tensões residuais em estado estacionário e tensões em transientes; e
 - tamanho de trincas.
- Deve ser previsto um sistema para remover o calor transferido pelo Reator e Circuito Primário ao ambiente interno à estrutura de CONTENÇÃO sob as CPIN-1 a 4;
- Devem ser previstos meios para reduzir a concentração de produtos de fissão, hidrogênio e outros gases que podem ser liberados para o ambiente interno da estrutura de CONTENÇÃO que poderiam vir a provocar um processo de combustão ou explosão;
- Deve ser previsto um sistema para controlar eventuais descargas para a atmosfera interna e externa do submarino de materiais radioativos e de outras substâncias que possam ser liberadas da CONTENÇÃO sob as condições acidentais postuladas;

- Devem ser previstos sistemas que permitam a realização dos testes e inspeções especificados; e
- Cada sistema deve ter suficiente redundância e capacidade para executar sua função de segurança assumindo-se a ocorrência de uma falha única.

5.6.5.3 Resfriamento de Emergência

O projeto do Sistema de Resfriamento de Emergência SRE deve considerar os seguintes requisitos:

- O número de trens redundantes do SRE deve satisfazer o critério de probabilidade das CPIN apresentados pelo Capítulo 4, sendo os trens devidamente segregados e com um grau de redundância que considere não somente os modos de falha como também sua manutenção e possibilidades de reparo a bordo;
- O SRE deve manter a máxima integridade dos elementos combustíveis, minimizando danos ao encamisamento, após a ocorrência de um APRP seguido de desligamento automático do reator. Uma ampla e diversa alimentação de água de resfriamento para núcleo deve ser prevista, a pressões e vazões satisfatórias, até que, a longo prazo, calor gerado pelo combustível possa ser removido de modo seguro pelos sistemas de remoção de calor residual;
- No caso do emprego de acumuladores de água de resfriamento pressurizados, os mesmos devem ser dotados de válvulas de segurança, medidores de pressão e indicadores de nível e sistemas de pressurização dedicados para manter um colchão de gás no seu interior;
- Com exceção das válvulas de bloqueio principais que ligam o SRE ao Circuito Primário, que permanecem normalmente fechadas, todas as válvulas devem ser mecanicamente intertravadas na posição requerida para entrada em operação imediata do sistema;
- Como um requisito mínimo, todos os componentes de controle do SRE devem ser operáveis tanto da ECM como da estação de controle de emergência;
- Sem prejuízo ao seu funcionamento e confiabilidade, os componentes ativos do SRE devem ser capazes de ser testados a qualquer momento, assegurando-se que eles executarão satisfatoriamente suas funções quando demandado;

- Deve ser possível prover alimentações elétrica, hidráulica e pneumática aos componentes do SRE que delas necessitam a partir de todas as respectivas fontes de potência disponíveis a bordo que sejam independentes da energia gerada pela IPN; e
- Para resfriamento de emergência do núcleo a curto prazo, i.e. imediatamente após a ocorrência de um acidente, o SRE não deve requerer uma fonte de água de resfriamento externa ao submarino;
- O emprego de água do mar para resfriamento de emergência do núcleo somente pode ser considerado para as CPIN e SOS complementares.

5.7 INSTALAÇÕES DE MÁQUINAS

Nesta seção serão abordados requisitos aplicáveis às máquinas principais, entendidas como os componentes de máquinas a vapor do Circuito Secundário associado à IPN, às máquinas auxiliares, entendidas como os sistemas e componentes de máquinas associados à operação da plataforma-navio do SNA, que têm relação com a operação da IPN, e aos sistemas elétricos de serviço necessários à operação da IPN.

A estas máquinas e sistemas, basicamente convencionais, aplicam-se não somente os requisitos que serão aqui apresentados como também aqueles não especificamente ligados à segurança nuclear, de caráter de emprego geral em submarinos e navios de guerra, que não serão abordados.

5.7.1 REQUISITOS DE PROJETO

Devem ser previstos arranjos adequados, que facilitem a limpeza, inspeção e manutenção das máquinas principais e auxiliares, incluindo meios e procedimentos para descontaminação radioativa, onde requerido.

Devem ser previstos arranjos e dispositivos para proteger qualquer sistema de máquinas principais e auxiliares cujo funcionamento seja direta ou indiretamente necessário à operação de sistemas CS-1 e CS-2 de eventuais projetis internos e efeitos dinâmicos de rupturas de tubulações (chicoteamento e jatos fluidos) decorrentes das CPIN postuladas e gerados dentro dos compartimentos de máquinas.

Onde existir possibilidade de falhas provocadas por perda de lubrificação ou sobrepressão que conduza a sua perda total, danos externos, incêndio ou explosão, os equipamentos devem ser dotados de dispositivos para desligamento automáticos. Os ângulos de inclinação nos quais as máquinas principais e auxiliares devem ser capazes de operar são aqueles apresentados pelo Capítulo 4.

Penetrações na estrutura de Contenção por linhas componentes dos sistemas de máquinas devem ser evitadas e, quando indispensáveis, devem ser encaminhadas através do corredor de passagem do Compartimento do Reator.

Pelo menos um sistema de comunicações deve estar disponível no caso de perda completa de potência elétrica, interligando pelo menos as seguintes posições:

- Centro de Operações de Combate COC do submarino;
- Estação de Controle de Máquinas ECM;
- Estação de controle de máquinas em emergência;
- Compartimentos de máquinas principais, geradores elétricos de serviço, geradores elétricos de emergência e motores de propulsão principal e de emergência;
- Espaços acessíveis do Compartimento do Reator, particularmente o corredor de passagem e suas ante câmaras.

A confiabilidade da instalação elétrica deve ser proporcional aos princípios, critérios e requisitos de segurança tanto nucleares como navais. Para todas as CPIN, excluídas as complementares, o sistema elétrico de serviço como um todo, i.e. excluindo os turbo-geradores dependentes da IPN, deve ser capaz de desligar o reator e mantê-lo em um estado seguro durante pelo menos 30 dias, assumindo um falha simples além do evento inicializador que causou a CPIN.

A instalação elétrica deve consistir em um Sistema Elétrico de Serviço SES principal e um Sistema Elétrico de Serviço em emergência. O projeto do SES deve permitir inspeções e testes periódicos dos equipamento importantes para segurança tanto da IPN como do submarino. O SES de emergência, assim como cada seção redundante do SES principal, deve ser independentemente capaz de prover potência suficiente para os sistemas de segurança da IPN, assegurando que:

- Não sejam excedidos os limites de projeto especificados para o combustível, assim como outras condições limitantes de projeto da IPN como resultado de qualquer CPIN e SOS, excluídas as complementares; e
- O núcleo seja resfriado e sejam mantidas as demais funções básicas de segurança no caso de ocorrência dos acidentes postulados, em todas as atitudes do submarino previstas pelos critérios do Capítulo 4.

Devem ser previstas tomadas de energia de terra capazes de alimentar qualquer seção do SES principal e de emergência.

Os equipamentos e componentes elétricos do SNA que atendem funções de segurança em um acidente postulado, devem resistir as condições ambientais (pressão, temperatura, umidade, etc.), associadas àquele acidente.

Os cabos de alimentação de sistemas, quadros elétricos e equipamentos de segurança redundante devem ser roteados por caminhos físicos completamente segregados ou protegidos.

As penetrações de cabos elétricas na estrutura de Contenção e limites do Compartimento do Reator devem ser mantidas num número mínimo, consistente com os requisitos de segurança. As penetrações não devem comprometer a sua estanqueidade requerida e resistência a incêndios, nem devem impedir suas inspeções e testes.

5.7.2 MÁQUINAS PRINCIPAIS

Não serão aqui abordados requisitos específicos para o sistema de acionamento do eixo propulsor (vide Anexo A), que poderá ser elétrico, onde o eixo é acionado por um Motor Elétrico de Propulsão MEP alimentado pelas máquinas principais (Turbo-Geradores de Propulsão TGP), ou mecânico, onde o eixo é acionado diretamente pelas máquinas principais (Turbinas de Propulsão TP).

Sob o ponto de vista de segurança nuclear, entretanto, o sistema de acionamento do eixo propulsor deverá atender a um requisito, associado a uma proteção ativa contra efeitos de colisões, choque com o fundo e mergulho a profundidades superiores à cota máxima de operação do submarino: a partir da sua velocidade máxima, independentemente de sua

atitude, i.e. ângulo de trim, e profundidade, o submarino deverá ser capaz de parar, i.e. atingir um estado de velocidade nula, dentro de uma distância percorrida de no máximo três vezes o seu comprimento total.

A máxima taxa de variação da potência fornecida ao eixo pelo seu acionador, i.e. TP no caso de acionamento mecânico e MEP no caso de acionamento elétrico, os tempos envolvidos na manobra de reversão do hélice e a máxima potência desenvolvida na operação em marcha a ré deverão portanto ser compatíveis com este requisito.

Uma falha única de um componente dos circuitos de vapor e água de alimentação não deverá conduzir à perda da propulsão nem a perda da alimentação elétrica normal. Para tal, uma análise de modos de falha e efeitos destes circuitos deve ser realizada. Os seguintes eventos básicos devem ser considerados, a princípio:

- Perda de bombas de alimentação dos geradores de vapor;
- Perda de bombas de extração de condensado;
- Abertura ou fechamento inopinado de válvulas nas tubulações principais de vapor, de água de alimentação e de água do mar de resfriamento dos condensadores principais;
- Ruptura de tubos dos condensadores principais;
- Súbita perda total de vácuo nos condensadores principais, e sua eventual pressurização positiva.

Devido às características de saturação do vapor produzido pelos GV, as turbinas devem ser protegidas contra a possibilidade de danos decorrentes de eventuais variações no título do vapor de admissão. Esta proteção pode ser obtida pela inclusão de estágios de extração de umidade, nos quais as paletas móveis possuem ranhuras sobre as quais as gotículas de água arrastadas pelo vapor vêm a se romper e a película de água assim formada, sob a ação da força centrífuga, projeta esta água numa câmara periférica de onde ela é retirada por um sistema de purga. Materiais e revestimentos especiais das paletas devem também ser considerados para esta proteção.

Os condensadores principais devem ser protegidos contra sobrepressão positiva no caso de perda de vácuo, com ou sem ocorrência de ruptura dos tubos de resfriamento a água do mar.

Os possíveis escapes de fluido de resfriamento do Circuito Secundário, tais como as purgas do sistema de selagem das turbinas e do sistema de ejeção de ar dos condensadores principais, devem ter sua atividade monitorada e serem coletados de forma a não serem imediatamente liberados para o ambiente interno dos compartimentos de máquinas principais, permitindo o decaimento do Nitrogênio-16 (meia-vida de 7,3 s) que poderia estar neles contidos no caso de vazamentos nos geradores de vapor.

5.7.3 MÁQUINAS AUXILIARES

Outras necessidades de vapor do submarino, que não sejam de propulsão e de geração de energia elétrica principal, não devem ser atendidas diretamente pelo vapor gerado na IPN. Deverão ser empregados nestes casos vapor terciário, i.e. gerado indiretamente pela IPN, ou vapor gerado diretamente por fontes não nucleares.

Os sistemas de esgoto, lastro e de drenagem devem ser projetados de forma a prevenir a disseminação a bordo de líquidos radioativos. As partes destes sistemas que servem compartimentos nos quais líquidos radioativos podem vazar em serviço normal devem ser segregados e independentes do sistema de esgoto principal do submarino, e devem ser capazes de funcionar apropriadamente nas CPIN-1 a 4 e SOS-1 a 4. Bombas e tubulações que possam conter material radioativo em uma base temporária ou permanente devem ser adequadamente blindadas. Os drenos de compartimentos que não contêm materiais radioativos não devem atravessar o compartimento do reator nem os compartimentos de confinamento.

Os fluidos usados para resfriamento de componentes conectados ao Circuito Primário devem ser compatíveis com todos os materiais normalmente em contato com o refrigerante primário.

O desenvolvimento dos circuitos de água do mar a bordo deve ser o mais limitado possível. Estes circuitos não devem ser localizados em compartimentos normalmente inacessíveis, particularmente, tubulações e válvulas de água do mar não devem ser localizadas no Compartimento do Reator.

Para prover água do mar de resfriamento para as máquinas principais e as auxiliares essenciais, devem ser previstos sistemas com tomadas (caixas de mar) altas e baixas separadas em ambos os bordos. As descargas para o mar correspondentes devem ser asseguradas em todas as condições, incluindo aquelas de pouso no fundo, encalhe e atracação.

Devem ser previstas instalações para assegurar resfriamento ininterrupto e confiável para auxiliares essenciais quando o submarino está em dique seco. Podem ser usadas tomadas de água de cais, preferentemente com duas conexões independentes.

Os sistemas hidráulicos e pneumáticos servindo equipamentos auxiliares essenciais ou usado para propósitos de controle, devem ser providos de dois compressores ou bombas independentes, cada um capaz de atender à demanda requerida. Pelo menos um destes sistemas deve ser conectado ao Sistema Elétrico de Serviço em emergência.

Para cada sistema hidráulico e pneumático essencial a segurança da IPN devem ser previstos pelo menos dois reservatórios independentes e segregados, cada um com capacidade suficiente para atender aos serviços essenciais para os quais o sistema é projetado. A falha única de qualquer componente ativo destes sistemas deve ser considerada.

5.7.4 PROPULSÃO DE EMERGÊNCIA

Um SNA, cuja IPN é constituída por um único reator, deve ser dotado de uma fonte de geração de energia não nuclear para propulsão em emergência que deve ter potência e autonomia, em combustível, suficiente para permitir ao submarino:

- Manter condições mínimas de manobrabilidade na ocorrência de CPIN-3 e 4;
- Retornar a porto ou fundeadouro seguro em 20 dias, supondo-se que a perda da IPN ocorra nos limites externos da área de mobilidade especificada;
- Operar seguramente em áreas portuárias, mantendo o governo quando navegando na superfície em estado de mar 6 pela proa (escala Beaufort);
- Parar, i.e. atingir um estado de velocidade nula, a partir de uma velocidade inicial de 20 nós, após percorrer uma distância máxima de 5 vezes seu comprimento total.

Considerando as características particulares do SNA, a propulsão em emergência de um SNA deverá ser constituída, a princípio, por um MEP alimentado pelo Sistema Elétrico de Serviço SES em emergência:

- No caso de um SNA com sistema de acionamento mecânico do eixo propulsor, deverá ser previsto um MEP de emergência, acoplado ao eixo através de transmissão mecânica (embreagens, polias);
- No caso de acionamento elétrico do eixo de propulsor, o próprio MEP principal deverá poder ser chaveado para alimentação pelo SES em emergência, ou poderá ser previsto um MEP auxiliar para este fim específico, similar ao requerido para SNA com acionamento mecânico, caso a confiabilidade de um tal arranjo não possa atender aos critérios de probabilidade das CPIN.

A propulsão de emergência deve permanecer continuamente em estado de prontidão quando o submarino encontra-se navegando em áreas costeiras ou portuárias e quando operando próximo aos limites de seu envelope de segurança (profundidade x velocidade).

Quando operando sob propulsão de emergência, o SNA deverá ser capaz de navegar tanto na superfície como em imersão na cota máxima de operação ou em imersão na cota periscópica. Nesta condição, o Coeficiente de Indiscrição CI determinado pelas necessidade de recarga das fontes de potência transitórias do SES em emergência (baterias de acumuladores) deverá ser não superior a 50%. O CI é definido como a razão entre o tempo de navegação na cota periscópica ou na superfície e o tempo total de navegação do SNA.

5.7.5 SISTEMAS ELÉTRICOS

5.7.5.1 Sistema Elétrico de Serviço Principal

O sistema elétrico principal é composto de Turbo-Geradores de Serviço TGS, Diesel-Geradores Auxiliares DGA, quadros elétricos de distribuição principal e alimentações para os consumidores da IPN, plataforma-navio do submarino e seus sistemas de combate, devendo ser projetado de tal modo que:

- a falha de um único componente de um gerador elétrico principal ou de seus respectivos acionador principal e sistemas auxiliares não deva implicar em:
 - desligamento do reator;

- perda de manobrabilidade do submarino; e
- alterações nas condições operacionais normais da IPN e dos demais sistemas do SNA, nem nas condições de habitabilidade normais do submarino;
- a falha de um único componente do sistema de distribuição principal não deva implicar em:
 - desligamento do reator;
 - perda de manobrabilidade do submarino.

O Sistema Elétrico de Serviço principal deve ser dotado de pelo menos dois TGS, cada um com capacidade suficiente para prover a potência elétrica mínima necessária para manter o submarino em condições operacionais e de habitabilidade normais e anormais (CPIN-1, CPIN-2, SOS-1 e SOS-2), com a IPN em potência, sem recurso a geração auxiliar ou de emergência.

Os DGA são geradores elétricos independentes da IPN, dotados de sistemas próprios de suporte (óleo combustível, óleo lubrificante, resfriamento e partida) requeridos para substituir os TGS no caso destes tornarem-se inoperantes. O Sistema Elétrico de Serviço principal deve ser dotado de pelo menos um DGA, com capacidade suficiente para prover a potência elétrica necessária para atender condições operacionais mínimas de propulsão e de segurança nuclear, com a IPN desligada, e para manter condições mínimas de habitabilidade no submarino. Os DGA devem ainda ser capazes de manter a IPN na condição do reator desligado a quente e promover sua partida a partir desta condição. Os DGA podem ainda ser usados para promover a partida da IPN a partir da condição do reator desligado a frio, se sua capacidade é suficiente para prover, ao mesmo tempo, os serviços essenciais à segurança de submarino.

Os DGA devem ser projetados para partir e assumir carga automaticamente tão depressa quanto praticável e seguro (valor típico de 3 min.), no caso de perda de voltagem do barramento a eles associado. Para assegurar disponibilidade imediata dos sistemas de segurança da IPN, devem ser previstos dispositivos para redução imediata de carga, desconectando automaticamente os circuitos não essenciais à segurança da IPN e do submarino.

O sistema de óleo combustível para os DGA deve ser projetado considerando-se o critério de falha única e deve permitir a operação segura do SNA por pelo menos 30 dias. O

óleo combustível pode ser armazenado em tanques arranjados fisicamente de tal forma que tenham também funções de blindagem radiológica. Neste caso, tais tanques devem permanecer permanentemente cheios, sendo portanto lastrados à medida que óleo for sendo consumido.

Os DGA devem possuir um sistema de alimentação de ar para combustão do tipo “esnorquel” que permita sua operação com o SNA navegando à sua cota periscópica. O SNA deverá ainda possuir um sistema de exaustão dos gases de combustão adaptado à operação dos respectivos motores diesel tanto na superfície como na cota periscópica.

O sistema elétrico principal deve ser dividido em pelo menos duas seções de distribuição segregadas e independentes, cada seção tendo seu próprio painel de chaveamento principal alimentado alternativamente por qualquer um dos TGS. As seções devem ser projetadas de forma que qualquer CPIN-1 e 2 ou SOS-1 e 2 que incapacite uma delas não incapacite simultaneamente a outra.

A alimentação elétrica de equipamentos redundantes deve ser igualmente dividida entre as seções de distribuição e apropriadamente segregada. Os sistemas de distribuição devem ser projetados e localizados de forma a minimizar a probabilidade de falhas em modo comum.

5.7.5.2 Sistema Elétrico de Serviço em Emergência

O sistema elétrico de emergência é composto de fontes de potência elétrica transitória de emergência e de quadros elétricos de distribuição associados que provêem potência elétrica para os consumidores vitais à segurança da IPN e do submarino.

Uma fonte de potência elétrica transitória, tipicamente bancos de baterias, é uma fonte de potência que assegura a continuidade de alimentação elétrica aos consumidores especificados como vitais, quando as outras fontes de potência elétrica são indisponíveis. Os bancos de baterias devem ser mantidos permanentemente no seu melhor estado de carga tanto pelos TGS, durante a operação em potência da IPN, como pelos DGA, durante as condições de desligamento da IPN.

O Sistema Elétrico de Serviço em emergência, o DGA que alimenta cargas de emergência e os sistemas de distribuição associados devem ter independência, redundância e testabilidade suficientes para executar a sua função de segurança em todas as CPIN, assumindo-se uma falha única.

O Sistema Elétrico de Serviço em emergência deve ter capacidade suficiente para:

- Desligar o reator de forma segura;
- Levar o reator para um estado subcrítico a frio e mantê-lo neste estado por 30 dias, sem auxílio externo; e
- Garantir o atendimento de todas as funções de segurança de reator.

O sistema de distribuição de emergência das cargas associadas ao atendimento destes requisitos deve ser subdividido em seções segregadas, de forma que nenhuma CPIN incapacitará simultaneamente mais de uma delas. Cada painel de comando de distribuição em emergência deve ser capaz de ser alimentado por qualquer seção do Sistema Elétrico de Serviço principal. Os sistemas de proteção e de segurança do reator, assim como as demais cargas relacionadas com a segurança, devem ser alimentados pelo sistema de distribuição de emergência.

Cada DGA deve ser capaz de ser partido e controlado a partir do painel de comando de distribuição de emergência ao qual é conectado, ambos devendo estar localizados no mesmo compartimento. Os DGA devem ser capazes de ser partidos independentemente, tanto da ECM, como da estação de controle de emergência e de seu painel de controle local, a indisponibilidade das duas primeiras não impedindo a partida local. Equipamentos e sistemas não relacionados à função de emergência não devem ser arranjados nos mesmos compartimentos onde são arranjados os DGA e seus painéis de comando e controle. A partida dos DGA deve ser automática, em resposta a um sinal de perda de voltagem em seu barramento associado.

O Sistema Elétrico de Serviço em emergência deve assumir suas cargas elétricas dentro de um curto período de tempo após a partida dos DGA. Este tempo deve ser compatível com os tempos de evolução dos cenários associados às CPIN e SOS postuladas. Ele deve ser capaz de ser testado periodicamente a plena carga, verificando-se os tempos de

partida e de carregamento dos DGA sob condições de falhas simuladas. O SES em emergência deve ser independente das outras alimentações elétricas, de forma que falhas nestas últimas não comprometam sua confiabilidade e disponibilidade. O projeto do Sistema Elétrico de Serviço em emergência deve ser tal que a sincronização direta de suas fontes de potência não seja requerida para atender à demanda imediata dos sistemas de segurança da IPN.

Devem ser previstas fontes de potência transitórias com independência, redundância e testabilidade suficientes para executar suas funções de segurança em todas as CPIN e SOS, assumindo uma falha única. As fontes de potência transitórias devem ser segregadas de forma que nenhuma CPIN ou SOS incapacite mais de uma fonte de potência redundante. Cada fonte de potência transitória deve ser projetada para alimentar por um período mínimo de 30 minutos os seguintes consumidores da IPN:

- os controles e equipamentos de monitoração dos sistemas de proteção e de segurança do reator;
- sistemas de monitoração da radiação;
- outros controles e equipamentos de monitoração cujo funcionamento é previsto durante as CPIN e SOS acidentais;

Se baterias de acumuladores são empregadas como fontes de potência transitórias, a capacidade do sistema de carregamento destas baterias deve estar baseada na pior combinação de cargas permanentes e transitórias para restaurar o estado de carga do mínimo ao máximo.

6 PROCESSO DE LICENCIAMENTO

Neste Capítulo são propostas diretrizes para o estabelecimento dos procedimentos de análise e verificação da segurança do projeto e da fiscalização da construção e operação. Estes procedimentos estão associados à regulamentação do “Processo de Licenciamento” dos SNA. São ainda propostos e discutidos o conteúdo e a organização do Relatório de Análise de Segurança RAS, documento básico deste processo, concluindo assim a estrutura da Doutrina de Segurança proposta.

6.1 RESPONSABILIDADES E CONDIÇÕES

Um SNA deverá ser empregado no contexto de suas missões navais sem que a natureza nuclear de sua propulsão gere efeitos detrimenais à tripulação, pessoal de apoio em terra, público e meio ambiente em geral acima dos níveis de risco socialmente aceitáveis. A garantia do cumprimento deste objetivo geral é dada pelo Estado, que deve organizar uma base regulamentar legal adequada à análise e verificação das implicações sobre a segurança da obtenção deste tipo de navio de guerra.

Esta base regulamentar legal deve incluir o estabelecimento de uma Autoridade de Segurança Nuclear totalmente independente da Organização Operadora. Os requisitos gerais a serem satisfeitos pela implantação da ASN são estabelecidos por (IAEA, 1989). Para ser eficaz, a ASN deve ser provida de poderes legais, autoridade institucional e de recursos materiais e humanos necessários a garantir que possa desempenhar suas responsabilidades e funções. Tais poderes incluem a autoridade de controlar o processo de obtenção do SNA pela emissão de licenças administrativas, com condições associadas, e por inspeções de desempenho e conformidade a estas condições.

O objetivo da ASN é garantir à sociedade que os indivíduos, o público e o ambiente são efetivamente protegidos contra os potenciais efeitos adversos da obtenção do SNA, sendo os riscos associados à sua operação aceitáveis. Para atender a este objetivo, a ASN deve estabelecer políticas gerais e normas de segurança (princípios, critérios e requisitos) sobre as quais estão baseadas sua ação de regulamentação. Ela deve também executar a revisão e análise das informações de segurança submetidas pela Organização Operadora,

administrando as prescrições legais, tais como emissão, emenda e revogação de licenças ou condições de licenças, a partir de resultados de auditorias e inspeções, e fornecendo informações a outros órgãos governamentais e ao público, quando apropriado.

Em que pese estas responsabilidades da ASN, a responsabilidade pela segurança do SNA e de sua IPN e pela demonstração de que os riscos incorridos são aceitáveis permanece sobre a Organização Operadora, e não sobre a ASN.

Um dos meios pelos quais a Organização Operadora pode demonstrar que um nível de segurança adequado foi atingido é constituído pelas informações incorporadas no Relatório de Análise de Segurança RAS da Instalação. Estas informações também constituem a base para a tomada de decisões administrativas referentes ao processo de licenciamento da Instalação e as condições sob as quais ela é inspecionada.

O controle sobre a segurança nuclear é mantido, em última instância, pela emissão de licenças governamentais que autorizam, por etapas, o desenvolvimento do processo de obtenção de um SNA, estabelecendo condições a serem cumpridas pela Organização Operadora. Portanto, a tarefa primária da ASN é determinar quando conceder ou negar a solicitação de uma licença, com base em sua revisão e análise das propostas da Organização Operadora, contidas no RAS da Instalação. O conteúdo e profundidade destas propostas que fundamentam uma solicitação de licença deverá ser proporcional aos riscos potenciais associados e ao estágio particular do processo de licenciamento.

O processo de licenciamento deve englobar a regulamentação das seguintes etapas principais, que se desenvolvem paralelamente às fases do processo de obtenção do SNA (DGMM, 1994):

- Áreas de mobilidade e localizações fixas
 - Estudos de Exequibilidade
 - Projeto de Concepção
- Projeto e construção
 - Projeto Preliminar
 - Projeto de Detalhamento
 - Construção
- Comissionamento
 - Provas de Cais

- Operação
 - Descomissionamento
- Provas de Mar
 - Subordinação ao Comando Operativo
 - Desarmamento

O licenciamento é um processo dinâmico, iniciando-se na primeira fase do processo de obtenção do submarino, de estudos de exequibilidade, continuando até o descomissionamento. A primeira ação formal de licenciamento deve referir-se às áreas de mobilidade e localizações fixas, denominada Aprovação de Local AL. Em continuação, após aprovados os conceitos de segurança adotados no projeto, deve ser emitida uma Licença de Construção LC. Após a conclusão da construção e dos testes de montagem e comissionamento “a frio” (sem combustível), devidamente acompanhados pela ASN, deverá ser emitida uma Autorização para Utilização de Materiais Nucleares AUMN, que permitirá o carregamento do combustível e início dos testes de comissionamento “a quente”. Concluídos estes testes com sucesso, deverá ser emitida uma Autorização para Operação Inicial AOI, durante a qual será verificado o desempenho da Instalação sob condições de funcionamento reais. Sendo este desempenho satisfatório, será emitida uma Autorização para Operação Permanente AOP.

A emissão de cada uma destas licenças e autorizações é precedida pela apresentação do RAS pela Organização Operadora e subsequente revisão e análise pela ASN, acompanhada de inspeções, auditorias e testemunho de atividades críticas, antes do processo de obtenção do submarino avançar para sua fase seguinte.

6.1.1 ORGANIZAÇÃO OPERADORA

A Organização Operadora tem a responsabilidade global pela garantia da segurança durante todas as fases do processo de obtenção do submarino e do seu ciclo de vida. A conformidade com os requisitos impostos pela ASN não releva, entretanto, a Organização Operadora de sua fundamental obrigação de garantir a proteção dos tripulantes, do pessoal de apoio em terra, do público e meio ambiente. A Organização Operadora deve demonstrar à ASN que é capaz de assumir esta responsabilidade.

A Organização Operadora deve submeter as informações requeridas pela ASN em tempo hábil, sendo de sua responsabilidade os entendimentos com fornecedores que garantam a disponibilidade destas informações. É também de responsabilidade da Organização Operadora apresentar à ASN novas informações e alterações nas informações previamente submetidas.

A revisão e análise das informações pela ASN é um processo contínuo. As seções do RAS ou outros documentos devem ser submetidos à ASN assim que disponíveis, de acordo com um planejamento previamente acordado entre as partes. Esta abordagem permite a análise e procedimentos de aprovação sistemáticos, prevenindo atrasos desnecessários no processo de licenciamento.

6.1.2 AUTORIDADE DE SEGURANÇA NUCLEAR

A ASN é responsável basicamente por determinar que um SNA proposto pode ser construído, ser comissionado, navegar nas áreas de mobilidade, estacionar nas localizações fixas, passar por períodos de manutenção e ser descomissionado sem que os indivíduos, a sociedade e o meio ambiente incorram em riscos inaceitáveis. Em conexão com esta responsabilidade, a ASN deve:

- Adquirir um conhecimento aprofundado sobre o projeto da plataforma-navio e da IPN do SNA, dos conceitos de segurança sobre os quais estão baseados, do Programa de Garantia da Qualidade e dos procedimentos de operação propostos pela Organização Operadora;
- Realizar a revisão e análise da documentação técnica submetida pela organização Operadora. Esta revisão e análise se desenvolve desde um ponto de vista global de verificação da segurança do SNA até uma revisão e análise detalhada do projeto de sistemas, componentes e estruturas individuais, e de seu comportamento quando submetidos às CPIN e SOS postuladas;
- Exigir, sempre que necessário, modificações nos itens supracitados.

A base para revisão e análise dos aspectos de segurança nuclear de um SNA proposto são as informações contida no RAS apresentado pela Organização Operadora. A ASN deve tomar decisões referentes a:

- Se a Organização Operadora apresentou as informações necessárias ao propósito e escopo da revisão e análise de modo adequado;
- Se estas informações estão de acordo com os objetivos, princípios, critérios e requisitos de segurança para SNA, assim como outras normas e regulamentos aplicáveis;
- Se estas informações são corretas e precisas, com base em verificações independentes do projeto, fabricação e construção, incluindo realização de cálculos, testes e ensaios por métodos alternativos àqueles utilizados pela Organização Operadora, e testemunho de atividades críticas, por auditorias no Programa de Garantia da Qualidade aplicado pela Organização Operadora e por inspeções em suas instalações;
- Se as soluções de engenharia, em particular aquelas não usuais e consagradas, são viáveis e capazes de atender aos objetivos do projeto com respeito à segurança.

Em colaboração com a Organização Operadora, a ASN deve estabelecer previamente um cronograma para apresentação dos documentos que dão suporte técnico à solicitação de licenças e autorizações. A ASN deve preparar um programa de revisão e análise apropriado aos estágios do processo de licenciamento. A ASN deve acompanhar tão de perto quanto possível o desenvolvimento das atividades do processo de obtenção do SNA.

6.1.3 CONDIÇÕES DE ACEITABILIDADE

As condições de aceitação do SNA devem refletir uma adequada aplicação dos objetivos, princípios, critérios e requisitos de segurança. Elas devem ser estabelecidas tanto para os estados operacionais (CPIN-1/2 e SOS-1/2) como para os estados acidentais (CPIN-3/4 e SOS-3/4) do SNA.

As condições são estabelecidas de comum acordo entre a ASN e a Organização Operadora antes do efetivo início da construção do SNA, devendo incluir considerações sobre:

- Condições radiológicas:
 - Níveis de dose ALARA;
 - Limites (ou objetivos) de dose para a tripulação, pessoal de apoio em terra e o público em geral;

- Limites autorizados de liberação de materiais radioativos para o ambiente;
- Objetivos Detalhados de Segurança, conforme apresentados pelo Capítulo 4.
- Condições de desempenho, incluindo
 - Limites para danos no revestimento do combustível;
 - Limites para danos na barreira de pressão do Circuito Primário;
 - Limites para danos nos sistemas de Contenção e taxas de vazamento;
 - Manutenção do resfriamento do núcleo;
 - Limites de frequência para ocorrência de eventos operacionais antecipados e para condições acidentais particulares, incluindo limites de frequência para ocorrência de danos significativos para o combustível.

6.1.4 INFORMAÇÕES REQUERIDAS

A Organização Operadora deve fornecer à ASN todas as informações relevantes para a segurança do SNA. Estas informações deverão estar incluídas no RAS. Será apresentado a seguir um resumo das informações requeridas para cada um dos estágios do processo de licenciamento, notando-se que a requisição sequencial das informações levará a sucessivas atualizações, com cada versão do RAS correspondendo a um estágio particular do processo de licenciamento.

A elaboração do RAS deve ser iniciada simultaneamente ao projeto, de forma a permitir que seja tirado o máximo benefício das análises de segurança, assim como para permitir que a ASN familiarize-se paulatinamente com o projeto e a segurança do SNA. A quantidade de informações contidas no RAS, em cada estágio, deve ser aquela necessária e suficiente para que, tanto a Organização Operadora como a ASN, tomem as decisões sobre a aceitabilidade do SNA correspondentes àquele estágio.

6.1.4.1 Planejamento de Apresentação das Informações

O cronograma para elaboração das diferentes seções do RAS deve ser estabelecido desde o início do processo de obtenção do SNA. Como a aprovação de uma fase é requerida antes de começo da fase seguinte, é importante que o RAS esteja disponível para revisão e análise numa sequência e intervalos de tempo previamente acordados entre a

Organização Operadora e a ASN. A abrangência e detalhamento das análises apresentadas em cada etapa também deve ser previamente acordada, de modo a evitar atrasos no processo de revisão devido a exigências adicionais da ASN.

Este cronograma deverá prever períodos razoáveis de tempo para que cada revisão e sua correspondente análise pela ASN possam ser completadas antes do começo da fase subsequente.

6.1.4.2 Áreas de Mobilidade e Localizações Fixas

Deverá ser requerido da Organização Operadora, nesta fase, o fornecimento de informações suficientes para demonstrar à ASN que as áreas de mobilidade e as localizações fixas propostas são compatíveis com os Riscos Residuais da IPN do SNA. Devem ser identificadas possíveis dificuldades que deverão ser solucionadas durante as fases subsequentes do processo de licenciamento. As informações sobre as áreas marítimas e as localizações litorâneas deverão ser apresentadas, juntamente com informações preliminares sobre o SNA e sua interação com o ambiente. Além disto, uma avaliação preliminar do impacto radiológico da operação nas CPIN e SOS postuladas para a tripulação, o pessoal de apoio em terra, o público e o ambiente deverá ser apresentada, discutindo-se o caráter “envelope” dos resultados obtidos.

6.1.4.3 Projeto e Construção

Para obtenção da Licença de Construção LC, a Organização Operadora deverá submeter informações que demonstrem que o projeto resultará em uma Instalação segura e a construção atenderá às especificações. Estas informações deverão conter uma descrição do projeto da IPN e da plataforma-navio do SNA e dos sistemas de processo e segurança associados, e os resultados das análises de segurança que demonstrem a adequação do projeto de sistemas, componentes e estruturas aos objetivos, princípios, critérios e requisitos de segurança nuclear. Estas informações deverão ser submetidas à ASN sob a forma do RAS, que terá um caráter preliminar e portanto sujeito a atualizações conforme a evolução do projeto.

Aqueles aspectos do projeto que devem ser submetidos à ASN para revisão e análise antes de se encontrarem finalizados devem ser explicitamente identificados, de forma que as atividades para sua conclusão possam ser efetivamente desenvolvidas durante a fase de construção. As informações contidas no RAS preliminar deverão ser portanto atualizadas e submetidas à ASN conforme o projeto de detalhamento e construção do SNA se desenvolve. Estas informações complementares poderão ser submetidas sob forma de versões revisadas do RAS, ou sob forma de suplementos técnicos, conforme o caso.

O RAS é o documento principal para revisão e análise da segurança do SNA pela ASN nesta fase, e cuja aprovação permitirá o progresso de projeto de detalhamento e construção.

A interação entre a Organização Operadora e a ASN deverá ser intensiva nesta fase, com a ASN revisando o projeto e inspecionando as atividades de construção para confirmar que as intenções declaradas no RAS estão sendo realmente cumpridas e os programas de gerenciamento, em particular o PGQ, estão operando efetivamente.

6.1.4.4 Comissionamento

Quando a construção estiver suficientemente avançada, as informações contidas no RAS serão atualizadas e revisadas para que a Organização Operadora obtenha as autorizações exigidas para executar o comissionamento. O RAS atualizado e revisado incluirá o Programa de Comissionamento, demonstrando sua adequação e suficiência. A descrição da IPN e da plataforma-navio do SNA “como construída” (*as-built*), as análises das CPIN e SOS postuladas e a capacidade dos sistemas de segurança para limitar suas consequências deverão ser documentadas completamente nesta versão do RAS, que será a base técnica para solicitação à ASN da Autorização para Utilização de Materiais Nucleares AUMN.

6.1.4.5 Operação

Para solicitação da Autorização para Operação Inicial AOI, a Organização Operadora submeterá a revisão final de todas as informações apresentadas nas versões anteriores do RAS, acrescidas dos resultados obtidos durante a execução do Programa de Comissionamento e das Especificações Técnicas de operação e Procedimentos Operacionais

a serem efetivamente implementados. Os resultados do Programa de Comissionamento deverão demonstrar que as especificações de projeto e construção foram plenamente atendidas.

Durante a fase de operação inicial, cuja duração deverá ser previamente acordada entre a Organização Operadora e a ASN, serão verificados, durante períodos de operação assistida contínuos, a real adequação e segurança dos procedimentos operacionais preconizados e do desempenho da Instalação.

Concluída esta fase, o RAS será revisto e atualizado de acordo com os resultados obtidos, atingindo assim sua versão final. A partir da revisão e análise desta última versão do RAS, a ASN emitirá uma Autorização para Operação Permanente AOP por um período determinado a seu critério.

Durante a fase de operação permanente, com uma periodicidade não inferior a 5 anos, e sempre após qualquer alteração significativa de projeto ou de procedimentos operacionais, uma revisão do RAS deverá ser empreendida. Nestas revisões serão feitas comparações do RAS existente com a experiência operacional precedente, incluindo eventos relevantes para a segurança ocorridos, resultados de monitoramento radiológico, e outros aspectos verificados durante a operação. Estas revisões do RAS deverão ser submetidas pela Organização Operadora à ASN, solicitando-se a renovação da AOP.

Eventuais necessidades operativas que necessitem variações temporárias das condições de funcionamento previstas pelo RAS existente deverão ser submetidas previamente à ASN, indicando-se claramente quais os desvios solicitados e o período de tempo no qual estes desvios seriam efetivados. A ASN emitirá então autorizações específicas para estes casos. Caso a necessidade destes desvios ocorra de forma não antecipada, durante períodos de missão no mar do SNA, a decisão quanto a sua execução caberá a um colegiado formado pelo Comandante, Imediato e Chefe do Departamento de Máquinas do SNA. Caso a situação operativa do submarino permita, esta decisão deverá ser documentada antes de sua execução. Em todos os casos, ao final da missão, com retorno ao porto, uma tal ocorrência deverá ser relatada à ASN, sugerindo-se, conforme sua relevância para a

segurança, a implementação de novos procedimentos operacionais especificamente adaptados. Aprovados estes novos procedimentos, eles seriam incorporados ao RAS.

6.1.4.6 Descomissionamento

A Organização Operadora deverá incluir, já nas versões iniciais do RAS uma proposta de estratégia de descomissionamento do SNA, que deverá ser devidamente aprovada pela ASN. O detalhamento desta estratégia, sob a forma de um Programa de Descomissionamento, entretanto, somente será elaborado nos estágios finais do ciclo de vida útil do submarino, assim que for definida uma data para o seu desarmamento

A inclusão desta estratégia tem como objetivo verificar se o projeto prevê disposições específicas visando facilitar a realização futura das atividades de descomissionamento e avaliar, preliminarmente, que as mesmas resultam em Riscos Residuais Aceitáveis, especialmente no que tange à radioproteção do pessoal de apoio em terra que irá executá-las e ao gerenciamento dos rejeitos que serão gerados.

Após a remoção de todo o combustível da IPN do SNA, o RAS deixa de ser o documento principal de licenciamento. A partir desta condição, serão elaborados Relatórios de Descomissionamento periódicos, que apresentarão o progresso das atividades previstas pelo Programa de Descomissionamento previamente aprovado pela ASN e eventos relevantes à segurança ocorridos durante a execução destas atividades, que poderão implicar em revisão do Programa.

6.2 RELATÓRIO DE ANÁLISE DE SEGURANÇA

6.2.1 PROPÓSITO E ESCOPO

O RAS é elaborado pela Organização Operadora para a justificação do projeto e constitui a base para a operação segura da IPN do SNA. Este documento é um principal vínculo entre a Organização Operadora e a ASN, desde que é o documento que fundamenta tecnicamente a emissão das requeridas licenças e autorizações. Além disto, a elaboração do RAS serve também aos seguintes propósitos:

- Realimentar o projeto, confirmando que os sistemas individuais estão corretamente integrados, desde que o projeto do SNA e o desenvolvimento do RAS sejam processos complementares e interativos;
- Assegurar que a análise de segurança identificou corretamente os problemas de segurança pertinentes ao projeto e que a análise de segurança e o projeto são consistentes;
- Auxiliar na avaliação dos critérios de projeto adotados, suas limitações e requisitos, e na avaliação dos Riscos Residuais da Instalação;
- Auxiliar no treinamento dos tripulantes do SNA, em especial aqueles diretamente afetos à operação da IPN;
- Assegurar o estabelecimento de limites e condições operacionais para os parâmetros importantes para a segurança, que deverão ser respeitados durante todas as fases do Ciclo de Vida do SNA, de forma a ter margens de segurança adequadas à proteção dos indivíduos e meio ambiente.

O RAS apresentará uma descrição detalhada das áreas de mobilidade e localizações fixas do SNA, da IPN e da plataforma-navio, dos sistemas de missão que possuem importância para a segurança e das instalações de apoio em terra, referenciando, para estas últimas, aquelas que possuem RAS específico. Apresentará uma descrição detalhada dos princípios, critérios e requisitos de segurança adotados no projeto, demonstrando seu efetivo atendimento. Analisará os Riscos Potenciais associados à operação da IPN do SNA, demonstrando que os Riscos Residuais, após a consideração das ações de segurança adotadas, encontram-se a um nível aceitável. Conterá análises de segurança das CPIN e SOS postuladas e das características de segurança incorporadas para evitar ou minimizar a probabilidade de ocorrência de acidentes, ou para mitigar as suas conseqüências tanto no projeto como nos procedimentos operacionais.

O RAS estabelecerá um conjunto de limites e condições operacionais a ser incorporado nas licenças e autorizações solicitadas. Também apresentará os detalhes da condução da operação, incluindo sua organização e distribuição de responsabilidade, do Programa de Garantia da Qualidade estabelecido para o projeto e operação, do

planejamento de emergências e da segurança física da IPN. Estes últimos tópicos poderão ser objeto de documentos separados, porém devidamente referenciados pelo RAS.

6.2.2 REQUISITOS ESPECÍFICOS

O Relatório de Análise de Segurança RAS consiste na documentação submetida inicialmente à ASN, juntamente com apreciações, complementações e correções posteriores.

O RAS deve conter análises sistemáticas da segurança nuclear do SNA, tanto em termos de projeto como de construção, de operação e de descomissionamento do submarino e sua IPN, para assegurar que os riscos para a tripulação, o pessoal de apoio em terra, o público e o ambiente sejam socialmente aceitáveis. O RAS deve conter todas as informações necessárias e suficientes para permitir que a ASN realize a sua própria análise da segurança do SNA. As informações devem ser apresentadas de forma concisa, os vários itens sendo tratados em profundidade proporcional à sua importância para a segurança do SNA.

O RAS do SNA é um documento classificado com grau de confidencialidade determinado previamente pela ASN, em conformidade com a legislação nacional para salvaguarda de assuntos sigilosos.

A ASN poderá requerer que o RAS seja avaliado por um grupo independente de revisão e análise. Neste caso, os resultados da revisão e análise serão informados diretamente à ASN, que acatará ou não as proposições feitas, notando-se que somente a ASN tem autoridade para exarar exigências e emitir licenças e autorizações à Organização Operadora. Adicionalmente, a ASN poderá determinar que os resultados das análises de impacto ambiental da operação do SNA sejam submetidos a uma audiência pública. Para este propósito, a Organização Operadora deverá elaborar uma versão simplificada e ostensiva do RAS.

O RAS apresentará as referências bibliográficas necessárias para o processo de sua revisão e análise. Este material de referência deverá estar livremente disponível à ASN, sendo o acesso a ele não sujeito a qualquer restrição que possa comprometer a revisão e análise adequadas. Tais referências não precisam ser submetidas em conjunto com o RAS, mas

devem ser mantidas disponíveis pela Organização Operadora para consulta pela ASN, através de solicitação formal.

Devido ao volume de documentos que apoiam tecnicamente as informações contidas no RAS, um sistema de controle de documentação deve ser estabelecido para administrar e controlar seu trâmite. Este sistema controlará a atualização, revisão e análise, emissão ou cancelamento de relatórios conforme o Programa de Garantia da Qualidade, de forma que as informações estejam sempre atualizadas.

O RAS deve ser preparado de forma a facilitar a inclusão de informações complementares ou de revisões, todas as páginas sendo datadas e marcadas claramente em seqüência. As páginas revisadas e as complementações devem ser nitidamente identificadas de acordo com o número de revisão e análise e a data da mudança.

Desenhos, gráficos, diagramas, informações tabulares e quadros devem ser usados sempre que as informações puderem ser apresentada de forma mais adequada ou conveniente por esses meios.

Todas as informações apresentadas devem ser legíveis, os símbolos devem ser definidos e os desenhos não devem ser reduzidos a escalas que tornem a interpretação difícil. Deve-se usar o sistema de unidades SI e as unidades de medida aplicadas na prática pela instrumentação real da instalação. Podem ser chamadas referências específicas ao longo do texto, contanto que as mesmas estejam imediatamente disponíveis para a ASN.

6.2.3 DESENVOLVIMENTO DA ANÁLISE

O desenvolvimento da análise de segurança e do projeto do SNA são processos complementares, que devem ser conduzidos de forma interativa. A análise de segurança é empregada principalmente para permitir ao operador um entendimento completo das bases para a operação segura da IPN e para demonstrar à ASN o modo pelo qual o projeto do SNA e os procedimentos operacionais relacionados contribuirão para a prevenção de acidentes. A análise de segurança incluirá análises de resposta da IPN ao espectro de CPIN e SOS postulados. A análise de segurança também contribui significativamente para a

determinação dos limites e condições operacionais, como também das especificações de projeto e construção de sistemas, componentes e estruturas.

A análise de segurança deverá identificar os Acidente Básicos de Projeto. Adicionalmente, a análise de segurança deverá identificar os acidentes além da base de projeto, cuja análise determinará os procedimentos de gerenciamento de acidentes e os planos de emergência.

A análise das CPIN e SOS postuladas identificarão claramente todos os parâmetros que caracterizam as condições iniciais assumidas, que deverão ser apresentados no RAS, e determinarão a base para a determinação dos limites e condições operacionais. É apresentada a seguir uma lista, não exaustiva, destes parâmetros.

- Coeficiente de reatividade do moderador;
- Coeficiente de reatividade dos vazios no moderador;
- Coeficiente de reatividade da temperatura do combustível;
- Tempo de vida efetivo dos nêutrons prontos;
- Fração de nêutrons retardados;
- Fluxo de calor médio;
- Fluxo de calor máximo;
- Mínimo *Departure from Nucleate Boiling* DNB;
- Mínimo fluxo crítico de calor;
- Margem de injeção de vazios;
- Margem de injeção de instabilidade de vazão;
- Distribuição axial de potência;
- Distribuição radial de potência;
- Fator de canal quente;
- Vazão de refrigerante no núcleo;
- Temperatura de saída do refrigerante do núcleo;
- Temperatura de entrada do refrigerante do núcleo;
- Temperatura de saída do refrigerante do canal quente;
- Máxima temperatura na linha de centro do combustível;

- Temperatura do revestimento do combustível;
- Inventário de refrigerante no Reator e Circuito Primário;
- Nível de refrigerante no Reator e Circuito Primário;
- Fluxo de massa e temperatura do vapor do secundário do Gerador de Vapor;
- Fluxo de massa, temperatura da água de alimentação do secundário do Gerador de Vapor;
- Queima (*burnup*) do combustível (valor de descarregamento, razão valor máximo/valor médio)
- Valores das barras de controle (reatividade diferencial e integral, margens de desligamento)
- Inserção de reatividade durante o transiente.

Os métodos básicos de análise usados para as avaliações de segurança da IPN do SNA são determinísticos. Estas técnicas são caracterizadas pelo seu caráter conservador e estão baseado em:

- Definição a priori do conjunto de CPIN (1 a 4) e SOS (1 a 4) que compõem a base de projeto e do conjunto de CPIN e SOS complementares que dão suporte aos procedimentos de gerenciamento de acidentes e planejamento de emergências
- Modelos físicos e métodos matemáticos de análise de desempenho e comportamento de sistemas, componentes e estruturas
- Definição de condições iniciais e parâmetros físicos “envelope”;
- Critérios objetivos de aceitação.

Pelo emprego destes métodos, garante-se, com uma razoável margem de certeza, que o objetivo último de limitar a liberação de materiais radioativos pode ser alcançado. O caráter conservador dos métodos tende a superestimar as quantidades de materiais radioativos liberados, permitindo porém a efetiva modelagem dos fenômenos complexos envolvidos.

A mais severa destas liberações, decorrente do Acidente Básico de Projeto (ou “máximo acidente verossímil”) deverá ser considerada na análise de conseqüências requerida para aprovação das áreas de mobilidade e localizações fixas e para estabelecer os requisitos de projeto dos dispositivos especiais de segurança da IPN. A seleção deste acidente está

baseada na experiência operacional de instalações semelhantes e no *engineering judgement*, sem considerar explicitamente as probabilidades dos cenários acidentais que a ele conduzem.

Esta abordagem verifica então o desempenho dos três primeiros níveis de defesa em profundidade da Instalação, que constituem sua base de projeto. Complementar-mente, ainda dentro da abordagem determinística, deverão ser verificados os dois últimos níveis de defesa em profundidade.

Para o quarto nível, de gerenciamento de acidentes, deverá ser garantida a continuidade do controle das conseqüências do ABP a longo prazo, ainda que ocorram determinados eventos indesejados não postulados na base de projeto. Para tal, são desenvolvidos procedimentos operacionais e dispositivos de emergência especiais para enfrentar eventos pós-acidentais que venham a ameaçar a manutenção das três funções básicas de segurança, em especial a remoção de calor residual do núcleo acidentado e a estanqueidade da Contenção. Estes eventos, específicos a cada projeto, podem ser agrupados em quatro famílias:

- Distúrbios na disponibilidade da fonte fria;
- Distúrbios na continuidade das alimentação de energia;
- Elevação da taxa de vazamentos da Contenção (com relação à taxa de vazamentos postulada na base de projeto); e
- Sobrepressão no interior da Contenção (com relação à pressão máxima postulada pela base de projeto).

Estes procedimentos operacionais de emergência constituem o chamado Plano de Emergência Local PEL, cuja execução é de exclusiva responsabilidade da Organização Operadora. O PEL terá então como objetivos proteger a tripulação e o pessoal de apoio em terra e evitar liberações reais de materiais radioativos para o ambiente em quantidades superiores àquelas definidas pela base de projeto, sendo composto por ações segurança tomadas dentro dos limites do SNA e das instalações de apoio em terra.

Para o quinto nível, de resposta a emergências, postula-se a falha na execução do PEL, não sendo mais garantida a continuidade do controle das conseqüências do ABP no caso ocorrência dos eventos indesejados não postulados pela base de projeto, mas

considerados pelo quarto nível. Neste caso, ocorrerão liberações reais de materiais radioativos para o ambiente em quantidades superiores às aquelas definidas pela base de projeto, o que requer medidas de mitigação de consequências para o público e o meio ambiente no sentido de tornar aceitáveis as consequências decorrentes. Estas medidas, tomadas fora dos limites do SNA e das instalações de apoio em terra, compõem o Plano de Emergência Externo PEE. Devido à abrangência destas medidas, elas já não são mais de responsabilidade da Organização Operadora, sendo assumidas por outras organizações governamentais ao nível local e nacional.

A abrangência geográfica e o tipo das ações de segurança a serem implementadas pelo PEE dependerão da magnitude do termo-fonte acidental postulado (tipos e atividades dos materiais radioativos liberados) e das características do local onde ele será disperso. A intensidade do termo-fonte dependerá do inventário de produtos radioativos da IPN acidentada e da eficiência das ações de segurança executada pelo PEL.

Para aperfeiçoar a análise realizada pelos métodos determinísticos, avaliando a verossimilhança de suas hipóteses e postulados, deverão ser aplicados métodos probabilísticos. Estes métodos assumem que todos os eventos são possíveis e que qualquer número de falhas simultâneas pode ocorrer, embora suas probabilidades possam ser muito baixas. Alguns acidentes ou combinações de acidentes podem ter consequências menores do que aquelas consideradas pelos métodos determinísticos, mas quando eles são ponderados pela sua verossimilhança, eles podem representar uma parcela significativa do Risco Residual da Instalação, impondo portanto novas demandas de segurança ao projeto.

Além disto, a abordagem determinística tem dificuldades em tratar efetivamente as interdependências de sistemas, tais como falhas de causa comum, as quais os métodos probabilísticos podem tratar analítica e quantitativamente. A aplicação destas técnicas também conduz a significativas melhorias na compreensão de comportamento dos sistemas e suas interações, assim como do papel desempenhado pelos operadores nas condições acidentais.

A execução de uma Análise Probabilística de Segurança APS global para o SNA deve ser considerada como um objetivo a ser alcançado a longo prazo, não tendo, a

princípio, um caráter de exigência. A aplicação de métodos probabilísticos para análise limitada de sistemas ou funções de segurança específicas podem, entretanto, ser requeridas pela ASN.

A definição destes casos deve ser previamente acordada entre a Organização Operadora e o ASN. Exemplos típicos são a análise de confiabilidade do Sistema de Resfriamento de Emergência SRE e do Sistema de Proteção do reator, e a análise de modos de falha, efeitos e criticidade dos sistemas da contenção e da função de desligamento automático do reator.

Os resultados globais obtidos da análise de segurança pelos métodos determinísticos, complementados pelos resultados parciais obtidos da análise de segurança pelos métodos probabilísticos da IPN do SNA deverão ser apresentados no RAS e comparados com as condições mínimas preconizadas pela ASN, determinando assim se os Riscos Residuais são socialmente aceitáveis.

6.2.4 CONTEÚDO DO RELATÓRIO

A seguir serão identificadas as seções que devem compor o RAS, acompanhadas de uma apresentação sucinta de seu conteúdo. O Anexo O apresenta uma itemização proposta para o RAS.

6.2.4.1 Informações Gerais e Sumário:

A introdução deve oferecer ao leitor uma apresentação global do SNA, incluindo seu projeto, construção e operação do submarino e a de sua IPN, assim como um resumo das conclusões relativas à segurança do navio. Deve incluir uma breve descrição dos seguintes tópicos:

- Projeto do submarino e suas características principais;
- Reator e Circuito Primário, identificando seus parâmetros do projeto;
- Estruturas de contenção e confinamento;
- Instalação Propulsora Nuclear;
- Máquinas e sistemas auxiliares;
- Sistemas de geração e distribuição de energia elétrica;

- Sistema de propulsão auxiliar;
- Proteção contra carregamentos impulsivos e impactos diretos.

O sumário deve incluir uma avaliação da segurança nuclear juntamente com uma discussão das disposições adotadas para prevenir e limitar as consequências de acidentes e comentários relativos ao nível de segurança proporcionado à tripulação, ao público e ao ambiente.

6.2.4.2 Base de Projeto Ambiental

Essa seção deve oferecer informações sobre as condições ambientais assumidas como base de projeto, dando ênfase especial a fatores importantes para a segurança nuclear assim como para a segurança global do submarino. Deve haver uma especificação dos fundamentos lógicos empregados para a seleção destas condições, incluindo:

- Estados do mar;
- Fenômenos meteorológicos extremos;
- Seleção dos tempos de vida útil e carregamentos cíclicos assumidos para os requisitos de resistência à fadiga;
- Fatores de riscos ambientais específicos às áreas de mobilidade e localizações fixas.

6.2.4.3 Normas de Segurança

Esta seção deve identificar a base normativa adotada para o SNA, tanto para o submarino propriamente dito quanto para sua IPN, listando as normas de engenharia naval e nuclear, de radioproteção, e os regulamentos administrativos sobre os quais o projeto, a construção e a operação estão baseados. Uma discussão detalhada deve abordar os seguintes itens:

- Projeto, construção e operação
 - Normas de projeto;
 - . Engenharia naval;
 - . Engenharia nuclear;
 - . Proteção radiológica;
 - . Projeto mecânico de vasos de pressão e tubulações nucleares;
 - . Projeto mecânico das estruturas do casco, vasos de pressão e tubulações resistentes à pressão da água do mar;
 - . Regulamentos da ASN.

- Códigos e práticas de construção empregadas
- Procedimentos de Operação:
 - . Condições normais, anormais e de emergência com o submarino operando nas áreas de mobilidade;
 - . Condições normais, anormais e de emergência com o submarino atracado ou fundeado nas localizações fixas pré-determinadas;
 - . Condições normais, anormais e de emergência com o submarino em períodos de manutenção nas localizações fixas pré-determinadas;
 - . Condições em que a operação é autorizada na presença de desvios dos parâmetros básicos de segurança.
- Garantia da Qualidade:
 - garantia de qualidade no planejamento e controle, projeto e fornecimentos;
 - garantia de qualidade na construção, fabricação e comissionamento;
 - garantia de qualidade na operação e manutenção.

6.2.4.4 Descrição Técnica e Avaliação do Projeto

Esta seção deve oferecer uma descrição técnica e uma avaliação do projeto dos vários sistemas, estruturas e componentes que são importantes para a segurança do submarino e de sua IPN. Nesta seção devem ser especificados os parâmetros de desempenho e de projeto requeridos dos sistemas, assim como as condições ambientais em que deverão ser atendidos. A avaliação do projeto deve ser feita para demonstrar que o projeto dos sistemas e componentes são compatíveis com as bases de projeto adotadas.

Devido à natureza de alguns sistemas, recomenda-se que um determinado sistema existente seja listado sob mais de um subtítulo, para que se possa reconhecer os vários requisitos envolvidos no seu projeto e operação.

A avaliação deve considerar as seguintes informações como aplicáveis ao sistema ou estrutura que está sendo analisado:

- definição das funções desempenhadas;
- descrição;
- base de projeto;
 - parâmetros operacionais normais e limitantes;
 - seleção e qualificação dos materiais;

- projeto mecânico;
- projeto termohidráulico;
- projeto nuclear;
- inspeção e testes;
- manutenção;
- requisitos de garantia de qualidade;
- avaliação do projeto;
 - análise estrutural;
 - cálculos termohidráulicos;
 - cálculos de neutrônica e blindagem.

A descrição e informações requeridas devem aplicar-se aos sistemas listados indicativamente a seguir, notando-se não constituir uma lista exaustiva:

- Submarino e seus sistemas de plataforma e de missão;
 - Arranjo físico;
 - Características gerais;
 - Estabilidade e subdivisão;
 - Capacidade de sobrevivência;
 - Estrutura e resistência do casco;
 - Proteção contra choques e impactos;
 - Proteção contra efeitos de Interferências Eletro-Magnéticas IEM
 - Navegação;
 - Comunicações;
 - Dispositivos de salvatagem;
 - Instalações de Máquinas;
 - . Geração e distribuição de energia elétrica;
 - . Eixo propulsor e hélice
 - . Aparelho de governo;
 - . Aparelho de suspender e fundear
 - . Proteção e combate a incêndio;
 - . Sistemas de condicionamento de ar e controle ambiental interno;
 - . Sistemas de esgoto e lastro;
 - Sistemas associados à missão
 - . Armazenagem e movimentação de armas e munições;
 - Sistemas de Apoio em Terra;
 - . Movimentação de combustível nuclear;
 - . Transferência de rejeitos;
 - . Alimentação elétrica, hidráulica, pneumática e de vapor auxiliar
- Reator e Circuito Primário
 - Barreira de pressão;
 - . Vaso de pressão do reator;

- . Bombas de circulação de refrigerante primário;
- . Válvulas de segurança, alívio e isolamento;
- . Tubulação principal do Circuito Primário;
- . Geradores de Vapor;
- . Pressurizador;
- Sistemas auxiliares:
 - . Purificação do refrigerante primário
 - . Controle volumétrico do refrigerante primário;
 - . Descarga de refrigerante primário;
 - . Resfriamento de componentes do Circuito Primário;
 - . Desaeração do Circuito Primário
- Núcleo do Reator;
 - . Elementos combustíveis, incluindo enriquecimento;
 - . Veneno queimável e barras de controle;
 - . Física do núcleo;
 - Fluxos de nêutrons e distribuição de potência;
 - Estabilidade de potência;
 - Cálculos de reatividade;
 - . Estruturas internas do Reator;
 - . Termohidráulica do núcleo;
- Instrumentação e Controle;
 - . instrumentação e controle do reator;
 - . instrumentação e controle para operação normal;
 - . instrumentação e controle de segurança;
- Dispositivos de Segurança
 - . Sistemas para controle de reatividade;
 - . Desligamento do reator;
 - . Sistema de proteção do reator;
 - . Resfriamento de emergência do núcleo;
 - . Remoção do calor residual;
 - . Injeção de veneno solúvel;
 - . Estrutura e isolamento da contenção;
 - . Detecção de vazamentos
- Estações de Controle de Máquinas (principal e de emergência):
 - Controles disponíveis;
 - Instrumentação;
 - Localização e descrição;
 - Proteção contra incêndio;
 - Condições de habitabilidade e de acesso.
- Outros sistemas:
 - Rejeitos radioativos;
 - Água de suplemento do Circuito Primário e Circuito Secundário;

- Controle de veneno solúvel;
- Controle ambiental da Contenção;
- Sistemas auxiliares de processo;
- Controle químico da água do Circuito Primário e Circuito Secundário;
- Condicionamento e purificação do ar nos compartimentos de máquinas

6.2.4.5 Performance da IPN

Esta seção deve apresentar informações detalhadas sobre o comportamento da Instalação em funcionamento normal. Para cada fase descrita abaixo e quaisquer outras julgadas necessárias, as condições dos sistemas envolvidos e os valores dos parâmetros importantes devem ser especificados, mostrando que a Instalação pode funcionar dentro dos limites estabelecidos pela base do projeto e análise de segurança. As informações sobre o funcionamento normal devem incluir:

- Partida
- Operação em potência constante
- Transientes de potência;
- Parada a quente;
- Parada a frio
- Partida após desligamento não intencional.

6.2.4.6 Proteção Radiológica

Os critérios básicos de radioproteção devem ser discutidos, com informações sobre:

- Meios para garantir que os níveis de radiação sejam tão baixos quanto razoavelmente praticável;
- Limites de dose equivalente;
- Limites de liberação de radioisótopos e correspondentes atividades;
- Níveis de fluxo de dose e de contaminação referentes à subdivisão do submarinos em zonas de radiação e restrições de acesso resultantes;
- Procedimentos para gerenciamento de materiais radioativos e controle de acesso às áreas controladas e supervisionadas em condições normais (CPIN-1);
- Procedimentos para acessar as áreas controladas e supervisionadas em condições anormais, incidentais e acidentais (CPIN-2, CPIN-3, CPIN-4).

As blindagens radiológicas devem ser apresentadas e discutidas, oferecendo o máximo de informações para cada uma delas:

- Identificação da fonte a ser blindada;
- Localização e objetivo da blindagem;
- Dimensões e materiais empregados;
- Verificação do projeto através de cálculos e ensaios, conforme apropriado.

Os níveis de radiação esperados ou permitidos durante qualquer CPIN devem ser comparados com níveis pré-estabelecidos.

As informações de monitoramento da radiação devem incluir a discussão dos princípios do projeto e a localização, tipo, sensibilidade, extensão das medidas e métodos de apresentação e alarme aplicáveis aos detetores empregados, e a sua capacidade para suportar as CPIN.

As informações relativas à liberação de radioatividade no ambiente devem incluir a discussão de:

- Instrumentação e monitoramento dos efluentes da IPN;
- Atuação manual e automática de sistemas de limitação das liberações.

Os laboratórios, vestiários, locais e dispositivos empregados para lidar com pessoas ou objetos contaminados devem ser descritos e a localizados.

6.2.4.7 Análise de Falhas e Acidentes

A análise de segurança deve conter informações detalhadas sobre as seqüências possíveis de eventos que afetem a IPN e o submarino, devido a:

- Falhas ou mau funcionamento de sistemas, componentes ou estruturas;
- Erro humano na operação da IPN;
- Agressões externas tais como incêndio, explosões, alagamentos, “fortunas do mar”.

A análise deve descrever as seqüências possíveis de eventos subsequentes a falhas ou acidentes através de:

- Identificação de eventos inicializadores;
- Estabelecimento das causas dos eventos inicializadores;

- Determinação da sequência de eventos subsequentes ao evento inicializador;
- Determinação das consequências resultantes.

A análise deve:

- Verificar se a base do projeto é adequada;
- Descrever a distribuição dos materiais radioativos no SNA usada na análise e como uma base para a avaliação dos efeitos radiológicos;
- Identificar os ABP e fornecer os termos-fonte assumidos na análise.

A análise deve incluir, para as CPIN e SOS apresentadas pelo Capítulo 4:

- Valores iniciais dos parâmetros utilizados;
- Hipóteses sobre as quais os cálculos são baseados;
- Demonstração dos resultados obtidos;
- Precisão e margens de segurança adotadas nos cálculos;
- Inventários radioativos e composições de isotópicas considerados;
- Defeitos de revestimento e falhas do combustível postuladas;
- Revisão e análises de vazamento e de eficiência de absorção e filtração da Contenção,;
- Ações automáticas ou manuais do operador necessárias ou assumidas;
- Tempo após o evento em que as ações devem ser executadas;
- Análise dos eventos cobertos pelo critério de falha única.

