INSTITUTO DE PESQUISAS ENERGÉTICAS E NUCLEARES

Autarquia associada à Universidade de São Paulo

**APLICAÇÃO DA TÉCNICA DE ANÁLISE DE MODOS DE FALHA E EFEITOS
AO SISTEMA DE RESFRIAMENTO DE EMERGÊNCIA DE UMA INSTALAÇÃO
NUCLEAR EXPERIMENTAL**

OSMAR CONCEIÇÃO JÚNIOR

Dissertação apresentada como parte
dos requisitos para obtenção do Grau
de Mestre em Ciências na área de
Tecnologia Nuclear – Reatores.

Orientador:

Prof. Dr. Antonio Teixeira e Silva

São Paulo

2009

INSTITUTO DE PESQUISAS ENERGÉTICAS E NUCLEARES

Autarquia associada à Universidade de São Paulo

**APLICAÇÃO DA TÉCNICA DE ANÁLISE DE MODOS DE FALHA E EFEITOS
AO SISTEMA DE RESFRIAMENTO DE EMERGÊNCIA DE UMA INSTALAÇÃO
NUCLEAR EXPERIMENTAL**

OSMAR CONCEIÇÃO JÚNIOR

Dissertação apresentada como parte dos requisitos para obtenção do Grau de Mestre em Ciências na área de Tecnologia Nuclear – Reatores.

Orientador:

Prof. Dr. Antonio Teixeira e Silva

São Paulo

2009

DEDICATÓRIA

À minha esposa Daniela.
Aos meus pais Osmar e Cecy.

AGRADECIMENTOS

A Deus, em primeiro lugar, pelo dom da vida, pelo Seu infinito amor, misericórdia e pela salvação graciosa em Jesus Cristo.

À Marinha do Brasil, por ter me proporcionado esta oportunidade de crescimento e aprimoramento profissional.

À minha esposa Daniela pelo apoio e contribuição em todas as etapas de realização desta dissertação.

Aos meus pais, irmãos, familiares e amigos pela educação, pelo caráter, pelo exemplo, pelos valores e pelo imenso amor e carinho demonstrados.

Ao meu orientador Prof. Dr. Antonio Teixeira e Silva, pela pronta recepção e concordância na realização deste trabalho, bem como por todas as sugestões e contribuições oferecidas ao longo destes dois últimos anos.

Ao Prof. Dr. Ricardo Sbragio e ao Prof. Dr. Eduardo Henrique Rangel Honaizer, pelo suporte técnico prestado no âmbito da Marinha do Brasil.

Ao Prof. Dr. Gilberto Francisco Martha de Souza, pelos conhecimentos transmitidos na área de Análise de Risco, fundamentais para a confecção deste estudo.

Aos demais professores da USP e do IPEN, por sua contribuição na minha formação acadêmica.

Aos engenheiros Walther José Ferreira e Ricardo Takeshi Vieira da Rocha, pela concessão em analisar o sistema por eles desenvolvido e pelos esclarecimentos prestados em relação ao mesmo.

Às equipes de Análise de Risco do Centro Tecnológico da Marinha em São Paulo e do IPEN, em especial à Beatriz, Antonio Souza e Eugênia, pela troca de informações nesta área.

Aos colegas de trabalho, alunos e funcionários do IPEN (particularmente os da Comissão de Pós-Graduação), pela convivência, pelo auxílio e pelos esclarecimentos prestados.

A todos que, direta ou indiretamente, contribuíram para o sucesso deste projeto.

EPÍGRAFE

“É minha convicção de que nos encontramos em face de um dilema decisivo e irrecurível: ou nos preparamos para tomar posse de nossas riquezas naturais – no caso específico atômicas – ou nos veremos constrangidos ao espetáculo degradante de assistirmos, impotentes, à evasão delas, por bem ou por mal.”

Almirante Álvaro Alberto da Motta e Silva (1889 a 1976),
Idealizador, fundador e primeiro presidente do CNPq.

RESUMO

Este trabalho consiste em aplicar a técnica de identificação de perigos e análise de risco conhecida como Análise de Modos de Falha e Efeitos (AMFE) ao Sistema de Resfriamento de Emergência (SRE) de uma instalação nuclear experimental, cuja função é a de mitigar as conseqüências de um eventual acidente de perda de refrigerante no circuito primário de um reator a água pressurizada. Esse tipo de análise tem como objetivo identificar as possíveis vulnerabilidades desse sistema e propor melhorias de modo a maximizar sua confiabilidade.

Para isso foi realizado o estudo detalhado do sistema (por intermédio de sua documentação técnica), obtido o diagrama de blocos correspondente, feita a análise do tipo AMFE e, finalmente, apresentadas algumas sugestões.

ABSTRACT

This study consists on the application of the Failure Modes and Effects Analysis (FMEA), a hazard identification and a risk assessment technique, to the Emergency Cooling System (ECS) of an experimental nuclear power plant, which is responsible for mitigating the consequences of an eventual loss of coolant accident on the Pressurized Water Reactor (PWR). Such analysis intends to identify possible weaknesses on the design of the system and propose some improvements in order to maximize its reliability.

To achieve this goal a detailed study of the system was carried on (through its technical documentation), the correspondent reliability block diagram was obtained, the FMEA analysis was executed and, finally, some suggestions were presented.

SUMÁRIO

1 INTRODUÇÃO	1
2 REVISÃO DA LITERATURA E ESCOLHA DA TÉCNICA	4
2.1 O CONCEITO DE RISCO	4
2.2 AS PRINCIPAIS TÉCNICAS DE IDENTIFICAÇÃO DE PERIGOS	9
2.3 A ESCOLHA DA TÉCNICA A SER UTILIZADA	38
3 A INSTALAÇÃO NUCLEAR EXPERIMENTAL	40
3.1 DESCRIÇÃO	40
3.2 O SISTEMA DE RESFRIAMENTO DE EMERGÊNCIA (SRE)	45
3.2.1 Descrição Geral	45
3.2.2 Função do SRE	48
3.2.3 Modos de operação do SRE	48
3.2.3.1 Operação do SRE durante resfriamento normal do primário	49
3.2.3.2 Operação do SRE durante resfriamento anormal do primário	50
3.2.3.3 Remoção do calor residual por circulação natural	51
3.2.3.4 Acidentes de perda de refrigerante do reator	51
3.2.3.4.1 Pequenas perdas de refrigerante do reator	52
3.2.3.4.2 Grandes perdas de refrigerante do reator	53
4 RESULTADOS	56
4.1 CONSIDERAÇÕES INICIAIS	56
4.2 ANÁLISE TIPO AMFE	64
4.3 ANÁLISE DOS RESULTADOS	81
5 CONCLUSÕES	88
REFERÊNCIAS BIBLIOGRÁFICAS	90

LISTA DE TABELAS

Tabela 1 – Análise tipo AMFE do SIE (tanques de compensação)	65
Tabela 2 – Análise tipo AMFE do SIE (acumuladores).....	67
Tabela 3 – Análise tipo AMFE do SIE (tanques de inundação)	69
Tabela 4 – Análise tipo AMFE do SIE (linha de equalização de pressão)	75
Tabela 5 – Análise tipo AMFE do SRCR.....	78

LISTA DE FIGURAS

Figura 1 – Blocos 20, 30 e 40 (extraído do RPAS, 2007).....	40
Figura 2 – Aparência externa da instalação nuclear experimental (RPAS, 2007).....	41
Figura 3 – Diagrama esquemático do SRE (TAKESHI, 2004a).....	47
Figura 4 – Diagrama resumido da seqüência de atuação dos equipamentos do SRE, durante um APRPGR (obtido de TAKESHI, 2004a).....	55
Figura 5 – Diagrama de blocos da injeção de emergência, através do tanque de compensação	59
Figura 6 – Diagrama de blocos da injeção de emergência, através do acumulador .	60
Figura 7 – Diagrama de blocos da injeção de emergência, através do tanque de inundação	61
Figura 8 – Diagrama de blocos da linha de equalização de pressão (injeção por gravidade).....	62
Figura 9 – Diagrama de blocos do Subsistema de Remoção de Calor Residual (SRCR).....	63
Figura 10 – Gráfico da pressão no pressurizador em função do tempo, a partir de um APRPGR no instante 100s (TAKESHI, 2004a)	81
Figura 11 – Gráfico da temperatura do refrigerante no reator em função do tempo, a partir de um APRPGR no instante 100s (TAKESHI, 2004a).....	82

LISTA DE ABREVIATURAS E/OU SIGLAS

AE	Árvore de Eventos
AF	Árvore de Falhas
AIEA	Agência Internacional de Energia Atômica
ALARP	<i>“As low as reasonable practicable”</i>
AMFE	Análise de Modos de Falha e Efeitos
AMECF	Análise de Modos, Efeitos e Criticidade de Falhas
APR	Anexo do Prédio do Reator
APRP	Acidente de Perda de Refrigerante do Primário
APRPGR	Acidente de Perda de Refrigerante do Primário por Grande Ruptura
APT	Anexo do Prédio das Turbinas
ASES	Área do Sistema de Evaporação do Sítio
BIAP	Bomba de Injeção à Alta Pressão
BIBP	Bomba de Injeção à Baixa Pressão
BSI	<i>“British Standards Institution”</i>
CCPS	<i>“Center for Chemical Process Safety”</i>
CE	Chaminé de Exaustão
CHS	<i>“Coarse Hazard Studies”</i>
CIA	<i>“Central Intelligence Agency”</i>
CNPq	Conselho Nacional de Pesquisa
CTMSP	Centro Tecnológico da Marinha em São Paulo
ECS	<i>“Emergency Cooling System”</i>
ET	Evento Topo
FMEA	<i>“Failure Modes and Effects Analysis”</i>
FMECA	<i>“Failure Modes, Effects and Criticality Analysis”</i>
HAZOP	<i>“Hazard and Operability Study”</i>
HSE	<i>“Health and Safety Executive”</i>
ICI	<i>“Imperial Chemical Industries”</i>
IEA	Infra-estrutura de Apoio
INB	Indústrias Nucleares do Brasil
INE	Instalação Nuclear Experimental
IPEN	Instituto de Pesquisas Energéticas e Nucleares

LOCA	<i>“Loss of Coolant Accident”</i>
MME	Ministério de Minas e Energia
NPSH	<i>“Net Positive Suction Head”</i>
OESP	“O Estado de São Paulo”
PA	Prédio de Apoio Administrativo
PAC	Prédio Auxiliar Controlado
PAIR	Prédio de Armazenamento Intermediário de Rejeitos
PANC	Prédio Auxiliar Não Controlado
PC	Prédio do Combustível
PCAL	Prédio das Caldeiras
PHA	<i>“Preliminary Hazard Analysis”</i>
PO	Prédio de Apoio Operacional
PPTE	Prédio de Preparação e Teste de Embalagens
PR	Prédio do Reator
PROTER	Protótipo em Terra
PT	Prédio das Turbinas
PWR	<i>“Pressurized Water Reactor”</i>
RPAS	Relatório Preliminar de Análise de Segurança
RSSG	<i>“Royal Society Study Group”</i>
SAB	Subsistema de Água Borada
SARSP	Sistema de Água de Resfriamento de Segurança da Planta
SCRAM	Desligamento emergencial de um reator nuclear
SIE	Subsistema de Injeção de Emergência
SIR	Sistema de Injeção de Refrigerante
SIS	Sinal de Injeção de Segurança
SPP	Sistema de Proteção da Planta
SRCR	Subsistema de Remoção de Calor Residual
SRE	Sistema de Resfriamento de Emergência
SRR	Sistema de Resfriamento do Reator
SUB1	Prédio da Cabine Primária
SUB2	Prédio de Emergência
TDE	Tanque do Diesel de Emergência
TFD	Tanque do Freio Dinamométrico
TR	Torre de Resfriamento

TS	Tanque SARSP
UR	Unidade de Resfriamento do PROTER
USP	Universidade de São Paulo

1 INTRODUÇÃO

A recente escalada dos preços do petróleo, com valorização de mais de 1.000% em nove anos, leva os analistas a acreditar que tenha ocorrido o terceiro choque desta “commodity”, no ano passado (OESP e ISTO É, 2008).

Ao contrário do ocorrido nos dois choques anteriores, quando houve basicamente um problema de restrição da oferta por motivos políticos, desta feita a crise se deveu a um desequilíbrio provocado pelos dois parâmetros da curva oferta e demanda.

Enquanto a procura pelo produto vinha crescendo significativamente ao longo dos últimos anos (até a eclosão da crise econômica atual), impulsionada em sua maior parte pelos países em desenvolvimento; a capacidade de produção tinha atingido valores muito próximos ao seu limite, conforme demonstram LAHERRERE (1997), IVANHOE (1997) e DUNCAN e YOUNGQUIST (1998).

Com os preços naqueles patamares, a tendência era (e, com o fim da crise, deve voltar a ser) de restringir o uso deste recurso a suas aplicações mais nobres, como a química fina e a produção de polímeros, procurando-se alternativas a sua utilização como combustível, inclusive como forma de minimizar seus efeitos em relação às emissões de CO₂ e, por conseguinte, ao aquecimento global (ECOBIDGE, 2008).

Como consequência direta desses fatores, tem-se notado uma aceleração na busca por novas fontes de energia, capazes de substituir os combustíveis fósseis, diminuindo a dependência mundial em relação aos mesmos (já que suas participações na matriz energética chegam a 55,7%, segundo o MME (dados referentes ao ano de 2005)).

Há várias fontes de energias alternativas que estão sendo exploradas com esta finalidade. No Brasil o etanol parece ter tomado a frente nessas iniciativas, superando inclusive a participação da geração hidro-elétrica (MME, dados referentes ao ano de 2007).

Contudo, é importante salientar que deve haver uma maior diversificação da matriz energética brasileira, buscando-se um maior equilíbrio entre as diversas opções, de forma a que não seja simplesmente transferida a dependência de uma modalidade de energia para outra, para que problemas devidos, por exemplo, a grandes períodos de estiagem ou quebra de safra possam ser minimizados.

Dentre as opções que se apresentam, a opção pela energia nuclear é particularmente interessante no caso brasileiro porque, além de não emitir gases causadores do efeito estufa e aquecimento global, apresenta vantagens competitivas em relação às demais, uma vez que o país possui a 6ª maior reserva de Urânio do mundo, com apenas 25% do seu território prospectado (INB, dados referentes ao ano de 2001); e domina as tecnologias de fabricação do combustível nuclear e de construção de reatores de pequeno e médio porte.

As grandes preocupações em relação a esta tecnologia resumem-se basicamente quanto à questão do rejeito radioativo e da segurança. Com relação à primeira, pode-se afirmar que, ao contrário do que acontece com os combustíveis fósseis, os produtos de fissão são armazenados em locais isolados e seguros e apresentam volume bastante reduzido. Já no caso dos hidrocarbonetos, por exemplo, os resíduos são de grande volume e, muitas vezes, liberados diretamente na atmosfera.

A segunda questão é um pouco mais delicada, tendo-se em vista que, segundo FROSDICK (1997), o ser humano por natureza tende a temer aquilo que julga não ter controle, ou que não lhe seja familiar ou ainda que possa afetar negativamente um grande número de pessoas de uma única vez.

A tecnologia nuclear, por ser relativamente nova e em virtude do seu grande potencial de geração energética, encaixa-se em todos os fatores mencionados acima, sendo motivo de grande apreensão por parte de um número não desprezível de pessoas.

Para minimizar esses temores as regulamentações são extremamente exigentes e cerca de 90% dos custos de implementação desta tecnologia são relacionados à segurança (KUMAMOTO, 1996).

Neste contexto, durante o projeto de centrais nucleares, aplicam-se várias técnicas de identificação de perigos e de análise de risco, a fim de se identificar os diversos eventos iniciadores de acidentes e verificar suas possíveis conseqüências. Dentre essas técnicas, há a Análise de Modos de Falha e Efeitos (AMFE), cuja aplicação é consagrada pela sua utilização em diversos campos da indústria como a aeronáutica, a automobilística e a nuclear.

O objetivo desta dissertação é aplicar essa técnica de análise de risco ao Sistema de Resfriamento de Emergência (SRE) de uma instalação nuclear experimental de modo a verificar os possíveis modos de falha de seus componentes e propor sugestões de melhoria, a fim de maximizar sua confiabilidade.

A escolha desse sistema deve-se basicamente ao fato de ser ele o principal responsável pela mitigação de um dos piores acidentes passíveis de ocorrência em uma planta nuclear e, juntamente com a escolha da técnica de análise, será justificada ao longo deste trabalho.

Segundo HYMAN (1998), o processo decisório é uma escolha entre alternativas. Sendo assim, a eliminação precipitada ou sem critério de uma fonte de energia pode prejudicar a tomada de decisão.

Através do uso correto de ferramentas de análise de risco pode-se, com o auxílio de critérios lógicos, minimizar a componente subjetiva da percepção de perigo do ser humano e dessa maneira evitar o descarte prematuro de uma opção técnica e economicamente viável, como a energia nuclear.

A seqüência a ser seguida neste texto é a seguinte: no capítulo 2, será feita a revisão da literatura e explicitada a técnica a ser utilizada, no capítulo 3, serão descritos a instalação nuclear experimental e o sistema a ser analisado, no capítulo 4, serão mostrados e analisados os resultados obtidos e no capítulo 5, serão apresentadas as conclusões e recomendações.

2 REVISÃO DA LITERATURA E ESCOLHA DA TÉCNICA

2.1 O CONCEITO DE RISCO

Antes de apresentar a definição de risco é necessário conceituar o termo perigo. MACDONALD (2004) afirma que este vocábulo pode ser entendido como uma propriedade física ou química, inerente a um elemento, que tem potencial para causar danos às pessoas, propriedades ou ao ambiente. Em outras palavras, é uma condição necessária para ocorrência de um acidente.

Os perigos podem ser classificados em:

- perigos naturais, tais como enchentes, terremotos, furacões, etc.;
- perigos tecnológicos, por exemplo: plantas industriais, estruturas civis ou mecânicas, sistemas de transporte, medicamentos, pesticidas, e outros;
- perigos sociais, como guerras, assaltos, terrorismo, sabotagem, etc.

A idéia de risco, segundo DOUGLAS (1990), surgiu no século XVII, com os cálculos associados às apostas e referia-se a uma probabilidade combinada à magnitude de perdas ou ganhos.

No século XIX, os economistas introduziram novos conceitos nesta área. Todas as pessoas eram consideradas avessas ao risco, sendo assim os empreendedores precisariam de incentivos para aceitar os desafios inerentes aos investimentos.

No campo das ciências exatas e da engenharia, apenas no século XX foi introduzida a mudança no conceito de risco, referindo-se apenas às conseqüências negativas de um dado evento (com ênfase nos perigos apresentados pelos avanços tecnológicos recentes nos setores de tecnologia nuclear, petroquímico e de “*offshore*”).

Conforme o “*ROYAL SOCIETY STUDY GROUP*” (RSSG, 1992), risco é a probabilidade que um certo evento adverso ocorra num determinado período de tempo, ou que resulte de uma ação ou projeto. De uma forma simplificada pode-se inferir o risco através de três perguntas: o que pode dar errado? (perigos); qual a probabilidade? (freqüência) e qual a conseqüência? (perdas).

De acordo com KUMAMOTO (1996) e a “*BRITISH STANDARD INSTITUTION*” (BSI, 1991a), risco é uma combinação de probabilidade (ou frequência) com que se prevê a ocorrência de um evento adverso definido e a magnitude das conseqüências desta ocorrência; sendo, por vezes, extremamente difícil medir estes efeitos (como quantificar a perda de uma vida humana, uma incapacitação profissional ou um dano ao meio ambiente?).

Praticamente toda atividade humana envolve risco, o ideal seria eliminá-lo por completo mas seria ingenuidade acreditar que isto seja possível. O que pode e deve ser feito é tomar medidas para reduzi-lo a um valor aceitável.

Segundo MUHLBAUER (2004), a sociedade (direta ou indiretamente) decide qual é o nível de risco aceitável para um determinado empreendimento. Este patamar varia conforme o ramo de atividade; o que é aceitável em relação, por exemplo, a acidentes de trânsito certamente não o será em relação a acidentes em plantas nucleares.

Muitas considerações de ordem sócio-econômica influenciam a tolerância das pessoas em relação ao risco (como será visto ainda neste item), por este motivo, muitas vezes, o risco aceitável para um dado empreendimento é definido pela entidade reguladora de classe.

Algumas características do risco são:

- traduz-se, necessariamente, por uma expectativa de perda;
- é sempre um elemento de incerteza;
- refere-se única e exclusivamente ao futuro.

E pode ser classificado em:

a) Negligenciável – quando a ocorrência do evento é muito improvável e suas conseqüências desprezíveis. Nenhuma ação é requerida para este nível de risco além de revisões periódicas;

b) Baixo – os riscos são considerados administráveis através de medidas de mitigação apropriadas, que são tomadas para manter o risco neste patamar;

c) Intermediário – quando os riscos são maiores que o desejado e ações devem ser tomadas para reduzi-lo a um nível tão baixo quanto o economicamente praticável (“*as low as reasonably practicable*” - ALARP);

d) Alto – os riscos são considerados inaceitáveis e devem ser substancialmente reduzidos para níveis seguros ou o projeto deve ser descartado.

FISCHHOFF ET AL. (1981) afirmam que o risco nunca é aceito incondicionalmente. Ele só é aceito caso traga algum benefício que o compense. Em outras palavras, é a decisão por uma alternativa, envolvendo risco, que é aceitável e não o risco por si só.

Neste ponto, é preciso fazer distinção entre risco individual e coletivo, em virtude das diferentes maneiras como são percebidos. O primeiro é definido pela “*HEALTH AND SAFETY EXECUTIVE*” (HSE, 1988) como sendo o risco específico para um indivíduo, seja ele trabalhador ou membro do público. Em outras palavras, alguém que resida dentro de uma área delimitada, a uma certa distância da instalação, ou que siga um determinado padrão de comportamento.

O segundo representa o risco para a sociedade como um todo e foi definido como a chance de ocorrer um grande acidente, causando um número de mortes pré-determinado.

Como WARNER (1992) salienta, os cientistas e os engenheiros utilizam estas definições porque elas fornecem a base com a qual eles podem desempenhar seu trabalho.

Estes conceitos de risco não são compartilhados pelos cientistas sociais, para os quais há sérias dificuldades em enxergar o risco como um conceito unidimensional, quando um determinado risco significa coisas diferentes para pessoas diferentes em contextos diferentes.

Uma das críticas às técnicas de análise de risco é que elas baseiam-se na experiência anterior para identificação dos riscos e esta dependência gera pelo menos três pontos fracos nessas técnicas:

- o primeiro, como acentua TOFT (1992) é que, em muitas ocasiões, as organizações responsáveis têm falhado em transformar o conhecimento passivo, de acidentes ocorridos, em conhecimento ativo, necessário a prevenir repetições com conseqüências potencialmente desastrosas;

- outra questão a ser mencionada é que quando se transforma a experiência adquirida com estes eventos em conhecimento ativo geralmente isto acontece apenas naquele ramo de atividade ou, na grande maioria dos casos, ficando restrito apenas à indústria onde ocorreu o acidente. De acordo com TURNER (1978), muitos desastres e acidentes de grandes proporções apresentam aspectos e características similares;

- por fim, as experiências passadas, obviamente, não podem prever os riscos associados a novas tecnologias. KASPERSON E KASPERSON (1991) discutem potenciais perigos da chuva ácida e do aquecimento global para a humanidade, uma vez que esses problemas apareceram como conseqüências indesejadas da atividade humana nos últimos anos. Segundo DOUGLAS E WILDAVSKY (1982), devem existir perigos substanciais à vida humana, que ainda não são conhecidos.

Outra questão de debate em relação a essas técnicas diz respeito à influência cultural. WILDAVSKY E DAKE (1990) afirmam que as influências culturais são as melhores maneiras de prever a percepção de risco de um grupo ou uma sociedade porque os indivíduos escolhem o que temer (e como temer), a fim de viabilizar seu modo de vida.

Uma vez que as influências culturais compõem-se de elementos subjetivos, torna-se muito difícil sua incorporação nas técnicas “objetivas” de análise de risco.

O analista pode ser acometido de uma “cegueira ao risco” porque suas influências culturais impedem-no de identificá-lo, simplesmente porque ele não o enxerga ou o considera aceitável. Este fato é bem ilustrado em KASPERSON E KASPERSON (1991) que concluem que alguns riscos estão escondidos porque estão enfronhados em uma teia de valores que enfatiza os benefícios e minimiza as conseqüências. Outros riscos, que afetam grupos minoritários, passam despercebidos por aqueles que detêm o poder.

