



INSTITUTO DE PESQUISAS ENERGÉTICAS E NUCLEARES

Autarquia associada à Universidade de São Paulo

**Avaliação probabilística de segurança de projetos de sistemas elétricos de
instalações nucleares**

SAD SANDRINI BORSOI

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

**Orientador:
Prof. Dr. Miguel Mattar Neto**

**São Paulo
2022**

INSTITUTO DE PESQUISAS ENERGÉTICAS E NUCLEARES
Autarquia Associada à Universidade de São Paulo

**Avaliação probabilística de segurança de projetos de sistemas elétricos de
instalações nucleares**

Versão Corrigida

Versão Original disponível no IPEN

SAD SANDRINI BORSOI

**Dissertação apresentada como parte
dos requisitos para obtenção do
Grau de Mestre em Ciências na Área
de Tecnologia Nuclear - Reatores**

**Orientador:
Prof. Dr. Miguel Mattar Neto**

**São Paulo
2022**

Autorizo a reprodução e divulgação total ou parcial deste trabalho, para fins de estudo e pesquisa, desde que citada a fonte.

Como citar:

SANDRINI BORSOI, S. ***Avaliação probabilística de segurança de projetos de sistemas elétricos de instalações nucleares***. 2022. 165 f. Dissertação (Mestrado em Tecnologia Nuclear), Instituto de Pesquisas Energéticas e Nucleares, IPEN-CNEN, São Paulo. Disponível em: <<http://repositorio.ipen.br/>>
(data de consulta no formato: dd/mm/aaaa)

Ficha catalográfica elaborada pelo Sistema de geração automática da Biblioteca IPEN,
com os dados fornecidos pelo(a) autor(a).

SANDRINI BORSOI, SAD
Avaliação probabilística de segurança de projetos de sistemas elétricos de instalações nucleares / SAD SANDRINI BORSOI; orientador Miguel Mattar Neto. -- São Paulo, 2022.
165 f.

Dissertação (Mestrado) - Programa de Pós-Graduação em Tecnologia Nuclear (Reatores) -- Instituto de Pesquisas Energéticas e Nucleares, São Paulo, 2022.

1. Análise probabilística de segurança. 2. Sistemas elétricos de instalações nucleares. 3. Base normativa. 4. Projeto e licenciamento. 5. Instalações nucleares não convencionais. I. Mattar Neto, Miguel, orient. II. Título.

FOLHA DE APROVAÇÃO

Autor: Sad Sandrini Borsoi

Título: Avaliação probabilística de segurança de projetos de sistemas elétricos de instalações nucleares

Dissertação apresentada ao Programa de Pós-Graduação em Tecnologia Nuclear da Universidade de São Paulo para obtenção do título de Mestre em Ciências.

Data: 19/05/2022

Banca Examinadora

Prof. Dr.: Miguel Mattar Netto

Julgamento: aprovado

Instituição: Instituto de Pesquisas Energéticas e Nucleares (IPEN)

Prof. Dr.: José Roberto Castilho Piqueira

Julgamento: aprovado

Instituição: Escola Politécnica da Universidade de São Paulo (POLI – USP)

Prof. Dr.: Pedro Luiz da Cruz Saldanha

Julgamento: aprovado

Instituição: Instituto de Engenharia Nuclear (IEN)

À minha esposa e filhos pelo amor incondicional

AGRADECIMENTOS

Em especial, ao meu avô Antonio Carlos Borsoi, em memória, que nos deixou recentemente, por ter sido o espelho de bondade, fraternidade, amor e dedicação que me guiou e me inspirou ao longo de toda minha caminhada.

À minha querida esposa Vanessa pelo seu amor incondicional e por compreender minha dedicação ao projeto de pesquisa.

Aos meus filhos Bernardo e Benício que me motivam diariamente a seguir o caminho da sabedoria e do amor.

Ao meu professor orientador Dr. Miguel Mattar pela confiança e contribuições assertivas dadas durante todo o processo.

À minha coorientadora Dra. Patrícia Pagetti pela valiosa orientação técnica, dedicação e qualidade nas correções textuais, essenciais para que o trabalho fosse concluído satisfatoriamente.

Ao Dr. Marcos Maturana pelo companheirismo e orientação técnica voluntária que me guiaram nas escolhas do projeto.

Ao meu amigo Douglas Baroni pelo apoio técnico e motivacional, necessários para enfrentar os inúmeros desafios, sempre com espírito colaborativo.

Ao coordenador do Laboratório de Análise, Avaliação e Gerenciamento de Risco (LabRisco), Dr. Marcelo Martins, pela disponibilização dos recursos computacionais que subsidiaram o desenvolvimento deste trabalho.

À Marinha do Brasil por ter me concedido estes dois últimos anos para me dedicar exclusivamente ao projeto de pesquisa.

Também quero agradecer ao Instituto de Pesquisas Energéticas e Nucleares (IPEN/CNEN) e ao seu corpo docente que demonstrou estar comprometido com a qualidade e a excelência do ensino.

“Que os vossos esforços desafiem as impossibilidades, lembrai-vos de que as grandes coisas do homem foram conquistadas do que parecia impossível”.

Charles Chaplin

RESUMO

BORSOI, Sad S. **Avaliação probabilística de segurança de projetos de sistemas elétricos de instalações nucleares**. 2022. 165 p. Dissertação (Mestrado em Tecnologia Nuclear) – Instituto de Pesquisas Energéticas e Nucleares – IPEN/CNEN. São Paulo.

Este trabalho apresenta uma metodologia para avaliação de segurança de projetos de sistemas elétricos de instalações nucleares. A metodologia adota a frequência de dano ao núcleo como principal medida de risco para avaliar as diferentes arquiteturas dos sistemas de energia elétrica de uma instalação nuclear, subsidiando a seleção do projeto e o licenciamento destas instalações. Entre as motivações do trabalho está a ausência de uma base normativa que seja específica para o projeto de instalações nucleares que diferem das usinas nucleares de potência convencionais. A adoção de normas de usinas nucleares de potência para aplicação em outros tipos de instalações nucleares, nomeadas não convencionais, não leva em consideração suas particularidades funcionais e operacionais, impondo critérios muitas vezes superestimados, que podem acarretar, inclusive, em um aumento do risco financeiro para execução dos projetos. Nestes casos, análises probabilísticas de segurança tornam-se ferramentas imprescindíveis para o projeto e o licenciamento destas instalações nucleares. Como estudo de caso, considerou-se uma instalação nuclear não convencional com aplicações navais em que foram realizadas, no ambiente do software CAFTA, modelagens e quantificações das falhas dos sistemas responsáveis por garantir a segurança nuclear dessa instalação em modo de desligamento, durante uma parada para troca de combustíveis. Destaca-se neste estudo uma análise comparativa das possíveis configurações dos sistemas elétricos e a influência destas para o risco global da instalação. Como resultado, em função das particularidades funcionais, recomenda-se a revisão da base normativa das instalações nucleares não convencionais com aplicações navais.

Palavras-chave: Análise probabilística de segurança, risco, frequência de dano ao núcleo, segurança nuclear, base normativa, projeto, licenciamento, instalações nucleares não convencionais, sistemas elétricos, apagão de energia.

ABSTRACT

BORSOI, Sad S. **Probabilistic safety assessment of the design of electric power systems in nuclear installations**. 2022. 165 s. Master Thesis. (Master's Degree in Nuclear Technology) – Nuclear and Energy Research Institute – IPEN/CNEN. São Paulo.

This work presents a methodology for safety assessing of electric power systems design in nuclear installations. The methodology adopts core damage frequency as the main risk measure to evaluate distinct configurations of electric power systems of a nuclear installation, subsidizing design selection and installation licensing. One of the motivations of this work is the lack of a normative basis specific to the design of nuclear facilities that differ from conventional nuclear power plants design basis. Functional and operational particularities of non-conventional nuclear facilities tend not to be considered when conventional standards are adopted in the normative basis, leading to the application of criteria that are often overestimated and resulting in an increase in the financial risk of project deployment. In these cases, probabilistic safety analyses may be essential tools for the design and licensing of nuclear facilities. As a case study, the analysis of a non-conventional nuclear installation with naval applications was performed using CAFTA software, and modeling and quantification of safety systems failures in plant shutdown mode during the refueling outage were carried out. This study highlights the comparative analysis of possible configurations of electrical systems and their impact on the overall installation risk. As a result, it is recommended to review the normative basis in terms of the functional particularities of non-conventional nuclear installations with naval applications.

Keywords: Probabilistic safety analysis, risk, core damage frequency, nuclear safety, regulatory basis, design, licensing, non-conventional nuclear facilities, electric power systems, station blackout.