6.2.4.8 Condições para Operação Autorizada

Esta seção deve especificar detalhadamente as condições que devem ser preenchidas antes e durante a operação, incluindo a observação de limites superiores e inferiores das variáveis do processo que sejam relevantes para a segurança nuclear assim como outros requisitos de natureza técnica, administrativa e de procedimentos.

No mínimo, os itens listados abaixo devem ser indicados:

- Limites de segurança,
- Limites de alarme;
- Sinais de desligamento automático;
- Condições limitantes para operação em emergência do navio;

- Verificações e inspeções das condições técnicas:
 - frequência e escopo dos registros e testes;
 - calibrações e aferições;
- Controles administrativos
 - organização e cadeias hierárquicas de autoridade e responsabilidade;
 - procedimentos para alteração e aprovação de procedimentos e ordens de operação;
 - quantidade e qualificação do pessoal de operação;
 - procedimentos e instruções que norteiam a operação normal, a operação anormal (ocorrências operacionais antecipadas), o controle de avarias e o gerenciamento de acidentes.
- Requisitos de vigilância e manutenção.

6.2.4.9 Segurança Física do Submarino e da IPN

Os dispositivos técnicos e procedimentos para a proteção da IPN contra intrusões de pessoas não autorizadas, sabotagem e desvio de materiais nucleares devem ser descritos, observando-se, em particular, eventuais conflitos entre requisitos de segurança física e de segurança nuclear.

As informações fornecidas para esse fim devem ser apresentadas em um documento separado, classificado de acordo com os procedimentos de confidencialidade da Organização Operadora, somente sendo fornecido à ASN mediante requisição formal específica, e sob compromisso legal de sigilo.

6.2.4.10 Descomissionamento

A Organização Operadora deverá apresentar a estratégia proposta para o descomissionamento da IPN embarcada. Esta estratégia deverá orientar a regulamentação específica necessária para estabelecer, oportunamente:

- O procedimento de verificação da segurança nuclear do descomissionamento, adotando-se a definição de três níveis previstos por (IAEA, 1990):
 - Nível 1, onde a IPN encontra-se numa situação análoga àquela da parada a frio, com retirada de todo o combustível nuclear, nos períodos de manutenção de longa duração;
 - Nível 2, onde o compartimento do reator (Contenção) é separado do resto do submarino, e reduzido ao mínimo volume, e onde a estanqueidade deste compartimento é reforçada. A vigilância da Instalação pode então ser reduzida;

- Nível 3, onde todos os materiais radioativos são retirados do compartimento, já separado do submarino. Neste nível a IPN não mais existe como tal, nenhum controle sendo mais previsto do ponto de vista radiológico.
- As responsabilidades das organizações envolvidas direta e indiretamente com as atividades de descomissionamento.

A estratégia proposta deverá definir:

- O estado da IPN nos diferentes níveis de descomissionamento;
- As atividades necessárias para atingir o nível de descomissionamento requerido;
- O gerenciamento de rejeitos produzidos pelas atividades de descomissionamento;
- Os procedimentos de vigilância e controle periódicos a serem executados tanto durante a execução das atividades quanto durante os períodos de espera entre os diferentes níveis de descomissionamento.
- Opções técnicas adotadas para:
 - Reconstituição de duas barreiras de confinamento entre o ambiente e as superfícies contaminadas, com tamponamento de bocais de equipamentos do Circuito Primário desmontados (1ª barreira) e das penetrações na Contenção (2ª barreira), antes da separação do compartimento do reator do resto do submarino;
 - Limitação dos riscos de corrosão dos circuitos remanescentes pelo seu total esvaziamento, remoção dos isolamentos térmicos e preenchimento do compartimento do reator com gás inerte;
 - Limitação dos riscos de incêndio pela supressão de toda alimentação elétrica permanente;
 - Controle dos equipamentos e estruturas desmontados durante a passagem para os Níveis 1 e 2.
- Tempos máximos de espera para transição entre níveis de descomissionamento
 - O início das atividades para passagem ao Nível 1 deverá ser imediato ao desarmamento do submarino, devendo estarem concluídas em prazo não superior a um (1) ano;
 - O início das atividades para passagem do Nível 1 ao Nível 2 deverá ocorrer até dois (2) dois anos após o desarmamento do submarino, devendo estarem concluídas em no máximo cinco (3) anos, i.e. o Nível 2 deverá ser atingido até cinco (5) anos após o desarmamento;
 - O início das atividades para passagem do Nível 2 ao Nível 3 deverá ocorrer após um período de tempo tal que a atividade residual total, avaliada na passagem ao Nível 2, seja reduzida de um fator significativo, estabelecido de forma orientativa, entre 10 e 20.

6.2.5 REVISÃO E ANÁLISE

A revisão e análise das informações submetidas pela Organização Operadora como justificativa técnica para obtenção de licença ou autorização serão executadas pela ASN, de forma a determinar se o SNA proposto é compatível com as áreas de mobilidade e localizações fixas, pode ser construído, pode ser comissionado, pode ser operado e, finalmente descomissionado sem riscos radiológicos inaceitáveis para a tripulação, pessoal de apoio em terra, público geral e meio ambiente. Dentro deste objetivo global, identifica-se objetivos específicos da revisão e análise:

- Determinar se as áreas de mobilidade e localizações fixas são adequadas para o tipo, potência e emprego do SNA proposto;
- Determinar, antes de construção, se o projeto da IPN e da plataforma-navio do SNA proposto satisfaz as exigências de segurança da ASN e impor exigência ou condições adicionais julgadas necessárias;
- Determinar se a Organização Operadora tem a habilidade, confiabilidade, recursos, estrutura organizacional e pessoal competente para satisfazer às exigências de segurança da ASN;
- Determinar se as técnicas e procedimentos de fabricação de componentes e estruturas, construção e montagem são consistentes com as especificações de projeto aprovadas pela ASN;
- Determinar se o Programa de Comissionamento é adequado e se efetivamente verifica o atendimento das especificações de projeto, fabricação e construção aprovadas pela ASN;
- Determinar se os limites e condições operacionais são consistentes com os requisitos de segurança da ASN e se um nível adequado de segurança pode ser assegurado pelo cumprimento dos procedimentos operacionais, inclusive nas condições de acidente e se a formação e treinamento dos operadores asseguram que estes procedimentos serão efetivamente cumpridos adequadamente;
- Determinar se o Programa de Descomissionamento assegura que as atividades de desmontagem da instalação podem ser realizadas com impactos radiológicos aceitáveis e dentro de um gerenciamento de rejeitos eficiente.

Uma programação para revisão e análise do RAS, apropriada ao estágio do processo de licenciamento, deverá ser estabelecido de comum acordo entre a ASN e a Organização Operadora. Esta programação será feita com base no cronograma de submissão de informações pela Organização Operadora à ASN, abordado no item 6.1.4.

Antes de autorizar a construção da IPN do SNA, a ASN revisará e avaliará:

- A competência e capacidade da Organização Operadora para satisfazer as exigências de segurança da ASN e as condições da licença;
- As características das áreas de mobilidade e localizações fixas, confirmando sua aceitabilidade e os fatores ambientais usados no projeto;
- O projeto básico da IPN e da plataforma-navio do SNA, confirmando que suas especificações poderão atender as exigências de segurança da ASN;
- O Programa de Garantia da Qualidade da Organização Operadora e de seus fornecedores;
- O Plano de Proteção Física da IPN do SNA, caracterizando os aspectos relevantes para a segurança nuclear
- As informações necessárias à verificação do projeto.

Antes de autorizar o carregamento de combustível nuclear e a criticalidade inicial, a ASN deverá completar a revisão e análise da segurança da IPN do SNA, incluindo:

- O Programa de Comissionamento da IPN do SNA;
- O projeto “como-construído” (*as built*) da IPN e da plataforma-navio do SNA;
- Os limites e condições para operação durante o comissionamento;
- As providências tomadas para a proteção radiológica em operação;
- A suficiência das instruções e procedimentos operacionais e normas administrativas da Organização Operadora aplicáveis ao SNA;
- Os registros e documentação de montagem dos sistemas;
- O treinamento e qualificação dos operadores da IPN, dos demais tripulantes e do pessoal de apoio em terra, incluindo todos os níveis hierárquicos, e sua adaptação à execução das tarefas previstas;

- A organização da Garantia da Qualidade e o correspondente programa para aplicação à operação;
- Os planos de emergência (PEL e PEE, caso este último seja requerido);
- O sistema de contabilidade e controle de materiais nucleares e radioativos;
- Os procedimentos e dispositivos de proteção física importantes para segurança nuclear;
- Os programas de monitoramento, testes, inspeções e manutenção periódicos;

Antes de autorizar a operação permanente da IPN a plena potência, a ASN completará a revisão e análise do RAS, levando em conta os resultados do Programa de Comissionamento e da experiência da operação inicial, considerando eventuais alterações nos limites e condições para operação e Procedimentos Operacionais deles decorrentes.

Antes de implementar qualquer proposta de alteração na configuração e nos procedimentos operacionais e de manutenção relevantes para a segurança nuclear, a ASN deverá avaliar as informações submetidas pela Organização Operadora. Esta revisão e análise seguirão os mesmos procedimentos adotados para o projeto original.

7 CONCLUSÕES

A afirmação de que uma instalação industrial é, simultaneamente, muito perigosa e muito segura, pode não ser necessariamente contraditória. Através de padrões de segurança tão altos quanto razoavelmente praticáveis, é possível garantir que um processo potencialmente muito perigoso seja objetivamente seguro, i.e os riscos a ele associados sejam socialmente aceitáveis.

A segurança não é absoluta. Na vida cotidiana faz-se uma série de julgamentos relativos, muitos deles inconscientes, sobre os perigos associados às possibilidades de conduzir uma determinada atividade de um modo ou de outro, como também sobre as conseqüências indesejadas que podem ser incorridas, caso não seja tomada nenhuma ação de segurança. As experiências individuais de cada pessoa, assim como o conhecimento das experiências vividas por outrem, tanto positivas como negativas, são um fator determinante dos julgamentos relativos, sendo um meio fundamental para se ganhar confiança nas decisões e atingir efetivas melhorias na segurança.

Estas idéias simples aplicam-se, integralmente, à avaliação, manutenção e melhoria da segurança dos SNA, que devem atender às necessidades operativas da Marinha sem induzir, devido às peculiaridades de sua IPN, riscos inaceitáveis para a tripulação, o pessoal de apoio logístico em terra, o público em geral e o meio ambiente.

Um navio é um veículo que opera de maneira autônoma em um ambiente que apresenta riscos que devem ser controlados. Esta realidade torna-se ainda mais crítica no caso de submarinos, onde o ambiente possui três dimensões. Estes riscos podem ser classificados em três categorias: acidentes internos, que podem rapidamente assumir proporções graves devido ao ambiente; riscos externos específicos ao ambiente; e riscos operativos associados ao caráter militar, no caso de navios de guerra e submarinos.

A natureza dos riscos apresentados pela IPN de um SNA, assim como pelas instalações de apoio logístico em terra que lhe são associadas, não são fundamentalmente diferentes daqueles associados às atividades nucleares civis de natureza similar. Existem entretanto

algumas diferenças altamente relevantes, que devem ser consideradas quando estas são comparadas às instalações nucleares de potência estacionárias:

- O inventário de produtos radioativos presentes num SNA é significativamente menor do que aquele de um reator de potência eletronuclear, na razão direta das potências térmicas envolvidas (50-100Mwth para reatores navais, 1800-3600 Mwth para reatores eletronucleares). A grosso modo, isto implica que, considerando-se cenários acidentais similares, as consequências radiológicas seriam da ordem de 50 vezes inferiores para um SNA, quando comparado com uma central nuclear.
- O ambiente “móvel” naval induz uma fonte de agressões sobre a IPN sem paralelo com o ambiente “estacionário” em terra de uma central nuclear. Estas potenciais agressões devem ser levadas em consideração, sobretudo em situações de operação do submarino dentro de instalações portuárias e nas proximidades da costa. Isto implica incluir na base de projeto carregamentos significativamente mais rigorosos que os utilizados para uma central nuclear, que não é submetida à mesma diversidade e intensidade de agressões.
- As restrições impostas pela arquitetura naval limitam a variedade de soluções viáveis para o arranjo físico da instalação. A IPN torna-se então extremamente compacta, dificultando a segregação de equipamentos, suportação de tubulações e interposição de barreiras anti-mísseis, anti-fogo e para proteção contra efeitos dinâmicos de ruptura de tubulações. De forma a evitar a propagação de agressões e falhas em modo comum, torna-se portanto necessária uma análise detalhada de suas consequências, cuja complexidade é seguramente maior do que as análises equivalentes para uma central nuclear, cuja arquitetura “civil” não impõe tais limitações.
- Um reator de propulsão é projetado para funcionar como um seguidor de carga que, pelas características da missão do navio, é extremamente variável. Isto implica suportar transitórios bruscos e freqüentes sem desligamento. Consequentemente, as margens de projeto, construção e operação normal são significativamente maiores do que aquelas usualmente adotadas para centrais nucleares, de modo a permitir que estes transitórios sejam operacionais, i.e. não impliquem em desligamento da IPN.
- Um SNA no mar só se encontra em segurança com respeito aos diversos riscos operativos e de navegação se ele puder dispor rapidamente da energia fornecida pela IPN. Isto

posto, se a continuidade da geração de energia não for assegurada, em particular por razões ligadas à segurança nuclear, a manobrabilidade do navio, e portanto sua própria segurança naval, pode ser gravemente afetada. Pode-se então considerar que a segurança da IPN depende da segurança da plataforma-navio do SNA, que por sua vez depende da disponibilidade da instalação nuclear.

Comparando os conceitos de Segurança Naval e de Segurança Nuclear, que devem ser conciliados de forma a otimizar a segurança global de um SNA, tornando os riscos associados à sua operação socialmente aceitáveis, pode-se identificar as seguintes similaridades: mesmo objetivo, i.e. evitar consequências indesejadas à vida humana; presença de uma abordagem analítica; a necessidade de desenvolver normas regulamentares em resposta a eventos inesperados e anteriormente não considerados nas análises.

Entretanto, é também identificada uma diferença básica de abordagem, que deve ser conciliada em uma abordagem de segurança única para um navio dotado de propulsão nuclear, consistente com a segurança da tripulação, do público e do meio ambiente: a Segurança Naval enfatiza a capacidade de sobrevivência do navio como meio de atingir seu objetivo; e a Segurança Nuclear, por outro lado, tem sua ênfase principal colocada sobre a integridade do reator e, complementarmente, sobre a integridade das barreiras físicas que contêm os produtos radioativos em caso de ocorrência de acidentes, como meio de atingir seu objetivo.

Esta abordagem unificada deve considerar que os submarinos poderão situar-se em três domínios de operação distintos: Normal; Anormal, no qual o navio somente operará involuntariamente (avaria, agressão externa, erro humano), sendo o objetivo retornar a uma condição segura; e Acidental, para o qual não se preconiza uma operação propriamente do navio, sendo o objetivo nesta situação a execução de procedimentos de salvaguarda ou de emergência para tornar aceitáveis as consequências do acidente.

Assim, uma Doutrina de Segurança para Submarinos Nucleares de Ataque deverá considerar que:

O submarino deve ser projetado, construído e operado de forma a ser dotado de características intrínsecas e de meios complementares suficientes para garantir que, na presença das três categorias de riscos:

- I. a possibilidade da operação normal do navio evoluir para o domínio anormal seja extremamente reduzida;*
- II. a partir de uma condição de operação anormal, o navio possa retornar o mais rápido possível a uma condição segura;*
- III. na ocorrência de acidentes, a máxima prioridade seja dada à proteção da vida humana; isto requer que as conseqüências dos acidentes para o próprio navio sejam minimizadas, de modo a proteger sua tripulação, o público e o meio ambiente.*

Esta doutrina estabelecerá que o submarino (note-se que não somente o reator mas o submarino como um sistema que inclui o reator), deve ser projetado, construído e operado de forma a não ocorrerem liberações descontroladas de materiais radioativos. Isto implica que a integridade da plataforma-navio será de importância primária, pois a sobrevivência do submarino será em si mesmo o fator mais importante para a segurança da IPN e para a contenção e confinamento de materiais radioativos. Em situações de risco iminente, a continuidade da operação da IPN deverá ser possível, mesmo que isto possa implicar em aumento dos riscos residuais de danos à IPN, de forma a evitar conseqüências graves para a plataforma-navio e garantir a Segurança Global do SNA.

Esta necessidade deriva do fato incontestável de que um submarino governável, ainda que com uma IPN com alguns danos, é intrinsecamente mais seguro do que um submarino com um reator íntegro mas desligado, logo com a propulsão principal indisponível. Isto não quer dizer, sob nenhuma hipótese, que a segurança da IPN deva deixar de ser considerada importante, nem que não deva ser analisada detalhadamente, ou que não existam situações nas quais a segurança da IPN preceda a segurança da plataforma-navio.

Obviamente, um submarino em situações extremas, pousado inerte no fundo do mar com o reator desligado em estado seguro é uma situação mais favorável, em termos de liberação de produtos radioativos, do que um submarino, nas mesmas condições, mas com o Circuito Primário ou a estrutura de Contenção rompidos. Portanto, se o funcionamento da IPN além das condições normais previstas em suas especificações técnicas não garantir o

salvamento do submarino (logo também da própria IPN), o reator deverá ser compulsoriamente desligado.

Da constatação destes fatos, decorre que a segurança de um SNA fundamenta-se na otimização do conjugado disponibilidade x seguridade. Esta otimização é alcançada através de soluções de compromisso, derivadas de análises do tipo custo/benefício.

Para a maioria dos engenheiros navais e submarinistas, esta premissa deve parecer óbvia. Entretanto, a efetiva percepção da diferença que isto implica com respeito ao fundamento de otimização exclusiva da seguridade aplicado às instalações nucleares estacionárias nem sempre deve parecer evidente para os técnicos de outras áreas envolvidos com o projeto, construção, operação e licenciamento dos Submarinos Nucleares de Ataque.

Com base na experiência operacional de submarinos, navios de guerra de superfície e navios mercantes nucleares até o presente, pode-se afirmar que é muito pouco provável que o comandante venha a realmente enfrentar uma situação onde tenha que decidir entre a IPN e o plataforma-navio e sua tripulação.

Entretanto, esta possibilidade existe e será justamente a aplicação de uma doutrina de segurança adaptada a estas circunstâncias ao longo de todas as fases da vida útil do SNA que poderá reduzir a probabilidade de que uma tal decisão venha um dia a ter que ser tomada. Um profundo entendimento desta doutrina e das conseqüências de sua aplicação, de modo a retirar o submarino de uma situação de risco iminente, ainda que aceitando algum dano no reator e seus sistemas, é de fundamental importância para a segurança dos SNA, entendidos como um sistema integrado naval/nuclear.

Considerando tanto os aspectos nucleares quanto os navais, esta tese propôs-se então a organizar e sistematizar uma Doutrina de Segurança Global aplicável a futuros Submarinos Nucleares de Ataque (SNA) nacionais que atenda a estas premissas.

A doutrina proposta tem a forma de um conjunto de Princípios Básicos, Critérios Gerais, Requisitos Específicos e Procedimentos de verificação do projeto e de inspeção da construção e operação, que propõe-se a garantir um alto padrão de segurança a esta classe de navio de guerra. Com ela, pretende-se constituir uma base consistente e coerente sobre a

qual a Autoridade de Segurança Nuclear possa avaliar a aceitabilidade dos riscos associados ao Ciclo de Vida do SNA, tomando assim suas competentes decisões quanto ao licenciamento do submarino.

Entendendo-se segurança como percepção social de riscos, foram discutidos o detalhamento, as interpretações, as derivações e as aplicações tecnológicas deste conceito básico em três contextos específicos: a disciplina de aplicação geral denominada Segurança de Funcionamento de Sistemas Industriais (*Reliability-Availability-Maintanability-Safety*); a Segurança de Instalações Nucleares “Estacionárias”, em especial de reatores de potência eletronucleares; a Segurança Naval, que engloba tanto a Segurança Marítima (segurança da navegação, salvaguarda da vida humana no mar), típica de condições normais de paz, como a Capacidade de Sobrevivência (*Survivability*), típica das condições de guerra ou conflito.

Com base nesta discussão inicial, foi feita, em seguida, uma primeira abordagem global à Segurança da Propulsão Nuclear, onde foram sintetizadas as aplicações do conceito básico nestes três contextos, ressaltando-se sua fundamentação na otimização do conjugado disponibilidade x seguridade.

Os Princípios Básicos de Segurança foram, a partir desta síntese, adaptados às particularidades da propulsão nuclear de SNA. Os Princípios Básicos incluem os Objetivos Gerais de Segurança, assim como os Princípios de Gerenciamento, Princípios de Defesa em Profundidade e Princípios Técnicos que orientam como estes objetivos poderiam ser alcançados.

Em seguida foram propostos Critérios Gerais de Segurança para o projeto da IPN e de suas interfaces com a plataforma-navio do SNA. Os Critérios Gerais incluem Critérios de Probabilidade e Critérios de Consequências, que foram associados formando Critérios de Risco (Objetivos Detalhados de Segurança ODS).

Pretende-se que, com base nestes ODS desenvolvidos (Tabela 7.1), seja futuramente constituída, pela ASN, uma base objetiva sobre a qual a aceitabilidade dos riscos associados ao Ciclo de Vida do SNA possa ser avaliada.

São ainda desenvolvidos Critérios para determinação das Condições de Processo da Instalação Nuclear CPIN e Situações Operacionais do Submarino SOS postuladas para análise de segurança pelos Critérios de Risco e Critérios de Projeto determinísticos, que orientam o desenvolvimento do projeto integrado do conjunto de sistemas que compõem o SNA e que garantem a adequação da segurança aos Princípios Básicos qualitativos.

SÍNTESE DE DOCTRINA DE SEGURANÇA
PARA PROJETO E OPERAÇÃO DE SUBMARINOS NUCLEARES

TABELA 7.1:
OBJETIVOS DE SEGURANÇA PARA SUBMARINOS NUCLEARES DE ATAQUE

CLASSE	VEROSSIMILHANÇA	FAO	CONSEQUÊNCIAS PARA O SUBMARINO	CONSEQUÊNCIAS PARA A TRIPULAÇÃO	CONSEQUÊNCIAS PARA O PÚBLICO	CONSEQUÊNCIAS PARA O AMBIENTE
1	contínuo ou freqüente: ocorre continuamente ou é provável ocorrer diversas vezes durante o ciclo de vida do SNA	> 1	<p style="text-align: center;">OPERAÇÃO NORMAL</p> <ul style="list-style-type: none"> Submarino disponível imediatamente com plena capacidade operacional; Situações de operação normais sob propulsão nuclear. 	<ul style="list-style-type: none"> Situação com riscos ocupacionais normais; Doses efetivas (corpo inteiro) para os operadores da IPN dentro do limite anual de 20 mSv e tão reduzidas quanto razoavelmente realizável. Doses efetivas (corpo inteiro) para os demais tripulantes dentro do limite anual de 5 mSv e tão reduzidas quanto razoavelmente realizável. 	<ul style="list-style-type: none"> Dose efetiva (corpo inteiro) sobre o membro do público mais afetado inferior a 100 μSv 	<ul style="list-style-type: none"> Observância dos limites anuais para liberação de efluentes autorizados pela ASN Classificação das áreas internas do submarino por zonas de radiação conforme condições normais de projeto
2	infreqüente: não ocorre freqüentemente mas é provável que ocorra pelo menos uma vez durante o ciclo de vida do SNA	$1 > \text{FAO} > 10^{-2}$	<p style="text-align: center;">OPERAÇÃO DEGRADADA</p> <ul style="list-style-type: none"> Submarino disponível com capacidades operacionais reduzidas (redução de potência) imediatamente ou após uma intervenção de reparo passível de ser realizada pela própria tripulação; Situações de operação degradadas sob propulsão nuclear. 	<ul style="list-style-type: none"> Risco de danos imediatos leves para a tripulação, não associados a causas radiológicas; Doses efetivas (corpo inteiro) para os operadores da IPN dentro do limite anual de 50 mSv; Doses efetivas (corpo inteiro) para os demais tripulantes dentro do limite anual de 20 mSv . 	<ul style="list-style-type: none"> Dose efetiva (corpo inteiro) sobre o membro do público mais afetado inferior a 1 mSv 	<ul style="list-style-type: none"> Observância dos limites anuais para liberação de efluentes autorizados pela ASN Possibilidade de reclassificação temporária das áreas internas do submarino por zonas de radiação, retornando-se às condições normais após intervenção da tripulação
3	possível: a princípio, não deve ocorrer durante o ciclo de vida	$10^{-2} > \text{FAO} > 10^{-4}$	<p style="text-align: center;">ACIDENTES COM RECUPERAÇÃO DA OPERAÇÃO</p> <ul style="list-style-type: none"> Capacidades operacionais seriamente 	<ul style="list-style-type: none"> Risco de danos imediatos graves com uma pequena probabilidade de morte de um 	<ul style="list-style-type: none"> Dose efetiva (corpo inteiro) sobre o membro do público mais afetado 	<ul style="list-style-type: none"> Observância, por incidente, dos limites anuais de liberação de efluentes autorizados pela

SÍNTESE DE DOCTRINA DE SEGURANÇA
PARA PROJETO E OPERAÇÃO DE SUBMARINOS NUCLEARES

de um único SNA, mas poderia ocorrer quando considera-se o ciclo de vida de um esquadrão composto por mais de uma unidade		<p>comprometidas, podendo ir até perda total da potência nuclear ou incapacidade de navegar submerso, implicando retorno prematuro à base sob propulsão auxiliar convencional;</p> <ul style="list-style-type: none">• Situações de operação incidentais sérias sob propulsão auxiliar convencional (reator desligado com remoção de calor residual).	<p>membro da tripulação;</p> <ul style="list-style-type: none">• Dose efetiva (corpo inteiro) sobre tripulante mais afetado inferior a 100mSv.	<p>inferior a 5 mSv</p> <ul style="list-style-type: none">• Dose efetiva (tireóide) sobre o membro do público mais afetado inferior a 15 mSv	<p>ASN</p> <ul style="list-style-type: none">• Possibilidade de reclassificação permanente das áreas internas do submarino por zonas de radiação, o retorno às condições normais requerendo intervenção do apoio em terra
---	--	---	--	--	---

SÍNTESE DE DOCTRINA DE SEGURANÇA
PARA PROJETO E OPERAÇÃO DE SUBMARINOS NUCLEARES

TABELA 7.1 (continuação):
OBJETIVOS DE SEGURANÇA PARA SUBMARINOS NUCLEARES DE ATAQUE

CLASSE	VEROSSIMILHANÇA	FAO	CONSEQUÊNCIAS PARA O SUBMARINO	CONSEQUÊNCIAS PARA A TRIPULAÇÃO	CONSEQUÊNCIAS PARA O PÚBLICO	CONSEQUÊNCIAS PARA O AMBIENTE
4	improvável: a princípio, não deve ocorrer durante o ciclo de vida de um esquadrão de SNA composto por mais de uma unidade, sendo porém possível	$10^{-4} > \text{FAO} > 10^{-6}$	ACIDENTES SEM RECUPERAÇÃO DA OPERAÇÃO, COM SALVAMENTO DO SUBMARINO <ul style="list-style-type: none"> Degradações materiais importantes, podendo ir até a incapacidade de mover-se por seus próprios meios (necessidade de reboque para retorno à base), mantida, entretanto, uma mínima disponibilidade de fontes de energia internas; Situações de operação acidentais com perda total da propulsão (reator desligado com resfriamento de emergência). 	<ul style="list-style-type: none"> Risco de vida elevado para um ou vários membros da tripulação; Abandono do submarino dos tripulantes não envolvidos nas ações do Plano de Emergência Interno 	<ul style="list-style-type: none"> Dose efetiva (corpo inteiro) sobre o membro do público mais afetado inferior a 50 mSv Dose efetiva (tireóide) sobre o membro do público mais afetado inferior a 250 mSv 	<ul style="list-style-type: none"> Termo-fonte liberado (relativo ao inventário de produtos radioativos): <ul style="list-style-type: none"> ✓ 2% dos gases raros ✓ 1% do iodo Taxa máxima de vazamento da Contenção: <ul style="list-style-type: none"> ✓ 0,4%/dia no primeiro dia após o acidente ✓ 0,2%/dia nos 29 dias subsequentes
			ACIDENTES SEM RECUPERAÇÃO DA OPERAÇÃO, COM PERDA DO SUBMARINO <ul style="list-style-type: none"> Degradações materiais importantes, podendo ir até a perda de todas as fontes de energia internas (necessidade de fornecimento externo de energia ou meios passivos para manutenção das funções de segurança); Situações de operação acidentais com perda total do submarino por naufrágio ou encalhe (reator desligado com resfriamento passivo ou provido por meios externos). 	<ul style="list-style-type: none"> Abandono de toda tripulação do submarino; 		

SÍNTESE DE DOCTRINA DE SEGURANÇA
PARA PROJETO E OPERAÇÃO DE SUBMARINOS NUCLEARES

Complementar	hipotético: a princípio, não ocorrerá durante o ciclo de vida de um esquadrão de SNA composto por mais de uma unidade, sendo sua remota possibilidade de ocorrência associada à perda total de sistemas e funções de segurança atuantes em cenários de classe 4	$10^{-6} > \text{FAO}$	<p style="text-align: center;">ACIDENTES SEVEROS</p> <ul style="list-style-type: none"> • Perda do submarino e das funções básicas de segurança (resfriamento do núcleo e contenção); • Situações de operação acidentais complementares. 	<ul style="list-style-type: none"> • Abandono de toda tripulação do submarino; • Perda da tripulação. 	<ul style="list-style-type: none"> • Dose efetiva (corpo inteiro) sobre o membro do público mais afetado inferior a 100 mSv • Dose efetiva (tireóide) sobre o membro do público mais afetado inferior a 450 mSv 	<ul style="list-style-type: none"> • Termo-fonte liberado (relativo ao inventário de produtos radioativos): <ul style="list-style-type: none"> ✓ 80% dos gases raros ✓ 0,6% do iodo orgânico ✓ 60% do iodo inorgânico ✓ 40% do cézio ✓ 5% do estrôncio
--------------	---	------------------------	--	---	---	---

Os Requisitos Específicos de segurança aplicáveis ao projeto de estruturas, componentes e sistemas da plataforma-navio do SNA, da IPN e instalações de máquinas, derivados dos Critérios Gerais foram, a seguir, desenvolvidos, englobando ainda os aspectos de Garantia da Qualidade, Proteção Radiológica, Operação, Inspeções e Testes. Os Requisitos Específicos constituem regras quantitativas que determinam o projeto individual das partes integrantes do SNA, e que asseguram que os sistemas individuais do submarino, quando integrados, atendam aos Critérios Gerais.

Foram propostas diretrizes para o estabelecimento de uma regulamentação do processo de licenciamento dos SNA pela Autoridade de Segurança Nuclear e dos procedimentos de verificação da segurança do projeto e de fiscalização da construção e operação associados, e discutidos o conteúdo e a organização do Relatório de Análise de Segurança (RAS), documento básico deste processo, finalizando-se assim o desenvolvimento da estrutura da Doutrina de Segurança proposta.

À ASN caberá, no futuro, implementar a regulamentação e controle das atividades relacionadas ao Ciclo de Vida do SNA, de forma a garantir, perante a sociedade brasileira, que os riscos a elas associadas são aceitáveis. Pretende-se que a Doutrina de Segurança desenvolvida pela presente tese e proposta para aplicação aos SNA nacionais, que se espera estarem operacionais no início do próximo século, venha a constituir uma efetiva contribuição para um eficaz e eficiente desempenho desta missão constitucional.

Esta ASN, com jurisdição sobre os SNA, deverá ser estabelecida com base num modelo organizacional similar àquele praticado para a ASN com jurisdição sobre as instalações nucleares estacionárias de natureza civil (STXN, 1994). Poderá, dentro de um escopo ampliado para além dos SNA, constituir um Autoridade de Segurança Nuclear Militar ASNM, distinta da ASN civil, sendo responsável pela regulamentação e controle de todas as atividades nucleares afetas ao Ministério da Defesa, que se encontra, em 1999, sendo implantado pelo Governo Brasileiro.

ANEXO A

INSTALAÇÕES PROPULSORAS NUCLEARES

A instalação propulsora nuclear é entendida como aquela parte do navio cuja função é fornecer a energia necessária à propulsão do navio e à produção de energia elétrica para consumo interno; ela compreende, para instalações baseadas em reatores PWR “clássicos”:

a) os grandes componentes nucleares do Circuito Primário:

- núcleo e vaso de pressão do reator;
- mecanismo de acionamento de elementos de controle;
- geradores de vapor;
- pressurizador;
- bombas de circulação; e
- tubulações principais de resfriamento;

b) os auxiliares diretamente associados ao circuito primário:

- purificação, controle volumétrico, amostragem e detecção de vazamentos da água de resfriamento;
- resfriamento de componentes;
- remoção de calor residual em condições normais; e
- acionamento de válvulas;

c) dispositivos especiais de segurança:

- injeção de água em emergência;
- resfriamento em emergência;
- estrutura da contenção; e
- controle ambiental da contenção;

d) dispositivos especiais de blindagem:

- tanque de blindagem primária;
- água de blindagem;
- anteparas de blindagem secundária.

e) Instalação de Máquinas:

- Circuito Secundário;
- Sistemas auxiliares associados ao Circuito Secundário;
- Sistema de Resfriamento dos Condensadores Principais do Circuito Secundário;
- Sistema de Acionamento do Eixo Propulsor;
- Eixo Propulsor e Hélice;
- Sistema Elétrico de Serviço;
- Sistema Hidráulico de Serviço;
- Sistema Pneumático de Serviço;

- Sistema de Ventilação e Condicionamento de Ar.

O grande interesse militar da propulsão naval nuclear, historicamente a primeira aplicação efetiva da energia nuclear “controlada”, se prende ao seu caráter anaeróbio e à autonomia energética que ela proporciona. Apesar de um número bastante grande de estudos, experimentações e tentativas tão engenhosas quanto aquelas efetuadas entre e durante as duas guerras mundiais, tais como o aperfeiçoamento das baterias de acumuladores, invenção do “esnorquel”, sistemas a oxigênio líquido ou peróxido de hidrogênio, motor diesel em circuito fechado, motor stirling, estocagem de calor sob forma de sais fundidos (GUIMARÃES, 1991), as limitações da propulsão convencional de submarinos os condenava, na prática, à necessidade de navegar na superfície a maior parte do tempo, o que implicava numa grande indiscrição. O mergulho só podia ser realizado por curtos períodos de tempo e a velocidades submersas muito baixas.

A propulsão nuclear vem então possibilitar o desenvolvimento do “SUBMARINO TOTAL”, ou seja, aquele projetado para operar todo o tempo submerso, a altas velocidades.

Desde as origens da descoberta da possibilidade da reação nuclear em cadeia, assim como quando da construção da primeira “pilha atômica” por Enrico Fermi em 1942, a aplicação “propulsão de submarinos” foi imediatamente identificada como das mais promissoras. Em 20 de março de 1953, o reator S1W, primeiro protótipo em terra de propulsão naval atingiu sua primeira criticalidade e, em 1955, o USS NAUTILUS, primeiro navio nuclear, efetuou seu primeiro mergulho (RODDIS e SIMPSON, 1958). A concepção de reatores PWR, tanto de propulsão naval como para geração de energia elétrica, guardam até hoje uma marca indelével dos conceitos básicos desenvolvidos por estes pioneiros, destacando-se o fundamental papel desempenhado pelo Almirante Hyman G. Rickover (SIMPSON, 1995; ROCKWELL, 1992; DUNCAN, 1990; POLMAR, 1982; HEWLETT e DUNCAN, 1974).

Existem diversos tipos genéricos de instalações nucleares que poderiam ser, a princípio, utilizadas para propulsão naval (CROUCH, 1962). Alguns tipos poderiam ser rejeitados a priori por serem muito volumosos, muito pesados ou insuficientemente resistentes aos carregamentos dinâmicos típicos do ambiente naval. Outros, que empregam fluidos “exóticos”

para resfriamento ou moderação, tais como hélio, sódio, água pesada são também pouco atrativos.

No atual “estado-da-arte” da engenharia nuclear, somente a família de reatores resfriados e moderados a água leve atendem aos variados requisitos navais e, à exceção do SNA americano Seawolf, o qual foi inicialmente equipado com um reator resfriado a sódio mas que pouco tempo depois teve esta instalação removida e substituída por outra do tipo PWR (LANING, 1992), e dos seis SNA soviéticos classe ALFA, equipados com reatores resfriados a chumbo-bismuto (BREEMER, 1989) e desativados após um período de vida útil da ordem de 10 anos, nenhuma instalação propulsora naval tem se afastado desta categoria.

Dentro da família de reatores de água leve, pode-se considerar, além dos reatores PWR “clássicos” (BATTLE e KILLINGLEY, 1977), com arranjo segregado para os seus componentes principais, os PWR integrados (*Integrated Pressurized Water Reactor* IPWR), que podem ser auto-pressurizados (*Integrated Self-Pressurized Water Reactor* ISPWR) ou pressurizados externamente (*Integrated Externally Pressurized Water Reactor* IEPWR), os PWR acoplados (*Close Coupled Pressurized Water Reactor* CCPWR) e os reatores a água em ebulição (*Boiling Water Reactor* BWR). A Figura A.1 apresenta um arranjo esquemático destes cinco tipos de reatores.

Não existem aplicações reais de reatores BWR à propulsão naval. As principais razões para sua rejeição são a presença de produtos radiativos no vapor produzido, especialmente o Nitrogênio-16 gerado pela ativação da água no interior do núcleo do reator, criando problemas de radioproteção no compartimento das turbinas, a qualidade do vapor produzido (baixa pressão e temperatura) e os efeitos de instabilização da reatividade provocados pelos movimentos do navio no mar.

Os reatores CCPWR têm características intermediárias entre os PWR e os IPWR, dispensando as tubulações de interligação sem implicar na interdependência total dos componentes. Não existe até o presente experiência operacional com este tipo de instalação. Um projeto baseado nesta concepção foi desenvolvido na França (VERDEAU e BAUIAC, 1977). Note-se, entretanto, que os problemas de segurança colocados pelas conexões entre as grandes massas representadas pelo vaso de pressão e os geradores de vapor não tornam

este conceito atrativo para instalações submetidas a severos carregamentos dinâmicos impulsivos como é o caso de navios de guerra e, em especial, de submarinos.

FIGURA A.1: REATORES A ÁGUA LEVE

Os reatores IPWR tem sido objeto de numerosas propostas de emprego em propulsão naval. A versão auto-pressurizada IAPWR chegou ao nível de realização prática com o navio mercante experimental alemão Otto Hahn (GKSS, 1975). A versão externamente pressurizada chegou ao nível de realização prática industrial com os SNA franceses da classe Rubis/Amethyste e com os submarinos nucleares lançadores de mísseis balísticos SNLMB classe Le Triomphant (MNF, 1992, 1995).

Reatores PWR com uma potência da ordem de 50 a 100 MWth equipam cerca de 330 SNLMB, submarinos nucleares lançadores de mísseis de cruzeiro SNLMC, SNA, navios

aeródromos nucleares NAeN e cruzadores nucleares CN pertencentes às marinhas de guerra dos EUA, Rússia, Grã-Bretanha, França e China. Equipam ainda os navios mercantes nucleares experimentais Mutsu Maru, japonês, e Savannah, americano, os quebra-gelos nucleares russos Lenin, classe Tamyr (2 unidades) e classe Artika (6 unidades) e o porta-contenedor Sevmorput.

Para os navios de superfície e submarinos, a instalação nuclear assegura simultaneamente a propulsão e a produção de energia elétrica necessária à autonomia normal do navio. No caso de acionamento direto (Figura A.2), o vapor de origem nuclear aciona, tanto turbinas de propulsão acopladas ao hélice como turbo-geradores que constituem as fontes elétricas normais do navio. No caso de acionamento elétrico (Figura A.3), o vapor nuclear alimenta turbo-geradores que acionam um motor elétrico de propulsão ao mesmo tempo que produzem a eletricidade de bordo. Em ambos os casos, existe uma propulsão em emergência, de potência limitada, a partir de motores elétricos alimentados por um banco de baterias principal, para o submarino em mergulho, e por um diesel-gerador elétrico, para o submarino na superfície.

Um submarino no mar não será portanto operacional para suas missões militares, nem estará em segurança com respeito aos riscos diversos de navegação tanto na superfície como submerso, se ele não puder dispor rapidamente da energia fornecida pela instalação nuclear.

Para os navios-aeródromos (Figura A.4), pelo menos duas instalações nucleares idênticas asseguram a propulsão da plataforma por intermédio de turbinas a vapor que acionam duas linhas de eixo independentes, a alimentação elétrica normal do navio por turbo-geradores a vapor e a alimentação em vapor das catapultas necessárias à decolagem dos aviões embarcados. A continuidade do fornecimento de energia nuclear é portanto indispensável, não somente para permitir a atividade operacional de catapultagem dos aviões, mas igualmente para a segurança dos aviões em voo, garantindo condições que permitam o pouso. Com efeito, o navio deve poder se posicionar corretamente com relação ao vento e à pista de pouso oblíqua de modo a garantir um vento relativo suficiente sobre o convés de voo que permita a recuperação das aeronaves. A presença de duas instalações nucleares a bordo permite a recuperação de aviões em voo com uma delas indisponível, eventualmente por

razões de segurança. Além disto, os riscos associados aos alagamentos e às avarias dos sistemas de manobra da plataforma não são da mesma amplitude que para os submarinos, permitindo tempos de reação significativamente maiores. Por outro lado, a usual ausência de uma propulsão em emergência requer a disponibilidade, pelo menos parcial de uma instalação nuclear para a manobrabilidade da plataforma.

Os cruzadores e outros navios de superfície nucleares possuem características semelhantes aos submarinos, ressaltando-se entretanto que os riscos associados a uma eventual perda da geração de energia nuclear serão menos críticos, pela simples razão de operarem somente na superfície.

FIGURA A.2: ACIONAMENTO MECÂNICO DE SUBMARINOS NUCLEARES

FIGURA A.3: ACIONAMENTO ELÉTRICO DE SUBMARINOS NUCLEARES

SÍNTESE DE DOCTRINA DE SEGURANÇA PARA PROJETO E OPERAÇÃO DE SUBMARINOS NUCLEARES

ARRANJO GERAL:

CATAPULTA:

FIGURA A.4: PROPULSÃO NUCLEAR DE NAVIOS-AERÓDROMOS

ANEXO B

CICLO DE VIDA DE UM SUBMARINO NUCLEAR DE ATAQUE

B.1 PERFIL DE VIDA ÚTIL

A vida útil de um SNA é em geral prevista para 30 anos (360 meses), sendo composta por dois Ciclos de Atividades Básicos CAB, dois Ciclos de Atividades Intermediários CAI, dois Períodos de Atualização e Modernização PAM e um Ciclo de Atividades Final CAF.

TABELA B.1: PERFIL DE VIDA UTIL DO SNA

Duração dos ciclos (meses)	----63----	----57----	----24----	----63----	----57----	----24----	----72----
ciclos	CAB	CAI	PAM	CAB	CAI	PAM	CAF
Duração da vida útil (meses)	-----63	-----120	-----144	-----207	-----264	-----288	-----360

O CAB é composto por um Período Operativo Básico POB, com duração de 50 meses, e de um Período de Manutenção Geral PMG, com duração de 13 meses, realizado ao término do POB. O POB é dividido em 16 Ciclos Básicos - CB, cada um com duração de 13 semanas, compreendendo um Missão de Patrulha Básica - MPB, com 9 semanas (63 dias) e um Período de Manutenção de Rotina PMR, de 4 semanas. Após 8 CB's (2 anos) é previsto um Período de Docagem de Rotina PDR, com duração de 4 meses.

O CAI é composto por um Período Operativo Intermediário POI, com duração de 57 meses. O POI é composto por 8 CB, seguidos de um PDR (4 meses) e de 10 CB.

Os PAM, visam a não-obsolescência do SNA, através de alterações no navio e instalação de sistemas, sub-sistemas ou componentes no estado-da-arte, tendo duração de 24 meses.

O CAF é composto por um Período Operativo Final POF, com duração de 72 meses. O POF é composto por 8 CB, seguido de um PDR, de mais 7 CB seguidos de um

PDR, seguido 7 CB . Após a última MPB, inicia-se o descomissionamento do SNA, com um Período de Docagem Final PDF.

TABELA B.2: CICLO DE ATIVIDADES BÁSICO DO SNA

	3 meses		6 meses		9 meses		12 meses	
ANO 1	MPB	PMR	MPB	PMR	MPB	PMR	MPB	PMR
ANO 2	MPB	PMR	MPB	PMR	MPB	PMR	MPB	PDR
ANO 3	PDR		MPB	PMR	MPB	PMR	MPB	PMR
ANO 4	MPB	PMR	MPB	PMR	MPB	PMR	MPB	PMR
ANO 5	MPB	PMG						
ANO 6	PMG							

TABELA B.3: CICLO DE ATIVIDADES INTERMEDIÁRIO DO SNA

	3 meses		6 meses		9 meses		12 meses	
ANO 1	MPB	PMR	MPB	PMR	MPB	PMR	MPB	PMR
ANO 2	MPB	PMR	MPB	PMR	MPB	PMR	MPB	PDR
ANO 3	PDR		MPB	PMR	MPB	PMR	MPB	PMR
ANO 4	MPB	PMR	MPB	PMR	MPB	PMR	MPB	PMR
ANO 5	MPB	PMR	MPB	PMR	MPB	PMR	Início do PAM	

TABELA B.4: CICLO DE ATIVIDADES FINAL DO SNA

	3 meses		6 meses		9 meses		12 meses	
ANO 25	MPB	PMR	MPB	PMR	MPB	PMR	MPB	PMR
ANO 26	MPB	PMR	MPB	PMR	MPB	PMR	MPB	PDR
ANO 27	PDR		MPB	PMR	MPB	PMR	MPB	PMR
ANO 28	MPB	PMR	MPB	PMR	MPB	PMR	MPB	PDR
ANO 29	PDR		MPB	PMR	MPB	PMR	MPB	PMR
ANO 30	MPB	PMR	MPB	PMR	MPB	PMR	MPB	PDF
ANO 31	PDF e descomissionamento							

B.2 TRANSIENTES OPERACIONAIS NORMAIS

Os transientes operacionais normais a serem considerados no dimensionamento dos diversos sistemas, equipamentos, redes e estruturas são resumidos pela Tabela B.5.

TABELA B.5: TRANSIENTES NORMAIS AO LONGO DA VIDA UTIL

TRANSIENTES NORMAIS	OCORRÊNCIAS EM 30 ANOS
Aquecimento/resfriamento a taxa de 60 C ⁰ /hora até a condição de Desligado a Quente	550(cada)
Aumentos e decréscimos de potência em degraus de 15% da potência nominal de propulsão.	16.000(cada)
Decréscimos de potência em degraus de 100 % da potência nominal de propulsão, com uso de desvio de vapor para o condensador	270
Aumentos de potência de 0 a 100 % da potência nominal de propulsão em 60 segundos	2.000
Decréscimos de potência de 100 a 0 % da potência nominal de propulsão em 30 segundos, sem uso do desvio de vapor (<i>steam dump</i>)	2.000
Aumentos de potência de desligado a quente até a condição de automático	980
Decréscimos de potência da condição de automático até a condição de desligado a quente	550
Flutuações em regime estacionário com amplitudes inferiores a 2 %	Infinitas
Movimentos do navio no mar na condição de submerso	Infinitas
Aumentos e decréscimos na potência auxiliar em de graus de 10% (da potência auxiliar nominal)	Infinitas
Mergulho até a cota máxima de operação	1.500

- a) Aquecimento e Resfriamento a taxa de 60^o/hora até a condição de desligado a quente: 550 ocorrências para cada um.

- Para este transiente é assumido como sendo aquele necessário para operar o reator durante uma partida/parada normais, que compreende o intervalo de operação entre a condição de pressão e temperatura ambientais até a condição de desligado a quente.
 - Assim sendo, de acordo com a vida útil de 30 anos, admite-se que este transiente ocorra 3 vezes em cada período operativo, ($3 \times 88 = 264$), 3 vezes em cada período de manutenção/reparo ($3 \times 90 = 270$) e pelo menos 4 vezes no comissionamento. No total, teremos ocorrências de pelo menos 538 vezes, que podem ser arredondadas para 550.
- b) Aumentos e decréscimos de potência em degraus de 15 % da Potência Nominal de Propulsão: 16.000 ocorrências: vezes para cada um
- Este transiente tem relação com a operação normal do submarino em termos de variação de velocidade.
 - Admitindo-se que a velocidade do submarino varie com a potência de forma aproximada à curva EHP(submerso) x VELOCIDADE, temos a seguinte relação adimensional:
Velocidade:	30%	60%	80%	85%	90%	95%	100%	(% V_{max})
Potência:	15%	30%	45%	60%	75%	90%	100%	(% P_{max})
- Tendo em vista a distribuição acima, admitindo-se que por ciclo operativo chegue-se a executar até 3 viagens, é considerado o seguinte número de vezes com que se atingirá cada valor de percentagem da potência nominal por viagem:
0-15%	15-30%	30-45%	45-60%	60-75%	75-90%	90-100%
1	30	10	5	3	3	3
- Multiplicando-se pelo número de viagens (3), tem-se o total por ciclo operativo que é de 165. O total de ocorrências para os 88 ciclos fica sendo igual a 14.520 (88×165).
 - Considerando-se os períodos de manutenção/reparo e o Comissionamento, temos os seguintes valores:
 - Períodos de Manutenção Curta = 800 (10 x 80)
 - Períodos de Manutenção Demorada = 200 (20 x 10)
 - Comissionamento = 400 (estimativa)
 - Sendo assim o total de ocorrências de cerca de 16.000.

- c) Decréscimos de potência em degraus 100 % da potência nominal de propulsão, com uso do desvio de vapor para o condensador: 270 ocorrências
- Este transiente relaciona-se com a parada rápida do navio. Com relação ao número de ocorrências, o transiente deverá ocorrer pelo menos 1 vez em cada período de reparo/manutenção e pelo menos 2 vezes em cada ciclo operativo e cerca de 4 vezes durante o comissionamento. No total, pode-se ter pelo menos 270 vezes.
- d) Aumentos de potência de 0 a 100 % da Potência Nominal de Propulsão em 60 segundos; e
- e) Decréscimo de potência de 100 % a 0 % da potência nominal de propulsão em 30 segundos, sem uso do desvio de vapor (*steam dump*): 2000 ocorrências cada um.
- Estes transientes têm relação com a aceleração/desaceleração do navio em uma situação tática de importância, como por exemplo o deslocamento para a zona de patrulha e/ou o ataque ou mesmo uma manobra evasiva.
 - Sendo assim, este transiente poderá ocorrer cerca de 20 vezes por ciclo operativo, 2 vezes por ciclo de reparo/manutenção e 5 vezes durante o comissionamento. No total tem-se então cerca de 1945 vezes, que podem ser arredondadas para 2000.
- f) Decréscimos de potência da condição de automático até a condição de desligado a quente: 550 ocorrências
- Este transiente deverá ocorrer quando desejarmos reduzir a potência do reator até a condição de desligado a quente. Neste caso, assume-se que isto esteja ocorrendo quando desejamos "desligar" a instalação nuclear em operação normal, o que terá ocorrido tantas vezes quanto ocorreu o primeiro transiente da Tabela B.5, Aquecimento e Resfriamento a taxa de 60⁰/hora até a condição de desligado a quente.
- g) Aumentos da potência de desligado a quente até a condição automático: 980 ocorrências:
- Este transiente ocorrerá em duas situações distintas:
 - Em Operação Normal: quando queremos elevar a potência do reator, após o aquecimento (condição de Desligado a Quente) ; e

- Após um desligamento automático (SCRAM), o que significa a elevação da potência para o "retorno" a uma condição normal de operação.
- Assim, o total de ocorrências será composto de duas parcelas:
 - Operação Normal: tantas vezes quanto ocorreu o transiente 1 desta Tabela B.5 de transientes normais, ou seja, 550 vezes; e
 - Após um SCRAM: tantas vezes quanto ocorreu o transiente 4 da Tabela B.6 de transientes anormais apresentada a seguir ou seja, 430 vezes.
- A soma das duas parcelas corresponde ao total de ocorrências deste transiente, ou seja, 980 vezes.

B.3 TRANSIENTES OPERACIONAIS ANORMAIS

Os transientes operacionais anormais a serem considerados no dimensionamento dos diversos sistemas, equipamentos, redes e estruturas são resumidos pela Tabela B.6.

TABELA B.6: TRANSIENTES NORMAIS AO LONGO DA VIDA UTIL DO SNA

TRANSIENTES ANORMAIS	OCORRÊNCIAS EM 30 ANOS
Redução da potência em degrau, a partir de 100%, sem desligamento imediato do reator (<i>crash</i>)	300
Perda de potência elétrica	200
Perda parcial de escoamento no reator	110
Desligamento do reator, quando em 100% da potência (SCRAM)	430
Despressurização súbita do sistema primário	50
Operação inadvertida do sistema de injeção de emergência	70
Queda inadvertida de um elemento de controle	90
Retirada inadvertida de um banco de controle	90
Movimentos do navio no mar, na condição de superfície	Infinitas

- a) Redução da potência em degrau, a partir de 100%, sem desligamento imediato do reator: 300 ocorrências

- Este transiente tem relação direta com a operação do navio em uma situação de emergência ou diferente da condição normal, refletindo-se nos períodos de mudança da potência necessária para a execução da manobra de *Crash*, não havendo o desligamento imediato do reator.
 - Sendo assim, o número de ocorrências foi estimado levando-se em conta a ocorrência de pelo menos três vezes por ciclo operativo e duas vezes nos períodos de reparo de duração maior que o PMR. Neste último caso, trata-se de uma etapa de acompanhamento e aceitação dos trabalhos executados durante os referidos períodos de reparo, em Provas de Mar, o que normalmente acontece com todo o tipo de navio nestas circunstâncias. O total de ocorrências ao cabo dos 30 anos é assim estimado em 284, que podem ser aproximado para 300.
- b) Perda da potência elétrica: 200 ocorrências
- Este tipo de transiente é relacionado com a confiabilidade e operação da instalação elétrica. Neste caso, assumiu-se a ocorrência de até duas vezes por ciclo operativo, uma vez que o sistema elétrico deve possuir uma elevada confiabilidade, fruto do conhecimento do funcionamento que hoje já se consegue avaliar em instalações similares (navios/submarinos). Considerando-se que ocorra 1 vez por ciclo de manutenção demorada, face aos testes de aceitação, podemos esperar um total de 186 ocorrências ao longo da vida útil do SNAC II, que pode ser aproximado para 200 vezes.
- c) Perda parcial de escoamento no reator: 110 ocorrências:
- Este tipo de transiente pode receber os mesmos comentários que foram feitos acima porque se relaciona com uma elevada confiabilidade em operação. Além disso, podemos considerar também que ocorra quatro vezes no período de Comissionamento, 2 vezes por ciclo de manutenção demorada e no máximo uma vez por o ciclo operativo, totalizando-se assim cerca de 102 ocorrências em trinta anos, ou melhor dizendo 110 vezes.
- d) Desligamento do reator, quando em 100% da potência: 430 ocorrências
- Consideramos que este transiente decorra de um SCRAM, que fará com que o reator saia da condição de operação de Automático para a condição de Desligado a Quente.

- Este transiente deverá ter uma maior probabilidade de ocorrer quando do Comissionamento e dos primeiros ciclos operativos do SNA, não se descartando porém qualquer possibilidade de sua ocorrência nos períodos posteriores.
 - Assim sendo, estimamos a sua ocorrência em média de quarenta vezes durante o Comissionamento, quarenta vezes durante os testes dos períodos de reparo e manutenção, cinco vezes durante cada ciclo operativo dos primeiros quinze anos e três vezes em cada ciclo operativo dos quinze anos finais. Ao término de sua vida útil, o SNA poderá ter experimentado assim cerca de 430 ocorrências deste tipo de transiente.
- e) Despressurização súbita do sistema primário: 50 Ocorrências
- Este tipo de transiente admitimos que possa existir com uma probabilidade de ocorrência razoavelmente maior quanto mais próximo dos períodos de reparo de longa duração e, no caso, admitimos que possam ocorrer cerca de uma vez a cada três ciclos operativos do navio e cerca de duas vezes durante os períodos de reparo (PMG, PMF, PDR, PAM). No total, estimamos que possam existir cerca de 50 ocorrências.
- f) Operação inadvertida do sistema de resfriamento de emergência: 70 Ocorrências
- Este tipo de transiente pode ser preconizado por questões de adestramento, disfunções na operação do reator, sinais espúrios nos sistemas de acionamento de válvulas, interpretação errônea de avarias que tenha ocorrido no sistema primário. Como podemos observar, nossas hipóteses têm um cunho mais relacionado com o aspecto de treinamento e com o material humano do que estritamente com a parte técnica/equipamentos.
 - Assim sendo, estimamos a ocorrência de cerca de cinco vezes durante o período de comissionamento, uma vez durante os períodos longos de reparo (PMG, PDR, PAM e PMF) e duas vezes a cada três ciclos operativos, perfazendo um total de 70 vezes.
- g) Queda inadvertida de um elemento de controle: 90 ocorrências
- h) Retirada inadvertida de um banco de controle: 90 ocorrências

- Estes dois transientes têm relação com problemas de adestramento de operadores e/ou mal funcionamento de equipamentos acarretando distúrbios na geração de potência térmica do reator.
- Assim sendo, admitimos que tais transientes tenham uma maior probabilidade de ocorrência durante o período de Comissionamento e nos primeiros ciclos de reparo e operação. Com isso, pressupomos que ocorram 5 vezes durante o Comissionamento, 4 vezes após períodos de reparo de duração maior de um PMR e 1 vez a cada 3 ciclos de operação, nos primeiros 15 anos. Para os últimos 15 anos, admitimos 2 vezes após os períodos de reparo mencionados acima e 1 vez a cada 4 ciclos de operação.
- No total, teremos a ocorrência de no máximo de 86 vezes ao longo dos 30 anos, ou, aproximando-se, cerca de 90 vezes.

B.4 CONDIÇÕES DE PRONTIDÃO

A condição de prontidão para o submarino atender às Missões de Patrulhas Básicas, deve ser considerado no planejamento de um ciclo de atividades, levando em conta o número de submarinos em serviço ativo, de modo a se atender ao número de submarinos previsto para a Força Pronta e a tradicional regra dos terços de emprego de submarinos em tempo de guerra (um terço em manutenção, um terço em trânsito e um terço em patrulha).

- Condição I - Postos de Combate: toda tripulação em Postos de Combate. Nenhuma atividade de manutenção e rancho é executada. Todos sistemas deverão estar completamente guarnecidos. Máxima duração esperada de 8 horas, com frequência de ocorrência de 20 vezes por Missão de Patrulha.
- Condição II - Patrulha de Guerra: submarino guarnecido em dois quartos de serviço; somente as atividades essenciais de manutenção preventiva serão realizadas; metade da tripulação permanece em descanso; as atividades de rancho permanecem normais; o submarino deve ser capaz de lançar torpedos em 1 minuto; esta condição deverá ter ocorrência prevista em até 50% da duração da Missão de Patrulha Básica.
- Condição III - Patrulha de Paz: submarino guarnecido em três quartos de serviço; manutenção corretiva e preventiva realizada normalmente; o submarino deve ser capaz de lançar torpedos em 5 minutos.

- Condição IV - Porto: tripulação empregada em inspeções, manutenção corretiva e preventiva e administração; a tripulação deve ser organizada em divisões e quartos de serviço de porto normal (energia de terra) e especial (reator ligado) para atender às situações de emergência e atender à prontidão operacional desejada.
- Condição V - Navio em Período de Manutenção ou Reparo: a tripulação deve ser empregada no acompanhamento e execução da manutenção e reparo, adestramento em terra e férias/licenças regulamentares.

Partindo-se das condições IV e V o submarino deverá ser capaz de suspender no tempo máximo previsto na Tabela B.7.

TABELA B.7: TEMPO MAXIMO PARA O SNA SUSPENDER

TEMPO MÁXIMO PARA SUSPENDER		
CONDIÇÃO	III	II
IV – NORMAL	24 horas	6 horas
IV – EMERGÊNCIA	6 horas	imediato
V – PMR	Após teste de imersão a grande profundidade (IGP)	Após fim do período de manutenção
V- PMG	Após inspeção de eficiência operativa e de segurança nuclear	Após teste de imersão a grande profundidade (IGP) e inspeção de segurança nuclear

ANEXO C

LICENCIAMENTO DE INSTALAÇÕES NUCLEARES

C.1 ASPECTOS GERAIS

O projeto, construção, operação e manutenção de instalações nucleares deverá garantir que:

- a) em toda a situação de funcionamento, a exposição à radiação dentro da instalação ou devida a toda descarga planejada de material radioativo proveniente da instalação seja mantido abaixo dos limites prescritos e tão reduzidos quanto razoavelmente praticável;
- b) garantir, com alto nível de confiança, que, para todos os acidentes possíveis previstos, incluindo aqueles a probabilidade muito pequena, toda consequência radiológica será mínima e abaixo dos limites prescritos e que a possibilidade de acidentes que causem consequências severas é extremamente pequena.
- c) garantir que as consequências radiológicas de qualquer acidente podem ser mitigadas

A Segurança Nuclear das instalações e do transporte e armazenamento de materiais radioativos cobrirá os seguintes aspectos:

- 1) Segurança Técnica, incluindo:
 - a) Garantia da Qualidade;
 - b) Análise de Confiabilidade;
 - c) Simulação e Análise Funcional de Transientes Operacionais e Acidentes.
 - d) Avaliação de Consequências de Acidentes
- 2) Proteção Radiológica, incluindo:
 - a) Contenção e Blindagem biológica das fontes de radiação;
 - b) Contabilidade e Vigilância dos materiais radioativos;
 - c) Gerenciamento das Exposições à radiação, através da minimização do número de pessoas expostas e dos tempos de exposição, bem como a maximização da distância das fontes de radiação e da proteção individual.
- 3) Proteção Ambiental, incluindo:
 - a) Monitoração do Meio-Ambiente e da população nas vizinhanças das instalações;

b) Processamento e Gerenciamento de rejeitos e efluentes produzidos pelas instalações.

As instalações nucleares , bem como o transporte e armazenamento de materiais nucleares estão sujeitas, por força da legislação em vigor no Brasil , ao processo de Licenciamento Nuclear e ao processo de Licenciamento Ambiental.

O Licenciamento Nuclear consiste no conjunto de procedimentos técnico-administrativos que visam garantir que a Segurança Nuclear das instalações encontra-se em nível socialmente aceitável. Estes procedimentos estão sob autoridade da Comissão Nacional de Energia Nuclear - CNEN, sendo regidos pela Norma Experimental “NE-1.04 - Licenciamento de Instalações Nucleares”, aprovada pela Resolução CNEN- 11/84, de 04/dez/84.

O Licenciamento Ambiental consiste no conjunto de procedimentos técnico-administrativos que visam garantir que o impacto ambiental das instalações encontra-se em nível socialmente aceitável; estes procedimentos estão sob autoridade do Instituto Brasileiro do Meio Ambiente e Recursos Naturais Renováveis - IBAMA, e se processam através da elaboração do Estudo de Impacto Ambiental / Relatório de Impacto no Meio Ambiente - EIA/RIMA.

As instalações nucleares brasileiras estão ainda submetidas ao Regime de Salvaguardas de instalações e materiais nucleares estabelecido pelo Acordo Internacional Quadripartito e pelo Acordo Brasil - Argentina. Este regime é exercido pela Agência Brasil-Argentina de Controle e Contabilidade - ABACC e pela Agência Internacional de Energia Atômica - AIEA.

C.2 LICENCIAMENTO NUCLEAR

O processo de licenciamento nuclear pela CNEN consiste numa seqüência de autorizações administrativas concedida com base na análise de documentos padronizados elaborados pelo requerente:

- I. Aprovação do Local AL
- II. Licença de Construção LI
- III. Autorização para Utilização de Materiais Nucleares AUMN

IV. Autorização para Operação Inicial AOI

V. Autorização para Operação Permanente AOP.

Para a obtenção da Aprovação do Local AL junto à CNEN torna-se necessário desenvolver uma capacitação tecnológica multi-disciplinar requerida para elaboração do Relatório de Análise de Local RAL das instalações nucleares, que implica nas seguintes atividades:

- a) descrição da instalação, com as seguintes características gerais de projeto e de operação: emprego pretendido, capacidade nominal, cronograma do empreendimento, natureza e inventário dos materiais radioativos a serem contidos, probabilidade de liberação acidental de materiais radioativos, segurança do sistema de contenção
- b) características do local: distribuição da população, vias de acesso e meios de transporte, sismologia, meteorologia, geologia, hidrologia, usos do solo e atividades econômicas
- c) descrição dos sistemas de processamento de rejeitos e dos procedimentos para seu gerenciamento
- d) análise preliminar da influência no meio ambiente durante a construção e operação, usos do solo, água e liberações atmosféricas
- e) análise preliminar da influência no meio ambiente para possíveis acidentes: dispersão atmosférica e doses de radiação
- f) Programa Preliminar de Monitoração Pré-Operacional

Para a obtenção da Licença de Construção LC junto à CNEN é necessário apresentar o Cronograma Preliminar da Obra, o Plano Preliminar de Proteção Física (conforme norma CNEN NE 2.01 - Proteção Física de Unidades Operacionais da Área Nuclear) e Relatório Preliminar de Análise de Segurança RPAS das instalações nucleares. Para elaboração dos RPAS está sendo desenvolvida a complementação da capacitação tecnológica multi-disciplinar requerida para elaboração do RAL, o que implica nas seguintes atividades:

- a) qualificações técnicas do requerente;
- b) descrição e análise de segurança do local e da instalação;
- c) projeto preliminar da instalação (materiais, critérios, bases de projeto, cronograma);
- d) análise preliminar e avaliação do projeto e desempenho dos itens da instalação;

- e) descrição e justificativa da escolha das variáveis, condições ou outras características objeto de especificações técnicas para a instalação;
- f) planos preliminares de treinamento de pessoal para Operação Inicial;
- g) Programa de Garantia da Qualidade;
- h) caracterização dos itens da instalação que requeiram pesquisa e desenvolvimento;
- i) identificação dos riscos potenciais para funcionamento de itens importantes à segurança, decorrentes de eventuais atividades de construção de mais de uma instalação no mesmo local;
- j) Plano de Radioproteção;
- k) planos preliminares para procedimentos em situações de emergência;
- l) descrição dos sistemas de controle de liberação de efluentes e rejeitos;
- m) descrição do Plano Preliminar de Proteção Contra Incêndio; e
- n) Análise Sismológica

Para a obtenção da Autorização para Utilização de Materiais Nucleares AUMN junto à CNEN é necessário que a instalação esteja pronta para receber os materiais nucleares, cumprindo os requisitos da norma CNEN NE2.02 “Controle de Material Nuclear, Equipamento Especificado e Material Especificado” e que seja apresentado o Plano de Controle e Contabilidade de Materiais Nucleares PCCMN.