Mas a “cegueira ao risco” pode não ser fruto apenas da influência cultural, o excesso de estímulos também pode provocá-la. TOFT (1993), discutindo a hipótese de Easterbrook, demonstra como um indivíduo fica mais estimulado à medida que aumenta o número de informações a que ele é exposto.

Ao atingir o ponto máximo de estímulo, o nível ótimo de informação também é atingido. A partir deste ponto, o indivíduo apresentará excesso de estímulos e começará a rejeitar informações adicionais.

Outros fatores que influenciam a percepção de risco são: a experiência pessoal, a memória de situações já ocorridas, a familiaridade com o problema, a voluntariedade ou imposição do risco por terceiros, a sensação de exercer o controle sobre ele e/ou se o mesmo deve-se a causas naturais ou provocadas pelo homem.

Devido a esta complexidade, mesmo entre as ciências comportamentais não há um consenso sobre o conceito de risco. Os psicólogos, como SLOVIC (1991), acreditam que o risco seja uma percepção individual influenciada por fatores como familiaridade e medo. Já os antropólogos, representados por WARNER (1993) afirmam que o risco é um perigo ou uma ameaça cuja percepção dependerá da cultura dominante, que pode ser dividida em quatro grupos: hierarquistas, igualitários, fatalistas e individualistas. Essa discussão não faz parte do escopo deste trabalho.

Recentemente, no contexto de uma cultura globalizada mais individualista, o conceito de risco está sendo transformado em uma obrigação contábil, um recurso forense ou uma ferramenta do sistema jurídico.

Segundo FROSDICK (1997), a redução da influência da igreja nessa cultura tem papel decisivo nessa mudança de comportamento. Quando a sociedade era mais hierárquica, cometer um pecado ou quebrar certos tabus significava que o indivíduo estava fora de sincronia com a sociedade. Na cultura atual, estar em situação de risco significa que a sociedade está fora de sincronia com o indivíduo, cujos direitos necessitam de proteção.

A pressão política atualmente não é mais explicitamente contrária a que as pessoas aceitem riscos para si próprias mas sim, no sentido de não expor outros indivíduos ao risco. PRIEST (1990) observa que a principal função da lei civil moderna é controlar o risco. FAIRLIE (1989) vai além, dizendo que as pessoas deveriam ser protegidas não somente da negligência mas também da falta de sorte.

Um último fator a ser mencionado é a comunicação do risco ao público. HOOD ET AL. (2001) asseveram que a confiança das gerações passadas na habilidade da ciência em prover respostas às questões transformou-se em desconfiança, em parte devido à ausência de consenso entre os cientistas em determinados assuntos; também porque as respostas que a ciência fornece atualmente são muito mais complexas e contingentes e por fim, porque “eles” estão sempre mudando de opinião.

As divergências entre os especialistas podem causar confusão na mente das pessoas quanto à validade da análise de risco (COVELLO, 1984), como também uma certa desconfiança em relação ao próprio analista (MORGAN e HENRION, 1990).

A confiança pode ser facilmente perdida mas é dificilmente recuperada e, em certas situações, irrecuperável. Portanto é imprescindível que haja transparência e sinceridade no processo de comunicação do risco, por pior que seja o teor da informação.

Segundo STARR (1984), a confiança do público repousa mais na capacidade das autoridades em lidar com o risco do que a esperança de que este possa ser eliminado por completo.

Assim pode-se concluir que as limitações do processo de análise de risco, a complexa natureza do conceito de risco e a importância e a dificuldade em se manter a confiança na comunicação entre as partes apontam para uma abordagem mais democrática do processo decisório, através da participação do público no processo de análise de risco e de tomada de decisão. Esta nova concepção proporciona um aumento da relevância e da qualidade da análise técnica, legitimando e tornando mais aceitáveis para o público as decisões resultantes (SLOVIC, 1999).

2.2 AS PRINCIPAIS TÉCNICAS DE IDENTIFICAÇÃO DE PERIGOS

A identificação de áreas de vulnerabilidade e de perigos específicos é de fundamental importância para a prevenção de acidentes. Uma vez identificados grande parte do problema foi equacionada, entretanto esta tarefa não é trivial; geralmente, quanto maior a tecnologia envolvida mais complexo se torna o processo.

Segundo LEES (1996), a prevenção de acidentes tende a depender, cada vez mais, do sistema de gerenciamento e nem sempre é uma tarefa simples descobrir pontos fracos neste sistema. Os perigos físicos também, na maior parte das vezes, não estão evidentes de forma que possam ser identificados através de uma simples inspeção visual. Por outro lado, há à disposição, atualmente, uma ampla gama de métodos de identificação de perigos que podem ser utilizados para resolver este problema.

Diferentes métodos são indicados para as diversas fases do projeto (embora existam casos onde uma mesma técnica pode ser aplicada a mais de uma fase) e não há um procedimento único, ou ideal, para o processo de identificação de perigos.

Assim como sistema mais apropriado para uma indústria depende da tecnologia disponível, do seu ramo de atividades e dos processos que executa, a escolha da técnica de identificação de perigos também depende do objetivo para o qual é realizado o estudo.

A experiência anterior é sempre desejável e a obediência às normas e procedimentos certamente contribui para evitar perigos que poderiam passar despercebidos para a grande maioria das pessoas mas é preciso estar atento ao fato de que a maioria das situações, nas quais serão empregadas as técnicas de identificação de perigos, apresentam algum aspecto inovador.

a) “*Checklist*”

É um dos instrumentos mais úteis no processo de identificação de perigos. Como uma norma ou regra de conduta, o “*checklist*” é uma garantia de que um determinado procedimento, que mostrou-se o mais adequado para aquela prática até o momento, está sendo seguido.

Sem o aproveitamento efetivo das experiências adquiridas anteriormente torna-se impossível enfrentar os desafios inerentes ao controle do risco e o “*checklist*” é uma das principais ferramentas existentes para se garantir isso.

Os “*checklists*” são aplicáveis aos sistemas de gerenciamento em geral e em um projeto, durante todas as suas fases. Há um grande número de exemplos de “*checklists*” na literatura, na verdade é muito provável encontrá-los em qualquer trabalho prático de engenharia.

O seu uso apropriado é discutido por MILLER e HOWARD (1971), que afirmam que esta técnica deveria ser utilizada com um único propósito: o de efetuar uma última verificação, de forma a garantir que nenhuma ação ou tarefa foi esquecida ou negligenciada.

Ele também se torna mais eficaz se as perguntas nele contidas não puderem ser respondidas através de um simples “SIM” ou “NÃO” mas se exigirem algum tipo de exercício mental na formulação da resposta.

Alguns exemplos de utilização de “*checklists*” são: “*DOW CHEMICAL CO.*” (1994), na área de propriedades físicas e químicas; SCOTT e CRAWLEY (1992), no comissionamento de plantas e HSE (1989) em falhas humanas.

Obviamente os “*checklists*” são eficazes desde que sejam utilizados. Há uma forte tendência a deixá-los sobre as prateleiras acumulando poeira, esta talvez seja uma das razões que impulsionaram o desenvolvimento de outras técnicas de análise de risco.

b) “*What if?*”

É uma técnica preliminar de identificação de perigos, que consiste na revisão de todo o projeto através de uma série de perguntas iniciadas com a expressão “O que aconteceria se” (embora as questões colocadas não necessariamente iniciem-se com esta expressão).

A metodologia é executada por uma equipe de especialistas, freqüentemente com o auxílio de um “*checklist*”, e provavelmente seja, depois deste último, o mais antigo método de identificação de perigos.

BURK (1992) fornece um exemplo de aplicação da técnica, assim como KAVIANIAN, RAO e BROWN (1992), na análise de um planta de polietileno de baixa densidade.

c) “*Preliminary Hazard Analysis*” (PHA)

É um termo normalmente usado para descrever uma técnica qualitativa de identificação de perigos a ser empregada na etapa inicial do projeto.

Como a identificação de perigos é de fundamental importância, muitas empresas desenvolveram algum tipo de técnica para esta finalidade, algumas das quais batizadas de PHA, o que fez com que o termo original perdesse um pouco do seu significado.

Segundo o “CCPS GUIDELINES” (1992) o PHA deve ser utilizado apenas no estágio preliminar do desenvolvimento da planta, nos casos em que a experiência passada auxilie a encontrar perigos potenciais.

O primeiro passo no PHA é a identificação de componentes ou elementos perigosos existentes no sistema. Este processo é facilitado pela experiência do analista, pelo exercício de julgamento de engenharia e pelo uso de “*checklists*” que têm sido desenvolvidos ao longo dos anos para auxiliar nesta técnica.

O segundo passo é a identificação dos eventos que podem transformar condições específicas de perigo em potenciais acidentes. A partir daí, a gravidade destes potenciais acidentes é avaliada para determinar se há necessidade de medidas corretivas.

Um formato simplificado de PHA é:

- componente/subsistema e modos de perigo;
- efeitos possíveis;
- compensação e controle;
- observações.

As informações necessárias para o estudo são: o critério de projeto, as especificações de material, de equipamentos, etc.. Os itens a serem examinados para a identificação de perigos são:

- matérias-primas, produtos intermediários e finais;
- equipamentos da planta;
- plantas auxiliares;
- equipamentos de segurança;
- interfaces entre os componentes do sistema;
- local de operação;
- operação (manutenção, testes, etc.).

d) “*Coarse Hazard Studies*” (CHS)

Outro método de identificação de perigos que deve ser utilizado preferencialmente na fase inicial do projeto é o “*Coarse Hazard Studies*” (CHS) ou “*checklist*” criativo, que é conduzido através de um exercício em equipe.

É uma técnica desenvolvida para ser utilizada como preparação para o “*Hazard and Operability Study*” (HAZOP). Foi descrita pela primeira vez no “*CIA HAZOP Study Guide*”, sendo posteriormente aprimorada no “*Chemetics Hazard Study Manual*” e pode ser considerada também como uma alternativa ao PHA.

Deve ser realizada na fase inicial de projeto, quando for conhecida a localização dos componentes da planta. O objetivo é determinar se há problemas em áreas como “*layout*” e localização da planta, características do processo ou informação sobre os perigos.

Há um grande número de vantagens a serem obtidas com a execução deste estudo antes do HAZOP. Ele auxilia na identificação daqueles perigos e outros problemas que são básicos e que podem, em princípio, ser detectados neste estágio. O CHS revela deficiências nas informações do projeto e expõe perigos devido à interação entre a planta e o meio ambiente ou entre ela e outras plantas, nas quais o estudo de HAZOP não é tão eficaz. Estas características contribuem para remover potenciais atrasos no caminho crítico do projeto.

A condução deste tipo de metodologia envolve a combinação de duas listas: uma de um banco de dados de perigos e outra de perigos potenciais e outros fatores preocupantes.

O estudo contempla então, de modo distinto do HAZOP, as duas características essenciais do projeto:

- materiais;
- equipamentos e atividades.

O CHS é um trabalho em equipe, liderado por um especialista. Os documentos necessários para este trabalho são: “*layout*” da planta, mapa do local e das vizinhanças.

Para sua aplicação emprega uma lista de palavras-chave tais como: fogo, explosão, toxicidade, corrosão, cheiro, efluentes, etc.. Outras palavras-chave podem ser geradas considerando-se:

- energia;
- interações;
- ambiente.

Cada um destes tópicos pode ser ainda desmembrado. A energia pode ser classificada segundo suas formas conhecidas: cinética, potencial, térmica, etc..

Para as interações o manual fornece: pessoas, materiais e equipamentos. Para ambiente: clima, geotérmico/geotécnico e biológico. A categoria geotérmica/geotécnica pode ser subdividida ainda nos principais perigos naturais como terremotos e maremotos e a categoria biológica, nos seres vivos, como pássaros e insetos.

O estudo resulta em um conjunto de tarefas destinadas a mitigar as questões levantadas.

e) “*Hazard and Operability Studies*” (HAZOP)

Um método muito usado atualmente para identificação de perigos na etapa de (ou próximo da) confecção do fluxograma de processo é o HAZOP. Esta técnica é executada através de um trabalho em equipe que envolve o exame da finalidade do projeto à luz de palavras-chave.

A técnica foi empregada pela primeira vez nos anos 60 na “*Imperial Chemical Industries*” (ICI) mas como muitas outras ferramentas de identificação de risco há mais de uma fonte responsável pelo seu desenvolvimento como KLETZ (1986) e KNOWLTON (1992), através do “*Chemetics Manual*” e tem sido objeto de numerosas variações até hoje.

O estudo é conduzido analisando-se o processo, a fim de descobrir perigos potenciais e problemas operacionais, utilizando uma abordagem direcionada por palavras-chave.

Em princípio, a metodologia pode ser aplicada quando estiverem disponíveis o “*layout*” da planta, o fluxograma de processo, o conjunto de palavras-chave e outras informações que revelem os objetivos do projeto.

O conceito básico do HAZOP é, a partir de uma descrição completa do processo, questionar todos os detalhes do mesmo para descobrir que desvios da concepção original podem ocorrer e quais as causas e as consequências destes possíveis desvios.

As características mais importantes para o estudo são:

- objetivo do projeto;
- desvios do objetivo;
- causas dos desvios;
- consequências (perigos, dificuldades operacionais, etc.).

O objetivo do projeto é examinado com respeito aos itens a seguir:

- material;
- atividade;
- equipamentos;
- origem;
- destino.

Em algumas situações, outros itens relevantes são:

- tempo;
- espaço.

Para cada um dos itens listados acima é aplicado um conjunto de palavras-chave de modo a identificar possíveis desvios no processo. As palavras-chave mais comumente utilizadas e seus respectivos significados são:

NÃO	Negativa de intenção
MAIS	Aumento quantitativo
MENOS	Diminuição quantitativa
TANTO QUANTO	Aumento qualitativo
PARTE DE	Diminuição qualitativa
REVERSO	Lógica oposta da intenção
OUTRO	Substituição completa

Quase sempre é possível aplicar todas as palavras-chave de maneira lógica às atividades e, com a possível exceção de “REVERSO”, às substâncias.

Na aplicação das palavras-chave ao tempo, os seguintes aspectos podem ser relevantes: duração, frequência, tempo absoluto e seqüência. As palavras-chave “MAIS” e “MENOS” são aplicáveis à duração ou frequência, enquanto as palavras-chave “MAIS CEDO” e “MAIS TARDE” podem ser mais aplicáveis que “OUTRO” para tempo absoluto ou seqüência.

De modo similar, na aplicação de palavras-chave a espaço ou lugar os seguintes aspectos podem ser relevantes: posição, origem e destino. As palavras-chave “MAIS ALTO” ou “MAIS BAIXO” podem ser mais aplicáveis que “MAIS” ou “MENOS” para elevação, enquanto a palavra-chave “ONDE MAIS” pode ser mais aplicável que “OUTRO” para posição, origem ou destino.

Algumas palavras-chave adicionais são: “INICIANDO”, “PARANDO”, “CONTROLANDO”, “ISOLAMENTO”, “INGRESSO”, “ESCAPE” e “DESCONTAMINAÇÃO”.

Os estágios para condução de um HAZOP são os seguintes:

- definição dos objetivos;
- escolha da equipe;
- preparação;
- condução;
- acompanhamento;
- registro.

Em geral, os objetivos de um estudo de HAZOP, como originalmente definido, são checar o projeto e os procedimentos operacionais, de modo a identificar perigos e problemas operacionais, além de possíveis danos ao meio ambiente.

Associados a isto, deve haver verificações em:

- informações ainda faltantes;
- alguns equipamentos que mereçam atenção especial;
- informações de fornecedores;
- fases de operação da planta;
- procedimentos de manutenção;
- entes a serem protegidos (trabalhadores da unidade, outras pessoas que estejam no sítio, o público em geral, a planta e o meio ambiente).

O HAZOP é conduzido por uma equipe multidisciplinar, que deve conter os responsáveis pelo projeto e pela operação, que possam responder pelas áreas mais relevantes e que possuam experiência e autonomia suficientes para tomar decisões importantes em tempo hábil.

É, também, fundamental que tenham disponibilidade para o projeto, fazendo-se presentes a todos os compromissos dele decorrentes. Por fim, é recomendável que a equipe seja formada por um número não muito grande de pessoas.

Uma boa dose de preparação é requerida antes do início do HAZOP, incluindo decisão do tipo de estudo desejado, a obtenção, validação e tratamento dos dados, o planejamento da seqüência de estudos e a organização do calendário de reuniões.

Há uma série de fatores importantes para o sucesso do estudo:

- o objetivo deve ser muito bem definido;
- o líder da equipe deve ter experiência na técnica de HAZOP (não necessariamente no processo específico);
- o papel do líder é fundamental e ele deve receber treinamento adequado para desempenho das suas funções;
- os preparativos para o processo devem ser feitos criteriosamente de modo a assegurar que todos os documentos necessários estejam atualizados, precisos e à disposição no momento adequado.

O estudo utiliza uma abordagem formal, até mesmo mecânica, e as questões levantadas podem, em certos casos, parecer triviais ou mesmo irrealistas. Deve-se salientar, entretanto, que a abordagem é concebida como um auxílio à criatividade da equipe em visualizar desvios, bem como suas causas e conseqüências. A eficácia da técnica depende sobretudo da forma com que é encarada, não só pela equipe envolvida no estudo como também pelos altos escalões da empresa.

O momento ideal para se aplicar a técnica HAZOP é uma decisão importante. As desvantagens de um estudo prematuro são que as informações necessárias para sua eficácia podem, ainda, não estar disponíveis e há um risco maior de mudanças de projeto, visando melhorias na sua operacionalidade e/ou segurança, no decorrer do estudo. As vantagens são as facilidades de incorporar ao projeto quaisquer mudanças provenientes do estudo, em particular, para alcançar uma concepção inerentemente mais segura.

Por outro lado, um estudo tardio apresenta as desvantagens de uma implementação mais cara e difícil das opções de melhoria. Além disso elas tendem a ser implementadas de forma conjunta, muitas vezes, sem o devido cuidado em verificar se há sobreposição ou interferência entre elas.

A equipe responsável pela condução do estudo de HAZOP é composta, normalmente por pessoas responsáveis pelo projeto, comissionamento e operação da instalação, apresentando especificidades entre empresas diferentes, e mesmo dentro de uma mesma companhia dependendo do tipo de projeto.

Uma equipe padrão é formada por um líder, um engenheiro de projeto, um engenheiro de processo, um instrumentista e o gerente de comissionamento. Outras pessoas que são freqüentemente incluídas, conforme a natureza do projeto, são: um químico, um engenheiro civil, um engenheiro elétrico, um técnico em materiais, um supervisor de operação, um representante do fornecedor, etc..

O “*Chemetics Manual*” discute o papel dos seguintes participantes do estudo: o líder, o secretário, os membros da equipe técnica e o coordenador de acompanhamento do processo. Mostra também as funções das várias partes envolvidas indiretamente com o estudo, tais como o cliente e os funcionários da empresa que tenham ligação com o estudo.

Os membros da equipe técnica são responsáveis em prover as respostas em relação aos desvios sugeridos pelas palavras-chave. Eles também devem ser capazes de responder as dúvidas de projeto surgidas no decorrer do processo e podem receber incumbências adicionais durante as reuniões (uma delas é a de coordenador de acompanhamento do processo).

A função do líder é a de atuar como facilitador, de modo a trazer a tona o conhecimento técnico da equipe, através de uma interação estruturada. Não é sua função identificar perigos e problemas operacionais mas sim assegurar que isto será feito pelos responsáveis.

O líder deve ser alguém não envolvido diretamente no projeto mas que possua as habilidades requeridas para exercer esta função. A eficácia de um estudo deste tipo depende muito da sua capacidade, por isso é imprescindível que os líderes sejam treinados e experimentados.

As responsabilidades do líder são: a definição do projeto, o agendamento e preparo das reuniões (como também a definição da freqüência e do momento apropriado para sua realização), a formação da equipe, assegurando que cada membro saiba exatamente o seu papel (recebendo treinamento adequado para desempenhá-lo, se necessário), a provisão das informações e da documentação necessárias a cada reunião, a condução e o registro das reuniões e o acompanhamento das questões surgidas nestes encontros.

No estágio final do estudo, o líder deve ainda assegurar que há uma boa relação com o cliente, de forma a que ele se comprometa com os resultados do estudo.

Durante a preparação o líder deve avaliar até que ponto a planta em questão é similar a alguma outra, já analisada, e de que maneira isto poderá afetar o estudo a ser conduzido. Em muitos casos o projeto não é inteiramente novo mas uma modificação de um outro já existente. Neste caso, o líder deverá verificar quais são as inovações (matérias-primas, equipamentos, materiais de construção, condições ambientais, etc.) e decidir o que poderá ser aproveitado do estudo já realizado, certificando-se da confiabilidade das informações.

A habilidade mais importante do líder deve ser na condução das reuniões. Um requisito fundamental é assegurar que o estudo não seja muito superficial nem extremamente detalhado (identificando todos os perigos mas em um intervalo de tempo inaceitável), outro é gerenciar as interações pessoais entre os membros da equipe, obtendo contribuições equilibradas e minimizando as influências individuais, quando o projeto é submetido à análise. Estes conceitos são facilmente percebidos mas constituem-se em habilidade significativa.

O HAZOP apresenta como resultado uma série de questões sobre o projeto, havendo a necessidade de um arranjo formal para assegurar que elas serão acompanhadas. Uma maneira de se fazer isto é garantir que em cada reunião todas as questões levantadas sejam direcionadas a um indivíduo específico para acompanhamento das mesmas e também para que ele designe o membro da equipe mais qualificado para responder cada uma das questões e fiscalize para que isso de fato aconteça.

O acompanhamento é uma das funções principais de programas de computador desenvolvidos para auxiliar o HAZOP e há um grande número de opções disponíveis para este fim. Estes programas não devem ser confundidos com códigos que fazem a identificação de perigos através da emulação de estudos de HAZOP.

A metodologia HAZOP é uma técnica efetiva para descobrir perigos potenciais e dificuldades operacionais na fase de projeto. Há evidências de redução de pelo menos uma ordem de magnitude no número de perigos e problemas encontrados na operação graças à aplicação desta técnica.

Por este motivo é largamente empregada nas indústrias de processo, em pequenas e grandes empresas como o primeiro, ou o principal método de identificação de perigos. Nas empresas em que é utilizado, os estudos de HAZOP tendem a se tornar uma parte considerável dos esforços de projeto.

Esta metodologia foi originalmente desenvolvida de modo a enfatizar os desvios nas variáveis de processo. Com o passar dos anos, sua aplicação foi estendida às atividades de manutenção e operação, que são fonte de muitos outros desvios.

Não é surpresa que o amplo uso desta técnica tenha levado também ao desenvolvimento de variantes locais e adaptações às necessidades específicas das companhias. A técnica de HAZOP também tem sido utilizada para analisar outras áreas como meio-ambiente, por exemplo. Em alguns casos, o mesmo estudo é utilizado para cobrir de um lado a segurança e operação e de outro, o ambiente.

Uma análise deste método foi feito por ROACH E LEES (1981), que registraram e avaliaram os entendimentos verbais de um HAZOP industrial. Além da escolha do item da planta e do desvio de parâmetro a ser analisado, as atividades relacionadas por eles foram:

- identificação de possíveis causas e conseqüências dos desvios iniciais;
- explicação das características do processo ou item da planta;
- estimativa dos aspectos quantitativos da dinâmica da planta, confiabilidade e disponibilidade do projeto, perigo e risco;
- checagem de características de projeto e operação e dos perigos potenciais e problemas operacionais, incluindo a detecção dos desvios/falhas e perigos potencialmente catastróficos, além dos procedimentos para iniciar, controlar e parar a operação da planta;
- especificação de qualquer ação a ser tomada.

A atividade de identificação de possíveis causas e conseqüências, através da aplicação de palavras-chave a um determinado parâmetro deve ser sistemática, explorando as possíveis conseqüências da falha.

A explicação das características do processo ou item da planta é uma atividade significativa. Geralmente em um projeto há itens que são ambíguos, que têm que ser modificados e cujas características podem não ter sido consideradas.

Estes itens podem necessitar de maiores explicações por várias razões:

- as informações podem estar documentadas mas pode ser mais conveniente obtê-las por explanação verbal;
- a informação é, ou deveria ser, parte do projeto mas não foi documentada até aquele instante;
- a informação foi gerada pela equipe de HAZOP durante o processo.