LISTA DE TABELAS

	Página
Tabela 1 – Componentes típicos dos sistemas elétricos de segurança.....	31
Tabela 2 – Modelo de probabilidade de falha para diferentes configurações do sistema....	65
Tabela 3 – Fator de causa comum para diferentes configurações de sistemas k-de-n.....	66
Tabela 4 – Fatores de falha de causa comum para componentes de diferentes configurações de sistema.....	67
Tabela 5 – Expressões de cálculo dos fatores de causa comum do modelo de múltiplas letras gregas	68
Tabela 6 – Métodos de cálculo da probabilidade de eventos básicos implementados no código computacional CAFTA.	73
Tabela 7 – Tipos de distribuição de incerteza da taxa de falha considerados no código computacional CAFTA.....	74
Tabela 8 – Alternativas de projetos do sistema elétrico CA simplificado.....	82
Tabela 9 – Resultado do risco para os projetos do sistema elétrico CA.....	86
Tabela 10 – Eventos básicos do projeto A com maiores contribuições para o risco.....	87
Tabela 11 – Eventos básicos do projeto B com maiores contribuições para o risco	87
Tabela 12 – Eventos básicos do projeto C com maiores contribuições para o risco.....	87
Tabela 13 – Eventos básicos do projeto D com maiores contribuições para o risco.....	87
Tabela 14 – Resultado do risco para os projetos do sistema elétrico CA – sem premissa de teste.....	89
Tabela 15 – Resultado do risco para os projetos do sistema elétrico CA – análise de sensibilidade DGEs.....	90
Tabela 16 – Resultado do risco para os projetos do sistema elétrico CA – análise de sensibilidade do sistema elétrico externo.....	91
Tabela 17 – Tipos de parada para instalações com reator tipo PWR no modo de desligamento.....	96
Tabela 18 – Fases do procedimento de troca de combustíveis de um protótipo em terra da propulsão naval.....	98
Tabela 19 – Alternativas de projeto do sistema elétrico da instalação estudada.....	109
Tabela 20 – Possíveis eventos iniciadores.....	110
Tabela 21 – Resultados do risco para a instalação medido pela Frequência de Dano ao Núcleo	

(CDF) considerando as alternativas de projeto do sistema elétrico.....	113
Tabela 22 – Contribuição dos sistemas para a Frequência de Dano ao Núcleo (CDF) da instalação considerando as alternativas de projeto do sistema elétrico.	114
Tabela 23 – Variação percentual do risco dos sistemas na comparação das alternativas de projeto do sistema elétrico em relação ao projeto A (original).....	114
Tabela 24 – Contribuição dos sistemas elétricos para o risco da instalação considerando as alternativas de projeto desses sistemas.	115
Tabela 25 – Variação percentual do risco associado aos sistemas elétricos comparando alternativas de projeto em relação ao projeto A (original).	115
Tabela 26 – Risco da instalação medido pela Frequência de Dano ao Núcleo devido a um evento de <i>Station Blackout</i>	116
Tabela 27 - Risco da instalação devido à perda do sistema elétrico externo (LOOP).	117
Tabela 28 – Eventos básicos com maiores contribuições para o CDF calculado para cada alternativa de projeto do sistema elétrico.	118
Tabela 29 – Eventos básicos de falhas do sistema elétrico do projeto A com maiores contribuições para o CDF.	119
Tabela 30 – Eventos básicos de falhas do sistema elétrico do projeto B com maiores contribuições para o CDF.	119
Tabela 31 – Eventos básicos de falhas do sistema elétrico do projeto C com maiores contribuições para o CDF.	120
Tabela 32 – Eventos básicos de falhas do sistema elétrico do projeto D com maiores contribuições para o CDF.	120
Tabela 33 – Resultado do risco para a instalação considerando manutenção/teste simultâneo de equipamentos do sistema elétrico para as alternativas de projeto analisadas.	122
Tabela 34 – Resultado do risco para a instalação associado ao <i>Station Blackout</i> considerando manutenção/teste simultâneo de equipamentos do sistema elétrico para as alternativas de projeto analisadas.....	122
Tabela 35 – Resultado do risco para a instalação considerando variações na taxa de falha dos DGEs para as alternativas de projeto analisadas.	123
Tabela 36 – Resultado do risco para a instalação associado ao <i>Station Blackout</i> considerando variações na taxa de falha dos DGEs para as alternativas de projeto analisadas.....	124
Tabela 37 – Resultado do risco para a instalação considerando variações na taxa de falha do sistema elétrico externo para as alternativas de projeto analisadas.	124
Tabela 38 – Resultado do risco para a instalação associado ao <i>Station Blackout</i> considerando	

variações na taxa de falha do sistema elétrico externo para as alternativas de projeto analisadas.....	125
Tabela 39 – Taxa de falha dos componentes.....	138
Tabela 40 – Taxa de falha do sistema elétrico externo.....	139
Tabela 41 – Taxa de falha de causa comum dos componentes.....	139
Tabela 42 – Cortes mínimos com maiores contribuições para o risco da instalação para as quatro alternativas de projeto do sistema elétrico.....	164

LISTA DE FIGURAS

	Página
Figura 1 – Fonte preferencial de energia de uma instalação e suas interfaces.	29
Figura 2 – Arquitetura do sistema elétrico de uma usina nuclear de potência em conformidade com os requisitos mínimos previstos no GDC 17.	30
Figura 3 – Categorias de eventos de perda do sistema elétrico externo de uma instalação.	33
Figura 4 – Resultados de Análises Probabilísticas de Segurança (APS) para o modo de desligamento de plantas americanas.	46
Figura 5 – Níveis da Análise Probabilística de Segurança (APS).	54
Figura 6 – Etapas da aplicação da APS Nível 1 para uma instalação.	55
Figura 7 – Exemplo ilustrativo de uma árvore de eventos.	57
Figura 8 – Estrutura fundamental da árvore de falhas de um sistema.	60
Figura 9 – Exemplo comparativo entre um diagrama de blocos de confiabilidade e uma árvore de falhas de um sistema simplificado.	61
Figura 10 – Árvore de falhas referente a uma configuração 2 de 3 componentes de um sistema.	63
Figura 11 – Árvore de falhas expandida em relação às falhas de causa comum associadas ao componente A.	64
Figura 12 – Grupo de componentes sujeitos a falha de causa comum (falha global).	66
Figura 13 – Interação entre o banco de dados e as árvores de falhas na arquitetura do código computacional CAFTA.	72
Figura 14 – Janela de edição dos dados de um evento básico apresentada no código computacional CAFTA.	74
Figura 15 – Processo de edição usado no CAFTA para quantificação da probabilidade do evento topo da árvore de falhas.	75
Figura 16 – Exemplo de funcionamento da ferramenta <i>Delete Term</i> implementada no CAFTA.	76
Figura 17 – Método de avaliação de projetos de sistemas elétricos.	78
Figura 18 – Diagrama ilustrativo do sistema elétrico CA simplificado.	81
Figura 19 – Árvore de eventos para o evento iniciador de perda do barramento de segurança A – alternativas de projeto A e D.	83
Figura 20 – Árvore de eventos para o evento iniciador de perda do barramento de segurança	

A – alternativas de projeto B e C.....	83
Figura 21 – Janelas de edição do banco de dados do evento básico LOOP2 no programa computacional CAFTA.....	85
Figura 22 – Importância dos eventos básicos de falha do sistema elétrico externo para o risco de cada projeto.	88
Figura 23 – Importância dos eventos básicos de falha dos DGEs para o risco de cada projeto.	89
Figura 24 – Protótipo da propulsão nuclear do submarino <i>Nautilus</i>	93
Figura 25 – Estruturas envolvidas durante a troca de combustíveis de um submarino nuclear.	93
Figura 26 – Sequência cronológica das fases de troca de combustíveis.....	99
Figura 27 – Sistema elétrico simplificado avaliado no estudo de caso.....	109
Figura 28 – Árvore de eventos do cenário %T1.	111
Figura 29 – Árvore de falhas do cenário %T2.....	111
Figura 30 – Importância dos sistemas para o risco associado a cada alternativa de projeto do sistema elétrico.	121
Figura 31 – Importância dos sistemas elétricos para o risco associado a cada alternativa de projeto.....	121
Figura 32 – Fluxograma de processo do Sistema de Remoção de Calor Residual – SRCR.	142
Figura 33 – Fluxograma de processo do Sistema de Água de Segurança - SAS – Parte 1.	143
Figura 34 – Fluxograma de processo do Sistema de Água de Segurança - SAS – Parte 2.	144
Figura 35 – Fluxograma de processo do Sistema de Resfriamento de Componentes do Primário – SRCP.....	145
Figura 36 – Fluxograma de processo do Sistema Primário de Resfriamento da Piscina de Estocagem de Combustíveis Irradiados – SPRP.....	146
Figura 37 – Fluxograma de processo do Sistema Secundário de Resfriamento da Piscina de Estocagem de Combustíveis Irradiados – SSRP.....	147
Figura 38 – Diagrama unifilar do Sistema Elétrico CA – Parte 1.	148
Figura 39 – Diagrama unifilar do Sistema Elétrico CA – Parte 2 (Barramentos de Emergência).	149
Figura 40 – Diagrama unifilar do Sistema Elétrico CC – Trem A.	150

Figura 41 – Diagrama unifilar do Sistema Elétrico CC (original) – Trem B.	151
Figura 42 – Diagrama unifilar do Sistema Elétrico CA Ininterrupto – Trem A.	152
Figura 43 – Diagrama unifilar do Sistema Elétrico CA Ininterrupto – Trem B.	153
Figura 44 – Árvore de falhas do evento iniciador BAR-A do projeto A do sistema elétrico.	154
Figura 45 – Árvore de falhas do evento subsequente BAR-B do projeto A do sistema elétrico.	155
Figura 46 – Árvore de falhas do evento subsequente AAC-1 do projeto A do sistema elétrico.	156
Figura 47 – Árvore de falhas do evento subsequente AAC-2 do projeto A do sistema elétrico.	157
Figura 48 – Árvore de falhas <i>master</i> (integradora) do projeto A do sistema elétrico.	158
Figura 49 – Árvore de falhas dos eventos mutuamente exclusivos de componentes do sistema elétrico.	159
Figura 50 – Árvore de falhas <i>master</i> da instalação em modo de desligamento para o projeto A (original) do sistema elétrico.	160
Figura 51 – Árvore de falhas <i>master</i> da instalação em modo de desligamento - Eventos topo do SRCR para o projeto A (original) do sistema elétrico.	161
Figura 52 – Árvore de falhas <i>master</i> da instalação em modo de desligamento - Eventos topo do SPRP para o projeto A (original) do sistema elétrico.	162
Figura 53 – Exemplo de ramo da árvore de falhas contendo eventos básicos do sistema elétrico CA do projeto A (original).	163