Para a obtenção da Autorização para Operação Inicial AOI junto à CNEN é necessário que a construção da instalação esteja substancialmente concluída, tendo-se suficientes garantias de não haver riscos indevidos para a população e meio-ambiente. Deverão ser apresentados o Cronograma Preliminar para Operação Inicial, o Plano Final de Proteção Física (conforme norma CNEN NE 2.01), AUMN já concedida, garantia financeira (conforme Lei de Responsabilidade Civil por Danos Nucleares), a Qualificação para Operação Inicial e o Relatório Final de Análise de Segurança RFAS. Implica nas seguintes atividades:

- a) resultados de programas de monitoração ambiental e meteorológico desenvolvidos desde a Licença de Construção;
- b) descrição e análise dos itens da instalação (funções de segurança a serem cumpridas);

- c) descrição dos sistemas e processos;
- d) controle de liberação de materiais radioativos;
- e) espécies e quantidades de materiais radioativos;
- f) análise e avaliação final do projeto;
- g) descrição e avaliação dos programas, incluindo pesquisa e desenvolvimento, para demonstrar que foram solucionados quaisquer problemas de segurança identificados na fase de construção;
- h) Programa de Operação da instalação, incluindo Programa de Garantia da Qualidade, programa de testes pré-operacionais e operação inicial, e programa de condução de operação normal;
- i) Especificações Técnicas propostas; e
- j) descrição do Plano de Proteção Contra Incêndio.
- k) descrição do Plano de Emergência;
- l) estrutura organizacional para fazer face à emergência;
- m) funções e posições do pessoal, com descrição das qualificações;
- n) meios de avaliação da amplitude do acidente;
- o) acordos firmados com autoridades locais, estaduais ou federais para medidas protetoras da população e do meio ambiente;
- p) exercícios para ensaiar o plano de emergência;
- q) atualização do quadro de pessoal para fazer face à emergência;
- r) instalações para primeiros socorros e descontaminação de pessoal;
- s) tratamento de pessoas em instalações hospitalares externas;
- t) treinamento do pessoal empregado na Organização Operadora;
- u) critérios para avaliar a conveniência quanto à reentrada ou reinício de operação após acidente;
- v) equipamentos para coleta de dados meteorológicos e hidrológicos; e
- w) descrição do Centro de Suporte Técnico

Para a obtenção da Autorização para Operação Permanente AOP junto à CNEN é necessário que as obras estejam concluídas e executadas conforme as normas, tendo-se

suficientes garantias de que a operação permanente não implicará em riscos indevidos para a população e meio-ambiente. Implica as seguintes atividades:

- a) Prazo e perfil de operação desejado,
- b) Relatório de Operação Inicial ROI, com o desenvolvimento e resultados dos testes realizados nesta fase
- c) Programa de garantia da Qualidade para Operação
- d) Garantia financeira (conforme Lei de Responsabilidade Civil por Danos Nucleares)
- e) Qualificação para Operação Permanente.

C.3 LICENCIAMENTO AMBIENTAL

Para o licenciamento ambiental junto ao IBAMA é necessário desenvolver-se a capacitação tecnológica multi-disciplinar requerida para elaboração do Estudo de Impacto Ambiental EIA e do Relatório de Impacto no Meio-Ambiente RIMA. Este relatório possui a seguinte itemização:

- a) Introdução
- b) Sumário Conclusivo
- c) Preliminares
- d) Informações Gerais
- e) Análise de Alternativas
- f) Descrição do Empreendimento
- g) Caracterização das Instalações
- h) Análise da Legislação
- i) Compatibilidade com Planos e Programas
- j) Metodologias Aplicáveis
- k) Análise da Propagação das Liberações
- l) Abrangência da Área de Estudos
- m) Diagnóstico das Áreas de Estudo
- n) Documentos de Referência
- o) Documentos de Apoio
- p) Relação de Documentos Anexos

- q) Aferição da Qualidade Ambiental
- r) Identificação dos Potenciais Impactos Ambientais
- s) Avaliação Ambiental
- t) Diretrizes para Gerenciamento Ambiental
- u) Conclusões e Recomendações

ANEXO D

INCIDÊNCIA DE PERIGOS INDUSTRIAIS E RADIOLÓGICOS

D.1 PERIGO E RISCO

Tradicionalmente, perigo é definido como um prejuízo potencial que pode recair sobre pessoas, bens ou meio-ambiente. Esta noção é geral, e deve corresponder a uma situação suficientemente bem determinada e descrita num grau de detalhe adaptado ao uso que se pretende fazer deste conceito.

Esta definição pode se referir tanto às situações perigosas de natureza aleatória, de origem natural, tecnológica ou econômica, como às situações ameaçadoras de natureza determinista, ligadas a ações intencionais ou atos de sabotagem.

O conceito de perigo está baseado somente nas consequências potenciais de um evento indesejável ou temido E , sem considerar as possibilidades reais de que o mesmo venha a efetivamente ocorrer. Estas consequências podem por sua vez serem classificadas numa escala hierárquica de gravidade g : um perigo será tanto maior como forem mais graves as suas consequências. Perigo é então um conceito unidimensional, associado unicamente a gravidade das consequências do evento E .

Risco é a percepção ou avaliação das possibilidades da efetiva ocorrência de um evento indesejável E que conduza a concretização a um perigo, que por definição é algo potencial, ou seja, que ainda não ocorreu. Como foi visto, um perigo está associado ocorrência de consequências com uma determinada gravidade.

Diferentemente de perigo, o conceito de risco está então baseado não somente nas consequências (e sua gravidade), mas também nas possibilidades de ocorrência destas consequências. Concretamente, risco é um conceito bidimensional mais abrangente do que perigo, que conjuga tanto a possibilidade como a gravidade de um evento E .

Este caráter bidimensional do risco torna sua hierarquização impossível: a teoria dos conjuntos mostra que não existe relação de ordem em $\Re^2$, conjunto dos conjugados de números reais, donde se conclui que, em teoria, não se pode comparar (p_1, g_1) e (p_2, g_2) .

Para que os conceitos de perigo e risco possam ser efetivamente utilizados na Segurança de Funcionamento de Sistema, torna-se necessário quantificar p e g. Estabelecendo-se uma relação funcional que os conjuga para formação de R, pode-se contornar o problema teórico de hierarquização.

Para quantificar a possibilidade p, o método mais utilizado é associar uma probabilidade $P(E)$ de ocorrência do evento E. A quantificação da escala de gravidade, que possibilita medir g dependerá da natureza do evento E, pois conforme foi visto, o perigo incide sobre as pessoas, os bens e o meio-ambiente. Para eventos cujas conseqüências são de mesma natureza, o estabelecimento desta escala torna-se relativamente simples, como por exemplo:

- a) para um perigo cujas conseqüências correspondam a um tipo único de injúria (como morte), incidindo somente sobre um grupo homogêneo de seres humanos para o qual se espera respostas somáticas à injúria sofrida semelhantes (como o grupo de operadores de uma instalação), a escala é definida pelo número de pessoas atingidas;
- b) para um perigo cujas conseqüências correspondam a um tipo único de injúria (como vazamento de petróleo bruto no ambiente), incidindo somente sobre uma área homogênea e definida (como uma determinada e limitada zona litorânea), a escala é definida pela quantidade liberada para o meio-ambiente;
- c) para um perigo que incida exclusivamente sobre bens materiais e propriedades, a escala monetária é definida pelos custos associados às perdas e danos ocorridos.

Estas condições ideais, entretanto, muito poucas vezes se aproximam da realidade de uma análise de segurança, pois dentre outros aspectos:

- a) os perigos geralmente incidem simultaneamente sobre as pessoas, os bens e o meio ambiente;
- b) os grupos de pessoas sobre os quais os perigos incidem não são homogêneos (o chamado "público", que não é individualmente identificável, envolve diversas faixas etárias, ambos os sexos, pessoas eventualmente já debilitadas ou particularmente suscetíveis, implicando em diferentes sensibilidades aos efeitos dos evento incorridos);
- c) as injúrias sobre as pessoas são de tipos diversos, cuja gravidade relativa é de difícil comparação, tais como:

- distúrbios psicológicos temporários e permanentes;
 - ferimentos leves e graves;
 - invalidez temporária e permanente;
 - morte imediata e a curto prazo após o evento;
 - efeitos retardados, de caráter em geral estocásticos, ocorrendo a longo prazo após o evento tais como:
 - aumento da possibilidade de contrair um câncer devido à incorporação de produtos químicos e/ou exposição às radiações ionizantes;
 - aumento da probabilidade de ocorrência de distúrbios genéticos sobre as gerações futuras
- d) as liberações para o meio ambiente são compostas por mais de um produto, com nocividades diferentes sobre o público e as demais formas de vida animal e vegetal;
- e) as áreas físicas do ambiente que recebem as liberações não são homogêneas, isto é, possuem diferentes respostas ecológicas às agressões, nem perfeitamente definidas.

Por estas razões, as escalas de conseqüências usadas na prática possuem um forte conotação subjetiva e em geral não abrangem todas as conseqüências associadas a um evento, retendo-se em geral um único tipo de conseqüência, considerada a mais grave.

Para conseqüências relativamente leves, que não envolvam a morte imediata de pessoas identificáveis ou danos irreparáveis ao meio ambiente, tais como as que envolvem efeitos retardados de caráter estocástico, com as exposições a pequenas doses de radiação ionizante, existe uma tendência a adotar-se escalas de gravidade monetárias.

Cumprе ressaltar que o estabelecimento e quantificação de escalas de gravidade de eventos acidentais catastróficos é um problema que extrapola as técnicas de engenharia, reportando-se também à economia, epidemiologia, sociologia, ecologia, dentre outras ciências sociais e bio-médicas. Estas escalas suscitam diversos questionamentos de ordem ética e deontológica, que a engenharia não pode deixar de considerar.

O terceiro aspecto relevante para aplicação do conceito de risco na Segurança de Funcionamento de Sistema, é o estabelecimento de uma relação funcional que conjugue p e g

, supondo-os numericamente determinados, numa medida única para formação do valor de R , e sua conseqüente quantificação unidimensional.

Uma função racional considerada para esta relação é a expectância matemática das conseqüências, ou seja, o produto ($p \times g$). Neste modelo, supõe-se que o risco independe de p e g , dependendo somente do seu produto ($p \times g$), ou seja, para uma probabilidade constante, o risco aumenta linearmente com a gravidade e vice-versa.

Para probabilidades relativamente elevadas, de conceito clássico ou conceito de frequência relativa e, ainda mais importante, para conseqüências com gravidade limitada, a utilização desta função não apresenta problemas especiais, além daqueles associados ao rigor da modelagem do sistema em estudo.

Quando, entretanto, os eventos são raros, ou seja, probabilidades muito reduzidas e conceitualmente indutivas (probabilidade como verossimilhança) com conseqüências severas, incluindo, por exemplo, morte de grande número de pessoas, surgem importantes restrições ao seu uso:

- a) uma terceira componente do risco, até aqui citada mas não considerada, passa a ser preponderante, i.e. a percepção individual ou coletiva da situação perigosa e do evento E que a provoca; e
- b) considerações éticas e deontológicas que suscitam o modelo de expectância, devidas basicamente à aplicação de uma racionalidade tecnocrática a problemas de cunho fortemente social e psicológico, e em última instância políticos. Estas considerações fogem completamente ao escopo da engenharia propriamente dita, porém os técnicos envolvidos na análise de segurança de sistemas que podem ensejar este tipo de risco devem estar conscientes de sua existência, sabendo que as decisões tomadas ao nível individual ou coletivo na área de prevenção de eventos com conseqüências severas escapam à racionalidade técnica.

A percepção individual ou coletiva do risco pode, em teoria, ser integrada a uma função que conjugue probabilidade e gravidade. O modelo de expectância matemática de conseqüências supõe que a percepção seja independente da gravidade. Pode-se então, através dos métodos de pesquisa sociológicos modelar a aversão às conseqüências severas,

que empiricamente observa-se nas pessoas e nas sociedades. Note-se que a aversão individual pode divergir sensivelmente da coletiva: por exemplo, a mesma pessoa, individualmente pode ser tabagista e coletivamente rejeitar a instalação de uma fábrica que se supõe poluente na sua vizinhança.

Considerando que todas as atividades humanas, notadamente as atividades industriais complexas como a operação de instalações nucleares e navios, são associadas a riscos de vários tipos, relacionados a diferentes efeitos nocivos aos indivíduos, sociedade, meio ambiente, bens materiais e propriedades, pode-se depreender que risco zero e uma abstração totalmente irreal.

A abordagem lógica, intuitiva, de otimização é então fazer com que um acidente seja tanto mais improvável quanto suas conseqüências poderiam ser mais sérias. É absolutamente necessário que um acidente muito grave, tendo severas conseqüências possa ser considerado como altamente improvável.

Este procedimento “instintivo” guiou os primeiros trabalhos no campo da segurança, sendo simbolizado pela “curva de Farmer” que representa, sobre um diagrama probabilidade x conseqüência, um domínio autorizado e um domínio proibido, sendo as conseqüências expressas em valores assumidos para os rejeitos de matérias radioativas feitos por uma instalação nuclear após um acidente (a curva do trabalho original de Farmer tratava de rejeitos em Iodo-129).

Os projetistas de centrais nucleares buscaram em seguida aprofundar e precisar esta curva, determinando os pares (probabilidade; conseqüências radiológicas) consideradas como aceitáveis. Após, os organismos de segurança definiram limites indicativos da probabilidade máxima de acidentes suscetíveis de provocar conseqüências consideradas como inaceitáveis, sendo as situações de probabilidade ainda menores consideradas como o inevitável risco residual.

Estabelecidos estes objetivos, resta demonstrar que todos os tipos de acidentes julgados como plausíveis foram considerados e analisados pelos estudos de acidentes da

instalação e que os sistemas de segurança e emergência dos quais a instalação é dotada permitem efetivamente satisfazer este objetivo.

D.2 SEGURANÇA ABSOLUTA E RISCO ACEITÁVEL

A segurança absoluta (ou total) de uma atividade ou sistema corresponde à impossibilidade de ocorrência de um acidente catastrófico qualquer que seja o momento considerado (no presente ou no futuro) e qualquer que seja o estado do sistema ou de seu ambiente para o conjunto de todas as falhas, erros humanos e agressões externas possíveis.

Um tal projeto necessitaria então o conhecimento perfeito e exaustivo do sistema, além dos problemas de qualidade no projeto, fabricação, construção e operação, e de todos os seus estados possíveis, assim como a consideração de todos os ambientes exteriores, mesmo os mais extremos e raros.

Esta hipótese de trabalho não é, obviamente razoável, seja por razões de conhecimentos científicos, seja por razões tecnológicas e, mais simplesmente, por razões da imaginação humana. Isto se traduz por um dos princípio de base da segurança dos sistemas:

A segurança absoluta é uma utopia.

Esta noção primária de “segurança absoluta e certa”, correspondendo aprioristicamente à impossibilidade de ocorrência de acidentes catastróficos, deve ser substituída pela noção de “segurança objetiva”, relativa a um risco aceitável com respeito a esforços financeiros e técnicos realistas dispendidos.

Apesar da abordagem acima descrita ser bastante clara e objetiva, ela apresenta dificuldades para ser colocada em prática, pois é baseada nos conceitos de "plausibilidade" e "aceitabilidade" que estão diretamente ligados à percepção individual e social do risco.

Primeiramente, a definição dos acidentes plausíveis pode ser extremamente controversa. Por exemplo, a queda de um pequeno avião civil sobre uma instalação industrial é plausível? e de um Jumbo 747? e de um avião militar de caça? e de um meteoro? A resposta a estas perguntas depende do nível de risco residual socialmente aceito, que por sua vez depende do local onde a instalação está implantada e da significância estatística da base de dados históricos sobre eventos similares ocorridos no local.

Por outro lado, encontrar um consenso social sobre qual é o nível de risco residual aceitável é tarefa das mais difíceis, pois a percepção psico-social do risco varia sensivelmente de pessoa a pessoa e de comunidade a comunidade.

Quando o risco é avaliado como o produto probabilidade x consequência, ou seja, segundo o modelo de expectativa matemática das consequências, e é assim utilizado para definir limites de aceitabilidade, infinitos questionamentos individuais podem ser gerados, pois ao nível psicológico individual, o risco muito dificilmente será percebido da mesma forma, o que explica a eterna polêmica sobre a segurança das instalações nucleares em todo o mundo (a parte certos aspectos políticos que não nos cabe aqui discutir). A pergunta “quanta segurança e suficientemente segura” resta sempre sem resposta social definitiva.

Resta ainda um outro ponto importante: além das consequências dos acidentes ao nível individual e coletivo, um acidente grave envolve outras consequências, tais como a poluição do meio-ambiente, restrições ao uso da terra e seus produtos, problemas sociais ligados a evacuação de populações, dentre outros. Agregar todas estas consequências em uma avaliação de risco unificada é tarefa das mais complexas, ou mesmo impossível.

Finalmente, a avaliação prática da probabilidade de eventos altamente improváveis é extremamente imprecisa, o que lhe retira todo caráter de valor absoluto. Sua utilidade se restringe à comparação com valores, calculados pela mesma metodologia, obtidos para outras instalações similares.

Os indivíduos toleram diferentes níveis de risco dependendo dos benefícios que eles imaginam ganhar assumindo-os. Igualmente, a tolerância social de diferentes riscos varia significativamente devido a uma série de razões, algumas objetivas e passíveis de avaliação científica e outras totalmente subjetivas, derivadas de atitudes psicológicas complexas.

Frank Layfield introduziu o termo tolerabilidade em seu relatório sobre a audiência pública da usina nuclear de Sizewell B, na Grã-Bretanha. Tolerável não significa aceitável: implica nos limites máximos de aceitabilidade, enquanto aceitável implica numa aquiescência voluntária. Tolerar um risco não significa que ele seja desprezível, ou que possa ser ignorado, mas que é necessário mantê-lo sobre constante revisão e reduzi-lo ainda mais, se for técnica e

economicamente possível. Existe ainda uma clara implicação de que alguns riscos simplesmente não podem ser tolerados.

Uma consolidação da filosofia de tolerabilidade de riscos foi desenvolvida na Grã-Bretanha, em resposta às considerações feitas por ocasião da audiência pública de Sizewell B. Uma das maiores dificuldades desta filosofia está no fato de que as regulamentações de segurança estão baseadas na necessidade dos riscos serem reduzidos a um nível tão baixo quanto razoavelmente praticável - o princípio da otimização *As Low As Reasonable Achievable* ALARA. Teoricamente, isto implica numa redução contínua do risco, na qual o custo desta redução, qualquer que seja o grau de risco envolvido, é comparado com os benefícios obtidos, em termos da redução das consequências, ou do “detrimento”, segundo jargão próprio). Quando os custos tornam-se desproporcionais aos benefícios, pode-se considerar que o sistema encontra-se num nível aceitável.

Entretanto, deve-se reconhecer que existe sempre um nível máximo de risco que simplesmente não pode ser tolerado, a não ser em circunstâncias extraordinárias. O Princípio ALARA somente pode ser aplicado quando este limite é estabelecido implícita ou explicitamente. Igualmente, existe um nível mínimo de risco de um sistema que pode ser considerado como desprezível quando comparado com os riscos associados a outras atividades humanas.

O princípio ALARA irá conseqüentemente ser aplicado entre o limite superior de tolerabilidade do risco e o limite inferior onde este risco pode ser negligenciado. À medida que o risco é reduzido, a atividade (ou sistema) torna-se progressivamente mais aceitável e, conseqüentemente, menos esforços devem ser despendidos para reduzi-lo.

Para que um tal modelo possa efetivamente ser utilizado em Segurança de Sistemas, torna-se necessário, inicialmente, definir quantitativamente os níveis de tolerabilidade e de negligibilidade. Em seguida é preciso desenvolver uma metodologia para demonstrar que a segurança de um sistema está conforme a este modelo.

D.3 COMPROMISSO ENTRE RISCOS LOCAIS E RISCOS GLOBAIS

Como foi visto, os riscos incidem basicamente sobre as pessoas, o meio-ambiente e os bens ou propriedades. No que tange as pessoas, pode-se entretanto discriminar pelo menos três grupos humanos que podem ser afetados, em ordem crescente de gravidade:

- a) os operadores e trabalhadores no interior da instalação perigosa;
- b) as populações mais diretamente afetadas pelas potenciais conseqüências da operação da instalação industrial, em geral vivendo próximo a ela (“grupo crítico”), que em alguns casos se beneficia da existência da instalação, em termos de empregos e infra-estrutura social; e
- c) o público em geral, afetado de modo indireto e em geral pouco severo, pelas potenciais conseqüências da operação da instalação.

A percepção do risco e conseqüentemente sua aceitabilidade varia sensivelmente para cada grupo. O poder de pressão político de cada um destes grupos influenciará de forma significativa as opções técnicas adotadas para a instalação. Deve-se portanto ter a preocupação de verificar se uma determinada opção de segurança que reduz o risco de um dos grupos, não aumenta, de forma desproporcionada, o risco dos outros.

No que tange o meio-ambiente, também pode-se identificar áreas físicas de incidência das conseqüências da operação da instalação industrial: local, regional, macro-regional e global.

A percepção do risco também varia sensivelmente de acordo com a extensão da área potencialmente afetada. Por exemplo, um indivíduo (ou grupo social) pode estar fortemente motivado a defender ações que supostamente reduzem o chamado “efeito estufa” global e ser relativamente indiferente à poluição por esgoto urbano do rio que passa ao lado de sua residência.

Da mesma forma dos riscos sobre as pessoas, o poder de pressão político dos grupos que defendem o ambiente das diferentes áreas afetadas influenciará de forma significativa as opções técnicas de adotadas para a instalação. Deve-se portanto também ter a preocupação de verificar se uma determinada opção de segurança que reduz o risco para uma área, não aumenta, direta ou indiretamente de forma desproporcionada, o risco para as outras.

Estes dois aspectos são altamente significativos para a determinação da estratégia de gestão de rejeitos e efluentes normais e acidentais de instalações industriais.

D.4 ASPECTOS ECONÔMICO-FINANCEIROS

A terceira área de incidência dos riscos de uma instalação industrial refere-se aos bens e às propriedades individuais ou coletivas, envolvendo aspectos econômico-financeiros.

A ocorrência de um evento indesejado numa instalação industrial implica em significativas perdas materiais:

- a) perdas de produção devido à interrupção da operação, que poderá ser mais ou menos demorada dependendo do evento e do tipo de instalação, chegando até mesmo ao descomissionamento definitivo;
- b) perdas de capital devido às avarias decorrentes do evento indesejado e gastos associados à reparo destas avarias;
- c) perdas de valor mobiliário devido a possível desvalorização das ações da empresa à qual pertence a instalação acidentada;
- d) perdas devido a indenizações e auxílios a serem pagos às pessoas diretamente e indiretamente injuriadas pelo acidente, sejam trabalhadores da instalação ou público em geral; e
- e) perdas devido a eventuais ações de evacuação, descontaminação e recuperação de áreas internas e externas à instalação.

Analisando o problema sob estes aspectos, nota-se que a segurança é um investimento que propicia significativos retornos, ou seja, a não ocorrência destas perdas. Entretanto, os recursos para investimento são por definição limitados e portanto a segurança também tem um limite, principalmente quando se observa que o objetivo de uma instalação industrial é a produção, a preços competitivos, e não exclusivamente a segurança.

Note-se ainda que todo processo produtivo implica em custos externos, não incluído nos preços da produção, que são arcados, indiretamente, pela sociedade como um todo. Os riscos da instalação industrial produtora constituem uma destas externalidades. Uma estratégia

sócio-política válida para a melhoria da segurança das instalações industriais seria a internalização do custo dos riscos a ela associados. Tal política beneficiaria, em termos de preços, as instalações com melhores padrões de segurança.

D.5 RISCOS RADIOLÓGICOS

A radioatividade é o fenômeno pelo qual um átomo instável se desintegra emitindo radiações sob a forma de partículas α e/ou β e fótons energéticos (raios γ e/ou X) até atingir um estado de equilíbrio (FOOS, 1993). Sua unidade de medida é o bequerel (Bq), igual a 1 desintegração/s.

Estas radiações quando em interação com a matéria provocam ionizações e excitações eletrônicas. Se a matéria em interação é constituída por tecidos biológicos, estes efeitos podem causar a destruição de moléculas vitais ao funcionamento das células, tais como proteínas e ácidos nucléicos. Portanto, todas as radiações capazes de causar estes efeitos direta ou indiretamente constituem fontes potenciais de agressões aos seres vivos (BERTIN, 1991).

Duas unidades de medida são empregadas para expressar os efeitos biológicos das radiações ionizantes:

- a) Gray (Gy), que corresponde a 1J/kg, expressando diretamente a energia depositada na matéria pela radiação, ou seja, a dose de radiação absorvida;
- b) Sievert (Sv), que corresponde ao produto da dose absorvida por um “fator de qualidade” associado a cada tipo de radiação, que exprime, com relação aos fótons energéticos (X e γ) o número de ionizações provocadas por Gy absorvido; por exemplo, o fator de qualidade da radiação α é igual a 20, ou seja 1 Gy de α provoca 20 vezes mais ionizações que 1 Gy de γ ; a esta medida denomina-se “dose equivalente”.

Se um número suficientemente grande de células é destruído, um dano físico pode ser observável, correspondendo à perda de função do tecido atingido. A partir de um certo nível de exposição, a deterioração se tornará evidente e sua gravidade aumentará com a dose recebida. Este tipo de efeito é denominado “determinístico”.

Uma célula viva porém transformada pela ionização decorrente da radiação pode levar à formação de um câncer ou tumor maligno após um longo lapso de tempo, conhecido como “período de latência”. A probabilidade deste tipo de câncer ocorrer depende da dose equivalente recebida. Este tipo de efeito é denominado “estocástico”.

Se a função da célula afetada é transmitir caracteres genéticos aos descendentes, efeitos de variados tipos e graus de gravidade podem aparecer nas gerações futuras da pessoa irradiada. Este tipo de efeito é denominado “hereditário”.

Como pode ser depreendido, não é simples avaliar as consequências da exposição dos seres vivos às radiações ionizantes, que podem incluir um aumento da probabilidade de ocorrência de câncer, que poderá surgir 20 ou 30 anos após a irradiação, efeitos deterministas a partir de certo limiar de dose (200-300 Gy) e possível transmissão de efeitos negativos às gerações futuras. Além disto, a sensibilidade às radiações é individualmente variável, dependendo do sexo e da idade.

Os métodos de avaliação dos efeitos biológicos da radiações ionizantes são estabelecidos pela International Committee on Radiological Protection ICRP, particularmente por (ICRP, 1991).

O sistema de proteção radiológica recomendado pela ICRP é baseado em três princípios gerais:

- a) Justificação: nenhuma prática deve ser adotada se o benefício a ser obtido não for suficientemente superior ao detrimento radiológico que poderia provocar;
- b) Limitação: a exposição de qualquer pessoa às radiações emitidas por fontes radiativas controladas associadas a uma prática justificada deve ser sujeita a limites máximos aceitáveis; os limites fixados são:
 - 100 mSv durante 5 anos para trabalhadores com radiações, sem exceder em nenhum ano 50 mSv;
 - 1 mSv por ano para o público em geral;
- c) Otimização: as doses induzidas por quaisquer fontes radioativas associadas a uma prática justificada e limitada devem ser mantidas tão baixas quanto razoavelmente alcançável,

levando-se em conta fatores econômicos e sociais (*As Low As Reasonable Achievable* ALARA).

Para limitação de doses sobre trabalhadores em caso de incidentes ou acidentes, os seguintes princípios devem ser respeitados:

- a) a redução de dose que se espera alcançar por meio de uma intervenção deve ser suficiente para contrabalançar os efeitos sobre os trabalhadores envolvidos na execução da intervenção e seu custo, incluindo o custo social;
- b) a intervenção deve ser planejada em detalhe para garantir que o benefício em redução de dose seja abrangente e efetivamente alcançado;
- c) certas intervenções passíveis de provocar altas doses para alguns trabalhadores somente podem ser justificadas pela necessidade de prevenir efeitos determinísticos graves para uma população ampla; neste caso, o princípio de limitação de doses individuais não é aplicável, já que ele poderia limitar os efeitos benéficos da intervenção para a comunidade.

Para limitação de doses sobre o público em geral no caso de incidentes e acidentes não existem recomendações explícitas da ICPR nem um consenso internacional. No caso de reatores núcleo-elétricos, valores orientativos, sem caráter regulamentar, são apresentados por (ANSI/ANS, 1983; HSE, 1992; LIBMANN, 1996). Estes limites são expressos sob forma de riscos de exposição individual de corpo inteiro e da tireóide, i.e. pares (dose, probabilidade). A ênfase sobre limitação de dose sobre a tireóide prende-se ao fato da liberação de isótopos radioativos de iodo, que são incorporados nesta parte do corpo, ser particularmente relevante em acidentes nestas instalações.

ANEXO E

ANÁLISE DE MODOS DE FALHA EM SISTEMAS

E.1 SISTEMA

Um sistema é um conjunto determinado de elementos discretos (ou componentes) interconectados ou em interação. A palavra "determinado" implica que o sistema considerado é identificável, o que constitui um requisito indispensável para que possa ser analisado. É necessário também notar que a definição indica que o sistema é feito de partes componentes em interação: supõe-se assim que o sistema não é simplesmente a soma de suas partes. Isto implica que se a natureza de uma parte componente se modifica em consequência de um determinado evento, todo o sistema é modificado.

Pode-se encontrar na literatura diferentes termos para designar a hierarquia entre as partes componentes de um sistema. Com o objetivo de padronização e clareza, no presente trabalho utilizaremos as noções de item, componente, sub-sistema, sistema elementar e sistema, com as seguintes relações inclusivas:

$$(\text{ITEM}) \subset (\text{COMPONENTE}) \subset (\text{SUB-SISTEMA}) \subset (\text{SISTEMA ELEMENTAR}) \subset (\text{SISTEMA})$$

Deste modo, um sistema será representado pela Figura E.1 e caracterizado por:

- a escolha de um limite de resolução definindo os componentes considerados, o que definirá o nível de detalhe da análise a ser efetuada sobre o sistema; as fronteiras entre os diversos sistemas elementares será denominada "interface";
- a escolha dos limites exteriores e do ambiente do sistema; os limites exteriores envelopam o conjunto de sistemas em interação com o sistema estudado e são determinantes para a descrição do próprio sistema e de suas funções.

Neste trabalho será utilizado o termo "entidade" sempre que não existir necessidade de fazer referência à estrutura interna do sistema (e portanto a suas partes componentes). Caso contrário, será utilizado o termo "sistema".

Todo sistema se define geralmente por uma ou várias funções (ou missões) que devem ser cumpridas dentro de condições e dentro de um ambiente previamente estabelecidos (desempenho requerido), a partir de partes componentes determinadas.

FIGURA E.1: REPRESENTAÇÃO DE UM SISTEMA

As características mais importantes de um sistema, que devem ser precisadas antes de sua análise são:

a) funções do sistema:

- funções ou missões principais;
- funções ou missões secundárias ; e
- hierarquia (gradação de importância) destas funções.

b) estrutura do sistema:

- partes componentes, com suas funções individuais, suas características de funcionamento e desempenho;
- interrelações entre as partes componentes; e
- localização da partes componentes.

c) condições de funcionamento do sistema:

- estados de funcionamento;
- condições de funcionamento dos componentes e do sistema; e
- possibilidades de mudanças de configuração (ou reconfigurações).

d) condições de operação (ou exploração, no sentido mais amplo) do sistema:

- condições de monitoração (ou vigilância, num sentido mais amplo) do sistema (alarmes, inspeções, verificações, testes periódicos);
- condições de intervenção sobre o sistema (manutenção, reparo); e
- especificações técnicas de operação, isto é, os procedimentos, condições e restrições que devem ser respeitados durante a operação do sistema.

e) ambiente do sistema:

- outros sistemas elementares da instalação ou do processo global dentro do qual o sistema analisado se situa;
- conjunto de operadores humanos que intervêm sobre o sistema; e
- meio-ambiente propriamente dito, que pode manifestar-se por condições ambientes desfavoráveis (temperatura, pressão, umidade, vibrações, níveis de radiações eletromagnética e ionizante), fenômenos meteorológicos particularmente severos (inundações, ventos, estados de mar), ou agressões externas de origem natural (sismos, maremotos, vulcanismo) ou industrial (queda de aeronaves, explosões próximas)

Ao longo das diferentes fases do projeto do sistema, nem todas estas características são conhecidas. Isto implica na necessidade de aproximações e hipóteses. Na medida que a concepção do sistema avança e estas diferentes informações podem ser precisadas, as análises de segurança de funcionamento devem ser corrigidas, modificadas, aperfeiçoadas, ou seja devem ser periodicamente revistas.

E.2 ANÁLISE DE UM SISTEMA

A análise de um sistema é um processo orientado em direção da aquisição, investigação e tratamento ordenado de informações específicas ao sistema e pertinentes a uma decisão ou um objetivo dado. Este processo implica no desenvolvimento de um modelo do sistema.

Segundo esta definição, a função principal da análise do sistema é a aquisição de informações. Este processo deve ser realizado segundo regras ou métodos, caso contrário o modelo correspondente pode demonstrar-se pouco útil ou pouco adaptado aos objetivos.

A primeira pergunta que se coloca é: quais as informações que devem ser obtidas? A resposta não é tão evidente quanto possa parecer à primeira vista.

Considere-se a Figura E.2. Um círculo representa a informação que é essencial de ser obtida para o objetivo de análise do sistema. Um analista especialista nos problemas do tipo A começa seu estudo neste domínio e é conduzido a certas questões interessantes que o levam ao domínio A1. A pesquisa do domínio A1 o conduz a A2 e assim por diante. Um outro analista especialista dos problemas do tipo B segue o mesmo procedimento que o leva a B1, depois a B2, e assim por diante.

FIGURA E.2: INFORMAÇÕES NECESSÁRIAS À ANÁLISE DO SISTEMA

Para ilustrar este problema, considere-se um sistema de segurança de uma grande instalação industrial: o analista começa pelas causas de falha de natureza elétrica dos acionadores do sistema, prossegue examinando as fontes elétricas internas da instalação, depois as alimentações elétricas externas. Expirado o prazo do trabalho, especialmente o momento de apresentar a análise ou de tomar decisões, a informação pertinente não está disponível, apesar dos grandes esforços feitos.

Para evitar esta "deriva" na análise é muito importante fixar, já a partir do seu início, as principais características do sistema a serem consideradas, tais como:

- a) limites interiores da análise: onde serão definidos notadamente os limites físicos, geográficos e funcionais do sistema, assim como as interfaces com outros sistemas e o meio-ambiente; e

b) limites de resolução da análise: onde serão definidos notadamente os níveis de profundidade da análise, ou seja, se ela deverá descer até o nível de item, ou se será restrita ao nível de componente ou sub-sistema ou sistema elementar.

Evidentemente, estes limites podem ser revistos ao longo do estudo, mas esta revisão deve ser feita com pleno conhecimento de todas as suas implicações, tais como carga de trabalho, tempo de análise, ponderação da distribuição de esforços pelas áreas mais importantes.

O processo de análise deve conduzir à obtenção de um primeiro modelo do sistema. Estudos complementares conduzem a novas informações que são agregadas ao modelo, gerando revisões que devem convergir para o modelo final do sistema. As conclusões da análise assim com as decisões a serem tomadas são então baseadas neste último modelo. A Figura E.3 ilustra este conceito.

FIGURA E.3: ETAPAS DO PROCESSO DE ANÁLISE

E.3 FALHA

Entende-se como falha um evento que implica na interrupção da capacidade de uma entidade atender a um função requisitada.

Diz-se então que uma entidade sofreu uma falha, quando ela deixa de estar em condições de cumprir sua(s) função(ões). Por extensão, pode-se considerar que há uma falha quando existe uma alteração na capacidade de uma entidade cumprir uma função requerida: as tolerâncias associadas devem neste caso serem definidas.

Com o objetivo de melhor definir esta noção de falha, podem ser estabelecidas diversas classificações:

- a) quanto a rapidez de manifestação:
 - falha progressiva: falha devida a uma evolução no tempo das características de uma entidade; em geral pode ser antecipada pela vigilância (monitoração, inspeção, testes, ensaios); e
 - falha abrupta: falha que não se manifesta por uma perda progressiva de desempenho e que não pode ser antecipada pela vigilância.
- b) quanto à amplitude:
 - falha parcial: resultante do desvio de características além dos limites especificados, mas de tal forma que não implique numa interrupção completa da função requerida ;
 - falha total: resultante do desvio de características além dos limites especificados, implicando numa interrupção completa da função requerida.
- c) quanto ao conjugado rapidez x amplitude:
 - falha cataléptica: falha ao mesmo tempo abrupta e total;
 - falha por degradação: falha ao mesmo tempo progressiva e parcial, que a longo prazo pode tornar-se total.
- d) quanto à época de surgimento dentro da vida útil do sistema:

Consideremos um conjunto de entidades supostas idênticas e em funcionamento desde o instante inicial $t = 0$. Define-se a taxa de falhas como a fração λ , normalizada na unidade de tempo, das entidades que, tendo sobrevivido num instante qualquer t , sofrem uma falha total até o instante $t + \Delta$. Passando ao limite, obtemos a taxa de falhas instantânea, que é uma função de t .

Observe-se que as entidades freqüentemente apresentam uma taxa de falhas em função do tempo sob a forma de uma curva dita “banheira” (Figura E.4).

Depreende-se desta curva três períodos distintos, associados a três diferentes tipos de taxa de falhas, na vida útil das entidades que têm esta característica:

- falha precoce (ou juvenil), que ocorre no início da vida útil da entidade, com uma taxa de ocorrência decrescente com o tempo, o início de vida sendo contado a partir de um instante $t = 0$ especificado;
- falha a taxa constante, que ocorre na maior parte da vida da entidade de forma sensivelmente constante; e
- falha de desgaste, que aparece no fim da vida útil da entidade, com uma taxa de ocorrência crescente com o tempo, sendo geralmente devida a processos de "envelhecimento" inerentes à entidade, tais como a deterioração por fadiga e corrosão.

FIGURA E.4: CURVA “BANHEIRA”

e) Quanto aos efeitos:

As falhas que ocorrem em um sistema são suscetíveis de provocar efeitos muito diferentes. Certas falhas não afetam diretamente as funções do sistema e necessitam tão somente de uma ação corretiva simples (reparo sem urgência, por exemplo). Outras falhas afetam a disponibilidade do sistema ou a sua segurança. Os efeitos das falhas são então avaliados, utilizando-se uma escala de gravidade pela qual se reparte os níveis de degradação do funcionamento do sistema em categorias ou classes. Habitualmente considera-se quatro categorias apresentadas pela Tabela E.1.

Esta classificação pode igualmente qualificar as conseqüências de um evento. Tem-se, entretanto, a seguinte diferença entre os dois conceitos:

- efeitos são todas as manifestações que resultam da ocorrência de um evento, que se supõe produzir-se isoladamente;
- conseqüências são todas as seqüências lógicas associadas à ocorrência de um evento; elas compreendem assim os efeitos do evento quando ele ocorre, por exemplo, ao mesmo tempo que outro evento; em certa medida, pode-se falar de conseqüências menores, significativas, críticas, catastróficas.

TABELA E.1: CLASSIFICAÇÃO DAS FALHAS EM FUNÇÃO DOS EFEITOS

FALHA MENOR	falha que perturba o bom funcionamento de um sistema, causando um dano desprezível ao dito sistema ou a seu ambiente, sem apresentar riscos a vida humana
FALHA SIGNIFICATIVA	falha que perturba o bom funcionamento de um sistema, sem causar danos notáveis, nem apresentar riscos importantes para a vida humana
FALHA CRÍTICA	falha que implica na interrupção de uma ou mais funções essenciais de um sistema e causa danos sérios ao dito sistema ou a seu ambiente, apresentando entretanto pequenos riscos de morte ou de injúrias graves
FALHA CATASTRÓFICA	falha que ocasiona a perda de uma ou mais funções essenciais de um sistema, causando danos graves ao dito sistema ou a seu ambiente e/ou implica em morte ou injúrias graves

f) quanto às causas:

A falha de uma entidade resulta de causas, que são definidas como “circunstâncias ligadas a concepção, fabricação ou ao emprego e que implicam em falha”.

As causas têm por conseqüência a falha por intermédio de um modo de falha, definido como todo "processo físico, químico, ou outro que implique numa falha".

As falhas podem então ser classificadas em três categorias segundo suas causas:

- Falha primária: falha de uma entidade cuja causa direta ou indireta não está associada a uma outra entidade; geralmente um reparo da entidade é necessário para recolocá-la em funcionamento; se considerarmos um componente, a causa será interna, ou seja em um item; ela pode ser devida a problemas de desgaste, defeitos de projeto ou de fabricação, defeitos de especificação técnica de operação. Por exemplo, uma

tubulação que, em seguida à pressurização numa pressão inferior àquela de dimensionamento, se rompe;

- Falha secundária: falha de uma entidade cuja causa direta ou indireta é a falha de uma outra entidade que resulta condições para as quais aquela entidade não foi qualificada e dimensionada. Geralmente um reparo da entidade é necessário para recolocá-la em funcionamento. Falhas de outras entidades, condições ambientais particulares, erros humanos podem originar as falhas secundárias. Por exemplo, uma tubulação que se rompe após ser pressurizada a uma pressão superior àquela de dimensionamento, sendo esta sobre-pressão resultante da falha de outro componente;
- Falha de comando: falha de uma entidade cuja causa direta ou indireta é a falha de uma outra entidade para a qual esta entidade foi qualificada e dimensionada; geralmente não é necessário o reparo para que a entidade volte a seu estado de funcionamento; uma tal falha ocorre quando uma entidade muda de estado como efeito de um sinal de controle intempestivo (fechamento inadvertido de uma válvula, por exemplo)

A Tabela E.2 representa estas três categorias de falhas. Uma tal classificação deve ser considerada como um guia para o analista. Será visto que ela será muito útil para aplicação do método das árvores de causas.

TABELA E.2: CLASSIFICAÇÃO DAS FALHAS EM FUNÇÃO DAS CAUSAS

"Envelhecimento"	Respeito ao Dimensionamento	Falha Primária
Projeto	Erros Humanos	
Fabricação		
Instalação		
Erros Humanos de Operação	Condições e carregamentos excessivos	Falha Secundária
Ambiente		
Outros Componentes		
Outros Componentes	Sinais incorretos de comando e controle	Falha de Comando
Ambiente		
Erros Humanos de Operação		

Um conceito muito próximo ao de falha é o conceito de pane: "incapacidade de uma entidade cumprir uma função requerida". Após uma entidade sofrer uma falha, diz-se que ela encontrE-se em pane, ou seja, uma pane resulta sempre de uma falha. Evidentemente, as panes podem ser classificadas de modo similar às falhas. Entretanto, existe uma classificação especial das panes em função das possibilidades de sua constatação:

- a) pane intermitente: pane de uma entidade que ocorre durante um intervalo de tempo limitado, após o qual a entidade volta a cumprir as funções requeridas, sem ter sido submetida a uma operação de manutenção corretiva;
- b) pane fugidia: pane de uma entidade que é intermitente e dificilmente constatável;
- c) pane permanente: pane de uma entidade que persiste até que seja feita uma operação de manutenção corretiva;
- d) pane latente: pane que existe mas que não foi ainda constatada; diz-se também "pane escondida";

E.5 RELAÇÕES ENTRE DEFEITO, FALHA E PANE

Defeito é todo desvio entre uma característica de uma entidade e a característica requerida, desvio este que ultrapassa os limites de aceitabilidade, dentro de condições dadas. Assim , um defeito é definido como uma não-conformidade aos objetivos ou às especificações.

Entretanto, nem todo defeito conduz a uma falha: um defeito constatado ao nível do sistema ou de um componente do sistema pode perfeitamente não afetar a capacidade do sistema cumprir uma função requerida.

Inversamente, toda falha conduz a um estado de pane, que por sua vez caracteriza um defeito, pois a interrupção da capacidade da entidade a cumprir sua função está indiscutivelmente ligada a um desvio. Uma falha deve então ser caracterizada pelos seus efeitos imediatos e a pane pelo estado da entidade a mais longo termo. A Figura E.5 ilustra as relações entre defeito, falha e pane.

E.6 MODOS DE FALHA

Tendo definido os conceitos de falha e causa de falha, torna-se importante definir o conceito de modo de falha: "um modo de falha é o efeito pelo qual uma falha é observada".

Assim, a cada falha de uma entidade, associa-se modos e causas: os modos são gerados pelas causas, um modo representando o efeito ou efeitos pelos quais se manifesta a causa. A Figura E.6 ilustra as estreitas ligações e as interações que existem entre estes conceitos.

FIGURA E.5: RELAÇÕES ENTRE DEFEITO, FALHA E PANE

FIGURA E.6: CAUSAS, EFEITOS E MODOS DE FALHA

Esta figura ilustra igualmente a dificuldade que por certas vezes existe para diferenciar os modos e as causas de falhas. Para auxiliar nesta distinção, pode-se dizer que as causas de falhas de um componente são geralmente falhas de itens do componente. Os modos de falha são, por sua vez, a tradução dos efeitos destas falhas sobre as funções do componente.

Assim, todas as causas de falhas devem ser associadas a modos de falhas: se uma causa de falha não pode ser ligada a modos de falha, por exemplo, porque seus efeitos sobre as funções são diferentes daqueles considerados anteriormente, torna-se necessário elaborar um novo modo de falha.

Os conceitos de causas e de modos de falhas estão intimamente ligados aos níveis de decomposição do sistema: assim, por exemplo, os modos de falha de um componente de um sistema podem ser as causas de falha deste sistema, ou as causas de um modo de falha definido ao nível do sistema.

O modo de falha está estreitamente associado à modelagem adotada para os efeitos da falha. Ela depende igualmente das funções do componente dentro do sistema. Os modos de falha podem diferir, para um mesmo tipo de componente, segundo sua função dentro de diferentes sistemas. Assim, para uma bomba, uma vazão inferior à nominal será um modo de falha desta bomba dentro de um sistema particular, mas no caso de outro sistema poderá ser necessário considerar várias possibilidades de vazão inferior à nominal com vários modos de falha associados.

Os modos de falha podem ser classificados conforme sua propagação:

- a) Modo de Falha Independente: aquele de natureza estritamente aleatória, que ocorre individualmente a uma entidade, não sendo portanto resultante da propagação de modos de falha de outras entidades do mesmo sistema; e
- b) Modo de Falha Dependente: aquele cuja ocorrência está condicionada à ocorrência de modos de falha de outras entidades do sistema, caracterizando as correlações e a propagação entre falhas de múltiplos componentes.

Os modos de falha podem ser classificados conforme suas causas:

- a) Modo de Falha de Causa Simples: caracterizado como o efeito da ocorrência de um evento inicializador interno ou externo à entidade considerada, que afeta única e exclusivamente esta entidade;
- b) Modo de Falha de Causa Comum: caracterizado como efeito da ocorrência de um evento inicializador interno ou externo à entidade considerada, que afeta simultaneamente outras entidades componentes do sistema.

O tratamento dos modos de falha dependentes e de causa comum conduz a problemas de análise particularmente difíceis. Sua abordagem é no entanto incontornável, pois a maioria dos acidentes constatados, especialmente para sistemas complexos, na realidade prática se processam quase sempre segundo estes modos.

E.7 DEPENDÊNCIA ENTRE FALHAS

Falhas dependentes são aquelas que ocorrem de maneira simultânea ou concomitante sobre múltiplas entidades e que guardam entre elas relações de dependência. Este tipo de falha surge com a crescente complexidade dos sistemas industriais e as exigências sempre maiores de confiabilidade e segurança, que conduzem à redundância de componentes.

A redundância consiste na multiplicação dos componentes necessários ao sistema para que ele cumpra sua missão, permitindo assim superar uma ou várias falhas. Entretanto, as falhas que têm uma mesma origem (erros de projeto, por exemplo) podem afetar simultaneamente os componentes redundantes, comprometendo assim a eficácia da redundância.

Duas falhas E_1 e E_2 são dependentes se e somente se:

$$P[E_1.E_2]=P[E_1]*P[E_2 | E_1] \neq P[E_1]*P[E_2] \quad [A.1]$$

Em outros termos, a probabilidade do evento $E_1.E_2$ não pode ser expressa simplesmente como o produto das probabilidades dos eventos E_1 e E_2 . De maneira geral, considerando-se um conjunto de falhas $E_1, E_2, \dots, E_n$, se estas falhas são dependentes:

$$P[E_1.E_2. \dots .E_i. \dots .E_n]= \\ P[E_1]*P[E_2 | E_1]* \dots P[E_i | E_1.E_2. \dots .E_{i-1}]* \dots *P[E_n | E_1.E_2. \dots .E_{n-1}] \quad [A.2]$$

Assim, a probabilidade de cada falha sucessiva depende das falhas que a precedem na seqüência. Demonstra-se que a probabilidade de falhas dependentes é maior que o produto das probabilidades destas falhas supostas independentes.

A definição de falha dependente requer alguns comentários:

- a) nível de ocorrência das falhas: elas afetam múltiplas entidades (itens, componentes, subsistemas, sistemas elementares); os componentes podem pertencer a um mesmo sistema elementar ou a sistemas elementares diferentes; considera-se também as falhas dependentes do sistema "operador humano";
- b) simultaneidade e concomitância: as falhas surgem de maneira simultânea, ou seja, no mesmo momento, ou de maneira concomitante, ou seja, numa seqüência que se desenrola dentro de um determinado intervalo de tempo; se este intervalo é muito grande, elas podem ser confundidas com múltiplas falhas independentes;
- c) relações de dependência: elas traduzem as ligações físicas, funcionais, humanas ou de outra natureza que estabelecem uma relação de causa-efeito determinista entre as falhas.

As falhas dependentes podem ser classificadas em três categorias:

- a) eventos inicializadores que provocam causa comum de falhas: compreendem eventos internos e externos ao sistema que potencialmente podem originar um acidente devido a indução de múltiplas falhas de sistemas elementares; estes eventos tem geralmente graves conseqüências sobre a instalação, seus componentes e suas estruturas; cite-se como exemplo os incêndios, inundações, sismos, quedas de aeronaves, para eventos externos, e perda de alimentação elétrica ou de um sistema elementar importante, para eventos internos;
- b) dependência entre sistemas elementares: são eventos ou causas de falhas que criam dependência entre eventos indesejados de numerosos sistemas elementares; pode-se distinguir vários tipos destas dependências:
 - dependências funcionais, que resultam do projeto da instalação;
 - dependências ligadas a equipamentos comuns, por exemplo alimentações em energia (elétrica, hidráulica, pneumática);

- interações físicas, quando a falha de um componente irá afetar os componentes que lhe são próximos (explosões, incêndios, emissão de projetis, efeitos dinâmicos de ruptura de tubulações);
 - dependências ligadas às ações humanas, que resultam da intervenção do homem em todas as fases da vida dos sistemas elementares (projeto, fabricação, montagem, operação, manutenção);
- c) dependências entre componentes: similares às anteriores, entretanto afetando componentes de um mesmo sistema elementar.

E.8 FALHAS DE CAUSA COMUM E EM CASCATA

Falhas por causa comum são aquelas falhas dependentes que têm por origem a mesma causa direta. Constituem portanto um subconjunto das falhas dependentes.

Como “mesma causa” pode-se identificar, dentre outras:

- a) evento ligado ao ambiente;
- b) erro humano durante as diferentes fases da vida dos componentes;
- c) erro humano em operação; e
- d) falha de um outro componente.

Esta causa não é necessariamente única, podendo resultar de uma combinação de eventos.

O conceito de “causa direta” é importante, pois permite diferenciar as falhas de causa comum e as falhas em cascata. Seja um evento E implicando falhas simultâneas dos componentes A e B, a falha de A implicando por sua vez na falha de C. As falhas A, B e C são dependentes porém não são de causa comum, pois o evento E causa indiretamente a falha C. Somente as falhas A e B são efetivamente de causa comum. Evidentemente, este conceito está associado a uma definição prévia dos diferentes sistemas elementares (e seus componentes) a serem analisados.

Falhas de modo comum são falhas de causa comum que se manifestam pelo mesmo modo de falha dos componentes. Estas falhas representam um subconjunto das falhas de

causa comum. Concerne a componentes que devem ser ‘a priori’ idênticos ou muito semelhantes para poderem desenvolver o mesmo modo de falha.

Falhas em cascata de ordem n são falhas dependentes que podem ser classificadas em ordem cronológica $A_1, \dots, A_i, \dots, A_n$, tal que cada falha A_i ($i \neq n$) seja a causa direta da falha seguinte A_{i+1} .

Quando estas falhas afetam n componentes, fala-se em falhas em cascata de ordem n . As falhas de causa comum e as falhas em cascata se excluem mutuamente.

As falhas de causa comum e em cascata se relacionam com os conceitos de falha primeira, segunda e de comando, apresentados anteriormente.

E.9 CLASSIFICAÇÃO DAS FALHAS DE CAUSA COMUM

Pode-se identificar cinco classes de falhas de causa comum segundo a natureza de sua causa:

- a) Agressões do ambiente: eventos ligados ao ambiente externo do sistema ou interno ao sistema porém externo ao sistema elementar considerado:
 - ambiente normal de origem interna ou externa ao sistema (poeira, salinidade, umidade, temperatura, vibrações, atmosfera agressiva, radiação);
 - ambiente natural extremo (condições meteorológicas extremas, sismos, inundações);
 - ambiente acidental de origem interna ao sistema (condições ambientais decorrentes de um acidente, chicoteamento de tubulações, projetis, inundação local, incêndio local, explosão local);
 - ambiente acidental de origem externa ao sistema (queda de aeronaves, inundação por rompimento de represas, explosão em instalações vizinhas, incêndio em instalações vizinhas, acidentes de transporte rodo-ferroviário próximos, sabotagem);
- b) erros de projeto: erros humanos ocorridos durante o projeto de componentes e de sistemas elementares, que comprometem a missão do sistema:
 - inadaptação funcional de componente (erros de dimensionamento);
 - relações funcionais de um sistema elementar apresentando falhas de causa comum potenciais;

- testes periódicos inadequados ou prejudiciais;
 - sistema ou componente de operação difícil;
 - sistema ou componente de manutenção difícil;
- c) erros de fabricação: erros humanos cometidos durante a fabricação de componentes:
- não-conformidade às especificações técnicas de fabricação;
 - inadequação da tecnologia adotada;
- d) erros de montagem: erros humanos cometidos durante a montagem eletro-mecânica dos componentes, na fábrica ou no campo, e durante os testes de comissionamento;
- e) erros de operação: erros humanos cometidos durante inspeções e testes periódicos, ações de manutenção e operação normal, incidental ou acidental do sistema, afetando componentes ou sistemas elementares reconhecidos previamente como aptos ao funcionamento.

E.10 ANÁLISE DOS MODOS DE FALHA

Seja um sistema S cuja missão, que necessita seu funcionamento nominal entre os instantes t_0 e t_1 é representada pela Figura E.7.

FIGURA E.7: FALHA EM AVANÇO E FALHA EM ATRASO

Quatro modos de falha genéricos são considerados na análises por métodos estáticos do tipo AMFE:

- a) funcionamento intempestivo ou falha em avanço, que corresponde à partida e ao funcionamento de S antes de t_0 ;
- b) indisponibilidade na partida, que corresponde ao não funcionamento de S em t_0 ;
- c) parada prematura ou falha em atraso ou ainda não funcionamento intempestivo de S antes de t_1 ; e
- d) falha na parada, que corresponde ao funcionamento de S após t_1 .

A estes modos de falha genéricos juntam-se ainda os modos de falha derivados de variações inaceitáveis dos parâmetros de funcionamento de S entre t_0 e t_1 .

Na prática, considerE-se geralmente:

- a) falha em avanço;
- b) falha em atraso, em geral ligada à indisponibilidade no momento de partida.

A ação do projetista é então introduzir redundâncias que respondem ao objetivo de segurança com respeito à falha em avanço e à falha em atraso.

A estes modos de falha intrínsecos e a cada um dos elementos em redundância, é necessário juntar-se o modo de falha em causa comum, que implica, sob determinadas circunstâncias, na ineficácia simultânea das redundâncias.

E.11 FALHA EM ATRASO E FALHA EM AVANÇO DE ELEMENTOS EM REDUNDÂNCIA TOTAL

Seja o esquema funcional de S apresentado pela Figura E.8, onde os elementos A e B são ‘a priori’ independentes e ligados em série.

FIGURA E.8: ESQUEMA FUNCIONAL

Os diagramas de confiabilidade de S para falha em atraso e para falha em avanço são apresentados respectivamente pelas Figuras E.9 e E.10.

FIGURA E.9: FALHA EM ATRASO

FIGURA E.10: FALHA EM AVANÇO

Para que S sofra uma falha em atraso S_{at} , é necessário que A ou B sofram falha em atraso, ou seja, aplicando diretamente a fórmula de Poincaré:

$$S_{at} = A_{at} \cup B_{at} \quad [E-3]$$

$$P(S_{at})=P(A_{at} \cup B_{at})=1-(1-P(A_{at}))(1-P(B_{at})) \quad [E-4]$$

Para que S sofra uma falha em avanço S_{av} , é necessário que A e B sofram falha em avanço, ou seja, aplicando diretamente a fórmula de Poincaré:

$$S_{av} = A_{av} \cap B_{av} \quad [E-5]$$

$$P(S_{av})=P(A_{av} \cap B_{av})=1-(1-P(A_{av}))(1-P(B_{av})) \quad [E-6]$$

O diagrama de confiabilidade para falha em atraso tem sempre a mesma forma do esquema funcional. O diagrama de confiabilidade para falha em avanço tem sempre a forma do esquema funcional dual.

A Tabela E.3 apresenta as expressões de falha em atraso e falha em avanço para sistemas com redundâncias simples de elementos idênticos.

TABELA E.3: EXPRESSÕES PARA FALHA EM AVANÇO E FALHA EM ATRASO
DE REDUNDÂNCIAS SIMPLES

TIPO	FALHA EM AVANÇO	FALHA EM ATRASO
elemento simples	P_{av}	P_{at}
paralelo	$P_{av}(2-P_{av})$	P_{at}^2
série	P_{av}^2	$P_{at}(2-P_{at})$
série/paralelo	$P_{av}^2(2-P_{av}^2)$	$P_{at}^2(2-P_{at})^2$

paralelo/série	$P_{av}^2(2 - P_{av})^2$	$P_{at}^2(2 - P_{at})^2$
série/meio paralelo	$P_{av}^2(2 - P_{av})$	$P_{at}(1 + P_{at} - P_{at}^2)$
paralelo/meio série	$P_{av}(1 + P_{av} - P_{av}^2)$	$P_{at}^2(2 - P_{at})$

A Figura E.11 representa as posições relativas das probabilidades de falha em avanço e falha em atrasos para estes tipos de redundâncias.

FIGURA E.11: COMPARAÇÃO DE PROBABILIDADES PARA FALHA EM AVANÇO E FALHA EM ATRASO DE REDUNDÂNCIAS SIMPLES

E.12 FALHA EM ATRASO DE ELEMENTOS EM REDUNDÂNCIA PARCIAL

Um sistema em redundância parcial (k/n) é formado por n elementos e sofre uma falha se pelo menos um número k de elementos falham ($k < n$). Para resolver este caso utilizE-se a lei binomial.

A probabilidade de que pelo menos k elementos falhem é dada por:

$$P(S) = P(K \geq k, n) = \sum_{i=k, n}^n \binom{n}{i} p^i (1-p)^{n-i} \quad [E-7]$$

$$\binom{n}{i} = \frac{n!}{i!(n-i)!} \quad [E-8]$$

K = número de elementos em falha

p = probabilidade de falha de um elemento

A confiabilidade é expressa pela relação:

$$R(t)=P(S)=P(K \leq k-1, n) = \sum_{i=0, k-1}^n \binom{n}{i} p^i (1-p)^{n-i} \quad [E-9]$$

Por exemplo, para n=4 e k=3 (redundância 3/4), teremos:

$$P(S)=4p^3(1-p)+p^4 \quad [E-10]$$

E.13 MODOS DE FALHA DE CAUSA COMUM

Independentemente da falha aleatória e individual dos elementos de uma redundância, deve ser considerado no projeto o tipo de elemento redundante, a origem das entradas no elemento (alimentação em energia, sinais de controle e comando) e sua implantação física no sistema:

- a) no primeiro caso, erros de projeto, fabricação ou manutenção de elementos idênticos podem provocar modos de falha simultâneos por causa comum;
- b) no segundo caso, falhas externas aos elementos, tais como perda de fontes de alimentação, podem provocar a indisponibilidade simultânea dos elementos; e
- c) no terceiro caso, uma agressão externa pode atingir simultaneamente ou propagar-se pelos elementos, caso não haja uma segregação física adequada.

Estes aspectos, se não forem devidamente verificados podem comprometer a eficácia das redundâncias.

Deve-se então diferenciar, na avaliação da confiabilidade de um sistema redundante:

- a) taxa de falha independente, individual de cada um dos elementos, notada como λ_i que integra as taxas de falha em avanço e em atraso; e
- b) taxa de falha de causa comum λ_c .

Sendo os dois tipos de falhas incompatíveis por definição pode-se definir para a taxa de falha global λ de cada elemento e a parte β devido as falhas de modo comum:

$$\lambda = \lambda_i + \lambda_c \quad [E-11]$$

$$\beta = \lambda_c / \lambda = \lambda_c / (\lambda_i + \lambda_c) \quad [E-12]$$

$$\lambda_i = (1 - \beta) \lambda \quad [E-13]$$

$$\lambda_c = \beta \lambda \quad [E-14]$$

Sendo um sistema S com redundância total paralela dos elementos A e B, com $\lambda_i A = \lambda_i B = (1 - \lambda) \beta$ e $\lambda_c = \beta \lambda$, três possibilidades podem ser consideradas, para as quais pode-se calcular a probabilidade:

- a) dois elementos funcionam - esta hipótese corresponde ao cálculo clássico da taxa de falha de uma redundância total em paralelo:

$$P(S_0) = P(A \cap B) = (1 - \lambda)(1 - \lambda) = (1 - \lambda)^2 = 1 - 2\lambda + \lambda^2 \quad [E-15]$$

$$\text{se } \lambda \text{ é pequeno, } (1 - \lambda)^2 \approx 1 - 2\lambda \quad [E-16]$$

- b) um dos elementos funciona: esta hipótese corresponde ao caso onde A falha ($\bar{A}$) e B funciona, ou B falha ($\bar{B}$) e A funciona; isto implica que não existe falha em modo de causa comum:

$$P(S_1) = P(\bar{A}, B) \cup P(A, \bar{B}) = P(\bar{A} \cap B) + P(A \cap \bar{B}) = P(B) * P(\bar{A} | B) + P(A) * P(\bar{B} | A) \quad [E-17]$$

$$\text{sendo A e B independentes, } P(\bar{A} | B) = P(\bar{A}) \text{ e } P(\bar{B} | A) = P(\bar{B}) \quad [E-18]$$

$$P(S_1) = 2(1 - \lambda)(1 - \beta)\lambda \quad [E-19]$$

- c) dois elementos falham - esta hipótese subentende que A e B sofrem falha independente (I) ou A e B sofrem falha de causa comum (C):

$$P(S_2) = P(\bar{A} \cap \bar{B})_I + P(\bar{A} \cap \bar{B})_C = \lambda\beta + (1 - \beta)^2 \lambda^2 \quad [E-20]$$

ANEXO F

PROBABILIDADES EM SEGURANÇA DE SISTEMAS

As probabilidades são um dos meios de medir uma situação perigosa podendo conduzir à ocorrência de um ou vários eventos indesejáveis. Entretanto, o conceito e a utilização das probabilidades em seguridade podem parecer muito distantes da teoria das probabilidades tal como definida axiomáticamente.

F.1 UTILIZAÇÃO DAS PROBABILIDADES

A partir de um conjunto mensurável Ω dos eventos elementares, chamado conjunto das eventualidades, do possível ou fundamental, forma-se o conjunto das partes de Ω , que nota-se como A , utilizando-se a união e a complementação como leis de composição interna, para as quais A deve ser estável (fechado) para todas as uniões enumeráveis de eventos.

Do ponto de vista dos eventos, o conjunto A compreende:

- Ω , evento certo;
- $\emptyset$, evento impossível; e
- todos os eventos aleatórios formados a partir dos eventos elementares de Ω e a partir das leis de composição interna.

Uma probabilidade é uma aplicação de A sobre o intervalo $[0; 1]$ que satisfaz aos três axiomas seguintes:

- a) $1 \geq P(A) \geq 0$ para todo $A \in A$ e $P(\Omega) = 1$
- b) para toda família finita $\{A_i, i \in I\}$ de eventos disjuntos 2 a 2, tem-se que:

$$P(\cup_i A_i) = \sum P(A_i) \text{ (aditividade)}$$

- c) para toda seqüência $\{A_n, n \geq 1\}$ de eventos decrescentes em direção a $\emptyset$, isto é

$$A_1 \supset A_2 \supset A_3 \dots, \text{ e que } \cap_i A_n = \emptyset \text{ tem-se que:}$$

$$\lim_{n \rightarrow \infty} P(A_i) = 0 \text{ (continuidade monótona seqüencial em } \emptyset)$$

Uma variável aleatória é então uma aplicação de Ω em $\mathcal{R}$, conjunto dos números reais.

A avaliação formal de uma probabilidade sobre A requer inicialmente o conhecimento perfeito do conjunto do possível Ω e a identificação completa dos eventos de A .

A busca deste conhecimento é simplificada quando Ω é definido por um número finito de valores (por exemplo, o número de faces de um dado). Ela pode se limitar a uma descrição global do conjunto do possível, como é o caso de um ensaio podendo levar a um número indefinido de valores (por exemplo, a altura de uma onda).

Em segurança de sistemas, o conjunto Ω corresponde à integralidade dos estados de funcionamento e de pane (não funcionamento e mal funcionamento) do sistema, aos quais são associadas suas conseqüências dentro de todos os ambientes para os quais sua missão é (ou será) realizada.

Para sistemas complexos ou ambientes mal ou incompletamente conhecidos, o conhecimento exaustivo de Ω_S é inviável. O mesmo pode-se afirmar, em particular, para o conjunto das combinações de causas internas (ou externas) de falhas que conduzam a um dano grave. Entretanto, uma partição *a priori* de A_S em classe de estados do sistema S durante ou após funcionamento pode ser realizada em função de uma escala de gravidade de conseqüências, tal como definido anteriormente.