Outra atividade importante é a estimativa de aspectos quantitativos ou semi-quantitativos de dinâmica da planta, sua confiabilidade e disponibilidade, perigo e risco.

A atividade central é a checagem das características de projeto e operação, bem como dos perigos e problemas operacionais. É preciso transformar os eventos intermediários em falhas principais, de interesse para o estudo. Deve-se atentar também para as falhas ocultas e problemas de comunicação no projeto.

A ênfase dos estudos de HAZOP é na geração de desvios/falhas mas esta metodologia não é simplesmente uma ferramenta de identificação. Uma parte significativa da atividade em um HAZOP é relacionada à filtragem dos desvios identificados, de modo a evitar que os sistemas de projeto sejam inundados com informações irrelevantes. A contribuição de profissionais experientes é tão importante na filtragem quanto na geração.

A técnica HAZOP tem sido amplamente utilizada e é a parte mais importante do sistema de identificação de perigos em muitas empresas mas ela possui suas limitações.

Estas limitações são de dois tipos:

- a primeira advém das hipóteses concernentes ao método e é uma limitação de escopo. Na sua forma original, o método assume que o projeto foi conduzido de acordo com as normas apropriadas;
- a outra restrição é inerente ao método. O HAZOP não é indicado, por exemplo, para tratar com características espaciais associadas ao “*layout*” da planta e os seus efeitos resultantes.

Há um grande número de variantes do método original. Muitas (talvez a maior parte das) empresas adaptaram a técnica às suas próprias necessidades. Muitas destas adaptações ampliam a abrangência do método para condições anormais de operação ou outras atividades como manutenção, ou ainda para levar em conta outros fatores, tais como efeitos ambientais. Outro tipo de variante é a aplicação da técnica básica de HAZOP a sistemas que não tubulações e vasos de pressão. A este respeito deve ser lembrado que o HAZOP é a aplicação de uma metodologia de estudo e, freqüentemente, é melhor retornar às suas origens para depois dar um passo à frente ao invés de aplicá-lo diretamente a novos casos.

Alguns outros exemplos de aplicação da metodologia HAZOP são:

- modificações na planta;
- comissionamento da planta;
- manutenção;
- desligamento de emergência e sistemas de emergência;
- carregamento e descarregamento de reservatórios;
- construção e demolição;
- trânsito de produtos.

Muitas dessas aplicações são de interesse da indústria de processo.

É importante ressaltar que a execução do HAZOP (assim como qualquer outra técnica de identificação de perigos) não substitui um bom projeto. Há algo fundamentalmente errado se a aplicação do método revelar muitas falhas básicas de projeto.

“COMPUTER HAZOP”

O método HAZOP convencional foi desenvolvido para plantas nas quais o sistema de controle era baseado em mecanismos analógicos. Ele não é orientado para falhas associadas a sistemas de controle computadorizados. O *“COMPUTER HAZOP”* foi desenvolvido para potencializar a eficácia do HAZOP em relação a esta particularidade.

Uma preocupação inicial foi apontada por KLETZ (1982) expondo os erros e falhas humanos associados ao controle desses sistemas. A HSE também o identificou como um fator merecedor de atenção especial. Um resultado desse trabalho foi o *“HSE PES Guide”*, que trata da confiabilidade apenas do sistema computacional mas, conforme JONES (1991) salientou, o problema é ainda maior.

f) Análise de Modos de Falha e Efeitos (AMFE)

Outra técnica de identificação de perigos que é freqüentemente utilizada como alternativa ao HAZOP é a AMFE. Ela envolve a revisão dos sistemas para descobrir os modos de falha que podem ocorrer e seus possíveis efeitos. A análise é orientada para os equipamentos, ao invés de parâmetros de processo.

O “*BS 5760 Reliability of Systems, Equipment and Components, Part 5: 1991 Guide to Failure Modes, Effects and Criticality Analysis*” (BSI, 1991b) trata dos propósitos, princípios, procedimentos e aplicações da AMFE, suas limitações e sua relação com outros métodos de identificação de perigos.

A AMECF é uma complementação da AMFE, na qual é realizada uma análise de criticidade, que é uma função da severidade do efeito e da freqüência com a qual espera-se que ele ocorra. A análise de criticidade envolve a determinação das freqüências de ocorrência de cada modo de falha e a severidade de cada efeito desta mesma falha.

O propósito da AMFE é a identificação das falhas que conduzam a eventos indesejados na operação do sistema. Seus objetivos incluem:

- identificação de cada modo de falha, da seqüência de eventos a ele associados e seus possíveis efeitos;
- uma classificação de cada modo de falha de acordo com características relevantes, incluindo capacidade de detecção, diagnóstico e teste, possibilidade de substituição, compensação e provisões operacionais;
- a determinação da criticidade de cada modo de falha (no caso da AMECF).

Ainda segundo a BS 5760, a informação necessária para uma AMFE pode ser organizada nos seguintes tópicos:

- estrutura do sistema;
- partida, operação, controle e manutenção do sistema;
- ambiente onde se localiza o sistema;
- modelagem do sistema;
- software do sistema;
- fronteiras do sistema;
- estrutura funcional do sistema;

- representação da estrutura funcional do sistema;
- diagrama de blocos;
- relevância da falha e provisões para compensação.

A informação básica de cada um dos itens analisados é: nome, função, identificação, modos de falha, causas da falha, efeitos da falha no sistema, métodos de detecção de falha, provisões para compensação, severidade dos efeitos e comentários (como mostram as tabelas, constantes do item 4.2).

A documentação principal utilizada em uma AMFE é o fluxograma de engenharia, que possibilita a preparação do diagrama de blocos. A identificação dos modos de falha, e seus efeitos é precedida pela preparação de uma lista de modos de falha esperados, à luz da utilização do sistema, do elemento envolvido, do modo de operação, da especificação da operação, das restrições de carácter temporal e do meio-ambiente.

Os modos de falha podem ser classificados em dois níveis: genéricos e específicos.

Como exemplos de modos de falha genéricos, temos:

- falha durante a operação;
- falha em operar num determinado instante;
- falha em cessar a operação em determinado instante;
- iniciar a operação antes do previsto.

Dos específicos:

- trincado/quebrado;
- distorcido;
- sub-dimensionado; etc..

As causas de falha associadas a cada modo devem ser identificadas. A BS 5760 fornece um “*checklist*” de causas de falha potenciais, dividido nos seguintes itens: especificação, projeto, fabricação, instalação, operação, manutenção, ambiente e forças da natureza.

Os efeitos da falha envolvem mudanças na operação, função ou status do sistema e isto deve ser identificado na análise. Os efeitos da falha podem ser classificados em locais ou terminais. Efeitos locais referem-se às conseqüências no nível do elemento sob análise e os terminais àqueles ao nível mais alto do sistema.

Quando a AMFE deve ser aplicada a uma estrutura hierarquizada é preferível restringir-se a apenas dois níveis e executar a análise separadamente em cada um deles. Os efeitos da falha, identificados em um nível, podem ser usados como modos de falha no nível superior e assim por diante.

A AMFE é uma metodologia eficaz de análise de elementos que podem provocar a falha de todo, ou grande parte de, um sistema. Ela não é muito indicada quando uma lógica complexa é necessária para descrever a falha do sistema.

Uma técnica complementar a ela, de caráter dedutivo é a Árvore de Falhas, que é mais indicada nos casos em que a lógica da falha é mais complexa.

A AMFE pode ser um processo ineficiente e trabalhoso se não for corretamente aplicado e não deve ser incluído indiscriminadamente nas especificações. Sua amplitude de aplicação é muito vasta, variando desde um simples instrumento a uma instalação inteira.

Passos para execução de uma análise do tipo AMFE:

1º) Definir o sistema e seus requisitos funcionais e operacionais:

- incluir as funções primárias e secundárias, o desempenho esperado, as restrições do sistema e as condições explícitas que constituam uma falha. A definição do sistema deve incluir a definição de cada modo de operação, bem como a sua duração;

- apontar quaisquer fatores ambientais relevantes como temperatura, umidade, radiação, vibração e pressão durante o período de operação e na parada da instalação;

- considerar falhas que possam levar ao não cumprimento de requisitos mínimos exigidos pelas entidades reguladoras.

2º) Fazer o diagrama de blocos do sistema, de modo a mostrar as relações entre os elementos e eventuais interdependências. Diagramas separados podem ser necessários para cada modo de operação.

O diagrama de blocos deverá conter:

- uma divisão do sistema em seus principais subsistemas, incluindo relações funcionais;

- identificação apropriada do subsistema, assim como as suas entradas e saídas;

- quaisquer redundâncias, caminhos alternativos ou outras características de projeto que tornem o sistema mais seguro.

3º) Identificar os modos de falha, suas causas e seus efeitos:

- identificar as possíveis causas associadas a cada modo de falha postulado;

- identificar, avaliar e registrar as conseqüências para cada modo de falha, na operação do componente, considerando manutenção, pessoal e os objetivos do sistema, assim como qualquer efeito no nível superior.

4º) Identificar métodos de detecção de falha e isolamento e verificar se outros modos de falha forneceriam a mesma indicação (gerando a necessidade de separação dos métodos de detecção).

5º) Identificar características de projeto e provisões operacionais que previnam ou reduzam os efeitos do modo de falha. Isto pode incluir:

- itens redundantes que possibilitem a continuidade da operação se um ou mais componentes falharem;

- modos alternativos de operação;

- dispositivos de alarme ou monitoramento;

- quaisquer outros meios que possibilitem a operação efetiva ou que limitem os danos.

6º) Identificar combinações específicas de falhas múltiplas a serem consideradas, sabendo que quanto maior o número de falhas múltiplas consideradas mais complexa a análise se torna. Caso se opte pelo AMECF, a severidade dos efeitos da falha é categorizada, a probabilidade é determinada e o número de recursos redundantes de mitigação, necessários para manter a probabilidade de falha em níveis aceitáveis, é determinado.

7º) Revisar ou repetir a análise tipo AMFE toda vez que o projeto for modificado.

g) Árvore de Eventos (AE)

Segundo OLIVEIRA ET AL. (2000), a AE é um diagrama lógico que caracteriza a propagação de um evento iniciador de acidente em termos de falhas e/ou sucessos de funções ou sistemas, segundo uma determinada ordem lógica de prioridade (cronológica e/ou funcional), definindo as seqüências de acidentes. Ela começa com um evento inicial específico (como uma falta de energia ou ruptura de uma tubulação) e é desenvolvida de “baixo para cima” (técnica indutiva).

Ela pode ter uma abordagem qualitativa ou quantitativa. Qualitativamente é utilizada para identificar as saídas do evento inicial, quantitativamente para estimar as freqüências ou probabilidades de cada saída.

O evento inicial é geralmente colocado à esquerda e os ramos vão sendo construídos em direção à direita. Cada ramo representa uma diferente seqüência de eventos resultando em uma saída.

Os principais elementos da árvore são as definições dos eventos e os vértices lógicos. O evento inicial é usualmente expresso como uma freqüência (eventos/ano) e as subdivisões seqüentes como probabilidades e, portanto, a saída final é expressa também como freqüência (eventos/ano). Na construção de uma AE, a convenção normal é pelo uso de saídas binárias, ao invés de múltiplas saídas, assim a soma das probabilidades das saídas deve ser igual à unidade e a soma das freqüências das saídas deve igualar a do evento inicial.

Cada ramo da AE representa um cenário particular, a árvore é um meio de estimar a freqüência de saída para aquele cenário. Ela é usada juntamente com um conjunto de modeladores de perigo para determinar as conseqüências daquele cenário. Por exemplo, para um vazamento de material inflamável, uma série de modelos poderiam ser feitos para emissão, dispersão, ignição e explosão.

Em certos casos, uma AE pode ser reduzida a outra equivalente. Exemplos desta redução podem ser observados em SCHREIBER (1982).

h) Árvore de Falhas (AF)

É um diagrama lógico destinado a apresentar as causas de um dado evento indesejável, freqüentemente um perigo. A possibilidade de ocorrência deste evento, chamado Evento Topo (ET), deve ser prevista antes da construção da árvore, através da utilização de outro método de identificação de perigos.

A AF é, portanto, uma técnica dedutiva e de natureza qualitativa e quantitativa, sendo largamente utilizada na avaliação de perigos mas de grande valor também na sua identificação. Em muitos casos, basta identificar os caminhos críticos e os eventos iniciadores que podem ocasionar o ET, sendo desnecessária a quantificação da freqüência de ocorrência destes eventos.

A AF é normalmente utilizada em grandes sistemas, onde se requeira altíssima confiabilidade e onde o projeto deva incorporar várias barreiras de proteção, como ocorre nas plantas nucleares.

Em relação à estimativa da freqüência dos eventos, a primeira abordagem é ter como base as informações disponíveis em banco de dados e utilizar a AF somente onde essas informações não existam e o valor tenha que ser calculado.

O conceito original da AF foi desenvolvido pela “*Bell Telephone Laboratories*” no início dos anos 60, e em 1965 o interesse pelo método cresceu, por ocasião de um simpósio no qual colaboradores, dessa empresa e da “*Boeing Company*”, mostraram seus trabalhos com essa técnica (“*BOEING COMPANY*”, 1965).

Desenvolvimentos na metodologia aconteceram na essência do método, através de sua análise para descobrir os cortes mínimos para ocorrência do ET e na avaliação da freqüência ou probabilidade deste evento. O corte mínimo é um conjunto de eventos primários (básicos ou não desenvolvidos) que podem causar o ET, o conjunto completo dos cortes mínimos constitui o grupo de modos de falha principais, causadores do ET.

Houve também progressos relacionados ao método em algumas características. Um importante avanço a ser mencionado nessa área é a teoria cinética da árvore, que foi desenvolvida por VESELY (1969, 1970), permitindo a determinação de características tais como confiabilidade e disponibilidade de sistema ao longo do tempo.

Segundo FUSSEL (1976), os maiores benefícios auferidos com uma AF são:

- direcionar o analista a enxergar a falha de modo dedutivo;
- apontar os aspectos importantes do sistema em relação às falhas de interesse para o estudo;
- proporcionar auxílio gráfico, dando visibilidade aos gerenciadores do sistema;
- prover opções de análise qualitativa ou quantitativa da confiabilidade do sistema em questão;
- permitir ao analista concentrar-se em uma determinada falha do sistema por vez;
- propiciar ao analista uma visão privilegiada do comportamento do sistema.

Fussel também cita algumas dificuldades no trabalho com a AF. Por ser uma forma sofisticada de análise de confiabilidade ela requer tempo e esforço considerável da parte de analistas bem treinados e, embora ela seja uma das melhores ferramentas para se analisar o sistema como um todo, ela não garante, por si só, a detecção de todas as falhas, especialmente as que possuam uma causa comum.

Neste ponto é necessário fazer uma distinção entre erro e falha. Uma falha é um estado incorreto que pode ser provocado por problema em um componente ou induzido por influência externa, portanto é um conceito mais abrangente que erro. Todos os erros são falhas mas a recíproca nem sempre é verdadeira.

Um componente de uma árvore de falhas pode estar em um dos seguintes estados binários: operando corretamente ou em falha. Em outras palavras, para efeito da AF o espectro contínuo dos estados de um componente (que vai desde operacionalidade total até falha completa) foi reduzido a apenas dois estados. O estado do componente que constitui uma falha é essencialmente aquele que induz a falha que está sendo analisada.

Como uma árvore lógica, a AF é uma representação dos estados de um sistema que são consistentes com o ET, num determinado instante. Na prática, a AF é geralmente utilizada para representar um estado do sistema que tenha se desenvolvido num curto período de tempo. Isto é particularmente

importante para aplicação da álgebra Booleana, que necessita que os estados sejam contemporâneos para sua aplicação.

As falhas podem ser classificadas em: primárias, secundárias ou de comando. A falha primária é aquela que ocorre quando o componente está operando nas condições para as quais foi projetado. Uma falha é chamada secundária quando o componente está operando em condições para as quais não foi projetado. Uma falha de comando acontece quando o componente está operando nas condições para as quais foi projetado mas em momento ou local inadequados.

Alguns componentes são passivos, outros ativos. Itens como vasos e tubulações são passivos, enquanto válvulas e bombas são ativos. Um componente passivo é um transmissor ou recipiente no processo de propagação da falha e um ativo pode ser um iniciador. Em termos gerais, a taxa de falha de um componente passivo é comumente duas ou três ordens de magnitude menor que a de um componente ativo.

Há uma diferença entre a ocorrência de uma falha e a existência de uma falha. A atenção deve se concentrar na frequência com a qual (ou a probabilidade que) uma falha ocorra, isto é na não-confiabilidade, ou na probabilidade de que em dado momento o sistema esteja em estado de falha, isto é indisponível.

O caso mais simples é a determinação da confiabilidade de um sistema não reparável. Isto é, em algumas vezes, chamado de “missão”: o sistema é enviado para executar uma tarefa na qual os componentes que falham não são reparados. Os exemplos mais comuns são as missões espaciais mas há casos nas indústrias de processo que podem se aproximar disto, como estações remotas de bombeamento ou módulos submersíveis em alto mar. A disponibilidade de um sistema não-reparável também pode ser determinada mas a longo prazo, que é usualmente o dado de interesse, ela tende a zero.

Na maioria dos casos, entretanto, os sistemas de processo são reparáveis e para estes tanto a confiabilidade quanto a disponibilidade podem ser de interesse. Se a preocupação é centrada na frequência de ocorrência de um perigo, é a confiabilidade que é importante. Por outro lado, se a preocupação é com a percentagem de tempo gasta com a manutenção, o enfoque passa a ser na disponibilidade.

Uma AF deve ser analisada para se descobrir os cortes mínimos, ou seja a menor quantidade de eventos capazes de causar o ET.

Os elementos básicos de uma AF podem ser classificados em:

- evento topo (ET);
- eventos primários;
- eventos intermediários;
- portões lógicos.

Os símbolos mais utilizados em uma AF estão detalhados no “*BS 5760 Reliability of Systems, Equipment and Components, part 7: 1991 Guide - Fault Tree Analysis*” (BSI, 1991b).

O ET é, normalmente, algum evento indesejado como, por exemplo, vazamentos de materiais radioativos, tóxicos ou inflamáveis, fogo, explosão ou outros tipos de falha.

Eventos primários são aqueles que não apresentam desdobramentos.

Um tipo de evento primário é um evento básico, que é um evento que não requer desenvolvimento.

Outro tipo é um evento não desenvolvido, que é um evento que poderia ter sido desenvolvido mas não foi, por não ser de interesse para o problema ou porque seu desenvolvimento ultrapassa as fronteiras do sistema em análise. O símbolo para este tipo de evento é um diamante e, por isso, ele é normalmente conhecido como “evento diamante”.

Um terceiro tipo de evento primário é o evento condicionante, que especifica condições aplicáveis para um portão lógico. Um quarto tipo é o evento externo, que tem ocorrência normalmente esperada.

Eventos intermediários são eventos posicionados na AF entre o ET e os eventos primários, localizados na sua base.

Os portões lógicos definem a lógica relacionada às entradas e às saídas. Os portões principais são “E” e “OU”. A saída de um portão lógico “E” ocorre apenas se todas as entradas acontecerem, já a saída de um portão lógico tipo “OU” ocorre contanto que apenas uma das entradas aconteça. Outros portões são o “OU EXCLUSIVO”, “E PRIORITÁRIO” e o portão “INIBIDOR”. A saída de um portão lógico “OU EXCLUSIVO” existe se uma, e apenas uma, entrada acontece. A saída de um portão “E PRIORITÁRIO” acontece se as entradas ocorrerem na seqüência especificada pelo evento condicionante associado. A

saída de um portão lógico “INIBIDOR” ocorre se uma (única) entrada acontece na presença do evento condicionante associado.

Há também símbolos para “TRANSFERÊNCIA PARA DENTRO” e “TRANSFERÊNCIA PARA FORA” que possibilitam que grandes AF sejam desenhadas como um conjunto de árvores menores.

A construção de uma AF parece um exercício simples mas nem sempre é tão direto quanto parece e há algumas particularidades (maiores detalhes podem ser obtidos no “*Fault Tree Handbook*”).

Uma condição básica para sua construção é a definição e o entendimento do sistema a ser estudado. Ambos, o sistema em si e suas fronteiras precisam ser claramente definidos. A qualidade do estudo final dependerá crucialmente do bom entendimento do sistema e todo o tempo gasto nessa fase será bem recompensado.

FUSSELL (1976) enfatiza que as condições de contorno do sistema não devem ser confundidas com suas fronteiras físicas. As condições de contorno definem a situação para a qual a AF deve ser construída. Uma condição de contorno importante é o evento topo. As configurações iniciais do sistema constituem condições de contorno adicionais. Esta configuração deveria representar o sistema em condições normais. Quando o componente tem mais de um estado operacional, uma condição inicial deve ser especificada para ele.

Árvores de Falha para plantas de processo classificam-se em dois grupos principais, cuja definição é feita pelo evento topo considerado. O primeiro grupo compreende aquelas árvores onde o ET é uma falha interna à planta, incluindo as que podem resultar em vazamentos ou explosões internas. No segundo grupo, o ET é um evento perigoso fora da planta, por exemplo, incêndios e explosões.

Se o ET é uma falha de equipamento, é necessário decidir se o interesse é pela confiabilidade, pela disponibilidade ou por ambas. Intimamente relacionado a isto é a extensão na qual os componentes do sistema são considerados reparáveis ou irreparáveis.

Cada evento da árvore seja ele topo, intermediário ou primário deve ser cuidadosamente definido e a identificação dada aos eventos também é importante. Se um mesmo evento recebe duas identificações distintas, a AF em si

pode estar correta mas vai haver confusão quando, por ocasião da definição dos cortes mínimos, o mesmo evento aparecer com nomes diferentes.

Para um sistema de processo, o ET será normalmente um modo de falha de um equipamento. As causas imediatas serão os mecanismos de falha para aquela falha em particular. Estes, por sua vez, constituem os modos de falha dos subsistemas relacionados e assim por diante.

O procedimento seguido para a construção de uma AF deve assegurar que a mesma seja consistente. Devem ser verificados basicamente dois tipos de consistência: a consistência em série, dentro de cada ramo e a consistência em paralelo, entre dois ou mais trechos. Deve-se atentar também para os eventos com grande probabilidade de ocorrência e aqueles que são raros.

A construção de uma AF é um processo criativo. Ele envolve a identificação dos efeitos da falha, seus modos e mecanismos. Embora ela seja freqüentemente utilizada na quantificação de eventos perigosos (o que é correto), sua função primordial é auxiliar na identificação de perigos.

Deve-se atentar para o fato de que AF criadas por diferentes analistas tendem a ser diferentes. As diferenças podem ser de estilo, de julgamento e/ou devidas à omissão e erros.

Uma hipótese fundamental no trabalho com confiabilidade de um modo geral (e com AF de modo particular) é que os eventos são considerados independentes, a menos que formalmente expresso em contrário.

Geralmente os eventos são assumidos como estatisticamente independentes (na prática há várias situações em que isso não ocorre). Na construção das Árvores de Falhas este problema ficou originalmente conhecido como “modo de falha comum”, depois como “causa de falha comum” e mais recentemente como “falha dependente”.

O problema é particularmente delicado em sistemas tais como os pertencentes ao reator nuclear, onde é exigido um alto grau de confiabilidade. A maneira de se conseguir isto é através do uso de sistemas de proteção, que incorporam um alto grau de redundância.

Teoricamente, as confiabilidades calculadas são extremamente altas mas há uma certa preocupação quanto a um possível sub-dimensionamento desta proteção devido ao fenômeno da falha dependente, que pode estar “disfarçado” de muitas maneiras.

Se ocorre este tipo de falha, então a intenção de projeto não é inteiramente alcançada e a confiabilidade pode ser menor (algumas vezes bem menor), em outras palavras o fenômeno de falhas dependentes tende a limitar a confiabilidade que pode ser alcançada, constituindo-se então em uma das maiores preocupações dos projetistas de sistemas de alta confiabilidade.

As preocupações com falhas dependentes são maiores na construção de AF para a indústria nuclear, algumas situações que podem ocasioná-las são:

- uso comum;
- mesmo defeito de fabricação;
- mesmo defeito na utilização;
- mesma exposição a um fator degradante;
- influência externa;
- operação inadequada;
- manutenção inapropriada.