LISTA DE ABREVIATURAS E SIGLAS

AAC	<i>Alternate Alternating Current</i>
ACN	Área de Estocagem de Combustíveis Novos
AIEA	Agência Internacional de Energia Atômica
ANS	<i>American Nuclear Society</i>
ANSN	Autoridade Nacional de Segurança Nuclear
APS	Análise Probabilística de Segurança
CA	Corrente Alternada
CC	Corrente Contínua
CCCG	<i>Common Cause Component Group</i>
CCF	<i>Common Cause Failure</i>
CDF	<i>Core Damage Frequency</i>
CNEN	Comissão Nacional de Energia Nuclear
DGE	Diesel Gerador de Emergência
EUA	Estados Unidos da América
IEC	<i>International Electrotechnical Commission</i>
IEEE	<i>Institute of Electrical and Electronics Engineers</i>
FMEA	<i>Failure Mode and Effect Analysis</i>
GE	<i>General Electric</i>
HEP	<i>Human Error Probabilities</i>
INL	<i>Idaho National Laboratory</i>
IPEN	Instituto de Pesquisas Energéticas e Nucleares
I&C	Instrumentação e Controle
LERF	<i>Large Early Release Frequency</i>
LOOP	<i>Loss of Offsite Power</i>
LT	Linha de Transmissão
MGL	<i>Multiple Greek Letter</i>
MTC	Máquina de Troca de Combustíveis
NNSA	<i>National Nuclear Security Administration</i>
NSSS	<i>Nuclear Steam Supply System</i>
ONS	Operador Nacional do Sistema Elétrico
PECI	Piscina de Estocagem de Combustíveis Irrradiados
PPS	<i>Preferred Power Supply</i>

PWR	<i>Pressurized Water Reactor</i>
RIR	<i>Risk-Informed Regulation</i>
RCA	<i>Radio Corporation of America</i>
SAS	Sistema de Água de Segurança
SBO	<i>Station Blackout</i>
SEP	Sistema Elétrico de Potência
SMR	<i>Small Modular Reactors</i>
SPRP	Sistema Primário de Resfriamento da Piscina de Estocagem de Combustíveis Irradiados
SRMTC	Sistema de Resfriamento da Máquina de Troca de Combustíveis
SSRP	Sistema Secundário de Resfriamento da Piscina de Estocagem de Combustíveis Irradiados
SRCP	Sistema de Resfriamento de Componentes do Primário
SRCR	Sistema de Remoção de Calor Residual
TMI	<i>Three Mile Island</i>
USP	Universidade de São Paulo
U.S.AEC	<i>United States Atomic Energy Commission</i>
U.S.DOE	<i>United States Department of Energy</i>
U.S.NRC	<i>United States Nuclear Regulatory Commission</i>
VPR	Vaso de Pressão do Reator

SUMÁRIO

	Página
1	INTRODUÇÃO 20
1.1	Motivação para o desenvolvimento do trabalho 23
1.2	Objetivo 25
1.3	Estrutura do trabalho 25
2	REVISÃO DA LITERATURA..... 27
2.1	Visão geral sobre sistema elétrico de plantas nucleares de potência 27
2.1.1	Requisitos regulatórios para o sistema elétrico de plantas nucleares de potência . 30
2.1.2	Eventos de falha do sistema elétrico externo..... 32
2.2	Base normativa para projeto de sistemas elétricos de instalações nucleares . 34
2.2.1	Base normativa de sistemas elétricos de plantas nucleares de potência..... 34
2.2.2	Base normativa de sistemas elétricos de instalações nucleares não convencionais com aplicações navais..... 37
2.3	Análise probabilística de segurança de instalações nucleares 38
2.3.1	Histórico 39
2.3.2	Banco de dados de confiabilidade de equipamentos 41
2.3.3	Análise de confiabilidade humana..... 44
2.3.4	Avaliação probabilística de segurança para modos de baixa potência e desligamento 45
2.4	Projeto de instalações nucleares baseado em informação do risco 48
3	METODOLOGIA..... 52
3.1	Fundamentos da análise probabilística de segurança de instalações nucleares 52
3.1.1	Níveis da APS de uma instalação nuclear 53
3.1.2	Elementos básicos da APS 54
3.1.3	Etapas para se conduzir a APS Nível 1 55

3.2	Métodos de análise implementados no código computacional CAFTA.....	71
3.2.1	Visão Geral do código computacional CAFTA.....	71
3.2.2	Definição dos atributos associados aos eventos básicos dos modelos de falha dos sistemas.....	73
3.2.3	Quantificação dos modelos de árvore de falhas	74
3.3	Seleção dos dados de confiabilidade aplicáveis à avaliação probabilística de sistemas elétricos	76
3.4	Método de avaliação probabilística de projetos de sistemas elétricos	78
3.5	Procedimento para aplicação do método de avaliação probabilística considerando um modelo hipotético de um sistema elétrico CA simplificado	80
3.5.1	Alternativas de projeto do sistema elétrico CA simplificado	81
3.5.2	Evento iniciador e delineamento das sequências do acidente	82
3.5.3	Análise do sistema – modelo lógico	83
3.5.4	Banco de dados de confiabilidade e análise de confiabilidade humana	84
3.5.5	Integração do modelo e quantificação	85
3.5.6	Interpretação dos resultados	86
3.5.7	Classificação de importância	86
3.5.8	Análise de sensibilidade	89
4	INSTALAÇÕES NUCLEARES NÃO CONVENCIONAIS COM APLICAÇÕES NAVAIS EM MODO DE DESLIGAMENTO – OBJETO DE ESTUDO	92
4.1	Descrição das instalações nucleares não convencionais com aplicações navais.	92
4.1.1	Descrição dos tipos de paradas em modo de desligamento.....	95
4.2	Avaliação do protótipo em terra da propulsão nuclear em modo de desligamento.....	96
4.2.1	Configurações da planta em modo de desligamento para troca de combustíveis..	97
4.2.2	Descrição dos sistemas envolvidos.....	100
4.2.3	Descritivo operacional do sistema elétrico	104

4.2.4	Principais suposições de operação dos sistemas de segurança da instalação em modo de desligamento	105
5	APLICAÇÃO DO MÉTODO E DISCUSSÃO DOS RESULTADOS	108
5.1	Eventos iniciadores e delineamento da sequência de acidentes	110
5.2	Análise dos sistemas – modelos lógicos	111
5.3	Banco de dados de confiabilidade e análise de confiabilidade humana	112
5.4	Integração do modelo e quantificação	112
5.5	Interpretação dos resultados	113
5.6	Classificação de importância	117
5.7	Análise de sensibilidade	122
5.7.1	Manutenção/teste simultâneo de equipamentos do sistema elétrico	122
5.7.2	Taxa de falha dos DGEs	123
5.7.3	Taxa de falha do sistema elétrico externo	124
6	CONCLUSÕES	126
7	TRABALHOS FUTUROS	128
	REFERÊNCIAS BIBLIOGRÁFICAS	129
	ANEXOS	138

1 INTRODUÇÃO

A confiabilidade do sistema elétrico é de suma importância para a operação segura de plantas nucleares de potência e, em especial, tem impacto na probabilidade de ocorrência de um evento de *Station Blackout*, o qual é caracterizado por uma perda total do sistema elétrico de corrente alternada que supre os barramentos de segurança da instalação. Após o catastrófico acidente da Usina Nuclear de Fukushima Daiichi em 2011, houve um aumento global da percepção da necessidade de se melhorar o nível de confiabilidade do suprimento de energia elétrica para o desligamento seguro de reatores nucleares [1-2].

O *General Design Criteria 17* (GDC 17) do Apêndice A do 10CFR50 [3], que é o código de regulamentações federais dos Estados Unidos da América (EUA), estabelece que o sistema elétrico local de uma usina nuclear seja suprido, a partir do sistema de transmissão, por dois circuitos fisicamente independentes, projetados e localizados de maneira a minimizar a probabilidade de falhas simultâneas. Cada um desses circuitos deve ser projetado para estar disponível dentro de um tempo adequado após a perda de todas as fontes locais de corrente alternada e do outro circuito de energia proveniente do sistema de transmissão. Os circuitos devem ser projetados para estarem disponíveis dentro de alguns segundos após um acidente de perda de refrigerante, para garantir o resfriamento do núcleo, a integridade da contenção e a execução de outras funções de segurança críticas. O 10CFR50 estabelece que o GDC 17 apresentado no Apêndice A [3] deve ser atendido no que diz respeito ao projeto elétrico de plantas nucleares de potência, de forma a minimizar a probabilidade de ocorrência de um acidente nuclear decorrente da perda do suprimento de energia elétrica.

A Agência Internacional de Energia Atômica (AIEA), no que diz respeito aos projetos de sistemas elétricos de plantas nucleares de potência, estabelece requisitos equivalentes aos da U.S.NRC, que é a comissão reguladora nuclear dos EUA. Assim, o *Specific Safety Guide SSG-34* [4] contém as diretrizes para que os requisitos de segurança do *Specific Safety Requirements SSR-2/1* [5] da AIEA sejam atendidos, corroborando com os requisitos do GDC 17 do Apêndice A do 10CFR50 [3] adotados pela U.S.NRC.

No Brasil, o órgão responsável pela regulamentação, licenciamento, controle e

fiscalização da energia nuclear no país é a Comissão Nacional de Energia Nuclear (CNEN). A CNEN é uma autarquia federal criada em 1956 que, a partir de 1974, tornou-se a autoridade reguladora na área nuclear no Brasil. A missão da CNEN é garantir o uso seguro e pacífico da energia nuclear, desenvolver e disponibilizar tecnologias nucleares e correlatas, visando o bem-estar da população. Nas responsabilidades da CNEN estão incluídas a emissão e a garantia do cumprimento de normas e posições regulatórias em segurança nuclear. A CNEN tem um conjunto extenso de normas em vigor, as quais possuem status de Normas Técnicas, ou seja, são obrigatórias. O arcabouço regulamentar da CNEN é mandatário.