Pode-se definir dois domínios relativos ao funcionamento de um sistema:

- a) Domínio de Conhecimento, dentro do qual é possível descrever precisamente todos os estados de funcionamento e de pane e suas conseqüências sobre o ambiente dentro do qual ele evolui; o mesmo se aplica aos carregamentos e imposições do ambiente sobre o sistema;
- b) Domínio de Desconhecimento (ou Ignorância) sobre os estados de funcionamento do sistema ou sobre seu ambiente.

Se dentro do Domínio de Conhecimento pode-se esperar avaliar com mais ou menos precisão a probabilidade de um modo de falha de S ou de uma de suas conseqüências, não se deve ter a pretensão de estimar a probabilidade de um evento não ou mal definido qualitativamente. Em outras palavras, é absurdo probabilizar o desconhecido.

O Domínio de Conhecimento pode ser estruturado em duas zonas complementares, visualizadas pela Figura F.1:

- a) Zona de Incerteza;

b) Zona de Certeza.

FIGURA F.1: DOMÍNIOS DE FUNCIONAMENTO DE UM SISTEMA

A Zona de Incerteza é aquela que corresponde a um conhecimento qualitativo dos estados do sistema associado a um conhecimento aleatório de cada um deles para uma situação determinada. É, por exemplo, o estado de um veículo (perfeitamente identificado) após 50.000 km e, mais precisamente, sua probabilidade de atingir, ‘a priori’, 50.000 km. A incerteza pode ser associada à imprecisão sobre um dos estados de um sistema, definido por grandezas, associando a ela uma densidade de probabilidade. Seu conhecimento permite caracterizar desvios em torno de uma média. Esta abordagem é uma das bases da lógica imprecisa (*fuzzy logic*).

A Zona de Certeza corresponde a um conhecimento determinista de todos os estados do sistema e de suas conseqüências. De uma maneira geral, este conhecimento pode ser de dois tipos:

- a) Conhecimento Teórico, que se exprime por meio de leis físicas infinitamente reprodutíveis e inúmeras vezes validadas pela experiência (leis de Newton, por exemplo); este tipo de conhecimento pode ser chamado de determinismo teórico; note-se que este determinismo pode ser expresso sob a forma de leis probabilísticas, como em física quântica;
- b) Conhecimento Estatístico, que se exprime por valores estatísticos deduzidos de observações, tais como o valor médio da altura de ondas numa determinada região

marítima; este determinismo estatístico só é verificado numa média de grande número de observações, não podendo ser aplicado individualmente a cada elemento observado.

As decisões técnicas na prática fazem intervir os duas zonas do Domínio de Conhecimento: por exemplo, o momento do lançamento de um satélite será definido indiretamente pela escolha do local de lançamento, que terá privilegiado um sítio meteorologicamente favorável (Zona de Certeza Estatística), e diretamente pelas condições meteorológicas imediatas sobre o local de lançamento (Zona de Incerteza).

A tomada de decisões no Domínio da Incerteza faz-se aplicando o Princípio da Certeza Prática, relativo à consideração de eventos quase impossíveis. Ele é enunciado como se segue:

"Se a probabilidade de um evento E qualquer numa experiência dada é suficientemente pequena, pode-se estar quase certo que quando esta experiência é realizada uma só vez, o evento E não ocorrerá."

Este princípio adapta-se da mesma maneira às probabilidades quase unitárias, correspondendo aos eventos certos.

É evidente que este "princípio" não pode ser demonstrado matematicamente, mas é confirmado pela experiência cotidiana, que formaliza a experiência pessoal (subjettiva) aos conceitos de certo e impossível. É a partir deste princípio que a quase totalidade das decisões da vida quotidiana são tomadas. Ele faz com que sejam ignorados eventos de probabilidade próxima de zero, considerados *a priori* como impossíveis (choque de um grande meteoro com a Terra) ou de probabilidade próxima de um, considerados *a priori* como certos (amanhecer seguindo-se à noite).

Cumpra entretanto ressaltar que a quase certeza ou quase impossibilidade de ocorrência de um evento baseada simples na experiência deve ser tratada com extrema cautela no contexto das análise de segurança. Com efeito, a duração real ou prática de observação pode ser várias ordens de grandeza inferior àquela que seria necessária para observar o evento indesejável considerado dentro dos objetivos de segurança. Por

consequente, este evento não deve ser *a priori* excluído da análise por ser julgado impossível exclusivamente pela justificativa de que ele nunca foi observado.

Por exemplo, a observação de 50 anos de funcionamento sem acidente de uma instalação industrial não pode razoavelmente satisfazer a um objetivo de acidente grave de 10^{-7} /ano, porque o período de retorno deste último é de 10.000.000 anos. A probabilidade de observar um tal acidente durante os 50 anos é de 5×10^{-6} , o que o torna altamente improvável. O mesmo pode-se dizer de riscos naturais, onde a implantação de residências em locais de risco em geral somente levam em consideração as observações da geração em curso, ainda que relatos históricos indiquem ocorrência de fenômenos acidentais graves, tais como inundações, terremotos.

Em resumo, pode-se enfatizar que a proximidade de um evento não é refletida por sua probabilidade de ocorrência.

O princípio da certeza prática é um corolário da lei dos grandes números, que consiste em afirmar que:

"Durante uma experiência, quando o número de ensaios aumenta indefinidamente, a frequência observada de um evento dado considerado como resultado possível tende a um limite que é igual à sua probabilidade"

Dentro do princípio da certeza prática, esta probabilidade é muito próxima de 0 ou 1. É a grande repetição de observações de um evento dado que leva à experiência e à confiança posterior que decorre da tomada de decisão. O princípio da maximização da entropia permite tirar de um conjunto de observações relativas ao funcionamento de um sistema toda a informação que ele contém, com o objetivo de poder orientar as decisões concernentes.

As regulamentações e os procedimentos diversos têm por objetivo eliminar todo caráter aleatório no projeto, implantação e operação de um sistema. O respeito a estas regulamentações e procedimentos permitem associar às opções e ações consequências quase deterministas que pertencem portanto à Zona de Certeza, permitindo a aplicação do princípio da certeza prática. Um dos instrumentos desta ação é a Garantia da Qualidade.

Por exemplo, o projeto e construção de um vaso de pressão a partir de um código consagrado (ASME, por exemplo) é ditada pela necessidade de eliminar os elementos dos quais uma das características pertence aos extremos da distribuição de probabilidade de um parâmetro mal conhecido, e por isto mesmo com valor incerto.

Pela força do hábito de repetidos êxitos, a diminuição da vigilância pode levar um dos estados de funcionamento do sistema para a zona de incerteza, isto é, onde as causas de falhas são de natureza aleatória, e portanto mal controladas. Compreende-se bem então que a segurança de um sistema complexo ou mais simplesmente seu bom funcionamento não pode ser garantido dentro de uma zona de certeza cujos limites foram estabelecidos através somente do retorno da experiência, e portanto dos erros feitos e corrigidos do passado (mas também, obviamente, dos acertos).

A uma pequena probabilidade pode-se associar o conceito de evento raro, definido como:

"Um evento raro, no sentido da segurança de sistemas, é um evento podendo conduzir a conseqüências graves ao qual as decisões que são tomadas devem permitir assinalar-lhe uma probabilidade muito pequena"

Um conceito que se evitou utilizar até este ponto foi o de acaso, que resume classicamente a soma de nossos desconhecimentos. Uma definição literária, porém bastante significativa de acaso é dada pelo escritor brasileiro Millor Fernandes:

"Acaso é a desculpa que nossa vaidade dá à nossa ignorância".

O desconhecimento, e portanto o acaso, pode ser de duas naturezas:

- a) falta de conhecimento sobre a própria natureza de um perigo; e
- b) falta de conhecimento sobre o processo e o instante de realização de um cenário de riscos, ainda que conhecendo a fonte do perigo de onde ele decorre.

Pode-se então concluir que o domínio que cobre o conceito de acaso agrupa o Domínio de Desconhecimento e a Zona de Incerteza do Domínio do Conhecimento.

A partir deste fato, compreende-se bem que a introdução da linguagem probabilística na segurança de sistemas é uma tentativa de controlar a incerteza através de uma medida de

hierarquização das ocorrências de cenários de acidentes (causas e efeitos), esta medida só pode ser feita sobre elementos perfeitamente descritos e portanto conhecidos. Isto exclui de fato o lado “ignorância” do acaso, e por isto mesmo seu controle. Assim se justifica a eliminação da palavra acaso em segurança de sistemas.

F.2 DIFERENTES DEFINIÇÕES DE PROBABILIDADES

Existem essencialmente quatro maneiras de definir probabilidade:

A definição clássica corresponde àquela definição mais corrente que poderíamos chamar "instintiva": se num experimento identifica-se N alternativas possíveis de realização e N_A alternativas que interessam ao experimentados, então

$$P(A) = N_A / N \quad [F-1]$$

A definição axiomática é aquela baseada na Teoria da Medida de Kolmogoroff, que utiliza-se somente de conceitos matemáticos abstratos, não associando a probabilidade a nenhuma propriedade dos sistemas físicos. Esta é a definição formal, apresentada pela Teoria das Probabilidades.

Uma aplicação da definição axiomática é a medida contável, feita através da contagem de objetos particulares contidos em um conjunto de objetos observados e da razão entre os tamanhos dos dois conjuntos. As proporções assim calculadas podem ser consideradas *a priori* como probabilidades, dado que verificam os axiomas de base. Uma tal contagem pode ser feita numa linha de fabricação, sendo o número k de elementos defeituosos observados sobre uma série de n . A proporção k/n permitindo calcular os elementos defeituoso na fabricação da série considerada.

Associa-se geralmente a este tipo de medida uma parte da estatística denominada estatística descritiva, ou exploratória. Esta última terminologia corresponde ao fato dela servir de base ao conhecimento do funcionamento de um sistema. Dentro desta ótica, a medida contável é um dos elementos do retorno da experiência (diagrama de Pareto, por exemplo).

A definição de Frequência Relativa é aquela mais utilizada em engenharia e física, tendo sido formalizada por Von Mises: se um experimento é repetido n vezes, então a probabilidade $P(A)$ é definida como o limite da frequência relativa n_A / n quando n tende a infinito

$$P(A) = \lim_{n \rightarrow \infty} (n_A / n) \quad [F-2]$$

A frequência é uma contagem direta (número inteiro. Deve-se ter os cuidados necessários para definir de modo preciso o conjunto fundamental. Assim, a observação de três eventos por ano não pode se traduzir diretamente por uma probabilidade, guardando-se o ano como escala de tempo. Por outro lado, uma frequência de três observações em 365 dias pode ser considerada como uma medida contável, e portanto uma probabilidade, se as observações forem consideradas numa base diária, tendo-se entretanto o cuidado de verificar previamente que a duração do evento é *a priori* inferior a um dia.

Considerando-se o exemplo anterior sobre o controle de fabricação, a proporção k/n só poderá ser tomado como um estimador da proporção de elementos defeituosos se as condições de fabricação não evoluem no tempo.

A busca de uma probabilidade a partir de uma frequência constitui uma outra parte da estatística chamada estatística inferencial, cujo objetivo é a dedução, a partir de uma amostra, das propriedades da população de onde é proveniente. Conseqüentemente, ele cobre a determinação dos parâmetros das leis de probabilidade a partir de amostras de observações, assim como os intervalos de confiança que a elas são associados com respeito a um limite de risco estatístico definido *a priori*.

A definição de probabilidade como verossimilhança, também chamada probabilidade subjetiva, é uma medida da confiança que pode ser dada a uma proposição incerta. Esta definição não tem nenhuma relação com as anteriores, pois ela não é deduzida de observações diretas que permitam uma efetiva medida.

O desenvolvimento da teoria da decisão na incerteza deu origem ao conceito de probabilidade como verossimilhança, aplicável aos fatos que podem estar fora das possibilidades reais de experimentação (por exemplo, 10^{-7} /ano) ou mesmo da simples observação devido a impossibilidade espacial ou temporal.

Usando um exemplo de Morlat, os historiadores podem associar um peso à afirmação "Júlio César esteve na Inglaterra". O peso desta afirmação, normalizada entre 0 e 1,

corresponde à verossimilhança que cada historiador pode estimar, a partir de sua própria erudição e reflexão: é portanto uma medida do possível.

Deve-se notar que este peso é geralmente dado com relação a proposições complementares, e não com relação ao conjunto do possível. No exemplo anterior, o conjunto do possível é formado por dois eventos:

$$E_1 = \{\text{Júlio César esteve ...}\} ; e \\ E_2 = \{\text{Júlio César não esteve}\}.$$

A verossimilhança acordada a E_1 será então a medida contável dos historiadores tendo escolhido E_1 , que pode valer 0,8. De toda forma, a realidade é tal que $P(E_1) = 0$ ou $P(E_1) = 1$.

Pode-se então afirmar que a verossimilhança não é sempre uma medida direta da ocorrência de um evento estudado, mesmo que certos eventos que lhe são associados sejam mensuráveis. Existem técnicas para avaliação de especialistas, chamados métodos Delphi, para auxiliar a resolver estes tipos de problemas.

A probabilidade como medida de verossimilhança está associada à estatística decisória ou de decisão, cujo objetivo é, a partir da estruturação de do tratamento de dados, em parte subjetivos, otimizar uma decisão na presença de incerteza, e portanto de risco.

F.3 PERÍODO DE RETORNO DE UM EVENTO

Recorda-se inicialmente que:

- a) para que uma função f possa ser considerada como uma densidade de probabilidade de uma variável aleatória X , é necessário que seja verificada, sobre seu domínio de definição D , a igualdade seguinte:

$$\int_D f(x) dx = 1$$

- b) para $D=[a, b]$, a relação entre função densidade de probabilidade e função de distribuição acumulada (ou função repartição à não-ultrapassagem) é:

$$F(x) = \int_a^x f(x) dx$$

$$F(a) = 0 \text{ e } F(b) = 1$$

Por definição, um quantil x é uma das realizações de uma variável aleatória X . Mais precisamente, um quantil de ordem p , notado como x_p , é o quantil associado à probabilidade p de X não ultrapassar o valor x :

$$p = P(X < x_p) = F(x_p)$$

Deve-se ter especial atenção ao manipular este conceito pois certos autores associam a x_p a probabilidade de ultrapassagem $p = P(X > x)$.

FIGURA F.2: QUANTIL x_p DE UMA VARIÁVEL ALEATÓRIA X

O período de retorno (ou de recorrência) $T(E)$ de um evento E é o intervalo médio de tempo entre duas ocorrências ou duas observações de ultrapassagem de um quantil x_p de uma variável aleatória X . A partir da função de repartição $F(x)$ ou da densidade de probabilidade $f(x)$, o período de retorno é formalizado por:

$$T(E) = 1 / f(E) = 1 / (1 - F(x_p))$$

Os eventos podem ser pontuais (instantâneos) ou necessitar uma duração D de observação (hora, ... , ano) numa base de tempo contínua. Neste último caso, o período de retorno T será um múltiplo de D .

Isto significa que em média, observa-se uma realização de X maior que x_p a cada T unidades de tempo, o que não implica dizer que num período $\Delta t = T$ dado não ocorra nenhuma observação de $X > x_p$ ou que não possam ocorrer várias.

A noção de período de retorno integra a hipótese de que não existe mudança nos parâmetros da população a partir da qual são feitas as observações que permitem estimar $P(X)$, o que é praticamente impossível de ser demonstrado no caso de longos períodos de

recorrência (ou pequenas probabilidades, o que vem a ser o mesmo). Este conceito está muito ligado à definição de probabilidade como medida contável: seu uso dentro de contextos que se valem das outras definições de probabilidade deve ser cuidadoso, pois pode conduzir a conclusões carentes de sentido objetivo.

F.4 APROXIMAÇÕES E ERROS

A fórmula clássica de Poincaré define o algoritmo de cálculo da probabilidade da união de eventos quaisquer. Seja $S = \cup_{i=1,n} E_i$ a união dos n eventos E_i sobre os quais não é feita nenhuma hipótese, tem-se que:

$$P(S) = \sum_{i=1,n} P(E_i) - \sum_{\forall i,j} P(E_i \cap E_j) + \dots + (-1)^{n-1} P(\cap_{i=1,n} E_i) \quad [F-3]$$

Somente o conhecimento das probabilidades respectivas dos eventos E_i não é suficiente para calcular a probabilidade de sua união. Com efeito, é necessário calcular as probabilidades compostas, calculadas a partir das probabilidades condicionadas, que expressem o grau de dependência entre os eventos:

$$P(E_i \cap E_j) = P(E_i) \cdot P(E_j | E_i) = P(E_j) \cdot P(E_i | E_j) \quad [F-4]$$

Dois casos particulares da fórmula de Poincaré podem ser identificados, implicando em simplificações na sua forma:

- a) Eventos mutuamente excludentes (ou incompatíveis): quando a ocorrência de um deles implica na não ocorrência de todos os demais, isto é:

$$E_i \cap E_j = \emptyset \quad \forall i, j \quad [F-5] \quad \text{o que implica}$$

no desaparecimento das probabilidades compostas da fórmula, que se nota sob sua forma reduzida: $P(S) = \sum_i P(E_i)$ [F-6]

- b) Eventos independentes: quando a ocorrência de um não tem nenhuma influência sobre a ocorrência dos outros, isto é:

$$P(E_i | E_j) = P(E_i) \text{ e } P(E_j | E_i) = P(E_j) \quad [F-7] \quad \text{isto}$$

implica que as probabilidades compostas se decompõe em produto das probabilidades dos eventos considerados, a fórmula de Poincaré tornando-se:

$$P(S) = \sum_i P(E_i) - \sum_{i,j} P(E_i) \cdot P(E_j) + \dots + (-1)^{n-1} \prod_i P(E_i) \quad [F-8] \quad \text{que pode ser também}$$

ser expressa através das regras de Morgan para operações com conjuntos por

$$P(S) = 1 - \prod_i [1 - P(E_i)] \quad [F-9]$$

Em segurança de sistemas torna-se necessário analisar com cuidado os eventos do tipo $(B|A)$, que correspondem a uma falha de causa comum ou à propagação de falhas. No primeiro caso, um modo de falha de causa comum reduz a eficácia de redundâncias. No segundo caso, uma agressão ou falha particular implica na falha "em cascata" dos elementos redundantes ou dos elementos à jusante da cadeia funcional analisada.

É possível empregar a fórmula de Poincaré reduzida se as probabilidades elementares são pequenas e se o número de eventos considerados não é muito grande. Por exemplo, para n elementos idênticos de probabilidade p , a utilização da fórmula reduzida é aceitável se $np < 0,1$. Com efeito, para elementos independentes ou incompatíveis idênticos:

$$P(S) = 1 - (1-p)^n = 1 - e^{-np} \quad [F-10]$$

pois $1 - p = e^{-p}$ para $p < 0,1$

da mesma forma: $1 - e^{-np} = np$ para $np < 0,1$

donde: $P(S) = np$ para $np < 0,1$

Este resultado é imediato para n eventos incompatíveis idênticos.

Considerando um evento indesejado E relativo ao funcionamento de uma instalação cuja probabilidade de ocorrência é constante no tempo e igual a p , pode-se então calcular os seguintes eventos:

a) Ocorrência de E no n -ésimo ano: $p_n = (1 - p)^{n-1} \cdot p \quad [F-11]$

b) Ocorrência de E ao menos uma vez ao longo de n anos consecutivos:

$$P_n = 1 - (1 - p)^n \quad [F-12]$$

c) Ocorrência de E entre o ano m e o ano n : $P_{n-m} = P_n - P_m = (1 - p)^m - (1 - p)^n \quad [F-13]$

Ressalta-se o fato de que é falso afirmar que um evento cuja probabilidade anual é *a priori* igual a p se realizará com uma probabilidade igual a 1 (certeza) ao longo de $n = p^{-1}$ pois tem-se as seguintes aproximações possíveis para o cálculo de P_n :

a) para $p > 0,1$: não há aproximação possível da fórmula básica; por conseguinte, para $n = p^{-1}$ deve-se utilizar diretamente esta última: $P_n = 1 - (1 - p)^{1/p} \quad [F-14]$

b) para $p < 0,1$: a primeira aproximação da fórmula básica permite exprimir:

$$(1 - p) = e^{-p} \Rightarrow P_n \approx 1 - e^{-np} \quad [F-13] \text{ para } n = p^{-1}$$

pode-se calcular diretamente:

$$P_n = 1 - e^{-1} = 0,632$$

[F-14] note-se que

pela fórmula exata, para $p=0,1$ e $n=10$ obtêm-se 0,6513; esta aproximação tende a subestimar as probabilidades P_n ;

c) para $p<0,1$ e $np<0,1$: a segunda aproximação da fórmula de base (exata) permite exprimir:

$$e^{-np} = 1 - np \Rightarrow P_n = np$$

[F-15] neste

caso pode-se calcular P_n por $n = p^{-1}$ pois esta última aproximação só é válida para $np < 0,1$ e não para $np = 1$; esta aproximação tende a superestimar as probabilidades P_n .

F.5 REFLEXÕES SOBRE A FIXAÇÃO DE LIMITES MÍNIMOS DE PROBABILIDADE

Este item introduz um conjunto de reflexões sobre as probabilidades muito pequenas, associadas, com sem razão, a eventos "julgados" quase impossíveis. Estas probabilidades aparecem em diferentes etapas da análise de segurança:

- a) na definição e na demonstração de cumprimento de objetivos, onde probabilidades de natureza subjetiva são explicitamente associadas a eventos indesejados e às condições do ambiente do sistema a serem considerados como requisitos;
- b) na escolha dos cenários considerados *a priori* como podendo conduzir ao evento indesejado, julgados por um "decisor" como os mais plausíveis dentre o conjunto dos cenários identificados ou imaginados pelos analistas;
- c) na avaliação *a posteriori* da probabilidade destes cenários, que fazem aparecer valores quase desprezíveis para determinadas combinações de eventos.

Estas três etapas de análise e de avaliação correspondem a três etapas de decisão, cuja adequabilidade tem um impacto direto sobre o nível estimado de segurança do sistema. A questão que se coloca para estas três categorias de probabilidades pode ser formulada da seguinte maneira:

"A partir de que limite de probabilidade ou de inverossimilhança pode-se desprezar, nas análises de segurança, os eventos ou os cenários de eventos identificados, e portanto conhecidos, e em seguida ignorá-los nas decisões que poderiam levá-los em consideração ?"

Um objetivo de segurança probabilístico é definido por dois parâmetros:

- a) a descrição do evento indesejado, que pode ser descrito por um limite de dano;

b) a frequência ou a verossimilhança associada a este evento indesejado, em unidades coerentes com a sua descrição.

A fixação da probabilidade que figura no objetivo está ligada à gravidade das consequências do evento indesejado durante a atividade considerada. Segue-se então que a fixação da probabilidade tem por base a frequência observada de um evento natural ou tecnológico que tenha consequências similares.

A credibilidade da segurança de um sistema está diretamente ligada ao nível de segurança visado e demonstrado, que pode ser definido através de:

- a) a ambição do objetivo de segurança associando a um dano inaceitável uma probabilidade muito pequena, fora das possibilidades de observação;
- b) a confiança na demonstração do cumprimento do objetivo por meio de um conjunto de tarefas bem identificadas e claramente descritas pela análise de segurança.

Sendo sempre possível, de uma maneira mais ou menos simples, definir e emitir objetivos de segurança, garantir o nível de segurança atingido por técnicas probabilísticas, a partir dos dados disponíveis demonstra-se ser tarefa bem mais complexa. Com efeito, esta última atividade é baseada na confiança adquirida durante os estudos e ações empreendidas durante o projeto, desenvolvimento, fabricação, construção e montagem e operação de sistemas semelhantes atuais e anteriores.

Isto coloca o problema real da credibilidade dos objetivos de segurança demonstrada, que correspondem principalmente à eficácia das ações de segurança validadas por sua verificação experimental ao nível considerado (sistema elementar, subsistema, componente, item). Entretanto, esta validação pode ser materialmente impossível, ou inaceitável considerando os danos que dela resultariam. A impossibilidade material pode decorrer não só do número considerável de ensaios a serem realizados para permitir a observação do evento indesejável definido pelo objetivo mas também do fato que a validação esteja fora das possibilidades de experimentação, por exemplo, devido a escala de tempo considerada, que pode ser de vários séculos.

Dois exemplos ilustram as dificuldades de realizar uma experimentação de validação adaptada:

- a) a regulamentação do transporte aéreo associa a uma probabilidade objetivo, compreendida entre 10^{-5} e 10^{-7} por hora de voo, a uma situação que implique "redução significativa das margens de segurança concretizadas por uma dificuldade da tripulação enfrentar situações desfavoráveis que possam conduzir a ferimentos aos passageiros";
- b) a regulamentação de grandes barragens requer que os sangradouros permitam o escoamento de uma cheia decamilenar (período de retorno de 10.000 anos), sem danos para a barragem.

Os períodos de retorno destes dois eventos são respectivamente da ordem de 100 anos e 10.000 anos, o que nos dois casos está fora das possibilidades experimentais, sem contar os problemas ligados à experimentação em si mesma.

Conseqüentemente, a demonstração direta do tipo binário ("não será observado nenhuma vez o evento em n anos") não sendo possível, a validação do cumprimento do objetivo está associado em grande parte à validação dos esforços em termos metodológicos e técnicos descritos na análise de segurança.

Se em certos casos a avaliação do nível de segurança pode ser feita ao nível de sistema utilizando as leis de valores extremos, a maioria das análises de segurança executam modelagens de cenários de acidente, cuja credibilidade passa por:

- a) a representatividade dos modelos, que correspondem, em particular, a exaustividade definida pelo número de parâmetros ou de variáveis e pelas leis regendo as relações entre as variáveis internas e externas ao sistema; e
- b) a credibilidade dos dados.

Isto implica uma incerteza (e mais globalmente um desconhecimento) "natural" sobre o procedimento de demonstração, sobre seus resultados e sobre sua interpretação. Esta incerteza não deve entretanto ser comparada à incerteza associada à afirmação, sem estudo suficiente, da impossibilidade *a priori* de ocorrência de um evento indesejável definido no objetivo.

Com efeito, no primeiro caso medidas apropriadas foram estudadas e propostas, e no segundo caso a falta de medidas decorrente unicamente da afirmação “isto não pode acontecer” deixa persistir um verdadeiro estado de insegurança que pode conduzir a uma catástrofe que poderia ser evitada.

Classicamente, a identificação de cenários conduzindo a um evento indesejado passa pela experiência e pela imaginação daqueles que desenvolvem a Análise Preliminar de Riscos do sistema considerado.

Os cenários que resultam desta análise são, em geral não ponderados ou hierarquizados por avaliações preliminares. A única hierarquização é feita segundo quatro classes:

- a) C1: Cenários já observados, julgados realistas;
- b) C2: Cenários já observados, mas julgados não realistas, tendo em conta as medidas de prevenção já tomadas;
- c) C3: Cenários não observados, mas julgados realistas;
- d) C4: Cenários não observados e julgados não realistas

A qualidade do julgamento entre realistas e não realistas está intimamente ligada à profundidade do corpo de conhecimentos do conjunto dos analistas, completada por aquela do decisor, que tem um peso preponderante devido sua função na organização. Com efeito, o dilema do decisor pode ser resumido por:

- a) aceitar a consideração de um cenário cuja ocorrência, se bem que possível, é *a priori* pouco provável durante a vida do sistema; esta consideração pode penalizar inutilmente o projeto, introduzindo requisitos técnicos, econômicos ou operacionais suplementares;
- b) rejeitar a consideração de um cenário cuja ocorrência é considerada ‘a priori’ como pouco plausível durante a vida do sistema e então aceitar, implícita ou explicitamente suas consequências; esta decisão não penaliza o projeto, mas pode engendrar custos adicionais de operação, podendo mesmo levar até ao descomissionamento prematuro do sistema já a partir do primeiro incidente julgado socialmente inaceitável.

Cumprе ressaltar que, segundo a componente do risco considerada, probabilidade ou gravidade, o decisor se inclinará para uma ou outra opção:

- a) se somente considerar a pequena verossimilhança do cenário, ele o rejeitará qualquer que seja sua gravidade, o que constitui uma decisão baseada no curto prazo; ou
- b) se considera antes de tudo a gravidade das conseqüências, o cenário será aceito independentemente de sua verossimilhança, o que constitui uma decisão baseada no longo prazo.

Sob incerteza, uma regra simplista de decisão para consideração de cenários consiste em lhes associar *a priori* um limite de verossimilhança a partir do objetivo associado ao evento indesejado considerado. Este limite pode ser fixado fazendo-se a hipótese que não devem existir mais de 100 cenários possíveis, identificados ou não, que conduzem ao evento indesejado. Isto implica em considerar apenas cenários cuja verossimilhança seja duas ordens de grandeza menores do que o evento indesejado.

Assim, para um objetivo de 10^{-3} /ano, a análise se limitará a cenários cuja probabilidade é superior a 10^{-5} /ano. Por outro lado, para um objetivo de 10^{-7} /ano, serão considerados cenários (formados possivelmente pela conjunção de vários eventos) ou eventos raros de probabilidade igual ou superior a 10^{-9} /ano. Obviamente uma tal regra não pode ser aplicada sem uma análise prévia, mesmo que sucinta.

O último exemplo apresentado traz à tona uma questão fundamental sobre a existência de um limite mínimo de probabilidade desprezível, ou seja, determinar o evento desprezível e cuja probabilidade p serve de borne inferior de truncamento nos cálculos e avaliações probabilísticas de segurança.

Pode-se buscar este evento envelope desprezível e considerando-se eventos naturais que são abstratamente possíveis, mas que não são levados em conta na vida normal dos homens e das sociedades, tal como o chamado “fim do mundo”.

Definindo-se e como a sobrevivência do Universo após N anos e sabendo-se que ele existe há n anos, pode-se associar a e uma probabilidade q que se formaliza a partir de sua duração de vida ou existência T cuja expressão clássica é dada por:

$$\begin{aligned} P(T \geq n, T \geq N) &= P(T \geq N) \text{ com } n < N \\ &= P(T \geq n) \times P(T \geq N \mid T \geq n) \end{aligned}$$

$$\text{com } P(T \geq N \mid T \geq n) = q$$

$$\log q = [P(T \geq N) / P(T \geq n)]$$

faz-se então as seguintes hipóteses:

a) a probabilidade anual de desaparecimento do Universo é constante e igual a p:

$$P(T \geq N) = (1-p)^N$$

b) o Universo foi criado a $n = 1,5 \cdot 10^{10}$ anos;

c) $P(T \geq n) = 1$, já que observa-se que o Universo sobrevive hoje; e

d) arbitrariamente, existe uma chance de 1 contra 2 que o Universo continue existindo no ano que vem.

pode-se então calcular p:

$$(1 - p)^N = 0,5$$

$$p = 4,6 \cdot 10^{-11}, \text{ ou seja, } p > 10^{-11} / \text{ano}$$

para verificar a sensibilidade de p à hipótese arbitrária d), poderíamos verificar:

d') existe uma chance contra 2 que o Universo sobreviva a $N = 2n = 3 \cdot 10^{10}$

$$p = 2,3 \cdot 10^{-11}, \text{ ou seja, } p > 10^{-11} / \text{ano}$$

d'') existe uma chance contra 99 que o Universo sobreviva a $N = n + 1$ anos

$$p = 10^{-12} / \text{ano}$$

constata-se assim que os resultados são de mesma ordem de grandeza, não sendo portanto sensíveis à hipótese arbitrária d).

Sabendo-se que nada pode ser mais catastrófico que o desaparecimento do Universo, o limite mínimo de probabilidade desprezível pode ser fixado entre 10^{-11} e 10^{-12} por ano, ou 10^{-15} a 10^{-16} por hora. Conseqüentemente, pode-se considerar como não realista, se não totalmente absurdo levar em conta e manipular dentro de análises de segurança probabilidades iguais ou inferiores a este limite.

F.6 LEIS DE PROBABILIDADES

As probabilidades são usadas em Segurança de Funcionamento de Sistemas para avaliar os riscos diretamente associados a um perigo identificado e os riscos residuais consecutivos à implementação de uma ação de prevenção ou de proteção. Mesmo que estas

probabilidades sejam geralmente pontuais, sua avaliação necessita o conhecimento, no todo ou em parte, da distribuição de probabilidades donde elas são provenientes.

Segundo a natureza da variável aleatória, discreta ou contínua, que intervém na modelagem do fenômeno perigoso, ou na ação de redução de risco, serão consideradas leis de distribuição de probabilidades discretas ou contínuas.

Dentre as diversas leis de distribuição, consideraremos as listadas a seguir como de maior aplicação. O desenvolvimento matemático e caracterização destas leis é apresentado por inúmeras referências:

a) Leis de Variáveis Discretas:

- a.i Hipergeométrica
- a.ii Binomial
- a.iii Pascal ou Binomial Negativa
- a.iv Geométrica
- a.v Poisson

b) Leis de Variáveis Contínuas:

- b.i Gauss ou Normal
- b.ii Galton ou Log-Normal
- b.iii Exponencial
- b.iv Gama Incompleta
- b.v Beta Incompleta
- b.vi Weibull

Como em Segurança de Sistemas se está em geral interessado pela cauda destas distribuições ou seja, os maiores ou menores quantis, são de grande utilidade também as leis chamadas de Valores Extremos, que serão desenvolvidas em maior detalhe:

- a) Tipo I: Lei de Gumbel;
- b) Tipo II: Lei de Frechet;
- c) Tipo III: Lei de Weibull

A seleção de uma lei de probabilidade é inicialmente ligada à natureza e ao conhecimento do fenômeno estudado, discreto ou contínuo. Numa segunda etapa, a escolha é

guiada pela forma da distribuição medidas pelo coeficiente de assimetria e pelo coeficiente de achatamento (ou curtose). Numa terceira etapa, a escolha é guiada pelo número de parâmetros que intervêm na expressão matemática da função de repartição. Este número varia geralmente entre 1 a 4. Finalmente, o próprio valor destes parâmetros pode modificar consideravelmente a forma da distribuição, como é o caso da lei Beta incompleta e da lei de Weibull.

A escolha *a priori* da lei de probabilidade possui, evidentemente, um impacto significativo sobre o valor da probabilidade associada a um dado quantil. Para concretizar este fato e a título de exemplo, estima-se a probabilidade de sobrevivência de um sistema além de 90 horas e de 100 horas, sabendo que sua média é igual a 50 e seu desvio-padrão é igual a 10. Os resultados são apresentados pela Tabela F.1.

TABELA F.1: COMPARAÇÃO DE LEIS DE PROBABILIDADES

LEI	$P(T \geq 90h)$	$P(T \geq 100h)$
Weibull	$4,0 \cdot 10^{-9}$	$3,5 \cdot 10^{-16}$
Gauss	$3,2 \cdot 10^{-5}$	$2,9 \cdot 10^{-7}$
Beta incompleta	$7,7 \cdot 10^{-5}$	$9,2 \cdot 10^{-7}$
Gama incompleta	$4,5 \cdot 10^{-4}$	$3,5 \cdot 10^{-5}$
Galton	$1,1 \cdot 10^{-3}$	$1,6 \cdot 10^{-4}$
Gumble	$3,3 \cdot 10^{-3}$	$9,2 \cdot 10^{-4}$
Frechet	$6,9 \cdot 10^{-3}$	$3,2 \cdot 10^{-3}$

A análise desta tabela mostra o aspecto majorante das leis de valores extremos, que geram as mais altas probabilidades de sobrevivência. Estas leis são entretanto utilizadas exclusivamente para estimativa de eventos extremos.

Com efeito, o conhecimento da média e do desvio-padrão de uma lei é geralmente obtido a partir de uma amostra cujo tamanho nem sempre é coerente com os quantis que servem de base à avaliação das probabilidades a serem comparadas aos objetivos de segurança.

Sobre o domínio coberto pela amostra, muitas leis podem ser aplicadas para a modelagem, mas para os quantis muito grandes ou muito pequenos, os desvios entre as leis pode tornar-se muito grande e a seleção deve se orientar para as leis de valores extremos que, por construção, permitem melhor estimá-los do ponto de vista da segurança.

A escolha propriamente dita deve levar em conta as leis físicas do fenômeno estudado, que integram explicitamente o conjunto de fatores ativos., cuja importância influi sobre a forma da densidade de probabilidade e, conseqüentemente, sobre os coeficientes que podem servir como indicadores.

F.7 LEIS DE VALORES EXTREMOS

Em análise de segurança de sistemas considera-se geralmente os eventos de probabilidade muito próxima de 1 ou muito próxima de 0, correspondendo a quantis muito grandes ou muito pequenos. De fato eles pertencem às caudas da função distribuição de probabilidade da variável aleatória estudada.

Na prática, o conhecimento desta variável é obtido a partir de uma amostragem de medidas observadas. A função distribuição de probabilidade da maior ou da menor medida da amostra observada leva o nome lei de valor extremo.

Seja uma amostra de n observações independentes $(x_1, \dots, x_n)$, correspondendo a n realizações de uma variável aleatória X , que representa um parâmetro ou uma característica de uma população de dimensão infinita.

Se um número infinito de amostras de mesma dimensão n é tirada desta população e se dentro de cada amostra os valores observados são ordenados em ordem crescente, então os valores de ordem i tem uma distribuição estatística chamada distribuição do quantil x_i , que é *a priori* função do tamanho da amostra.

Esta distribuição, chamada função de repartição empírica do quantil x_i , é utilizada para ajustar a amostra a uma lei de probabilidade teórica.

Para determinar a Lei de Probabilidade de um quantil de ordem dada, seja um valor x da variável aleatória X tal que dentro da amostra existam:

- a) $(i-1)$ valores independentes inferiores a x (evento $E1$);

- b) $(n-1)$ valores independentes superiores a x (evento E2);
- c) 1 valor x_i compreendido entre $x \pm dx$ onde dx é infinitamente pequeno (evento E3).

A partir destas considerações descritivas, vamos procurar determinar a lei de distribuição do quantil de ordem i pertencente ao intervalo $(x-dx/2, x+dx/2)$. Faz-se então as seguintes hipóteses:

- a) as n realizações de x independentes de uma variável aleatória X são equivalentes a uma realização x_i de n variáveis aleatórias independentes X_i ;
- b) ‘a priori’, as n tiragens ou realizações x_i são equi-prováveis, ou seja, a função repartição F_i de cada uma das variáveis aleatórias X_i á uma mesma lei F contínua e uniforme sobre $[0,1]$

Para n e i dados, os eventos E1, E2 e E3 definidos anteriormente são bem identificados e suas probabilidades respectivas P1, P2 e P3 são facilmente calculáveis, já que as tiragens são independentes:

- a) $P1 = \Pr (E1) = \Pr (X < x) = (F(x))^{i-1}$
- b) $P2 = \Pr (E2) = \Pr (X > x) = (1-F(x))^{n-1}$
- c) $P3 = \Pr (x-dx/2 < X < x+dx/2) = f(x) dx$

Deve-se ainda notar que existem:

- a) $(i-1)!$ maneiras de observar E1, correspondentes a $i - 1$ permutações dos $i - 1$ valores inferiores a x ;
- b) $(n-1)!$ maneiras de observar E2 correspondentes a $n - 1$ permutações possíveis dos $n-1$ valores superiores a x ;
- c) uma (1) só maneira de observar E3.

Por consequência, o evento (E1, E2, E3) tal que E1 se produza $(i - 1)!$ vezes, E2 se produza $(n - 1)!$ vezes e E3 se produza uma (1) vez é distribuído segundo uma lei multinomial. Se G_i é sua função repartição, temos:

$$dG_i = \frac{n!}{(i-1)!(n-1)!} [F(x)]^{i-1} \{1-[F(x)]\}^{n-1} f(x) dx \quad [F-16]$$

Reconhece-se nesta expressão uma lei Beta incompleta cuja expressão matemática da densidade de probabilidade se escreve:

$$d\beta(a, b, t) = \frac{t^{a-1} (1-t)^{b-1}}{\beta(a, b)} Dt \quad [F-17]$$

com $a = i$, $b = n - i + 1$ e $t = F(x)$

Por conseguinte, a lei de repartição do valor F_i da probabilidade associada a ordem i se escreve:

$$dG_i = \frac{1}{\beta(i, n - i + 1)} [F_i^{i-1} (1 - F_i)^{n-i}] dF \quad [F-18]$$

Para $i = 1$, obtém-se a lei de probabilidade do menor elemento (mínimo) de uma amostra ordenada dentro da ordem crescente $X_1 = \inf(x_1, \dots, x_n)$. Sendo $\beta(1, n) = 1/n$, temos uma lei genérica para distribuição de mínimos:

$$G_1(x) = \{1 - [1 - F(x)]^n\} \quad [F-19]$$

Para $i = n$, obtém-se a lei de probabilidade do maior elemento (máximo) de uma amostra ordenada dentro da ordem crescente $X_n = \sup(x_1, \dots, x_n)$. Sendo $\beta(n, 1) = 1/n$, temos uma lei genérica para distribuição de máximos:

$$G_n(x) = [F(x)]^n \quad [F-20]$$

A seguir será discutida a distribuição do maior quantil (máximos). Deve-se entretanto lembrar que, consideradas as regras de operações com variáveis aleatórias, um problema de mínimos pode ser convertido em um problema de máximos através de transformações algébricas dos dados da amostra convenientes.

Os limites triviais da lei genérica de distribuição de máximos (maior quantil) se escrevem:

$$a) \text{ Para } F(x) < 1, \text{ temos } \lim_{n \rightarrow \infty} G_n(x) = 0$$

$$b) \text{ Para } F(x) = 1, \text{ temos } \lim_{n \rightarrow \infty} G_n(x) = 1$$

Mais precisamente, a equação de $G_n(x)$ pode ser escrita como:

$$G_n(x) = (F(x))^n = (1 - (1 - F(x)))^n \quad [F-21]$$

Para n suficientemente grande e $1 - F(x)$ pequeno, logo x grande, obtém-se:

$$G_n(x) = e^{-n(1 - F(x))} \quad [F-22]$$

Gumbel demonstrou que, respeitadas certas hipóteses,

$$\text{se } \lim_{x \rightarrow \infty} \frac{d}{dx} \frac{[1 - F(x)]}{F'(x)} = 0, \quad [F-23]$$

a distribuição limite de X_n quando n tende ao infinito se escreve:

$$G_n(x) = \exp \{ - \exp [- n F'(x_{on}) \cdot (x_n - x_0)] \} \quad [F-24]$$

onde $x_{on} = F^{-1}(1 - 1/n) \Leftrightarrow F(x_{on}) = 1 - 1/n$

Obtém-se desta forma matemática da distribuição de Gumbel:

$$G(x) = \exp \{ - \exp [(x - x_{on}) / a] \} \quad [F-25]$$

onde x_{on} é o parâmetro de posição

$$a = \frac{1}{n F'(x_{on})} \quad \text{é o parâmetro de escala}$$

Deve-se notar o caráter arbitrário desta lei na ausência de conhecimento da lei parente $F(x)$, o que ocorre em praticamente todos os casos reais.

Supondo que a distribuição de origem da amostra ou lei parente seja normal (lei de Gauss) de parâmetros μ e σ , a expressão matemática da distribuição do quantil de ordem n se escreve:

$$G(x_n) = \exp \{ - \exp [\frac{(2 \ln n)^{1/2}}{\sigma} \cdot (x_n - \mu - \sigma (2 \ln n)^{1/2})] \} \quad [F-26]$$

Conforme visto anteriormente, a forma matemática da distribuição de probabilidade do maior quantil fazia aparecer a lei de repartição da variável X da população inicial. Gnedenko demonstrou que qualquer que seja a lei de distribuição inicial contínua em $[0;1]$, existem somente três tipos de leis assintóticas do maior (e também do menor) quantil observado, chamadas leis de valores extremos. A lei de tipo I é dita de decrescimento exponencial. As leis de tipo II e III são ditas de decrescimento algébrico.

a) Tipo I: Lei de Gumbel $F(x) = \exp \{ - \exp [- (x - x_0) / a] \}$, $a \neq 0$ [F-27]

b) Tipo II: Lei de Frechet $F(x) = \exp \{ - [(x - x_0) / b]^{-1/a} \}$, [F-28]

para $x > x_0$, $b > 0$ e $0 < a < 0,5$

que também pode ser escrita como:

$$F(x) = \exp \{ - \exp [(\ln(x - x_0) - \ln b) / a] \} \quad [F-29]$$

Se X segue uma lei de Frechet, então

$\ln(X - x_0)$ segue uma lei de Gumbel.

c) Tipo III: a lei de Weibull: $F(x) = 1 - \exp \{ - [(x - x_0) / a]^b \}$, $a, b > 0$ [F-30]

Aplicações da Lei de Gumbel

A função repartição se escreve:

$$F(x) = \exp(-\exp(-(x - x_0)/a)) \quad [F-31]$$

A variável reduzida de Gumbel é definida por:

$$u = (x - x_0)/a, \text{ donde } F(u) = \exp(-\exp(-u)) \quad [F-32]$$

A densidade de probabilidade se escreve então:

$$f(u) = F'(u) = \exp(-u) * \exp(-\exp(-u)) \quad [F-33]$$

A curva representativa é uma curva em sino assimétrica (a assimetria é devida ao sinal do parâmetro a). A curva tem seus pontos de inflexão em $u = \pm 0,96243$. As principais características estatísticas são apresentadas pela Tabela F.2.

TABELA F.2: ESTATÍSTICAS DA LEI DE GUMBEL

Média	$\mu = x_0 + 0,577216 a$
Desvio - Padrão	$\sigma = 1,2825 a$
Moda	$X_0 = x_0$
Mediana	$X_{0,5} = x_0 + 0,366513 a$
Coeficiente de Assimetria	$\gamma_1 = \pm 1,139 \text{ (sinal de } a)$
Coeficiente de Achatamento	$\gamma_2 = 2,4$

A probabilidade correspondente à média μ é igual a:

- 0,570 se $a > 0$
- 0,43 se $a < 0$

A probabilidade correspondente à moda x_0 é igual a:

- 0,368 se $a > 0$
- 0,632 se $a < 0$

Dado $F(u) = p$, determina-se o valor de x pela inversão da forma matemática da função repartição. Obtém-se então para o valor x_p do quantil de probabilidade p :

$$u = -\ln(-\ln p), \text{ donde } x_p = x_0 + a \ln(-\ln p) \quad [F-34]$$

O quantil u associado a um período de retorno (ou recorrência) T é determinado diretamente por:

$$u = -\ln(-\ln(1 - 1/T)) \quad [F-35]$$

onde $x_p = x_0 + a \ln(-\ln(1 - 1/T))$

Para avaliação de parâmetros a partir de uma amostra pelo método da máxima verossimilhança obtém-se:

$$\frac{\sum x_i \exp (x_i / a)}{\sum \exp (x_i / a)} + a = X \quad [F-36]$$

$$x_0 = - a (\ln (1/n) \sum \exp (x_i / a)) \quad [F-37]$$

Pelo método dos momentos obtém-se:

$$a = 0,7797 \sigma \quad \leftrightarrow \quad \mu = x_0 + 0,577216 a \quad [F-38]$$

$$x_0 = \mu - 0,45 \sigma \quad \leftrightarrow \quad \sigma = 1,28255 a \quad [F-39]$$

Para avaliação dos intervalos de confiança, tem-se que o afastamento T entre x_p e x_p ponderado por s_x pode ser considerado como uma variável aleatória:

$$T = \frac{x_p - x_p}{s_x} = \frac{X - \mu - \sigma v_p}{s_x} + v_p \quad [F-40]$$

$$\text{onde } v_p = -[0,450 + 0,7797 \ln (- \ln (1 - p))]$$

Esta estatística que mede o afastamento entre o quantil de ordem p e sua estimativa a partir de uma amostra de tamanho n foi estudada por Bernier. Ele propõe dois ábacos para estimar os bornes dos intervalos de confiança a 70% e a 95%. Para um limite de risco α (confiança $1 - \alpha$), os bornes do intervalo de confiança de x_p se escrevem, para um número de observações n:

$$a) \ x_p' = x_p + T_2 (p, m, \alpha) s_x$$

$$b) \ x_p'' = x_p + T_1 (p, m, \alpha) s_x$$

Por exemplo, para $p = 10^{-3}$, $n = 120$ e $\alpha = 0,05$ pode-se determinar através dos ábacos:

- $T_1 (10^{-3} ; 120; 0,05) = 1,25$
- $T_2 (10^{-3} ; 120; 0,05) = - 0,95$

O ajustamento à lei de Gumbel não se faz diretamente a partir de uma amostra de observações de uma característica, mas a partir de uma amostra “sintética” dos valores máximos observados sobre uma duração correspondente ao período ou base de tempo associada à ocorrência dos eventos extremos considerados.

O procedimento para obtenção da amostra “sintética” utilizada para o ajustamento é realizado em quatro etapas:

- a) Fixação da unidade de tempo: esta unidade de tempo T serve de base para definir a ordenação relativa à característica do evento extremo; ela pode ser o mês, ano, etc.
- b) Segmentação da amostra inicial: a amostra inicial é segmentada em n períodos de T unidades de tempo.
- c) Dentro de cada período determina-se o valor máximo da característica observada.
- d) Agrupa os n valores máximos sob a forma de uma amostra “sintética”.

A média e desvio padrão são então calculados a partir da amostra para determinar a moda x_p e o parâmetro de forma a conforme as relações apresentadas anteriormente.

Os valores da amostra podem também ser plotados sobre um papel de Gumbel, verificando-se a adequação do ajuste. O teste de aderência de Kolmogorov-Smirnov permite consolidar a qualidade do ajuste a um limite de risco α (confiança $1 - \alpha$).

Aplicações da Lei de Frechet

A função repartição se escreve:

$$F(x) = \exp [(- (x - x_0) / b)]^{-1/a} \text{ ou} \quad [F-41]$$

$$F(x) = \exp \{- \exp [(\ln (x - x_0) - \ln b) / a]\} \quad [F-42]$$

para $x > x_0$ e $b > 0$ e $0 < a < 0,5$

A segunda forma é comparável àquela da Lei de Gumbel após transformação logarítmica da variável e levando em conta um limite inferior x_0 . A variável reduzida de Frechet é definida por:

$$u = (x - x_0) / b \quad [F-43]$$

A densidade de probabilidade se escreve então:

$$f(u) = (1/ab) * [(x - x_0)/b]^{-(1/a)-1} . \exp \{ [(x - x_0)/b]^{-(1/a)} \} \quad [F-44]$$

A Lei de Frechet é representada por uma família de curvas parametrizadas em a. Estas curvas tem a forma de sino assimétrica. As principais características estatísticas são apresentadas pela Tabela F.3.

TABELA F.3: ESTATÍSTICAS DA LEI DE FRECHET

Média	$\mu = b \Gamma(1 - a) + x_0$
Desvio - Padrão	$\sigma = b [\Gamma(1 - 2a) - \Gamma^2(1 - a)]^{1/2}$

Moda	$X_0 = b (1 + a)^{-a} + x_0$
Mediana	$X_{0,5} = b (\ln 2)^{-a} + x_0$

Dado $F(u) = p$, determina-se o valor de x pela inversão da forma matemática da função repartição. Obtém-se então para o valor x_p do quantil de ordem p :

$$x_p = x_0 + b \exp[-a \ln(-\ln p)] \quad [F-45]$$

Deve-se notar a dificuldade de escolha entre a Lei de Gumbel e a Lei de Frechet a partir de amostras em geral limitadas. Pode-se entretanto afirmar que a Lei de Gumbel é aquela mais utilizada para ajustar a amostra de máximos de um conjunto de observações.

Seleção de uma Lei de Valores Extremos

As leis de distribuição de valores extremos (*Extreme-Value Distributions* ou *Weakest-Link distributions*) tratam da probabilidade de ocorrência $F^*(x^*)$ de máximos ou mínimos de x^* quando um grande número de eventos independentes são amostrados de uma distribuição inicial $F(x)$.

Foi visto que a forma matemática da distribuição de máximos (ou mínimos) fazia aparecer a lei de repartição da variável aleatória X da população inicial.

Demonstra-se que qualquer que seja a distribuição inicial, existem somente três tipos de leis assintóticas de máximos (ou mínimos):

- a) Tipo I (Gumbel)
- b) Tipo II (Frechet)
- c) Tipo III (Weibull)

Não existe um critério absoluto para selecionar um determinado tipo para modelagem de um dado fenômeno. Entretanto, à guisa de orientação pode-se fazer as seguintes recomendações:

- a) para fenômenos com distribuição inicial normal (gaussiana), tais como a resistência dos materiais, vazão de cheias de rios, deve-se utilizar a Lei de Gumbel;

- b) para fenômenos com distribuição inicial log-normal, tais como frequência e magnitude de terremotos, deve-se utilizar a Lei de Frechet;
- c) para fenômenos com distribuição inicial Gama, tais como velocidade do vento, altura de ondas, deve-se utilizar a Lei de Weibull.

ANEXO G

CONCEITOS E MÉTODOS DA SEGURANÇA DE FUNCIONAMENTO

A Segurança de Funcionamento de Sistemas Industriais constitui hoje uma verdadeira disciplina de engenharia, aplicada dentro de todas as diferentes fases de vida de um sistema industrial, desde sua concepção até o seu descomissionamento, passando pelas fases de desenvolvimento e operação.

Num sentido amplo, a Segurança de Funcionamento de Sistemas pode ser definida como a “Ciência das Falhas”. Ela inclui assim o conhecimento, a avaliação, a previsão, a medida e o controle das falhas de um sistema.

Num sentido estrito, a Segurança de Funcionamento de Sistemas é a capacidade de um sistema cumprir com sucesso a missão para a qual foi concebido, sem que ocorram eventos com conseqüências indesejáveis tanto para os componentes do próprio sistema como para o ambiente onde o sistema encontra-se em interação.

Como cumprimento da “missão”, entende-se o desempenho de uma ou várias funções requeridas, dentro de condições internas e externas ao sistema preestabelecidas, e o conseqüente atendimento aos objetivos técnicos para os quais o sistema foi concebido.

A não ocorrência dos “eventos com conseqüências indesejáveis” deve ser garantida nos três casos possíveis de resultados finais da missão, que são:

- a) sucesso (pleno cumprimento das funções requeridas);
- b) sucesso parcial (degradação sem perda total das funções requeridas); e
- c) insucesso (perda total das funções requeridas).

As “conseqüências indesejáveis” estão associadas a morte ou injúrias aos operadores do próprio sistema (entendidos como aqueles que podem ser individualmente identificados), e ao público em geral circundante às implantações físicas do sistema, ou indiretamente impactados pelo funcionamento do sistema (entendido como aqueles que não podem ser individualmente identificados), bem como a impactos negativos (degradações de funções)

inaceitáveis aos demais sistemas que compõe o meio ambiente em interação com o sistema industrial em estudo.

A segurança do funcionamento de um sistema pode ser caracterizada pelos seguintes conceitos (ou técnicas) componentes, que serão a seguir definidos individualmente:

- a) Confiabilidade;
- b) Disponibilidade;
- c) Manutibilidade; e
- d) Seguridade (ou Segurança propriamente dita).

A partir destes conceitos define-se as características de segurança de funcionamento de um sistema ilustradas pela Figura G.1:

- a) *Mean Time To Failure* MTTF: duração média do funcionamento do sistema antes da primeira falha;
- b) *Mean Time To Repair* MTTR: duração média de reparo;
- c) *Mean Up Time* MUT: duração média de funcionamento após reparo;
- d) *Mean Down Time* MDT: duração média de indisponibilidade, correspondente às fases de detecção da pane, reparo da pane e recolocação em serviço; e
- e) *Mean Time Between Failures* MTBF: duração média entre duas falhas consecutivas de um sistema reparável.

FIGURA G.1: CARACTERÍSTICAS DE SEGURANÇA DE FUNCIONAMENTO

De uma maneira geral, outros conceitos tem sido introduzidos em estudos específicos, derivados dos quatro conceitos básicos, e podem ser igualmente incluídos na Segurança de Funcionamento de Sistemas, tais como:

- a) Durabilidade: capacidade de uma entidade permanecer em estado de cumprir uma função requerida, dentro de condições dadas de utilização e de manutenção, até que um estado limite seja atingido;
- b) Continuabilidade: capacidade de uma função, uma vez obtida, continuar a ser garantida, dentro de condições determinadas, durante um intervalo de tempo desejado;
- c) Vulnerabilidade: suscetibilidade de um sistema às agressões potenciais;
- d) Capacidade de Sobrevivência (*survivability*): capacidade de um sistema resistir a agressões internas e externas.

O ponto comum entre os conceitos componentes da Segurança de Funcionamento de Sistemas é o emprego da linguagem probabilística como meio de avaliação. Entretanto, quando utilizada no domínio da Segurança de Funcionamento de Sistemas, esta linguagem perde em parte seu rigor formal de origem, estabelecido pela Teoria das Probabilidades. Consequentemente, avaliações quantitativas diferentes associadas a uma situação similar podem ser efetuadas por analistas de cultura e experiência diversas.

Tal fato decorre da incerteza implícita ou explícita que existe sobre o universo que serve de base ao cálculo das probabilidades. A introdução de um universo condicional ou Corpo de Keynes feita por diferentes teóricos das probabilidades (dentre os quais Emile Borel), associada à Análise da Decisão na Incerteza, conduz a uma abordagem subjetiva das probabilidades, diversa da abordagem matemática formal.

G.1 CONFIABILIDADE

Resumindo as inúmeras definições existentes, confiabilidade é a capacidade de um sistema cumprir uma função requerida, dentro de condições preestabelecidas, durante um período determinado.

A confiabilidade é geralmente medida pela probabilidade de uma entidade E cumprir uma função requerida em condições fixadas durante o intervalo de tempo $[0, t]$:

$$R(t) = P(E \text{ sem falha sobre } [0, t]) \quad [G-1]$$

A capacidade contrária, que denominaremos "Desconfiabilidade", poderá então ser medida por:

$$D(t) = 1 - R(t) \quad [G-2]$$

Deve-se distinguir três tipos de medida de diferentes naturezas que podem ser feitas de $R(t)$:

- a) confiabilidade operacional (ou observada ou estimada), que resulta da observação e da análise estatística do comportamento de entidades idênticas dentro de condições operacionais definidas;
- b) confiabilidade extrapolada, que resulta de uma extensão, feita com base em hipóteses de extrapolação ou interpolação, da confiabilidade operacional de uma entidade para intervalos de tempo e/ou condições diferentes; e
- c) confiabilidade previsional (ou prevista), que estima a confiabilidade futura de um sistema a partir de considerações sobre seu projeto e sobre a confiabilidade de seus componentes.

A confiabilidade operacional é uma estatística, a confiabilidade extrapolada é um modelo de um processo estocástico e a confiabilidade previsional é uma probabilidade subjetiva, cada uma tendo uma utilização específica que não deve ser confundida.

G.2 DISPONIBILIDADE

Disponibilidade é entendida como a capacidade de uma entidade estar em estado de cumprir uma função requisitada dentro de condições preestabelecidas e num instante determinado.

A disponibilidade é geralmente medida pela probabilidade de uma entidade E encontrar-se em estado de cumprir uma função requisitada dentro de condições determinadas num instante t :

$$A(t) = P(E \text{ sem falha em } t) \quad [G-3]$$

A capacidade contrária, que denominaremos "Indisponibilidade", poderá então ser medida por:

$$I(t) = 1 - A(t) \quad [G-4]$$

Deve-se distinguir três tipos de medida de diferentes naturezas que podem ser feitas de A(t):

- a) disponibilidade instantânea (ou imediata), que corresponde a definição clássica apresentada; em particular, esta disponibilidade é aquela que permite a um sistema enfrentar uma situação de urgência;
- b) disponibilidade potencial (ou prevista ou contínua ou estatística), que corresponde a capacidade do sistema funcionar de modo contínuo durante um intervalo de tempo determinado, considerando seu estado atual; esta disponibilidade está diretamente condicionada pela manutenção do sistema e pela inspeção em serviço de seus componentes; e
- c) disponibilidade pós-incidental (ou capacidade de sobrevivência), que caracteriza a capacidade do sistema continuar a desempenhar suas funções, mesmo que de forma degradada ou parcial, após um incidente que tenha afetado algumas de suas partes.

G.3 MANUTEBILIDADE

Manutabilidade é entendida como a capacidade de uma entidade ser mantida ou restabelecida no estado de cumprir uma função requisitada, quando atividades de manutenção são realizadas dentro de condições preestabelecidas, seguindo um conjunto de procedimentos e meios previamente prescritos. A manutabilidade é geralmente medida pela probabilidade que a manutenção de uma entidade E, executada dentro de condições dadas, com procedimentos e meios prescritos, seja concluída num tempo t, sabendo que a entidade falhou em t=0:

$$M(t) = P(\text{manutenção de E concluída em } t) \quad [G-5]$$

$$\text{ou } M(t) = P(E \text{ é reparado sobre } [0, t]) \quad [G-6]$$

A capacidade contrária, que denominaremos "Não-manutabilidade", poderá então ser medida por:

$$\bar{M}(t) = 1 - M(t) \quad [G-7]$$

Este conceito somente diz respeito, obviamente, aos sistemas reparáveis. A manutabilidade caracteriza a capacidade de um sistema reiniciar o cumprimento de suas funções após uma falha.

Torna-se aqui muito importante distinguir os três tipos básicos de atividades de manutenção:

- a) manutenção preventiva: aquela que é feita segundo um planejamento preestabelecido, baseado no histórico de operação do sistema, e visa evitar a ocorrência de uma falha;
- b) manutenção preditiva: aquela que é feita no momento em que uma variável monitorada (temperatura, pressão, vibração, composição físico-química de fluidos de processo, corrente, tensão) do sistema atinge um valor crítico preestabelecido, e visa restabelecer o funcionamento normal do sistema antes que o mesmo se degrade a um nível inaceitável;
- c) manutenção corretiva (ou reparo): aquela que é feita após a ocorrência de uma falha ou degradação inaceitável do sistema, e visa restabelecer suas condições de funcionamento normal.

G.4 SEGURIDADE (OU SEGURANÇA)

Seguridade ou Segurança propriamente dita é entendida como a capacidade de uma entidade evitar a ocorrência, dentro de condições preestabelecidas, de eventos críticos para o seu funcionamento ou catastróficos para seus operadores e meio-ambiente. A seguridade é geralmente medida pela probabilidade de uma entidade E não ensejar, dentro de condições internas e externas determinadas, a ocorrência de um conjunto de conseqüências catastróficas preestabelecido, ao longo de sua vida útil.

$$S(T) = P(E \text{ sem falha} \Rightarrow \{C\} \text{ em } [0, T]) \quad [G-8]$$

A capacidade contrária, que denominaremos "Inseguridade", poderá então ser medida por:

$$\bar{S}(t) = 1 - S(T) \quad [G-9]$$

G.5 CINDINÍSTICA

Os conceitos teóricos e as aplicações da linguagem das probabilidades apresentados pelo presente trabalho são associadas diretamente à sua utilização no conceito de Seguridade da Segurança de Funcionamento de Sistemas, tratada dentro da disciplina geral da Cindinística ou Ciência do Perigo. Com efeito, as probabilidades utilizadas são várias ordens de grandeza inferiores às utilizadas pelos conceitos de Confiabilidade, Disponibilidade e

Manutibilidade, outros principais componentes da Segurança de Funcionamento de Sistemas, constituindo então a uma "norma adaptada" a eventos raros ou improváveis e não a estatísticas. Conseqüentemente, mesmo que certos conceitos e técnicas matemáticas (probabilidades e estatística) sejam comuns aos outros componentes da Segurança de Funcionamento de Sistemas, os conceitos básicos são específicos e as técnicas são próprias à Seguridade dos sistemas.

G.6 NÍVEIS DE SEGURANÇA

A partir do conceito de Segurança de Funcionamento de Sistemas aplicado ao projeto preliminar de uma instalação é que serão identificados os eventos tais como falhas combinadas ou não a erros humanos ou a agressões externas ou ameaças que poderão conduzi-la a um estado inseguro. Isto feito, os métodos estatísticos e probabilísticos permitirão avaliar as probabilidades destas falhas e dos estados inseguros resultantes, através sua propagação e transformação dentro do sistema, sob a forma de cenário.

As análises de Segurança de Funcionamento de Sistemas de sistemas irão então se desenvolver com três objetivos distintos e complementares, que podem ser associados a níveis de segurança de uma instalação:

- a) Nível Primário (Nível 1): atendimento dos objetivos técnicos para os quais o sistema foi concebido (sucesso total ou parcial da missão); este nível contém implicitamente a "capacidade" do sistema, sendo uma atividade de engenharia à qual estão associadas as técnicas de projeto e as tecnologias empregadas; está associado ao grau de prevenção do sistema quanto a ocorrência de eventos inicializadores de um evento indesejado;
- b) Nível Secundário (Nível 2): está associado ao grau de proteção do sistema quanto a ocorrência do evento indesejado, ou seja, a capacidade do sistema em se auto-proteger e proteger o ambiente caso o evento indesejado venha a ocorrer; a este nível, o sucesso da missão está comprometido;
- c) Nível Terciário (Nível 3): está associado à severidade dos efeitos do evento indesejado sobre o sistema e o ambiente, ou seja, como as conseqüências do evento indesejado são sentidas no interior do próprio sistema e no meio ambiente, envolvendo a aplicação de eventuais procedimentos de emergência internos e externos ao sistema.

G.7 COMPROMISSO ENTRE CONFIABILIDADE E SEGURANÇA

A confiabilidade pode entrar em conflito com a seguridade. Isto ocorre em situações onde se torna necessário priorizar entre a possibilidade de sucesso da missão e a possibilidade de ocorrência de evento catastrófico.

Um exemplo muito simples pode auxiliar a visualizar este tipo de situação: seja um sistema de disparo de uma arma, baseada no fechamento de um relê. Este relê comporta dois tipos de falha:

- a) fechamento intempestivo, com probabilidade 0,01; e
- b) travamento em aberto, com probabilidade 0,02.

Considerando que o fechamento intempestivo é um evento catastrófico e que o travamento em aberto implica no insucesso da missão, poder-se-ia adotar três tipos de solução:

- a) sem redundância: neste caso a confiabilidade seria de 0.97 e a seguridade seria 0.99;
- b) redundância paralelo: neste caso a confiabilidade seria 0.9797 e a seguridade 0.9801;
- c) redundância série: neste caso a confiabilidade seria 0.94 e a seguridade 0.9999.

Observa-se então que a adoção de um ou outro tipo de redundância implica privilegiar um dos dois tipo de pane: a confiabilidade requer a redundância paralelo e a seguridade requer a redundância série.

Um outro exemplo seria de um sistema embarcado em um submarino, cujo bom funcionamento é necessário à segurança do navio. Pode-se imaginar três estruturas possíveis, derivadas dos procedimentos de operação, resumidos pela Tabela G.1, que considera, em todos os casos que a confiabilidade do sistema ao longo de uma missão é 0,999.