Talvez a dependência mais óbvia seja o suprimento comum de energia elétrica.

Os equipamentos podem sofrer defeitos comuns devido à fabricação ou à especificação e aplicação. Os fatores degradantes mais comuns são: vibração, corrosão, poeira, umidade e variações extremadas de condições de tempo e temperatura. Influências externas incluem terremotos e colisões de veículos. Um evento como fogo ou explosão pode danificar vários equipamentos. O equipamento também pode ser indevidamente operado ou sua manutenção ser incorreta, nestes casos a redundância não resolve o problema.

A localização comum é um fator a ser analisado na falha dependente mas não é essencial. Ações incorretas de manutenção, por exemplo, podem ser mais prejudiciais (ainda assim, a separação dos equipamentos é desejável).

Um tipo de falha dependente, que é importante no contexto atual, é aquela resultante de um acidente operacional. A grande maioria dos equipamentos, incluindo os de proteção e combate a incêndio, podem ser suscetíveis a um incêndio ou explosão, justamente no instante em que seriam mais necessários.

Há evidências de que as falhas dependentes estejam associadas particularmente a componentes cuja falha esteja oculta. Um estudo dos relatórios de acidentes nucleares conduzido por TAYLOR (1978) mostra que, das falhas dependentes encontradas, apenas uma não era associada a um sistema em “*stand-by*” ou em operação intermitente.

Nem todas as falhas dependentes se relacionam a equipamentos redundantes, um outro tipo importante de falha dependente é a sobrecarga que pode ocorrer quando um equipamento falha e sua função é assumida por outro aparelho em funcionamento. Falhas causadas por efeito dominó e falhas em progressão também podem ser classificadas como falhas dependentes.

As falhas dependentes são um problema crucial em sistemas de alta confiabilidade mas elas só podem ser levadas em consideração em uma AF se o seu potencial é identificado.

Há também o caso de alguns sistemas que passam por mais de uma fase de operação. Tipicamente isto ocorre quando o mesmo equipamento é utilizado em momentos distintos, em diferentes configurações e para vários propósitos.

Um exemplo desse tipo de sistema é o Sistema de Resfriamento de Emergência (SRE) dos reatores nucleares tipo PWR. Após a ocorrência de um acidente de perda de refrigerante por grande ruptura do circuito primário, o SRE passa, normalmente, por três fases:

- resfriamento inicial do núcleo;
- alagamento do núcleo;
- remoção de calor residual (BURDICK ET AL., 1977).

De modo semelhante, em certas instalações de gás liquefeito de petróleo o mesmo equipamento é utilizado em diferentes modos para operação normal e à plena carga.

Com efeito, o ET para uma AF de um sistema de missão por fases é a saída de um portão lógico “OU”, na qual as entradas são os eventos topo de cada uma das fases da missão. Este “OU” particular difere, entretanto, do tipo convencional, uma vez que suas entradas ocorrem em diferentes momentos.

Embora um sistema de missão por fases possa ser analisado pela construção de um AF para cada fase, surgem alguns problemas na interface entre elas cuja solução não é trivial.

Para sistemas não-reparáveis (e somente eles), ESARY E ZIEHMS (1975) desenvolveram uma transformação para converter uma AF especial, do tipo mencionado acima, em uma AF convencional.

i) Diagrama Causa-Conseqüência

Uma outra técnica, que incorpora características tanto da Árvore de Falhas quanto da Árvore de Eventos, é o Diagrama Causa-Conseqüência, desenvolvido por NIELSEN (1971, 1974, 1975) e TAYLOR (1974, 1978).

O Diagrama Causa-Conseqüência é construído através da definição de um evento crítico e da análise das possíveis causas e conseqüências deste evento, o desenvolvimento do diagrama para frente tem as características de uma AE e para trás de uma AF.

Os elementos principais do diagrama são: definições de eventos e condições, bem como dos símbolos lógicos. Os símbolos lógicos incluem tanto os portões, que descrevem as relações entre os eventos causadores, como os vértices, que descrevem as relações entre as conseqüências.

Os símbolos de evento e condição descrevem os tipos de evento ou condição. Os principais portões lógicos são o portão “E” e o portão “OU”, há também os vértices correspondentes na forma de “E” ou de “OU”.

Algumas características importantes do Diagrama Causa-Conseqüência são a sua habilidade em tratar com caminhos que gerem conseqüências alternativas e com a cronologia dos eventos. O diagrama também pode ser utilizado para análise quantitativa.

j) Análise de Falhas Humanas

Uma fonte importante de danos e perigos é a operação incorreta de uma planta. Há alguns métodos que estudam este problema, um deles é o HAZOP que, conforme descrito, utiliza ferramentas para descobrir a possibilidade de ocorrência de desvios de operação. Outros métodos são a Análise das Tarefas

e a Análise dos Erros na Execução. O problema da falha humana é, contudo, muito complexo.

A Análise das Tarefas é uma técnica que foi originalmente desenvolvida como uma ferramenta de treinamento. Quando aplicada ao procedimento operacional da planta, ela procura desmembrá-lo em sub-rotinas, com o objetivo de descobrir potenciais dificuldades (ou mesmo erros) na execução das tarefas ou do procedimento como um todo.

Certamente esta análise serve também como uma técnica de identificação de perigos e tem sido aplicada a plantas de processamento com bons resultados. Deve ser notado também que o trabalho de escrever as instruções operacionais constitui um tipo menos formal da Análise de Tarefas, servindo também para identificação de perigos.

Outra técnica de identificação de erros operacionais é a Análise de Erros na Execução, desenvolvida por TAYLOR (1979). Este é o método de análise de procedimentos operacionais para descobrir possíveis erros na operação da planta, propriamente dita.

As ações a serem tomadas no processo são listadas, uma a uma, sendo cada qual seguida por seu efeito na planta, obtendo-se as seguintes seqüências: ação – efeito sobre a planta – ação – efeito sobre a planta

As ações são intervenções na planta, tais como acionamento de botões, abertura de válvulas, etc..

Os efeitos dos possíveis erros são examinados usando-se as palavras-chave para ação. As principais são:

MUITO CEDO
MUITO TARDE
MUITO
POUCO
MUITO LONGO
MUITO CURTO
DIREÇÃO ERRADA
OBJETO ERRADO
AÇÃO INCORRETA

Na análise dos efeitos de um erro, uma consideração importante é se o efeito pode ser observado e corrigido, é necessário também limitar o escopo da análise. Considerações de ações em OBJETO ERRADO devem se restringir aos objetos próximos (física ou psicologicamente) ao objeto correto e o número de ações incorretas a serem consideradas deve ser mantido pequeno.

Erros múltiplos devem ser considerados até certo ponto, de modo que em grandes procedimentos operacionais, por questões de ordem prática, devem ser levados em conta somente os erros iniciais.

A técnica de Análise de Erros na Execução é bastante utilizada nos países nórdicos mas não tanto em outros lugares do mundo.

2.3 A ESCOLHA DA TÉCNICA A SER UTILIZADA

A análise tipo AMFE foi a escolhida porque, conforme atesta KUMAMOTO (1996), ela detalha sistematicamente, componente a componente, todos os possíveis modos de falha e identifica suas conseqüências na planta, possibilitando introdução de melhorias ou a correção dos defeitos, ainda na fase de projeto. Prováveis deficiências em cada componente da planta são analisadas para determinar seus efeitos em outros componentes a ele relacionados. De acordo com a MIL-STD-1629A (1980), esta técnica pode ser orientada para o equipamento, concentrando-se nas potenciais falhas dos mesmos ou para os eventos, onde a ênfase é nas saídas funcionais e seus efeitos para o sistema em caso de falha.

A principal limitação deste método é considerar a progressão dos modos de falha individualmente, dificultando a avaliação dos efeitos para combinação de diversos modos de falha ocorrendo simultaneamente. Para minimizar essa deficiência foi introduzido o conceito de condição latente na análise, o que ocorre quando a falha de um componente não provoca maiores problemas mas cria condições para que, caso haja falha de outro componente a ele relacionado (física ou funcionalmente), aconteça um acidente.

Uma técnica complementar a AMFE, de caráter dedutivo é a Árvore de Falhas, que é mais indicada nos casos em que a lógica da falha é mais complexa.

Como já visto anteriormente, algumas dificuldades no trabalho com a AF são que ela requer tempo e esforço considerável da parte de analistas bem treinados e, embora ela seja uma das melhores ferramentas para se analisar o sistema como um todo, ela não garante, por si só, a detecção de todas as falhas, especialmente as que possuam uma causa comum.

Esse problema é particularmente delicado em sistemas tais como os pertencentes ao reator nuclear, onde é exigido um alto grau de confiabilidade. A maneira de se conseguir isto é através do uso de sistemas de proteção, que incorporam um alto grau de redundância.

Teoricamente, as confiabilidades calculadas são extremamente altas mas há uma certa preocupação quanto a um possível sub-dimensionamento desta proteção devido ao fenômeno da falha dependente, que pode estar “disfarçado” de muitas maneiras. Se ocorre este tipo de falha, então a intenção de projeto não é inteiramente alcançada e a confiabilidade pode ser menor (algumas vezes bem menor), em outras palavras o fenômeno de falhas dependentes tende a limitar a confiabilidade que pode ser alcançada, constituindo-se então em uma das maiores preocupações dos projetistas de sistemas de alta confiabilidade.

Já o HAZOP, além de ser uma técnica mais utilizada para a análise de processos, apresenta basicamente dois tipos de limitações:

- a primeira advém das hipóteses concernentes ao método e é uma limitação de escopo. Na sua forma original, o método assume que o projeto foi conduzido de acordo com as normas apropriadas; e
- a outra restrição é inerente ao método. O HAZOP não é indicado, por exemplo, para tratar com características espaciais associadas ao “*layout*” da planta e os seus efeitos resultantes.

3 A INSTALAÇÃO NUCLEAR EXPERIMENTAL

3.1 DESCRIÇÃO

De acordo com o RPAS (2007), a instalação nuclear experimental (INE) é um empreendimento composto por onze prédios principais e o protótipo em terra (PROTER) de uma planta propulsora nuclear para emprego em submarinos. Seu componente principal é um reator compacto à água pressurizada, tipo PWR, a ser instalado no interior do prédio do reator. As outras unidades da INE abrigam todos os sistemas e componentes necessários à operação segura desse reator.

O PROTER é formado por blocos (estruturas metálicas, cilíndricas e com eixos horizontais) que pretendem simular, física e operacionalmente, a propulsão de um submarino. Essas estruturas denominadas blocos 20, 30 e 40, estarão localizados no interior de dois prédios: o bloco 40 no prédio do reator, e os blocos 20 e 30 no prédio das turbinas. Os blocos serão instalados sobre jazentes fixos ao piso dos prédios, como mostra a FIG. 1.

Figura 1 – Blocos 20, 30 e 40 (extraído do RPAS, 2007).

O reator e o circuito primário serão montados no interior do bloco 40, o circuito secundário será montado internamente ao bloco 30 e a propulsão elétrica no bloco 20. Os blocos 20 e 30 são contíguos e solidários, formando uma estrutura única.

A INE será composta dos seguintes sub-empresendimentos principais, conforme esboçado na FIG. 2:

- protótipo em terra (PROTER);
- prédio do reator (PR) e anexo (APR);
- prédio das turbinas (PT) e anexo (APT);
- prédio auxiliar não-controlado (PANC);
- prédio auxiliar controlado (PAC) e chaminé de exaustão (CE);
- prédio do combustível (PC);
- prédio da cabine primária (SUB 1);
- prédio do diesel gerador de emergência (SUB 2);
- infra-estrutura de apoio (IEA);
- unidade de resfriamento do PROTER (UR);
- prédio de preparação e testes de embalagens (PPTE); e
- prédio de armazenamento intermediário de rejeitos (PAIR).

Figura 2 – Aparência externa da instalação nuclear experimental (RPAS, 2007).

O bloco 40 constitui o compartimento do reator, onde serão instalados os componentes do “circuito primário”, sendo suportado por selas de sustentação, apresentando alto grau de estanqueidade (dotado de anteparas de blindagem secundárias nas suas extremidades) e resistência à pressão pós-acidental, permanecendo submerso na água da piscina de blindagem externa, a qual será construída em concreto dentro do prédio do reator.

Adjacentes e solidários ao compartimento do reator, formando uma estrutura única (denominada contenção), têm-se os sub-compartimentos denominados bloco 40V e bloco 40R (respectivamente localizados à vante e à ré do bloco 40), que servem como volume de expansão para redução da pressão pós-acidental na contenção e abrigam alguns dos sistemas auxiliares e de segurança do circuito primário, incluindo as escotilhas de acesso de pessoal e de instalação e remoção de equipamentos.

Dentre os principais componentes inseridos no bloco 40, estão: o reator, os geradores de vapor, o pressurizador, as bombas de resfriamento do reator, o tanque de blindagem, os trocadores de calor, as bombas de resfriamento de componentes do primário e o Sistema de Injeção de Refrigerante (SIR).

Também fazem parte do bloco 40 os seguintes componentes básicos:

- penetrações das tubulações de processo, de cabos elétricos, de instrumentação e de dutos de ventilação;
- válvulas de isolamento; e
- “*dampers*”.

O bloco 40V contém os seguintes equipamentos:

- dois trocadores de calor do Sistema de Resfriamento de Emergência;
- duas bombas de circulação do refrigerante do Sistema de Resfriamento de Emergência;
- dois painéis de indicação de posição do mecanismo de acionamento de barras;
- um painel do excitador do mecanismo de acionamento de barras.

O bloco 40R abriga, essencialmente, os dois acumuladores do Sistema de Resfriamento de Emergência.

O reator tipo PWR da INE possui uma potência de 48 MW térmicos e o circuito primário segregado. Seu núcleo é composto por 21 elementos combustíveis formados por varetas de aço austenítico em arranjo quadrado 17x17, contendo pastilhas cilíndricas de dióxido de Urânio (UO_2) enriquecido a 4,3% em massa. Cada elemento combustível é dotado de um grupo de barras de controle ou segurança, respectivamente na liga Prata-Índio-Cádmio (Ag-In-Cd) e carbeto de Boro (B_4C), acionado individualmente por um mecanismo elétrico do tipo porca rotativa. Para otimizar a queima do combustível são inseridas em 20 posições do elemento combustível central, varetas de veneno queimável, de B_4C em alumina (Al_2O_3).

O Sistema de Resfriamento do Reator é composto por dois circuitos; cada um contendo um gerador de vapor e três bombas de circulação encapsuladas, sendo uma delas utilizada como reserva das outras duas. O circuito possui ainda um pressurizador ligado à perna quente de um dos circuitos.

O vapor saturado seco gerado pelo circuito primário alimenta o sistema de conversão de energia (secundário), constituído por dois circuitos a vapor em ciclo Rankine idênticos e interligados. Cada circuito é composto por um turbo-gerador de 3.800 KWe, destinado a alimentar o sistema elétrico de propulsão, um turbo-gerador de 1.800 KWe, que supre o sistema elétrico de serviço (cargas próprias da instalação), um condensador principal, duas bombas de extração de condensado e duas bombas de água de alimentação dos geradores de vapor. O vácuo nos condensadores principais é garantido por grupos ejetores a vapor. O resfriamento de cada condensador principal é feito por uma bomba de circulação e por um conjunto de torres de resfriamento. Cada condensador está dimensionado para operar com 70% da potência nominal da planta, ou seja, apenas um circuito do ciclo secundário operando com os dois geradores de vapor, cada um a 70% de sua potência nominal. Cada circuito dispõe ainda de um tanque de armazenamento de condensado de 8.000 litros chamado de tanque de alimentação de emergência com a função de fornecer água de emergência para os geradores de vapor. As bombas de alimentação dos geradores de vapor estão ligadas a um barramento elétrico que proporciona energia mesmo no caso de desligamento do reator.

O sistema elétrico de propulsão é composto por um motor elétrico de 7.400 KWe, alimentado pelos dois turbo-geradores de 3.800 KWe, e ligado a um eixo propulsor através de um acoplamento flexível. A dissipação da energia transferida ao eixo é feita por um freio dinamométrico, que simula a resistência ao avanço do submarino no mar.

O circuito secundário e o sistema de propulsão elétrica estão instalados no interior de dois compartimentos metálicos cilíndricos horizontais sem características específicas de contenção ou confinamento, os blocos 20 e 30. Estes blocos estão localizados no interior de um prédio sem características de confinamento mas cujas estruturas são sísmicas, o prédio das turbinas.

O sistema de contenção nuclear da INE é concebido como uma contenção dual de pressão total, conforme conceito recomendado pela Agência Internacional de Energia Atômica (AIEA).

A estrutura da contenção é composta essencialmente por duas barreiras. A primeira barreira é definida pelo envelope estanque do bloco 40 e constitui a contenção propriamente dita, ou seja, resistente à pressão máxima pós acidente básico de projeto. O envelope confinado do prédio do reator constitui a segunda barreira, controladora de eventuais fugas limitadas da primeira barreira.

O bloco 40 (contenção) tem as seguintes funções:

- a) conter todos os sistemas que, em condições normais de operação, são submetidos à pressão do circuito primário;
- b) suportar plenamente os aumentos momentâneos de pressão e temperatura decorrentes dos acidentes postulados de projeto, especialmente do acidente de perda de resfriamento do primário;
- c) prover um primeiro nível de blindagem radiológica para o ambiente externo e para os operadores da instalação durante operação normal e sob condições acidentais;
- d) prover proteção contra agressões de origem interna, decorrentes dos acidentes postulados de projeto;
- e) proteger os sistemas e componentes no interior da contenção contra agressões externas postuladas, provenientes do confinamento secundário.

O prédio do reator (confinamento secundário) tem as seguintes funções:

- a) prover blindagem radiológica para o ambiente externo e para os operadores da instalação, durante operação normal e sob condições acidentais;
- b) proteger os sistemas e componentes no interior do confinamento secundário contra agressões externas postuladas, provenientes do confinamento primário;
- c) coletar vazamentos provenientes da contenção;
- d) prover proteção contra agressão de origem interna, decorrente dos acidentes postulados de projeto.

3.2 O SISTEMA DE RESFRIAMENTO DE EMERGÊNCIA (SRE)

3.2.1 Descrição geral

Conforme TAKESHI (2004a), o SRE é composto por equipamentos destinados a receber, estocar e injetar o refrigerante no reator, além de remover o calor residual do núcleo em condições normais e anormais de operação, ou ainda, durante os acidentes de perda de refrigerante.

Este sistema utiliza, em parte, a concepção desenvolvida nos recentes projetos de sistemas de segurança passivos, que atuam na remoção do calor residual do núcleo ou em casos de acidentes de perda de refrigerante de reatores de pequeno e médio porte.

Também foram introduzidos componentes ativos no sistema, baseados em reatores nucleares comerciais em operação, possibilitando uma maior flexibilidade na sua operação e uma maior eficiência na mitigação das consequências do acidente.

O SRE é dividido em dois subsistemas:

a) Subsistema de Injeção de Emergência (SIE), que atua na reposição da água do circuito primário, quando houver um vazamento superior a $1,0 \text{ m}^3/\text{h}$, ou ainda de modo a garantir a integridade e a geometria do núcleo, através da inundação do vaso do reator, no caso de acidentes de perda de refrigerante por pequena ou grande ruptura do primário.

Para perdas a taxas menores que a mencionada acima, a atuação estará a cargo do Sistema de Injeção de Refrigerante (SIR).

O SIE é composto por:

- dois tanques de compensação, situados na parte superior do compartimento do reator e com capacidade para $1,75 \text{ m}^3$ cada, contendo água desmineralizada à mesma pressão do SRR;
- dois acumuladores, instalados na contenção e com capacidade para $2,57 \text{ m}^3$ cada, contendo água borada e pressurizados por Nitrogênio a 28 bar;
- dois tanques de inundação, localizados acima da piscina de blindagem externa e com capacidade para $70,00 \text{ m}^3$ cada, contendo água borada à mesma pressão do prédio do reator;
- duas bombas centrífugas para injeção de água borada à alta pressão (90 bar) no reator, colocadas no lado externo da contenção;
- duas bombas centrífugas para injeção de água borada à baixa pressão (14 bar) no reator, localizadas em área próxima às bombas de alta;
- uma bateria de cilindros de Nitrogênio para a pressurização dos acumuladores, localizada no edifício anexo.

O subsistema conta ainda com um tanque, um misturador e uma bomba centrífuga para preparação da solução de ácido bórico (água borada) e sua injeção nos acumuladores e tanques de inundação. Em virtude destes equipamentos atuarem apenas na fase de preparação inicial do SIE, os mesmos não serão considerados, para efeito das análises a serem executadas neste trabalho.

A função do Boro, presente na solução de água que abastece os acumuladores e os tanques de inundação, é compensar a inserção de reatividade positiva com a injeção de água fria no vaso do reator, contemplando uma eventual falha no desligamento por meio das barras de controle e de segurança, num acidente de perda de refrigerante.

b) Subsistema de Remoção de Calor Residual (SRCR), que é o responsável pelo resfriamento do reator após o desligamento nas diversas condições de operação da instalação, incluindo-se o caso de um acidente de perda de refrigerante.

Para isso, este subsistema dispõe de:

- dois trocadores de calor, tipo casco-tubo, para a remoção do calor residual do núcleo do reator (instalados dentro da contenção);
- duas bombas centrífugas para a circulação de refrigerante do reator ou do fluido presente no compartimento do reator após a sua inundação, através dos tubos dos trocadores de calor supracitados;
- duas bombas centrífugas para a circulação de água de resfriamento (da fonte fria) pelos cascos dos trocadores de calor;
- um trocador de calor para remoção de calor residual do reator em circulação natural.

A FIG. 3 mostra um diagrama esquemático do SRE. A localização exata e a interligação dos equipamentos deste sistema, bem como a instrumentação e os controles associados, encontram-se em TAKESHI (2004b).

Figura 3 – Diagrama esquemático do SRE (TAKESHI, 2004a).

3.2.2 Função do SRE

O Sistema de Resfriamento de Emergência é projetado para executar as seguintes funções básicas:

- resfriar o reator, após seu desligamento, com a remoção do calor residual do núcleo, de modo a reduzir a temperatura do refrigerante do reator até que esta atinja o valor previsto para a parada a frio da instalação (ou seja, reator com as barras de controle e de segurança totalmente inseridas, temperatura média de 60°C , pressão de 1 a 10 bar abs, com ou sem calor residual);
- garantir a integridade do núcleo do reator, em caso de acidente de perda de refrigerante do Sistema de Resfriamento do Reator, por meio da injeção de água no vaso do reator;
- Assegurar o resfriamento do reator, por tempo indeterminado, após um acidente de perda de refrigerante.

3.2.3 Modos de operação do SRE

O SRE foi concebido para remover o calor armazenado no circuito primário e o calor gerado no núcleo do reator, após o desligamento, devido ao decaimento dos produtos de fissão. Com isso, evita-se a elevação da temperatura do revestimento, assegurando-se a integridade dos elementos combustíveis e impedindo-se a liberação de material radioativo para o refrigerante. Esse calor deve ser removido durante as paradas normais da instalação, no caso de um resfriamento anormal ou de emergência, ou ainda em casos de acidentes de perda de refrigerante do primário (APRP).

3.2.3.1 Operação do SRE durante o resfriamento normal do primário

No caso de desligamento do reator com a parada normal da instalação, um resfriamento inicial é feito dissipando-se o calor nos geradores de vapor. O vapor produzido é descarregado diretamente no condensador principal por meio da abertura das válvulas do subsistema de desvio de vapor do circuito secundário.

As bombas de circulação de refrigerante do reator continuam operando na rotação nominal, para promover o resfriamento e a despressurização do circuito primário.

A alimentação elétrica dos componentes ativos é assegurada pela concessionária fornecedora de energia (em caso de interrupção do fornecimento, a alimentação é garantida por intermédio de um grupo de geradores diesel).

A taxa de remoção de calor e, por consequência, a taxa de resfriamento do primário são controladas pela pressão nos geradores de vapor, a qual regula a diferença de temperaturas entre o primário e o secundário. Esta pressão, por sua vez, é controlada pela abertura das válvulas de desvio de vapor.

A redução do volume de refrigerante do reator devido ao resfriamento é compensada pela injeção de água desmineralizada pelo SIR.

Com a despressurização controlada do primário, o SIE deve ser mantido isolado, a fim de evitar a sua atuação indevida no processo de resfriamento do reator (para isso são fechadas as válvulas nas linhas de descarga dos acumuladores).