Recentemente, foi criada, a partir de um desmembramento da CNEN, a Autoridade Nacional de Segurança Nuclear (ANSN), à qual caberá regular e fiscalizar as atividades e instalações nucleares no Brasil. O processo de transferência de responsabilidade entre as autarquias está em curso, sendo assim, a edição de normas, fiscalizações, avaliações sobre segurança, expedições de licenças, autorizações, aprovações e certificações ainda estão sob a égide da CNEN.

A norma que regulamenta o processo geral de licenciamento de instalações nucleares no Brasil é a Norma CNEN-NE-1.04 / Resolução CNEN 15/02 [6], a qual inclui, entre outros, requisitos que são aplicáveis ao projeto dos sistemas elétricos destas instalações. Para o caso de instalações nucleares não convencionais, tais como protótipos da propulsão nuclear naval e estaleiros que prestam apoio a submarinos nucleares, não há uma base normativa específica definida pela CNEN, fazendo com que as normas aplicáveis às usinas nucleares de potência sejam adotadas para estas instalações também. Estas normas, em geral, impõem requisitos de segurança que podem penalizar financeiramente o projeto de instalações nucleares não convencionais.

Com base na Norma CNEN-NE-1.04 [6], o processo de licenciamento de instalações nucleares no Brasil envolve, necessariamente, a solicitação pelo requerente, e a emissão pela CNEN, dos seguintes atos: a) Aprovação do Local; b) Licença de Construção; c) Autorização para utilização de material nuclear; d) Autorização para Operação Inicial; e e) Autorização para Operação Permanente. Assim, a construção de uma nova instalação em um local aprovado só pode ser iniciada após a concessão de uma licença de construção ou de uma licença parcial de construção. Além disso, em um dos requisitos estabelecidos na Norma CNEN-NE-1.04 [6], a CNEN exige que o requerimento de Licença de Construção venha acompanhado de um conjunto de documentos que inclui um Relatório Preliminar de Análise de Segurança (RPAS). Do mesmo modo, para conceder a autorização para operação, a qual

deve ser requerida em duas etapas complementares (a primeira relativa à operação inicial e a segunda à entrada em operação em caráter permanente), a CNEN exige que o requerente forneça informações sobre o cronograma preliminar para cada fase de operação, com prazos e datas estimadas para seu início e término, e submeta um conjunto de documentos que inclui o Relatório Final de Análise de Segurança (RFAS). O RPAS e o RFAS são relatórios que devem conter informações que descrevam a instalação, apresentem as bases de projeto, os limites de operação e uma análise de segurança da instalação como um todo.

Do ponto de vista histórico, a análise de segurança apresentada no RPAS/RFAS tem sido desenvolvida adotando-se uma abordagem determinística para avaliação de acidentes postulados, tendo em vista a verificação da aplicação do conceito de defesa em profundidade. Ao mesmo tempo, a análise de segurança baseada em uma abordagem probabilística, a qual é conhecida na área nuclear pelo termo Análise Probabilística de Segurança (APS), tem sido incluída em algumas resoluções específicas emitidas pela CNEN. A APS se destaca por usar uma abordagem abrangente e estruturada na identificação de perigos e avaliação dos possíveis cenários de acidentes decorrentes de eventos iniciadores e constitui todo um ferramental conceitual e matemático para que o risco associado à operação de uma instalação nuclear seja estimado numericamente.

Um dos primeiros documentos a apresentar o desenvolvimento de uma APS para usinas nucleares comerciais com reatores refrigerados a água leve foi o relatório WASH-1400 [7], publicado em 1975 e elaborado por um comitê de especialistas a serviço da U.S.NRC. Inicialmente, este relatório sofreu várias críticas da comunidade nuclear, mas após o acidente na usina nuclear Three Mile Island (TMI) em Março de 1979, passou a ser uma tradição aplicar este tipo de estudo em avaliações de segurança de plantas nucleares de potência. Desde a década de 1980, a APS tem sido aprimorada no que diz respeito à metodologia, bases de dados, programas computacionais para cálculos e procedimentos de revisão. Organizações internacionais com reconhecida experiência na área nuclear têm publicado normas, guias e documentos técnicos que abordam o desenvolvimento de estudos de APS para instalações nucleares [8-10].

No entanto, até o momento, não existem normas técnicas ou guias publicados pela CNEN que estabeleçam os requisitos para o desenvolvimento da APS e para o uso dos resultados de avaliações probabilísticas em tomadas de decisão que envolvam a segurança das instalações.

1.1 Motivação para o desenvolvimento do trabalho

A contribuição dos sistemas elétricos para a segurança de instalações nucleares em geral e, em especial, com relação às restrições de segurança impostas pelo evento de *Station Blackout* que foram evidenciadas após o acidente da Usina Nuclear de Fukushima Daiichi, torna a utilização da APS uma opção importante para subsidiar a escolha das arquiteturas de projeto e o licenciamento dessas instalações.

O surgimento de novas tecnologias de reatores e a diversificação da funcionalidade e aplicação de tecnologias existentes tem demandado uma nova base normativa ou a revisão da existente para adequação aos novos projetos e viabilização do licenciamento. Neste aspecto, a utilização da APS para demonstrações de segurança vai ao encontro das necessidades de melhorias no desenvolvimento destes projetos. Reatores modulares pequenos (*small modular reactors, SMR*), reatores multipropósitos, reatores da propulsão nuclear de navios, entre outras tecnologias e aplicações, destacam-se entre os projetos aos quais é necessária uma adequação da base normativa, corroborando para a utilização da APS como uma abordagem adequada para a análise de segurança.

Nos EUA, em especial, os protótipos em terra de submarinos nucleares e os estaleiros que prestam apoio aos submarinos de propulsão nuclear atendem aos critérios de projeto estabelecidos pelo Departamento de Energia dos Estados Unidos (U.S.DOE) [11], e não aos da U.S.NRC. No Brasil, é comum a CNEN fazer uso de normas da U.S.NRC e da AIEA, as quais são voltadas para usinas nucleares de potência, em suas deliberações. Conforme estabelecido no item 6.5.2 da Norma CNEN-NE-1.04 [6], “na ausência de normalização brasileira adequada, devem ser usados, preferencialmente, Códigos, Guias e Recomendações da Agência Internacional de Energia Atômica e, na ausência destes, normas internacionais ou de países tecnicamente desenvolvidos, desde que essas normas e regulamentações sejam aceitas pela CNEN”. A base normativa endossada pelo U.S.DOE não faz parte do arcabouço regulamentar da CNEN.

Por outro lado, os reatores de potência das instalações nucleares não convencionais com aplicações navais, no caso dos protótipos em terra de submarinos nucleares e os estaleiros que prestam apoio aos submarinos de propulsão nuclear, operam isolados da rede e não geram energia para o sistema elétrico integrado, sendo, portanto, apenas instalações consumidoras. O atendimento ao GDC 17 [3], o qual requer que o suprimento de energia do sistema de transmissão para a planta nuclear seja feito por ao menos duas linhas de transmissão (LTs) independentes encaminhadas em diferentes torres, onera financeiramente

o projeto destas instalações nucleares não convencionais com aplicações navais. Isto se deve ao fato de que o encaminhamento de uma segunda LT pode alcançar cifras muito elevadas, devido a possíveis desapropriações e instalação de torres em locais isolados e de difícil acesso, tais como morros e encostas.

Além disso, o Sistema Elétrico de Potência (SEP), conduzido pelo sistema de transmissão, está sujeito a fenômenos transitórios que podem ser ocasionados, por exemplo, por descargas atmosféricas, acionamento de cargas indutivas (motores, transformadores), chaveamentos de capacitores, faltas sustentadas, etc., que prejudicam o fornecimento adequado de energia. As faltas podem ocorrer devido à falha de diversos componentes, dentre os quais é possível destacar as LTs como o elemento mais suscetível, especialmente se considerarmos suas dimensões físicas e suas complexidades funcionais. Por percorrerem longos percursos, as LTs são submetidas a intempéries ambientais, que podem ser severas, resultando inclusive pela falha comum entre LTs independentes. Problemas associados à monitoração, localização de eventos e manutenções corretivas também são fatores a se destacar, pois as LTs passam por áreas isoladas e de difícil acesso. Tal observação pode ser notada em indicadores de qualidade do Operador Nacional do Sistema Elétrico (ONS) [12], onde as LTs são responsáveis por cerca de 70% das falhas do SEP.

Adicionalmente, ressalta-se que a perda do sistema elétrico externo, o qual inclui o sistema de transmissão, não é considerado um evento iniciador para as instalações nucleares não convencionais com aplicações navais, quando se encontram em operação em potência, pois, nesse modo de operação, o reator destas instalações opera isolado do sistema elétrico externo, gerando energia exclusivamente para seus próprios sistemas. Assim, um *trip* no reator induzido pela perda do sistema elétrico externo não é considerado crível. Por outro lado, quando estão no modo de desligamento, tais instalações nucleares não convencionais são dependentes do sistema elétrico externo para fornecimento de energia para seus barramentos de segurança. Neste caso, a perda da rede externa configura-se como um evento iniciador para a análise de segurança destas instalações. Além disso, a perda do sistema elétrico externo é um dos elementos do cenário de *Station Blackout* que impõe restrições operacionais, contribuindo para o aumento do risco global da instalação.

É importante citar que, a utilização da APS para as demonstrações de segurança requer o uso de bancos de dados de confiabilidade de componentes e equipamentos atualizados e aplicáveis para as instalações em estudo. Muitas vezes, os bancos de dados disponíveis na literatura estão desatualizados ou não são de domínio público, estando restritos a determinados grupos de usuários ou fabricantes. Portanto, sempre existirá um

conjunto de dados que precisam ser investigados e selecionados para se conduzir de forma adequada a APS de uma instalação nuclear.

Tendo em vista a susceptibilidade do sistema de transmissão e as diferenças operacionais das instalações nucleares não convencionais com aplicações navais, quando comparadas às usinas nucleares de potência, soluções alternativas de projeto que apresentem um menor risco para a segurança da instalação e uma maior disponibilidade de energia para os sistemas de segurança podem ser necessárias, devendo ser submetidas ao órgão licenciador.