TABELA G.1: CONFLITO ENTRE CONFIABILIDADE E SEGURIDADE

Sistema Único falha simples $\Rightarrow$ acidente	Confiabilidade sucesso: 0,999 não reparo: 0,999 Seguridade: 0,999
Sistema com redundância simples falha simples $\Rightarrow$ insucesso	Confiabilidade sucesso: 0,998 não reparo: 0,998

falha dupla $\Rightarrow$ acidente	Seguridade: 0,999999
Sistema com redundância dupla	Confiabilidade sucesso: 0,999997
falha simples $\Rightarrow$ reparo	não reparo: 0,997
falha dupla $\Rightarrow$ insucesso	Seguridade: 0,9999999
falha tripla $\Rightarrow$ acidente	

Este exemplo também mostra que a Confiabilidade e a Seguridade podem entrar em conflito, à medida que as exigências relativas a estes dois conceitos podem conduzir a soluções técnicas diferentes, em alguns casos incompatíveis. A Tabela G.2 resume as diferenças e os pontos comuns entre os dois conceitos:

TABELA G.2: COMPARAÇÃO ENTRE CONFIABILIDADE E SEGURIDADE

DIFERENÇAS	
CONFIABILIDADE	SEGURIDADE
1. Aplica-se, em geral, a um componente ou item considerado isoladamente	1. Aplica-se necessariamente a um sistema e dá ênfase aos problemas de interação
2. Geralmente não leva em conta os fatores humanos	2. Considera o homem como uma parte do sistema estudado
3. Estuda o bom funcionamento de uma entidade dentro de condições de operação bem especificadas	3. Deve abordar toda circunstância, normal ou anormal, podendo conduzir a situações perigosas
4. Envolve falhas cujo custo é da mesma ordem de grandeza do custo normal da missão	4. Envolve eventos cujo custo é de uma ordem de grandeza claramente superior àquela do custo normal de uma missão
5. Envolve eventos que podem ser geralmente avaliados pela experiência e pelo tratamento estatístico	5. Envolve múltiplas combinações de eventos, individualmente pouco prováveis, que escapam a um tratamento estatístico convencional
6. Pode entrar em conflito com a Seguridade e exigir em certos casos soluções técnicas diferentes	6. Pode ser melhorada por múltiplos meios, sendo o aumento da Confiabilidade de certas partes do sistema apenas um deles
SEMELHANÇAS	
CONFIABILIDADE	SEGURIDADE
7. Utilizam-se do cálculo de probabilidades e dos métodos estatísticos	
8. Estabelecem-se por meios comparáveis (aplicação de especificações, programa de qualidade, revisões de projeto, coleta e tratamento de informações técnicas)	
9. As análises e programas de confiabilidade e de segurança se estendem por todo o ciclo de vida de um sistema, desde seu projeto até seu descomissionamento	

G.8 NORMAS CLÁSSICAS DE SEGURANÇA

As regras e normas de segurança envolvem, geralmente, a identificação um certo número de casos críticos e a imposição, com carácter regulamentar, de normas de projeto que permitem conservar um nível de segurança conveniente nestes casos. Os casos críticos são definidos a partir da análise de situações reais observadas e que conduziram (ou poderiam ter conduzido) a um acidente. As normas de projeto constituem portanto soluções técnicas cuja experiência tem demonstrado, ao menos dentro de um certo domínio de conhecimento, resultados adequados.

Mesmo fazendo abstração de todo aspecto regulamentar, tais normas de projeto constituem um referência extremamente útil nas fases de projeto e desenvolvimento, onde não se pode ainda levar a termo análises mais precisas. É entretanto necessário saber o mais cedo possível em que medida as técnicas utilizadas no projeto se afastam do domínio do conhecimento abrangido pela experiência adquirida, podendo assim potencialmente derroga as condições técnicas assumidas implícita ou explicitamente pelas regulamentações e normas de segurança.

Se um sistema possui um domínio de funcionamento próximo àquele dos sistemas similares que o precederam, se ele é projetado e fabricado segundo procedimentos análogos e se ele satisfaz às mesmas condições técnicas, aos mesmos regulamentos, às mesmas normas, então ele poderá ser considerado como tendo uma segurança equivalente. Assim, as normas de segurança oferecem, de forma racional, meios aceitáveis de demonstração de segurança para soluções clássicas.

Deve-se considerar que os regulamentos e normas de segurança tem um alcance jurídico-legal: servem de base para a avaliação de sistemas que devem obter uma autorização governamental para operarem (homologação, licenciamento), bem como auxiliam no estabelecimento das responsabilidades das partes envolvidas em caso de acidente.

Existem entretanto grandes inconvenientes em aplicar de maneira dogmática regulamentos e normas de segurança, pois a rapidez de evolução da tecnologia e a diversidade e especialização dos sistemas torna muito complexa a elaboração de procedimentos de aplicação universal. Com efeito, a aplicação "ao pé da letra" de métodos

baseados na definição *a priori* de casos críticos e sobre a utilização obrigatória de certas soluções técnicas consagradas podem conduzir a absurdos, por diversas razões:

- a) os casos considerados *a priori* como críticos não são sempre na realidade os mais críticos; sua identificação é baseada normalmente sobre hipóteses, em geral implícitas, relativas à utilização do sistema e à confiabilidade de suas diversas partes; a própria noção de caso crítico definido *a priori* pode ser questionada, pois sua identificação deveria ser precedida de uma análise da confiabilidade das diferentes partes do sistema;
- b) certas normas que se revelaram satisfatórias para sistemas de gerações anteriores podem tornar-se um empecilho para aqueles de nova geração, considerando as evoluções ocorridas nos procedimentos de operação e ao nível tecnológico;
- c) transformar uma solução técnica, um procedimento de projeto válido em um dado momento histórico, em uma exigência imutável conduz a uma esclerose técnica, freia o progresso e constitui a longo prazo um impedimento à melhoria da segurança;
- d) o simples enunciado dos casos críticos e dos procedimentos de projeto, tal como em geral figuram nos regulamentos e normas, não permite discernir os objetivos de segurança que foram visados; e
- e) quando uma exigência particular é imposta a uma parte de um sistema, torna-se necessário, para interpretar esta exigência, considerar com grande ênfase a integração desta parte dentro do sistema e o emprego do sistema.

G.9 SEGURANÇA COMO QUALIDADE

A qualidade é a medida dentro da qual um produto específico encontra-se adaptado aos requisitos para os quais ele é destinado a atender. É definida como a “capacidade de um produto ou serviço satisfazer as necessidades dos utilizadores”.

Rigorosamente, a qualidade de um produto é caracterizada não somente pela sua conformidade às especificações que o definem, mas também pela sua capacidade de permanecer conforme às suas especificações durante toda sua vida útil. Uma das características fundamentais de um produto, que concorre a sua qualidade é sua confiabilidade, isto é, sua capacidade de conservar as características de origem.

Entretanto, uma abordagem bastante disseminada considera a qualidade como a conformidade do produto a sua especificação na saída da fábrica. A confiabilidade seria então sua capacidade de permanecer conforme ao longo do período de utilização. Neste sentido, a confiabilidade torna-se uma extensão da qualidade no tempo.

Em realidade, o conceito de Segurança de Funcionamento de Sistemas está intimamente ligado ao de Qualidade, mais precisamente, ao de Garantia da Qualidade. A confiabilidade, disponibilidade, manutibilidade e seguridade são, em última instância, meios para garantir que um “produto” (entendido aqui no seu sentido mais amplo) satisfaça, ao longo de toda sua vida útil, as necessidades de seus utilizadores, que incluem obrigatoriamente a não ocorrência de prejuízos aos próprios utilizadores e ao ambiente dentro do qual esta utilização é feita. Deve-se entretanto ressaltar que a Garantia da Qualidade ensejou teorias e métodos específicos que não serão tratados pelo presente trabalho.

G.10 SEGURANÇA E PROCESSO DECISÓRIO

Entende-se como decisão toda escolha, entre muitas ações possíveis que comporte riscos de insucesso da "missão" e/ou de danos às pessoas, aos bens e ao meio-ambiente. Nestes termos, o processo decisório pode ser interpretado como um gerenciamento de riscos.

Todas as técnicas de análise e avaliação da segurança de sistemas têm o mesmo objetivo: fornecer ao responsável pela decisão (“decisor”) os elementos que lhe permitam tomar a melhor decisão possível, a partir do conjunto de informações conhecidas e consideradas na análise de segurança e resumidas pela síntese de resultados que lhe é apresentada.

A determinação da melhor decisão possível ou decisão “ótima” se faz, pela aplicação, implícita ou explícita, de um procedimento de análise do tipo relação custo-benefício, dentro da qual os riscos constituem um custo a ser considerado ou, inversamente, a redução de riscos constitui um benefício.

Uma base teórica para elaboração de um procedimento decisório racional pode ser derivada da teoria geral da decisão, ou teoria da probabilidade-utilidade que resulta da

confrontação das funções de decisão estatística, e das teorias neo-bayesianas. Dentro deste contexto, a estatística decisória agrupa um conjunto de métodos cujo objetivo é a tomada de decisões racionais em presença da incerteza.

G.11 “LEIS” DE MURPHY

A capacidade de apreciação de um evento indesejável e a percepção dos riscos envolvidos está intimamente associada à experiência adquirida pelo analista e pelo decisor. O capitão Murphy, do exército dos EUA, exprimiu, sob uma forma humorística, uma lista de axiomas fatalistas que descrevem de modo determinista e negativo os comportamentos e situações diversas. Doze destes axiomas são apresentados a seguir:

- Tudo que pode ir mal, irá mal;
- Se mais de uma coisa pode ir mal, aquela que irá mal será a que for mais catastrófica;
- Um defeito escondido se tornará muito aparente nas piores circunstâncias possíveis;
- Um atalho para executar uma operação perigosa é o caminho mais rápido que leva ao desastre.
- Toda tarefa que pode ser feita de uma maneira incorreta, não importando o quanto reduzida é a probabilidade, será um dia feita desta maneira.
- Toda peça suscetível de ter uma falha, falhará no momento mais inoportuno e prejudicial.
- Não importa a dificuldade requerida para danificar um equipamento: será encontrado um meio de fazê-lo.
- Prever o pior é, em geral, o que há de melhor a fazer.
- Um número infinito de pessoas aparecerá de um número infinito de lugares, dentro de um intervalo infinitesimal de tempo para dizer o que deveria ter sido feito para evitar o acidente antes dele ter ocorrido.
- Nada pode ser feito a prova de burrice: os burros são extremamente engenhosos.
- Após ter apertado todos os trinta e seis parafusos de um flange, será percebido que a junta foi esquecida.
- Duas unidades idênticas, com funcionamento idêntico sob condições de ensaio idênticas funcionarão de modo completamente diferente após instaladas.

Estes “axiomas” exprimem de maneira muito precisa o fato de que, em segurança, se uma situação é *a priori* possível, é necessário considerá-la provável nas análises. Consequentemente, deve-se tentar limitar sua probabilidade de ocorrência ou minimizar a gravidade de suas conseqüências, e não tentar ignorá-la a custo de um grande esforço de justificação, cuja verificação quase nunca é possível.

G.12 MÉTODOS DE ANÁLISE E AVALIAÇÃO DA SEGURANÇA DE SISTEMAS

Pode-se identificar três tipos gerais de análises complementares para a avaliação do nível de segurança de sistemas industriais:

- a) Análise por Eventos;
- b) Análise por Zonas, e
- c) Análise Temporal.

Existem ainda métodos específicos aplicados a domínios bem definidos, tais como:

- a) Falhas Dependentes e de Causa Comum;
- b) Fatores Humanos;
- c) Mecânica (método da resistência-carregamento, mecânica probabilística da fratura); e
- d) Desenvolvimento de "Software".

G.13 TIPOS GERAIS DE ANÁLISES

A análise por eventos pretende identificar e avaliar os cenários de eventos que conduzem a eventos indesejados. Pode-se identificar quatro grandes grupos de métodos de análise por eventos:

- a) Métodos Estáticos Indutivos;
- b) Métodos Estáticos Dedutivos;
- c) Métodos Estáticos Combinados;
- d) Métodos Analíticos; e
- e) Métodos de Simulação.

A análise por zonas tem por objetivo identificar o local de ocorrência e o modo de propagação do evento indesejado devido à implantação geográfica de elementos perigosos ou particulares dentro do arranjo físico do sistema considerado. Seus métodos permitem especialmente identificar os modos de falha de causa comum devidos à implantação física de redundâncias.

A Figura G.2 permite visualizar os fundamentos e objetivos da análise por zona para três elementos A, B e C que podem se interfacear e propagar eventos indesejados.

FIGURA G.2: ANALISE POR ZONAS

Constata-se nesta figura que o elemento B está situado dentro do campo coberto pelos efeitos do elemento C. Os elementos que estão localizados na região hachurada podem então sofrer agressões provenientes dos efeitos dos elementos A e C.

A análise temporal introduz a dimensão do tempo à evolução de cenários (seqüências de eventos) perigosos e aos atrasos das ações de diminuição de riscos, considerando os quatro tempos:

- a) t_1 : atraso de aquisição de informação;
- b) t_2 : atraso de tratamento da informação;
- c) t_3 : atraso de decisão; e
- d) t_4 : atraso de colocação em segurança do sistema.

FIGURA G.3: ANÁLISE TEMPORAL

G.14 MÉTODOS ESTÁTICOS

Distingue-se dois tipos de processos estáticos dentro da análise de segurança de funcionamento de um sistema: indutivo e dedutivo.

No processo indutivo parte-se do particular para o geral. Face a um sistema e uma falha (ou uma combinação de falhas), estuda-se de modo detalhado os efeitos ou conseqüências desta falha (ou uma combinação de falhas) sobre o próprio sistema e/ou seu ambiente. Assim, por exemplo, as análises de conseqüências da perda de um motor de um avião ou de ruptura de uma tubulação do circuito primário de um reator nuclear são de natureza indutiva. Os principais métodos estáticos indutivos são:

- a) Análise Preliminar de Riscos APR;
- b) Análise de Modos de Falha e seus Efeitos AMFE;
- c) Método do Diagrama de Sucesso MDS;
- d) Método da Tabela de Verdade MTV;
- e) Método da Combinação de Panes Resumidas MCPR; e
- f) Método da Árvore de Conseqüências MACQ.

No processo dedutivo, parte-se do geral para o particular. Supondo-se que o sistema esteja em pane, serão buscadas as causas e modos de falha que conduzem ao estado de pane. A análise e investigações que se seguem à ocorrência de catástrofes, para encontrar suas causas, são de natureza dedutiva.

O principal método dedutivo é o Método da Árvore de Causas MAC. Pode-se também considerar como um método dedutivo para análise de segurança o chamado *Structured Analysis and Design Technic* SADT utilizado no projeto de sistemas para análise funcional e identificação das interfaces entre as partes componentes.

Identifica-se ainda o Método do Diagrama Causas-Conseqüências MDCC, que combina os processos indutivos (MACQ) e dedutivos (MAC).

A análise preliminar de riscos foi utilizada pela primeira vez nos EUA, no início dos anos 60, para análise de segurança de mísseis a propelente líquido. Ela foi em seguida

formalizada para a indústria aeronáutica, notadamente pela Boeing. Depois desta utilização, ela generalizou-se em numerosas indústrias: química, nuclear, aeronáutica e militar.

O método de análise de modos de falha e seus efeitos foi empregado pela primeira vez a partir dos anos 60 no domínio da aeronáutica, para analisar a segurança de aviões. Em seguida, a utilização deste método se generalizou em numerosos domínios industriais:

- a) este método é regulamentar para a análise de segurança de aviões nos EUA e na França; notadamente, ele foi empregado para a homologação dos aviões Concorde e Airbus (LIEVENS, 1976); ele igualmente serviu como método de base para a análise de segurança do módulo lunar;
- b) ele foi recomendado para a indústria nuclear dos EUA após o acidente de Three Mile Island (NRC, 1983);
- c) numerosos textos regulamentares e normas existem a seu propósito tais como: *Military Standards* nos EUA (DON, 1975) e guia elaborado pelo *Institute of Electric and Electronic Engineers* (IEEE, 1975);
- d) foi publicada pela *Commission Electrotechnique International* CEI uma norma internacional sobre o método (CEI, 1985);
- e) existe abundante literatura relativa a este método e às suas aplicações: inicialmente dentro dos domínios tradicionais da aeronáutica, espaço, nuclear, depois para química e outros domínios tais como o automóvel, mais recentemente.

Uma extensão do AMFE é a Análise de Modos de Falha, Efeitos e Criticidade AMFEC onde se considera a probabilidade de ocorrência de cada modo de falha e a classe de gravidade dos efeitos destas falhas (SAE, 1967). Pode-se assim assegurar que os modos de falha com efeitos graves tenham probabilidades de ocorrência suficientemente pequenas.

Outro método derivado do AMFE é a análise *Hazard and Operability* HAZOP, desenvolvido na Grã-Bretanha para a indústria química (HENLEY e KUMAMOTO, 1981).

O AMFE e AMFEC constituem análises preliminares que devem geralmente ser completadas pela utilização de outros métodos para identificação das combinações de falhas pertinentes.

A Figura G.4 esquematiza as etapas de elaboração de uma AMFE e a Figura G.5 detalha a etapa principal de estabelecimento de modos de falha de um componente e suas causas.

Historicamente, o MDS foi o primeiro a ter sido utilizado para analisar sistemas e permitir cálculos de confiabilidade. Sua origem se confunde com o desenvolvimento dos métodos matemáticos associados à confiabilidade (NRC, 1981; PAGÈS, 1981; DHILLON e SINGH, 1981). Seus limites entretanto foram em seguida percebidos, o que deu origem a métodos mais refinados como o MAC e o AMFE. Ele resta entretanto bastante utilizado para sistemas relativamente simples e não reparáveis.

A partir do MDC pode-se deduzir o Método de Desconto de Componentes, *Parts Count Reliability Prediction* (ANDERSON, 1976), largamente utilizado para sistemas eletrônicos, onde a falha de um componente provoca a falha de todo o sistema.

FIGURA G.4: ETAPAS DE UMA AMFE

FIGURA G.5: ESTABELECIMENTO DE MODOS DE FALHA DE UM COMPONENTE E SUAS CAUSAS

O MDS conduz a uma modelagem do funcionamento do sistema. O diagrama de sucesso obtido permite o cálculo, geralmente simples, da confiabilidade (ou disponibilidade) do sistema, suposto irreparável.

Este método é utilizável quando uma análise detalhada das causas de falha (e de suas combinações) não é requerida e quando há independência entre as falhas, existindo uma correspondência entre os modelos MDS e os modelos do método MAC.

O Método da Tabela de Verdade MTV, cujos aspectos matemáticos são bastante conhecidos nos domínios eletrotécnico e eletrônico, consiste em recensar todas as combinações de estados de funcionamento e de pane dos componentes, uns após outros e a estudar seus efeitos. Este princípio, aparentemente simples, revela-se entretanto rapidamente irrealizável para análise manual de grandes sistemas. Entretanto, aplicações foram desenvolvidas a partir deste método.

O MTV é teoricamente o método mais rigoroso que pode ser empregado, A tabela de verdade obtida pode ser objeto de uma redução de natureza booleana, obtendo-se assim as combinações pertinentes. Entretanto, o MTV não é mais aplicável quando o número de componentes aumenta, dado o enorme número de combinações a considerar. Porém, pode-

se imaginar sua aplicação a um nível de decomposição elevado do sistema, em especial ao nível de funções básicas.

Os inconvenientes deste método são reduzidos pela sua informatização, através do Método da Tabela de Decisão MTD (POLLACK, 1971), que lhe é derivado.

A AMFE só permite geralmente evidenciar as falhas simples e deve então ser completado pelo estudo das combinações de falhas que conduz a eventos indesejados. O MCPR é justamente o método que permite determinar de maneira indutiva estas combinações de falhas após a realização da AMFE. O conjunto de funcionamentos anormais (ou modos de falha) de um sistema é assim obtido.

Este método foi criado para a análise de segurança dos aviões Concorde e Airbus (LIEVENS, 1976). Os estudos desenvolvidos na área nuclear contribuíram para o desenvolvimento deste método, notadamente seus fundamentos teóricos (VILLEMEUR, 1988).

O método se caracteriza pela introdução de certos conceitos específicos: panes resumidas internas, panes resumidas externas, panes resumidas globais. A noção de “efeitos” permite estabelecer a ligação entre as panes e os funcionamentos anormais, os eventos indesejados, etc.

O Método da Árvore de Causas ou Árvores de Falhas (*Fault Tree*) foi desenvolvido no início dos anos 60 para avaliar e melhorar a confiabilidade do sistema de lançamento dos mísseis Minuteman, tendo eliminado vários pontos fracos deste projeto, sua utilização considerada então um grande êxito. Nos anos seguintes o método foi aperfeiçoado e formalizado por Haasl (HENLEY e KUMAMOTO, 1981).

A partir de 1965 o método foi generalizado aos mais diversos domínios de aplicação, podendo-se dizer hoje que é o método mais utilizado para a análise da confiabilidade, disponibilidade e segurança de sistemas. O método deu origem a um grande número de publicações técnicas das quais ressalta-se o guia de utilização elaborado para a Autoridade de Segurança Nuclear nos EUA (NRC, 1981).

O MAC tem por objetivo o recenseamento de todas as causas, de todas as falhas (e de suas combinações) que conduzam à ocorrência de um evento indesejado. Ele permite então identificar os pontos fracos de um projeto, constituindo igualmente um meio de representação da lógica das falhas. A existência de numerosos programas informáticos de cálculo associados a este método favorecem sua utilização.

Entretanto, seu emprego revela-se difícil, se não impossível, para a análise de sistemas elementares em interação e fortemente dependentes do tempo. Neste caso ele pode constituir um complemento útil aos outros métodos mais adaptados. Pode-se ainda dizer que a representação do método (árvore) é um excelente instrumento para comunicação entre equipes multidisciplinares.

O Método da Árvore de Conseqüências ou Árvore de Eventos (*Event Tree*) foi empregado pela primeira vez entre 1972 e 1975 para avaliação do risco associado às centrais nucleares a água leve nos EUA (NRC, 1975). Ele permite elaborar e avaliar seqüências de eventos conduzindo a um evento indesejado, chamadas "seqüências acidentais" e assim caracterizar a probabilidade das conseqüências associadas. Ele vem sendo crescentemente utilizado para a execução de Análises Probabilísticas de Segurança de instalações nucleares, sendo o principal método recomendado (NRC, 1983).

Este método é geralmente empregado em ligação com o Método da Árvore de Causas ou com o Método de Combinação de Panes Resumidas.

A Figura G.6 apresenta esquematicamente as etapas de elaboração das árvores de conseqüências através de um procedimento dedutivo.

O MDCC foi inicialmente elaborado para análise de confiabilidade e risco de centrais nucleares escandinavas, pelo laboratório Risø, na Dinamarca, no início dos anos 70, encontrando-se hoje consolidado pelo sistema computacional "Risk-Spectrum" desenvolvido pela empresa RELCON sueca (RELCON, 1994).

FIGURA G.6: ELABORAÇÃO DE UMA ÁRVORE DE CONSEQUÊNCIAS

Ruptura de uma tubulação do primário	Missão do reservatório comum aos 2 sistemas	Missão do sistema elétrico	Missão do sistema de injeção	Missão do sistema de aspersão	Sequências
--------------------------------------	---	----------------------------	------------------------------	-------------------------------	------------

FIGURA G.7: EXEMPLO DE ÁRVORE DE CONSEQUÊNCIAS

O caráter simultâneo da análise dedutiva das causas e da análise indutiva das consequências, combinando assim os princípios do MAC e do MACQ, revela o método como útil para análise de eventos inicializadores específicos, onde a ordem pela qual as falhas ocorrem tem grande influência sobre a ocorrência do evento indesejado.

A análise pelo método SADT (SCIENTECH, 1994) é realizada através da construção de um modelo de forma descendente, modular, hierárquica e estruturada, diferenciando o aspecto funcional (quais são as funções a serem asseguradas?) do aspecto material (com que meios o sistema realizará suas funções?). A coerência do conjunto dos vários níveis do diagrama realiza-se através de um programa. O interesse do método é o seguinte:

- a) fornecer uma modelização do sistema tão fina quanto for necessário,
- b) evidenciar para cada função o conjunto das interfaces com o resto do sistema, assim como com o seu meio,
- c) dissociar os aspectos funcionais da concepção do material.
- d) Em especial, destaca-se para cada função ou sub-função:
- e) dados de entrada que são transformados pela realização da função,
- f) saídas correspondendo à transformação dos dados de entrada,
- g) os mecanismos que permitem o desenrolar da função,
- h) as imposições do meio.

A aplicação do SADT começa com a descrição mais geral ou a mais abstrata do sistema. Essa função principal contida em uma caixa fragmenta-se em compartimentos mais detalhados, cada um representado uma função maior do compartimento inicial. Cada um desses compartimentos decompõe-se novamente para expor a informação que contém. As interfaces entre as várias funções são realizadas por flechas, definidas da seguinte maneira:

TABELA G.3: FUNÇÕES SADT

Entrada	E	Dados transformados ou utilizados pela função
Saída	S	Dados criados pela função
Mecanismo	M	Meios que realizam a função
Imposição	C	Imposições do desenrolar da função

G.15 MÉTODOS ANALÍTICOS E DE SIMULAÇÃO

Os métodos analíticos foram desenvolvidos particularmente para sistemas reparáveis, modelando o sistema considerado em um espaço de estados no qual a transição é feita segundo uma certa probabilidade. O método analítico por excelência é o Método do Espaço de Estados MEE, desenvolvido inicialmente para análise de processos do tipo Markoviano, e posteriormente estendido a processos Semi-Markovianos e Não-Markovianos (VILLEMEUR, 1988).

Os métodos de simulação podem ser interpretados como uma extensão dos métodos analíticos. Buscam a modelagem física das partes do sistema, das transições de estado de

cada parte e das ações de interface entre as partes segundo o estado em que se encontre. Associa-se então leis probabilísticas de transição de estados das partes, e eventualmente também das ações de interface, podendo-se assim determinar, através de tiragem aleatória do tipo Monte Carlo, as probabilidades dos estados do sistema, e destas sua disponibilidade e reparabilidade (NIMAL, 1991).

O método de simulação mais conhecido é o Método da Rede de Petri Estocástica MRPE (LEROY, 1992)].

O MEE foi desenvolvido para a análise da segurança de funcionamento de sistemas reparáveis. As primeiras utilizações no domínio industrial datam dos anos 50 e se aplicavam à classe particular de processos estocásticos ditos “processos de Markov”. Os processos não-Markovianos foram em seguida introduzidos.

Um processo estocástico é dito markoviano se para cada n e $t_1 < t_2 \dots < t_n$ (PAPOULIS, 1965):

$$P[x(t_n) \geq x_n \mid x(t_{n-1}), \dots, x(t_1)] = P[x(t_n) \geq x_n \mid x(t_{n-1})] \quad [G-10]$$

Considere-se um sistema constituído de n componentes, cada um tendo um número finito de estados de funcionamento e de pane. Este sistema é suposto reparável, sendo os componentes reparados após a constatação da pane. Ele possui então (CULMAN, 1975):

- a) estados de funcionamento: são os estados para os quais a função do sistema é realizada, podendo alguns dos componentes encontrarem-se em estado de pane; o estado de bom funcionamento é aquele no qual nenhum componente encontra-se em pane;
- b) estados de pane: são os estados para os quais a função do sistema não é mais realizada, estando um ou vários componentes em pane.

A análise compreenderá três partes:

- a) recenseamento e classificação de todos os estados do sistema em estados de funcionamento ou em estados de pane; se cada componente possui dois estados (funcionamento e pane) e se o sistema possui n componentes, o número máximo de estados é 2^n ; ao longo da vida do sistema os estados de pane podem aparecer em consequência de falhas ou desaparecer em seguida a reparos;

- b) O recenseamento de todas as transições possíveis entre estes diferentes estados e a identificação de todas as causas destas transições, que geralmente são devidas a falhas de um ou vários componentes do sistema, ou ao reparo de um componente;
- c) cálculo das probabilidades do sistema encontrar-se nos diferentes estados ao longo de um período de vida, ou seja, o cálculo das características de segurança de funcionamento do sistema (MTTF, MTTR, MUT, MDT, MTBF).

A análise qualitativa pode ser representada por um grafo de estados construído da seguinte maneira, conforme Figura G.8:

FIGURA G.8: GRAFO DE ESTADO DE UM SISTEMA COM UM COMPONENTE

- a) cada vértice representa um estado do sistema;
- b) cada arco simboliza uma transição entre dois vértices que une; a um arco é associada uma taxa de transição entre dois estados.

Se a probabilidade de passar diretamente do estado i ao estado j entre os instantes t e $t + dt$ é $a_{ij}dt$, a_{ij} é a taxa de transição entre os estados i e j . Quando as taxas de transição são constantes, o processo é dito markoviano homogêneo. No sistema de um componente representado pela Figura G.8 a taxa de transição (falha) $1 \rightarrow 2$ é dada por λ e a taxa de transição (reparo) $2 \rightarrow 1$ é dada por μ . Um sistema constituído por dois componentes em redundância ativa (Figura G.9) possui 4 estados:

- a) estado 1 (00): dois componentes em funcionamento;
- b) estado 2 (10): componente 1 em pane e componente 2 em funcionamento;
- c) estado 3 (01): componente 1 em funcionamento e componente 2 em pane; e
- d) estado 4 (11): dois componentes em pane.

FIGURA G.9: GRAFO DE ESTADOS PARA UM SISTEMA COM DOIS COMPONENTES

Constata-se neste grafo que, quando o sistema está no estado 4, ele pode ser reparado para retornar ao estado 2 ou 3. Este grafo está então adaptado à modelagem da disponibilidade do sistema.

A modelagem da confiabilidade do sistema necessita o cálculo da probabilidade do sistema encontrar-se num estado de funcionamento (1, 2 ou 3), sem ter transitado pelo estado de pane (4). Com este objetivo, os estados de pane são tornados "absorventes, suprimindo-se as transições para os estados de funcionamento. A Figura G.10 ilustra o grafo que modela a confiabilidade do sistema.

FIGURA G.10: GRAFO DE ESTADOS PARA CONFIABILIDADE

As principais vantagens das redes de Petri em relação aos gráficos de Markov são as seguintes (LEROY, 1992):

- a) A construção de um modelo por redes de Petri é mais simples graças à possibilidade de modelizar condições e mensagens que levam a um pequeno número de lugares e transições,
- b) Os resultados obtidos são cheios de informações, especialmente no que se refere ao número de tiragem de transições,

- c) Permitem integrar leis de transição descontínuas em função do tempo.

As redes de Petri são construídas com a ajuda de “lugares”, “transições”, “condições” e “mensagens” (ALLA e DAVIS, 1989):

- a) Os “lugares” representam os vários estados dos componentes de um sistema (funcionamento, parada, pane),
- b) As “transições” representam as passagens de um estado para o outro e são definidas por leis:

TABELA G.4: LEIS DE TRANSIÇÃO DAS REDES DE PETRI ESTOCASTICAS

Pane em funcionamento	lei L	funcionamento→pane
Pane na partida	lei G	parada→pane
Reparo	lei M	pane→funcionamento ou parada

- a) As “condições” são os dados que autorizam ou impedem a tiragem das transições,
- b) As “mensagens” são os novos dados após a tiragem das transições que serão retomadas como “condições” de outras tiragens de transições.

As “condições” e as “mensagens” permitem portanto representar a lógica do funcionamento de um sistema. Após ter fixado:

- a) A duração de funcionamento; e
- b) um número de “histórias” estatisticamente representativo,

o funcionamento do sistema pode ser simulado por tiragem de Monte Carlo. Os cálculos efetuados permitem então conhecer:

- a) O “tempo de permanência” nos vários lugares, ou seja a disponibilidade e a indisponibilidade (temporária ou definitiva) dos diversos componentes,
- b) O número de tiragem das “transições”, ou seja a probabilidade de ocorrência de cada fato elementar ou de cada fato temido.

G.16 VANTAGENS E INCONVENIENTES DOS DIVERSOS MÉTODOS

Análise de Modos de Falha e seus Efeitos (AMFE)

Vantagens:

- a) permite identificar sistematicamente os efeitos dos modos de falha das partes do sistema;
- b) fornece uma primeira lista dos modos de falha (e de suas causas) que comprometem a segurança de funcionamento;
- c) pode ser prolongado por uma Análise de Modos de falha, seus Efeitos e suas Criticidades (AMFEC), que permite classificar os modos de falha segundo o conjugado (probabilidade, gravidade).

Inconvenientes:

- a) o um volume de trabalho exigido para sua realização pode ser muito grande, eventualmente incompatível com os benefícios esperados de seus resultados;
- b) evidencia somente as falhas simples;
- c) não conduz a um modelo para a avaliação quantitativa da segurança de funcionamento.

Método do Diagrama de Sucesso (MDS)

Vantagens:

- a) o diagrama de sucesso pode ser obtido, quase diretamente, a partir do diagrama funcional;
- b) as combinações de falhas que comprometem a função do sistema são facilmente identificadas;
- c) o cálculo da confiabilidade de um sistema não-reparável é facilmente realizado a partir do diagrama de sucesso;
- d) um cálculo aproximado da disponibilidade de um sistema reparável pode ser realizado quando existe independência entre as partes do sistema considerado.

Inconvenientes:

- a) não é adaptado à análise de relações complexas entre efeitos e causas de falhas;
- b) não permite tratar sistemas reparáveis que possuam estratégias complexas de manutenção.

Método da Tabela de Verdade (MTV)

Vantagens:

- a) conduz a um estudo sistemático de todas as combinações de falhas das partes do sistema;
- b) um cálculo de probabilidade é facilmente efetuado a partir da Tabela de verdade;

- c) o Método da Tabela de Decisão (MTD), que lhe é derivado, permite levar em conta partes do sistema possuindo mais de dois estados e de realizar automaticamente uma análise para certos sistemas;

Inconvenientes:

- a) não é aplicável a sistemas que possuam grande número de partes;
- b) não é adaptado à análise de relações complexas entre efeitos e causas de falhas;
- c) não é adaptado à análise de um sistema reparável.

Método da Combinação de Panes Resumidas (MCPR)

Vantagens:

- a) permite identificar todos os modos de funcionamento anormal e todos os modos de falha de um sistema;
- b) conduz a uma análise detalhada das causas e dos efeitos das falhas (e de suas combinações);
- c) permite analisar um conjunto de sistemas elementares em estreita interação e de evidenciar todas suas interações;

Inconvenientes:

- a) a análise pode ser muito longa e pesada;
- b) é dificilmente utilizável para sistemas "muito seqüenciais" ou tendo estratégias complexas de manutenção;
- c) a análise quantitativa pode necessitar a utilização de outros métodos.

Método da Árvore de Conseqüências (MAC)

Vantagens:

- a) permite identificar todas as conseqüências de um evento inicializador;
- b) fornece a probabilidade das seqüências de eventos inaceitáveis; este cálculo é facilitado quando todos os eventos são independentes, porém complexo no caso contrário (utilização, por exemplo, de processos semi-markovianos)
- c) evidencia as interações entre sistemas elementares.

Inconvenientes:

- a) não permite demonstrar a exaustividade dos eventos inicializadores;
- b) necessita geralmente da utilização de outros métodos para a análise dos eventos genéricos;
- c) não permite considerar estratégias de manutenção complexas sobre os sistemas elementares que intervêm para o controle do evento inicializador.

Método da Árvore de Causas (MAC)

Vantagens:

- a) permite identificar todas as causas (e suas combinações) de falhas conduzindo a um evento indesejado;
- b) evidencia certas formas de dependência entre falhas
- c) fornece a lista de cortes mínimos de um evento indesejado;
- d) permite geralmente realizar um cálculo da probabilidade de ocorrência de um evento indesejado
- e) aplica-se a uma grande variedade de sistemas.

Inconvenientes:

- a) pode conduzir a árvores de causas de tamanho considerável e difíceis de serem tratadas, mesmo através de códigos computacionais;
- b) nem sempre permite identificar, para um sistema complexo, as seqüências de falhas que conduzem a um evento indesejado;
- c) não permite tratar sistema reparáveis que possuam estratégias de manutenção complexas.

Método do Diagrama Causas-Conseqüências (MDCC)

Vantagens:

- a) permite identificar simultaneamente as causas e conseqüências de um evento inicializador;
- b) evidencia as dependências entre as causas e as conseqüências de um evento inicializador;
- c) possui, teoricamente as vantagens tanto do MAC como do MACQ.

Inconvenientes:

- a) a análise quantitativa combina as análises quantitativas do MAC e do MACQ, implicando que o cálculo automático via códigos computacionais somente pode ser feito para diagramas causa-consequência particulares;
- b) sua utilização é difícil para um conjunto complexo de sistemas elementares.

Método do Espaço de Estados (MEE)

Vantagens:

- a) permite identificar todos os estados de funcionamento e de pane de um sistema reparável, assim como todas as suas transições;
- b) fornece medidas de confiabilidade, disponibilidade e manutibilidade de um sistema reparável;
- c) considera estratégias complexas de manutenção.

Inconvenientes:

- a) a análise quantitativa pode tornar-se muito complexa, até mesmo impossível, para um sistema que comporte um grande número de estados;
- b) a análise quantitativa somente é relativamente fácil para os processos markovianos e semi-markovianos.

G.17 COMPARAÇÃO DOS DIVERSOS MÉTODOS

Para os métodos de análise apresentados, distingue-se:

- a) características intrínsecas, independentes *a priori* daquelas do sistema a ser analisado;
- b) características dependentes do sistema a ser analisado.

A Tabela G.5 ilustra a comparação entre os métodos sob diferentes aspectos das características intrínsecas.

Quanto à classificação quanto a natureza do método, ela é relativa aos princípios. Em realidade, na prática, os métodos são de natureza mista, por exemplo:

- a) AMFE: a pesquisa de causas dos modos de falha é sobretudo de natureza dedutiva;
- b) MAC: o analista não poderá impedir-se de examinar os efeitos dos eventos intermediários e dos eventos de base evidenciados.

Quanto às maneiras de apresentação associadas ao método, somente a MCPR não possui meios específicos. É entretanto importante distinguir o método de seu meio de apresentação: assim, uma árvore de causas pode muito bem ser utilizada como representação de uma pane resumida obtida pela MCPR.

TABELA G.5: COMPARAÇÃO DE CARACTERÍSTICAS INTRINSECAS DOS
METODOS

	NAT.			EVENTOS INICIAIS	comb ?	REPRE- SENTAÇÃO
	I	D	M			
AMFE	S			modos de falha componentes	N	tabelas de análise
MDS		S		funções do sistema	S	diagrama de sucesso
MTV	S			modos de falha componentes	S	tabela de verdade
MAC		S		evento indesejado	S	árvore de causas
MACQ	S			evento inicializador	S	árvore de consequências
MCPR	S			modos de falha componentes	S	xx
MDCC			S	evento inicializador	S	diagrama causas- consequências
MEE	S			estados de funcionamento e de pane	S	grafo de estados (Markov)
nat. = natureza do método: I = indutivo, D = dedutivo, M = misto						
comb.? = pesquisa de combinações de falhas?						

Certas Características Dependentes do sistema a ser analisado auxiliam o analista a escolher o método a ser utilizado:

- a) Sistema não-reparável: para um tal sistema, todos os componentes são considerados como irreparáveis dentro dos limites de uma função dada; note-se que um sistema pode ser considerado irreparável para uma função dada e reparável para outra: por exemplo, no caso de um acidente A_1 , um sistema de segurança, sobre o qual é possível fazer-se reparos, deve operar durante 1 hora; este tempo, muito curto para que seja feita qualquer manutenção, conduz a considerá-lo não reparável; entretanto, para um acidente A_2 , deve operar durante 24 horas, quando então poderá ser considerado como reparável.

Estes sistemas são os de análise mais simples, e praticamente todos os métodos são utilizáveis. Note-se que o MEE também pode ser utilizado, com precaução, para os sistemas parcialmente reparáveis, onde certos estados não possuem transição de reparo.

- b) Sistema reparável: em diversos graus, os métodos apresentados podem tratar os sistemas reparáveis.
- AMDE: pela identificação dos modos de falha que dão lugar a uma manutenção, ele permite um julgamento parcial da manutibilidade do sistema;
 - MDS: a disponibilidade de um sistema reparável pode ser calculada quando existe independência entre as partes;
 - MAC: pode tratar sistemas reparáveis, mesmo complexos; a análise quantitativa supõe independência entre as partes; para considerar estratégias complexas de manutenção, por exemplo, a existência de um só reparador para numerosas partes, a MEE torna-se indispensável;
 - MACQ: o evento inicializador e os eventos genéricos podem ser associados a sistemas reparáveis; admite-se entretanto, como regra geral, a independência entre estes eventos;
 - MCPR, MDCC: a análise quantitativa pode levar em conta o caráter reparável das partes;
 - MEE: é o método por excelência para tratar sistemas reparáveis; ele torna-se insubstituível para a consideração de estratégias complexas de manutenção.
- c) Sistema seqüencial: para um sistema seqüencial, o sucesso da missão depende diretamente da ordem pela qual surgem as falhas; geralmente, os métodos indutivos são mais adaptados a estes sistemas que os métodos dedutivos, e isto é tanto mais notável quanto a complexidade do sistema aumenta; com efeito, torna-se difícil identificar as causas de falha, por exemplo com auxílio do MAC, quando as causas devem se produzir segundo uma seqüência complexa; por isto as árvores de causas foram há muito abandonadas para análise de quedas de aviões e de fusão do núcleo de reatores nucleares.
- d) Sistema multi-fases: a análise de um tal sistema é complicada; somente os métodos mais elaborados como o MAC, MACQ e MEE podem tratá-los em certas condições

G.18 CRITÉRIOS DE SELEÇÃO DE MÉTODOS

Numeroso critérios intervêm na escolha de um ou vários métodos de análise: eles são ditados por imperativos técnicos ou pelo hábito ou familiaridade dos analistas. Classifica-se os critérios de escolha de acordo com fatores determinantes:

- a) Critérios ligados aos objetivos da análise: - avaliação de confiabilidade, de disponibilidade, de manutibilidade ou de seguridade? - o evento indesejado é conhecido? existem outros eventos indesejado a serem considerados? - é necessário uma quantificação? Ou uma análise qualitativa pode ser suficiente? Uma definição clara dos objetivos conduz geralmente a limitar a lista de métodos de passível utilização.
- b) Critérios ligados ao sistema a analisar: a natureza do sistema e sua complexidade são elementos importantes na escolha dos métodos; deve-se notar que a complexidade não é forçosamente ligada diretamente ao número de partes componentes: um sistema constituído de um grande número de partes que podem ser agrupadas em macro-componentes pode-se revelar de fácil análise; o que realmente complica a análise são fatores tais como a existência de redundâncias, as possibilidades de intervenção humana em operação, o caráter reparável dos componentes, a presença de "software". Uma primeira análise funcional e técnica se demonstra indispensável antes de uma decisão sobre a seleção de métodos, examinando as propriedades do sistema (reparável, não-reparável, sequencial).
- c) Critérios ligados às análises já realizadas: os projetistas e operadores não aguardaram análises de segurança para prever panes e acidentes, e conseqüentemente levá-los em conta quando do projeto e da operação dos sistemas existentes; deste modo, para uma central nuclear, por exemplo, a lista de incidentes e acidentes considerados para dimensionamento constitui uma primeira lista de eventos inicializadores. De uma maneira geral, todo conhecimento acumulado em matéria de previsão do comportamento do sistema constitui um elemento importante à orientação da seleção de métodos.
- d) Critérios ligados aos recursos de análise: com relação aos objetivos, os métodos têm eficácias diferentes e requerem meios também diferentes; convém adaptar-se desde o início os métodos aos recursos disponíveis, tanto em especialistas e códigos computacionais, como em termos de bancos de dados de funcionamento; deste modo, é

ilógico adotar métodos quantitativos sofisticados se não dispõe de dados conhecidos com grande grau de confiança.

G.19 MÉTODOS ESPECÍFICOS

Métodos de Análise de Falhas Dependentes

Os principais métodos de análise previsional apresentados anteriormente permitem evidenciar as dependências entre falhas. Entretanto, a relativa dificuldade de previsão de todas estas dependências conduz a multiplicar as abordagens a utilizar métodos mais específicos.

As vantagens diversas destes métodos, classificadas segundo o nível de seus efeitos sobre um conjunto de sistemas em interação são resumidos pela Tabela G.6, onde o sinal + dá uma indicação aproximada e qualitativa do interesse de cada um destes métodos.

TABELA G.6: INTERESSE DOS METODOS DE ANALISE PREVISIONAL PARA
FALHAS DEPENDENTES

	AMDF	MAC	MCPR	MACQ
Iniciadores externas				
Iniciadores internos			+	+
SISTEMAS ELEMENTARES				
Dependências funcionais			+	+
Dependências equipamentos comuns			+	+
Interações físicas			+	+
Dependências ações humanas			+	+
COMPONENTES				
Dependências funcionais	+	+	+	+
Dependências equipamentos comuns	+	+	+	+
Interações físicas	+	+	+	+
Dependências de ações humanas		+	+	+

Numerosos outros métodos específicos têm sido desenvolvidos para análise de falhas dependentes. Eles podem ser agrupados em três famílias principais:

- a) análises particulares de eventos inicializadores de falhas dependentes;
- b) análises de causas genéricas; e
- c) análise da experiência de operação.

Os estudos particulares de eventos inicializadores de falhas dependentes têm por objetivo analisar em detalhe os efeitos de eventos externos (queda de aeronaves, sismo, etc.) ou de eventos internos (acidentes de dimensionamento, perda de quadros elétricos, chicoteamento de tubulações, etc.) do sistema, para limitar suas conseqüências, tornando-as aceitáveis. Eles permitem dimensionar adequadamente os sistemas elementares e os componentes afetados.

As análise de causas genéricas têm por objetivo prever a ocorrência e os efeitos de falhas de causa comum provocadas por uma ou várias causas genéricas. Dentre estas análises pode-se citar:

- a) análise previsional de causas genéricas (ANCELIN, 1994), onde o analista busca a identificação das falhas sobre o sistema guiado pela classificação apresentada anteriormente; para as fontes potenciais de falhas, o analista verifica as disposições construtivas que permitem enfrentar estas falhas;
- b) análise por zonas (LIEVENS, 1976), que tem por objeto analisar as dependências entre falhas que resultam da localização "geográfica" de certos componentes ou subsistemas; ela utiliza: - os procedimentos de instalação; - o arranjo físico de componentes; - a identificação de panes possíveis; - identificação dos erros de manutenção.
- c) análise de fatores humanos, que devido a sua importância é objeto de métodos especiais.

A análise detalhada da experiência de operação é uma fonte inesgotável de falhas dependentes. Ela necessita a coleta padronizada e sistemática de todos os incidentes afetando componentes e sistemas. A riqueza desta análise depende muito da qualidade desta coleta de dados.

Para o cálculo das probabilidades das falhas dependentes e de causa comum, identifica-se dois tipos de métodos:

- a) métodos explícitos, baseados sobre um conhecimento preciso das causas destas falhas, que permitem a aplicação da fórmula geral das probabilidades condicionadas; e
- b) métodos paramétricos, que são baseados na modelagem estatística das falhas, sem pesquisa e enumeração de suas causas.

Identificam-se três métodos paramétricos, que tratam sobretudo as falhas de causa comum:

- a) método do parâmetro β (FLEMING, 1983);
- b) método das letras gregas múltiplas (FLEMING, 1985); e
- c) método dos choques (ATWOOD, 1984).

Os resultados da análise da experiência de operação de sistemas de segurança de centrais nucleares mostra a proporção relativamente elevada destas falhas dependentes nos incidentes e incidentes efetivamente ocorridos. Eles demonstram que os ganhos em disponibilidade ou em confiabilidade proporcionados pelas redundâncias são inferiores àqueles teoricamente previstos. Assim, para os componentes mais comuns nos sistemas de segurança, tais como bombas, válvulas, motores, o ganho pode ser estimado de 5 a 20 para uma redundância de ordem 2. Um aumento da redundância, até a ordem de 3 ou 4, conduz a ganhos suplementares muito limitados, no máximo da ordem 2 a 10. A partir daí os ganhos são marginais (MESLIN e BOURGADE, 1987).

A título indicativo e sem pretensão de exaustividade, indica-se a seguir alguns meios de prevenção geralmente utilizados para reduzir a importância destas falhas:

- a) Durante a fase de projeto:
 - Prevenção de inicializadores que originem falhas de causa comum: disposições construtivas para controlar os efeitos de: - ambiente e suas agressões; - ambiente accidental de origem interna à instalação, os principais acidentes plausíveis ou hipotéticos sendo considerados no projeto de modo conservativo
 - Prevenção das dependências entre sistemas elementares: - separação física e geográfica dos sistemas redundantes; - separação das funções de segurança asseguradas por sistemas diferentes; - diversidade funcional e diversidade de sistemas; - sistemas auxiliares diferentes; - possibilidade de testes periódicos; - otimização da interface homem-máquina (automação das ações humanas que não podem ser no tempo requerido com uma confiabilidade suficiente, procedimentos operacionais claros, precisos e comprovados em simulador, consideração dos erros humanos previsíveis); - pesquisa sistemática das dependências por métodos de análise previsional;

- Prevenção das dependências entre componentes: - separação física e geográfica de componentes redundantes; - diversidade de componentes redundantes (projetistas e fabricantes diferentes); - modos de falha seguros dos componentes; - possibilidade de testes periódicos; - pesquisa sistemática das dependências por métodos de análise previsional;

b) Durante a fase de operação:

- Prevenção das falhas dependentes pela análise sistemática e detalhada de todos os incidentes e acidentes ocorridos sobre a instalação e sobre instalações semelhantes;
- Prevenção de erros humanos: - formação e treinamento e motivação dos operadores, presença de vários operadores, realização de diagnósticos de incidentes por duas equipes independentes e separadas, utilizando meios diferentes; - interdição da manutenção simultânea de componentes redundantes, controle por outras equipes da manutenção efetuada sobre componentes importantes.

Fatores Humanos

O homem está sempre presente nas instalações industriais, quer seja ao nível de seu projeto ou ao nível de sua operação. Deve-se também considerar o sistema homem-máquina dentro do qual o homem é um componente. Constata-se que os erros humanos estão presentes em todas as etapas do ciclo de vida de um sistema: erros de projeto, de cálculo, de montagem, de manutenção, de operação. Daí a importância da avaliação previsional da confiabilidade humana, análise que tem progressivamente se desenvolvido tanto ao nível de métodos como de dados a partir dos anos 60. Torna-se necessário então estudar em profundidade o comportamento do operador humano, esquematizado pela Figura G.11.

O procedimento mais utilizado na indústria nuclear para avaliação previsional da confiabilidade humana é o de (NRC, 1983). Existem entretanto outros métodos, geralmente menos completos, porém melhor adaptados a problemas particulares.

FIGURA G.11: REPRESENTAÇÃO ESQUEMÁTICA DO COMPORTAMENTO DO OPERADOR HUMANO

Com o objetivo de guiar o utilizador, o *Electric Power Research Institute* EPRI, dos EUA, desenvolveu *Systematic Human Action Reliability Procedure* SHARP (HANNAMAN, 1984), que auxilia na escolha entre os diferentes métodos e à condução sistemática e verificável do análise.

Mecânica das Estruturas

O desenvolvimento de grandes estruturas mecânicas, tais como vasos de pressão de reatores eletro-nucleares e plataformas oceânicas de petróleo, em geral únicas ou construídas em número muito reduzido, cuja ruptura pode conduzir a consequências muito graves, e para as quais um super-dimensionamento pode demonstrar-se técnica ou economicamente inviável, necessita dispor de métodos de avaliação previsional de sua confiabilidade.

A alta qualidade requerida para estas estruturas e seu pequeno número tornam difícil, se não impossível, a utilização de métodos estatísticos. O único meio de avaliar sua fiabilidade reside então no desenvolvimento de modelos probabilísticos do comportamento mecânico destas estruturas.

Identifica-se então dois modelos probabilísticos que permitem modelar o comportamento mecânico das estruturas, segundo o tipo de carregamento a que são submetidas:

- a) Método da Resistência/Carregamento (R/C), que trata estas duas variáveis como aleatórias e determina a função distribuição de probabilidade da relação R-C (Figura G.12), que caso negativa implica na ruína da estrutura (HAUGEN, 1968; LIGERON, 1979; DESROCHES, 1992);
- b) Mecânica Probabilística da Fratura, que trata os problemas associados a propagação de trincas em componentes submetidos a carregamentos cíclicos de fadiga (coeficiente K_I de amplificação de tensões e K_{IC} de tenacidade, ou resistência à propagação brutal de uma trinca).

FIGURA G.12: METODO DA RESISTENCIA-CARREGAMENTO

Desenvolvimento de "Software"

O tamanho crescente dos códigos computacionais e sua penetração em praticamente todos os setores industriais tornam crucial o problema de sua confiabilidade. Se considerarmos os "softwares" de automação e controle de instalações industriais e veículos, à confiabilidade, associada ao sucesso da missão, soma-se a segurança, pois uma falha pode conduzir a um evento indesejado com conseqüências catastróficas.

Tais constatações conduziram os projetistas de códigos a desenvolver numerosas técnicas para obter programas o mais confiáveis possível, já a partir dos estágios iniciais de seu projeto. Deste modo, progressivamente foram sendo desenvolvidos procedimentos de projeto e de desenvolvimento abordando temas tão diversos quanto as linguagens e os

métodos de programação, a redação e validação das especificações funcionais. Estes métodos de criação são entretanto considerados insuficientes e testes tão completos quanto possível são efetuados para melhorar a qualidade e confiabilidade dos códigos.

Apesar de todos estes métodos, é difícil, se não impossível, garantir que um código não contém nenhuma falha. Paralelamente a estes métodos, tem sido então desenvolvidos trabalhos no sentido de medir a "confiança" que pode ser atribuída a um programa (MCLEOD e RIVERA, 1996).

ANEXO H

ALOCAÇÕES DE SEGURANÇA

H.1 CONCEITO

As alocações de segurança , têm por objetivo repartir o esforço correspondente à componente probabilidade do objetivo de segurança designado à missão (ou atividade) sobre o conjunto das partes do sistema que a realizam através de modelagem funcional, material e operacional.

O objetivo do procedimento de alocações de segurança é dar às diferentes equipes participantes do desenvolvimento de um sistema, um conjunto de requisitos de projeto, construção e operação definidos ao seu nível de responsabilidade.

O diagrama de Farmer descreve, para cada classe de gravidade G_k , a probabilidade máxima admissível P_k que lhe é associada. Este par (G_k, P_k) define um dos objetivos de segurança da missão. Para um objetivo missão de classe k , o procedimento de alocação consiste em repartir sobre as arquiteturas das partes do sistema, o peso em probabilidade de sua participação possível na ocorrência P_k do evento indesejado considerado, através dos cenários de acidente identificados que a ele conduzem.

Este procedimento se faz por etapas, a partir do objetivo de segurança da missão, tendo características simultaneamente objetivas e subjetivas. Ele é objetivo na medida que as análises diversas já realizadas permitiram identificar os elementos confiáveis e os cenários deterministas a partir de um eventual retorno da experiência. Ele é subjetivo porque o conjunto das arquiteturas individuais das partes do sistema somente são conhecidas e propostas após a realização das alocações preliminares, o que implica integrar uma parte de subjetivismo às decisões.

Para um elemento dado, os principais critérios que intervêm no procedimento de alocação são:

- a) peso (importância) na realização de um cenário crítico ou catastrófico;
- b) complexidade tecnológica;

- c) confiabilidade (se ela é conhecida ou alocada);
- d) característica: elemento funcional da missão, barreira de segurança, elemento funcional de segurança;
- e) duração de funcionamento para a missão considerada.

As características devem ser estabelecidas para os cenários em funcionamento nominal (excluídas falhas e agressões externas) e não nominais (falhas, agressões externas). O procedimento de alocação é interativo e deve ser realizado a todos os níveis considerados no desenvolvimento do sistema. O tipo do procedimento de alocação pode variar de um nível a outro segundo a natureza da etapa e o nível de conhecimento.

H.2 PRINCIPAIS MÉTODOS

Equi-repartição de Riscos

Consiste num modo de alocação preliminar, que não leva em conta os riscos específicos relativos às interfaces externas e aos ambiente de referência.

Considerando-se uma missão formada por n fases, ou um sistema formado por n sistemas elementares, ou uma cadeia funcional ou material formada por n elementos, para um objetivo de segurança p_0 de nível missão, sistema ou cadeia, e na ausência de qualquer informação complementar, o objetivo alocado para cada fase, sistema elementar ou elemento será p_0/n .

Por exemplo, se a duração da missão do sistema é de 100 horas e que o objetivo de segurança associado a ocorrência do evento indesejado E é $p_0 < 10^{-5}$, teremos:

- a) a probabilidade de ocorrência de E deve ser menor ou igual a 10^{-7} por hora de missão:

$$p_H < (10^{-5}/100) / h$$

- b) se análise da missão permite decompô-la em 10 fases, a probabilidade de ocorrência de E em qualquer fase da missão deve ser menor ou igual a 10^{-6} :

$$p_\phi = (10^{-5} / 10) = 10^{-6} / \text{fase} \quad \text{este objetivo}$$

seria o mesmo qualquer que seja a duração e a criticidade da fase; para contornar este inconveniente, pode-se ponderar o objetivo médio por fase integrando a duração de uma fase. Se t_i é a duração em horas da fase ϕ_i , então: $p\phi_i = 10^{-7} \cdot t_i$

note-se que este ajuste continuaria a não considerar a criticidade de cada fase.

- c) se o sistema deve realizar 20 funções para cumprir a missão, a probabilidade de ocorrência de E em seguida à falha de uma função qualquer deve ser menor ou igual a $5 \cdot 10^{-7}$ durante a duração da missão:

$$p_f < (10^{-5} / 20) = 5 \cdot 10^{-7} / \text{função} \quad \text{este}$$

objetivo não levaria em conta a criticidade da função;

- d) se o sistema pode ser decomposto em 10 sistemas elementares, a probabilidade de ocorrência de E em seguida a uma falha de um subsistema deve ser menor ou igual a 10^{-6} durante a duração da missão:

$$p_s < (10^{-5} / 10) = 10^{-6} / \text{sistema} \quad \text{este}$$

objetivo não levaria em conta a criticidade dos sistemas elementares nem seu peso na ocorrência de E

O método de equi-repartição de riscos não leva em consideração o peso de cada função, sistema elementar e fase na ocorrência do evento indesejado. Para contornar este inconveniente, três métodos são considerados:

- a) Ponderação *a priori*;
- b) Ponderação por Número de Relações Estruturais;
- c) Ponderação pelos Objetivos ou Avaliações de Confiabilidade.

Ponderação *a priori* de Riscos

A alocação por ponderação ‘a priori’ usa as técnicas Delphi. A cada fase, função ou sistema elementar é designada uma fração ‘a priori’ aceitável do objetivo de segurança de nível superior, através de coeficientes de ponderação V_i .

Seja um sistema S realizando uma missão com um objetivo de segurança igual a p. Se a análise funcional sucinta permite identificar n funções (ou fases ou sistemas elementares) para executar a missão, vários tipos de coeficientes de ponderação poderão lhe ser associados:

- a) a_i : coeficiente de complexidade, que caracteriza globalmente a exequibilidade dos elementos executando a função f_i considerada; associa-se também a este coeficiente os

aspectos ligados à inovação e a condições diferentes de funcionamento; a escala proposta para os níveis de complexidade a_i seria 1 (fraco), 2 (médio) e 3 (forte);

- b) b_i : coeficiente de criticidade que caracteriza o peso ‘a priori’ da função f_i na ocorrência do evento indesejado; a escala proposta para os níveis de criticidade a_i seria 1(fraco), 2(médio) e 3 (forte).

Adicionalmente faz-se as seguintes hipóteses:

- a) quanto mais uma função é potencialmente crítica, mais ela intervém potencialmente na ocorrência do cenário de acidente, o que leva a ser mais restritivo no objetivo que lhe é alocado;
- b) mais uma função é complexa a ser executada, mais é necessário conferir-lhe peso através de um objetivo restritivo.

Esta última hipótese não é independente do fato que quanto mais uma função é complexa a executar, maior sua incerteza em termos de falhas e portanto mais ela é geradora de risco. Isto é tanto mais verdadeiro quanto a maturidade de sua tecnologia.

Segue-se que, a partir do objetivo p_0 , o objetivo alocado a função f_i seria:

$$p_i = V_i \cdot p_0, \text{ com } \sum V_i = 1$$
$$\text{onde } V_i = [(a_i / c_i) / \sum (a_i / c_i)]$$

Ponderação de Riscos por Número de Relações Estruturais

A Ponderação por Número de Relações Estruturais é baseada numa avaliação ‘a priori’ destas relações, entendidas como uma ligação possível de interface direta ou indireta entre elementos do sistema. Uma tal ligação é o ponto potencial de encaminhamento direto ou após transferência de um conjunto de agressões internas ao sistema (conjunto de caminhos críticos).

A partir desta avaliação por fase, função ou sistema elementar, pode-se deduzir por cada um o objetivo a alocar. Seja N_k o número de relações estruturais da fase ϕ_i . Fazendo a hipótese (que pode ser modulada) de equi-probabilidade p_c de ocorrência de cada um deles:

$$p_k = N_k \cdot p_c$$
$$p_0 = \sum_{k=1,n} p_k = \sum_{k=1,n} N_k \cdot p_c = p_c \cdot \sum_{k=1,n} N_k$$

$$p_c = p_0 / \sum_{k=1,n} N_k$$

$$p_k = (N_k / \sum_{k=1,n} N_k) \cdot p_0$$

o parâmetro $(N_k / \sum_{k=1,n} N_k)$ é chamado número ponderado de relações estruturais.

Na ausência de informação ‘a priori’, este modo de alocação preliminar é o mais realista pois a cada fase ele já associa os riscos potenciais, independentemente da sua duração.

A Figura H.1 apresenta um exemplo de determinação do número de relações estruturais de um sistema formado por um veículo tripulado V, uma base B, um sistema elementar perigoso D e um ambiente de referência R. Identifica-se neste caso 7 relações estruturais que convergem sobre a tripulação.

FIGURA H.1: RELAÇÕES ESTRUTURAIS

Ponderação de Riscos por Objetivos ou Avaliações de Confiabilidade

A Ponderação pelos Objetivos ou Avaliações de Confiabilidade permite beneficiar a segurança com os esforços empreendidos ou a empreender para o sucesso técnico da missão. Este método requer as seguintes informações prévias:

- a) conhecimento do sistema e de seus sistemas elementares;
- b) duração da missão e situações potencialmente perigosas;
- c) objetivo geral de segurança p_0 associado a um acidente dado A;
- d) objetivos ou avaliações de confiabilidade R_i dos n sistemas elementares S_i .

Sejam os eventos D (situação potencialmente perigosa na fase considerada), S_i (falha do sistema elementar S_i dentre os n existentes) e A (acidente):

$$\begin{aligned} P(A) &= P(D) \cdot \sum_i P(A \cap (S_i \cup \bar{S}_i)) \\ &= P(D) \cdot \sum_i [P(S_i) \cdot P(A | S_i) + P(\bar{S}_i) \cdot P(A | \bar{S}_i)] \end{aligned}$$

Existem então dois tipos de configurações de acidente: resultante de um ambiente de referência inadaptado, de um sub-dimensionamento de desempenho em projeto ou de uma operação inadequada, sem falha de S_i (Tipo 1) e resultante de falha de S_i (Tipo2). Sendo $P(D)$ a fração do tempo em que a situação é perigosa e $P(S_i)$ a desconfiabilidade do sistema elementar S_i na fase considerada, teremos:

$$\begin{aligned} p_1 &= \sum_i P(S_i) \cdot P(A | S_i) = a \cdot p_0 / P(D) \\ p_2 &= \sum_i P(\bar{S}_i) \cdot P(A | \bar{S}_i) = (1 - a) \cdot p_0 / P(D) \end{aligned}$$

onde a é a proporção verossimilhante entre os eventos do tipo 1 e do tipo 2, p_1 e p_2 são os pesos em probabilidade associados ou alocados a parte do acidente devido a estes eventos.

A avaliação das probabilidade associadas à ocorrência de eventos tipo 1 é feita diretamente por tratamento estatístico. Para eventos tipo 2, define-se ‘a priori’ para cada sistema elementar um peso b_i , tal que:

$$P(\bar{S}_i) \cdot P(A | \bar{S}_i) = b_i \cdot p_2 \text{ com } \sum_i b_i = 1$$

onde $P(S_i) = 1 - R_i = F_i$ é a desconfiabilidade alocada ou avaliada do sistema elementar S_i .

O objetivo de segurança, condicionado pela confiabilidade, que deve ser alocado ao sistema S_i será então:

$$q_i = P(A | \bar{S}_i) = (b_i / F_i) \cdot p_2$$

b_i é a parte verossimilhante de insegurança associada ao sistema elementar S_i , correspondendo à probabilidade condicional a posteriori $P(S_i | A)$ da fórmula de Bayes. O valor de b_i é inversamente proporcional ao peso relativo sobre o acidente que o especialista atribui ao sistema elementar S_i .

Os resultados obtidos são os valores dos objetivos detalhados de segurança alocados aos sistemas elementares e, por iteração, aos subsistemas, componentes e itens.

Para exemplificar o procedimento, seja um sistema composto por três sistemas elementares $\{S_1, S_2, S_3\}$ preponderantes com respeito ao acidente A considerado. Sendo $P_0 = 10^{-5}$ por missão para o sistema, $F_1=10^{-2}$, $F_2=5.10^{-2}$, $F_3=5.10^{-3}$ e a probabilidade de encontrar-se em situação perigosa durante a missão é $P(D)=10^{-2}$:

- a) Hipótese 1: o projeto do sistema e o ambiente operacional são bastante conhecidos; em seguida um peso preliminar de 10% ($a=0,1$) ligado à utilização pode ser designado à ocorrência do acidente em condições normais de funcionamento; os objetivos preliminares de segurança em condição normal serão: $p_1 = 10^{-4}$ e $p_2 = 9.10^{-4}$
- b) Hipótese 2: um especialista concluiu, por exemplo, que o acidente A teria por origem os três sistemas elementares com as verossimilhanças $b_1 = 0,05$; $b_2 = 0,35$; $b_3 = 0,60$, implicando nos objetivos detalhados apresentados pela Tabela H.1.