Quando a temperatura atingir o valor de 176°C e a pressão for reduzida a 28 bar abs, a fase final do processo de resfriamento é realizada com a intervenção do SRCR. Para essa finalidade, este subsistema dispõe de dois circuitos de resfriamento independentes, cada um composto por um trocador de calor, uma bomba de circulação de refrigerante e uma bomba de circulação de água de resfriamento. Caso necessário, o operador pode colocar qualquer um dos circuitos de resfriamento em funcionamento, enquanto o outro é mantido na condição de espera, em caso de falha.

A operação do trocador de calor é iniciada com o acionamento da bomba de circulação de água de resfriamento. A seguir, a bomba de circulação de refrigerante é acionada para succionar o refrigerante do reator da perna quente e retorná-lo à perna fria do mesmo circuito do Sistema de Resfriamento do Reator (SRR), após o resfriamento no trocador.

O calor é então dissipado para o Sistema de Água de Resfriamento de Segurança da Planta (SARSP), com a circulação de água pela fonte fria (piscina de blindagem), mantida sempre resfriada pelos resfriadores evaporativos do SARSP.

O processo de resfriamento é considerado encerrado quando o circuito primário atingir a temperatura de 60°C e a pressão suficiente para assegurar o NPSH para as bombas de circulação do SRE.

3.2.3.2 Operação do SRE durante o resfriamento anormal do primário

No caso de um desligamento súbito do reator por queda das barras de controle e segurança, e quando não há possibilidade de se realizar o resfriamento do reator por intermédio dos geradores de vapor, o SRE atua como um sistema alternativo para a remoção de calor residual. Nesta situação, o SRE é acionado automaticamente com o sinal de baixo nível no gerador de vapor, provocando o desligamento do reator e das bombas de circulação do primário.

Este modo de operação é previsto no caso de falhas de tubos dos geradores de vapor, falhas na tubulação principal de vapor, ruptura da linha de alimentação dos geradores de vapor, falta de energia elétrica externa, ou ainda, com o fechamento inadvertido das válvulas de isolamento do reator.

O resfriamento do reator é assegurado com a atuação do SRCR pelo Sistema de Proteção da Planta (SPP). A água do reator será bombeada para um dos trocadores de calor, em qualquer condição de pressão e temperatura do fluido do primário e, em seguida, será retornada fria para o reator, conforme descrito no item anterior.

Ainda neste modo de operação, com a finalidade de controlar a taxa de resfriamento do primário, válvulas são utilizadas para o controle manual da vazão do refrigerante do reator que passa nos trocadores de calor.

3.2.3.3 Remoção do calor residual por circulação natural

O SRCR possui também outro trocador de calor, projetado para a remoção de calor residual do reator em circulação natural, tanto para o refrigerante do reator como para a água de resfriamento que passa pelo trocador de calor.

O trocador de calor a circulação natural é considerado um dispositivo experimental, que será qualificado através de sua operação na instalação nuclear, visando sua aplicação no desenvolvimento de tecnologia para o projeto de reatores inerentemente seguros. Dessa maneira, este equipamento **não desempenha uma função de segurança na cadeia de proteção/controle do reator.**

Para permitir o resfriamento do reator por circulação natural do fluido primário, este trocador é instalado em um nível mais elevado que o núcleo do reator, interligado entre uma perna fria e outra quente do SRR.

3.2.3.4 Acidentes de perda de refrigerante do reator

Um acidente de perda de refrigerante pode ser caracterizado desde pequenos vazamentos nos componentes do SRE, ou nas linhas dos sistemas conectados com o SRR, que sejam de magnitude superior à capacidade de reposição do SIR (ou seja, $1,0 \text{ m}^3/\text{h}$), até o acidente básico de projeto de reatores nucleares a água pressurizada, qual seja a ruptura instantânea, tipo guilhotina, da tubulação principal de entrada do reator.

Para compensar a perda de capacidade normal de resfriamento, resultante de um APRP, o SIE atua através da injeção de água no vaso do reator, garantindo a integridade e a geometria do núcleo.

Um acidente de perda de refrigerante é constatado pelo SPP, através da ocorrência simultânea da queda de pressão no primário com o aumento de pressão e/ou radioatividade no interior da contenção, ou ainda com a queda do nível de água no pressurizador, abaixo do valor mínimo de desligamento do reator.

Ao se atingir a pressão mínima no pressurizador (120 bar), o SPP efetua inicialmente o desligamento do reator por meio da queda de barras de controle e segurança. Ao constatar um acidente de perda de refrigerante, o SPP efetua também o desligamento das bombas de circulação do primário e gera o Sinal de Injeção de Segurança (SIS) para atuação do SRE, colocando em prontidão os sistemas de segurança.

3.2.3.4.1 Pequenas perdas de refrigerante do reator

Para acomodar pequenas perdas de refrigerante, com a lenta despressurização do reator, em casos de pequenos acidentes, o SRE fará uso de seus dois tanques de compensação e da injeção à alta pressão.

Os tanques de compensação são interligados, cada um a um circuito do SRR. Uma linha de descarga sai do fundo de cada tanque para injeção de água na perna fria do reator. A parte superior do tanque é conectada por meio de uma tubulação com a perna quente do reator, denominada linha de equilíbrio de pressão.

Normalmente, os tanques de compensação são mantidos cheios com água desmineralizada à temperatura inferior a do refrigerante do reator e à mesma pressão do circuito primário. Para isso, as válvulas das linhas de descarga são mantidas fechadas, enquanto que as válvulas das linhas de equilíbrio de pressão encontram-se abertas.

Durante um acidente de perda de refrigerante, a pressão no SRR diminui provocando o desligamento do reator e das bombas de circulação do primário. Com o sinal de atuação enviado pelo SPP, ocorre a abertura automática das válvulas que comunicam os tanques de compensação às pernas frias do circuito primário. Estas ações viabilizam a descarga da água, contida nos tanques de compensação, nas pernas frias do reator para compensar a perda de refrigerante.

A injeção passiva da água, por ação da gravidade, é assegurada por meio da localização dos tanques de compensação na região superior do compartimento do reator, acima do vaso.

Ao se atingir uma pressão abaixo de 90 bar, é iniciada a injeção ativa, na perna fria ou quente do reator, através das bombas de injeção a alta pressão (BIAP), de modo a manter o núcleo sempre inundado.

As BIAP injetam água borada, succionada dos tanques de inundação, e são acionadas automaticamente por meio do SIS (que também comanda a abertura das válvulas de bloqueio nas linhas de injeção).

Uma BIAP é mantida em operação independente, para cada circuito do SRR, uma bomba injeta água borada na perna fria do circuito 1 do SRR, enquanto a outra injeta na perna quente, conectada com o pressurizador.

O SRE dispõe ainda de uma linha de recirculação, na descarga de cada bomba de injeção de emergência, para a proteção das mesmas, quando a pressão na descarga for igual à pressão de vazão nula da bomba. Esta linha retorna a água para o tanque de inundação correspondente.

3.2.3.4.2 Grandes perdas de refrigerante do reator

Em caso de grandes perdas de refrigerante do reator, resultando numa súbita despressurização do circuito primário, temos, além da atuação dos tanques de compensação e das BIAP (conforme descrito no item anterior), a injeção passiva, assegurada principalmente pelos dois acumuladores, que contribuem para o resfriamento do núcleo nos instantes iniciais do acidente.

Os acumuladores são vasos de pressão, contendo água borada e pressurizados com Nitrogênio a 28 bar abs. Durante a operação normal da instalação, cada acumulador é isolado do SRR por intermédio de duas válvulas de retenção em série.

Ao se atingir uma pressão inferior à dos acumuladores no SRR, ocorre a abertura das válvulas de retenção nas linhas de descarga, permitindo a injeção de água borada nas pernas quentes do reator.

Após a atuação dos acumuladores, quando seu nível atinge o valor mínimo, são fechadas as válvulas de bloqueio (na linha de descarga de cada acumulador) isolando-os automaticamente e interrompendo a injeção através dos mesmos.

Neste mesmo instante, um sinal é emitido para o desligamento das BIAP, possibilitando assim uma vazão mais alta nas linhas de injeção.

Em virtude do grande gradiente de pressão num acidente de perda de refrigerante por grande ruptura e devido à quantidade reduzida de água contida nos tanques de compensação e nos acumuladores, uma fonte adicional de injeção é requerida.

Nesta fase entram em operação as bombas de injeção à baixa pressão (BIBP), acionadas automaticamente pelo SIS quando a pressão do primário atingir 14 bar, injetando água borada, proveniente dos tanques de inundação, nas pernas fria e quente do reator.

Em caso de falha no funcionamento das BIBP, o sistema conta ainda com o recurso de injeção de água diretamente dos tanques de inundação, por gravidade, através das tubulações de descarga das bombas de injeção.

Estes vasos são mantidos à mesma pressão do prédio do reator. Para a descarga da água por gravidade, as válvulas dos respiros dos tanques são fechadas e são abertas as válvulas das linhas que ligam os tanques de inundação ao ambiente da contenção, possibilitando assim a equalização da pressão.

Parte da água injetada remolha o núcleo e deixa o SRR, através da tubulação que sofreu ruptura, ficando retida no fundo do compartimento do reator.

O volume de água borada, contido nos tanques de inundação, é suficiente para inundar o bloco 40 até o nível dos bocais do vaso do reator, possibilitando o início da fase de recirculação para o restabelecimento das condições de remoção de calor do núcleo.

Após o esgotamento dos tanques de inundação, o SRCR pode ser redirecionado pelo SPP para captar a água contida na parte inferior do compartimento do reator (água que escapou do circuito primário através da ruptura) e retorná-la ao vaso do reator, pela perna fria ou quente (dependendo da localização da ruptura), após ter sido resfriada nos trocadores de calor.

As bombas de circulação de água de resfriamento são ligadas juntamente com as bombas de circulação de refrigerante para promover a circulação da água da piscina de blindagem nos trocadores de calor. Esta operação continua até que a geração de calor residual atinja níveis seguros.

A FIG. 4 ilustra, de forma sintética, a seqüência de atuação dos equipamentos do SRE no caso de um APRPGR.

Figura 4 – Diagrama resumido da seqüência de atuação dos equipamentos do SRE, durante um APRPGR (obtido de TAKESHI, 2004a).

4 RESULTADOS

4.1 CONSIDERAÇÕES INICIAIS

A análise do tipo AMFE é documentada em uma planilha composta pelas seguintes colunas (conforme pode ser observado na MIL-STD-1629A (1980) e na tabela que consta do item 4.2, desta dissertação):

a) Número de identificação: pode ser o número de série ou outro número de referência, desde que identifique perfeitamente o item, de modo a garantir a sua rastreabilidade;

b) Item: o nome do item (ou função do sistema) que é objeto da análise;

c) Função: é um relato conciso da função executada pelo componente;

d) Modos de Falha: todos os modos de falha passíveis de serem previstos (e que sejam relevantes para a análise em questão) devem ser identificados e descritos;

e) Modo Operacional: é a descrição sucinta do modo de operação no qual a falha ocorre;

f) Efeitos da Falha: as conseqüências de cada modo de falha, listado na análise, devem ser identificadas, avaliadas e registradas. A falha em questão pode provocar impactos localmente, em níveis imediatamente superiores e na planta como um todo.

- Locais: concentram-se especificamente nos impactos que um determinado modo de falha possa causar na operação do item analisado ou de outros componentes neste mesmo nível;

- Próximo Nível: de modo similar, refere-se às conseqüências do modo de falha postulado verificadas no nível imediatamente superior ao do item analisado;

- Nível Final: avalia o resultado da falha daquele componente em análise no sistema como um todo.

g) Método de Detecção: cita os métodos pelos quais o operador pode detectar a ocorrência da falha.

h) Recursos de Compensação: podem ser tanto recursos de projeto (como redundâncias) ou procedimentos a serem tomados pelo operador e que servem para limitar ou mitigar a ocorrência de uma falha.

i) Classe de Severidade: cada modo de falha deve receber uma classificação de severidade, de acordo com o seu efeito no sistema. A MIL-STD 1629A (1980) sugere as seguintes categorias de severidade:

- I, Catastrófica: uma falha que pode causar morte ou perda do sistema;
- II, Crítica: uma falha capaz de provocar ferimentos graves e/ou grandes danos ao sistema, resultando no não cumprimento da missão, para o qual foi projetado;
- III, Marginal: uma falha que pode causar ferimentos de menor gravidade e pequenas perdas ao sistema que resultarão em atraso ou outros problemas para o cumprimento da missão; e
- IV, Desprezível: uma falha que não seja grave o suficiente para causar ferimentos ou danos ao sistema, mas que resultará em reparo ou manutenção não programada do mesmo.

h) Observações: Qualquer comentário pertinente necessário ao perfeito entendimento das outras colunas da planilha.

Quanto ao escopo da análise tipo AMFE, cumpre ressaltar que o Subsistema de Água Borada (SAB), por atuar apenas na fase de preparação inicial do SRE, não será considerado.

De modo similar, a remoção de calor por circulação natural do SRCR também não será analisada em virtude de seu caráter meramente experimental, não desempenhando, portanto, função de segurança na operação do SRE.

Por fim, conforme TAKESHI (2004a), é empregada redundância de quatro nos instrumentos de medição de todas as variáveis existentes no SPP. Portanto, para efeitos deste estudo, a análise destes componentes não faz parte do objetivo.

Com relação a falhas humanas, em virtude da atuação do SIE ser totalmente automatizada e não haver previsão de atuação do operador em nenhum momento durante a operação do mesmo e, no caso do SRCR, a atuação mais crítica consiste em realinhar o subsistema para o modo de recirculação de

água contida no poço da contenção, partimos da hipótese que esta operação foi efetuada com sucesso e, portanto, que não há ocorrência deste tipo de falha.

Outras formas de falha humana como erros de projeto, especificação inadequada de componentes do sistema e/ou erros em procedimentos de instalação e manutenção também não são objeto deste estudo.

Por fim, como preparação para a análise tipo AMFE, foram feitos os diagramas de blocos do Sistema de Resfriamento de Emergência, com base no seu fluxograma de engenharia (TAKESHI, 2004b).

Os diagramas encontram-se segregados da seguinte maneira:

a) Subsistema de Injeção de Emergência (SIE)

Os diagramas de blocos, referentes ao SIE estão representados nas figuras de números 5 a 8.

A FIG. 5 (na página 59) mostra a injeção de emergência através do tanque de compensação, a FIG. 6 (página 60) a injeção de emergência através do acumulador, a FIG. 7 (na página 61), a injeção de emergência através das bombas de alta pressão, de baixa pressão e a injeção por gravidade.

A FIG. 8 (página 62) retrata a linha de equalização de pressão, que possibilita a injeção por gravidade.

b) Subsistema de Remoção de Calor Residual (SRCR)

O diagrama de blocos, referente a este subsistema está representado na FIG. 9 (localizada na página 63).

Foi apresentado apenas um diagrama por figura mas cada uma delas apresenta uma linha redundante exatamente igual a ela. A análise feita para a linha em questão, obviamente é válida para a outra linha.

Para efeitos didáticos, as válvulas gaveta normalmente fechadas foram apresentadas em caixa vermelha, as normalmente abertas em verde e as de retenção em amarelo.

Figura 5 – Diagrama de blocos da injeção de emergência, através do tanque de compensação.

Figura 6 – Diagrama de blocos da injeção de emergência, através do acumulador.

Figura 7 – Diagrama de blocos da injeção de emergência, através do tanque de inundação.

Figura 8 – Diagrama de blocos da linha de equalização de pressão (injeção por gravidade).

Figura 9 – Diagrama de blocos do Subsistema de Remoção de Calor Residual (SRCR).

4.2 ANÁLISE TIPO AMFE

A análise tipo AMFE do SRE foi executada e as tabelas organizadas, conforme descrito no item anterior.

As tabelas de 1 a 4 mostram os resultados da análise para o Subsistema de Injeção de Emergência (SIE). A tabela 1 trata da linha de injeção através dos tanques de compensação; a tabela 2, da injeção por intermédio dos acumuladores; a tabela 3, da injeção através dos tanques de inundação (seja ela pelas bombas de alta pressão, pelas bombas de baixa pressão ou por gravidade) e a tabela 4 mostra a linha de equalização de pressão, necessária para a injeção por gravidade.

Finalmente a tabela 5 trata do Subsistema de Remoção de Calor Residual (SRCR), cuja atuação é precedida pelo SIE.

Como no caso dos diagramas de blocos, foi feita a análise de apenas uma linha em cada tabela mas cada um destes modos de injeção e resfriamento possui uma linha redundante idêntica, cujos resultados da análise são os mesmos e por este motivo não foram colocados neste trabalho.

Em toda a análise do sistema do SRE não foram encontradas falhas catastróficas ou críticas; ocorreram apenas falhas de menor severidade, sem prejuízos para as pessoas, em virtude de permanecerem restritas e confinadas ao ambiente da contenção.

Como observação final, os asteriscos (*) indicados na tabela referem-se a componentes sobressalentes da linha redundante e a notação “SCRAM” indica os casos onde a falha provocará o desligamento do reator por motivo de queda na pressão do circuito primário.

Tabela 1 – Análise tipo AMFE do SIE (tanques de compensação)– continua

Nº IDENT.	ITEM	FUNÇÃO	MODOS DE FALHA	MODO OPERACIONAL	EFEITOS DA FALHA			MÉTODO DE DETECÇÃO	RECURSOS DE COMPENSAÇÃO	CLASSE DE SEVERIDADE	OBS.
					LOCAIS	PROX. NÍVEL	NÍVEL FINAL				
2156-VP1	TANQUE DE COMPENSAÇÃO	ARMAZENAR ÁGUA DESMINERALIZADA PARA INJEÇÃO DE EMERGÊNCIA	- VAZAMENTO	INJEÇÃO DE EMERGÊNCIA	PERDA DO INVENTÁRIO DO TANQUE	IMPOSSIBILITA A ATUAÇÃO DESTE TANQUE NUM APRGR	NÃO ACARRETA MAIORES PROBLEMAS NO CASO DE UM APRGR	NÍVEL DO TANQUE DE COMPENSAÇÃO	VP2 (*)	IV	
4ADR-2156 03-1G70	TUBULAÇÃO	TRANSPORTAR A ÁGUA DESMINERALIZADA DO TANQUE DE COMPENSAÇÃO PARA O BLOCO 40	- VAZAMENTO	INJEÇÃO DE EMERGÊNCIA	NÃO LEVA FLUIDO SUFICIENTE AO BLOCO 40	IMPOSSIBILITA A ATUAÇÃO DESTE TANQUE NUM APRGR	NÃO ACARRETA MAIORES PROBLEMAS NO CASO DE UM APRGR	NÃO HÁ	04-1G70 (*)	IV	
HV 0711	VÁLVULA GAVETA NORMAL. FECHADA	PERMITIR INJEÇÃO PELOS TANQUES DE COMPENSAÇÃO	- NÃO ABRE - ABRE PARCIALMENTE	INJEÇÃO DE EMERGÊNCIA	NÃO DÁ PASSAGEM	EXIGE ATUAÇÃO DA VÁLVULA HV 0713	NÃO ACARRETA MAIORES PROBLEMAS NO CASO DE UM APRGR	PAINEL DE CONTROLE / INSPEÇÃO LOCAL	HV 0713	IV	
	ACIONAM. SOLENÓIDE REMOTO MANUAL	ISOLAR TANQUE PARA MANUTENÇÃO	- VAZAMENTO	INJEÇÃO DE EMERGÊNCIA	PERDA DO INVENTÁRIO DO TANQUE	IMPOSSIBILITA A ATUAÇÃO DESTE TANQUE NUM APRGR	NÃO ACARRETA MAIORES PROBLEMAS NO CASO DE UM APRGR	NÍVEL DO TANQUE DE COMPENSAÇÃO	HV 0712 E HV 0714 (*)	IV	
HV 0713	VÁLVULA GAVETA NORMAL. FECHADA	PERMITIR INJEÇÃO PELOS TANQUES DE COMPENSAÇÃO	- NÃO ABRE - ABRE PARCIALMENTE	INJEÇÃO DE EMERGÊNCIA	NÃO DÁ PASSAGEM	EXIGE ATUAÇÃO DA VÁLVULA HV 0711	NÃO ACARRETA MAIORES PROBLEMAS NO CASO DE UM APRGR	PAINEL DE CONTROLE / INSPEÇÃO LOCAL	HV 0711	IV	
	ACIONAM. SOLENÓIDE REMOTO MANUAL	ISOLAR TANQUE PARA MANUTENÇÃO	- VAZAMENTO	INJEÇÃO DE EMERGÊNCIA	PERDA DO INVENTÁRIO DO TANQUE	IMPOSSIBILITA A ATUAÇÃO DESTE TANQUE NUM APRGR	NÃO ACARRETA MAIORES PROBLEMAS NO CASO DE UM APRGR	NÍVEL DO TANQUE DE COMPENSAÇÃO	HV 0712 E HV 0714 (*)	IV	

Tabela 1 – Análise tipo AMFE do SIE (tanques de compensação) – conclusão

Nº IDENT.	ITEM	FUNÇÃO	MODOS DE FALHA	MODO OPERACIONAL	EFEITOS DA FALHA			MÉTODO DE DETECÇÃO	RECURSOS DE COMPENSAÇÃO	CLASSE DE SEVERIDADE	OBS.
					LOCAIS	PROX. NÍVEL	NÍVEL FINAL				
UV 011	VÁLVULA DE RETENÇÃO TIPO PORTINHOLA	IMPEDIR FLUXO NO SENTIDO CONTRÁRIO	- NÃO FECHA	INJEÇÃO DE EMERGÊNCIA	PERMITE A PASSAGEM EM SENTIDO CONTRÁRIO	NÃO OCORRERÁ O FLUXO EM SENTIDO CONTRÁRIO DEVIDO À DIF. DE PRESSÃO	NÃO ACARRETA MAIORES PROBLEMAS NO CASO DE UM APRGR	NÃO HÁ	HV 0711 E HV 0713	IV	
			- VAZAMENTO	INJEÇÃO DE EMERGÊNCIA	PERDA DE PERDA DO INVENTÁRIO DO TANQUE	IMPOSSIBILITA A ATUAÇÃO DESTE TANQUE NUM APRGR	NÃO ACARRETA MAIORES PROBLEMAS NO CASO DE UM APRGR	NÍVEL DO TANQUE DE COMPENSAÇÃO	UV 012 (*)	IV	
			- VAZAMENTO	OPERAÇÃO NORMAL	PERDA DE REFRIGERANTE DO PRIMÁRIO	DESLIGAMENTO DO REATOR	ACIONAMENTO DO SIE	PRESSÃO NO PRIMÁRIO	NÃO HÁ	III	SCRAM

Tabela 2 – Análise tipo AMFE do SIE (acumuladores) – continua

Nº IDENT.	ITEM	FUNÇÃO	MODOS DE FALHA	MODO OPERACIONAL	EFEITOS DA FALHA			MÉTODO DE DETECÇÃO	RECURSOS DE COMPENSAÇÃO	CLASSE DE SEVERIDADE	OBS.
					LOCAIS	PROX. NÍVEL	NÍVEL FINAL				
2156-VP3	ACUMULADOR	ARMAZENAR ÁGUA BORADA PARA INJEÇÃO DE EMERGÊNCIA	- VAZAMENTO	INJEÇÃO DE EMERGÊNCIA	PERDA DO INVENTÁRIO DO ACUMULADOR	IMPOSSIBILITA A ATUAÇÃO DESTE ACUMULADOR NUM APRGR	NÃO ACARRETA MAIORES PROBLEMAS NO CASO DE UM APRGR	NÍVEL DO ACUMULADOR	VP4 (*)	IV	
4BA-2156 11-2G40	TUBULAÇÃO	TRANSPORTAR A ÁGUA BORADA DO ACUMULADOR PARA O BLOCO 40	- VAZAMENTO	INJEÇÃO DE EMERGÊNCIA	NÃO LEVA FLUIDO SUFICIENTE AO BLOCO 40	IMPOSSIBILITA A ATUAÇÃO DESTE ACUMULADOR NUM APRGR	NÃO ACARRETA MAIORES PROBLEMAS NO CASO DE UM APRGR	NÃO HÁ	12-2G40 (*)	IV	
UV 001	VÁLVULA DE RETENÇÃO TIPO PORTINHOLA	IMPEDIR FLUXO NO SENTIDO CONTRÁRIO	- NÃO FECHA	INJEÇÃO DE EMERGÊNCIA	PERMITE A PASSAGEM EM SENTIDO CONTRÁRIO	EXIGE ATUAÇÃO DA VÁLVULA UV 003	NÃO ACARRETA MAIORES PROBLEMAS NO CASO DE UM APRGR	NÃO HÁ	UV 003	IV	
			- VAZAMENTO	INJEÇÃO DE EMERGÊNCIA	PERDA DO INVENTÁRIO DO ACUMULADOR	IMPOSSIBILITA A ATUAÇÃO DESTE ACUMULADOR NUM APRGR	NÃO ACARRETA MAIORES PROBLEMAS NO CASO DE UM APRGR	NÃO HÁ	UV 002 (*)	IV	
			- NÃO FECHA	OPERAÇÃO NORMAL	PERMITE A PASSAGEM EM SENTIDO CONTRÁRIO	EXIGE ATUAÇÃO DA VÁLVULA UV 003	CONDIÇÃO LATENTE	NÃO HÁ	UV 003	IV	
			- VAZAMENTO	OPERAÇÃO NORMAL	PERDA DO INVENTÁRIO DO ACUMULADOR	EXIGE ATUAÇÃO DA VÁLVULA UV 003 PARA NÃO HAVER SCRAM	EXIGE PARADA PARA MANUTENÇÃO	NÍVEL DO ACUMULADOR	UV 003	III	SCRAM