1.2 Objetivo

Este trabalho tem por objetivo propor uma abordagem probabilística para avaliação de segurança de sistemas elétricos de instalações nucleares, subsidiando a escolha da arquitetura do projeto e seu licenciamento, tendo em vista os requisitos regulatórios vigentes, diretrizes internacionais, o estado da arte em métodos e as melhores práticas adotadas atualmente. Esta abordagem envolve a análise da sequência de possíveis acidentes, a avaliação do impacto desses acidentes no risco global da instalação e a análise de risco associada aos sistemas elétricos, tomando como base os modelos de uma APS nível 1 para eventos internos.

1.3 Estrutura do trabalho

Este trabalho está organizado em 7 capítulos e 5 anexos. No capítulo 1, destaca-se a importância da confiabilidade do sistema elétrico para a operação segura de plantas nucleares, a utilização da APS como ferramenta para tomada de decisão de projeto e para o licenciamento de instalações nucleares, em especial para instalações nucleares não convencionais que carecem de adequação da base normativa. Neste capítulo, aborda-se, também, a problemática a respeito da necessidade da alimentação elétrica dos protótipos em terra de submarinos nucleares e de estaleiros que prestam apoio aos submarinos de propulsão nuclear por duas LTs.

No capítulo 2, é apresentada uma revisão da literatura com o estado da arte dos trabalhos, base normativa regulatória e documentos correlatos aos tópicos estudados neste trabalho, além de uma visão geral sobre sistemas elétricos de plantas nucleares de potência. Destaca-se o levantamento histórico da APS, os requisitos normativos que norteiam o desenvolvimento dos projetos, a utilização da APS como ferramenta de tomada de decisão

no licenciamento e em projetos de instalações nucleares.

No capítulo 3, primeiramente, é apresentado um embasamento teórico das principais técnicas e conceitos de APS, que subsidiam o entendimento e o desenvolvimento da metodologia. Em seguida, são tratadas as principais ferramentas de análise implementadas no programa computacional CAFTA, a principal fonte de seleção de dados genéricos de confiabilidade de equipamentos utilizados no trabalho e o método de análise probabilística adotado para avaliar os projetos de sistemas elétricos de instalações nucleares. Por fim, o método de avaliação proposto é ilustrado por meio da aplicação em um modelo hipotético simplificado de um sistema elétrico CA.

No capítulo 4 é apresentado o tipo de instalação nuclear abordado como objeto de estudo para este trabalho, sendo realizada, primeiramente, uma descrição geral sobre esse tipo de instalação e suas particularidades e, em seguida, uma avaliação específica do projeto e operação de um protótipo em terra da propulsão naval em modo de desligamento, durante a troca de combustíveis.

No capítulo 5 são apresentados os resultados e realizadas as discussões a respeito da aplicação da metodologia em uma instalação nuclear não convencional com aplicações navais em modo de desligamento, conforme descrito no Capítulo 4. No estudo de caso da aplicação da metodologia são avaliados projetos com diferentes arquiteturas do sistema elétrico, assim como, a possibilidade de adição de fontes locais que possam suprimir o não atendimento ao GDG 17 [3], no que se refere ao fornecimento de energia por duas LTs.

No capítulo 6, destacam-se as principais contribuições do trabalho e as conclusões sobre o mesmo. No capítulo 7, são apresentadas sugestões para a continuidade deste trabalho.

Finalmente, as referências bibliográficas e os anexos são apresentados na parte final desta dissertação.

2 REVISÃO DA LITERATURA

Neste capítulo, primeiramente, é realizada uma descrição geral do sistema elétrico de plantas nucleares de potência, abordando os principais conceitos e requisitos regulatórios dos sistemas elétricos aplicáveis à estas instalações. Realiza-se, também, um levantamento do estado da arte da base normativa regulatória para projetos de sistemas elétricos de instalações nucleares e do desenvolvimento da análise probabilística de segurança como ferramenta de avaliação dos projetos. Destaca-se, ainda, a base normativa de instalações nucleares não convencionais com aplicações navais, assim como a avaliação probabilística de segurança para plantas nucleares em modo de desligamento.

2.1 Visão geral sobre sistema elétrico de plantas nucleares de potência

O sistema elétrico de uma planta nuclear de potência é comumente classificado em relação a sua localização física como: sistema elétrico externo (*Offsite Power*) e sistema elétrico local (*Onsite Power*).

O sistema elétrico externo da usina origina-se no sistema de transmissão por meio de, pelo menos, duas LTs fisicamente independentes e supre energia CA à planta a partir da subestação primária/entrada (*switchyard*) durante a partida (*startup*), desligamento (*shutdown*) e todas as condições acidentais postuladas [4].

O sistema elétrico local é composto pelos sistemas de distribuição de energia internos à planta, que inclui os sistemas de energia CA e CC necessários para levar a planta a um estado controlado após ocorrências operacionais previstas ou condições acidentais, e mantê-la em um estado controlado e seguro, até que as fontes de alimentação externas sejam restauradas. O sistema elétrico local é classificado de acordo com sua função de segurança¹: sistemas importantes para a segurança (sistemas de segurança e sistemas relacionados à segurança) e sistemas não importantes para a segurança [4].

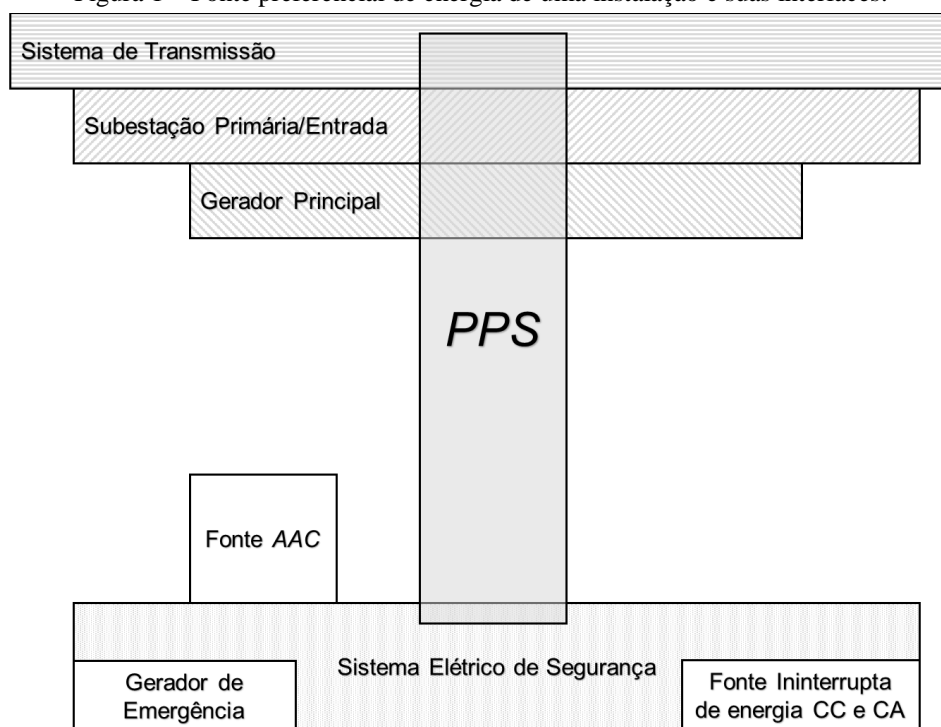
O sistema elétrico local, por sua vez, é geralmente subdividido em três tipos de sistemas elétricos de acordo com os requisitos de suprimento de energia das cargas:

¹ As terminologias de classificação de segurança utilizadas nos documentos da AIEA e da U.S.NRC diferem entre si.

- A. Sistema elétrico CA. As funções atribuídas às cargas CA toleram interrupções no suprimento de energia. Usualmente, o sistema de energia CA inclui os geradores de emergência que, em geral, são diesel geradores de emergência (DGEs), e as fontes alternativas de energia CA (*Alternate Alternating Current, AAC*). Os relés de proteção, ao detectarem a perda do suprimento de energia externo, comandam a partida automática dos geradores de emergência. Na análise de segurança, pressupõe-se que o gerador de emergência será utilizado para o desligamento seguro da planta dentro das bases de projeto e a fonte AAC para condições estendidas da base de projeto, tal como o *Station Blackout*;
- B. Sistema elétrico CC. Este sistema supre as cargas CC sem interrupção através das baterias. O sistema elétrico CC inclui, também, os retificadores que estão conectados ao sistema elétrico CA; e
- C. Sistema elétrico ininterrupto CA. Esse sistema supre energia, sem interrupção, para as cargas CA através de inversores conectados às baterias do sistema elétrico CC ou à conjuntos retificador/baterias dedicados.

Em relação à fonte de suprimento de energia CA para os barramentos de segurança, a fonte preferencial de energia (*Preferred Power Supply, PPS*) é o suprimento proveniente do sistema de transmissão, ou do gerador principal. A PPS deve ser composta por dois ou mais circuitos a partir do sistema de transmissão até o sistema de distribuição elétrico de segurança. Na Figura 1 estão ilustradas a PPS e as interfaces com os demais sistemas e fontes elétricas da planta.

Figura 1 – Fonte preferencial de energia de uma instalação e suas interfaces.