TABELA H.1: EXEMPLO DE ALOCAÇÃO DE SEGURANÇA POR PONDERAÇÃO
DE CONFIABILIDADE

i	F_i	b_i	$b_i p_0$	q_i
1	10^{-2}	0,05	$4,5.10^{-5}$	$4,5.10^{-3}$
2	5.10^{-2}	0,35	$3,15.10^{-4}$	$6,3.10^{-3}$
3	2.10^{-2}	0,60	$5,40.10^{-4}$	$2,7.10^{-2}$

ANEXO I

PRINCÍPIO DE DEFESA EM PROFUNDIDADE

As medidas relativas à defesa em profundidade são escalonadas segundo seus cinco níveis. Os quatro primeiros visam a proteção das barreiras físicas e a limitação dos rejeitos radioativos, assim como a proteção da tripulação e do pessoal de apoio em terra. O último nível corresponde aos procedimentos de emergência exteriores ao navio destinados à proteção do público em caso de ocorrência de rejeitos significativos.

A aplicação do Princípio de Defesa em Profundidade dependerá em grande medida das características peculiares ao projeto de cada instalação mas os conceitos essenciais serão sempre os mesmos.

PREVENÇÃO DAS CONDIÇÕES ANORMAIS DE FUNCIONAMENTO E DAS FALHAS PELA QUALIDADE

É necessário dotar a instalação de uma excelente resistência intrínseca em face de suas próprias falhas e em face das agressões internas definidas, visando a redução dos riscos de falhas. Isto implica numa análise, tão exaustiva quanto possível, de suas condições de funcionamento previsíveis de modo a determinar, para cada sistema ou componente importante para a segurança, as mais severas solicitações a considerar.

Os componentes da instalação podem então ser calculados, construídos, controlados, ensaiados e operados segundo regras bem estabelecidas, impondo-se ainda margens suficientes com relação aos limites definidos que assegurem o bom comportamento da instalação mesmos em condições não previstas inicialmente.

Do mesmo modo, devem ser definidas as agressões de origem externa que a instalação deverá ter capacidade de resistir, sem que isto perturbe seu funcionamento em condições seguras ou, caso a severidade do evento obrigue a interromper sua operação, sem provocar liberação de materiais radioativos acima dos limites máximos regulamentares.

Isto implica que o nível 1 serve como base inicial para a proteção contra agressões internas e externas, mesmo que complementos de proteção possam ainda ser necessários nos níveis superiores.

As medidas de nível 1 incluem uma extensa gama de características de dimensionamento prudentes, considerado todo o ciclo de vida do navio, tais como:

- a) definição clara e precisa das condições de funcionamento normais e anormais;
- b) margens suficientes de dimensionamento de sistemas e componentes, em especial no que tange à resistência às situações acidentais, com o objetivo de reduzir ao mínimo a necessidade de recorrer a medidas de nível 2 e 3;
- c) tempo suficiente para reação dos operadores aos eventos de funcionamento, e interfaces homem-máquina adequadas, compreendendo meios de auxílio à decisão, visando diminuir a tensão que os mesmos suportam;
- d) seleção cuidadosa dos materiais e recurso a procedimentos de fabricação homologados e a técnicas de eficácia comprovada, com ensaios sistemáticos de validação;
- e) seleção, formação e treinamento do pessoal de operação e manutenção rigorosos, incutindo sistematicamente a necessidade de comportamentos conformes a uma adequada cultura de segurança;
- f) procedimentos de operação apropriados e monitoração automática confiável do estado e das condições de funcionamento da instalação;
- g) registro, avaliação e efetiva aplicação da experiência operacional acumulada;
- h) programa completo de manutenção preventiva e preditiva, com prioridades estabelecidas em função da importância para a segurança e das exigências de confiabilidade dos sistemas.

CONTROLE DAS CONDIÇÕES DE FUNCIONAMENTO ANORMAIS E DETECÇÃO DE FALHAS PELA VIGILÂNCIA E PROTEÇÃO

É necessário impedir que a instalação saia do domínio de funcionamento normal e projetar os sistemas de regulação, controle e correção suficientemente confiáveis, capazes de limitar uma evolução anormal dos parâmetros de operação antes que os materiais sejam solicitados além de suas condições nominais.

Um sistema de proteção, constituído pelos componentes que cumprem funções corretivas, de proteção e de segurança automaticamente e com alta confiabilidade, deve ser previsto pelo projeto da instalação.

As funções corretivas que podem ser desempenhadas pela intervenção de operadores alertados pela monitoração da instalação são destinadas a evitar uma evolução natural tendendo a reduzir as margens de segurança em operação, mantendo os parâmetros de funcionamento da instalação dentro do domínio fixado pela análise de segurança.

O nível 2 compreende as características intrínsecas do navio e da instalação nuclear (tais como a estabilidade do núcleo, a inércia térmica) e dos sistemas que permitem o controle de condições anormais (incidentes de funcionamento cuja ocorrência é prevista mais de uma vez ao longo da vida útil da instalação), considerando fenômenos capazes de provocar uma degradação sensível do estado funcional do navio.

Os sistemas previstos para atenuar as consequências de tais incidentes são projetados de forma a atender critérios específicos, tais como redundância, segregação física, qualificação. O objetivo é levar o navio a condições de funcionamento normal o mais rápido possível.

Meios de diagnóstico e equipamentos tais como sistemas de regulação automáticos podem ser previstos para efetuar ações corretivas antes que os limites de proteção sejam atingidos. Serão por exemplo as válvulas de descarga com comando automático, os sistemas automáticos de limitação de potência no reator e de pressão, temperatura ou nível nos componentes principais do circuito primário, e sistemas de controle de funções e procedimentos que registram e alarmam as falhas detectadas aos operadores.

A vigilância contínua da qualidade e do respeito às hipóteses de cálculo por meio de inspeções em serviço e de controles periódicos de sistemas e componentes é igualmente necessário para detetar toda degradação dos equipamentos antes que possa ser afetada a segurança.

CONTROLE DE SITUAÇÕES ACIDENTAIS DENTRO DOS LIMITES DE PROJETO POR AÇÕES DE SALVAGUARDA

Os dois primeiros níveis da defesa em profundidade, prevenção e proteção, são destinados a eliminar, com alto grau de confiabilidade, o risco de falha da instalação. Entretanto, apesar dos esforços empreendidos nestes dois níveis, é postulada uma série de incidentes e de acidentes supondo a ocorrência de falhas cuja reduzida probabilidade é garantida pelos dois primeiros níveis. Tal prática visa a introduzir dispositivos especiais de segurança não requeridos pela operação normal que permitam limitar os efeitos destas falhas a um nível aceitável de conseqüências para a tripulação, o público e o meio-ambiente.

Perseguindo este objetivo, os sistemas de segurança e proteção da instalação devem assegurar, por ação automática incontornável em caso de acidente, funções específicas destinadas a evitar que:

- a) os limites fixados para as diferentes barreiras físicas que impedem o relaxamento de matérias radioativas sejam ultrapassados (função de proteção);
- b) a falha fortuita de uma barreira física não possa implicar a falha das duas outras (função de segurança).

Os dispositivos de salvaguarda podem ser ativos ou passivos. No curto prazo, os sistemas de segurança são acionados pelo sistema de proteção do reator. Eles são projetados em função dos acidentes postulados que representam os carregamentos limitantes provocados por grupos de eventos similares. Os acidentes postulados são geralmente acidentes tendo sua origem no interior da instalação nuclear, tais como a ruptura de uma tubulação principal do circuito primário ou de uma linha de vapor do circuito secundário, ou ainda uma perda do controle da reatividade provocada, por exemplo, por uma retirada intempestiva, ou mesmo uma total ejeção, de um elemento absorvedor de controle.

Com o objetivo de garantir uma confiabilidade elevada para os sistemas de salvaguarda, eles são projetados conforme os seguintes princípios:

- a) redundância;
- b) prevenção de falhas em modo comum devido a agressões internas ou externas através de distanciamento e/ou segregação física dos componentes, e ainda por interposição de barreiras de proteção física específicas;

- c) prevenção de falhas em modo comum devidas a erros de projeto, fabricação, montagem, comissionamento, manutenção ou outras intervenções humanas através de diversificação e de redundância funcional;
- d) automação visando reduzir a vulnerabilidade às falhas humanas, pelo menos nas fases iniciais de um incidente ou acidente;
- e) facilidade de monitoração, permitindo ter-se uma indicação clara da disponibilidade e do desempenho dos sistemas;
- f) qualificação dos sistemas, componentes e estruturas para as condições ambientais particulares que podem resultar de um acidente ou de uma agressão externa.

CONTROLE DE SITUAÇÕES GRAVES, VISANDO IMPEDIR A PROGRESSÃO DO ACIDENTE OU ATENUAR SUAS CONSEQUÊNCIAS

O objetivo visado pelo quarto nível de defesa é garantir que a probabilidade de um acidente comportando um dano grave ao núcleo do reator e significativos rejeitos de materiais radioativos dentro da hipótese pouco verossímil de uma situação acidental grave serão, tanto um como o outro mantidos a um nível o mais baixo que se possa razoavelmente atingir, levando-se em conta os fatores sociais e econômicos envolvidos.

Ressalta-se que não se pode justificar deficiências de projeto, construção ou operação relativas aos níveis anteriores com base em argumentações baseadas no gerenciamento de situações acidentais desenvolvidas a este nível.

O quarto nível trata das situações graves que não são explicitamente consideradas para o dimensionamento inicial (níveis 1 a 3) em razão da sua inverossimilhança. Tais situações podem ser causadas por falhas múltiplas tais como a perda completa de todos os “trens” de um sistema de segurança, ou por um evento externo muito improvável. Para algumas destas situações existe a possibilidade de liberação de quantidades significativas de materiais radioativos. A inércia térmica da instalação fornece o tempo necessário a enfrentar algumas destas situações por meio de dispositivos auxiliares específicos e de procedimentos operacionais complementares.

Os procedimentos de gerenciamento interno de situações acidentais graves visam retomar o controle da evolução do acidente e atenuar suas consequências. Em se tratando de

dano severo ao núcleo estes procedimentos compreendem medidas de prevenção e de atenuação. Com respeito ao Plano de Emergência Externo, as medidas são de caráter essencialmente preventivo.

Os objetivos fundamentais do gerenciamento interno de situações acidentais graves são:

- a) assegurar a vigilância dos principais parâmetros que definem o estado atual da instalação;
- b) controlar o estado sub-crítico do reator;
- c) restabelecer a remoção de calor residual do núcleo e manter o resfriamento a longo prazo;
- d) proteger a integridade do compartimento de contenção, garantindo a remoção de calor de seu interior e impedindo que sejam exercidos sobre ele carregamentos mecânicos e térmicos excessivos;
- e) retomar o controle da instalação, se possível, e caso a degradação não possa ser controlada, retardá-la o máximo possível, de modo a por em andamento os procedimentos de gerenciamento externos;
- f) proteger a integridade do navio e de sua tripulação (e das instalações e pessoal de apoio em terra, conforme o caso).

ATENUAÇÃO DAS CONSEQUÊNCIAS RADIOLÓGICAS DE REJEITOS RADIOATIVOS SIGNIFICATIVOS PARA O EXTERIOR

Mesmo considerando-se as disposições tomadas no nível 4, seria contrário à lógica de defesa em profundidade não prever Planos de Emergência Exterior.

Estes planos englobam as funções de coleta e de avaliação de dados sobre o nível de exposição do público previsto para estas situações, tais como dados meteorológicos e hidro-geológicos, caracterização da composição etária e hábitos sócio-culturais do grupo crítico que pode ser afetado, e também as ações de proteção a curto e longo prazo que constituem a execução dos planos propriamente ditos, tais como confinamento do público em locais fechados, evacuação do perímetro sob risco, distribuição de comprimidos de iodo estável.

A mera existência destes planos de emergência não é entretanto suficiente: eles devem ser sistematicamente exercitados através de simulações, de forma a serem plenamente conhecidos por todas as pessoas envolvidas, e periodicamente revisados de modo a

adaptarem-se aos meios efetivamente disponíveis e às deficiências identificadas pelos exercícios.

Note-se ainda que os planos a serem acionados dependem da gravidade do acidente e da localização geográfica do navio.

ANEXO J

ANÁLISE DETERMINÍSTICA DE SEGURANÇA NUCLEAR

A análise determinística de segurança consiste da análise das Condições de Processo da Instalação Nuclear CPIN, através do estudo dos cenários típicos associados a cada uma delas, em especial aqueles considerados *a priori* como "envelopes", sob o ponto de vista de solicitações à instalação.

J.1 CLASSIFICAÇÃO DAS CONDIÇÕES DE PROCESSO DA INSTALAÇÃO

O princípio que postula que incidentes e acidentes poderão ocorrer apesar das precauções tomadas para preveni-los é uma base inadequada para determinação das características destes fenômenos. Os acidentes não terão todos a mesma probabilidade e as consequências aceitáveis não serão idênticas.

Tendo como base a norma americana (ANSI, 1988), discussões conduzidas pela Autoridades de Segurança em todo o mundo tem levado à aceitação de um quadro de correspondência entre a variação de frequência anual de ocorrência FAO e a ordem de grandeza das consequências máximas admissíveis para cada categoria de CPIN (Tabela J.1),. Evidentemente, as frequências estimadas das condições de processo incidentais e acidentais não são derivadas diretamente da experiência operacional, dado a raridade destes fenômenos, mas com base em análises. Por esta razão, os valores correspondem a ordens de grandeza, cobrindo, em cada caso, duas décadas.

Com respeito aos níveis aceitáveis de consequências radiológicas indicados para CPIN3 e CPIN4, os valores constituem também somente ordens de grandeza, a serem propostos pelo operador e aceitos pela Autoridade de Segurança caso a caso, não tendo um caráter regulamentar. O valor adotado para a máxima consequência aceitável para CPIN3, 5mSv, corresponde ao limite anual para os membros do público proposto pela International Commission for Radiological Protection ICRP.

A frequência estimada das quatro categorias de condições de processo (normais, incidentais frequentes, incidentais pouco frequentes e acidentais) é determinada a partir da

freqüência de cada estado inicial da instalação e da freqüência do evento inicializador que conduz a um transitório.

TABELA J.1: CONDIÇÕES DE PROCESSO DA INSTALAÇÃO NUCLEAR

CAT	DESCRIÇÃO	F.A.O	CONSEQUÊNCIAS RADIOLÓGICAS
CPIN1	Situações normais de operação onde a instalação está plenamente disponível	$FAO > 1/\text{ano}$	Observância dos limites anuais de liberação de efluentes permitidos (cerca de $10\mu\text{Sv}$)
CPIN2	Incidentes menores, mas freqüentes e situações onde a instalação tem sua disponibilidade limitada de modo transitório ou permanente	$1/\text{ano} > FAO > 10^{-2}/\text{ano}$	Observância dos limites anuais de liberação de efluentes permitidos por incidente (cerca de $10\mu\text{Sv}$)
CPIN3	Incidentes de funcionamento significativos, mas de ocorrência pouco prováveis	$10^{-2}/\text{ano} > FAO > 10^{-4}/\text{ano}$	<ul style="list-style-type: none"> ▪ Corpo inteiro: $< 5\text{mSv}$ ▪ Tireóide: $< 15\text{mSv}$
CPIN4	Acidentes graves hipotéticos postulados, de ocorrência altamente improvável	$10^{-4}/\text{ano} > FAO > 10^{-6}/\text{ano}$	<ul style="list-style-type: none"> ▪ Corpo inteiro: $< 150\text{mSv}$ ▪ Tireóide: $< 450\text{mSv}$

A análise da segurança consiste em identificar os eventos inicializadores das três últimas categorias: por exemplo, para CPIN2, significa a pesquisa das causas possíveis de variação dos parâmetros que influenciam o resfriamento do combustível (retirada não controlada de um elemento de controle do fluxo neutrônico, abertura intempestiva de uma válvula) ou para CPIN3 e CPIN4, a pesquisa de eventos que possam causar o comprometimento das barreiras físicas da defesa em profundidade (ruptura de tubulações principais de resfriamento do reator, ruptura de tubulações principais de vapor, etc.).

Dessa forma, chega-se a um grande número de cenários possíveis, que são reagrupados por similaridade, em “famílias”. Para cada família de incidentes é identificado e analisado o caso envelope, ou seja aquele de consequências mais graves. Deve-se notar que não se considera um certo número de acidentes que levam a situações particularmente graves, diante das quais seria dificilmente viável a limitação das consequências através da utilização de sistemas de segurança. É o caso da ruptura brutal de grandes vasos de pressão do circuito primário, tais como o reator, o casco do gerador de vapor, o pressurizador ou a carcaça de uma bomba de resfriamento. Nesses vasos, bem projetados e bem construídos, a probabilidade de uma ruptura do gênero é extremamente pequena e convém não responder ao terceiro nível da defesa em profundidade, mas compensar essa deficiência através de um

aumento das margens de projeto, construção e operação, assim como através de uma vigilância reforçada, através de inspeções, durante toda a vida útil da instalação.

J.2 DEFINIÇÃO DAS CATEGORIAS DE CONDIÇÕES DE PROCESSO BÁSICAS DE PROJETO

As situações de operação normal correspondem aos diversos estados e transientes considerados no primeiro nível de defesa em profundidade. Elas cobrem toda faixa autorizada pelas especificações técnicas de operação da instalação, correspondendo a situações rotineiras.

Caso exista alguma possibilidade de liberação de materiais radioativos para o meio ambiente nestas situações, esta deverá ser totalmente controlada, realizada sob condições particulares especificadas e contabilizadas com razoável grau de precisão. O somatório total das liberações ao longo de um ano não deverá exceder os limites previamente autorizados pela Autoridade de Segurança para os efluentes líquidos e gasosos específicos para a instalação. Os efeitos das liberações definidas pelos limites não deverão exceder, com base em cálculos conservativos, algumas poucas dezenas de μSv .

Os incidentes CPIN2 são aqueles considerados no segundo nível de defesa em profundidade.. Eles podem resultar do funcionamento da instalação fora dos limites operacionais normais prescritos e devem ser controlados pelos sistemas de controle e proteção da instalação. A análise destes incidentes determinam os critérios básicos de projeto para estes sistemas.

São associadas a estes incidentes probabilidades de ocorrência relativamente elevadas, sendo portanto considerados praticamente inevitáveis ao longo da vida útil da instalação. Devido a este fato, as liberações resultantes de cada um destes incidentes, que ocorrerão durante um período curto de tempo, da ordem de algumas horas, não deverá exceder o limite anual autorizado. Isto implica que qualquer liberação devido a um incidente deste tipo, ainda que inadvertida e descontrolada, deverá ser feita por canais monitorados, de modo a serem devidamente contabilizados.

Os incidentes improváveis CPIN3 poderão envolver liberações descontroladas porém as conseqüências estimadas destas liberações deverão permanecer em níveis baixos: a dose

equivalente para o corpo inteiro após uma exposição de duas horas para o membro do público ocupando a posição mais desfavorável fora dos limites físicos da instalação e nas menos favoráveis condições meteorológicas deve ser inferior a 5mSv. Com base nos coeficientes de risco propostos pela ICRP, uma tal dose representa um aumento na probabilidade de ocorrência de um câncer neste indivíduo da ordem de 0,025%. Este valor deve ser comparado com a probabilidade natural de um indivíduo contrair um câncer ao longo de sua vida, da ordem de 20-25%.

Os acidentes limitantes CPIN4 são os acidentes mais graves considerados nesta primeira abordagem determinística. Nestas situações, significativos danos ao combustível são admitidos, mas a instalação deverá permanecer estável após a atuação automática dos sistemas de segurança. A dose equivalente para o corpo inteiro recebida em duas horas nos limites da instalação deverá permanecer abaixo de 150mSv sob as mesmas condições conservativas de cálculo das situações CPIN3. Apesar da inverossimilhança de ocorrência destes acidentes, as consequências consideradas aceitáveis permanecem muito abaixo do limiar de dose para surgimento de efeitos biológicos imediatos, que encontra-se entre 300-500mSv. O aumento da probabilidade de ocorrência de câncer fatal permanece abaixo de 1%.

J.3 SELEÇÃO DAS CONDIÇÕES DE PROCESSO

Os eventos inicializadores de situações de operação CPIN2 são identificados dentre as possíveis causas para a variação de parâmetros que afetam o resfriamento do combustível.

O fluxo neutrônico, e portanto a energia produzida pelo combustível, pode aumentar devido aos seguintes efeitos de reatividade:

- a) retirada intempestiva de um elemento de controle
- b) efeitos indiretos devidos à atuação inadvertida de sistemas que façam diminuir a temperatura da água de resfriamento ou diminuir a concentração de veneno solúvel (ácido bórico) nela contida;
- c) abertura inadvertida de uma válvula de vapor principal do circuito secundário;
- d) aumento brusco da potência demandada pela turbina.

A vazão de água de resfriamento do circuito primário, que transfere a energia produzida no núcleo do reator para os geradores de vapor, pode ser reduzida devido não só ao desligamento de uma bomba, como também, e neste caso de modo mais acentuado, à parada de todas as bombas, no caso de perda de alimentação elétrica.

Uma queda no nível de pressão do circuito primário, que também compromete o correto resfriamento do combustível, pode ser causada pela abertura inadvertida de uma válvula do pressurizador ou por seu excessivo resfriamento através do sistema de borrifio.

Outro fenômeno, ligado à resistência no longo prazo do vaso de pressão do reator, é também considerado: atuação inadvertida do sistema de injeção de água de resfriamento de segurança. A irradiação pelo fluxo neutrônico produzido no núcleo modifica as características do aço e das soldas: a temperatura de transição para o comportamento frágil aumenta até um nível próximo à temperatura da água de injeção de segurança.

Os acidentes postulados, divididos entre CPIN3 e CPIN4, são analisados dentro das mesmas linhas (aumento excessivo de potência, resfriamento inadequado do combustível) identificando-se eventos e falhas que possam conduzir à perda de barreiras. Os inicializadores não serão porém neste caso a variação de parâmetros de operação mas a ocorrência de falhas, envolvendo mesmo a ruptura de tubulações apesar das significativas margens adotadas para seu projeto.

O aumento do fluxo neutrônico analisado pode ser, por exemplo, devido a uma total ejeção de um elemento de controle para fora do núcleo ou uma ruptura completa da linha de vapor principal. A perda de vazão de água de resfriamento será, por exemplo, não devido a simples parada das bombas mas ao travamento instantâneo de seus rotores. A queda de pressão será acompanhada da perda de água de resfriamento através de rupturas de tubulações do circuito primário, chegando-se até a uma ruptura em guilhotina da tubulação do primário com deslocamento das duas extremidades de modo que a água de resfriamento atravessasse a segunda barreira sem retenção.

A liberação direta de materiais radioativos contidos em tanques de gases ou líquidos contaminados da instalação é também considerada, tal como a ruptura de um elemento combustível devido a uma queda durante sua manipulação para recarga.

Isto resulta num grande número de possíveis cenários acidentais envolvendo transientes ou falhas com os circuitos intactos e acidentes de perda de refrigerante, com falha de estanqueidade do envelope do circuito primário:

- a) anomalias de distribuição de reatividade e potência;
- b) liberação de radioatividade por um componente ou sub-sistema;
- c) redução na vazão de água de resfriamento do reator;
- d) redução do inventário de água de resfriamento contido no circuito primário;
- e) aumento do inventário de água de resfriamento contido no circuito primário;
- f) redução da remoção de calor pelo circuito secundário;
- g) aumento da remoção de calor pelo circuito secundário;
- h) transientes sem desligamento automático do reator.

Dentro destes cenários deverá ser feita uma seleção baseada em dois princípios:

- a) identificação dos acidentes “envelopes” em termos de consequências;
- b) exclusão de um certo número de acidentes pela implementação de prevenção adicional.

O número de acidentes ou incidentes a serem analisados pode ser reduzido pela identificação daquela situação mais penalizante dentro de um grupo de incidentes do mesmo tipo.

Por exemplo, se num determinado compartimento existem diversos tanques contendo materiais radioativos, todos de projeto e qualidade similares e possuem dispositivos de retenção e ventilação de eficiência equivalente, não seria necessário analisar as consequências da ruptura de cada um destes tanques. É suficiente analisar o pior caso em cada família de eventos e certificar-se que as consequências são aceitáveis de modo a generalizar este resultado para outros tanques do mesmo tipo. O acidente analisado será então considerado como o acidente envelope para toda a família.

A escolha das condições iniciais para o acidente analisado dará ao conceito de acidente envelope um aspecto ainda mais significativo, que irá além da simples maximização das consequências radiológicas.

A implantação de dispositivos especiais de segurança adequadamente projetados podem limitar as consequências da maioria dos acidentes a níveis aceitáveis. Entretanto identifica-se certos acidentes particulares para os quais o dimensionamento destes dispositivos de terceiro nível de defesa em profundidade torna-se inviável.

Em vista desta dificuldade em limitar as consequências destes acidentes, os esforços são concentrados na otimização da prevenção destas situações de forma a reduzir sua probabilidade a um nível que permita sua exclusão do escopo da análise.

Este é o caso da fratura frágil de grandes componentes como o vaso de pressão do reator, do casco externo dos geradores de vapor, do pressurizador ou da carcaça da bomba de circulação. Os esforços mecânicos sob os quais estes componentes estão submetidos tornam o controle direto destes acidentes extremamente difícil, senão totalmente impossível.

A experiência industrial mundial neste campo de vasos de pressão indica que equipamentos deste tipo quando bem projetados, bem construídos e cuidadosamente monitorados têm uma probabilidade de ocorrência deste tipo de falha extremamente baixa.

Considera-se então que este tipo de acidente não deverá ser considerado e que o terceiro nível de defesa em profundidade será omitido da base de projeto mas esta decisão deverá ser contrabalançada por um aumento nas margens de segurança de projeto, construção e operação e por procedimentos de inspeção inicial e em serviço especiais.

J.4 LISTAGEM E SUBDIVISÕES DAS SITUAÇÕES DE OPERAÇÃO

As situações CPIN-1 são aquelas cuja ocorrência é freqüente ou regular durante a operação normal da instalação, recarga de combustível e manutenção. Deste modo, as situações CPIN-1 são acomodadas dentro das margens entre os parâmetros de funcionamento e o valor limite para estes parâmetros que implicam ações automáticas ou manuais de proteção. Como estas situações são freqüentes ou regulares, elas devem ser consideradas do ponto de vista de sua influência sobre as consequências das situações

incidentais e acidentais (CPIN-2, CPIN-3 e CPIN-4). Sob este aspecto, a análise destas últimas situações devem ser baseadas em condições iniciais correspondendo às condições mais adversas que podem ocorrer durante a operação em situações CPIN-1. São apresentadas a seguir situações de operação CPIN-1 típicas.

a) Regime Estacionário e Condições de Partida e Parada

- i. Operação em potência sob controle automático, entre 20% e 100% da potência térmica nominal, com temperatura média entre a entrada e saída do reator constante;
- ii. Operação em potência sob controle manual, entre 0% e 20% da potência térmica nominal, com temperatura média entre a entrada e saída do reator proporcional ao nível de potência e $k_{ef} > 0,99$;
- iii. Parada a quente, com o reator sub-crítico ($k_{ef} < 0,99$), temperatura média correspondente ao nível de potência 0% e sistema de remoção de calor residual isolado;
- iv. Desligamento a quente, com o reator sub-crítico ($k_{ef} < 0,99$), temperatura média inferior àquela correspondente ao nível de potência 0% e sistema de remoção de calor residual em operação;
- v. Desligamento a frio, com o reator sub-crítico ($k_{ef} < 0,99$), com pressão e temperatura mínima;
- vi. Recarga, com o reator sub-crítico ($k_{ef} < 0,95$), tampo do reator removido, sistema na pressão atmosférica e carga de combustível no interior do vaso;

b) Operações com desvios permitidos

Alguns desvios autorizados pelas especificações técnicas da instalação podem ocorrer durante a operação continuada e são considerados em conjunção com as demais situações de operação. Estes desvios incluem:

- i. Operação com componentes ou sistemas fora de serviço, tal como uma das bombas de circulação de água de resfriamento do circuito primário;
- ii. Pequenas falhas no encamisamento do combustível;
- iii. Presença de radioatividade na água de resfriamento:
 - (I) Produtos de fissão;

- (II) Produtos de corrosão ativados;
- (III) Trítio.
- iv. Operação com pequenos vazamentos pelos tubos dos geradores de vapor
- v. Testes específicos
- c) Transientes operacionais
 - i. Aquecimento e resfriamento;
 - ii. Variação de carga em degraus;
 - iii. Variação de carga em rampa;
 - iv. Rejeição total de carga na potência máxima nominal;

No pior caso, as situações de operação CPIN2 devem resultar no desligamento automático do reator, com a instalação sendo capaz de retornar à operação num intervalo de tempo relativamente curto. Por definição, estas situações não deverão se propagar de modo a conduzir a instalação a uma situação de categoria superior (CPIN3 ou CPIN4). Adicionalmente, as situações CPIN2 não deverão resultar em falhas no encamisamento do combustível nem em sobre-pressão no circuito primário e no circuito secundário. São apresentadas a seguir situações de operação CPIN2 típicas.

- a) mau funcionamento do sub-sistema de água de alimentação dos geradores de vapor do circuito secundário causando redução da sua temperatura;
- b) mau funcionamento do sub-sistema de água de alimentação dos geradores de vapor do circuito secundário causando aumento da sua temperatura;
- c) aumento excessivo na vazão de vapor no sub-sistema de vapor vivo do circuito secundário;
- d) abertura inadvertida de uma válvula de alívio e segurança de um gerador de vapor causando a despressurização do sub-sistema de vapor vivo do circuito secundário;
- e) redução total da demanda de carga externa;
- f) desligamento automático (*trip*) de uma ou mais turbinas;
- g) fechamento inadvertido de uma válvula principal de bloqueio de vapor no sub-sistema de vapor vivo do circuito secundário;
- h) queda de vácuo nos condensadores principais do circuito secundário;

- i) perda de alimentação elétrica normal;
- j) perda da vazão normal de água de alimentação dos geradores de vapor;
- k) perda parcial da vazão de água de resfriamento do circuito primário;
- l) retirada descontrolada de um banco de elementos de controle na condição do reator sub-crítico ou a baixa potência (partida/parada);
- m) retirada descontrolada de um banco de elementos de controle na condição do reator em potência;
- n) desalinhamento de um elemento ou todo um banco de controle, considerando sua queda total ou parcial até a base do núcleo;
- o) partida de bombas de um “loop” inativo do circuito primário a uma temperatura incorreta;
- p) mau funcionamento de sistemas conduzindo a uma redução na concentração de veneno solúvel (ácido bórico) diluído na água de resfriamento do circuito primário;
- q) operação inadvertida do sistema de resfriamento de emergência do reator durante funcionamento em potência;
- r) mau funcionamento de sistemas conduzindo a injeção de refrigerante no circuito primário, aumentando o inventário de água de resfriamento;
- s) abertura inadvertida de uma válvula de alívio e segurança do pressurizador;
- t) falha em tubulações de pequeno diâmetro transportando água de resfriamento do circuito primário para fora da contenção.

Por definição, as situações CPIN-3 decorrem de falhas cuja probabilidade de ocorrência ao longo da vida útil da instalação é muito pequena e que podem resultar em danos no encamisamento do combustível. Neste caso, a instalação somente poderá voltar a operar após intervalo de tempo relativamente longo, requerido para os necessários reparos. A liberação de radioatividade nestas situações não deverá ser suficiente para interromper ou restringir o uso público de áreas além da área de exclusão em torno da instalação. Uma situação CPIN-3 não deverá propagar-se de modo a conduzir a instalação a uma situação CPIN-4, nem conduzir à perda das funções básicas de segurança de resfriamento do combustível e de contenção. São apresentadas a seguir situações de operação CPIN-3 típicas.

- a) pequenas falhas em tubulações de vapor do circuito secundário;
- b) perda total da vazão de água de resfriamento do circuito primário;
- c) desalinhamento de um elemento ou todo um banco de controle, considerando sua retirada total ou parcial até o topo do núcleo com o reator na potência máxima nominal;
- d) carregamento e operação inadvertida de um elemento combustível numa posição imprópria;
- e) perda de água de resfriamento primário devido a ruptura de tubulações de pequeno diâmetro ou a trincas em tubulações de grande diâmetro, com atuação do sistema de resfriamento de emergência;
- f) falha ou vazamentos em vasos de pressão contendo rejeitos gasosos;
- g) falha ou vazamentos em vasos de pressão contendo rejeitos líquidos.

As situações de categoria CPIN-4 decorrem de falhas extremamente improváveis de ocorrerem durante a vida útil da instalação, mas que são postuladas devido ao fato de suas consequências poderem incluir potencialmente significativas liberações de materiais radioativos. O projeto da instalação deverá então limitar estas liberações para o meio-ambiente a valores que não provoquem um aumento inaceitável nos riscos sanitários incorridos pelo público. Uma falha simples que conduza a instalação a uma situação CPIN-4 não deve ter como consequência a perda das funções de sistemas necessários à mitigação das consequências do acidente, incluindo o resfriamento de emergência e a contenção. São apresentadas a seguir situações de operação CPIN-4 típicas.

- a) ruptura total na tubulação principal de vapor do circuito secundário;
- b) ruptura total na tubulação principal de água de alimentação de um gerador de vapor;
- c) travamento do rotor de uma bomba de circulação de água de resfriamento do circuito primário;
- d) espectro de acidentes de ejeção total de um elemento de controle;
- e) ruptura de tubos dos geradores de vapor;
- f) acidentes de perda de água de resfriamento do circuito primário resultantes do espectro de rupturas postuladas para o envelope estanque do circuito primário;
- g) acidentes de manuseio de combustível irradiado.

A experiência operacional mundial em reatores PWR de potência tem demonstrado algumas falhas nesta listagem convencional. A ruptura de um tubo dos geradores de vapor, classificada em CPIN-4, tem se demonstrado na prática mais freqüente do que inicialmente suposto, o que conduz a reclassificá-la em CPIN-3, a ruptura de vários mantendo-se em CPIN-4. Evidentemente esta modificação não poderia ser implementada para as instalações em funcionamento: neste caso, medidas compensatórias devem ser tomadas.

Poder-se-ia imaginar que uma transferência de categoria deste tipo poderia ajudar a resolver o problema, já que acidentes CPIN-3 são menos graves do que acidentes CPIN-4. A realidade é entretanto muito diferente. A transferência deste acidente ocorre devido ao fato de sua probabilidade ser maior do que a hipótese inicial, mas isto não torna o acidente menos grave. Pelo contrário, requer que o acidente seja tornado menos grave. De modo a respeitar as conseqüências radiológicas aceitáveis para a nova categoria, que são 30 vezes menores, o projetista e o operador deverão modificar certos equipamentos e impor restrições especiais com respeito à atividade da água de resfriamento do circuito primário, por exemplo.

Outro exemplo de reclassificação é dado pelo travamento do rotor das bombas de circulação. A experiência internacional de operação mostra que freqüência de ocorrência deste evento, devido particularmente ao desgaste excessivo dos mancais do eixo destas bombas, é maior do que aquela inicialmente estimada. Entretanto esta falha simples não afeta significativamente o combustível nem implica em liberação de materiais radioativos. As modificações requeridas limitam-se a implementação de inspeções em serviço mais rigorosas e freqüente e, eventualmente, de sistemas específicos para monitoração da vibração do eixo das bombas, de modo a limitar os riscos de parada não programada da instalação.

A divisão dos acidentes em duas categorias tem certos efeitos limitantes sobre o conceito de acidente envelope. Se as conseqüências de uma grande ruptura de tubulações principais do secundário cobrem as conseqüências das menores, isto não implica na dispensa da análise destas últimas falhas. O fato de uma grande ruptura ter conseqüências aceitáveis em CPIN-4 não implica que uma pequena ruptura seja necessariamente aceitável em CPIN-3.

J.5 PROCESSO DE ANÁLISE DAS SITUAÇÕES DE OPERAÇÃO

As situações de operação não são estudadas por elas mesmas, mas para proteger a instalação contra determinadas classes de transitórios ou de fenômenos que possam apresentar riscos que possam ameaçar o cumprimento dos objetivos gerais de segurança. O incidente ou acidente analisado vai ser definido por uma série de hipóteses e de condições de estudo escolhidas de maneira a agravar o caso e a dar ao resultado um caráter "envelope".

Será estudada então a evolução dos parâmetros físicos fundamentais da instalação, a partir da escolha de condições iniciais, pela utilização de métodos de cálculo qualificados, aplicando o critério de falha única e o efeito de um evento agravante, até a obtenção de um “estado seguro” tal que o reator possa se manter estável, sem que sua evolução posterior possa conduzir a uma situação ainda mais degradada com relação aos critérios básicos de segurança (controle da reatividade, resfriamento do núcleo, estanqueidade da contenção), na ausência de falha suplementar independente.

Escolha das Condições Iniciais

Uma instalação nuclear embarcada dispõe, como toda instalação industrial, de uma região de funcionamento autorizada, desde a plena potência até a parada a frio, vaso aberto para recarga de combustível. Podemos distinguir as condições iniciais:

- a) “prováveis”, para as quais supõe-se que a probabilidade de ocorrência é unitária;
- b) “excepcionais”, correspondendo a configurações da instalação cuja probabilidade de ocorrência é pequena (da ordem de 10^{-2} /ano).

Dentro de cada um destes casos, os parâmetros característicos tais como pressão, temperatura, vazão, volume, tensão, frequência, radioatividade, etc. tem um valor nominal definido assim como limites de variação autorizados. Para cada estudo serão escolhidos valores para estes parâmetros que sejam “pessimistas” em relação ao fenômeno que se deseja evitar.

Utilização de Códigos Qualificados para a Segurança

Para a análise dos acidentes convencionais e a verificação do caráter aceitável de suas consequências, utilizam-se códigos cujos resultados tenham sido qualificados através de

experimentos. Estes códigos podem ter um caráter conservativo, incluindo significativas margens de segurança implícitas na modelização dos fenômenos físicos em jogo, ou um caráter realista (*best estimate*) no qual se procura uma aproximação da realidade a melhor possível, sendo as margens de segurança explicitadas através das condições iniciais e dos critérios de aceitabilidade. Estes códigos são objetos de estudos complementares e melhorias constantes.

Critério de Falha Única

Dada a importância de sua função, os sistemas de segurança que atuam em caso de incidente ou acidente devem possuir uma excelente confiabilidade. Na fase de concepção, entretanto, é extremamente difícil levar a cabo um estudo de confiabilidade, pois em geral os dados históricos de funcionamento (frequência de falhas, etc.) dos equipamentos não são disponíveis. É preferível então considerar-se um método “determinista”: o critério de falha única:

A função dos sistemas importantes para a segurança deve poder ser cumprida de maneira satisfatória mesmo em caso de falha de um de seus componentes qualquer.

O critério de falha única é aplicado para o estudo das situações de operação CPIN3 e CPIN4. Na prática, pode-se optar por uma solução que comporte redundâncias:

- a) dois “trens” capazes cada um de assegurar sozinho a função de segurança; esta solução impõe uma vigilância muito grande sobre a disponibilidade dos dois trens durante os períodos de funcionamento para os quais este sistema é necessário (restrições severas sobre a duração de uma indisponibilidade fortuita, interdição de colocação de um trem em indisponibilidade voluntária para manutenção);
- b) três ou quatro “trens” capazes cada um de assegurar dois terços ou metade da função de segurança.

Pode-se tentar dar uma explicação probabilística para este critério em termos de confiabilidade:

- a) a experiência mostra que, em geral, um sistema complexo recusa-se a funcionar uma vez em cem, quando se quer que o faça;
- b) se considerarmos um acidente CPIN4 que terá a probabilidade máxima (10^{-4} /ano), o risco de ver acumular-se esse iniciador e a recusa de funcionamento do sistema de segurança de via única correspondente é de $10^{-4} * 10^{-2} = 10^{-6}$, situação vista como muito séria;
- c) por outro lado, também de forma caricatural, um sistema de segurança de duas vias, terá uma probabilidade total de recusa de funcionamento da ordem de 10^{-4} ;
- d) essa probabilidade, associada àquela do mesmo iniciador anterior, dá uma probabilidade de acidente grave da ordem de 10^{-8} por ano, o que é muito mais aceitável.

Para poder negligenciar, como acabamos de fazer, as falhas simultâneas das duas vias redundantes, garantindo o ganho de confiabilidade obtido pela adoção de soluções de projeto comportando redundâncias, dois aspectos devem ser meticolosamente analisados:

- a) Evitar que uma mesma agressão, seja de origem interna ou externa (incêndio, alagamento, choque, etc.) atinja simultaneamente os equipamentos dos trens redundantes. Para tal, um certo grau de segregação física é requerido;
- b) Limitar a probabilidade de ocorrência de falhas em modo comum, devidas a erros de projeto, construção ou manutenção. Para tal, a diversidade de tipos de equipamentos utilizados em cada trem é extremamente benéfica;
- c) evitar que os diversos trens utilizem os mesmo sistemas de suporte, tais como alimentação elétrica, hidráulica ou pneumática.

Acumulação das Condições de Funcionamento (eventos agravantes)

Para bem caracterizar o aspecto “envelope” dos estudos de acidentes, além do critério de falha única considera-se ainda a ocorrência, durante o transitório resultante de um evento iniciador, de um evento agravante, que poderá ser:

- a) um segundo evento inicializador independente do primeiro, cuja frequência de ocorrência deve ser tomada como sua frequência anual própria multiplicada pela fração de tempo durante a qual sua ocorrência leva efetivamente ao agravamento das consequências;
- b) uma falha à solicitação de uma função corretora do comando-controle do sistema de proteção ou de um componente sensível de um sistema de segurança;

c) mudança desfavorável da atitude da plataforma navio (trim, banda).

Convencionalmente, vai-se então cumular os eventos agravantes às condições de operação mais graves CPIN4, sem que isto autorize um agravamento de consequências.

Prevenção da Propagação de Acidentes

Dentre os critérios de aceitação para as quatro categorias de situações de operação, é especificado que estes eventos não devem ser a causa de um evento de categoria superior. A análise de cada CPIN deve então determinar os carregamentos (mecânicos, térmicos, etc.) a que estarão submetidos outros componentes e sistemas que não aqueles responsáveis pelo evento inicializador de modo a garantir que eles não falharão “em cascata”. Esta análise implicará na consideração de diversas combinações de carregamentos para o projeto de cada componente.

De modo similar, um acidente CPIN4 ocorrendo em uma parte da instalação não deverá se propagar para outras partes nem impedir o funcionamento dos equipamentos disponíveis para limitar as consequências do evento inicial. Por exemplo, uma ruptura da tubulação de um “loop” do circuito primário não deve provocar ruptura em outro “loop” nem comprometer o funcionamento do sistema de resfriamento de emergência. Os esforços devidos à deformação da tubulação componente da segunda barreira (envelope do primário) rompida e ao jato fluido que escapa desta ruptura não deverão comprometer a integridade da terceira barreira (retenção).

Os resultados das análises de terceiro nível de defesa em profundidade são então usados como critérios básicos para o primeiro nível deste processo, pelo menos durante a fase inicial do projeto, evidenciando assim sua natureza iterativa.

Para a análise preliminar de segurança devem então ser introduzidas margens de segurança apropriadas, sendo sua adequação verificada durante a análise final.

J.6 SITUAÇÕES ACIDENTAIS COMPLEMENTARES

As situações cuja probabilidade de ocorrência é menor que aquela das CPIN4, i.e. inferior a 10^{-6} /ano, não são normalmente consideradas para o dimensionamento da instalação. Entretanto, as autoridades de segurança solicitam que algumas delas, cujas probabilidade de ocorrência não parecem completamente desprezíveis (compreendidas entre 10^{-7} e 10^{-6}) e cujas consequências poderiam ser mais graves que aquelas das CPIN4, sejam também analisadas com o propósito de buscar meios que permitam limitar suas consequências, que são os procedimentos de emergência.

Estas situações acidentais complementares podem corresponder a falhas em modo comum de sistemas importantes para a segurança e a acidentes ou agressões severas. Os resultados da análise dos acidentes estudados auxiliam à definição dos planos de emergência internos e dos procedimentos pós-acidentais do navio. Trata-se de limitar os rejeitos radioativos provocados por uma situação muito grave ou de retardá-los o tempo necessário à execução dos planos de emergência interna e os planos particulares de intervenção com respeito às populações.

Estas situações acidentais complementares correspondem geralmente a uma degradação notável do núcleo com o vaso fechado, envolvendo riscos de violação do confinamento, riscos de explosão ligado à liberação de hidrogênio, riscos ligados aos mísseis gerados pelo circuito primário, riscos ligados à interação do *corium* (núcleo fundido) com a estrutura do casco do navio, com consequências radiológicas à bordo, ou ainda a acidentes de criticalidade com o vaso aberto.

Cenários Acidentais Severos

A expressão “acidente severo” tem uma significação precisa. Refere-se a situações comportando sucessivamente:

- a) esvaziamento do circuito primário;
- b) descobrimento e degradação do núcleo;
- c) travessia do vaso do reator pelo núcleo fundido (*corium*);
- d) ataque do *corium* às estruturas da contenção sob o vaso de pressão do reator.

Neste estágio, a proteção do público e do meio-ambiente repousa exclusivamente sobre a resistência da contenção ou, se esta resistência não pode ser assegurada perfeitamente, sobre o atraso de sua perda de estanqueidade. O acidente de Tchernobyl é um infeliz exemplo de fusão do núcleo com liberação de materiais radioativos não contidos.

Existe uma série de cenários de falha que, sob hipóteses muito pessimistas, podem conduzir à fusão do núcleo. São apresentadas a seguir situações de operação complementares típicas, para as quais devem ser desenvolvidos procedimentos operacionais especiais:

- a) perda da fonte fria (água do mar, no caso do navio) ou de sistemas que garantam a transferência de calor para ela;
- b) perda total de água de alimentação para os geradores de vapor;
- c) perda total de energia elétrica;
- d) perda do subsistema de injeção de emergência durante o período de resfriamento a longo prazo após um acidente de grande perda de refrigerante primário;
- e) proteção contra alagamentos acima do cenário envelope adotado no projeto.

FIGURA J.1: EVOLUÇÃO DE UM ACIDENTE SEVERO

Os cenários de falha mais comumente analisados são os cenários TMLB, AB na perna quente e S2D na terminologia WASH-1400. Esta terminologia é sumarizada pela Tabela J.2. Ela proporciona um meio de descrever de forma sucinta diferentes cenários.

TABELA J.2: SIMBOLOGIA DE SEQUÊNCIAS ACIDENTAIS EM PWR

A	Grande perda de refrigerante primário
B	Perda de energia elétrica para os dispositivos especiais de segurança
B'	Falha na recuperação da energia elétrica após de 1 a 3 horas de ocorrência de perda de energia elétrica de emergência
C	Falha do sistema de aspersão de água no interior da contenção
D	Falha do sistema de injeção de água de resfriamento de emergência
F	Falha do sistema de recirculação da água de resfriamento acumulada no interior da contenção
G	Falha no sistema de remoção de calor da contenção
H	Falha do sistema de resfriamento de emergência
K	Falha no sistema de proteção do reator
L	Falha das válvulas de alívio de vapor do circuito secundário e do sistema de alimentação de emergência dos geradores de vapor
M	Falha das válvulas de alívio de vapor e do circuito secundário
Q	Falha das válvulas de alívio do circuito primário em fecharem após terem sido abertas
R	Ruptura catastrófica do vaso de pressão do reator
S₁	Pequena perda de refrigerante primário com diâmetro equivalente de 2" a 6"
S₂	Pequena perda de refrigerante primário com diâmetro equivalente de 1/2" a 2"

T	Evento transiente
V	Falha da válvula de retenção do sistema de injeção de refrigerante a baixa pressão
a	Falha da contenção devido a explosão de vapor do vaso de pressão do reator
b	Falha da contenção devido ao isolamento inadequado de aberturas e penetrações
c	Falha da contenção devido a explosão de hidrogênio
d	Falha da contenção por sobrepressão
e	Falha da contenção por interação direta com o corium

Modos de Falha da Contenção

Um acidente severo é caracterizado pela ocorrência de um modo de falha da contenção, o que implica em liberação incontrolada de relativamente grandes quantidades de materiais radioativos para o meio-ambiente, acarretando significativas consequências sanitárias para o público. Classicamente são identificados cinco modos de falha simbolizados pelas cinco primeiras letras do alfabeto grego, de acordo com a Tabela J.2. Os três primeiros referem-se a modos de falha no curto prazo e os dois últimos no longo prazo.

O modo alfa pressupõe uma interação violenta durante a fusão do núcleo dentro do vaso de pressão, liberando uma energia suscetível de projetar o tampo que viria a perfurar a contenção. Este modo de ruptura é atualmente considerado como pouco provável, mas certos estudos de acidentes de criticidade, relançados após o acidente de Tchernobyl, exploram novamente este domínio.

O modo beta consiste numa falha de estanqueidade da contenção que se produz nas penetrações e aberturas existentes antes do acidente. Este modo de perda de integridade é muito importante, pois ele pode intervir muito cedo durante a evolução do acidente e permitir a liberação de materiais radioativos para o meio-ambiente sem deixar tempo para decaimento radioativo e para os mecanismos de deposição no interior da contenção.

O modo gama corresponde aos efeitos de uma eventual combustão de hidrogênio e de monóxido de carbono dentro da contenção. Em caso de deflagração da totalidade do hidrogênio produzido pela oxidação da totalidade do encamisamento do combustível, o valor

máximo da pressão dentro da contenção poderia ser superior ao limite de resistência da estrutura, provocando sua ruína ou, pelo menos, provocando fissuras.

O modo delta corresponde a uma falha a médio prazo devido à liberação progressiva de uma grande quantidade de gases durante o ataque do corium às estruturas da contenção e ao vapor produzido pela água injetada no seu interior para tentar reduzir a progressão do corium através de seu resfriamento.

O modo epsilon corresponde à ruptura da contenção após a travessia do corium por suas estruturas externas.

Termos-Fontes

A análise de acidentes severos tem dois objetivos:

- a) avaliar a magnitude das liberações potenciais de materiais radioativos correspondentes a cada uma das evoluções consideradas;
- b) mitigar estas liberações para tornar possível o acionamento de planos de emergência externos à instalação nuclear.

As liberações potenciais são denominadas “termos fontes” e definidas como um rejeito típico, característico de uma família de reatores e representativo de um tipo de acidente, isto é, de um modo de falha da contenção derivado da fusão completa do núcleo. O termo-fonte é considerado para definir os procedimentos de emergência. Define-se três termos fontes de gravidade decrescente, expressos em termos de porcentagem de produtos de fissão inicialmente contidos no núcleo:

- a) S1: obtido em caso de falha precoce da contenção, dentro de algumas horas após o acidente;
- b) S2: corresponde a rejeitos diretos para o exterior devido a uma perda de estanqueidade da contenção alguns dias após o acidente;
- c) S3: corresponde a rejeitos indiretos e diferidos, liberados através de vias que permitem uma certa retenção dos produtos de fissão.

TABELA J.3: TERMOS-FONTE EM ACIDENTES SEVEROS

	S1 precoce	S2 diferido	S3 tardio
Gases Raros	80%	75%	75%
Iodo Orgânico	0,6%	0,55%	0,55%
Iodo Inorgânico	60%	2,7%	0,30%
Césio	40%	5,5%	0,35%
Estrôncio	5%	0,6%	0,04%

J.7 DETERMINAÇÃO DOS EQUIPAMENTOS IMPORTANTES PARA A SEGURANÇA (EIS)

São declarados “Importantes para a Segurança” ou “Classe de Segurança Nuclear” as funções e os equipamentos da instalação (mecânicos, elétricos, eletro-mecânicos, hardware e software) que respondem a um dos seguintes critérios:

- a) a sua falha pode iniciar diretamente um acidente desencadeando riscos de irradiação ou de contaminação; ou
- b) o seu funcionamento é necessário para limitar as consequências de um incidente ou acidente desencadeando riscos de irradiação ou de contaminação.

As Funções Importantes para a Segurança são as que permitem garantir o respeito dos seguintes princípios fundamentais de projeto:

- a) controlar a reatividade do núcleo
- b) evacuar a potência residual
- c) confinar e assegurar a proteção de produtos radioativos

Os Equipamentos Importantes para a Segurança EIS associados a essas funções dividem-se em seis classes de segurança hierarquizadas:

- a) três classes de segurança para os equipamentos mecânicos: 1M, 2M, 3M;
- b) duas classes de segurança para os equipamentos elétricos, de instrumentação e de controle: 1E, 2E;
- c) uma categoria Z referente aos EIS cujas exigências técnicas associadas podem ser aliviadas.

TABELA J.4: EQUIPAMENTOS IMPORTANTES PARA A SEGURANÇA

EQUIPAMENTO	PRINCÍPIO	CS
-------------	-----------	----

equipamentos do circuito primário principal	terceiro princípio	1M
mecanismos de acionamento de elementos de controle	primeiro princípio	1M
estrutura do compartimento do reator	terceiro princípio	2M
bateria principal	primeiro princípio	1E
sensores de pressão do primário e de temperatura de saída do núcleo	segundo princípio	1E

Para cada categoria e família de materiais e componentes correspondem exigências técnicas de projeto, construção, operação e manutenção.

a) são classificadas em 1M, 2M, 3M, 1E, 2E:

- componentes das três barreiras físicas de defesa em profundidade;
- componentes do sistema de proteção da instalação;

b) são classificados em Z:

- componentes participantes ao atendimento de um dos três princípios;
- equipamentos que constituem meios para a gestão dos acidentes do dimensionamento a “longo prazo”,
- equipamentos específicos à gestão de situações acidentais complementares.

J.8 QUALIFICAÇÃO

Qualificação dos Códigos de Projeto e Análise

Os projetos neutrônico e termohidráulico do núcleo implicam um grande número de variáveis e de parâmetros. Sua determinação só pode ser efetuada graças a ferramentas informáticas de cálculo denominadas “códigos”. Vários códigos de cálculo são utilizados para determinar a evolução da reatividade do núcleo, seu tempo de vida, para definir a estratégia de movimentação dos elementos de controle ou determinar o comportamento térmico e hidráulico do núcleo em condições de funcionamento normais, incidentais ou acidentais. A análise termohidráulica do núcleo deve verificar que, nos vários transitórios previsíveis, os critérios de segurança relativos a primeira barreira considerados na análise de segurança são

respeitados, levando-se em conta o dimensionamento dos componentes do núcleo e as ações previstas do sistema de proteção.

A qualificação desses códigos é obtida a partir de muitos ensaios efetuados em circuitos e bancadas experimentais. Os principais modelos físicos e correlações que são introduzidos nos códigos são estabelecidos a partir de estudos teóricos seguidos de adequada validação experimental. Para validação desses códigos, eles são utilizados para analisar inúmeros ensaios padronizados em reatores existentes. A adequada aderência dos resultados obtidos aos dados experimentais permitem então que eles possam ser empregados no projeto de novas instalações.

Qualificação dos EIS

A qualificação de componentes permite demonstrar sua capacidade de funcionar adequadamente nas condições de operação normais, incidentais, acidentais e, eventualmente, pós-acidentais. A qualificação de equipamentos, componentes e materiais pode ser obtida:

- a) operação em reator de pesquisa ou em bancadas experimentais especiais nas condições de funcionamento (temperatura, pressão, irradiação, atitude de plataforma, etc) em que será requisitado sob o ponto de vista da segurança por intervalo de tempo representativo;
- b) ensaios nos limites do domínio de funcionamento (combustível, gerador de vapor, etc.);
- c) retorno de experiência de materiais idênticos funcionando nas mesmas condições há vários anos (dados de confiabilidade, controle do envelhecimento, etc.);
- d) análises e cálculos.

J.9 PROJETO DAS BARREIRAS

Encamisamento do Combustível (Primeira barreira)

Os critérios de aceitação considerados na análises são os seguintes:

- a) em CPIN2, não há secagem do encamisamento (desvio do regime de resfriamento por ebulição nucleada), garantindo-se os critérios mínimos de resfriamento do canal quente (fluxo crítico de calor no encamisamento e taxa de vazios no fluido de resfriamento);

- b) em CPIN3, não há danos no combustível, admitindo-se uma secagem transitória do encamisamento, desde que não haja uma dilatação significativa do óxido; para tanto, a temperatura de máxima combustível não deve ultrapassar um determinado valor limite;
- c) em CPIN4, pode haver danos em um número limitado de elementos combustíveis (inferior a 1%), porém a temperatura do encamisamento não deve ultrapassar 1200 C, evitando-se assim a reação química entre o metal do encamisamento e a água de resfriamento.

Envelope do Circuito Primário (Segunda Barreira)

Alguns acidentes, como a ruptura brutal de grandes vasos de pressão do primário, assim como o reator, a câmara d'água do GV, o pressurizador ou a carcaça de uma bomba primária, levam a situações bastante graves, sendo inviável limitar as consequências que mesmas teriam.. Essa deficiência no terceiro nível da defesa em profundidade é compensada por um reforço das margens de projeto, fabricação e operação, por requisitos de garantia da qualidade altamente restritivos e por uma vigilância reforçada, através de inspeções em serviço, durante toda a vida útil destes equipamentos.

As diretivas de aplicação da regulamentação e dos códigos de caldeiraria referentes aos circuitos sob alta pressão, particularmente as instalações nucleares a bordo dos navios militares, são definidas por uma norma fundamental de projeto e construção, que estabelece uma base comum a ser seguida pelo gerenciamento do programa, o industrial fabricante e a autoridade de segurança, no que se refere às modalidades em que é considerado esse aspecto da segurança.

As regras gerais de projeto e de fabricação referem-se ao:

- a) circuito primário principal, compreendendo:
 - a vaso do reator e a seu tampo;
 - o envelope dos mecanismos de acionamento dos elementos de controle;
 - as tubulações que ultrapassam um determinado diâmetro;
 - a parte primária dos geradores de vapor;
 - o pressurizador, a sua conexão com o circuito primário (linha de surto) e suas válvulas de alívio e segurança;

- os envelopes das bombas de resfriamento principais e eventualmente outras bombas ligadas diretamente ao circuito primário;
 - os circuitos auxiliares até as válvulas ou diafragmas de isolamento.
- b) parte circuito secundário que compreende:
- o envelope do GV lado secundário;
 - as tubulações ligadas ao GV de diâmetro superior a d até as válvulas de isolamento;
 - as válvulas até o segundo isolamento.

O projeto dos circuitos sob pressão das instalações nucleares embarcadas é realizado, respeitando-se as exigências baseadas em normas de projeto e de construção mecânicas específicas para os equipamentos e tubulações de segurança 1M e 2M. Essas exigências utilizam conceitos de níveis de qualidade 1,2,3 associados às respectivas classes de segurança, referindo-se à:

- a) projeto: geometria, dimensionamento (memorial de cálculo), materiais e tecnologia;
- b) fabricação e seu controle;
- c) condições para testes hidrostáticos.

Para reduzir o vazamento causado por uma ruptura da tubulação principal do circuito primário, respeitam-se as seguintes disposições:

- a) instalação de válvulas de isolamento o mais perto possível dos componentes;
- b) colocação de diafragmas ou reguladores de vazão sobre as linhas de medida,
- c) implantação de válvulas de retenção sobre as linhas de entrada nas componentes;
- d) implantação, quando possível, de reguladores de vazão sobre as linhas de saída das capacidades
- e) implantações de juntas externas, quando as dimensões assim o justificarem, sobre as soldas mistas das picagens de tubulações mais solicitados pelos esforços térmicos,
- f) implantação de limitadores de escoamento.

Contenção (terceira barreira)

O papel do compartimento de contenção da instalação nuclear é o de assegurar a não disseminação das substâncias radioativas do reator para os outros compartimentos do navio e

para o meio-ambiente, em qualquer situação de operação, inclusive as situações acidentais provocada pela ruptura simultânea de uma tubulação principal do primário e de uma tubulação principal de vapor.

Os materiais que garantem a contenção devem resistir a todas as solicitações termohidráulicas, mecânicas, devidas às radiações e devidas a agressões ao navio definidas pelo Relatório de Análise de Segurança.

As opções de projeto para garantir a estanqueidade são as seguintes:

- a) dispositivo duplo de isolamento para as tubulações que atravessam o envelope da contenção;
- b) limitar as penetrações ao estritamente necessário;
- c) todas as penetrações cuja estanqueidade é garantida por uma junta são equipadas com um dispositivo que permite testá-las individualmente.

É difícil testar a resistência da contenção com relação a todas as solicitações previstas, tanto no fim da construção e como em funcionamento. Os testes realizados efetivamente são de dois tipos:

- a) teste hidrostático a 1 bar manométrico durante a construção e no fim dos períodos de manutenção e reparo;
- b) verificação da variação da depressão durante a operação normal (índice de escape inferior a 2% da massa de ar em 24 h para uma depressão superior a 30mb), monitorando-se as variáveis de processo do sistema de ventilação.

ANEXO K

ANÁLISE PROBABILÍSTICA DE SEGURANÇA NUCLEAR

Os cálculos de probabilidade são utilizados nos estudos de segurança para avaliar a probabilidade de um evento. As análises probabilísticas também são aplicadas à perda de funções simples ou complexas, após a definição de um objetivo de risco. Os estudos deterministas tendem a aproximar-se dos estudos probabilísticos, considerando-se os três critérios seguintes:

- a) critério de probabilidade, ou seja, a expressão qualitativa (frequente, provável, ocasional, raro, improvável) da probabilidade de ocorrência de um fato;
- b) critério de gravidade, ou seja, a expressão qualitativa (desprezível, marginal, crítico, catastrófico) da consequência potencial mais grave do fato; e
- c) critério de criticidade, ou seja, a expressão do par (probabilidade, gravidade).

Nos estudos probabilísticos, o critério de probabilidade é definido de maneira quantitativa na forma de índice de falibilidade ou índice de reparabilidade e o critério de gravidade é definido de maneira quantitativa na forma de frequências anuais de ocorrência. Os estudos de segurança que decorrem disso consistem em calcular as probabilidades de perda de uma prestação ou ocorrência de uma agressão. Portanto, é necessário fazer uma ligação entre as noções de probabilidade e frequência.

Uma probabilidade, por definição, é um termo sem dimensão inferior ou igual a 1, enquanto que uma frequência pode ser superior a 1 e é expressa por unidade de tempo. Convém, portanto, introduzir duas noções: a noção de reparabilidade e a noção de perfil de missão.

Um material não reparável (ou seja, que não se pode ser reparado, nem substituído por um material em estoque), em uma determinada missão, apresentará uma certa probabilidade de pane. O valor dessa probabilidade será inferior a 1, e será igual à sua frequência de pane por missão, visto que não poderá, por definição, falhar uma segunda ou uma terceira vez durante a missão.

Caso uma determinada missão durar um ano, um material não reparável durante o período dessa missão terá uma probabilidade de falhar inferior a 1 e será igual à sua frequência de pane por missão.

Se uma certa missão durar por exemplo dois meses, e for refeita quatro vezes por ano, esse mesmo material não reparável durante o período dessas missões terá uma probabilidade de pane por missão inferior a 1, porém, a sua frequência de pane, inferior a 4 por ano, poderá ser superior a 1 por ano.

Para um material reparável no período de uma missão, independentemente de suas características (igual a 1 ano ou igual a 2 meses 4 vezes por ano), sua frequência de pane poderá ser superior a 1 por ano e será inferior a um valor determinado em função de sua reparabilidade, do número de sobressalentes em estoque e do número de missões por ano.

Constata-se, portanto, que a noção de frequência leva ao conhecimento das seguintes informações:

- a) o perfil da missão a considerar,
- b) a reparabilidade (ou manutibilidade) dos materiais (nível de manutenção, estoque disponível).

Essa constatação é importante, pois, ela induz que os estudos realizados devem integrar a noção de disponibilidade, impossível de ser representada na forma de árvores de falhas. Estas só permitem resolver de fato os fenômenos sequenciais que levam a um evento indesejado não repetitivo para um determinado material ou acidente. O problema pode ser ocultado, mas de modo majorante e pouco realista, levando em consideração a totalidade da duração da missão e o número de vezes em que o material pode ser reparado. Quanto aos modelos de disponibilidade, eles permitem considerar a noção de reparabilidade, considerando portanto os fenômenos repetitivos.

K.1 QUANTIFICAÇÃO DE UMA ANÁLISE PROBABILÍSTICA DE SEGURANÇA

O campo da quantificação probabilística ainda é novo: a confirmação dos estudos de segurança efetuados por uma metodologia determinista através de uma metodologia probabilística é recente e ainda é pouco difundida. A quantificação probabilística é, de todos

os aspectos da análise de segurança, o mais “político”, pois os resultados numéricos das análises pode ser objeto de infundáveis questionamentos e discussões. Por outro lado, a quantificação é freqüentemente indevidamente tratada como o aspecto final de uma análise probabilística de segurança.

Todo o material pode ser definido por três estados: em funcionamento, parado ou em pane. O índice de falha em funcionamento levando à passagem do estado “funcionamento” para o estado “em pane” é chamado de λ . Esse índice é em geral, especialmente em eletrônica, considerado como independente do tempo. Nesse caso, o tempo médio entre falhas (MTBF: Mean Time Between Failure) é igual ao inverso do índice λ . Esse índice pode ser função do tempo, especialmente em mecânica, integrando dessa forma os fenômenos de envelhecimento.

No caso mais geral, ou seja, quando o índice de falha em funcionamento é independente do tempo, a probabilidade que um determinado componente de índice λ falhe antes do instante T é definido pela lei:

$$P = 1 - \exp(-\lambda \cdot T) \quad (H.1)$$

O índice de falha na solicitação que induz a passagem do estado “parado” ao estado “em pane” é chamado de g . Por definição, trata-se de uma probabilidade de não funcionamento na solicitação, independente do tempo. Considerar esse fenômeno é primordial, às vezes mesmo dimensionante: lembre-se que tanto os componentes eletrônicos quanto os componentes mecânicos suportam mal um número elevado de solicitações, estas levando geralmente a carregamentos instantâneos superiores àqueles definidos pelas especificações.

Da mesma forma, por analogia, as probabilidades de erro humano são assimiladas a probabilidades na solicitação. O fator “tempo” (entre outros fatores) é integrado ao valor dessas probabilidades, mais ou menos altas conforme o tempo (mais ou menos longo) de reação de que dispõe o operador. Os erros humanos podem ser de cinco tipos: omissão, ação intempestiva, ação errada, não controle ou controle errado.

O índice de reparabilidade que induz a passagem do estado “em pane” ao estado “em funcionamento” ou “parado” é chamado de m . Esse índice é em geral considerado como independente do tempo. Nesse caso, o tempo médio de reparo (*Mean Time To Repair* MTTR) é igual ao inverso do índice m . Esse índice integra o conjunto das restrições ligadas ao reparo de um componente: detecção, diagnóstico, encaminhamento dos reparadores, encaminhamento do componente de troca (eventualmente) e dos instrumentos, formação e documentação dos reparadores, desmontagem, troca ou conserto, acessibilidade, remontagem, testes após o reparo. No caso mais geral, ou seja, quando o índice de reparabilidade é independente do tempo, a probabilidade de que um determinado componente de índice m seja reparado antes do instante T é definido pela lei:

$$P = 1 - \exp(-m \cdot T) \quad (H.2)$$

K.2 MÉTODOS DE QUANTIFICAÇÃO

Vai-se tratar aqui de quatro métodos de quantificação probabilística: os bancos de dados, o retorno de experiência, os resultados de testes e o método resistência-carregamento.