Tabela 2 – Análise tipo AMFE do SIE (acumuladores) – conclusão

Nº IDENT.	ITEM	FUNÇÃO	MODOS DE FALHA	MODO OPERACIONAL	EFEITOS DA FALHA			MÉTODO DE DETECÇÃO	RECURSOS DE COMPENSAÇÃO	CLASSE DE SEVERIDADE	OBS.
					LOCAIS	PROX. NÍVEL	NÍVEL FINAL				
UV 003	VÁLVULA DE RETENÇÃO TIPO PORTINHOLA	IMPEDIR FLUXO NO SENTIDO CONTRÁRIO	- NÃO FECHA	INJEÇÃO DE EMERGÊNCIA	PERMITE A PASSAGEM EM SENTIDO CONTRÁRIO	EXIGE ATUAÇÃO DA VÁLVULA UV 001	NÃO ACARRETA MAIORES PROBLEMAS NO CASO DE UM APRGR	NÃO HÁ	UV 001	IV	
			- VAZAMENTO	INJEÇÃO DE EMERGÊNCIA	PERDA DO INVENTÁRIO DO ACUMULADOR	IMPOSSIBILITA A ATUAÇÃO DESTE ACUMULADOR NUM APRGR	NÃO ACARRETA MAIORES PROBLEMAS NO CASO DE UM APRGR	NÍVEL DO ACUMULADOR	UV 004 (*)	IV	
			- NÃO FECHA	OPERAÇÃO NORMAL	PERMITE A PASSAGEM EM SENTIDO CONTRÁRIO	EXIGE ATUAÇÃO DA VÁLVULA UV 001	CONDIÇÃO LATENTE	NÃO HÁ	UV 001	IV	
			- VAZAMENTO	OPERAÇÃO NORMAL	PERDA DO REFRIGERANTE DO PRIMÁRIO	ACIONAMENTO DA VÁLVULA HV 0771	EXIGE PARADA PARA MANUTENÇÃO	PRESÃO NO PRIMÁRIO	HV 0771	III	SCRAM
HV 0771	VÁLVULA GAVETA NORMAL. ABERTA ACIONAM. SOLENÓIDE REMOTO MANUAL	PERMITIR INJEÇÃO PELOS ACUMULADORES	- NÃO FECHA - PARCIALMENTE FECHADA	INJEÇÃO DE EMERGÊNCIA	DÁ PASSAGEM	PERMITE A ENTRADA DE NITROGÊNIO NO REFRIGERANTE	NÃO ACARRETA MAIORES PROBLEMAS NO CASO DE UM APRGR	PAINEL DE CONTROLE / INSPEÇÃO LOCAL	NÃO HÁ	IV	
			- VAZAMENTO	INJEÇÃO DE EMERGÊNCIA	PERDA DO INVENTÁRIO DO ACUMULADOR	IMPOSSIBILITA A ATUAÇÃO DESTE ACUMULADOR NUM APRGR	NÃO ACARRETA MAIORES PROBLEMAS NO CASO DE UM APRGR	NÃO HÁ	HV 0772 (*)	IV	
		ISOLAR ACUMULADOR DURANTE A PARTIDA / AQUECIMENTO DO SRR	- FECHAMENTO ESPÚRIO	INJEÇÃO DE EMERGÊNCIA	NÃO DÁ PASSAGEM	IMPOSSIBILITA A ATUAÇÃO DESTE ACUMULADOR NUM APRGR	NÃO ACARRETA MAIORES PROBLEMAS NO CASO DE UM APRGR	NÍVEL DO ACUMULADOR	HV 0772 (*)	IV	
			- VAZAMENTO	OPERAÇÃO NORMAL	PERDA DO REFRIGERANTE DO PRIMÁRIO	DESLIGAMENTO DO REATOR	ACIONAMENTO DO SIE	PRESÃO NO PRIMÁRIO	NÃO HÁ	III	SCRAM

Tabela 3 – Análise tipo AMFE do SIE (tanques de inundação) – continua

Nº IDENT.	ITEM	FUNÇÃO	MODOS DE FALHA	MODO OPERACIONAL	EFEITOS DA FALHA			MÉTODO DE DETECÇÃO	RECURSOS DE COMPENSAÇÃO	CLASSE DE SEVERIDADE	OBS.
					LOCAIS	PROX. NÍVEL	NÍVEL FINAL				
2156-VP5	TANQUE DE INUNDAÇÃO	ARMAZENAR ÁGUA BORADA PARA INJEÇÃO DE EMERGÊNCIA (E POR GRAVIDADE)	- VAZAMENTO	INJEÇÃO DE EMERGÊNCIA (E POR GRAVIDADE)	PERDA DO INVENTÁRIO DO TANQUE	PREJUDICA (OU IMPOSSIBILITA) A ATUAÇÃO DO SIE	NÚCLEO DO REATOR NÃO TOTALMENTE INUNDADO	VAZÃO NA LINHA DE INJEÇÃO	VP6 (*) SRCR	III	
HV 0775	VÁLVULA GAVETA NORMAL. ABERTA	PERMITIR TESTES DAS BOMBAS DE ALTA E DE BAIXA PRESSÃO	- FECHAMENTO ESPÚRIO	INUNDAÇÃO POR GRAVIDADE (FALHA DAS BIBP)	NÃO DÁ PASSAGEM	IMPOSSIBILITA A INJEÇÃO POR GRAVIDADE	NÚCLEO DO REATOR NÃO TOTALMENTE INUNDADO	PAINEL DE CONTROLE / INSPEÇÃO LOCAL	HV 0776 (*) SRCR	IV	
	ACIONAM. SOLENÓIDE REMOTO MANUAL	ISOLAR TANQUE PARA MANUTENÇÃO	- VAZAMENTO	INJEÇÃO DE EMERGÊNCIA (E POR GRAVIDADE)	PERDA DO INVENTÁRIO DO TANQUE	PREJUDICA (OU IMPOSSIBILITA) A ATUAÇÃO DO SIE	NÚCLEO DO REATOR NÃO TOTALMENTE INUNDADO	VAZÃO NA LINHA DE INJEÇÃO	HV 0776 (*) SRCR	III	
			- NÃO FECHA - PARCIALMENTE FECHADA	TESTES DAS BOMBAS E MANUTENÇÃO DO TANQUE	PERMITE A PASSAGEM	PREJUDICA TESTES DAS BOMBAS E MANUTENÇÃO DO TANQUE	NÃO HÁ	PAINEL DE CONTROLE / INSPEÇÃO LOCAL	HV 0776 (*)	IV	
UV 029	VÁLVULA DE RETENÇÃO TIPO PORTINHOLA	IMPEDIR FLUXO NO SENTIDO CONTRÁRIO	- NÃO FECHA	INJEÇÃO DE EMERGÊNCIA	PERMITE A PASSAGEM EM SENTIDO CONTRÁRIO	EXIGE ATUAÇÃO DA VÁLVULA UV 031	CONDIÇÃO LATENTE	NÃO HÁ	UV 031	IV	
			- VAZAMENTO	INJEÇÃO DE EMERGÊNCIA (E POR GRAVIDADE)	PERDA DO INVENTÁRIO DO TANQUE	PREJUDICA (OU IMPOSSIBILITA) A ATUAÇÃO DO SIE	NÚCLEO DO REATOR NÃO TOTALMENTE INUNDADO	VAZÃO NA LINHA DE INJEÇÃO	HV 0775 SRCR	III	
UV 031	VÁLVULA DE RETENÇÃO TIPO PORTINHOLA	IMPEDIR FLUXO NO SENTIDO CONTRÁRIO	- NÃO FECHA	INJEÇÃO DE EMERGÊNCIA	PERMITE A PASSAGEM EM SENTIDO CONTRÁRIO	EXIGE ATUAÇÃO DA VÁLVULA UV 029	CONDIÇÃO LATENTE	NÃO HÁ	UV 029	IV	
			- VAZAMENTO	INJEÇÃO DE EMERGÊNCIA (E POR GRAVIDADE)	PERDA DO INVENTÁRIO DO TANQUE	PREJUDICA (OU IMPOSSIBILITA) A ATUAÇÃO DO SIE	NÚCLEO DO REATOR NÃO TOTALMENTE INUNDADO	VAZÃO NA LINHA DE INJEÇÃO	HV 0775 SRCR	III	

Tabela 3 – Análise tipo AMFE do SIE (tanques de inundação) – continuação

Nº IDENT.	ITEM	FUNÇÃO	MODOS DE FALHA	MODO OPERACIONAL	EFEITOS DA FALHA			MÉTODO DE DETECÇÃO	RECURSOS DE COMPENSAÇÃO	CLASSE DE SEVERIDADE	OBS.
					LOCAIS	PROX. NÍVEL	NÍVEL FINAL				
UV 019	VÁLVULA GAVETA NORMAL. ABERTA ACIONAM. LOCAL MANUAL	ISOLAR BIAP PARA MANUTENÇÃO	- FECHAMENTO ESPÚRIO	INJEÇÃO DE EMERGÊNCIA PELA BIAP	NÃO DÁ PASSAGEM	IMPOSSIBILITA A INJEÇÃO PELA BIAP	AUMENTO DA PRESSÃO E TEMPERATURA NO BLOCO 40	MEDIDOR DE PRESSÃO NA SAÍDA DA BIAP	UV 020 (*) INJEÇÃO POR GRAVIDADE SRCR	IV	
			- VAZAMENTO	INJEÇÃO DE EMERGÊNCIA PELA BIAP	PERDA DO INVENTÁRIO DO TANQUE	PREJUDICA (OU IMPOSSIBILITA) A ATUAÇÃO DO SIE	NÚCLEO DO REATOR NÃO TOTALMENTE INUNDADO	NÍVEL DO TANQUE DE INUNDAÇÃO	UV 020 (*) SRCR	III	
			- NÃO FECHA - PARCIALMENTE FECHADA	MANUTENÇÃO DA BIAP	PERMITE A PASSAGEM	PREJUDICA A MANUTENÇÃO DA BIAP	NÃO HÁ	PAINEL DE CONTROLE/ INSPEÇÃO LOCAL	NÃO HÁ	IV	
2156-B1	BIAP (90 BAR) ACIONAM. SIS	INJEÇÃO DE EMERGÊNCIA A ALTA PRESSÃO	- NÃO BOMBEIA - BOMBEIA A UMA VAZÃO INFERIOR	INJEÇÃO DE EMERGÊNCIA PELA BIAP	VAZÃO INSUFICIENTE	PREJUDICA (OU IMPOSSIBILITA) A INJEÇÃO PELA BIAP	AUMENTO DA PRESSÃO E TEMPERATURA NO BLOCO 40	MEDIDOR DE PRESSÃO NA SAÍDA DA BIAP	B2 (*) INJEÇÃO POR GRAVIDADE SRCR	IV	
			- VAZAMENTO	INJEÇÃO DE EMERGÊNCIA PELA BIAP	PERDA DO INVENTÁRIO DO TANQUE	PREJUDICA (OU IMPOSSIBILITA) A ATUAÇÃO DO SIE	NÚCLEO DO REATOR NÃO TOTALMENTE INUNDADO	MEDIDOR DE PRESSÃO NA SAÍDA DA BIAP	UV 019 SRCR	III	
UV 017	VÁLVULA DE 3 VIAS NORMAL. ABERTA ACIONAM. MECÂNICO	RECIRCULAÇÃO DA BIAP	- FECHAMENTO ESPÚRIO	INJEÇÃO DE EMERGÊNCIA PELA BIAP	NÃO DÁ PASSAGEM	IMPOSSIBILITA A INJEÇÃO PELA BIAP	AUMENTO DA PRESSÃO E TEMPERATURA NO BLOCO 40	MEDIDOR DE PRESSÃO NA SAÍDA DA BIAP	UV 018 (*) INJEÇÃO POR GRAVIDADE SRCR	IV	
			- VAZAMENTO	INJEÇÃO DE EMERGÊNCIA PELA BIAP	PERDA DO INVENTÁRIO DO TANQUE	PREJUDICA (OU IMPOSSIBILITA) A ATUAÇÃO DO SIE	NÚCLEO DO REATOR NÃO TOTALMENTE INUNDADO	MEDIDOR DE VAZÃO NA LINHA	UV 019 SRCR	III	
UV 021	VÁLVULA GLOBO E RETENÇÃO NORMAL. ABERTA ACIONAM. LOCAL MANUAL	EVITAR RETORNO E ISOLAR A BIAP PARA MANUTENÇÃO	- FECHAMENTO ESPÚRIO	INJEÇÃO DE EMERGÊNCIA PELA BIAP	NÃO DÁ PASSAGEM	IMPOSSIBILITA A INJEÇÃO PELA BIAP	AUMENTO DA PRESSÃO E TEMPERATURA NO BLOCO 40	MEDIDOR DE VAZÃO NA LINHA	UV 022 (*) INJEÇÃO POR GRAVIDADE SRCR	IV	
			- VAZAMENTO	INJEÇÃO DE EMERGÊNCIA PELA BIAP	PERDA DO INVENTÁRIO DO TANQUE	PREJUDICA (OU IMPOSSIBILITA) A ATUAÇÃO DO SIE	NÚCLEO DO REATOR NÃO TOTALMENTE INUNDADO	MEDIDOR DE VAZÃO NA LINHA	UV 019 SRCR	III	
			- NÃO FECHA - PARCIALMENTE FECHADA	MANUTENÇÃO DA BIAP	PERMITE A PASSAGEM	PREJUDICA A MANUTENÇÃO DA BIAP	NÃO HÁ	MEDIDOR DE VAZÃO NA LINHA	UV 022 (*)	IV	

Tabela 3 – Análise tipo AMFE do SIE (tanques de inundação) – continuação

Nº IDENT.	ITEM	FUNÇÃO	MODOS DE FALHA	MODO OPERACIONAL	EFEITOS DA FALHA			MÉTODO DE DETECÇÃO	RECURSOS DE COMPENSAÇÃO	CLASSE DE SEVERIDADE	OBS.
					LOCAIS	PROX. NÍVEL	NÍVEL FINAL				
UV 023	VÁLVULA GAVETA NORMAL. ABERTA ACIONAM. LOCAL MANUAL	ISOLAR BIBP PARA MANUTENÇÃO	- FECHAMENTO ESPÚRIO	INJEÇÃO DE EMERGÊNCIA PELA BIBP	NÃO DÁ PASSAGEM	IMPOSSIBILITA A INJEÇÃO PELA BIBP	INJEÇÃO POR GRAVIDADE	MEDIDOR DE PRESSÃO NA SAÍDA DA BIBP	UV 024 (*) INJEÇÃO POR GRAVIDADE SRCR	IV	
			- VAZAMENTO	INJEÇÃO DE EMERGÊNCIA PELA BIBP	PERDA DO INVENTÁRIO DO TANQUE	PREJUDICA (OU IMPOSSIBILITA) A ATUAÇÃO DO SIE	NÚCLEO DO REATOR NÃO TOTALMENTE INUNDADO	NÍVEL DO TANQUE DE INUNDAÇÃO	UV 024 (*) SRCR	III	
			- NÃO FECHA - PARCIALMENTE FECHADA	MANUTENÇÃO DA BIBP	PERMITE A PASSAGEM	PREJUDICA A MANUTENÇÃO DA BIBP	NÃO HÁ	PAINEL DE CONTROLE/ INSPEÇÃO LOCAL	UV 024 (*)	IV	
2156-B3	BIBP (14 BAR) ACIONAM. SIS	INJEÇÃO DE EMERGÊNCIA A BAIXA PRESSÃO	- NÃO BOMBEIA - BOMBEIA A UMA VAZÃO INFERIOR	INJEÇÃO DE EMERGÊNCIA PELA BIBP	VAZÃO INSUFICIENTE	PREJUDICA (OU IMPOSSIBILITA) A INJEÇÃO PELA BIBP	INJEÇÃO POR GRAVIDADE	MEDIDOR DE PRESSÃO NA SAÍDA DA BIBP	B4 (*) INJEÇÃO POR GRAVIDADE SRCR	IV	
			- VAZAMENTO	INJEÇÃO DE EMERGÊNCIA PELA BIBP	PERDA DO INVENTÁRIO DO TANQUE	PREJUDICA (OU IMPOSSIBILITA) A ATUAÇÃO DO SIE	NÚCLEO DO REATOR NÃO TOTALMENTE INUNDADO	MEDIDOR DE PRESSÃO NA SAÍDA DA BIBP	UV 023 SRCR	III	
UV 027	VÁLVULA DE 3 VIAS NORMAL. ABERTA ACIONAM. MECÂNICO	RECIRCULAÇÃO DA BIBP	- FECHAMENTO ESPÚRIO	INJEÇÃO DE EMERGÊNCIA PELA BIBP	NÃO DÁ PASSAGEM	IMPOSSIBILITA A INJEÇÃO PELA BIBP	INJEÇÃO POR GRAVIDADE	MEDIDOR DE PRESSÃO NA SAÍDA DA BIBP	UV 028 (*) INJEÇÃO POR GRAVIDADE SRCR	IV	
			- VAZAMENTO	INJEÇÃO DE EMERGÊNCIA PELA BIBP	PERDA DO INVENTÁRIO DO TANQUE	PREJUDICA (OU IMPOSSIBILITA) A ATUAÇÃO DO SIE	NÚCLEO DO REATOR NÃO TOTALMENTE INUNDADO	MEDIDOR DE VAZÃO NA LINHA	UV 023 SRCR	III	
UV 025	VÁLVULA GLOBO E RETENÇÃO NORMAL. ABERTA ACIONAM. LOCAL MANUAL	EVITAR RETORNO E ISOLAR A BIBP PARA MANUTENÇÃO	- FECHAMENTO ESPÚRIO	INJEÇÃO DE EMERGÊNCIA PELA BIBP	NÃO DÁ PASSAGEM	IMPOSSIBILITA A INJEÇÃO PELA BIBP	INJEÇÃO POR GRAVIDADE	MEDIDOR DE VAZÃO NA LINHA	UV 026 (*) INJEÇÃO POR GRAVIDADE SRCR	III	
			- VAZAMENTO	INJEÇÃO DE EMERGÊNCIA PELA BIBP	PERDA DO INVENTÁRIO DO TANQUE	PREJUDICA (OU IMPOSSIBILITA) A ATUAÇÃO DO SIE	NÚCLEO DO REATOR NÃO TOTALMENTE INUNDADO	MEDIDOR DE VAZÃO NA LINHA	UV 023 SRCR	III	
			- NÃO FECHA - PARCIALMENTE FECHADA	MANUTENÇÃO DA BIBP	PERMITE A PASSAGEM	PREJUDICA A MANUTENÇÃO DA BIBP	NÃO HÁ	MEDIDOR DE VAZÃO NA LINHA	UV 026 (*)	IV	

Tabela 3 – Análise tipo AMFE do SIE (tanques de inundação) – continuação

Nº IDENT.	ITEM	FUNÇÃO	MODOS DE FALHA	MODO OPERACIONAL	EFEITOS DA FALHA			MÉTODO DE DETECÇÃO	RECURSOS DE COMPENSAÇÃO	CLASSE DE SEVERIDADE	OBS.
					LOCAIS	PROX. NÍVEL	NÍVEL FINAL				
6BA- -2156 22-2E50	TUBULAÇÃO	TRANSPORTAR A ÁGUA BORADA DO TANQUE DE INUNDAÇÃO PARA O BLOCO 40	- VAZAMENTO	INJEÇÃO DE EMERGÊNCIA (E POR GRAVIDADE)	NÃO LEVA FLUIDO SUFICIENTE AO BLOCO 40	PREJUDICA (OU IMPOSSIBILITA) A INJEÇÃO DE EMERGÊNCIA E POR GRAVIDADE	NÚCLEO DO REATOR NÃO TOTALMENTE INUNDADO	NÍVEL DE ÁGUA NO BLOCO 40	21-2E50 (*) SRCR	III	
HV 0752	VÁLVULA GAVETA NORMAL. FECHADA ACIONAM. SIS	POSSIBILITAR A INJEÇÃO DE EMERGÊNCIA (E POR GRAVIDADE)	- NÃO ABRE - PARCIALMENTE ABERTA	INJEÇÃO DE EMERGÊNCIA (E POR GRAVIDADE)	NÃO DÁ PASSAGEM (ADEQUADA)	BLOQUEIA UM TRECHO DA TUBULAÇÃO QUE TRANSPORTA ÁGUA BORADA	CONDIÇÃO LATENTE	PAINEL DE CONTROLE	HV 0754	IV	
			- VAZAMENTO	INJEÇÃO DE EMERGÊNCIA (E POR GRAVIDADE)	PERDA DO INVENTÁRIO DO TANQUE	PREJUDICA (OU IMPOSSIBILITA) A ATUAÇÃO DO SIE	NÚCLEO DO REATOR NÃO TOTALMENTE INUNDADO	NÍVEL DE ÁGUA NO BLOCO 40	HV 0751 (*)	III	
		VEDAR A CONTENÇÃO	- ABERTURA ESPÚRIA	OPERAÇÃO NORMAL	PERMITE A PASSAGEM	CONDIÇÃO LATENTE	CONDIÇÃO LATENTE	PAINEL DE CONTROLE	UV 066	IV	
			- VAZAMENTO	OPERAÇÃO NORMAL	PERDA DO INVENTÁRIO DO TANQUE	PREJUDICA (OU IMPOSSIBILITA) A INJEÇÃO DE EMERGÊNCIA E POR GRAVIDADE	CONDIÇÃO LATENTE (OPERAÇÃO NORMAL)	NÍVEL DO TANQUE DE INUNDAÇÃO/ INSPEÇÃO LOCAL	HV 0775	III	
HV 0754	IDEM	IDEM	IDEM	IDEM	IDEM	IDEM	IDEM	IDEM	HV 0752	IDEM	
			IDEM	IDEM	IDEM	IDEM	IDEM	IDEM	HV 0753 (*)	IDEM	
		IDEM	IDEM	IDEM	IDEM	IDEM	IDEM	IDEM	IDEM	IDEM	
			IDEM	IDEM	IDEM	IDEM	IDEM	IDEM	IDEM	IDEM	
UV 066	VÁLVULA DE RETENÇÃO TIPO PORTINHOLA	VEDAR A CONTENÇÃO	- NÃO FECHA	OPERAÇÃO NORMAL	PERMITE A PASSAGEM	CONDUZ O FLUIDO FORA DA CONTENÇÃO	CONDIÇÃO LATENTE	NÃO HÁ	HV 0752 E HV 0754	IV	
			- VAZAMENTO	OPERAÇÃO NORMAL	PERMITE A PASSAGEM P/ FORA DA LINHA	VAZAMENTO INTERNO À CONTENÇÃO	CONDIÇÃO LATENTE	NÃO HÁ	HV 0752 E HV 0754	IV	
		POSSIBILITAR A INJEÇÃO DE EMERGÊNCIA (E POR GRAVIDADE)	- VAZAMENTO	INJEÇÃO DE EMERGÊNCIA (E POR GRAVIDADE)	PERDA DO INVENTÁRIO DO TANQUE	PREJUDICA (OU IMPOSSIBILITA) A ATUAÇÃO DO SIE	NÚCLEO DO REATOR NÃO TOTALMENTE INUNDADO	NÍVEL DE ÁGUA NO BLOCO 40	UV 067 (*) SRCR	III	