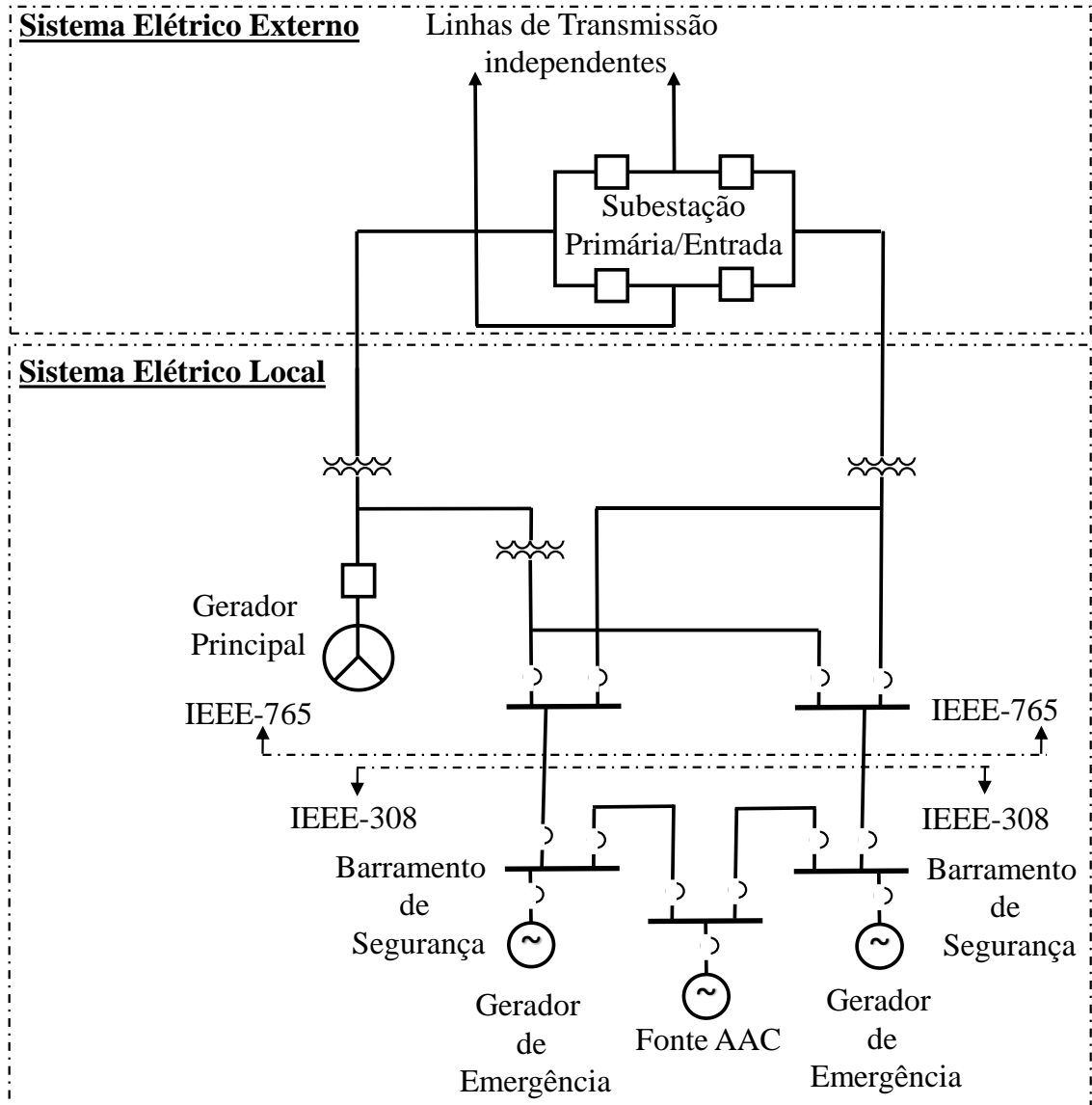
Fonte: SSG-34 [4].

Do ponto de vista determinístico, na Figura 2 é apresentada uma arquitetura do sistema elétrico de uma usina nuclear de potência que está em conformidade com os requisitos mínimos previstos no GDC 17 [3] para os circuitos PPS. Nesta mesma figura, estão representados os geradores de emergência e as fontes AAC que são responsáveis por conduzir a planta ao desligamento seguro nas condições de acidentes da base de projeto e de *Station Blackout*, respectivamente.

Projetos de arquitetura de sistemas mais robustos podem ser propostos, destacando-se os casos previstos na IEEE-1792 [13]:

- Implantação de duas subestações primárias independentes;
- Duas ou mais LTs independentes para cada subestação primária; e
- Circuitos da PPS conectados diretamente aos barramentos de segurança, ou seja, alimentação direta, sem passar por barramentos que não sejam do sistema de segurança.

Figura 2 – Arquitetura do sistema elétrico de uma usina nuclear de potência em conformidade com os requisitos mínimos previstos no GDC 17.



Fonte: adaptado IEEE-765 [14]/SSG-34 [4].

2.1.1 Requisitos regulatórios para o sistema elétrico de plantas nucleares de potência

Endossadas pelos guias regulatórios da U.S.NRC, as normas IEEE-765 [14] e IEEE-308 [15] abordam os critérios para PPS e sistemas elétricos de segurança, respectivamente. Na Figura 2 é possível verificar os limites de escopo para cada norma.

2.1.1.1 Fontes preferenciais de energia (PPS)

A PPS deve consistir em dois ou mais circuitos a partir do sistema de transmissão até o sistema de distribuição de energia de segurança, devendo estar disponível durante a partida

da planta e operação normal, para atender aos requisitos de acidente, pós-acidente e desligamento seguro.

Os circuitos da PPS para os sistemas elétricos de segurança devem ser fisicamente independentes, projetados e localizados de forma a minimizar a probabilidade de falha simultânea em ambos os circuitos. Especificamente, considerando a interface da PPS com o sistema de transmissão, as duas LTs que suprem a PPS devem ser projetadas de forma a minimizar a falha simultânea como resultado da falha de qualquer torre de transmissão ou a falha a partir do cruzamento das LTs.

2.1.1.2 Sistemas elétricos de segurança

Sistemas elétricos de segurança de plantas nucleares, que não usam reatores com sistemas de segurança passivos, consistem em sistemas CA, CC e I&C, que incluem tipicamente os equipamentos previstos na Tabela 1.

Tabela 1 – Componentes típicos dos sistemas elétricos de segurança.

Funcionalidade	Componente
Fontes de suprimento	Geradores de emergência
	Baterias
	Transformadores
Equipamentos de distribuição	Barramentos
	Painéis de manobra de disjuntores
	Cabos
	Retificadores
	Inversores
	Disjuntores
	Controladores
Dispositivos e equipamentos de atuação	Motores
	Solenoides
	Resistências de aquecimento
	Indicador de supervisão
Sensores e dispositivos de comando	Chaves
	Transformadores de corrente e tensão
	Transdutores
	Relés de proteção

Fonte: IEEE-308 [15].

Os sistemas elétricos de segurança devem atender a requisitos de redundância, independência e separação/segregação, critério de falha simples, e requisitos de qualificação

sísmica e de qualidade de equipamentos. No arcabouço de normas IEEE aplicável às plantas nucleares de potência, existem normas específicas para cada requisito mencionado. Alguns requisitos gerais de projeto são:

- A. Cargas elétricas dos sistemas de segurança devem ser separadas em dois ou mais grupos redundantes (trens);
- B. As proteções previstas para um grupo de cargas devem ser independentes das proteções do grupo de cargas redundantes;
- C. Cada grupo de cargas redundantes deve ter acesso à PPS e a um gerador de emergência; e
- D. Cada grupo de cargas CC deve ter acesso ao suprimento de energia proveniente de uma ou mais baterias e a um ou mais retificadores.

2.1.2 Eventos de falha do sistema elétrico externo

O sistema elétrico externo (*Offsite Power*) da instalação é composto pelo sistema de transmissão, subestação primária/entrada (*switchyard*) e os circuitos de energia que suprem as estruturas, sistemas e componentes importantes para a segurança nuclear da instalação [13].

Segundo o documento NUREG/CR-6890 [16] existem quatro categorias de eventos relacionadas à perda do sistema elétrico externo (*Loss of Offsite Power - LOOP*), conforme a Figura 3:

1. Eventos centrados na planta;
2. Eventos centrados na subestação primária/entrada;
3. Eventos relacionados à rede (sistema de transmissão); e
4. Eventos relacionados ao clima.

Figura 3 – Categorias de eventos de perda do sistema elétrico externo de uma instalação.



Fonte: adaptado NUREG/CR-6890 [16].

O Glossário do LOOP, disponibilizado em (<https://nrcoe.inl.gov/>) [17], detalha as categorias dos eventos de perda do sistema elétrico externo:

Eventos centrados na planta

A perda do sistema elétrico externo é ocasionada por falhas que ocorrem na própria planta nuclear, devido à falha de equipamentos, erro de projeto ou erro humano.

Eventos centrados na subestação primária/entrada

A perda do sistema elétrico externo é ocasionada por falhas que ocorrem na subestação primária/entrada da planta nuclear, devido à falha de equipamentos, erro de projeto ou erro humano.

Eventos relacionados à rede

A falha ocorre no sistema de transmissão, fora do escopo de atuação da equipe técnica da planta nuclear. As linhas de transmissão falham a partir de instabilidades na tensão e frequência do sistema, sobrecarga, ou outras causas que requerem esforços de restauração ou ações corretivas pelo operador do sistema de transmissão.

Eventos relacionados ao clima

São eventos de perda do sistema elétrico externo causados por condições climáticas severas.

2.2 Base normativa para projeto de sistemas elétricos de instalações nucleares

2.2.1 Base normativa de sistemas elétricos de plantas nucleares de potência

A base normativa de sistemas elétricos para usinas nucleares comerciais é bem estabelecida e tem sido atualizada constantemente, incorporando inclusive os aprendizados trazidos por acidentes como o de TMI e Fukushima Daiichi. O acidente da usina nuclear de Fukushima Daiichi foi um marco para a avaliação de segurança dos sistemas elétricos de usinas nucleares. Na ocasião do acidente, os seis suprimentos de energia externos às unidades da usina foram perdidos ao mesmo tempo devido ao abalo sísmico. Inicialmente, os sistemas de resfriamento do núcleo foram mantidos pela energia dos diesel geradores de emergência (DGEs), mas estes também falharam após serem inundados pelo tsunami que se formou, configurando-se o cenário de *Station Blackout* para a usina [18].