A quantificação pode ser efetuada ou dentro de um objetivo de previsão (para avaliar com antecedência o comportamento de um sistema), ou de um objetivo de observação (para avaliar a posteriori ou em tempo real o comportamento de um sistema). Entretanto, os dois se juntam: o observado no presente ou no passado ajuda a prever o futuro e a previsão presente é validada pelo observado futuro.

Bancos de Dados

Os bancos de dados de confiabilidade material provêm historicamente de tratamentos estatísticos de panes observadas no campo nuclear. Existem vários bancos de dados, desiguais tanto no que se refere à qualidade quanto aos campos técnicos que cobrem. Em geral, a separação é feita entre componentes não eletrônicos e componentes eletrônicos.

Esses bancos de dados são reatualizados, porém de forma bem espaçada (entre 5 a 10 anos), o que é prejudicial nos campos técnicos com grande desenvolvimento, como o eletrônico. Em contrapartida, nos campos técnicos que evoluem lentamente, os números indicados variam pouco de um índice para outro.

Os bancos de dados de confiabilidade humana são menos diretamente aplicáveis, os erros humanos são muito específicos conforme o tipo de pessoal e de sistemas estudados. Fornecem, por outro lado, informações interessantes na hierarquização das probabilidades de erros humanos, a partir dos quais podemos inspirar-nos de maneira analógica. Em geral, distinguem-se os erros humanos observados durante as atividades de rotina como os testes ou as atividades de manutenção e os erros humanos observados durante a atividade de reflexão, como a escolha e a prática de um procedimento incidental ou acidental. Naturalmente, é essa segunda categoria de erro que é a mais difícil e a mais importante.

Retorno de Experiência

O método conhecido como retorno de experiência consiste em analisar as panes observadas durante a operação de um sistema ou de um equipamento, determinando de maneira estatística as leis que definem os mal funcionamentos desse sistema ou desse equipamento. A exploração do retorno de experiência é uma análise que permite obter resultados ricos em informação, especialmente se trata de materiais específicos, para os quais os bancos de dados são pouco aplicáveis.

Resultados de Testes

O acompanhamento estatístico de testes é o método mais acurado para se poder quantificar as panes de um equipamento ou de um sistema. Formulam-se, entretanto, três tipos de críticas referentes a esse método.

- a) o primeiro consiste em pensar que os testes não duram o suficiente para serem estatisticamente representativos.
- b) o segundo consiste em pensar que os testes não são representativos do funcionamento durante a operação real do equipamento.
- c) o terceiro consiste em pensar que os teste servem principalmente para corrigir eventuais falhas de desempenho de um equipamento, e que, por conseguinte, as panes observadas durante os testes não representam de forma alguma o seu funcionamento durante a exploração.

Método da Resistência-Carregamento

Esse método tem como objetivo calcular a probabilidade de falha de uma estrutura em função da probabilidade de sua resistência e da probabilidade de ocorrência dos carregamentos que serão exercidos sobre ela.

K.3 ANÁLISE PROBABILÍSTICA DE SEGURANÇA GLOBAL

A tendência atual é de generalizar a abordagem probabilística, buscando determinar globalmente para o reator, o nível de risco efetivamente incorrido, comparado ao objetivo pré-estabelecido.

Foi nos Estados Unidos, em 1975, que foi apresentado o primeiro estudo global de risco de fusão de núcleo. Os estudos probabilísticos terão um papel importante na análise da segurança dos reatores do futuro. O objetivo probabilístico estabelecido para os futuros reatores europeus é de menos de uma chance em um milhão por ano de ver produzir-se um acidente com conseqüências graves em uma central nuclear, o que corresponde a um acidente por vinte mil anos de funcionamento em um parque de cinquenta reatores nucleares.

O princípio dos métodos probabilísticos é de partir de um evento inicializador, como a ruptura de uma tubulação, uma perda de energia elétrica ou uma manobra errada de um operador. A partir desse evento inicial, a evolução do cenário depende dos meios de controle disponíveis, dependendo, portanto, da disponibilidade de equipamentos e sistemas susceptíveis de falharem e das intervenções dos operadores, eventualmente errôneas.

A probabilidade que evento inicializador desencadeie um acidente grave provém de um série de falhas materiais ou erros humanos. Representa-se as seqüências acidentais através de uma árvore de conseqüências onde cada ramo corresponde a uma hipótese de falha. A análise da árvore permite determinar os ramos que levam ao acidente e obter a probabilidade global através da combinação dos índices de falha dos ramos.

Esses estudos fundam-se em dados de confiabilidade dos componentes onde o erro médio sobre os valores disponíveis é da ordem de um fator 2 a 3 e sobre os dados de confiabilidade humana, campo no qual é ainda mais difícil ter dados confiáveis.

O interesse de análise probabilística que forneça uma avaliação global reside sobretudo na análise de todos os fatores em jogo e na evidência dos pontos relativamente fracos da instalação.

ANEXO L

ANÁLISE DE SEGURANÇA DO NAVIO NUCLEAR

L.1 ANÁLISE FUNCIONAL DAS PRESTAÇÕES

O objetivo da análise funcional é representar o funcionamento de um sistema, em particular sua lógica, suas interfaces, seus requisitos e componentes. O principal interesse em fazer-se uma análise funcional antes de passar-se diretamente aos componentes consiste em deixar livre escolha ao projetista quanto aos meios a empregar para atender às funções requeridas. O outro interesse em passar por uma etapa funcional consiste em poder integrar o mais cedo possível certos critérios pouco identificáveis em termos de meios ao início do projeto de um sistema.

Assim, se for definido desde o início do projeto que a instalação nuclear tem necessidade de determinados serviços fornecidos pelo navio, torna-se mais simples especificar os objetivos detalhados destes serviços, antes de conhecer as características particulares dos sistemas, equipamentos e componentes que irão efetivamente prestá-los.

Numa primeira etapa, o nível de decomposição da análise funcional deve ter como objetivo somente a determinação das interfaces entre a plataforma-navio e a instalação nuclear e instalações de apoio em terra.

Numa segunda etapa, deve ter como objetivo a determinação das interfaces internas à plataforma-navio entre as diversas prestações de serviços requeridas. Nesse segundo nível, a análise funcional deve integrar:

- a) em termos de requisitos, o perfil de missão da plataforma-navio e as funções que ele desempenha conforme a situação de operação;
- b) em termos materiais, o arranjo físico e funcional; é preferível, para uma melhor compreensão da decomposição funcional, que os meios materiais que correspondem às várias funções analisadas reproduzam da forma mais próxima possível, a decomposição física da plataforma-navio.

O método adequado à análise funcional das prestações de serviço do navio à instalação nuclear é o chamado SADT. (Structured Analysis and Design Technic), orientado para o projeto. A análise pelo método SADT é realizada através da construção de um modelo de forma descendente, modular, hierárquica e estruturada, diferenciando o aspecto funcional (quais são as funções a serem asseguradas?) do aspecto material (com que meios o sistema realizará suas funções?). A coerência do conjunto dos vários níveis do diagrama realiza-se através de um programa computacional. O interesse do método é o seguinte:

- a) fornecer uma modelização do sistema tão fina quanto for necessário;
- b) evidenciar para cada função o conjunto das interfaces com o resto do sistema, assim como com o seu meio-ambiente;
- c) dissociar os aspectos funcionais do projeto do sistema dos componentes específicos que executam as funções.

Em particular, destaca-se para cada função ou sub-função:

- a) dados de entrada que são transformados pela realização da função;
- b) saídas correspondendo à transformação dos dados de entrada;
- c) os mecanismos que permitem o desempenho da função;
- d) as restrições do meio ambiente.

A aplicação de SADT começa com a descrição mais geral ou a mais abstrata do sistema. Essa função principal contida em uma bloco, fragmenta-se em blocos mais detalhados, cada um representado uma função maior do bloco inicial. Cada um desses blocos decompõe-se novamente para expor a informação que contém. As interfaces entre as várias funções são realizadas por flechas, definidas da seguinte maneira:

- a) Entrada E: dados transformados ou utilizados pela função
- b) Saída S: dados criados pela função
- c) Mecanismo M: meios que realizam a função
- d) Restrições R: restrições ao desempenho da função

A aplicação do método SADT na análise funcional das prestações de serviços, permite identificar claramente as interfaces que existem:

- a) entre as instalações e suas prestações diretas;

- b) entre essas prestações diretas e seus serviços, que são portanto prestações indiretas;
- c) entre essas prestações e as instalações de apoio em terra.

FIGURA L.1: BLOCO BÁSICO SADT

As interfaces, que são as entradas e as saídas das funções, e os materiais aplicados dependem das configurações navio/instalação nuclear que constituem os requisitos de desempenho da função. O modelo de aplicação do método SADT é apresentado pela Figura L.2, descrito a seguir:

- a) a função Z é uma função que pertence à plataforma-navio; compreende uma prestação direta da função T, que pertence à instalação nuclear; ela é garantida pelos materiais Z_n e $Z_{(n+1)}$;
- b) a função Y é uma função que pertence à plataforma-navio; compreende uma prestação direta da função Z que também pertence à plataforma-navio; trata-se portanto de uma prestação indireta da função T que pertence à instalação nuclear; ela é assegurada pelos materiais Y_n e $Y_{(n+1)}$ por um lado, $Y_{(n+2)}$, por outro;
- c) a função V é uma função pertencente à plataforma-navio; trata-se de uma prestação direta da função Y que pertence também à plataforma-navio; é também, pela função Z, uma prestação indireta da função T que faz parte da instalação nuclear;
- d) a função W é uma função que pertence à plataforma-navio; é servida pela função Y que pertence também à plataforma-navio;

- e) a função X é uma função que pertence ao apoio em terra; trata-se de uma prestação direta da função Y que pertence à plataforma-navio; é também, pela função Z, uma prestação indireta da função T que pertence à instalação nuclear;
- f) as energia Ye e Ze são aquelas que são necessárias à realização das funções Y e Z.
- g) as energias Ys e Zs são aquelas que são transformadas pela realização das funções Y e Z;

FIGURA L.2: APLICAÇÃO DO SADT

L.2 ANÁLISE PRELIMINAR DE RISCOS

Foi visto anteriormente que a análise funcional constituía o instrumento indispensável na análise das prestações de serviços da plataforma-navio à instalação nuclear. A análise das agressões da plataforma-navio à instalação nuclear deve ser realizada através de uma análise preliminar de riscos.

Esse procedimento tem como objetivo realizar um recenseamento exaustivo e sem idéias pré-concebidas do conjunto dos riscos incorridos pela instalação nuclear devido ao fato de estar embarcada. Esses riscos estão ligados à proximidade de fontes potenciais de agressões a bordo do navio (agressões geradas pelo próprio navio) ou ligadas à existência de fontes potenciais de agressões no ambiente onde o navio se encontra (agressões veiculadas pelo navio). Esses riscos decorrem de:

- a) amplitudes e velocidades anormais de variação da potência demandada (manobras bruscas de aceleração ou desaceleração do navio);
- b) ângulos de inclinação, deslocamentos, velocidades e acelerações extremas da plataforma devido ao comportamento do navio no mar (“seakeeping”);
- c) choques (carregamentos mecânicos dinâmicos impulsivos) devido à denotação de cargas explosivas próximas proveniente de armamentos inimigos;
- d) choques devido a explosões internas de misturas gasosas ou aerosóis, ou devido à presença de armas, munições ou outras cargas explosivas a bordo do navio;
- e) choques devido a acidentes durante operações conjuntas do navio com aeronaves (helicópteros, no caso de submarinos, mas também aeronaves de asa fixa no caso de navios aeródromos);
- f) contaminação físico-química de fluidos de processo;
- g) anomalias na composição da atmosfera interna do navio, comprometendo a habitabilidade de compartimentos cujo acesso é necessário para a operação ou reparo da instalação nuclear
- h) incêndios internos ao navio;
- i) alagamentos devido à perda de estanqueidade do casco do navio ou de tubulações internas de água do mar (água aberta);
- j) efeitos secundários (borrifos, chicoteamento, contaminação local, corrosão) de rupturas de tubulações;
- k) perturbações eletromagnéticas de origem interna ou externa ao navio;
- l) as chamadas “fortunas do mar”: encalhe, naufrágio e abalroamento (colisão), e ainda choque com o fundo e mergulho a cota superior à máxima de operação, no caso de submarinos.

Devem então serem tomadas disposições construtivas e operacionais especiais para o navio de forma a limitar esses riscos. A classificação das várias categorias de situações levam em conta os riscos residuais com a ordem de grandeza de sua probabilidade de ocorrência. A análise preliminar dos riscos deve indicar:

- a) conjunto das agressões potencialmente geradas ou veiculadas pelo navio;
- b) situações de operação do navio e das instalações nucleares, já que as causas e as conseqüências de agressões são diferentes segundo cada situação particular;
- c) causas das agressões (para as agressões potencialmente geradas pelo navio: sistemas, componentes e materiais ou operações que originam as agressões, assim como sua localização) e as características dessas causas (parâmetros na fonte de agressão);
- d) suas conseqüências (impacto sobre os sistemas, componentes e materiais da plataforma, incluídas a instalação nuclear e resto do navio, impacto sobre a tripulação, pessoal de apoio em terra, público) e as características dessas conseqüências (parâmetros finais),
- e) barreiras de defesa em profundidade (prevenção, detecção, mitigação).

A maior parte do trabalho consiste em avaliar as características das agressões em termos de causas e conseqüências, analisando numa primeira etapa as funções de transferência entre as fontes e os receptores potenciais. A análise das conseqüências deverá analisar numa segunda etapa, a sensibilidade dos sistemas, componentes e materiais potencialmente receptores de agressões.

Essas análises poderão ser feitas de forma quantitativa, com cálculos ou ensaios, ou de forma qualitativa, referindo-se sistematicamente aos domínios de operação resultantes.

Essa análise qualitativa será muito facilitada, se os domínios de operação forem perfeitamente caracterizados e se as especificações do conjunto dos sistemas, componentes e materiais forem perfeitamente definidas em relação a esses domínios.

É de suma importância a análise de cenários em que ocorra a propagação entre agressões, especialmente indesejados, com toda razão, pelas autoridades de segurança. Compreende-se por “propagação” o fato de uma agressão inicial gerar uma outra agressão já definida na análise preliminar dos riscos. O procedimento consiste, seja de maneira determinística ou de maneira probabilística, em:

- a) avaliar a possibilidade de propagação entre agressões (por exemplo, uma explosão pode levar a um incêndio, o qual pode levar a uma agressão elétrica, e assim sucessivamente),
- b) verificar a homogeneidade dos níveis de criticidade das agressões (por exemplo, uma explosão que leva automaticamente a um incêndio não deve ter uma criticidade menor que a criticidade do incêndio resultante).

Levar em conta os modos comuns é primordial. Constata-se, de fato, durante a análise funcional, que as prestações dentro da plataforma-navio se superpõe em muitos casos, pois as necessidades da instalação nuclear, tais como eletricidade, resfriamento, ar comprimido, transmissões, são comuns para o resto do navio. Por exemplo, o funcionamento de certos componentes de um quadro elétrico precisam de resfriamento, fornecido por sua vez por bombas que precisam de alimentação elétrica.

Portanto, a determinação das interfaces entre as prestações é indispensável para levar-se em conta modos comuns dentro da plataforma-navio. Ela também permitirá avaliar a verossimilhança dos eventos indesejado e dos objetivos detalhados de segurança que lhe serão designados.

A análise preliminar de riscos permitirá determinar os equipamentos da plataforma-navio importantes para a segurança. Estes equipamentos são classificados nas categorias 1M, 2M, 3M, 1E e 2E:

- a) os equipamentos e estruturas que constituem a terceira barreira e os equipamentos e serviços indispensáveis ao funcionamento as válvulas de isolamento da contenção;
- b) os equipamentos dos sistemas auxiliares indispensáveis para o funcionamento do sistema de proteção do reator, incluindo sua instrumentação e os acionadores associados.

São ainda classificados na categoria Z:

- a) os equipamentos de serviços necessários para o funcionamento dos EIS da instalação com a disponibilidade exigida;
- b) os equipamentos que participam da gestão a longo prazo dos acidentes de dimensionamento ou que participam especificamente na gestão dos acidentes graves.

L.3 ANÁLISE DOS MODOS DE FALHAS, EFEITOS E CRITICIDADE

A análise dos modos de falhas, de seus efeitos e de sua criticidade (AMFEC) é um método que constitui a ferramenta básica da análise de segurança. Ela apresenta-se na forma de quadros, constituídos pelas colunas a seguir identificadas. Note-se que, visando a homogeneidade, a lista dos elementos e das funções é uma saída direta da análise funcional detalhada realizada previamente.

- a) Elementos;
- b) Funções.
- c) Modos de falhas,
- d) Causas,
- e) Dados quantitativos:
 - índice de falhas em funcionamento ou tempo médio entre panes (*l* ou MTBF),
 - índice de falhas por solicitação (*g*), eventualmente
 - eventualmente índice de reparabilidade ou tempo médio de conserto (*m* ou MTTR)
- f) Conseqüências locais,
- g) Conseqüências globais,
- h) Gravidade das conseqüências,
- i) Barreiras (prevenção, detecção, mitigação).

Observe-se que esse procedimento aplica-se tanto para a análise de componentes quanto para a análise da instalação como um todo. Quanto à análise de programas computacionais, o aspecto quantitativo ainda permanece no campo da pesquisa.

L.4 ANÁLISE POR ÁRVORE DE CAUSAS

A partir de um certo evento indesejado, a árvore de causas representa graficamente as combinações de eventos elementares que levam à sua realização.

A árvore de causas é portanto formada por eventos decompostos em níveis cada vez mais detalhados e precisos, sendo a transição entre níveis feita através de portas lógicas. A decomposição por dedução é feita até chegar-se a eventos elementares caracterizados pelos seguintes critérios:

- a) são eventos mutuamente independentes;
- b) são eventos que podem ser o objeto de uma quantificação probabilística,

c) são eventos cuja decomposição não se mostra relevante para os objetivos da análise.

A árvore de causas é uma representação gráfica de um sistema de equações booleanas a partir da qual é possível:

- a) deduzir todas as combinações de eventos elementares (chamados de cortes mínimos) levando à realização do evento indesejado,
- b) calcular a probabilidade de ocorrência do evento indesejado, a partir das probabilidades de ocorrência dos eventos elementares.

Os símbolos utilizados para representação gráfica de uma árvores de causas são:

- a) retângulo: representação de um evento elementar ou resultante da combinação de outros eventos através de uma porta lógica;
- b) círculo: caracterização de um evento elementar cuja probabilidade pode ser avaliada;
- c) losango: caracterização de um evento cuja decomposição é vista como suficiente e portanto considerada como elementar;
- d) duplo losango: caracterização de um evento cuja decomposição não é desenvolvida (fora estudo);
- e) “casa”: caracterização de um evento que se realiza normalmente;
- f) triângulos: decomposição por sub-árvore (envio idêntico).
- g) triângulos invertidos: Decomposição por sub-árvore análoga (envio análogo);
- h) porta OU: o evento do nível superior se realiza se um dos eventos do nível inferior ocorrer;
- i) porta E: o evento do nível superior realiza-se se todos os eventos do nível inferior ocorrerem;
- j) condição: o evento do nível superior realiza-se se a condição expressa for verdadeira;

L.5 MODELAGEM POR GRAFOS DE MARKOV E POR REDES DE PETRI

Emprega-se dois métodos para avaliar as probabilidades de ocorrência de eventos indesejados e para realizar os cálculos da disponibilidade de sistemas: os grafos de Markov e as redes de Petri.

As principais vantagens das redes de Petri em relação aos gráficos de Markov são as seguintes:

- a) a construção de um modelo por redes de Petri é mais simples graças à possibilidade de modelar condições e mensagens que levam a um pequeno número de lugares e transições;
- b) os resultados obtidos são mais ricos em informações, especialmente no que se refere ao número de tiragem de transições;
- c) permitem integrar leis de transição descontínuas em função do tempo.

As redes de Petri são construídas com a ajuda de “lugares”, “transições”, “condições” e “mensagens”:

- a) “lugares” representam os vários estados dos componentes de um sistema (funcionamento, parada, pane);
- b) “transições” representam as passagens de um estado para o outro e são definidas por leis:
 - lei L Pane em operação funcionamento→ pane;
 - lei G Pane na partida parada→pane;
 - lei M Reparo pane→funcionamento ou parada.
- c) “condições” são os dados que autorizam ou impedem a tiragem das transições;
- d) “mensagens” são os novos dados após a tiragem das transições que serão retomadas como “condições” de outras tiragens de transições;
- e) “condições” e as “mensagens” permitem portanto representar a lógica do funcionamento de um sistema.

Após ter fixado a duração de funcionamento e um número de “histórias” estatisticamente representativo, o funcionamento do sistema pode ser simulado por tiragem de Monte Carlo. Os cálculos efetuados permitem então conhecer:

- a) o “tempo de permanência” nos vários lugares, ou seja a disponibilidade e a indisponibilidade (temporária ou definitiva) dos diversos componentes;
- b) o número de tiragem das “transições”, ou seja a probabilidade de ocorrência de cada fato elementar ou de cada evento indesejado.

L.6 MÉTODOS ESPECÍFICOS DE ANÁLISE DE AGRESSÕES

A análise da ocorrência de agressões, se elas são causadas por mau funcionamento ou falhas de instalações, poderá utilizar os métodos anteriormente discutidos.

Por outro lado, a análise de certas causas de agressões, de suas funções de transferência e das conseqüências que induzem exige cálculos ou testes específicos, tais como cálculos de potenciais de fogo ou de ensaios de comportamento sob fogo (incêndio), cálculos de equivalente TNT e de sobre-pressão (explosões) e cálculos de avaliação de energia cinética (quedas, choques, projeção de fragmentos).

Se a análise da segurança das prestações fornecidas pela plataforma-navio da instalação nuclear consiste em raciocinar em termos funcionais, a análise da segurança das agressões geradas ou veiculadas por meio navio à instalação nuclear consiste em raciocinar em termos “geográficos”, isto é, através do Recenseamento e Classificação dos Locais de Risco.

Dessa forma, pode-se proceder paralelamente as duas análises, especialmente analisando-se a “sensibilidade” geográfica das agressões da mesma forma que se analisa a “sensibilidade” funcional das prestações.

Chamaremos de “sensibilidade” o critério que permite definir o número de eventos elementares necessários para atingir um evento indesejável: por exemplo, dois elementos em redundância designados para a realização de uma dada função são de sensibilidade 2 no que se refere a essa função. Se esses dois elementos situam-se em dois locais diferentes, cada um desses locais é de sensibilidade 2; se eles se situam no mesmo local, este é de sensibilidade 1.

O objetivo de uma análise de recenseamento e de classificação dos locais sensíveis de um navio é, em uma primeira etapa, realizar uma cartografia do navio, hierarquizando os compartimentos e áreas específicas que o constituem em função da sensibilidade funcional dos materiais que eles contêm. Numa segunda etapa, quando os objetivos de FAO tiverem sido estabelecidos, será possível refinar essa cartografia, levando-se em conta a gravidade dos materiais contidos em cada área cuja lista terá sido feita anteriormente. Numa terceira etapa, o mapa obtido poderá ser comparado com uma outra cartografia do navio, representando a probabilidade de agressões.

Esse trabalho vai permitir recensear zonas críticas de compartimentação e deduzir soluções para minimizar os riscos corridos (prevenção, detecção, mitigação).

ANEXO M

ORGANIZAÇÃO DA RADIOPROTEÇÃO A BORDO

Os estudos de projeto de radioproteção buscam, em situações normais de exploração e em situações incidentais e acidentais:

- a) reduzir os equivalentes de doses suscetíveis de serem recebidas pelo pessoal,
- b) permitir a vigilância das zonas de risco.

A regulamentação geral impõe uma repartição do pessoal em categorias e a criação de zonas ao redor das fontes radioativas. O objetivo do projeto é então o dimensionamento das proteções biológicas para otimizar os meios empregados para atender à regulamentação.

Em função do conceito de emprego militar e do perfil de operação previsto para o navio, o tempo de permanência de cada categoria de pessoal em cada local é estimado para as CPIN de categorias 1 e 2.

Tendo em conta os equivalentes de dose determinados por categoria de pessoal, deduzem-se os fluxos de equivalente de dose máximos admissíveis por local, para uma determinada situação de operação da instalação. Esses locais podem então ser repartidos em diferentes zonas, considerando esses fluxos de dose. As proteções biológicas são dimensionadas para respeitar essa classificação por zonas.

O projeto é conduzido de forma a otimizar o arranjo, minimizando o peso das proteções e as doses. Para o estudo das condições incidentais e acidentais CPIN3 e CPIN4, é preciso determinar, no contexto da regulamentação militar específica, os equivalentes de dose permitidos para o pessoal mais exposto durante o evento, determinar os locais onde o pessoal deverá intervir, assim como a duração dessas intervenções, verificando que estas serão viáveis do ponto de vista radiológico. Caso for necessário, será preciso melhorar a proteção biológica e, em caso de impossibilidade, definir disposições específicas de operação da instalação acidentada, da propulsão em emergência e do resto do navio.

As consequências de emissão de radiações para fora do navio devem ser examinadas segundo as situações de operação. A extensão eventual das zonas fora do navio a serem

analisadas é definida de acordo com a regulamentação aplicável à posição geográfica do navio (porto, zona costeira, zona oceânica).

M.1 BLINDAGENS RADIOLÓGICAS

A blindagem dos reatores de propulsão naval deve atender aos requisitos internacionais de limitação de doses com mínimo peso e volume e empregando materiais compatíveis com o emprego naval. Para tal o navio é dividido em zonas definidas conforme sua frequência de ocupação pela tripulação. A blindagem radiológica é dividida em blindagem primária e blindagem secundária.

A blindagem primária atende aos seguintes requisitos funcionais:

- a) suficiente atenuação do fluxo de nêutrons para prevenir:
 - geração de atividade induzida nas estruturas externas à blindagem;
 - excessiva ativação do fluido secundário;
 - geração de raios gama de captura na blindagem secundária.
- b) redução do nível total de radiação para permitir acessibilidade limitada após o desligamento do reator com objetivo de execução de atividades de manutenção em componentes localizados entre as blindagens primária e secundária

A blindagem secundária atende aos seguintes requisitos funcionais:

- a) atenuação da radiação proveniente do reator, do fluido primário e de todos os componentes de forma a permitir um fluxo de dose permissível nas zonas adjacentes fora do compartimento do reator;
- b) prevenção de vazamentos (*streaming*) de radiação através das penetrações, tais como as tubulações de vapor e de água de alimentação;
- c) proporcionar proteção adicional em caso de acidentes onde haja liberação de materiais radioativos para o interior do compartimento do reator; já que o reator estará desligado neste caso, a blindagem secundária é essencialmente uma blindagem para raios gama.

O espaço sob o reator, no fundo do navio, usualmente não requer uma blindagem completa, já que a água do mar proporciona a blindagem adicional necessária para operação a máxima potência. Entretanto, os efeitos de espalhamento (*backscattering*) devem ser

considerados. As atividades de manutenção no fundo do navio devem ser possíveis em estaleiro após um tempo razoável de desligamento do reator (24h, por exemplo).

A estrutura da blindagem para um reator naval deve suportar os movimentos e acelerações do navio. A Figura M.1 apresenta os princípios gerais de projeto.

FIGURA M.1: ESQUEMA GERAL DE BLINDAGEM DE UM REATOR NAVAL

M.2 DELIMITAÇÃO POR ZONAS

A bordo tem-se três tipos de zonas radiológicas:

- a) a zona controlada,
- b) a zona vigiada,
- c) a zona não vigiada, que corresponde ao resto do navio não classificado em a) ou b).

A zona controlada é constituída pelo conjunto de locais onde o pessoal que deve nela permanecer pode receber um equivalente de dose anual devido a irradiação externa e interna (contaminação) superior a 15 mSv (1,5 rem). Considerando-se que o pessoal ocupa 30% do seu tempo na zona controlada e que o reator tem um fator de utilização também de 30%, tem-se um máximo de fluxo de dose permissível da ordem de 15 μ Sv/h (1,5mrem/h) para o reator operando na sua potência máxima nominal. O acesso na zona controlada é regulamentado.

Dentro da zona controlada, pode-se criar zonas de permanência administrativamente limitada se os riscos radiológicos forem tais que, apesar da medidas de segurança, o pessoal não poderá nelas permanecer por períodos superior a um limite estabelecido. Quando o fluxo de equivalente de dose ultrapassar 100mSv/h (10rem/h), a zona fica normalmente interdita. O acesso às zonas interditas será submetido a um procedimento específico de autorização.

A zona vigiada é aquela contígua à zona controlada. O pessoal que deve normalmente permanecer nesse local pode receber, em função da irradiação ambiente, um equivalente de dose anual superior a 5mSv (0,5rem), mas inferior a 15mSv (1,5rem). Considerando-se que o pessoal ocupa 30% do seu tempo na zona vigiada e que o reator tem um fator de utilização também de 30%, tem-se um máximo de fluxo de dose permissível da ordem de 5 μ Sv/h (0,5mrem/h) para o reator operando na sua potência máxima nominal.

Os limites da zona vigiada são adaptados em função das situações de operação da instalação nuclear e dos riscos radiológicos correspondentes. O acesso à zona vigiada não é regulamentado.

A zona não vigiada compreende o conjunto dos locais em que o pessoal que neles deve permanecer normalmente não pode receber o equivalente de dose superior a 5mSv (0,5rem). Pode-se distinguir:

- a) uma zona permanente onde a estadia normal pode chegar a 24 por 24 horas, com um máximo de fluxo de dose permissível da ordem de 1,5μSv/h (0,15mrem/h) para o reator operando na sua potência máxima nominal.
- b) uma zona semi-permanente onde a estadia normal não ultrapassa 12 horas por dia, com um máximo de fluxo de dose permissível da ordem de 3μSv/h (0,3mrem/h) para o reator operando na sua potência máxima nominal.

M.3 OBJETIVOS GERAIS POR CATEGORIA DE PESSOAL

O pessoal que pode ser encontrado a bordo do navio nuclear é dividido em três categorias:

- a) categoria 1: pessoas diretamente envolvidas em trabalhos sob radiações ionizantes;
- b) categoria 2: pessoas não envolvidas diretamente, de forma habitual, em trabalhos sob irradiações ionizantes;
- c) categoria 3: pessoas não pertencentes às duas categorias anteriores, chamadas de público.

A regulamentação determina limites de equivalente de dose individuais. Para o projeto, entretanto, são estabelecidos objetivos mais rígidos e detalhados, de modo a:

- a) obter a maior margem razoavelmente possível em relação aos limites regulamentares de equivalentes de dose individuais para o pessoal categoria 1 e 2 ,
- b) atingir um objetivo de equivalente de dose média para o pessoal categoria 1 significativamente inferior ao limite regulamentar.

M.4 SITUAÇÕES RADIOLÓGICAS CONSIDERADAS

A definição do perfil de missão do navio, detalhando os ciclos de funcionamento e de potência das instalações, assim como os métodos de operação (número de postos de trabalho, número de pessoas por posto, ritmo de rotatividade da tripulação), permitem determinar as doses recebidas pelo pessoal envolvido e pelo público em situações normais de exploração. Em caso de acidente com consequências radiológicas, os limites de equivalente

de dose integrada pessoal envolvido são elevados a 120mSv (12rem) para o pessoal categoria 1. Para as outras categorias os limites individuais são mantidos.

Na medida do possível e, em particular, para as zonas controladas permanentes, os limites das zonas radiológicas coincidem com aqueles dos compartimentos. Os locais classificados em zona controlada e em zona vigiado são submetidos a uma vigilância radiológica permanente, permitindo detectar um aumento anormal do nível de irradiação (gama e nêutrons, se necessário) e do nível de contaminação atmosférico e superficial desses locais. Na zona controlada soma-se a vigilância individual.

A vigilância em condição acidental deve ser prevista, incluindo a existência de posto de operação em emergência, a possibilidade de medida dos fluxos de dose fortes, existência de meios mínimos para controle da contaminação e da irradiação em zona vigiada, possibilidade de integração de fluxos de dose medidos em certos locais representativos.

ANEXO N

DETERMINAÇÃO DA VELOCIDADE DE AFUNDAMENTO

Após a flutuabilidade do submarino tornar-se negativa, o afundamento pode ser descrito pela seguinte equação diferencial:

$$m \frac{dv}{dt} + W \cdot v^2(t) = U_{\max} \quad [N-1]$$

onde: m = massa do submarino, incluindo massa adicional hidrodinâmica e a massa de água embarcada por alagamento;
 $U_{\max}$ = força de empuxo negativa máxima;
 v = velocidade vertical de afundamento
 t = tempo
 W = arrasto específico = $c \cdot A \cdot \rho / 2$
 c = coeficiente de arrasto
 A = seção reta do submarino projetada no plano horizontal
 ρ = densidade da água do mar

Para valores constantes de U e m , a solução desta equação é:

$$v(t) = v_f \tanh(b_0 \cdot t / v_f) \quad [N-2]$$

onde: $v_f = (U / W)^{1/2}$ = velocidade final
 $b_0 = U / m$ = aceleração inicial

As seguintes condições iniciais devem ser usadas para a avaliação deste modelo:

- a) Quando o afundamento começa, a flutuabilidade e a velocidade são nulas;
- b) O afundamento se inicia com o alagamento total do compartimento do reator na profundidade máxima de operação, considerando os demais compartimentos intactos, dentro de um período de tempo compatível com os dispositivos de inundação voluntária disponíveis.

As seguintes condições durante o alagamento devem ser assumidas no modelo:

- a) Na profundidade de projeto da estrutura resistente, escotilhas e válvulas do casco ocorre ruptura e alagamento instantâneo de todos os compartimentos intactos;
- b) Não são considerados movimentos no plano horizontal.

ANEXO O

ITEMIZAÇÃO PROPOSTA PARA O RELATÓRIO DE ANÁLISE DE SEGURANÇA

1. INTRODUÇÃO
 - 1.1 DESCRIÇÃO GERAL
 - 1.1.1 Características do Submarino
 - 1.1.2 Características da Instalação Propulsora Nuclear
 - 1.1.3 Comparação com Submarinos e Instalações Propulsoras Semelhantes
 - 1.2 IDENTIFICAÇÃO DAS ORGANIZAÇÕES ENVOLVIDAS
 - 1.2.1 Organização Operadora
 - 1.2.2 Organizações Envolvidas no Projeto e Construção
 - 1.2.3 Organizações Envolvidas no Comissionamento e Manutenção
 - 1.2.4 Autoridade de Segurança Nuclear e Órgãos de Supervisão Técnica Independente
 - 1.3 CICLO DE VIDA DO SUBMARINO
 - 1.3.1 Conceito de Emprego
 - 1.3.2 Perfil de Vida Útil
 - 1.3.3 Cronograma do Processo de Obtenção
 - 1.4 PRINCÍPIOS GERAIS DE SEGURANÇA
 - 1.4.1 Segurança Naval do Submarino
 - 1.4.2 Segurança Nuclear da Instalação Propulsora
 - 1.5 REFERÊNCIAS
 - 1.5.1 Documentos de Engenharia
 - 1.5.2 Relatórios Técnicos
 - 1.5.3 Documentos de Referência Gerais (não normativos)
 - 1.5.4 Informações Técnicas Pendentes
2. OBJETIVOS, CRITÉRIOS E REQUISITOS DE SEGURANÇA
 - 2.1 BASE NORMATIVA
 - 2.1.1 Normas de Segurança e de Licenciamento

- 2.1.2 Normas de Garantia da Qualidade
- 2.1.3 Normas de Projeto e Construção
- 2.1.4 Normas de Testes e Comissionamento
- 2.1.5 Normas de Operação
- 2.1.6 Normas de Manutenção e Reparos
- 2.2 OBJETIVOS
 - 2.2.1 Objetivos Gerais de Segurança
 - 2.2.2 Objetivos Detalhados de Segurança
 - 2.2.3 Análise do Atendimento aos Objetivos
- 2.3 CRITÉRIOS GERAIS
 - 2.3.1 Critérios Gerais de Projeto
 - 2.3.2 Critérios Gerais de Operação
 - 2.3.3 Classificação de Estruturas, Componentes e Sistemas
 - 2.3.4 Qualificação de Estruturas, Componentes e Sistemas
 - 2.3.5 Qualificação de Metodologias de Projeto e Análise de Estruturas, Componentes e Sistemas
 - 2.3.6 Agressões Externas ao Submarino
 - 2.3.7 Agressões Externas à IPN Originadas pelo Submarino
- 2.4 REQUISITOS ESPECÍFICOS
 - 2.4.1 Radioproteção da tripulação
 - 2.4.2 Gerenciamento de Rejeitos e Efluentes
 - 2.4.3 Proteção e Combate a Incêndios
 - 2.4.4 Proteção e Combate a Alagamentos
 - 2.4.5 Prevenção de Falhas de Causa Comum
 - 2.4.6 Segurança Física
- 3. CARACTERÍSTICAS DE LOCAL
 - 3.1 DIAGNÓSTICO AMBIENTAL DAS ÁREAS MARÍTIMAS DE OPERAÇÃO
 - 3.1.1 Oceanografia Física
 - 3.1.2 Meteorologia
 - 3.1.3 Oceanografia Biológica

- 3.1.4 Níveis Radiológicos de Referência
- 3.1.5 Cadeias Alimentares Significativas
- 3.1.6 Rotas de Tráfego Marítimo
- 3.2 IMPACTO AMBIENTAL NAS ÁREAS DE MOBILIDADE
 - 3.2.1 Dispersão de Materiais Radioativos nas Águas Oceânicas
 - 3.2.2 Transferência de Materiais Radioativos através das Cadeias Alimentares
 - 3.2.3 Mitigação de Consequências de Acidentes
 - 3.2.4 Análise da Aceitabilidade das Áreas Marítimas
- 3.3 DIAGNÓSTICO AMBIENTAL DA LOCALIZAÇÃO FIXA
 - 3.3.1 Efeitos Externos
 - 3.3.2 Geologia e Sismologia (Bases de Projeto Sísmico)
 - 3.3.3 Meteorologia
 - 3.3.4 Hidrologia
 - 3.3.5 Atividades Industriais, de Transportes e Militares nas Vizinhanças
 - 3.3.6 Distribuição Populacional
 - 3.3.7 Ecologia Regional e Uso da Terra e das Águas
 - 3.3.8 Níveis Radiológicos de Referência
- 3.4 IMPACTO AMBIENTAL NA LOCALIZAÇÃO FIXA
 - 3.4.1 Dispersão Atmosférica de Materiais Radioativos
 - 3.4.2 Dispersão de Materiais Radioativos através de Águas de Superfície e Subterrâneas
 - 3.4.3 Mitigação de Consequências de Acidentes
 - 3.4.4 Análise da Aceitabilidade das Localizações Fixas
- 4. PLATAFORMA-NAVIO
 - 4.1 ESTRUTURAS
 - 4.1.1 Casco Resistente
 - 4.1.2 Penetrações e Aberturas de Acesso
 - 4.1.3 Conveses, Plataformas e Anteparas
 - 4.1.4 Casco Não-Resistente
 - 4.2 ARRANJO GERAL
 - 4.2.1 Sub-divisão e Estabilidade

- 4.2.2 Proteção Contra Colisões
- 4.2.3 Proteção Contra Choques
- 4.2.4 Proteção Contra Incêndios
- 4.2.5 Proteção Contra Alagamentos
- 4.2.6 Proteção Contra Encalhe e Pouso no Fundo
- 4.2.7 Segurança Física do Navio e do Material Físsil
- 4.3 NAVEGAÇÃO E MANOBRA
 - 4.3.1 Auxílios à Navegação
 - 4.3.2 Comunicações Exteriores
 - 4.3.3 Sistemas de Governo e Profundidade
 - 4.3.4 Aparelho de Suspende e Fundear
 - 4.3.5 Dispositivos para Socorro e Salvamento
- 4.4 VENTILAÇÃO E CONDICIONAMENTO DE AR
- 5. INSTALAÇÃO NUCLEAR
 - 5.1 CRITÉRIOS GERAIS DE PROJETO
 - 5.1.1 Combustível
 - 5.1.2 Reator
 - 5.1.3 Circuito Primário
 - 5.1.4 Circuito Secundário
 - 5.2 REATOR
 - 5.2.1 Descrição Sumária
 - 5.2.2 Elementos Combustíveis
 - 5.2.3 Sistemas de Controle da Reatividade
 - 5.2.4 Projeto Neutrônico
 - 5.2.5 Projeto Termohidráulico
 - 5.2.6 Materiais do reator
 - 5.3 SISTEMAS DE RESFRIAMENTO DO REATOR
 - 5.3.1 Sistema de Resfriamento Primário
 - 5.3.2 Sistema de Resfriamento Secundário
 - 5.3.3 Sistema de Resfriamento em Emergência

- 5.3.4 Sistema de Remoção de Calor Residual
- 5.3.5 Sistema de Reposição e Controle Químico do Refrigerante Primário
- 5.4 SISTEMAS DE CONTENÇÃO E CONFINAMENTO DE MATERIAIS RADIOATIVOS
 - 5.4.1 Compartimento de Contenção
 - 5.4.2 Penetrações e Acessos ao Compartimento de Contenção
 - 5.4.3 Sistemas de Controle Ambiental da Contenção
 - 5.4.4 Dispositivos de Segurança do Compartimento de Contenção
 - 5.4.5 Compartimentos de Confinamento
 - 5.4.6 Sistemas de Controle Ambiental do Confinamento
- 5.5 INSTRUMENTAÇÃO E CONTROLE
 - 5.5.1 Sistema de Proteção do Reator
 - 5.5.2 Sistema de Controle de Potência
 - 5.5.3 Sistemas de Monitoração e Alarme
 - 5.5.4 Intertravamentos
 - 5.5.5 Estação de Controle da Instalação Propulsora
- 5.6 PROJETO MECÂNICO DE COMPONENTES
 - 5.6.1 Barreira de Pressão do Circuito Primário
 - 5.6.2 Carregamentos Estáticos
 - 5.6.3 Carregamentos Mecânicos
- 5.7 INTERFACES ENTRE SISTEMAS NUCLEARES E NAVAIS
- 5.8 CARGA E RECARGA DE COMBUSTÍVEL NUCLEAR
- 6. INSTALAÇÕES DE MÁQUINAS
 - 6.1 PROPULSÃO
 - 6.1.1 Acionamento do Eixo Propulsor
 - 6.1.2 Linha de Eixo e Hélice
 - 6.1.3 Sistemas de Propulsão em Emergência
 - 6.1.4 Sistemas de Óleo Combustível
 - 6.1.5 Sistemas de Óleo Lubrificante
 - 6.2 AUXILIARES
 - 6.2.1 Sistemas de Esgoto, Trim e Lastro

- 6.2.2 Sistemas de Água de Resfriamento
- 6.2.3 Sistemas Hidráulicos e Pneumáticos
- 6.2.4 Instalações de Vapor Auxiliar
- 6.2.5 Comunicações Interiores
- 6.3 INSTALAÇÕES ELÉTRICAS
 - 6.3.1 Sistema Elétrico de Serviço Principal
 - 6.3.2 Sistema Elétrico de Serviço de Emergência
 - 6.3.3 Fontes Transitórias de Potência
 - 6.3.4 Tomadas de Energia de Terra
 - 6.3.5 Cabeamento Elétrico e Isolamento de Componentes
 - 6.3.6 Penetração de Cabeamento em Barreiras Físicas
- 7. SEGURANÇA RADIOLÓGICA OPERACIONAL
 - 7.1 PROGRAMA DE PROTEÇÃO RADIOLÓGICA
 - 7.1.1 Política de Proteção Radiológica da Organização Operadora
 - 7.1.2 Organização, Pessoal e Responsabilidades
 - 7.1.3 Facilidades, Equipamentos e Instrumentação
 - 7.1.4 Procedimentos e Treinamento
 - 7.1.5 Programa de Monitoração de Efluentes
 - 7.1.6 Programas de Auditorias e Revisões
 - 7.2 FONTES DE RADIAÇÃO NA INSTALAÇÃO
 - 7.3 PROJETO DAS INSTALAÇÕES E EQUIPAMENTOS
 - 7.3.1 Zoneamento e Controle de Acesso
 - 7.3.2 Blindagem e Dispositivos de Proteção
 - 7.3.3 Ventilação para Proteção Radiológica
 - 7.3.4 Monitoração da Radiação
 - 7.4 SISTEMAS PARA GERENCIAMENTO DE REJEITOS
 - 7.4.1 Rejeitos Sólidos
 - 7.4.2 Rejeitos Líquidos
 - 7.4.3 Rejeitos Gasosos
 - 7.5 ANÁLISE DE DOSES EM OPERAÇÃO NORMAL

- 7.5.1 Doses para o Público em Geral
- 7.5.2 Doses Ocupacionais
- 7.5.3 Análise de Aceitabilidade da Instalação sob o Aspecto Radiológico
- 8. COMISSIONAMENTO
 - 8.1 PROGRAMA DE COMISSIONAMENTO
 - 8.1.1 Testes Pré-Operacionais a Frio
 - 8.1.2 Testes Pré-Operacionais a Quente
 - 8.1.3 Testes Operacionais a Baixa Potência
 - 8.1.4 Testes Operacionais de Elevação de Potência
 - 8.2 PROVAS DE CAIS
 - 8.3 PROVAS DE MAR
- 9. CONDUÇÃO DA OPERAÇÃO
 - 9.1 ESTRUTURA ORGANIZACIONAL
 - 9.2 QUALIFICAÇÃO E TREINAMENTO DE PESSOAL
 - 9.3 MÉTODOS PARA REVISÃO E AUDITORIA
 - 9.4 PROCEDIMENTOS E INSTRUÇÕES DE OPERAÇÃO
 - 9.5 MANUTENÇÃO, TESTES E INSPEÇÕES
 - 9.6 REGISTROS E RELATÓRIOS DE OPERAÇÃO
- 10. ANÁLISE DE SEGURANÇA
 - 10.1 ABORDAGEM E METODOLOGIA UTILIZADA NA ANÁLISE DE SEGURANÇA
 - 10.1.1 Métodos para Identificação e Seleção de Eventos Inicializadores
 - 10.1.2 Métodos de Análise
 - 10.1.2.1 Seqüência de Eventos
 - 10.1.2.2 Transientes
 - 10.1.2.3 Avaliação de Eventos Externos e Eventos Internos Especiais
 - 10.1.2.4 Análise Qualitativa
 - 10.1.2.5 Conseqüências Radiológicas
 - 10.1.3 Critérios de Aceitação
 - 10.2 PARÂMETROS E CONDIÇÕES INICIAIS
 - 10.2.1 Parâmetros do Núcleo

- 10.2.2 Funções Assumidas pelo Sistema de Proteção do Reator
- 10.3 SELEÇÃO DE EVENTOS INICIALIZADORES
- 10.4 AVALIAÇÃO INDIVIDUAL DAS SEQUÊNCIAS POSTULADAS
 - 10.4.1 Identificação de Causas
 - 10.4.2 Sequência de Eventos e Operação dos Sistemas
 - 10.4.3 Análise de Transientes
 - 10.4.3.1 Modelos Computacionais
 - 10.4.3.2 Parâmetros de Entrada e Condições Iniciais
 - 10.4.3.3 Resultados
 - 10.4.4 Classificação dos Estados Degradados
 - 10.4.5 Derivação de Termos-Fonte
 - 10.4.5.1 Análise de Liberações de Radionuclídeos para o Interior do Submarino
 - 10.4.5.2 Análise de Liberações de Radionuclídeos para o Ambiente
 - 10.4.5.3 Análise de Outros Riscos
 - 10.4.6 Avaliação de Consequências Radiológicas
 - 10.4.6.1 Métodos de Análise
 - 10.4.6.2 Doses Resultantes
 - 10.4.6.3 Campos de Radiação Diretos
 - 10.4.6.4 Liberações de Líquidos
 - 10.4.6.5 Liberações Atmosféricas
 - 10.4.6.6 Contaminação do Mar
- 10.5 SUMÁRIO E ANÁLISE DE RESULTADOS
- 11. LIMITES E CONDIÇÕES OPERACIONAIS
 - 11.1 LIMITES DE SEGURANÇA
 - 11.2 AJUSTES DOS SISTEMAS DE SEGURANÇA
 - 11.3 CONDIÇÕES LIMITANTES PARA OPERAÇÃO SEGURA
 - 11.4 REQUISITOS DE VIGILÂNCIA
 - 11.5 REQUISITOS ADMINISTRATIVOS
- 12. GARANTIA DA QUALIDADE
 - 12.1 PROGRAMAS DE GARANTIA DA QUALIDADE

- 12.2 PROCEDIMENTOS DE GARANTIA DA QUALIDADE
- 12.3 ESTÁGIO ATUAL DO GERENCIAMENTO DO PROGRAMA DE GARANTIA DA QUALIDADE
- 13. DESCOMISSIONAMENTO
 - 13.1 ESTRATÉGIA
 - 13.1.1 Gerenciamento de Rejeitos
 - 13.1.2 Gerenciamento de Doses Ocupacionais
 - 13.2 CARACTERIZAÇÃO DOS NÍVEIS DE DESCOMISSIONAMENTO
 - 13.2.1 Nível 1
 - 13.2.2 Nível 2
 - 13.2.3 Nível 3
 - 13.3 PLANEJAMENTO PRELIMINAR
- 14. PLANEJAMENTO E PREPARAÇÃO PARA EMERGÊNCIAS
 - 14.1 EVENTOS CONSIDERADOS
 - 14.2 PLANO DE EMERGÊNCIA INTERNO
 - 14.3 PLANO DE EMERGÊNCIA EXTERNO

ANEXO P

JUSTIFICAÇÃO DE DOSES COM RESPEITO A REQUISITOS DE SEGURANÇA NUCLEAR

Ao longo do ciclo de vida de um SNA, particularmente durante os períodos de manutenção e reparos, podem ocorrer situações onde a execução de determinadas intervenções na IPN em atendimento a requisitos de segurança nuclear é desejável, mas onde há incerteza sobre se as exposições à radiação, tanto em termos individuais como coletivos, que seriam inevitavelmente incorridas ao longo dos trabalhos seriam justificadas (dentro do Princípio da Justificação da Proteção Radiológica) em comparação com os eventuais benefícios em termos de segurança nuclear que deles resultariam.

Será então proposto um conjunto de critérios, com o objetivo de subsidiar os processos de tomada de decisão correlatos a estas situações de avaliação dos méritos relativos do benefício em termos de segurança nuclear e eficiência militar contra o detrimento radiológico em termos de exposição individual e coletiva do pessoal.

P.1 PARÂMETROS.

As atividades de inspeção, testes, manutenção e reparo sobre a IPN de um SNA não são executados somente para assegurar segurança nuclear, mas principalmente para assegurar sua disponibilidade e pleno desempenho. Para tais atividades, estes objetivos são normalmente coincidentes, sendo raras as situações que possam dar margem a conflitos, pois disponibilidade e seguridade estão intimamente relacionadas.

Os detrimentos decorrentes da execução de uma atividade de inspeção, testes, manutenção e reparo incluirão custos diretos e indiretos, tempos de indisponibilidade e doses individuais e coletivas de radiação.

Tanto durante a fase de planejamento destas atividades como durante sua efetiva execução, freqüentemente terão que ser tomadas decisões sobre se na verdade serão justificados certas tarefas propostas, i.e. se os benefícios reais ou percebidos em termos de disponibilidade e desempenho, ou de segurança nuclear, da IPN justificam os detrimentos associados. Para permitir tais tomadas de decisão em uma base objetiva e consistente, todos

os vários parâmetros devem ser quantificados nas mesmas unidades, ou pelo menos serem hierarquizados numa escala comum.

P.2 QUANTIFICAÇÃO DE PARÂMETROS

Teoricamente deveria ser possível quantificar todos os parâmetros associados aos benefícios e aos detrimientos em base unidades de medida comum, por exemplo uma base monetária. Quantificados estes parâmetros, seria necessário estabelecer um valor limite que definisse quanto o “decisor” estaria “disposto a pagar” para obter um benefício ou para evitar um detrimento.

Para o detrimento radiológico decorrente da dose coletiva, existem diversas propostas para tais análises do tipo custo / benefício (LOCHARD, 1990). A título de exemplo, o valor de £ 40.000 / homem-Sv é proposto por (NRPB, 1993) para a maioria dos casos de exposições ocupacionais. Tais valores limites definidos em termos de custos monetários por unidade de dose coletiva são usados como um guia para tomada de decisões objetivas em situações envolvendo trabalho na presença de radiação ionizante, particularmente quando o objetivo principal é evitar doses coletivas de radiação a níveis baixos individuais, e onde os outros fatores detrimenais são muito menos pertinentes.

A quantificação destes outros fatores é, porém, extremamente difícil, sendo ainda mais difícil chegar-se a um consenso geral o método a ser empregado. Poderiam ser desenvolvidos métodos de quantificação para o valor percebido da existência de um SNA, que seria pelo menos igual aos custos de construção mais os custos de manutenção periódica. Seria entretanto muito mais difícil estabelecer métodos de quantificação para os aspectos menos tangíveis, tais como a segurança nuclear adicional, ou a melhoria do desempenho.

Além disto, muitas destas atividades não são de fato executadas para melhorar diretamente o desempenho ou segurança de uma IPN particular, mas somente para aumentar o grau de confiança subjetiva que os operadores têm no funcionamento correto da Instalação, fator este evidentemente não quantificável. Certas atividades, especialmente inspeções e testes, também podem ser executadas não tanto por causa de um submarino em particular, mas por causa de um benefício percebido, a longo termo, para o conjunto da Força de SNA.

Para cada um destes casos poderia ser teoricamente determinado um método de quantificação, mas isto só poderia ser feito com base em hipóteses e avaliações de custo altamente especulativas, tornando tal método totalmente subjetivo. Na prática não seria possível produzir um método de quantificação consistente, objetivo e consensual.

P.3 COMPARAÇÃO QUALITATIVA DE PARÂMETROS

Considerando-se que não é possível estabelecer uma base quantitativa para comparação, deve-se então buscar como alternativa o estabelecimento de uma base qualitativa. Uma atividade poderá ser executada por ser considerada essencial, altamente desejável, desejável, ou benéfica (ou outros adjetivos equivalentes). Tais termos podem levantar uma série de questionamentos, tais como o grau pelo qual uma atividade é julgada essencial, o quanto seria o ganho com sua execução, o quanto seria perdido no caso de não executá-la. Tais termos, entretanto, são geralmente interpretados da mesma maneira pelo pessoal especialista de uma determinada área, e normalmente há consenso geral no grau de importância de uma atividade particular.

Para uma avaliação qualitativa do detrimento radiológico, direção oficial é esparsa que para a avaliação quantitativa. A ICRP recomenda que, para um trabalhador individual seria razoável adotar um risco anual de morte de cerca de 10^{-3} como limite de tolerabilidade das exposições à radiação. Considerando as estimativas atuais de risco radiológico, de 5×10^{-2} fatalidades por homem-Sv, a dose que corresponde a este limite é de 20 mSv. Pode-se então concluir que exposições individuais da ordem de 20mSv/ano ao longo de vários anos poderiam ser consideradas como toleráveis, enquanto exposições continuadas a doses superiores a este limite anual seriam inaceitáveis.

P.4 OBJETIVOS DETALHADOS

As atividades de inspeção, manutenção e reparo realizadas durante os períodos programados ao longo do ciclo de vida do SNA (vide Anexo B) atendem às seguintes motivações básicas, classificadas segundo a escala qualitativa proposta (Tabela P.1).

Estas indicações da importância dos objetivos declarados são necessariamente genéricas, sendo entretanto adaptadas a comparações com os riscos associados.

TABELA P.1: CLASSIFICAÇÃO DAS ATIVIDADES DE INSPEÇÃO,
MANUTENÇÃO E REPARO DE UM SNA

1. Assegurar diretamente a segurança nuclear	Essencial
2. Apoiar os interesses vitais de defesa nacional	Essencial
3. Assegurar a máxima disponibilidade	Altamente Desejável
4. Evitar ocorrência de eventos que possam comprometer a segurança nuclear	Altamente Desejável
5. Evitar ocorrência de eventos que possam comprometer a disponibilidade	Altamente Desejável
6. Melhorar confiança na segurança nuclear de uma classe de SNA, ou de todos os SNA existentes	Altamente Desejável
7. Melhorar diretamente ou restabelecer os padrões de desempenho	Desejável
8. Evitar ocorrência de eventos que possam comprometer o desempenho	Desejável
9. Melhorar confiança na disponibilidade de uma classe de SNA, ou de todos os SNA existentes	Desejável
10. Melhorar confiança no desempenho de uma classe de SNA, ou de todos os SNA existentes	Desejável
11. Melhorar confiança na segurança nuclear de um SNA em particular	Desejável
12. Melhorar confiança na disponibilidade de um SNA em particular	Benéfico
13. Melhorar confiança no desempenho de um SNA em particular	Benéfico

P.5 ANÁLISE QUALITATIVA DE DOSES INDIVIDUAIS

As atividades julgadas essenciais (itens 1 e 2 da Tabela P.1), sejam por razões de segurança nuclear ou de defesa nacional, devem ser realizadas independentemente da dose coletiva decorrente, contanto que os limites para doses individuais planejadas estabelecidos (50 mSv / ano para o corpo inteiro, conforme Capítulo 5) sejam respeitados e que estas sejam otimizadas, i.e. sejam tão baixas quanto razoavelmente praticável (ALARA).

As atividades julgadas como altamente desejáveis (itens 3 - 6 da Tabela P.1) devem ser realizadas respeitando-se os limites de dose individual para irradiação controlada (20 mSv / ano para o corpo inteiro, conforme Capítulo 5). Para tais atividades é aceitável que sejam irradiadas até dez pessoas. A dose individual média para o grupo deverá corresponder a metade da dose individual máxima, o que implicaria numa dose coletiva máxima aceitável de 100 homem-mSv.

As atividades julgadas como desejáveis (itens 7-11 da Tabela P.1) devem ser realizadas considerando-se um valor máximo de dose individual correspondente a metade do limite de dose individual para irradiação controlada (10 mSv / ano para o corpo inteiro). Para tais atividades seria também aceitável que fossem irradiados até dez pessoas, o que implicaria numa dose coletiva máxima aceitável de 50 homem-mSv.

As atividades julgadas como benéfica (itens 12 e 13 da Tabela P.1) devem ser realizadas considerando-se um valor máximo de dose individual correspondente a um quinto do limite de dose individual para irradiação controlada (4 mSv / ano para o corpo inteiro). Para tais atividades seria aceitável que fossem irradiados até cinco pessoas, o que implicaria numa dose coletiva máxima aceitável de 10 homem-mSv.

Deve-se enfatizar que, dado o amplo espectro de atividades e tarefas que são realizadas durante os períodos de manutenção de um SNA e o fato do grau de importância cada uma delas não poder ser definido objetivamente, regras rígidas não podem ser impostas. Entretanto, os valores acima apresentados podem representar uma orientação para auxílio a decisão, proporcionando uma certa consistência entre as abordagens de problemas semelhantes feitas pelos diferentes responsáveis envolvidos neste tipo de decisões.

P.6 IMPLEMENTAÇÃO

Da discussão apresentada acima, conclui-se que, para avaliar o balanceamento entre o grau de necessidade de execução de uma atividade de inspeção, testes, manutenção ou reparo em um SNA e as doses de radiação que serão incorridas, a autoridade responsável pela decisão de executá-la ou não poderia basear-se nas diretrizes apresentadas pela Tabela

P.2. Evidentemente, além do atendimento a estas diretrizes, todas as atividades devem ser planejadas e executadas de forma que as doses sejam ALARA.

TABELA P.2: DIRETRIZES PARA JUSTIFICAÇÃO DE DOSES

PROPÓSITO DE TAREFA	MAXIMA DOSE INDIVIDUAL	MÁXIMA DOSE COLETIVA
1. Assegurar diretamente a segurança nuclear	50 mSv	Nenhum limite (ALARA)
2. Apoiar os interesses vitais de defesa nacional	50 mSv	Nenhum limite (ALARA)
3. Assegurar a máxima disponibilidade	20 mSv	100 homem - mSv
4. Evitar ocorrência de eventos que possam comprometer a segurança nuclear	20 mSv	100 homem - mSv
5. Evitar ocorrência de eventos que possam comprometer a disponibilidade	20 mSv	100 homem - mSv
6. Melhorar confiança na segurança nuclear de uma classe de SNA, ou de todos os SNA existentes	20 mSv	100 homem - mSv
7. Melhorar diretamente ou restabelecer os padrões de desempenho	10 mSv	50 homem - mSv
8. Evitar ocorrência de eventos que possam comprometer o desempenho	10 mSv	50 homem - mSv
9. Melhorar confiança na disponibilidade de uma classe de SNA, ou de todos os SNA existentes	10 mSv	50 homem - mSv
10. Melhorar confiança no desempenho de uma classe de SNA, ou de todos os SNA existentes	10 mSv	50 homem - mSv
11. Melhorar confiança na segurança nuclear de um SNA em particular	10 mSv	50 homem - mSv
12. Melhorar confiança na disponibilidade de um SNA em particular	4mSv	10 homem - mSv
13. Melhorar confiança no desempenho de um SNA em particular	4mSv	10 homem - mSv

REFERÊNCIAS BIBLIOGRÁFICAS

- ADAMS, 1988; Adams, C. e Withey, W.R., **Escape and Rescue from Royal Navy Submarines**, Underwater Defense Technology Conference Proceedings UDT 88, Microwave Exhibitions and Publishers, Kent, Grã-Bretanha, 1988.
- AFCEN,1993; Association Française por les Règles de Conception et de Construction des Matériels des Chaudières Electro-Nucléaires (AFCEN), **Design and Construction for Mechanical Components of Nuclear Islands (RCC-M)**, Paris, França, 1993.
- ALDWINCKLE e POMEROY, 1982; Aldwinckle, D.S. e Pomeroy, R.V., **A Rational Assessment of Ship Reliability and Safety**, The Royal Institution of Naval Architects Proceedings, Londres, Grã-Bretanha, 1982.
- ALLA e DAVIS, 1989; Alla, H, e Davis, P., **Du Grafet aux Réseaux de Petri**, Hermès, Paris, 1989.
- ANCELIN, 1994; Ancelin, C. et ali, **Les Méthodes d'Analyse Prévisionnelle de la Fiabilité des Systèmes de Sûreté de Centrales Nucléaires**, in 4ème Colloque International de Fiabilité et Maintenabilité, Perros-Guirec, França, 21-25 maio de 1994.
- ANDERSON, 1976; Andersom, R.T., **Reliability Design Handbook**, Reliability Design Center NO RDH 376, Londres GB, 1976.
- ANSI,1988; American National Standards Institute, **Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactors Plants**, ANSI-N-18.2, Washigton, EUA, 1988
- ANSI/ANS, 1983; American Nuclear Society / American National Standard Institute, **Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactors Plants ANSI/ANS 51.1**, La Grange Park, EUA, 1983.
- ASQRAD, 1998; Centre d'Étude sur l'Évaluation de la Protection dans le Domaine Nucléaire, **Assessment System for the Quantification of Radiation Detriment: ASQRAD Code**, Rapport CEPN, Fontanay-aux-Roses, França, 1998.

- ATMA, 1994; Willm, I., **Sécurité et Fiabilité dans les Domaines Maritime et Aéronautique**, Association Technique Maritime et Aéronautique ATMA, Paris, França, 1994.
- ATWOOD, 1984; Atwood, C.L., **User's Guide to Binomial Failure Rate**, NUREG-CR-2729, U.S.Nuclear Regulatory Commission, Washington, EUA, 1984.
- BATTLE e KILLINGLEY, 1977; Battle, N. e Killingley, R.V., **The Influence of Safety and Licensing Requirements on the Selection of a Reactor Plant for an Icebreaker**, Compte-rendu du Symposium sur la Sûreté de Navires Nucléaires (5-9 déc. 1977), Hamburgo, Alemanha, 1977.
- BENTLEY, 1975; Bentley, J., **The Tresher Disaster: The Most Tragic Dive in Submarine History**, Doubleday & Company, Garden City, EUA, 1975.
- BERTIN, 1991; Bertin, M., **Les Effets Biologiques des Rayonnements Ionisants**, Électricité de France – SODEL, Paris, França, 1991.
- BNL, 1978; Brynda, W.J. et alli, **Design Guide for Category II Reactors: Light and Heavy Water Cooled Reactors, BNL 50831-II UC-80 (General Reactor Technology – TID-4500)**, Brookhaven National Laboratory, Upton, EUA, 1978.
- BREEMER, 1989; Breemer, J., **Soviet Submarines: Design, Development and Tactics**, Jene's Information Group, Surrey, Grã-Bretanha, 1989.
- BROWN e CHALMERS, 1989; Brown, D.K e Chalmers, D.W., **The Management of Safety of Warships in the UK**, Transactions of The Royal Institute of Naval Architects, Londres, Grã-Bretanha, 1989.
- BURCHER e RYDILL, 1994; Burcher, R. e Rydill, I., **Concepts in Submarine Design**, Cambridge University Press, Grã-Bretanha, 1994.
- CEA, 1998; Commissariat à l'Énergie Atomique, **Les Centrales Nucléaires dans le Monde**, Elecnucl Data Base Informations, Paris, França, 1998

- CEI, 1985; Commission Eletrotechnique International, **Techniques d'Analyse de la Fiabilité des Systèmes: Procédures d'Analyse des Modes de Défaillance et de leurs Effects (AMDE)**, Publication n0 812, Paris, França, 1985.
- CLANCY, 1993; Clancy, T., **Submarine**, Berkley Books, New York, EUA, 1993.
- CNEN, 1984; Comissão Nacional de Energia Nuclear, Norma Experimental 1.04 - **Licenciamento de Instalações Nucleares**, CNEN, Rio de Janeiro, 1984.
- COSTA, 1985; Costa, Luiz S.S., **O Emprego de Submarinos numa Concepção Estratégica para a Marinha do Brasil**, Revista Marítima Brasileira jul/set 1985, Serviço de Documentação da Marinha, Rio de Janeiro, 1985.
- COSTA, 1997; Costa, Luiz S.S., **A Importância dos Submarinos na Complexa Nova Ordem Mundial**, Revista do Clube Naval - Edição Especial de Março, Rio de Janeiro, 1997.
- CROUCH, 1960; Crouch, H.F., **Nuclear Ship Propulsion**, Cornell Maritime Press, Cambridge, EUA, 1960.
- CULLMAN, 1975; Cullmann, G., **Initiation aux Chaînes de Markov: Méthodes et Applications**, Masson, Paris, França, 1975.
- DE LADONCHAMPS e VERDEAU, 1972; De Ladonchamps, J. e Verdeau, J., **Réacteurs Nucléaires à eau pressurisée - theorie, technologie et applications à propulsion navale**, Masson et cie. éditeurs, Paris, França, 1972.
- DEBAENE, 1994; Debaene, J., **Traité de Mecanique et Chaleur: chapitre B3140 - Réacteurs à Eau Ordinaire de Propulsion Navale**, Les Techniques de l'Ingénieur, Paris, França, 1994.
- DESROCHES, 1986; Desroches, A., **Proposition d'une Méthodologie Préliminaire d'Allocation de Sécurité Relative aux Différents Configurations d'un Système**, in 4ème Séminaire Européen sur la Sécurité des Systèmes, Deauville, França, 1986

- DESROCHES, 1992; Desroches, A., **Introduction aux Méthodes Resistance-Contrainte**, apostila do Cours de Mastère de Sûreté, École Centrale, Paris, França, 1992.
- DEVIRON, 1983; Devron, G., **Les Réacteurs à l'Eau Ordinaire**, Eyrolles, Paris, França, 1983.
- DGMM, 1994; Diretoria-Geral do Material da Marinha, Normas para o Processo de Obtenção de Meios Navais, Minsitério da Marinha, Rio de Janeiro, 1994.
- DHILLON e SINGH, 1981; Dhillon, B.S. e Singh, C., **Engineering Reliability**, John Wiley and Sons, New York, EUA, 1981.
- DOD, 1969; Department of Defence, **System Safety Program for Systems and Associated Subsystems and Equipments: Requirements For**, Military Standard MIL-STD-882, Washington, EUA, 1969.
- DON, 1975; Department of Navy, **Procedures for Performing a Failure Modes and Effects Analysis**, MIL-STD-1629A, Washington, EUA, 1975.
- DREICER, 1995; Dreicer, M., **External Costs in Nuclear Power Production**, Report 132/95, Centre d'Études sur la Protection dans le Domaine Nucléaire, Fontenay-aux-Roses, França, 1995.
- DSIN, 1998; Nuclear Installations Safety Directorate, **Activity Report - 1997**, Direction de la Sûreté des Installations Nucléaires, Paris, França, 1998.
- DUNCAN, 1990; Duncan, F., **Rickover and the Nuclear Navy**, Naval Institute Press, Annapolis, EUA, 1990.
- FARMER, 1967; Farmer, F.R., **Reactor Safety and Siting: a Proposed Risk Criterion**, in Nuclear Safety no. 8 (6), Londres, Grã-Bretanha, 1967.
- FAULKNER e DAS, 1990; Faulkner, D. e Das, P.K., **A New Risk Analysis Approach for Structural Design and Adequately Safe Operations of Submarines**, Underwater Defense Technology Conference Proceedings UDT 90, Microwave Exhibitions and Publishers, Kent, Grã-Bretanha, 1990.