Tabela 3 – Análise tipo AMFE do SIE (tanques de inundação) – continuação

Nº IDENT.	ITEM	FUNÇÃO	MODOS DE FALHA	MODO OPERACIONAL	EFEITOS DA FALHA			MÉTODO DE DETECÇÃO	RECURSOS DE COMPENSAÇÃO	CLASSE DE SEVERIDADE	OBS.
					LOCAIS	PROX. NÍVEL	NÍVEL FINAL				
HV 0742	VÁLVULA GAVETA NORMAL. ABERTA ACIONAM. SIS	POSSIBILITAR A INJEÇÃO DE EMERGÊNCIA (E POR GRAVIDADE)	- FECHAMENTO ESPÚRIO	INJEÇÃO DE EMERGÊNCIA (E POR GRAVIDADE)	NÃO DÁ PASSAGEM	BLOQUEIA UM TRECHO DA TUBULAÇÃO QUE TRANSPORTA ÁGUA BORADA	CONDIÇÃO LATENTE	MEDIDOR DE PRESSÃO PT 0802	HV 0734 E UV 148 SRCR	IV	
			- VAZAMENTO	INJEÇÃO DE EMERGÊNCIA (E POR GRAVIDADE)	PERMITE A PASSAGEM P/ FORA DA LINHA	VAZAMENTO INTERNO À CONTENÇÃO	NÚCLEO DO REATOR NÃO TOTALMENTE INUNDADO	NÍVEL DE ÁGUA NO BLOCO 40	HV 0734 E UV 148 SRCR	III	
		VEDAR O BLOCO 40	- NÃO FECHA - PARCIALMENTE FECHADA	OPERAÇÃO NORMAL	PERMITE A PASSAGEM	NÃO ATUA COMO RESERVA DA VÁLVULA UV 160	CONDIÇÃO LATENTE	PAINEL DE CONTROLE	UV 160	IV	
			- VAZAMENTO	OPERAÇÃO NORMAL	PERMITE A PASSAGEM P/ FORA DA LINHA	VAZAMENTO INTERNO À CONTENÇÃO	CONDIÇÃO LATENTE	NÃO HÁ	UV 160	III	
UV 160	VÁLVULA DE RETENÇÃO TIPO PORTINHOLA	POSSIBILITAR A INJEÇÃO DE EMERGÊNCIA (E POR GRAVIDADE)	- VAZAMENTO	INJEÇÃO DE EMERGÊNCIA (E POR GRAVIDADE)	PERMITE A PASSAGEM P/ FORA DA LINHA	VAZAMENTO INTERNO AO BLOCO 40	ÁGUA NÃO PASSA ANTES PELO NÚCLEO DO REATOR	PRESSÃO E TEMPERATURA NO REATOR	HV 0734 E UV 148 SRCR	IV	
		VEDAR O BLOCO 40	- NÃO FECHA	OPERAÇÃO NORMAL	PERMITE A PASSAGEM	EXIGE ATUAÇÃO DA VÁLVULA HV 0742	CONDIÇÃO LATENTE	MEDIDOR DE PRESSÃO PT 0802	HV 0742	IV	
			- VAZAMENTO	OPERAÇÃO NORMAL	PERMITE A PASSAGEM P/ FORA DA LINHA	VAZAMENTO INTERNO AO BLOCO 40	DESLIGAMENTO DO REATOR	MEDIDOR DE PRESSÃO, NÍVEL E RADIO-ATIVIDADE	UV 159 (*)	III	SCRAM

Tabela 3 – Análise tipo AMFE do SIE (tanques de inundação) – conclusão

Nº IDENT.	ITEM	FUNÇÃO	MODOS DE FALHA	MODO OPERACIONAL	EFEITOS DA FALHA			MÉTODO DE DETECÇÃO	RECURSOS DE COMPENSAÇÃO	CLASSE DE SEVERIDADE	OBS.
					LOCAIS	PROX. NÍVEL	NÍVEL FINAL				
HV 0734	VÁLVULA GAVETA NORMAL. FECHADA ACIONAM. SIS	POSSIBILITAR A INJEÇÃO DE EMERGÊNCIA (E POR GRAVIDADE)	- NÃO ABRE - PARCIALMENTE ABERTA	INJEÇÃO DE EMERGÊNCIA (E POR GRAVIDADE)	NÃO DÁ PASSAGEM (ADEQUADA)	BLOQUEIA UM TRECHO DA TUBULAÇÃO QUE TRANSPORTA ÁGUA BORADA	CONDIÇÃO LATENTE	MEDIDOR DE PRESSÃO PT 0802	HV 0742 E UV 160 SRCR	IV	
			- VAZAMENTO	INJEÇÃO DE EMERGÊNCIA (E POR GRAVIDADE)	PERMITE A PASSAGEM P/ FORA DA LINHA	VAZAMENTO INTERNO À CONTENÇÃO	NÚCLEO DO REATOR NÃO TOTALMENTE INUNDADO	NÍVEL DE ÁGUA NO BLOCO 40	HV 0742 E UV 160 SRCR	III	
		VEDAR O BLOCO 40	- ABERTURA ESPÚRIA	OPERAÇÃO NORMAL	PERMITE A PASSAGEM	EXIGE ATUAÇÃO DA VÁLVULA UV 148	CONDIÇÃO LATENTE	PAINEL DE CONTROLE	UV 148	IV	
			- VAZAMENTO	OPERAÇÃO NORMAL	PERMITE A PASSAGEM P/ FORA DA LINHA	VAZAMENTO INTERNO À CONTENÇÃO	CONDIÇÃO LATENTE	NÃO HÁ	UV 148	III	
UV 148	VÁLVULA DE RETENÇÃO TIPO PORTINHOLA	POSSIBILITAR A INJEÇÃO DE EMERGÊNCIA (E POR GRAVIDADE)	- VAZAMENTO	INJEÇÃO DE EMERGÊNCIA (E POR GRAVIDADE)	PERMITE A PASSAGEM P/ FORA DA LINHA	VAZAMENTO INTERNO AO BLOCO 40	ÁGUA NÃO PASSA ANTES PELO NÚCLEO DO REATOR	PRESSÃO E TEMPERATURA NO REATOR	HV 0742 E UV 160 SRCR	IV	
		VEDAR O BLOCO 40	- NÃO FECHA	OPERAÇÃO NORMAL	PERMITE A PASSAGEM	EXIGE ATUAÇÃO DA VÁLVULA HV 0734	CONDIÇÃO LATENTE	MEDIDOR DE PRESSÃO PT 0802	HV 0734	IV	
			- VAZAMENTO	OPERAÇÃO NORMAL	PERMITE A PASSAGEM P/ FORA DA LINHA	VAZAMENTO INTERNO AO BLOCO 40	DESLIGAMENTO DO REATOR	MEDIDOR DE PRESSÃO, NÍVEL E RADIO-ATIVIDADE	UV 147 (*)	III	SCRAM

Tabela 4 – Análise tipo AMFE do SIE (linha de equalização de pressão) – continua

Nº IDENT.	ITEM	FUNÇÃO	MODOS DE FALHA	MODO OPERACIONAL	EFEITOS DA FALHA			MÉTODO DE DETECÇÃO	RECURSOS DE COMPENSAÇÃO	CLASSE DE SEVERIDADE	OBS.
					LOCAIS	PROX. NÍVEL	NÍVEL FINAL				
HV 0763	VÁLVULA GAVETA NORMAL. FECHADA ACIONAM. SIS (FALHA BIBP)	VEDAR A CONTENÇÃO	- ABERTURA ESPÚRIA	OPERAÇÃO NORMAL	NÃO VEDA	PERMITE A PASSAGEM DE AR PARA FORA DA CONTENÇÃO	CONDIÇÃO LATENTE	PAINEL DE CONTROLE	HV 0759 E HV 0767	IV	
			- VAZAMENTO	OPERAÇÃO NORMAL	PERMITE A PASSAGEM P/ FORA DA LINHA	PERMITE A PASSAGEM DE AR PARA FORA DO BLOCO 40	CONDIÇÃO LATENTE	MEDIDOR DE RADIOATIVIDADE NA CONTENÇÃO	HV 0759 E HV 0767	III	
		POSSIBILITAR EQUALIZAÇÃO DE PRESSÃO	- NÃO ABRE - PARCIALMENTE ABERTA	INUNDAÇÃO POR GRAVIDADE (FALHA DAS BIBP)	NÃO DÁ PASSAGEM (ADEQUADA)	EXIGE ABERTURA DA VÁLVULA HV 0769	CONDIÇÃO LATENTE	PAINEL DE CONTROLE	HV 0769 SRCR	IV	
			- VAZAMENTO	INUNDAÇÃO POR GRAVIDADE (FALHA DAS BIBP)	PERMITE A PASSAGEM P/ FORA DA LINHA	TANQUE COM PRESSÃO INSUFICIENTE	IMPOSSIBILITA INJEÇÃO POR GRAVIDADE	MEDIDOR DE PRESSÃO NO TANQUE	HV 0764 (*) SRCR	III	
HV 0769	IDEM	IDEM	IDEM	IDEM	IDEM	IDEM	IDEM	IDEM	IDEM	IDEM	
			IDEM	IDEM	IDEM	IDEM	IDEM	IDEM	IDEM	IDEM	
		IDEM	IDEM	IDEM	IDEM	IDEM (HV 0763)	IDEM	IDEM	HV 0763	IDEM	
			IDEM	IDEM	IDEM	IDEM	IDEM	IDEM	HV 0766 (*)	IDEM	
HV 0759	VÁLVULA GAVETA NORMAL. FECHADA ACIONAM. SIS (FALHA BIBP)	VEDAR A CONTENÇÃO	- ABERTURA ESPÚRIA	OPERAÇÃO NORMAL	NÃO VEDA	PERMITE A PASSAGEM DE AR PARA O TANQUE DE INUNDAÇÃO	CONDIÇÃO LATENTE	PAINEL DE CONTROLE	HV 0763 E HV 0769 RESPIRO	IV	
			- VAZAMENTO	OPERAÇÃO NORMAL	PERMITE A PASSAGEM P/ FORA DA LINHA	PERMITE A PASSAGEM DE AR PARA O PRÉDIO	CONDIÇÃO LATENTE	MEDIDOR DE RADIOATIVIDADE NO PRÉDIO DO REATOR	HV 0763 E HV 0769	III	
		POSSIBILITAR EQUALIZAÇÃO DE PRESSÃO	- NÃO ABRE - PARCIALMENTE ABERTA	INUNDAÇÃO POR GRAVIDADE (FALHA DAS BIBP)	NÃO DÁ PASSAGEM (ADEQUADA)	EXIGE ABERTURA DA VÁLVULA HV 0767	CONDIÇÃO LATENTE	PAINEL DE CONTROLE	HV 0767 SRCR	IV	
			- VAZAMENTO	INUNDAÇÃO POR GRAVIDADE (FALHA DAS BIBP)	PERMITE A PASSAGEM P/ FORA DA LINHA	TANQUE COM PRESSÃO INSUFICIENTE	IMPOSSIBILITA INJEÇÃO POR GRAVIDADE	MEDIDOR DE PRESSÃO NO TANQUE	HV 0760 (*) SRCR	III	
HV 0767	IDEM	IDEM	IDEM	IDEM	IDEM	IDEM	IDEM	IDEM	IDEM	IDEM	
			IDEM	IDEM	IDEM	IDEM	IDEM	IDEM	IDEM	IDEM	
		IDEM	IDEM	IDEM	IDEM	IDEM (HV 0759)	IDEM	IDEM	HV 0759	IDEM	
			IDEM	IDEM	IDEM	IDEM	IDEM	IDEM	HV 0768 (*)	IDEM	

Tabela 4 – Análise tipo AMFE do SIE (linha de equalização de pressão) – conclusão

Nº IDENT.	ITEM	FUNÇÃO	MODOS DE FALHA	MODO OPERACIONAL	EFEITOS DA FALHA			MÉTODO DE DETECÇÃO	RECURSOS DE COMPENSAÇÃO	CLASSE DE SEVERIDADE	OBS.
					LOCAIS	PROX. NÍVEL	NÍVEL FINAL				
PSV 0690	VÁLVULA DE ALÍVIO	ALIVIAR EVENTUAL SOBREPRESSÃO NO TANQUE DE INUNDAÇÃO	- NÃO ABRE	OPERAÇÃO NORMAL E INJEÇÃO DE EMERGÊNCIA	NÃO DÁ PASSAGEM	SAÍDA DE AR DO TANQUE PELO RESPIRO	CONDIÇÃO LATENTE	PAINEL DE CONTROLE	RESPIRO	IV	
	ACIONAM. MECÂNICO		- ABERTURA ESPÚRIA - VAZAMENTO	INUNDAÇÃO POR GRAVIDADE (FALHA DAS BIBP)	NÃO VEDA	PREJUDICA (OU IMPOSSIBILITA) A INJEÇÃO POR GRAVIDADE	NÚCLEO DO REATOR NÃO TOTALMENTE INUNDADO	PAINEL DE CONTROLE/ INSPEÇÃO LOCAL	PSV 689 (*) SRCR	III	
PSV 0694	VÁLVULA QUEBRA-VÁCUO	EVITAR A OCORRÊNCIA DE VÁCUO NO TANQUE DE INUNDAÇÃO	- NÃO ABRE	OPERAÇÃO NORMAL E INJEÇÃO DE EMERGÊNCIA	NÃO DÁ PASSAGEM	ENTRADA DE AR NO TANQUE PELO RESPIRO	CONDIÇÃO LATENTE	PAINEL DE CONTROLE	RESPIRO	IV	
	ACIONAM. MECÂNICO			INUNDAÇÃO POR GRAVIDADE (FALHA DAS BIBP)	NÃO DÁ PASSAGEM	PREJUDICA A ENTRADA DE AR NO TANQUE	PREJUDICA A INJEÇÃO POR GRAVIDADE	PAINEL DE CONTROLE	PSV 699 (*) SRCR	III	
			- ABERTURA ESPÚRIA - VAZAMENTO	INUNDAÇÃO POR GRAVIDADE (FALHA DAS BIBP)	NÃO VEDA	PREJUDICA (OU IMPOSSIBILITA) A INJEÇÃO POR GRAVIDADE	NÚCLEO DO REATOR NÃO TOTALMENTE INUNDADO	PAINEL DE CONTROLE	PSV 699 (*) SRCR	III	

Tabela 5 – Análise tipo AMFE do SRCR – continua

Nº IDENT.	ITEM	FUNÇÃO	MODOS DE FALHA	MODO OPERACIONAL	EFEITOS DA FALHA			MÉTODO DE DETECÇÃO	RECURSOS DE COMPENSAÇÃO	CLASSE DE SEVERIDADE	OBS.
					LOCAIS	PROX. NÍVEL	NÍVEL FINAL				
N/C	COLETOR	DRENAR A ÁGUA EXISTENTE NO PISO DO BLOCO 40 E DIRECIONÁ-LA AO SRCR	- ENTUPIMENTO	REMOÇÃO DE CALOR RESIDUAL	NÃO DRENA	NÃO ABASTECE O SRCR	IMPEDE A REMOÇÃO DE CALOR RESIDUAL	NÃO HÁ	NÃO HÁ	III	
UV 035	VÁLVULA DE RETENÇÃO TIPO PORTINHOLA	IMPEDIR FLUXO NO SENTIDO CONTRÁRIO	- VAZAMENTO	REMOÇÃO DE CALOR RESIDUAL	DERRAMAMENTO DO FLUIDO REFRIGERANTE NO COLETOR	O FLUIDO SERÁ RECOLETADO	NÃO ACARRETA MAIORES PROBLEMAS NO CASO DE UM APRGR	NÃO HÁ	UV 036 (*)	IV	
6ADR-2156-29-1G70	TUBULAÇÃO	TRANSPORTAR O FLUIDO DO COLETOR PARA O NÚCLEO DO REATOR	- VAZAMENTO PARA FORA DO BLOCO 40	REMOÇÃO DE CALOR RESIDUAL	PERDA DE FLUIDO REFRIGERANTE	DIMINUIÇÃO DO ESTOQUE DE REFRIGERANTE	PREJUDICA O DESEMPENHO DO SRCR	NÃO HÁ	30-1G70 (*)	III	
HV 0725	VÁLVULA GAVETA NORMAL. FECHADA	PERMITIR INJEÇÃO DE REFRIGERANTE NO NÚCLEO DO REATOR	- NÃO ABRE - ABRE PARCIALMENTE	REMOÇÃO DE CALOR RESIDUAL	NÃO DÁ PASSAGEM	IMPOSSIBILITA A INJEÇÃO POR ESTA LINHA	EXIGE A ATUAÇÃO DA OUTRA LINHA PARA QUE O SRCR POSSA ATUAR	PAINEL DE CONTROLE / INSPEÇÃO LOCAL	OUTRA LINHA	IV	
	ACIONAM. SOLENÓIDE REMOTO MANUAL	ISOLAR LINHA PARA MANUTENÇÃO	- VAZAMENTO	REMOÇÃO DE CALOR RESIDUAL	PERDA DE FLUIDO REFRIGERANTE	DIMINUIÇÃO DO ESTOQUE DE REFRIGERANTE	PREJUDICA O DESEMPENHO DO SRCR	NÃO HÁ	ISOLAR A LINHA	III	
2156-B5	BOMBA DE CIRCULAÇÃO DE REFRIGERANTE	BOMBEAR O FLUIDO PARA O TROCADOR DE CALOR	- NÃO BOMBEIA - BOMBEIA A UMA VAZÃO INFERIOR	REMOÇÃO DE CALOR RESIDUAL	NÃO DÁ PASSAGEM	IMPOSSIBILITA A INJEÇÃO POR ESTA LINHA	EXIGE A ATUAÇÃO DA OUTRA LINHA PARA QUE O SRCR POSSA ATUAR	MEDIDOR DE PRESSÃO NA SAÍDA DA BOMBA	B6 (*)	IV	
			- VAZAMENTO	REMOÇÃO DE CALOR RESIDUAL	PERDA DE FLUIDO REFRIGERANTE	DIMINUIÇÃO DO ESTOQUE DE REFRIGERANTE	PREJUDICA O DESEMPENHO DO SRCR	MEDIDOR DE PRESSÃO NA SAÍDA DA BIBP	ISOLAR A LINHA	III	
UV 037	VÁLVULA DE RETENÇÃO TIPO PORTINHOLA	IMPEDIR FLUXO NO SENTIDO CONTRÁRIO	- VAZAMENTO	REMOÇÃO DE CALOR RESIDUAL	PERDA DE FLUIDO REFRIGERANTE	DIMINUIÇÃO DO ESTOQUE DE REFRIGERANTE	PREJUDICA O DESEMPENHO DO SRCR	MEDIDOR DE VAZÃO NA SAÍDA DA BOMBA	ISOLAR A LINHA	III	

Tabela 5 – Análise tipo AMFE do SRCR – continuação

Nº IDENT.	ITEM	FUNÇÃO	MODOS DE FALHA	MODO OPERACIONAL	EFEITOS DA FALHA			MÉTODO DE DETECÇÃO	RECURSOS DE COMPENSAÇÃO	CLASSE DE SEVERIDADE	OBS.
					LOCAIS	PROX. NÍVEL	NÍVEL FINAL				
HV 0735	VÁLVULA GAVETA NORMAL. ABERTA	ISOLAR TROCADOR PARA MANUTENÇÃO	- FECHAMENTO ESPÚRIO	REMOÇÃO DE CALOR RESIDUAL	NÃO DÁ PASSAGEM	IMPOSSIBILITA O RESFRIAMENTO DO FLUIDO REFRIGERANTE	EXIGE A ATUAÇÃO DA OUTRA LINHA PARA QUE O SRCR POSSA ATUAR	MEDIDOR DE VAZÃO NA SAÍDA DA BOMBA	ISOLAR A LINHA	IV	
	- VAZAMENTO		REMOÇÃO DE CALOR RESIDUAL	PERDA DE FLUIDO REFRIGERANTE	DIMINUIÇÃO DO ESTOQUE DE REFRIGERANTE	PREJUDICA O DESEMPENHO DO SRCR	NÃO HÁ	ISOLAR A LINHA	III		
	- NÃO FECHA - PARCIALMENTE FECHADA		MANUTENÇÃO DO TROCADOR	PERMITE A PASSAGEM	PREJUDICA A MANUTENÇÃO DO TROCADOR	NÃO HÁ	PAINEL DE CONTROLE/ INSPEÇÃO LOCAL	NÃO HÁ	IV		
2156-TC1	TROCADOR DE CALOR	RESFRIAR O FLUIDO REFRIGERANTE	- VAZAMENTO	REMOÇÃO DE CALOR RESIDUAL	PERDA DE FLUIDO REFRIGERANTE	DIMINUIÇÃO DO ESTOQUE DE REFRIGERANTE	PREJUDICA O DESEMPENHO DO SRCR	NÃO HÁ	ISOLAR A LINHA	III	
			- INEFICIÊNCIA NA TROCA DE CALOR	REMOÇÃO DE CALOR RESIDUAL	REFRIGERANTE NÃO RESFRIA ADEQUADAMENTE	NÚCLEO DO REATOR NÃO RESFRIA ADEQUADAMENTE	PREJUDICA O DESEMPENHO DO SRCR	NÃO HÁ	NÃO HÁ	IV	
			- PROBLEMA NA CIRCULAÇÃO DA ÁGUA DE RESFRIAMENTO	REMOÇÃO DE CALOR RESIDUAL	REFRIGERANTE NÃO RESFRIA ADEQUADAMENTE	NÚCLEO DO REATOR NÃO RESFRIA ADEQUADAMENTE	PREJUDICA O DESEMPENHO DO SRCR	NÃO HÁ	NÃO HÁ	IV	
HV 0737	VÁLVULA GAVETA NORMAL. FECHADA	POSSIBILITAR O "BY PASS" DO TROCADOR DE CALOR	- VAZAMENTO	REMOÇÃO DE CALOR RESIDUAL	PERDA DE FLUIDO REFRIGERANTE	DIMINUIÇÃO DO ESTOQUE DE REFRIGERANTE	PREJUDICA O DESEMPENHO DO SRCR	NÃO HÁ	NÃO HÁ	III	
UV 033	VÁLVULA DE RETENÇÃO TIPO PORTINHOLA	IMPEDIR FLUXO NO SENTIDO CONTRÁRIO	- VAZAMENTO	REMOÇÃO DE CALOR RESIDUAL	PERDA DE FLUIDO REFRIGERANTE	DIMINUIÇÃO DO ESTOQUE DE REFRIGERANTE	PREJUDICA O DESEMPENHO DO SRCR	NÃO HÁ	NÃO HÁ	III	

Tabela 5 – Análise tipo AMFE do SRCR – conclusão

Nº IDENT.	ITEM	FUNÇÃO	MODOS DE FALHA	MODO OPERACIONAL	EFEITOS DA FALHA			MÉTODO DE DETECÇÃO	RECURSOS DE COMPENSAÇÃO	CLASSE DE SEVERIDADE	OBS.
					LOCAIS	PROX. NÍVEL	NÍVEL FINAL				
HV 0733	VÁLVULA GAVETA NORMAL. ABERTA	PERMITIR INJEÇÃO DE REFRIGERANTE NO NÚCLEO DO REATOR	- FECHAMENTO ESPÚRIO	REMOÇÃO DE CALOR RESIDUAL	NÃO DÁ PASSAGEM	IMPOSSIBILITA A INJEÇÃO POR ESTA LINHA	EXIGE A ATUAÇÃO DA OUTRA LINHA PARA QUE O SRCR POSSA ATUAR	PAINEL DE CONTROLE / INSPEÇÃO LOCAL	NÃO HÁ	IV	
	ACIONAM. SOLENÓIDE REMOTO MANUAL	ISOLAR LINHA PARA MANUTENÇÃO	- VAZAMENTO	REMOÇÃO DE CALOR RESIDUAL	PERDA DE FLUIDO REFRIGERANTE	DIMINUIÇÃO DO ESTOQUE DE REFRIGERANTE	PREJUDICA O DESEMPENHO DO SRCR	NÃO HÁ	ISOLAR A LINHA	III	
UV 147	VÁLVULA DE RETENÇÃO TIPO PORTINHOLA	IMPEDIR FLUXO NO SENTIDO CONTRÁRIO	- VAZAMENTO	REMOÇÃO DE CALOR RESIDUAL	PERDA DE FLUIDO REFRIGERANTE	DIMINUIÇÃO DO ESTOQUE DE REFRIGERANTE	PREJUDICA O DESEMPENHO DO SRCR	NÃO HÁ	NÃO HÁ	III	

4.3 ANÁLISE DOS RESULTADOS

Analisando-se o SRE pode-se observar que eventuais falhas nos tanques de compensação, nos acumuladores e nos componentes a eles interligados (para possibilitar seu funcionamento adequado) não apresentam maior gravidade, em função do reduzido volume de fluido refrigerante por eles armazenado e/ou do tempo de atuação dos mesmos em um APRGR, conforme podemos observar através da análise das figuras 10 e 11.