Nos EUA, a U.S.NRC possui o 10CFR50 [3] como regulação para o licenciamento de instalações de produção e utilização de material nuclear. A partir deste código são derivados os requisitos de projeto, incluindo os de sistemas elétricos de usinas nucleares de potência. No apêndice A do 10CFR50 são abordados os critérios gerais de projeto (critérios de alto nível) para usinas nucleares de potência, sendo o GDC 17 o principal conjunto de critérios para os sistemas elétricos da instalação. Os requisitos abordados no GDC 17 são:

- O suprimento de energia elétrica local, que inclui baterias e os sistemas locais de distribuição, deve ter suficiente independência, redundância e capacidade de testabilidade para realizar suas funções de segurança, assumindo-se uma falha única; e
- O sistema elétrico, a partir do sistema de transmissão para o sistema elétrico local de distribuição deve ser suprido por dois circuitos fisicamente independentes, projetados e localizados de maneira a minimizar a probabilidade de falhas simultâneas. É aceitável uma única subestação de entrada para ambos os circuitos (subestação que recebe as LTs).

Em particular, a seção 50.63 do 10CFR50 trata dos eventos de perda de todas as fontes de energia CA para os barramentos de segurança. Em 10CFR50.63 [19] é requerido que as plantas sejam capazes de suportar e se recuperar de um evento de *Station Blackout* (falha do sistema elétrico externo e do sistema elétrico CA de emergência) por um período especificado. A confiabilidade de fontes CA de emergência é um fator relevante para a probabilidade de ocorrer um acidente de dano ao núcleo, o qual pode ter origem em um

evento de *Station Blackout*.

Adicionalmente aos regulamentos previstos no 10CFR50 e suas seções, a U.S.NRC publica documentos regulatórios na denominada série NUREG, a qual compreende relatórios, livros e folhetos técnicos, que são resultados de pesquisa, investigação de incidentes, entre outras informações técnicas/administrativas.

Os guias regulatórios da U.S.NRC (*Regulatory Guides*) proveem o caminho e os métodos para se cumprir os regulamentos impostos no 10CFR50. Como tal, eles não precisam ser seguidos se outro método for comprovado pelo menos igualmente eficiente e proposto para conformidade. A U.S.NRC emite guias regulatórios para descrever e disponibilizar ao público métodos que a equipe da U.S.NRC considera aceitáveis para uso na implementação de partes específicas dos regulamentos da agência, técnicas que a equipe usa na avaliação de problemas específicos ou acidentes postulados e dados que a equipe necessita para analisar os pedidos de autorizações e licenças. Os guias regulatórios não substituem os regulamentos e o cumprimento dos mesmos não é obrigatório [18].

Endossadas pelos guias regulatórios da U.S.NRC, as normas do *Institute of Electrical and Electronics Engineers* (IEEE) proveem os caminhos aceitáveis e os métodos para projeto e especificação de equipamentos de plantas nucleares de potência. Destacam-se alguns dos principais guias regulatórios da U.S.NRC, assim como as respectivas normas do IEEE endossadas por essa comissão e que são particularmente importantes para os sistemas elétricos:

- *Regulatory Guide 1.9 - Application and Testing of Safety-Related Diesel Generators in Nuclear Power Plants* [20] (endossa a norma IEEE 387 [21]);
- *Regulatory Guide 1.32 - Criteria for Power Systems for Nuclear Power Plants* [22] (endossa a norma IEEE 308 [15]);
- *Regulatory Guide 1.53 - Application of the Single-Failure Criterion to Safety Systems* [23] (endossa a norma IEEE 379 [24]);
- *Regulatory Guide 1.75 - Criteria for Independence of Electrical Safety Systems* [25] (endossa a norma IEEE 384 [26]);
- *Regulatory Guide 1.118 - Periodic Testing of Electric Power and Protection Systems* [27] (endossa a norma IEEE 338 [28]);
- *Regulatory Guide 1.153 - Criteria for Safety Systems* [29] (endossa a norma IEEE 603 [30]); e
- *Regulatory Guide 1.155 - Station Blackout* [31] (guia para cumprir com o requisito

do 10CFR50.63 [19]).

No que diz respeito ao sistema elétrico externo, a norma IEEE 765 [14] aborda os requisitos de projeto para os circuitos preferenciais de energia que partem do sistema de transmissão até os barramentos de segurança da instalação, destacando a necessidade de dois ou mais circuitos. Em complemento, a norma IEEE 1792 [13] traz recomendações práticas de confiabilidade para os sistemas elétricos, citando por exemplo, como limitação de projeto, a utilização de uma única subestação primária de entrada comum aos sistemas de transmissão.

Em relação ao sistema elétrico local, a norma IEEE 308 [15] define os critérios de alto nível para os sistemas elétricos com classificação de segurança, tais como: independência, qualidade de energia, classificação de segurança de equipamentos e critério de falha simples. Na norma IEEE 308 [15] são indicadas as normas que tratam dos critérios de projeto de forma mais detalhada, citando-se como exemplo a norma IEC/IEEE 60780-323 [32] para qualificação de equipamentos elétricos, a IEEE 379 [24] para critério de falha simples e a IEEE 384 [26] para critério de independência de equipamentos e circuitos elétricos de segurança. Uma avaliação probabilística é exigida para os sistemas elétricos de segurança que cumprem os critérios de falha simples, mas que não satisfazem todos os requisitos de confiabilidade da base de projeto, citando as normas IEEE 352 [33] e IEEE 577 [34] como guias para essa avaliação.

No que se refere aos requisitos de qualificação de segurança de equipamentos elétricos, a norma IEC/IEEE 60780-323 [32] trata o assunto de forma mais generalizada, realizando a indicação das normas que tratam especificamente de cada tipo de equipamento, tais como: IEEE 334 [35] para motores, IEEE 387 [21] para diesel geradores de emergência e IEEE 383 [36] para cabos e emendas.

Considerando as publicações da AIEA, o *Specific Safety Guide* No. SSG-34 [4] é o principal guia para projeto de sistemas elétricos de plantas nucleares de potência e contém recomendações para atender aos requisitos de segurança. Este guia apresenta um compilado de diretrizes para o atendimento dos requisitos de segurança previstos no *Specific Safety Requirements* No. SSR 2/1 [5]. As diretrizes de projeto do guia SSG-34 [4] estão alinhadas com a regulação prevista no 10CFR50.

Considerando o sistema elétrico externo, é previsto tanto pelo SSG-34 [4] quanto pelo GDC 17 [3] que o sistema elétrico externo deve ser suprido por dois ou mais circuitos (sistemas de suprimento) e que estes sejam independentes. Entretanto, no item 6.15 do guia SSG-34 [4] é prevista a possibilidade de um único sistema de transmissão, desde que o

relatório de segurança atenda os objetivos técnicos de segurança definidos no documento de requisitos SSR 2/1 [5], e cita como exemplo a possibilidade de um único sistema de transmissão para projeto de reatores que possuem características de segurança passiva.

Além disso, nos requisitos específicos de segurança estabelecidos no SSR 2/1 [5], considera-se que os resultados da análise probabilística de segurança, juntamente com os da análise determinística, devem ser considerados no projeto, para garantir a prevenção de acidentes e a mitigação das consequências desses acidentes.

2.2.2 Base normativa de sistemas elétricos de instalações nucleares não convencionais com aplicações navais

Nos EUA, o Programa de Propulsão Nuclear Naval está sob a égide da Administração de Segurança Nuclear Nacional (*National Nuclear Security Administration*, NNSA), sendo uma agência semi-autônoma do U.S.DOE [11]. A norma DOE O 420.1C [37] é adotada por U.S.DOE e NNSA para estabelecer um programa de requisitos de segurança para as instalações nucleares. Para tanto, a norma DOE O 420.1C [37] invoca (*Invoked Standards*) um conjunto técnico de normas do U.S.DOE (*Technical Standards*) e um conjunto de normas industriais de outras instituições (*Industry Standards*). No que diz respeito aos sistemas elétricos das instalações nucleares, são invocadas as normas do IEEE que tratam dos critérios aplicáveis aos sistemas elétricos de segurança, que são: IEEE 323 (atual IEC/IEEE 60780-323 [32]), IEEE 379[24] e IEEE 384 [26]. Não é citado nenhum critério nem tampouco invocada alguma norma que trate da alimentação elétrica do sistema de transmissão para a instalação.

A norma DOE O 420.1C [37] cancelou a norma DOE O 5480.30 [38], a qual estabelecia os critérios de projeto de instalações nucleares com reatores. Os requisitos de projeto para os sistemas elétricos foram abordados e, em especial, o critério de falha simples e o critério de redundância para alimentação das cargas elétricas de segurança. A norma DOE O 5480.30 [38] destacou que os guias relacionados à implementação dos critérios de projeto de segurança dos sistemas elétricos de instalações reguladas pelo U.S.DOE contêm uma variedade de fontes que inclui as próprias normas técnicas do U.S.DOE, normas industriais e guias preparados pela U.S.NRC. Entretanto, a aplicabilidade de alguns critérios específicos poderia variar conforme o tipo de instalação e as atividades ou processos realizados.

A norma DOE 6430.1A [39], também substituída pela norma DOE O 420.1C [37],

trazia em sua divisão 16 um guia geral de projeto de sistemas elétricos de distribuição de energia para instalações reguladas pelo U.S.DOE. Esse guia abordava em detalhes os critérios para o sistema elétrico. Com relação ao sistema elétrico externo, era exigido que o sistema fosse dedicado e possuísse circuitos redundantes. Alternativamente, ao invés de fornecer os dois circuitos separadamente para a instalação, um único circuito poderia ser fornecido através de um sistema de transmissão em anel, com sistema de seccionamento, desde que atendesse aos requisitos de confiabilidade.