- FLEMING, 1983; Fleming, K.N. et ali, **On the Analysis of Dependent Failures in Risk Assessment and Reliability Evaluation**, in Nuclear Safety vol 24 n0 5, Setembro-Outubro, 1983.
- FLEMING, 1985; Fleming, K.N. et ali, **A Systematic Procedure for the Incorporation of Common Cause Events into Risk and Reliability Models**, in Nuclear Engineering and Design, International Post-Conference Seminar SMIRT 8, Bruxelas, Bélgica, 1985.
- FLORES, 1988; Flores, M.C., **Submarino de Propulsão Nuclear: o que o justifica? como chegar até ele? o que quer a Marinha com ele? e para quê?**, Revista Marítima Brasileira, Serviço Geral de Documentação da Marinha, Rio de Janeiro, maio de 1988.
- FOOS, 1993; Foos, J., **Manuel de Radioactivité**, Formascience, Orsay, França, 1993.
- GABLER, 1986; Gabler, U., **Submarine Design**, Bernard & Graefe Verlag, Kiel, Alemanha, 1985.
- GERALD, 1994; Gerald, J., **Survivabilité des Navires de Combat**, Association Technique Maritime et Aéronautique ATMA, Paris, França, 1994.
- GKSS, 1975; GKSS, **Nuclear Research Ship OTTO HAHN Safety Assessment**, Gesellschaft für Kernenergieverwertung in Schiffbau und Schifffahrt mbH, Hamburgo, 1974.
- GLASSTONE e SESSONSKE, 1994; Glasstone, S. e Sessonske, A., **Nuclear Reactor Engineering**, Chapman & Hall, Nova Iorque, EUA, 1994.
- GUIMARÃES, 1991; Guimarães, L.S., **Modernas Tendências no Projeto de Submarinos**, dissertação de mestrado, Escola Politécnica da Universidade de São Paulo EPUSP, São Paulo, Brasil, 1991.
- GUIMARÃES, 1993; Guimarães, L., **Conception des Réacteurs de Propulsion Navale**, projet de fin d'études, cours d'ingénieur atomique 1992-93, Institut National des Sciences et Techniques Nucléaires INSTN, Saclay, França, 1993.

- GUIMARÃES, 1996a; Guimarães, L., **Protótipos em Terra de Instalações Propulsoras Nucleares**, in Anais do VI Congresso Geral de Energia Nuclear, Rio de Janeiro, 1996.
- GUIMARÃES, 1996b; Guimarães, L., **Introdução às Instalações Propulsoras Nucleares Navais**, in Anais do VI Congresso Geral de Energia Nuclear, Rio de Janeiro, 1996.
- GUIMARÃES, 1997a; Guimarães, L., **Otimização do Conjugado Disponibilidade x Segurança para Instalações Propulsoras Nucleares de Navios Militares**, in Anais do XI Encontro Nacional de Física de Reatores, Poços de Caldas, 1997.
- GUIMARÃES, 1997b; Guimarães, L., **Impacto Ambiental de um Submarino Nuclear Naufragado**, in Anais do III Simpósio sobre Ondas e Marés e II Seminário de Engenharia Oceânica, Instituto de Estudos do Mar Almirante Paulo Moreira, Arraial do Cabo, 1997.
- GUIMARÃES, 1998; Guimarães, L., **Logística de Produção de Combustível para um Esquadrão de Submarinos Nucleares de Ataque**, in Anais do III Simpósio de Logística da Marinha, Rio de Janeiro, 1998.
- HANDLER, 1989; Handler, J. e Arkin, W., **Neptune Papers**, Greenpeace, Washington, EUA, 1990.
- HANNAMAN, 1984; Hannaman, S., **Systematic Human Action Reliability Procedure (SHARP)**, Electric Power Research Institute, EPRI NP-3583, Boston, EUA, 1984.
- HANSEN, 1982; Hansen, Lars P. e Kenneth J. Singleton, **Generalized Instrumental Variables Estimation of Nonlinear Expectation Models**, Econometrica 50 set. 1982
- HARRINGTON, 1970; Harrington, R.L. et al., **Reliability and Maintainability Analyses of Shipboard Systems**, in Marine Technology, jan. 70, Society of Naval Architects and Marine Engineers SNAME, New York, EUA, 1970.
- HARRIS, 1997; Harris, B., **The Navy Times Book of Submarines: a Political, Social and Military History**, The Berkley Publishing Group, New York, EUA, 1997.

- HAUGEN, 1968; Haugen,E.B., **Probabilistic Approaches to Design**, Wiley and Sons, New York, EUA, 1968;
- HELLER, 1972; Heller, S.R., **The Case Against Pump for Control of Flooding of a Submarine**, Naval Engineers Journal (feb.72), Londres, Grã-Bretanha, 1972
- HENLEY e KUMAMOTO, 1981; Henley, E.J. e Kumamoto, H., **Reliability Engineering and Risk Assessment**, Prentice-Hall, Englewood Cliffs, EUA, 1981.
- HEWLETT e DUNCAN, 1974; Hewlett, R.G. e Duncan, F., **Nuclear Navy: 1946-1962**, University of Chicago Press, Chicago, EUA, 1974.
- HOLANDA, 1983; Holanda, A.B., **Novo Dicionário da Língua Portuguesa**, Editora Nova Fronteira, Rio de Janeiro, 1983.
- HSE, 1988; Health and Safety Executive, **The Tolerability of Risks from Nuclear Power Stations**, HMSO, Londres, Grã-Bretanha, 1988.
- HSE, 1989a; Health and Safety Executive, **Risk Criteria for Land-use Planning in the Vicinity of Major Industrial Hazards**, HMSO, Londres, Grã-Bretanha, 1989.
- HSE, 1989b; Health and Safety Executive, **Quantified Risk Assessment: Its Input to Decision-Making**, HMSO, Londres, Grã-Bretanha, 1989.
- HSE, 1992; Health and Safety Executive, **Safety Assessment Principles for Nuclear Plants**, HMSO, Londres, Grã-Bretanha, 1992.
- IAEA, 1978; International Atomic Energy Agency, **Design for Safety of Nuclear Power Plants**, Safety Series n°50-C-D, Viena, Áustria, 1978.
- IAEA, 1979; International Atomic Energy Agency, **Operational Limits and Conditions for Nuclear Power Plants**, Safety Series n°50-SG-O3, Viena, Áustria, 1979.
- IAEA, 1986; International Atomic Energy Agency, **General Design Safety Principles for Nuclear Power Plants**, Safety Series n°50-SG-D11, Viena, Áustria, 1986.

IAEA, 1989; International Atomic Energy Agency, **Governmental Organization for the Regulation of Nuclear Power Plants**, Safety Series n°50-C-G, Viena, Áustria, 1989.

IAEA, 1990; International Atomic Energy Agency, **Regulatory Process for the Decomissioning of Nuclear Facilities**, Safety Series n°105, Viena, Áustria, 1990.

IAEA, 1993; International Atomic Energy Agency, **The Safety of Nuclear Installations**, Safety Series no. 110, Viena, Áustria, 1993.

IAEA, 1994; International Atomic Energy Agency, **Safety Assessment of Research Reactors and Preparation of the Safety Analysis Report**, Safety Series No. 35-G1, Viena, Áustria, 1994.

IAEA, 1996; International Atomic Energy Agency, **Fire Protection in Nuclear Power Plants** (rev.1), Safety Series n°50-SG-D2, Viena, Áustria, 1996.

IAEA, 1998; International Atomic Energy Agency, **Nuclear Research Reactors in the World**, Reference Data Series n°3, Viena, Áustria, 1998.

IAEA-INSAG, 1988; International Atomic Energy Agency, **Basic Safety Principles**, Safety Series n°75 INSAG-3, Viena, Áustria, 1988

IAEA-INSAG, 1991; International Atomic Energy Agency - International Nuclear Safety Advisory Group, **Safety Culture**, Safety Series n°75 INSAG-4, Viena, Áustria, 1991.

IAEA-INSAG, 1992; International Atomic Energy Agency, **The Safety of Nuclear Power**, Safety Series n°75 INSAG 5, Viena, Áustria, 1992.

IAEA-INSAG, 1997; International Atomic Energy Agency - International Nuclear Safety Advisory Group, **Defence-in-Depth Principle in Nuclear Safety**, Safety Series n°75 INSAG-10, Viena, Áustria, 1997.

ICRP, 1983; International Commission of Radiation Protection, **Cost-Benefit Analysis in the Optimization of Radiation Protection**, ICRP Publication no. 10, Pergamon Press, Oxford, GB, 1983.

- ICRP, 1991; International Commission of Radiation Protection, **Recommandations**, ICRP Publication no. 60, Pergamon Press, Oxford, GB, 1991.
- IEEE, 1975; Institute of Electrical and Electronic Engineers, **Guide for General Principles of reliability Analysis of Nuclear Power Generating Stations Protection Systems**, IEEE Std 352-1975 (ANSI N41-4-1976), EUA, 1975.
- IPSN, 1994; Institut de Protection et Sureté Nucléaire, **Rapport du Groupe de l'Observatoire sur les Risques et la Sécurité**, Fontenay aux Roses, França, 1992.
- JACKSON, 1992; Jackson, H.A., **Fundamentals of Submarine Concept Design**, Transactions of the Society of Naval Architects and Marine Engineers SNAME vol. 100, New York, EUA, 1992.
- JAEGUER, 1975; Jaeger, R.G., **Engineering Compendium on Radiation Shielding**, Springer-Verlag, Berlin, Alemanha, 1975.
- JONES LEE, 1989; Jones Lee, M.W., **The Economics of Safety and Physical Risk**, Beckwell, Oxford, GB, 1989.
- LANING, 1992; Laning, R.B., **The Seawolf's Sodium-Cooled Power Plant**, Naval History, U.S.Naval Institute, EUA, 1992.
- LANNING e IPPOLITO, 1989; Lanning, D.D. e Ippolito, T., **Some Technical Aspects of the Use of Low-Enriched vs. High-Enriched Uranium Fuel in Submarine Reactors**, comunicação apresentada in Conference on the Implications of Acquisition of Nuclear Powered Submarines (SSN) by Non-Nuclear Weapons States, Massachusetts Institute of Technology, Cambridge, EUA, 1989.
- LECOQ, 1989; Le Coq, **Les Allocations de Sûreté**, apostila do curso de Mastère de Sûreté da École Centrale, Paris França, 1989.
- LEFAURE, 1994; Lefaure, C., Lochard, J., Schneider, T. e Schieber, C., **Proposition pour un Système de Valeurs Monétaires de Référence de l'Homme-Sievert**, Centre d'Études pour l'Évaluation de la Protection dans le Domaine Nucléaire, Rapport CEPN-R-193, Fevereiro 1993.

- LEROY, 1992; Leroy, A., **Les Réseaux de Petri**, apostila do Cours de Mastère de Sûreté, École Centrale, Paris, França, 1992.
- LEWIS, 1977; Lewis, E.E., **Nuclear Power Safety**, John Wiley & Sons, New York, EUA, 1977.
- LIBMAN, 1996; Libmann, J., **Elements of Nuclear Safety**, IPSN / Les Éditions de Physique, Les Ulis, França, 1996.
- LIEVENS, 1976; Lievens, C., **Sécurité des Systèmes**, CEPADUES, Paris, França, 1976
- LIGERON, 1979; Ligeron, J.C., **La Fiabilité en Mécanique**, Desforges, Paris, França, 1979.
- LILLINGTON, 1995; Lillington, J.N., **Light Water Reactor Safety**, Elsevier Science, Amsterdam, Holanda, 1995.
- LOCHARD, 1990; Lochard, J. et ali, **ALARA: from Theory towards Practics**, Commission of European Communities, EUR-13795-EN, Luxemburgo, 1991.
- LMIS, 1994; Lloyd's Register of Shipping, **Casualties Database**, Lloyd's Information Services, Londres, Grã-Bretanha, 1993.
- MARPOL, 1978; International Maritime Organization IMO, **International Convention for the Prevention of Pollution from Ships**, IMO, Londres, Grã-Bretanha, 1978.
- MCLEOD e RIVERA, 1996; McLeod, J.E. e Rivera, S.S., **Métricas para una Programción Confiable**, in Anais do VI Congresso Geral de Energia Nuclear, Rio de Janeiro, Brasil, outubro de 1996.
- MESLIN e BOURGADE, 1987; Meslin, T. e Bourgade, E., **Common Cause Failure Analysis and Quantification on the Basis of Operating Experience**, International Topical Conference on Probabilistic Safety Assessment and Risk Management, Zurich, Suíça, 1987.
- MNF, 1992; Marine Nationale, **La Propulsion Nucléaire Navale**, Supplement de la Revue Cols Bleu Déc./90, Marinha Francesa, Paris, França, 1990.

MNF, 1995; Marine Nationale, **Le Triomphant**, Éditions du Perron, Cherbourg, França, 1995.

NATACCI, 1997; Natacci, B.F., **Análise de Modos de Falha e Efeitos do Sistema de Linha de Eixo de um Submarino**, in Anais do II Simpósio de Logística da Marinha, Rio de Janeiro, 1997.

NETHERLANDS, 1989; Ministry of the Environment of the Netherlands, **Premises for Risk Management**, Governo Holandês, Haia, Holanda, 1989.

NIMAL, 1991; Nimal, J-C., **Les Simulations de Monte-Carlo**, apostila do Cours de Mastère de Sûreté, École Centrale, Paris, França, 1991.

NRC, 1975; Rassmussen, C. et ali, **Reactor Safety Estudy: an Assessment of Accident Risks in US Commercial Nuclear Power Plants**, WASH-1400 (NUREG 74/014), U.S. Nuclear Regulatory Commission, Washigton, EUA, 1975.

NRC, 1978; U.S. Nuclear Regulatory Commission, **Standard Format and Content of Safety Analysis Report for Nuclear Power Plants (RG 1.70)**, Washington, EUA, 1978.

NRC, 1981; Vesely, W.E. et alli, **Fault Tree Handbook** (NUREG 0492), U.S. Nuclear Regulatory Commission, Washington, USA, 1981

NRC, 1983a; U.S. Nuclear Regulatory Commission, **A Guide to the Performance of Probabilistic Risk Assessments for nuclear Power Plants**, NUREG/CR 2300, Washington, EUA, 1983.

NRC, 1983b; Swain, A.D. e Guttmann, H.E., **Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Application**, NUREG/CR-1278, U.S.Nuclear Regulatory Commission, Washington, EUA, 1983.

NRC, 1989; U.S. Nuclear Regulatory Commission, **Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants**, Washington, EUA, 1989

- NRC, 1996; U.S. Nuclear Regulatory Commission, **Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors (NUREG – 1537)**, Washington, EUA, 1996
- NRPB, 1993; National Radiological Protection Board, **Occupational, Public and Medical Exposure**, NRPB, Chilton, Grã-Bretanha, 1993.
- OKRENT, 1991; Okrent, D., **Nuclear Reactor Safety: On the History of the Regulatory Process**, The University of Wisconsin Press, Madison, EUA, 1981.
- PAGÈS, 1981; Pagès, A. E Gondran, M., **Fiabilité des Systèmes**, Eyrolles, Paris, França, 1981.
- PAIVA, 1988; Paiva, P.G., **Comunicações com Submarinos - Tecnologia Atual**, Revista Marítima Brasileira vol 108 no. 10/12, Serviço de Documentação da Marinha, Rio de Janeiro, 1988.
- PAPOULIS, 1965; Papoulis, A., **Probability, Random Variables and Stochastic Processes**, McGraw-Hill Book Company, New York, USA, 1965.
- PEREIRA, 1997; Pereira, M.C.R., **Política de Defesa Nacional: A Marinha do Brasil**, Serviço de Relações Públicas da Marinha, Brasília, 1997.
- PERROTA, 1990; Perrota, José A., **Engenharia do Núcleo de Reatores**, apostila de curso, Instituto de Pesquisas Energéticas e Nucleares IPEN, São Paulo, 1990
- PERSHAGEN, 1989; Pershagen, B., **Light Water Reactor Safety**, Pergamon Press, Nova Iorque, EUA, 1989.
- PINIELLA, 1996; Piniella, F. et alli, **Fundamentos de Seguridad Marítima**, Universidad de Cádiz - Servicio de Publicaciones, Cádiz, Espanha, 1996.
- POLLACK, 1971; Pollack, S.L., **Decision Tables: Theory and Practice**, Wiley Interscience Publishers, New York, EUA, 1971.
- POLMAR, 1982; Polmar, D.J. e Allen, T.B., **Rickover, Controversy and Genius – a Biography**, Simon and Schuster, Nova Iorque, EUA, 1982.

- RELCON, 1994; Relcon, **Risk Spectrum Manual**, Relcon Teknik AB, Solnas, Suécia, 1994.
- RF, 1995; Republique Française, **Sûreté des Installations Nucléaires - Législation et Réglementation**, Journal Officiel de la République Française, Paris, França, 1995.
- ROCKWELL, 1992; Rockwell, T., **The Rickover Effect: How One man Made a Difference**, Naval Institute Press, Annapolis, EUA, 1992.
- RODDIS e SIMPSON, 1958; Roddis, L.H. e Simpson, J.W, **The Nuclear Propulsion Plant of the USS Nautilus**, SNAME Transactions, vol.62, Nova Iorque, EUA, 1958.
- ROSA DA SILVA, 1989; Rosa da Silva, J.E., **Comparação do Desempenho do Dióxido de Urânio Sinterizado sob a Forma Plana e Cilíndrica para Reatores a Água Pressurizada**, dissertação de mestrado, Instituto de Pesquisas Energéticas e Nucleares IPEN, São Paulo, 1989.
- SAE, 1967; Society of Aerospace Engineers, **Design Analysis Procedure for failure Mode, Effects and Criticality Analysis FMECA**, Recommended Practice ARP 926, EUA, 1967.
- SCHAFSTALL, 1977; Schafstall, H.G. et alli, **Safety Aspects for Fuel Element Handling on Board of Nuclear Ships**, in Compte-rendu du OECD/AIEA Symposium sur la sûreté des navires nucléaires, Hamburgo, Alemanha, 5-9 dez. 1977.
- SCHNEIDER, 1995; Schneider, T., Schieber, C. e Eeckoudt, **Valeurs Monétaires de l'Homme-Sievert et Prise en Compte du Temps**, Centre d'Études pour l'Évaluation de la Protection dans le Domaine Nucléaire, Rapport CEPN-R-214, Março 1993.
- SCIENTECH, 1994; Scientech, **REVEAL_W Manual**, Scientech Inc., Rockville, EUA, 1994
- SEVESTRE, 1991; Sevestre, B., **L'Entretien des Sous-marins Nucléaires de Attaque**, Compte-rendu de la Conference "Evolution de la Fabrication et de la Maintenance des Équipements des Tranches Nucléaires", Societé Française de l'Énergie Nucléaire, Paris, 1991.

- SHARPE, 1997; Sharpe, R., **Jane's Fighting Ships**, Jane's Information Group, Surrey, Grã-Bretanha, 1997.
- SHRADER-FRECHETTE, 1985; Shrader-Frechette, K.S., **Science Policy, Ethics and Economic Methodology**, Reidel Publishing Co., Dordrecht, Alemanha, 1985.
- SIMPSON, 1995; Simpson, J.W., **Nuclear Power From Undersea to Outer Space**, American Nuclear Society, La Grange Park, EUA, 1995
- SLOVIC, 1980; Slovic, P. et al., **The Assessment and Perception of Risk**, The Royal Society of London 34-17, Londres GB, 1980.
- SMETS, 1992; Smets, H., **Limites Supérieures des Risques Créés par les Installations Dangereuses**, Révue Préventive no. 43 (jan-fev/92), Paris, França, 1992.
- SNAME, 1994; Society of Naval Architects and Marine Engineers, **1994 Environmental Symposium Plenary Section Addresses**, SNAME, New York, EUA, 1994.
- SOLAS, 1992; International Maritime Organization IMO, **International Convention for the Safety of life at Sea**, IMO, Londres, Grã-Bretanha, 1992.
- SRPM, 1990; Serviço de Relações Públicas da Marinha - Marinha do Brasil, **O Preparo da Marinha nos Anos 90**, Serviço de Relações Públicas da Marinha, Brasília, 1990.
- SRPM, 1996; Serviço de Relações Públicas da Marinha - Marinha do Brasil, **A Arma Submarina**, Serviço de Relações Públicas da Marinha, Brasília, 1996.
- SRPM, 1997; Serviço de Relações Públicas da Marinha - Marinha do Brasil, **Poder Naval**, Action Editora, Rio de Janeiro, 1997.
- STANSFELD, 1994; Stansfeld, J.T. et al., **A Study of Casualty Data for Ships Carrying Hazardous and Noxious Substances**, Lloyd's Register of Shipping, Londres, Grã-Bretanha, 1994.
- STARR, 1973; Starr, C., **Social Benefit versus Technological Risk: What is our Society Willing to Pay for Safety?**, in Science 165-1232, Boston, USA, 1973.

- STXN, 1994; Service Technique Mixte des Chaufferies Nucléaires de Propulsion Navale, **Organisation de la Propulsion Navale**, Délégation Generale pour l'Armement, Paris, 1994.
- UFSG, 1977; U.S. Federal Government, **United States Code of Federal Regulations, Title 10, Part 50, Annex A**, Washigton, EUA, 1977
- VAN DER VAT, 1994; Van der Vat, D., **Stealth at Sea: The History of the Submarine**, Weidenfeld & Nicolson, Londres, Grã-Bretanha, 1994.
- VERDEAU e BAUJAC, 1977; Verdeau, J.J e Baujat, J., **Présentation des Chaufferies Nucléaires de Propulsion Navale CAS: Options Spécifiques de Sûreté**, Comptendu du Symposium sur la Sûreté de Navires Nucléaires (5-9 déc. 1977), Hamburgo, Alemanha, 1977.
- VILLEMEUR, 1988; Villemeur, A., **Sûreté de Fonctionnement des Systèmes Industriels - Fiabilité, Facteurs Humains et Informatisation**, Éditions Eyrolles, Paris, França, 1988.
- VILLEMEUR, 1992; Villemeur, A., **Reliability, Availability, Maintainability and Safety**, Mcgraw-Hill, New York, EUA, 1992.
- ZHAREN e DUNCAN, 1994; Von Zharen, W.M. e Duncan, W., **Environmental Risk Assessment and Management in the Maritime Industry**, Transactions of the Society of Naval Architects and Marine Engineers SNAME vol. 102, New York, EUA, 1994.

BIBLIOGRAFIA COMPLEMENTAR

SEGURANÇA DE SISTEMAS INDUSTRIAIS

Ablitt, F., **An Introduction to the SYREL Reliability Data Bank**, Report No SRS/GR/14, Systems Reliability Service, United Kingdom Atomic Energy Agency UKAEA, Culcheth, GB, 1984.

Amesz, J. et alli, **The European Reliability Data System (ERDS): Main Developments and Use**, ANS/ENS International Topical Meeting on Probabilistic Safety Methods and Applications, San Francisco, EUA, 1985.

Association Française des Normes Techniques (AFNOR), **Gestion de la Qualité** (NF50-109), Paris, França, 1986

Association Française des Normes Techniques (AFNOR), **Statistique et Qualité** (NF06-501), Paris, França, 1987

Batteau, P. e Marciano, J-P., **Probabilité et Décision dans l'Incertain**, Presses Universitaires Françaises, Paris, França, 1976.

Beam, W.R., **Systems Engineering: Architecture and Design**, McGraw-Hill Book Co., New York, EUA, 1990.

Bernier, J. E Veron, R., **Sur Quelques Difficultés Rencontrés dans l'Estimation d'un Débit de Crue de Probabilité Donnée**, Electricité de France EdF-DER, 1963.

Blanchard, J. e Fabrycky, W.J., **Systems Engineering and Analysis**, Prentice Hall, New York, EUA, 1990.

Boll, M., **Les Certitudes du Hasard**, Presses Universitaires Françaises, Paris, França, 1958

Borel, E., **Probabilités et Certitude**, Presses Universitaires Françaises (PUF), Paris, 1963.

Brunet-Moret, Y., **Statistiques des Rangs**, Cahier de l'ORSTOM, Paris, França, 1973.

Bureau de Normalization de l'Aéronautique et de l'Espace, **Guide d'Élaboration des Objectifs de Sécurité d'un Système Missile ou Spatial**, RG-AERO 701-12, Paris, França, 1987.

- Comission Electrotechnique Internationale, **Liste des Termes de Base, Définitions et Mathématiques Applicables à la Fiabilité**, publication 271C, Paris, 1985.
- Costa Neto, P.L., **Estatística**, Editora Edgard Blücher, São, Brasil, 1977.
- Courtot, H., **La Gestion des Risques dans les Projets**, Economica, Paris, 1998.
- De Finnetti, B., **Probability, Induction and Statistics**, John Wiley and Sons, New York, EUA, 1972.
- Denis, H., **Comprendre et Gérer les Risques Sociotechnologiques Majeurs**, Éditions de l'École Polytechnique de Montréal, Montréal, Canadá, 1998.
- Desroches, A., **Concepts et Méthodes Probabilistes de Base de la Sécurité**, Lavoisier TEC-DOC, Paris, França, 1995.
- Dumas de Rauly, D., **L'Estimation Statistique**, Éditions Gauthier-Villars, Paris, França, 1968.
- Engelhardt, B., **Simple Approximate Distributional Results for Confidence and Tolerance Limits for the Weibull Distribution Based on Maximum Likelihood Estimation**, Technometrics vol.23, New York, EUA, 1981.
- Engelund, S. E Rackwitz, R., **On Predictive Distribution Functions for the Three Asymptotic Extreme Values Distributions**, Elsevier Sciences Publishers, New York, EUA, 1992.
- Favez, B., **Les Études de Fiabilité: Utopie ou Réalité Industrielle?**, International RAM Conference, Toronto, Canadá, 1993.
- Feller, W., **An Introduction to Probability Theory and its Application**, Wiley and Sons, New York, 1988.
- Gnedenko, B.V., **Sur la Distribution Limite du Terme Maximum d'une Série Aléatoire**, Annales Mathématiques, Paris, França, 1943.
- Gumbel, E.J., **Méthodes Graphiques pour l'Analyse des Débits des Crues**, Société Hydrotechnique Française, Paris, 1956.

- Gumbel, E.J., **Statistics of Extremes**, Columbia University Press, Washington, EUA, 1958.
- Hammer, W., **Handbook of System and Product Safety**, Prentice Hall Inc., Englewood Cliffs, EUA, 1972.
- Hasofer, A.M. e Wang, Z., **System Reliability Calculations Using Extreme Value Theory**, University of South Wales, Austrália, 1985.
- Institute of Electrical and Electronic Engineers, **Guide to the Collection and presentation of Electrical, Electronic, Sensing Components and Mechanical Equipment Reliability Data for Nuclear Power Generating Stations**, IEEE Std 500, John Wiley and Sons, New York, EUA, 1984.
- Institut de Protection et Sûreté Nucléaire, **Perception des Risques et de la Sécurité: Résultats du Sondage de Novembre 1997**, Rapport IPSN, Fontenay-aux-Roses, França, 1998.
- Juram, J.M., **Gestion de la Qualité**, AFNOR, Collection Normes et techniques, Paris, França 1983
- Kaufmann, W., **Introduction à la Théorie des Sous-ensembles Flous à l'Usage des Ingénieurs**, Masson Éditeurs, Paris, França, 1977.
- Kervern, J.Y. e Rubise, P., **L'Archipel des Dangers**, Economica, Paris, França, 1991
- Keynes, J. M., **Treatise on Probability**, Macmillan Books, Londres, Grã-Bretanha, 1921.
- Linstone, H., e Turoff, H., **The Delphi Method**, Addison-Wesley Publishers, Chicago, EUA, 1975.
- Llory, M., Villemeur, A. e Portal, R., **Les Défaillances de Mode Commun: Identification et Prévention**, EDF-DER-HT/13/28/79, Electricité de France, Clamart, França, 1979.
- Lowrance, W.W., **Of Acceptable Risk**, Kaufmann, Los Altos, EUA, 1976
- Mayo, D.G. e Hollander, R.D., **Acceptable Evidence: Science and Values in Risk Management**, Oxford University Press, New York, USA, 1991.

McCormick, N.J., **Reliability and Risk Analysis**, Academic Press, New York, EUA, 1981.

Meyer, P.L., **Probabilidades - Aplicações à Estatística**, Livros Técnicos e Científicos Editora, Rio de Janeiro, Brasil, 1976.

Munier, B.R., **Risk, Decision and Rationality**, Reidel Publishing Co., Dordrecht, Alemanha, 1988.

Neveu, J., Bases **Mathématiques du Calcul des Probabilités**, Masson Éditeurs, Paris, França, 1970.

Morlat, G., **Sur la Théorie de la Décision Appliquée aux Événements Rares**, Nuclear Energy Agency - OECD, Paris, França, 1960.

Papalambros, P.Y. e Wilde, D.J., **Principles of Optimal Design: Modeling and Computation**, Cambridge University Press, Cambridge, EUA, 1988.

Power, G.J. et ali, **Fault Tree Synthesis for Chemical Processes**, AIChE Journal 20 (2), EUA, 1974.

Procaccia, H et ali, **Fiabilité des Équipements et Théorie de la Décision Fréquentielle et Bayésienne**, Collection EdF-DER n0 81, Eyrolles, Paris, 1992.

Raiffa, H., **Analyse de la Décision - Introduction aux Choix en Avenir Incertain**, Éditions Dunod, Paris, França, 1973

Rowe, N. D., **An Anatomy of Risk**, John Wiley and Sons, New York, EUA, 1973

Starr, C. et ali, **Philofical Basis for Risk Analisys**, in Ann.Rev.Energy 1-629, Washigton, EUA, 1976.

SEGURANÇA NUCLEAR

American Society of Mechanical Engineers (ASME), **ASME Boiler and Pressure Vessel Code** Section III, Division 1, Washington, EUA, 1977.

Baumier, J., **Economie de l'Énergie Nucléaire**, , Institut National des Sciences et Techniques Nucléaires, Saclay, França, 1986.

- Baumier, J., **Géopolitique et Économie du Cycle du Combustible Nucléaire**, Institut National des Sciences et Techniques Nucléaires, Saclay, 1989.
- Bourgeois, J., Tanguy, P. e Petit, J., **La Sureté Nucléaire en France et dans le Monde**, Polytechnica, Paris, 1996.
- British Nuclear Energy Society, **Thermal Reactor Safety Assessment**, Thomas Telford House, Londres, 1994.
- Commission des Communautés Européennes CCE, **Summary Report on Safety Objectives in Nuclear Power Plants**, Commission of the European Communities, Bruxelas, 1989.
- Degrange, J-P. e Guimarães, L.S., **Optimisation des Actions de Radioprotection de la Chaîne de Fabrication URE**, Centre d'Études pour l'Évaluation de la Protection dans le Domaine Nucléaire, Note Technique CEPN-NTE-005/95, Junho 1995.
- Direction de la Sûreté des Installations Nucléaires, **Proposition GPR/RSK pour une Approche Commune de la Sûreté pour les Réacteurs à Eau sous Pression du Futur**, Paris, França, 1993.
- Electricité de France, **Règles Générales d'Exploitation (RGE) des Centrales REP 1.300MW**, Lyon, França, 1990.
- Fauré, J., **Approche de la Sûreté des Sites Nucléaires**, Les Éditions de Physique, Les Ulis, França, 1994.
- Georgin, J.P., **Applications de Methodes Probabilistes à la Sûreté Nucléaire**, Centre d'Études sur l'Évaluation de la Protection dans le Domaine Nucléaire, Rapport n047, Fontenay-aux-Roses, França, 1981.
- Institut de Protection et Sûreté Nucléaire, **Étude Probabiliste de Sûreté des Réacteurs à Eau sous Pression de 900 Mwe - Rapport de Synthèse**, Commissariat à l'Énergie Atomique, Paris, França, 1990
- International Atomic Energy Agency, **Extension of the Principles of Radiation Protection to Sources of Potential Exposures**, Safety Series n0104, Viena, Áustria, 1990.

International Atomic Energy Agency, **Guidelines for Accident Analysis of WWER Nuclear Power Plants**, IAEA-EPB-WWER-01, Viena, Áustria, 1995.

International Atomic Energy Agency, **Potential Exposures in Nuclear Safety**, Safety Series n°75 INSAG-9, Viena, Áustria, 1995.

International Atomic Energy Agency, **Preparedness of the Operating Organization (Licensee) for Emergencies at Nuclear Power Plants**, Safety Series n°50-SG-O6, Viena, Áustria, 1982.

International Atomic Energy Agency, **Probabilistic Safety Assessment**, Safety Series n°75 INSAG-6, Viena, Áustria, 1992.

International Atomic Energy Agency, **Radionuclide Source Terms from Severe Accidents to Nuclear Power Plants with Light Water Reactors**, Safety Series n°75 INSAG-2, Viena, Áustria, 1987.

International Atomic Energy Agency, **Safety Functions and Component Classification for BWR, PWR and PTR**, Safety Series n°50-SG-D1, Viena, Áustria, 1979.

International Atomic Energy Agency, **Summary Report on the Post-Accident Review meeting on the Chernobyl Accident**, Safety Series n°75 INSAG-1, Viena, Áustria, 1986 e **The Chernobyl Accident: Updating INSAG-1** Safety Series n°75 INSAG-7, Viena, Áustria, 1993.

International Atomic Energy Agency, **Sûreté Radiologique**, Viena, Áustria, 1996.

International Atomic Energy Agency, **The Role of Probabilistic Safety Assessment and Probabilistic Safety Criteria in Nuclear Power Plant Safety**, IAEA Safety Series n°106, Viena, Áustria, 1992.

La Gorce, P-M., **L'Aventure de l'Atome**, Flammarion, Paris, França, 1992.

Layfield, F., **The Sizewell Public Inquiry**, HMSO, Londres, 1988.

Libmann, J., **Approche et Analyse de la Sûreté des Réacteur à Eau sous Pression**, INSTN-CEA, Collection Enseignement, Paris, França, 1987.

Nuclear Energy Agency, **The Role of Nuclear Reactor Containment in Severe Accidents**, Organisation for Economic Co-operation and Development, Paris, França, 1989.

Organização de Cooperação e de Desenvolvimento Econômicos OCDE, **Prévision de Coûts de l'Électricité Produites par des Centrales Nucléaires Mises en Service en 1995-2000**, Agência da OCDE para a Energia Nuclear AEN, Paris, França, 1989.

Otway, H.J. e Cohen, J.J., **Reactor Safety and Design from a Risk View Point**, in Nuclear Engineering and Design 13-365, Washington, EUA, 1970.

Rogers, J.T., **Fission Product Transport Processes in Reactor Accidents**, Hemisphere, New York, USA, 1990

San Diego Gas and Electric Company, **Sundesert Nuclear Plant Units 1 & 2 Preliminary Safety Analysis Report**, San Diego, EUA, 1977.

Simard, R.L., **Applications of NPRDS Data to Enhance Nuclear Plant Design and Operations**, Institute of Nuclear Power Operations (INPO), ANS/ENS International Topical Meeting on Probabilistic Safety Methods and Applications, San Francisco, EUA, 1985.

Tribus, M., **Décisions Rationnelles dans l'Incertain**, Masson Éditeurs, Paris, França, 1972.

U.S. Air Force, **Electronic Parts Reliability Data**, Military Handbook 217, Rome Air Development Center, Griffis, EUA, 1983.

U.S. Air Force, **Non-Electronic Parts Reliability Data**, NPRD2, Rome Air Development Center, Griffis, EUA, 1985.

Ventsel, H., **Théorie des Probabilités**, MIR, Moscou, Rússia, 1973.

Vigier, M., **Méthodes d'Assurance de Qualité-Fiabilité et d'Expérimentation**, Malione Éditeurs, Compiègne, França, 1981

Volkovsyski, L. et ali, **Problemas sobre a teoria de Funciones de Variable Compleja**, Editorial Mir, Moscou, Rússia, 1972

Wald, A., **Statistical Decision Functions**, John Wiley and Sons, New York, EUA, 1950.

SEGURANÇA NAVAL

Antier, J-J., **Histoire Mondiale du Sous-Marins**, Robert Lafont, Paris, França, 1968.

Chambard, C., **Les Sous-marins**, Éditions France-Empire, Paris, França, 1968

Friedman, N., **Submarine Design and Development**, Conway Maritime Press, London, 1984.

Horlick, T., **Submarine Propulsion in the Royal Navy**, Proceedings of Institute of Mechanical Engineers vol. 196, Londres, Grã-Bretanha, 1982.

Humble, R., **Undersea Warfare**, Book Club Associates, Londres, Grã-Bretanha, 1981.

Kaufman, Y. e Stillwell, P., **Sharks of Steel**, Naval Institute Press, Annapolis, EUA, 1993.

Louzeau, B. e Chourgnoz, JM, **Les Bateaux Noirs**, Éditions Courgnoz, Brest, França, 1992

Maclean, M., **Naval Accident Losses: a 25-year History**, in Navy International, Fevereiro, 1989.

Miller, D., Miller, C., **Modern Naval Combat**, Crescent Books, New York, EUA, 1986.

Meigs, C.H., **Recent Naval Steam Plant Design**, Transactions SNAME vol. 62, New York, EUA, 1954.

OREDA, **Offshore Reliability Data**, PennWell Books, Londres, G.B., 1984.

Sheets, H.E., **The Engineering of Sumarines**, Naval Engineers Journal, Londres, Grã-Bretanha, ago. 1962.

SEGURANÇA NUCLEAR NAVAL

Alexandrov, A.P., **The Atomic Icebreaker Lenin**, IAEA Conference on Peaceful Applications of Atomic Energy, Genebra, Suíça, 1958.

Ancellin, J., **Radioecologie Marine**, Eyrolles, Paris, 1979.

British Nuclear Fuels plc., **Annual Report and Accounts 1987/1988**, Risley, Warrington, UK, 1989.

- Colgate, S.A., **Plasma Reactors Promises**, Nucleonics vol.15, no.8, Interscience Publishers Inc., Nova Iorque, EUA, 1966.
- Considine, D.M., **Magnetohydrodynamic Generators and Thermionic Converters**, McGraw-Hill, Nova Iorque, EUA, 1977.
- Danilov, L.G. et alli, **Certain Results Concerning the Experience of Operation of the Nuclear Icebreaker Lenin**, in Compte-rendu du OECD/AIEA Symposium sur la sûreté des navires nucléaires, Hamburgo, Alemanha, 5-9 dez. 1977.
- École Nationale Supérieure de Techniques Avancées, **Approche et Analyse de la Propulsion Nucléaire des Navires Militaires**, apostila de curso ENSTA, Paris, França, 1994.
- Edwards, J. e Tucker, K.F., **Royal Navy Requirements and Achievements in Nuclear Training**, Journal of Nuclear Sciences vol. 4 no. 3, Londres, Grã-Bretanha, 1980.
- Giltsov, L., **La Dramatique Histoire des Sous-marins Nucléaires Soviétiques**, Éditions Robert Lafont, Paris, 1992.
- Guéguénat, P. et alli, **Radionuclides in the Oceans: Inputs and Inventories**, IPSN-les Éditions de Physique, Les Ulis, França, 1996.
- House of Commons Defence Committee, **Decommissioning of Nuclear Submarines**, 7th Report, Session 1988-1989, Her Majesty's Stationary Office, Londres, Grã-Bretanha, 1989.
- International Atomic Energy Agency, **GESAMP: An Oceanographic Model for the Dispersion of Wastes Disposed of in Deep Sea**, Reports and Studies n0 19, Viena, 1981.
- International Atomic Energy Agency, **Methodology for Assessing Impacts of Radioactivity on Aquatic Ecosystems**, Technical Reports Series n0 190, Viena, 1979.
- International Maritime Organization, **Code of Safety for Nuclear Merchant Ships**, Londres, Grã-Bretanha, 1988.

Japan Atomic Energy Research Institute, **Nuclear Research Ship MUTSU Safety Assessment**, Japan Atomic Energy Research Institute, Tóquio, Japão, 1992.

Lévy, M.E., **Inventaire rationnel des problèmes de sûreté posés par les navires nucléaires**, in Compte-rendu du OECD/AIEA Symposium sur la sûreté des navires nucléaires, Hamburgo, 5-9 dez. 1977.

Marietta, M.G. e Simmons, W.F., **Dispersal of radionuclides in the Oceans: Modes, Data Sets and Regional Descriptions**, Vol.8, Nuclear Energy Agency (NEA), Paris, 1988.

MacMillan, J.H., **NS Savannah Operating Experience**, Transactions SNAME, New York, EUA, 1964.

McGill, J.E., **The Design of Air Conditioning and Ventilation Systems for Nuclear Submarines**, Transactions SNAME, , New York, EUA, 1960.

National Academy of Sciences, **Radioactivity in the Marine Environment**, Report NAS, Washington, EUA, 1971.

Noshkin, V.E. e Wong, K.M., **Plutonium Mobilization from Sedimentary Sources to Solution in the Environment**, Marine Ecology Seminar held in Tokio 1979, NEA, Paris, 1980.

Nuclear Energy Agency (OECD), **Review of the Continued Suitability of the dumping Site for Radioactive Waste in the North-East Atlantic**, Nuclear Energy Agency (NEA) Report, Paris, 1985.

OECD/NEA, **Achieving Nuclear Safety: Improvements on Reactor Safety Design and Operation**, Organization for Economic Co-operation Development / Nuclear Energy Agency, Paris, França, 1993

OMCI, **Recueil de Règles de Sécurité Applicables aux Navires de Commerce Nucléaires**, 44ème session du Comité de la Sécurité Maritime, Londres, 1969.

Pepper, D.J., **Experience in the Design and Manufacture of Marine Nuclear Plant**, Naval Engineers Journal, Londres, Grã-Bretanha, nov. 1962.

Pentreath, R.J. e al., **Alpha-emitting Nuclides in Commercial Fish Species Caught in the Vicinity of Windscale UK and their Significance to Man**, Proceedings of Seminar IAEA, Viena 1979.

Pocock, R.F., **Nuclear Ship Propulsion**, Ian Allan Editor, Londres, Grã-Bretanha, 1970.

Rickover, H.G. et al., **Some Problems in the Application of Nuclear Propulsion to Naval Vessels**, comunicação apresentada no 65th Annual Meeting of the SNAME, New York, EUA, 14-15 Nov., 1957.

Rockwell, T., **Reactor Shielding Design Manual**, McGraw-Hill Book Company, New York, EUA, 1956.

Tabb, H.J. e Warren, A.T., **Quality Control Applied to Nuclear Submarine Construction**, Transactions of Royal Institute of Naval Architects, Londres, Grã-Bretanha, 1967.

Tournyol du Clos, A., **Bilan et Perspectives de la Propulsion Nucléaire Maritime**, in Compte-rendu de la Journée d'Études sur Réacteur Navales et Spatiaux, Association Technique Maritime et Aéronautique (ATMA), Arcueil, França, 1994.

U.S. Atomic Energy Commission, **NS 'Savannah' Safety Assessment**, U.S. Atomic Energy Commission, Washington, EUA, 1961.

Viana, I.A., **Programa Nuclear da Marinha**, Federação e Centro das Indústrias do Estado de São Paulo, Instituto Roberto Simonsen, Núcleo de Assuntos Estratégicos, São Paulo, 1995,

ARTIGOS TÉCNICOS PUBLICADOS

[1] Crouail, P., e Guimarães, L., **Deux défis à l'optimisation de la radioprotection: les expositions internes et les expositions potentielles**, in Compte-Rendu de la 1^{ère} Journée sur l'Optimisation de la Radioprotection, Société Française de Radioprotection, La Rochelle, 1994

[2] Crouail, P., e Guimarães, L., **Fundamental Principles for Potential Exposures Optimization**, in Proceedings from III International Workshop on ALARA in Nuclear Power Plants, Brookhaven National Laboratory, Long Island, EUA, 1994

- [3] Guimarães, L., **Protótipos em Terra de Instalações Propulsoras Nucleares**, in Anais do VI Congresso Geral de Energia Nuclear, Rio de Janeiro, 1996.
- [4] Guimarães, L., **Introdução às Instalações Propulsoras Nucleares Navais**, in Anais do VI Congresso Geral de Energia Nuclear, Rio de Janeiro, 1996.
- [5] Guimarães, L., **Introdução à Análise de Segurança da Propulsão Nuclear de Navios Militares**, in Anais do VI Congresso Geral de Energia Nuclear, Rio de Janeiro, 1996.
- [6] Viana, I.A., e Guimarães, L.S., **Estratégias de Implementação e Efeitos de Arraste dos Grandes Programas de Desenvolvimento Tecnológico Nacionais: Experiências do Programa de Propulsão Nuclear da Marinha do Brasil**, comunicação apresentada no evento comemorativo do 30^o aniversário da Sociedade Brasileira de Física, Águas de Lindóia, 1996.
- [7] Guimarães, L., **Introdução às Instalações Propulsoras Nucleares Navais**, in Revista Marítima Brasileira v117 nº 7/9 (jul/set 97), Serviço de Documentação da Marinha, Rio de Janeiro, 1997.
- [8] Guimarães, L., **Introdução à Análise de Segurança da Propulsão Nuclear de Navios Militares**, in Revista Marítima Brasileira v117 nº 10/12 (out/dez 97), Serviço de Documentação da Marinha, Rio de Janeiro, 1997.
- [9] Guimarães, L., **Otimização do Conjugado Disponibilidade x Segurança para Instalações Propulsoras Nucleares de Navios Militares**, in Anais do XI Encontro Nacional de Física de Reatores, Poços de Caldas, 1997.
- [10] Guimarães, L., **Otimização do Conjugado Disponibilidade x Segurança para Instalações Propulsoras Nucleares de Submarinos**, in Revista “O Periscópio” jul 97, Centro de Instrução Almirante Átila Monteiro Achè, Rio de Janeiro, 1997.
- [11] Degrange, J-P. e Guimarães, L., **Procedimento ALARA Aplicado à Fabricação de Combustível à Base de Urânio de Reprocessamento**, in Anais do XI Encontro Nacional de Aplicações Nucleares, Poços de Caldas, 1997.

- [12] Costa Veiga, J.P. e Guimarães, L., **Impacto Ambiental de um Submarino Nuclear Naufragado**, in Anais do III Simpósio sobre Ondas e Marés e II Seminário de Engenharia Oceânica, Instituto de Estudos do Mar Almirante Paulo Moreira, Arraial do Cabo, 1997.
- [13] Guimarães, L., **Protótipos em Terra de Instalações Propulsoras Nucleares**, in Revista Marítima Brasileira v118 nº 1/3 (jan/mar 98), Serviço de Documentação da Marinha, Rio de Janeiro, 1998.
- [14] Guimarães, L., **Otimização do Conjugado Disponibilidade x Segurança para Instalações Propulsoras Nucleares de Navios Militares**, in Revista Marítima Brasileira v118 nº 4/6 (abr/jun 98), Serviço de Documentação da Marinha, Rio de Janeiro, 1998.
- [15] Degrange, J-P. e Guimarães, L., **Procedimento ALARA Aplicado à Fabricação de Combustível à Base de Urânio de Reprocessamento**, Revista Pesquisa Naval nº 11 (out 98), Serviço de Documentação da Marinha, Rio de Janeiro, 1998.
- [16] Guimarães, L., **Logística de Produção de Combustível Nuclear para um Esquadrão de Submarinos Nucleares de Ataque**, in Anais do III Simpósio de Logística da Marinha, Rio de Janeiro, 1998.
- [17] Guimarães, L., **Impacto Ambiental de um Submarino Nuclear Naufragado**, in Anais do I Simpósio sobre Monitoramento do Meio Ambiente Marinho, Instituto de Estudos do Mar Almirante Paulo Moreira, Arraial do Cabo, 1998.
- [18] Guimarães, L., **Impacto Ambiental de um Submarino Nuclear Naufragado**, in Revista Marítima Brasileira v118 nº 7/9 (jul/set 98), Serviço de Documentação da Marinha, Rio de Janeiro, 1998.
- [19] Guimarães, L., **Radioatividade Artificial no Meio Ambiente Marinho**, in Anais do I Simpósio sobre Monitoramento do Meio Ambiente Marinho, Instituto de Estudos do Mar Almirante Paulo Moreira, Arraial do Cabo, 1998.

- [20] Guimarães, L., **Radioatividade Artificial no Meio Ambiente Marinho**, in Revista Marítima Brasileira v118 nºs 10/12 (out/dez 98), Serviço de Documentação da Marinha, Rio de Janeiro, 1998.
- [21] Guimarães, L., **Leis de Distribuição de Probabilidades de Valores Extremos**, submetido para publicação na Revista Pesquisa Naval nº10 (out 97), Serviço de Documentação da Marinha, Rio de Janeiro, 1998.
- [22] Guimarães, L., **Delineamento de uma Doutrina de Segurança Integral para Submarinos Nucleares no Brasil**, submetido para publicação nos Anais do VII Congresso Geral de Energia Nuclear, Belo Horizonte, 1999.
- [23] Guimarães, L., **Delineamento de uma Doutrina de Segurança Integral para Submarinos Nucleares no Brasil**, submetido para publicação na Revista “O Periscópio” jul 99, Centro de Instrução Almirante Átila Monteiro Achê, Rio de Janeiro, 1999.
- [24] Guimarães, L., **Conceituação da Segurança de Funcionamento de Sistemas**, submetido para publicação na Revista Pesquisa Naval nº12 (out 99), Serviço de Documentação da Marinha, Rio de Janeiro, 1999.
- [25] Guimarães, L., **Prospectivas e Estratégias para o Desenvolvimento da Energia Nuclear no Brasil: Contribuição a um Necessário Debate Nacional**, submetido para publicação na Revista Marítima Brasileira v119 nºs 1/3 (jan/mar 99), Serviço de Documentação da Marinha, Rio de Janeiro, 1999.
- [26] Guimarães, L., **Perfis de Operação de um Submarino Nuclear de Ataque**, submetido para publicação na Revista “O Passadiço”, Centro de Adestramento Almirante Marques Leão, Rio de Janeiro, 1999.

DADOS GERAIS SOBRE SUBMARINOS NUCLEARES EXISTENTES NO MUNDO

CLASSE	EMPREGO	ANO	PAÍS	UNIDADES	DESLOCAMENTO	COMPRIMENTO	DIÂMETRO	VELOCIDADE	POTÊNCIA DE PROPULSAO	REATOR	HÉLICES	
XIA	BALISTICO	1987	CHINA	1	8000	120,00	10,00	22	0	PWR	1	UNIDADES EM CONSTRUCAO TERA0 NUMERO DE MISSEIS AUMENTADO PARA 16 - APOIO TECNICO FRANCES
HAN	ATAQUE	1974	CHINA	2	5000	100,00	11,00	25	0	PWR	1	CADA UNIDADE TARDOU CERCA DE DEZ ANOS EM CONSTRUCAO E NAO SE ENCONTRAN PLENAMENTE OPERACIONAIS
TOTAL			CHINA	3								
NAS	ATAQUE	1998	EUA	4	7300	115,00	10,40	28	0	PWR	1	PROJETO EM DESENVOLVIMENTO
SEAWOLF	ATAQUE	1998	EUA	3	9137	107,00	12,90	35	52500	PWR	1	PRIMEIRA UNIDADE DA CLASSE COMISSONADA EM 1998
OHIO	BALISTICO	1981	EUA	8	18700	170,70	12,80	20	60000	PWRL(S8G)	1	CLASSE PROJETADA PARA TRANSPORTAR OS MISSEIS TRIDENT
LOS ANGELES	ATAQUE	1976	EUA	38	6927	109,70	10,10	30	35000	PWRL(S6G)	1	DOTADO DE TUBOS DE TORPEDOS LATERAIS E "ARRAY" DE HIDROFONES REBOCAVEL
GLENARD P. LIPSCOMB	ATAQUE	1974	EUA	1	6480	111,30	9,70	25	3500	PWRL(S5Wa)	1	SEGUNDO E ULTIMO SUBMARINO NUCLEAR AMERICANO COM PROPULSAO TURBO-ELETTRICA
NARWHAL	ATAQUE	1969	EUA	1	5350	95,90	11,50	30	17000	PWR(S5G)	1	CASCO SIMILAR AO STURGEON POREM DOTADO DE UM REATOR EXPERIMENTAL DE CIRCULACAO NATURAL
NR 1	PESQUISA	1969	EUA	1	400	41,60	3,80	0	0	PWR	2	MENOR SN CONSTRUIDO NOS EUA - EMPREGO DESCONHECIDO
STURGEON	ATAQUE	1967	EUA	37	4640	89,00	9,50	30	15000	PWRL(S5W)	1	DOTADO DE TUBOS DE TORPEDO LATERAIS DEVIDO AO SONAR ESFERICO NA PROA
LAFAYETTE	BALISTICO	1963	EUA	31	8250	129,50	10,10	30	15000	PWRL(S5W)	1	BENJAMIN FRANKLIN CONSIDERADO DE CLASSE INDEPENDENTE POR ALGUMAS REFERENCIAS
PERMIT	ATAQUE	1961	EUA	14	4300	84,90	9,60	30	15000	PWRL(S5W)	1	PRIMEIRO DA CLASSE PERDIDO (TRESHER) - UMA UNIDADE DOTADA DE 2 HELICES CONTRARROTATIVOS(SUBSTITUIDO)
TULLIBEE	ATAQUE	1960	EUA	1	2640	83,20	7,10	15	2500	PWRL(S2C)	1	PRIMEIRO SN DOS EUA TURBO-ELETTRICO E COM TUBOS DE TORPEDO LATERAIS - CONCEBIDO COMO SB ANTI-SB
ETHAN ALLEN	BALISTICO	1960	EUA	4	7880	125,00	10,10	30	15000	PWRL(S5W)	1	2 UNIDADES CONVERTIDAS EM SNA AINDA EM OPERACAO COMO NAVIOS-AUXILIARES
TRITON	ATAQUE	1959	EUA	1	6670	136,20	11,30	20	34000	PWRL(S4G)	2	ORIGINALMENTE PROJETADO COMO PIQUETE RADAR
SKIPJACK	ATAQUE	1959	EUA	5	3513	76,70	9,60	30	15000	PWRL(S5W)	1	PRIMEIRO SB NUCLEAR COM CASCO "EM FORMA DE GOTA" DERIVADO DO SB ALBACORE-SCORPION AFUND0U EM 1968
GEORGE WASHINGTON	BALISTICO	1959	EUA	3	6880	116,30	10,10	30	15000	PWRL(S5W)	1	PRIMEIRO LANCADOR DE BALISTICOS CONSTRUIDO - ADAPTADO DO CASCO DA CLASSE SKIPJACK
HALLIBUT	M.CRUZADOR	1959	EUA	1	5000	106,60	9,00	20	6000	PWRL(S3W)	2	UNICO LANCADOR DE MISSIL "CRUISE" DOS EUA - PROGRAMA MISSIL REGULUS FOI ABANDONADO - MODIFICADO SNA
SKATE	ATAQUE	1957	EUA	4	2360	81,50	7,60	25	6600	PWRL (S3W)	2	PRIMEIRO SUB NUCLEAR A ROMPER A CALOTA DE GELO ARTICO EMERGINDO NO POLO NORTE
SEAWOLF	ATAQUE	1956	EUA	1	4200	102,90	8,40	20	15000	PWRL(S2Wa)	2	ORIGINALMENTE LMFR (SEA INTERMEDIATE REACTOR-SIR) - APOS 1 ANO DE OPERACAO FOI SUBSTITUIDO POR PWR
NAUTILUS	ATAQUE	1955	EUA	1	4200	97,40	8,40	20	15000	PWRL(STR)	2	PRIMEIRO SUBMARINO NUCLEAR CONSTRUIDO- DERIVADO DO PROTOTIPO MARK I (SEA TEST REACTOR-STR)

DADOS GERAIS SOBRE SUBMARINOS NUCLEARES EXISTENTES NO MUNDO

CLASSE	EMPREGO	ANO	PAÍS	UNIDADES	DESLOCAMENTO	COMPRIMENTO	DIÂMETRO	VELOCIDADE	POTÊNCIA DE PROPULSAO	REATOR	HÉLICES	
TOTAL			EUA	159								
LE TRIOMPHANT	BALISTICO	1994	FRANCA	3	14200	138,00	12,50	25	41000	PWRI	1	EM PROJETO PARA TRANSPORTAR NOVO MODELO DE BALISTICO FRANCES
AMETHYSTE	ATAQUE	1991	FRANCA	2	2670	73,60	7,60	25	10000	PWRI	1	MODELO APERFEICOADO DA CLASSE RUBIS
L'INFLEXIBLE	BALISTICO	1985	FRANCA	5	8920	128,70	10,60	25	30000	PWRI	1	MODELO APERFEICOADO DA CLASSE LE REDOUTABLE
RUBIS	ATAQUE	1982	FRANCA	4	2670	72,10	7,60	25	10000	PWRI	1	MENOR SNA CONSTRUÍDO,JUNTAMENTE COM TULIBEE (MESMO DESLOCAMENTO)
LE REDOUTABLE	BALISTICO	1971	FRANCA	1	8940	128,70	10,60	25	16000	PWRL	1	PRIMEIRO SUBMARINO NUCLEAR FRANCES - TEVE DESENVOLVIMENTO INDEPENDENTE
TOTAL			FRANCA	15								
VANGUARD	BALISTICO	1992	GRÃ-BRETANHA	0	15000	148,30	12,80	25	27500	PWR	1	LANCADOR DE MISSIL TRIDENT BRITANICO - PROJETO E CONSTRUCAO DESACELERADO
TRAFALGAR	ATAQUE	1983	GRÃ-BRETANHA	4	5208	85,40	9,80	32	15000	PWRL	1	UNIDADES POSTERIORES A PRIMEIRA DOTADAS DE PROPULSOR EM DUTO TIPO "PUMP-JET"
SWIFTSURE	ATAQUE	1973	GRÃ-BRETANHA	6	4900	82,90	9,80	30	15000	PWRL	1	BATERIA AUXILIAR COM 112 CELULAS
RESOLUTION	BALISTICO	1967	GRÃ-BRETANHA	4	8500	129,50	10,10	25	15000	PWR	1	PRIMEIRO BALISTICO BRITANICO DOTADO DE MISSEIS AMERICANOS POSEIDON
VALLIANT	ATAQUE	1966	GRÃ-BRETANHA	5	4800	86,90	10,10	28	15000	PWRL(NR2)	1	BATERIA AUXILIARES COM 112 CELULAS - CONQUERROR AFUNDOU CRUZADOR BELGRANO NAS MALVINAS
DREADNOUGHT	ATAQUE	1960	GRÃ-BRETANHA	1	4000	81,00	9,80	30	15000	PWRL(\$SW)	1	PRIMEIRO SN INGLES - SISTEMA DE PROPULSAO NUCLEAR AMERICANO (REATOR \$SW)
TOTAL			GRÃ-BRETANHA	20								
SEVERODVINSK	ATAQUE	1998	RÚSSIA	2	11800	120,00	15,00	28	43000	PWR	1	PROJETO EM DESENVOLVIMENTO
AKULA	ATAQUE	1985	RÚSSIA	3	8000	107,00	13,00	42	0	LMFR	1	RECORDISTA DE VELOCIDADE ENTRE OS SN - DOTADO DE UM "BULBO" NO LEME VERTICAL SUPERIOR
DELTA IV	BALISTICO	1985	RÚSSIA	4	13600	160,00	12,00	24	60000	PWR	2	
SIERRA	ATAQUE	1984	RÚSSIA	2	7600	110,00	12,40	35	40000	PWR	1	
MIKE	ATAQUE	1984	RÚSSIA	1	6400	110,00	12,00	38	0	LMFR	1	PROTOTIPO EXPERIMENTAL , AFUNDOU NA COSTA DA NORUEGA EM 1989
YANKEE CONV.SLMC	M.CRUZADOR	1983	RÚSSIA	1	13650	153,00	15,00	23	35000	PWR	2	
X-RAY	PESQUISA	1983	RÚSSIA	1	250	39,60	3,00	0	0	??????????	0	MENOR SN CONSTRUÍDO URSS - EMPREGO DESCONHECIDO
TYPHOON	BALISTICO	1982	RÚSSIA	5	25000	170,00	25,00	30	80000	PWR	2	MAIOR SUBMARINO JA CONSTRUÍDO - BALISTICOS AVANTE DA VELA - 3 (OU 5?) CASCOS INDEPENDENTES

DADOS GERAIS SOBRE SUBMARINOS NUCLEARES EXISTENTES NO MUNDO

CLASSE	EMPREGO	ANO	PAÍS	UNIDADES	DESLOCAMENTO	COMPRIMENTO	DIÂMETRO	VELOCIDADE	POTÊNCIA DE PROPULSÃO	REATOR	HÉLICES	
UNIFORM	PESQUISA	1982	RÚSSIA	1	2500	73,00	7,00	0	0	?????????	0	EMPREGO DESCONHECIDO.POSSIVELMENTE UM PROTOTIPO DE DESENVOLVIMENTO
OSCAR	M.CRUZADOR	1980	RÚSSIA	4	16000	150,00	18,30	30	90000	PWR	2	
VICTOR III	ATAQUE	1978	RÚSSIA	22	6300	104,00	10,00	30	30000	PWR	1	DOTADO DE DOIS HELICES CONTRARROTATIVOS
DELTA II	BALISTICO	1976	RÚSSIA	4	5000	152,00	11,00	25	30000	PWRL	2	
DELTA III	BALISTICO	1976	RÚSSIA	14	13250	155,00	12,00	24	50000	PWR	2	
CHARLIE I	M.CRUZADOR	1973	RÚSSIA	10	4800	94,00	9,90	24	15000	PWR	1	
CHARLIE II	M.CRUZADOR	1973	RÚSSIA	6	5500	102,00	9,90	24	15000	PWR	1	
VICTOR II	ATAQUE	1972	RÚSSIA	7	6000	102,00	10,00	31	30000	PWR	1	
DELTA I	BALISTICO	1972	RÚSSIA	18	11000	139,00	12,00	26	50000	PWR	2	
ALFA	ATAQUE	1970	RÚSSIA	6	3700	81,40	10,00	42	47000	LMFR	1	SN REVOLUCIONARIO:EXTREMAMENTE PEQUENO,VELOZ,AUTOMATIZADO - REATOR RESFRIADO A CHUMBO-BISMUTO
PAPA	M.CRUZADOR	1969	RÚSSIA	1	8000	109,00	12,20	39	60000	PWR	2	
VICTOR I	ATAQUE	1968	RÚSSIA	16	5300	93,00	10,00	32	30000	PWR	1	
YANKEE I/II	BALISTICO	1967	RÚSSIA	17	9600	130,00	11,60	28	50000	PWR	2	DUAS UNIDADES CONVERTIDAS E 13 EM CONVERSAO PARA SNA
ECHO II	M.CRUZADOR	1967	RÚSSIA	29	6200	116,00	9,80	24	30000	PWR	2	DOTADO DE 4 TUBOS DE TORPEDO A RE
HOTEL II	BALISTICO	1962	RÚSSIA	7	5500	115,20	9,10	26	30000	PWR	2	UMA UNIDADE CONVERTIDA EM SSQN (SB ESPECIALIZADO EM COMUNICACOES) - 6 UNIDADES EM SNA
HOTEL III	BALISTICO	1962	RÚSSIA	1	6500	130,00	9,10	22	30000	PWR	2	DOTADO DE DOIS TUBOS DE TORPEDO A RE
HOTEL	BALISTICO	1960	RÚSSIA	6	6000	115,20	9,10	20	22500	PWR	2	PRIMEIRO LANCADOR DE BALISTICOS SOVIETICO - SILOS DE MISSEIS NA VELA
ECHO I	M.CRUZADOR	1960	RÚSSIA	5	5500	112,00	9,80	20	22500	PWR	2	DOTADO DE 4 TUBOS A RE - CONVERTIDOS EM SNA - VARIAS UNIDADES ACIDENTADAS
NOVEMBER	ATAQUE	1958	RÚSSIA	12	5000	109,70	9,10	30	30000	PWR	2	PRIMEIRO SN URSS - NAO FOI DESENVOLVIDO A PARTIR DE UM PROTOTIPO EM TERRA-1 UNIDADE AFUNDOU EM 1970
TOTAL			RÚSSIA	205								
TOTAL				402								