Figura 10 – Gráfico da pressão no pressurizador em função do tempo, a partir de um APRPGR no instante 100s (TAKESHI, 2004a).

Figura 11 – Gráfico da temperatura do refrigerante no reator em função do tempo, a partir de um APRPGR no instante 100s (TAKESHI, 2004a).

As únicas exceções ficam por conta de vazamentos nas válvulas UV 003, UV 011 e HV 0771, que em operação normal, podem ocasionar o desligamento do reator em virtude de queda na pressão do circuito primário, acarretando paradas desnecessárias e prejuízos com manutenções não programadas.

Prosseguindo a análise, pode-se verificar que um dos modos de falha mais graves do SRE é a perda de inventário de um dos tanques de inundação (seja ele por vazamento no tanque, na tubulação ou em seus componentes) mas, mesmo nesta circunstância, este tipo de acidente não implicaria em maior gravidade porque além da redundância da outra linha, temos o Subsistema de Remoção de Calor Residual, que recircula a água através do núcleo do reator até a temperatura de parada segura da instalação.

Sendo assim, podemos observar que um vazamento de grandes proporções da válvula HV 0775 teria o mesmo efeito da perda de um tanque de inundação, conforme visto acima.

As válvulas de retenção UV 029 e UV 031 têm a função de impedir o fluxo no sentido contrário e caso **ambas** apresentem falha por não fechamento pode haver problemas na injeção de emergência de um dos circuitos pelas bombas de alta e baixa pressão, com parte do fluido sendo bombeado novamente para o tanque de inundação (neste caso, a falha em apenas uma das válvulas gera uma condição latente). Por outro lado, se apenas uma destas válvulas falhar por vazamento (de grandes proporções) pode haver perda do inventário de um dos tanques, falha cuja severidade seria maior (nesse caso, a linha poderia ser isolada pelo fechamento da válvula HV 0775).

Passando para a análise da linha de injeção de alta pressão, pode-se observar que existe uma válvula de gaveta (UV 019), normalmente aberta, na entrada da bomba cujo objetivo é isolá-la para manutenção. Se houver um grande vazamento neste componente pode haver perda de inventário de um dos tanques de inundação, se a falha se der por fechamento espúrio ela impossibilita a injeção de alta pressão em um dos circuitos.

Se a falha ocorrer na própria bomba perde-se a injeção de alta pressão ou caso a falha seja devida a um grande vazamento na mesma pode ocorrer a perda de inventário do tanque de inundação de um dos circuitos, tendo-se como recurso para compensação, nesse caso, o fechamento da válvula UV 019.

Ainda na linha de injeção de alta pressão temos uma válvula de três vias, cuja função é permitir a recirculação da BIAP, podendo falhar por fechamento espúrio, impedindo a injeção de alta pressão ou por vazamento, acarretando a perda de inventário de um dos tanques, tendo-se como recurso para compensação, nesse caso também o fechamento da válvula UV 019.

O último componente dessa linha é uma válvula globo e retenção, normalmente aberta, cujo objetivo é evitar o retorno e isolar a BIAP para manutenção, que também pode falhar por fechamento espúrio, impossibilitando a injeção de alta em um dos circuitos ou por vazamento, ocasionando a perda de inventário de um dos tanques (contando como recurso para compensação o fechamento da válvula UV 019).

A linha de injeção de baixa pressão apresenta exatamente os mesmos componentes da linha de alta e, portanto, com os mesmos modos de falha e conseqüências descritos acima. A única diferença é que a severidade em caso de perda desta linha é maior, visto que a atuação das bombas de baixa no APRPGR é mais efetiva que a das de bombas de alta.

A falha da tubulação, por grande vazamento, apresenta os mesmos efeitos que uma falha deste tipo no tanque de inundação, com a exceção que em alguns pontos do sistema, como nas linhas de injeção de alta e baixa pressão, por exemplo, há recursos para compensação, o que não acontece com os tanques.

Prosseguindo-se com a análise, o próximo item é uma associação em paralelo de duas válvulas tipo gaveta, normalmente fechadas, cujo objetivo é vedar a contenção, durante a operação normal do sistema, e permitir a injeção de emergência e por gravidade, em caso de acidente.

Em operação normal estas válvulas podem falhar por abertura espúria, gerando uma condição latente que permitirá a passagem de fluido da contenção para o sistema (em caso de **falha conjunta** com a válvula UV 066) ou por vazamento, podendo ocasionar a perda de inventário de um dos tanques (em caso de grande ruptura), tendo como recurso para compensação, neste caso o fechamento da válvula HV 0775.

Já em condição de acidente, elas também poderão falhar por vazamento, acarretando perda do inventário de um dos tanques (mas, neste caso, sem recurso para compensação porque todo o fluido injetado na contenção, em caso de acidente, passa obrigatoriamente por estas duas válvulas) ou por não abrir (ou abrir parcialmente), tendo como recurso para compensação, neste caso, a válvula que está em paralelo a ela.

A seguir temos uma válvula de retenção, cuja função é a mesma da associação em paralelo descrita anteriormente e cuja falha em operação normal pode se dar por não fechar, permitindo a passagem de fluido para fora da contenção, com recurso de compensação das válvulas HV 0752 e HV 0754; ou por vazamento, gerando uma condição latente que, em caso de acidente, poderá acarretar a perda do inventário de um dos tanques de inundação, sem que haja recursos para compensação nesta linha.

Finalmente, no trecho de injeção de emergência, temos uma associação em paralelo de um conjunto de uma válvula de gaveta em série com uma válvula de retenção, cujo objetivo é vedar o compartimento do reator (Bloco 40), em operação normal, e possibilitar a injeção de emergência e por gravidade, em condição de acidente.

Em operação normal a válvula gaveta, normalmente aberta, pode falhar por vazamento gerando uma condição latente que permite passagem de fluido para fora do Bloco 40 (e tendo como recurso para compensação a válvula de retenção, que está em série a ela), ou por não fechar, neste caso falhando em atuar como reserva da válvula de retenção.

Em condição de acidente a falha neste componente pode se dar por fechamento espúrio, bloqueando este trecho da tubulação e tendo como único recurso para compensação, nesta linha, o outro trecho em paralelo; ou por vazamento, permitindo a passagem de fluido para fora da linha e sem recurso para compensação neste circuito, podendo ocasionar a perda de inventário de um dos tanques.

A válvula de retenção, em operação normal, pode falhar por vazamento, permitindo a passagem de fluido para fora da linha, acarretando perda de pressão no primário e o desligamento do reator ou por não fechar, exigindo a atuação da válvula HV 0742 para isolar o compartimento do reator. Em caso de acidente ela pode falhar por vazamento, ocasionando um vazamento interno ao Bloco 40 e fazendo com que a água borada de um dos tanques não passe pelo núcleo do reator, resfriando-o, antes de alagá-lo mas, se não houver falha conjunta do SRCR, o mesmo irá possibilitar a sua circulação pelo núcleo e seu resfriamento nos trocadores de calor.

A outra linha em paralelo apresenta os mesmos modos de falha e as mesmas conseqüências descritas, com a diferença que a válvula de gaveta desta linha é normalmente fechada e da anterior, normalmente aberta.

Na linha de equalização de pressão para injeção por gravidade, temos uma associação em paralelo de duas válvulas tipo gaveta, normalmente fechadas, em série com uma outra associação do mesmo tipo.

A função das válvulas da primeira associação em paralelo, em operação normal, é de vedar a contenção, podendo falhar por abertura espúria, possibilitando a passagem de fluido para fora dos limites da contenção mas

internamente a linha de equalização de pressão (tendo como recurso para compensação a outra associação em paralelo) ou vazamento, permitindo a passagem de ar para fora do Bloco 40 mas internamente à contenção.

Em caso de acidente, elas podem falhar por vazamento impedindo a equalização de pressão e por conseguinte a injeção por gravidade ou por não abrir após o comando que neste caso teria o recurso de compensação da válvula em paralelo (em caso de falha de **ambas** as válvulas, também prejudicando a injeção por gravidade em um circuito).

A função das válvulas da segunda associação em paralelo é idêntica a da primeira, assim como os modos de falha. Só mudam as fronteiras de escape do fluido nos casos de abertura espúria e vazamento, conforme descreve a Tabela 4, do item 4.2.

Nesse trecho há também comunicação com os tanques de inundação por intermédio da tubulação, cujas funções, modos de falha e conseqüências são os mesmos já listados na linha de injeção de emergência.

Há ainda duas válvulas tipo gaveta, normalmente abertas, associadas em série no respiro de cada tanque, cuja função em caso de acidente é fechá-lo para possibilitar a equalização de pressão, podendo falhar por vazamento (permitindo o escape de fluido proveniente da contenção para o prédio e impedindo a injeção por gravidade, através de um dos tanques) ou por não fechamento, com as mesmas conseqüências, só que neste último caso contando com o recurso para compensação da outra válvula em série. Pode ocorrer ainda a falha por fechamento espúrio, durante a operação normal do reator, bloqueando a saída pelo respiro do tanque, nesse caso eventuais problemas de sobrepressão do tanque seriam solucionados pela válvula de alívio.

Por fim, os tanques de inundação contam ainda com uma válvula de alívio e uma quebra-vácuo para sua proteção. As válvulas de alívio e quebra-vácuo podem falhar por vazamento ou por abertura espúria, prejudicando a injeção por gravidade em uma das linhas.

Quanto ao Subsistema de Remoção de Calor Residual (SRCR), suas falhas somente apresentarão maior gravidade caso tenha ocorrido falha no SIE. Se o núcleo do reator estiver, ao menos, parcialmente inundado a sua integridade estará preservada, independente da atuação do SRCR.

Assim, podemos inferir que as falhas no SRCR têm uma severidade menor que as do SIE e dentre as mais significativas podemos citar o entupimento do coletor ou falha em dois componentes-chave (um em cada linha), como por exemplo um trocador de calor e uma bomba, vazamento ou fechamento espúrio de duas válvulas, que façam parte do caminho crítico, etc..

Podemos observar que o SRE é inerentemente seguro, uma vez que mesmo que ocorra um evento capaz de impedir a utilização de uma linha do SIE (probabilidades de ocorrência extremamente baixas ($1,338 \times 10^{-5}$ para o SIE), conforme mostram OLIVEIRA ET AL. (2000)), há ainda o recurso da outra linha e do Subsistema de Remoção de Calor Residual.

5 CONCLUSÕES

O SRE é uma das últimas e mais importantes barreiras para mitigar as consequências de um dos piores acidentes, postulados, em uma instalação nuclear. Assim sendo é natural que algumas falhas apresentem elevada severidade (tendo-se em vista, contudo, que a sua probabilidade de ocorrência é extremamente baixa). Além disso, foi sempre considerado o pior caso, a favor da segurança, procurando minimizar a principal limitação da análise do tipo AMFE, que é a de não “enxergar” a degradação do sistema. Seguindo-se essa linha de raciocínio, as falhas em componentes com redundância foram analisadas conjuntamente com a falha no seu componente “reserva” procurando-se minimizar o efeito das falhas dependentes, através do aumento, nesses casos, da severidade da falha.

As principais recomendações para melhorias no sistema são:

- Afastar fisicamente os dois tanques de inundação para que um mesmo acidente, como o impacto de um objeto, não afete ambos simultaneamente;
- Comunicar as duas linhas de injeção e instalar válvulas na saída dos tanques, para proporcionar maior flexibilidade ao sistema e evitar a perda de inventário em caso de vazamentos;
- Procurar, sempre que possível, utilizar componentes redundantes de natureza diferente dos componentes da linha principal, para evitar que uma mesma condição adversa afete determinado item e seu sobressalente;
- Instalar um sistema de detecção de vazamentos ao longo de todo o sistema, evitando-se a ocorrência de “pontos cegos”;
- Realizar manutenção adequada e inspeções e testes regulares.

Convém lembrar que nem sempre é possível se colocar em prática sugestões como as mencionadas acima. Existem instalações nucleares onde o espaço é extremamente reduzido, sendo muitas vezes impraticável mudar um dos tanques de posição. Podem existir ainda variações extremas nas condições de operação do sistema, sendo que o mesmo deve se comportar de modo satisfatório em todas essas condições.

A comunicação das duas linhas pode ocasionar a probabilidade de perda de ambas, devendo ser, portanto, criteriosamente analisada e assim por diante.

Fica claro então que as recomendações variam conforme o caso mas existem algumas soluções para as quais não encontramos restrições e que valem para qualquer instalação como a realização de inspeções e teste regulares, manutenção adequada, componentes redundantes de natureza distinta e a instalação de um sistema de detecção de vazamentos em toda a linha.

Como recomendação para trabalhos futuros propõe-se a análise do tipo Árvore de Falhas do SRE, caso haja interesse em uma análise quantitativa do sistema. Nessa hipótese é fundamental a existência de um banco de dados de probabilidades de falha de equipamentos confiável e também atenção especial quanto ao problema de falhas dependentes.

Outra sugestão seria a execução de um HAZOP, como complemento a este trabalho. Nesta situação, será necessário trabalhar com o fluxograma de processo do sistema e os resultados estarão mais direcionados a falhas em procedimentos operacionais, havendo que se precaver quanto às limitações desta técnica, principalmente em relação ao “*layout*” do sistema, uma vez que o mesmo apresenta algumas características importantes dessa natureza como a altura dos tanques e acumuladores (acima do nível dos bocais do reator) e a localização dos equipamentos dentro ou fora do compartimento do reator, da contenção, etc.

REFERÊNCIAS BIBLIOGRÁFICAS

BOEING COMPANY; UNIVERSITY OF WASHINGTON. **System safety Symposium**. Seattle, WA, jun. 1965.

BRITISH STANDARDS INSTITUTION. Quality vocabulary. BS 4778, **BSI**, Londres, R.U., 1991a.

BRITISH STANDARDS INSTITUTION. Reliability of Systems, Equipment and Components, BS 5760, **BSI**, Londres, R.U., 1991b.

BURDICK, G.R.; FUSSELL, J.B.; RASMUSON, D.M.; WILSON, J.R. Phased mission analysis: a review of new developments and an application. **IEEE Trans. Reliab.**, R-26, p. 43, 1977.

BURK, A.F. **Strengthen process hazards reviews scientists**. Londres, R.U.: Chemical Engineering, 1992.

CENTER FOR CHEMICAL PROCESS SAFETY. **CCPS Guidelines**. Nova York, N.Y.: CCPS, 1992.

CENTRO TECNOLÓGICO da MARINHA em SÃO PAULO. **Relatório preliminar de análise de segurança**. São Paulo: CTMSP, 2007.

COVELLO, V.T. Social and behavioral research on risk: uses in risk management decision making. **Environ. Int.**, v. 10, p. 541, 1984.

DOUGLAS, M.; WILDAVSKY A. **Risk and culture**. Berkeley, CA: University of California Press, 1982.

DOUGLAS, M. Risk as a forensic resource. **Daedalus**, v. 119, n. 4, p. 1, 1990.

DOW CHEMICAL COMPANY. **Dow's fire and explosion index hazard classification guide**. Midland, MI.: Dow, 1994.

DUNCAN, R. C; YOUNGQUIST, W. The world petroleum life-cycle. In: THE PTTC WORKSHOP "OPEC OIL PRICING AND INDEPENDENT OIL PRODUCERS",

Oct. 22, 1998, Los Angeles. Disponível em <<http://www.dieoff.com/pg133.pdf>>. Acesso em 16 jun. 2008.

ECOBIDGE, Causes of global warming. Disponível em: <http://www.ecobridge.org/content/g_cse.htm>. Acesso em 16 jun. 2008.

ESARY, J.D.; ZIEHMS, H. Reliability analysis of phased missions. **SIAM**, p. 213 – 236, 1975.

FAIRLIE, H. Fear of living. **The new republic**, 23jan., p. 14 – 19, 1989.

FISCHHOFF, B.; LICHTENSTEIN, S.; SLOVIC, P.; DERBY, S.L.; KEENEY, R.L. **Acceptable risk**. Cambridge, R.U.: Cambridge University Press, 1981.

FROSDICK, S. The techniques of risk analysis are insufficient in themselves. **Disaster prevention and management** v.6, n. 3, p. 165 - 177, 1997.

FUSSEL, J.B. Generic techniques in systems reliability assessment - Fault tree analysis: concepts and techniques, **Noordhoff International Pub.**, p. 133 - 162, 1976.

HEALTH AND SAFETY EXECUTIVE. **The tolerability of risk from nuclear power stations**. Londres, R.U.: HM Stationery Office, 1988.

HEALTH AND SAFETY EXECUTIVE. **Human factors in industrial safety**. Londres, R.U.: HM Stationery Office, 1989.

HOOD, C.; ROTHSTEIN, H.; BALDWIN, R. The government of risk: understanding risk regulation regimes. **Oxford university Press**, 2001.

HYMAN, B. **Fundamentals of engineering design**. Upper Sadle River, N.J.: Prentice Hall, 1998.

Indústrias Nucleares do Brasil, Reservas de Urânio no Brasil. Disponível em: <<http://www.inb.com.br/reservasBrasil.asp>>. Acesso em 16 jun. 2008.

IVANHOE, L. F. Get ready for another oil shock!. **The Futurist**, jan.- fev., p. 20-23, 1997.

JONES, P.G. Computers in chemical plants, a need for safety awareness. **Hazards**, v. XI, p. 289, 1991.

KASPERSON, R; KASPERSON, J. Hidden hazards. Acceptable evidence: science and values in risk management, **Oxford University Press**, p. 9 - 28, 1991.

KAVIANIAN, H.R.; RAO, J.K.; BROWN G.V. **Application of hazard evaluation techniques to the design of potentially hazardous industrial chemical processes**. Cincinnati, OH: National Institute for Occupational Safety and Health, 1992.

KLETZ, T. A. Human problems with computer controlled plants. **Operations Prog.**, v. 1, p. 209, 1982.

KLETZ T.A. **Hazop and hazan**. 2.ed. Rugby, R.U.: Institution of Chemical Engineers, 1986.

KNOWLTON R.E. **A manual of hazard and operability studies**. Vancouver, B.C.: Chemetics International Company Ltd., 1992.

KUMAMOTO, H.; HENLEY, E.J. **Probabilistic risk assessment and management for engineers and scientists**. 2.ed. Nova York, N.Y.: IEEE Press, 1996.

LAHERÈÈRE, J. H. **Future sources of crude oil supply and quality considerations**. Rueil-Malmaison, France: DRI/Mc Graw-Hill/French Petroleum Institute, 1997.

LEES, F. P. **Loss prevention in the process industries: hazard identification, assessment and control**. 2.ed. Oxford, R.U.: Butterworth-Heinemann, 1996.

MACDONALD, D. **Practical hazops, trips and alarms**. Oxford, R.U.: Elsevier Inc., 2004.

MILITARY STANDARD – 1629A. **Procedures for performing a failure mode effects and criticality analysis**. Washington, DC: DEPARTMENT OF DEFENSE, 1980.

MILLER, R.L.; HOWARD, W.B. Management tools in loss prevention. **Major Loss Prevention**, p. 203, 1971.

MME, Dados sobre as matrizes energéticas brasileira (2007) e global (2005). Disponível em: <<http://www.mme.gov.br>>. Acesso em 16 jun. 2008.

MODÉ, L. Terceiro choque do petróleo já ameaça a economia mundial. **O Estado de São Paulo**, p. B1 e B4, 11 mai. 2008.

MORGAN, M.G. E HENRION, M. **Uncertainty: a guide to dealing with uncertainty in quantitative risk and policy analysis**. Nova York, N.Y.: Cambridge University Press, 1990.

MUHLBAUER, W.K. **Pipeline risk management. manual – ideas, techniques and resources**. 3 ed. Oxford, R.U.: Elsevier Inc., 2004.

NIELSEN D.S. **The cause-consequence diagram method as a basis for quantitative accident analysis**. Rep. Risö M – 1374. Risö, DM: Atom. Energy Comm., 1971.

NIELSEN D.S. **Use of cause-consequence charts in practical systems analysis**. Rep. Risö M – 1743. Risö, DM: Atom. Energy Comm., 1974.

NIELSEN D.S. Reliability and fault tree analysis theoretical and applied aspects of systems reliability and safety assessment: Use of cause-consequence charts in practical systems analysis, **Society for Industrial and Applied Mathematics**, p. 849 - 880, 1975.

OLIVEIRA, P.S.P.; JACQUES SAUER, M.E.L.; VIEIRA NETO, A.S.. **Análise de confiabilidade do sistema de resfriamento de emergência da INAP R11.99.8230-RA-04/00**. São Paulo: IPEN, 2000.

PRIEST, G. The new legal structure of risk control. **Daedalus**, v. 119, n. 4, p. 207 – 228, 1990.

ROACH, J.R.; LEES F.P. **Some features of and activities in hazard and operability (HAZOP) studies**. Londres, R.U.: Chemical Engineering, 1981.

ROYAL SOCIETY STUDY GROUP. **Risk: analysis, perception and management.** Londres, R.U.: RSSG, 1992.

SCHREIBER, A.M. **Using event trees and fault trees.** Londres, R.U.: Chemical Engineering, 1982.

SCOTT D.; CRAWLEY F. **Process plant design an operation.** Rugby, R.U.: Institution of Chemical Engineers, 1992.

SLOVIC, P. **Beyond Numbers: a broader perspective on risk perception and risk communication.** Oxford, R.U.: Oxford University Press, 1991.

SLOVIC, P. Trust, emotion, sex, politics and science: surveying the risk-assessment battlefield. **Risk Analysis**, n. 19, p. 689 – 701, 1999.

STARR, C. **Risk management, assessment and acceptability.** Knoxville, TN.: Society for risk analysis, 1984

TAKESHI, R.V.R. **Descrição do sistema de resfriamento de emergência R11.01-2156-MS-01.** São Paulo: CTMSP, 2004a.

TAKESHI, R.V.R. **Sistema de resfriamento de emergência – fluxograma de engenharia R11.01-2156-XE-001.** São Paulo: CTMSP, 2004b.

TAKESHI, R.V.R. **Sistema de resfriamento de emergência – fluxograma de processo R11.01-2156-XP-001.** São Paulo: CTMSP, 2004c.

TAYLOR J.R. **Sequential effects in failure mode analysis.** Rep. Risö M – 1470. Risö, DM: Atom. Energy Comm., 1974.

TAYLOR J.R. **Cause-consequence diagrams.** Urbino, Itália: Nato Advanced Study Inst. on Synthesis and Analysis Methods for Safety and Reliability Studies, 1978.

TAYLOR J.R. **A background to risk analysis** v. 1 – 4. Risö, DM: Risö Nat. Lab., 1979.

TOFT, B. The failure of hindsight. **Disaster prevention and management** v.1, n. 3, p. 48 - 59, 1992.

TOFT, B. Safety culture, **Centre for industrial safety and reliability - Cranfield University**, 13 jan., 1993.

TURNER, B. **Man-made disasters**, Londres, R.U.: Wykeham, 1978.

VESELY, W.E. **Analysis of fault trees by kinetic tree theory**. Rep IN – 1330. Idaho Falls, ID: Idaho Nucl. Corp., 1969.

VESELY, W.E. **Reliability and fault tree applications of NRTS**. Idaho Falls, ID: Idaho Nucl. Corp., 1970.

VILLAMÉA, L.; COSTA, O. Choque de realidade. **Isto é**, n. 2015, ano 31, p. 84-89, 2008.

WARNER, F. Calculated risks. **Science and Public Affairs**, inverno de 92, p. 44 – 49, 1992.

WILDAVSKY, A.; DAKE, K. Theories of risk perception: who fears what and why. **Daedalus**, v. 119, n. 4, p. 41 – 60, 1990.