Evidencia-se que as normas mais atuais não trazem em seu texto requisitos técnicos prescritivos que devem ser seguidos nos projetos, pautados apenas no conceito de defesa em profundidade e análises determinísticas, como ocorria principalmente com normas emitidas anteriormente aos anos 90. De fato, as normas mais atuais flexibilizam as possibilidades de soluções de engenharia para os projetos, desde que estas sejam amparadas em comprovações que utilizam a combinação da análise determinística com a probabilística. Desta forma, as normas atuais trazem requisitos de alto nível e delegam as opções técnicas de engenharia para os estudos e demonstrações de segurança fundamentadas em risco. O surgimento de instalações nucleares com novas tecnologias e funcionalidades tem corroborado para o caminho que as normas mais recentes têm seguido.

2.3 Análise probabilística de segurança de instalações nucleares

A Análise Probabilística de Segurança (APS) permite a identificação de cenários de acidentes e a estimativa numérica dos riscos associados a uma instalação. Associada à tradicional abordagem determinística, a APS é uma ferramenta poderosa na identificação das sequências de acidentes e das vulnerabilidades associadas às instalações, sendo possível avaliar o projeto e os riscos envolvidos em sua operação.

Na abordagem determinística é sugerida a utilização de margens de segurança como recurso para sobrepor as incertezas envolvidas no projeto e na operação dos sistemas. Nesta abordagem, todos os possíveis eventos indesejáveis são considerados como igualmente prováveis, resultando assim, por muitas vezes, num superdimensionamento das estruturas, o que pode inclusive inviabilizar financeiramente um projeto.

Na abordagem probabilística, as possíveis falhas dos sistemas são tratadas como aleatórias ou probabilísticas. Nesta abordagem, é possível estimar o tempo esperado para as falhas a partir de conhecimentos prévios do processo que desencadeia a falha, tais como o comportamento probabilístico dos esforços, das condições operacionais e dos fatores

ambientais.

2.3.1 Histórico

Nos EUA, as primeiras práticas de gerenciamento de risco utilizadas em usinas nucleares comerciais foram decorrentes do uso da energia nuclear por instituições militares no desenvolvimento de navios e submarinos nucleares. As primeiras usinas nucleares eram pequenas (geralmente menores que 100 MW elétricos) e consistiam em uma extrapolação do projeto dos submarinos. Sistemas secundários da contenção também tiveram suas origens no programa de submarinos como resultado de protótipos em terra do reator de submarinos localizados próximos a centros populacionais [40].

Inicialmente, medidas quantitativas de risco dos reatores e confiabilidade dos sistemas não foram um fator primordial no projeto das instalações. No entanto, a análise de confiabilidade começou a se disseminar com a formação de engenheiros nucleares na década de 1950. A Universidade Estadual da Carolina do Norte teve o primeiro programa de engenharia nuclear começando em 1957, seguido pelo Massachusetts Institute of Technology (MIT) logo depois. Ernst Frankel, professor do MIT, escreveu um livro-texto, *System Reliability and Risk Analysis*, publicado no início dos anos 1960, que forneceu tanto a estrutura matemática quanto os métodos probabilísticos para avaliação de sistemas de engenharia. A geração de engenheiros elétricos e nucleares que se formaram no MIT na década de 1960 estudou métodos de análise de confiabilidade, aos quais Frankel vinculou a abordagem determinística tradicional. Frankel ensinou aos engenheiros como estimar as probabilidades de falha de sistemas considerando as incertezas com certos parâmetros operacionais [41]. Outro livro de Green e Bourne [42], publicado no início dos anos de 1970, forneceu uma forte base teórica para aplicações de métodos de confiabilidade na avaliação de risco de sistemas complexos de engenharia.

Em 1972, a Comissão de Energia Atômica dos Estados Unidos (U.S.AEC) deu início à elaboração do Estudo de Segurança do (*Reactor Safety Study*, RSS). O estudo de segurança do reator levou três anos para ser concluído e foi um ponto de inflexão na maneira de pensar sobre a segurança das usinas nucleares. O estudo usou a usina nuclear Surry (reator de água pressurizada) e a usina nuclear Peach Bottom (reator de água fervente) como projetos de referência, e calculou o risco de operação de 100 reatores de água leve localizados nos EUA. As principais conclusões do RSS, também conhecido como WASH-1400 [7], foram que o risco associado à operação das usinas nucleares selecionadas é de fato pequeno, e que o

principal contribuinte para o risco não é o acidente de grande perda de refrigerante anteriormente enfatizado como o acidente de base do projeto. Em vez disso, os transientes e os acidentes com pequenas perdas de refrigerante geralmente são os maiores contribuintes para o risco. O relatório WASH-1400 [7] também indicou que fatores humanos desempenham um papel importante na avaliação do risco, contrariando a expectativa das bases de projeto [40].

Em um primeiro momento, o RSS não foi endossado pela comissão ou por seus pares e apenas ganhou notoriedade após o acidente na unidade 2 de TMI em 1979, quando a U.S.NRC concluiu que o transiente que ocasionou o acidente de TMI havia sido considerado em uma das sequências acidentais previstas no RSS. A partir de então, a abordagem probabilística proposta pelo RSS passou a ser incorporada por novos estudos que agregaram credibilidade, promovendo assim, uma melhor aceitação deste tipo de metodologia [40].

Em 1983, foi elaborado, sob os auspícios da *American Nuclear Society* (ANS) e do *Institute of Electrical and Electronics Engineers* (IEEE), o guia NUREG/CR-2300 [10] cujo objetivo era compilar os guias de procedimentos dos principais métodos de APS.

Em 1988, foi publicado o 10CFR50.54(f) (*Generic Letter* 88-20) [43] que passou a exigir inspeções individuais nas usinas americanas para avaliar a segurança e o risco à saúde da população próxima às instalações. A publicação indicava a APS como ferramenta sistêmica de análise de segurança para as instalações.

Em 1990, a U.S.NRC forneceu orientações adicionais sobre requisitos de segurança (*Safety Goals*), endossando a SERCY 89-102 [44]. Limites numéricos de $1E-4$ /ano para a frequência de dano ao núcleo (*Core Damage Frequency*, CDF) e $1E-5$ /ano para a liberação de termos fonte ²(*Large Early Release Frequency*, LERF) foram estabelecidos [45].

Em dezembro de 1990, foi publicado o documento NUREG-1150 [46] que realizou o estudo de acidentes severos para cinco usinas nucleares de potência americanas. Este relatório pode ser considerado uma atualização do relatório WASH-1400 [7], trazendo um refinamento das metodologias e melhorias das informações de confiabilidade de componentes. Estas modificações reduziram os valores calculados para CDF e LERF, tendo como um dos resultados encontrados um menor risco ao público do que havia sido previsto no WASH-1400 [7], atendendo aos requisitos de segurança previstos pela U.S. NRC [47].

Em 1995, a metodologia de APS já estava bem estabelecida na indústria nuclear.

² Material radioativo liberado como resultado de um acidente severo.

Como resultado, a U.S.NRC emitiu as diretrizes para sua política, 60FR-42622 [48], determinando que a APS fosse utilizada para questões regulatórias. No entanto, a U.S.NRC também evidenciou que a política de defesa em profundidade deveria ser mantida como ferramenta de licenciamento e tomada de decisões regulatórias. Essa nova política introduziu, de modo efetivo, um novo paradigma regulatório denominado Regulação com Informação de Risco (*Risk-Informed Regulation*, RIR), em que os resultados da APS em conjunto com as tradicionais análises determinísticas devem ser usados na tomada de decisão regulatória [45].

A partir de 1998, a U.S.NRC publicou diversos guias regulatórios (*Regulatory Guides*) como resultado da nova abordagem de RIR, no qual se destaca o *Regulatory Guide* 1.174 [49] que faz uma abordagem sobre o uso da APS para tomada de decisão em mudanças na base de licenciamento, seja por alteração de alguma atividade ou característica de projeto. Em 2004, foi emitido o *Regulatory Guide* 1.200 [50], abordando as diretrizes para adequação das técnicas de APS para tomadas de decisão. Este último atua como um guia genérico de suporte ao projeto, enquanto o *Regulatory Guide* 1.174 [49] tem uma aplicação específica dentro do arcabouço dos *Regulatory Guides* da U.S.NRC.

Destaca-se, ainda, um estudo emitido em 2003, realizado por *Sandia National Laboratories*, que originou a publicação do NUREG/CR-6823 [51], em que se realiza uma abordagem técnica sobre a estimativa de parâmetros para APS.

Em harmonia ao que tem sido desenvolvido pela U.S.NRC, a IAEA tem desenvolvido uma série de guias e normas de segurança que refletem as melhores práticas de segurança, tais como: SSG-3 [52], SSG-4 [53], SF-1 [54] e SSR-2/1 [5]. Estes guias de segurança fornecem as recomendações para aplicação da análise probabilística de segurança no projeto e na operação de usinas nucleares.

Vale ressaltar que, na década de 90, os avanços tecnológicos possibilitaram uma maior capacidade de armazenamento e processamento de dados pelos computadores, fomentando assim, a utilização e o desenvolvimento das técnicas de análise probabilística de segurança.

2.3.2 Banco de dados de confiabilidade de equipamentos

Toda análise cujo objetivo seja obter medidas quantitativas do desempenho (confiabilidade/disponibilidade) dos sistemas de engenharia e da segurança de uma instalação requer o uso de uma base adequada de dados de confiabilidade de equipamentos.

As falhas de equipamentos podem ser a origem de acidentes e representar riscos econômicos, ambientais e para a vida humana. Na literatura são evidenciados alguns casos de falhas que resultaram em acidentes com repercussões trágicas, tais como: *Bhopal*, *Chernobyl*, *Challenger*, *Three Mile Island* e *Virginia Electric and Power Company*. Tais ocorrências mostraram a necessidade de se ter programas de garantia da qualidade com manutenções e inspeções bem estabelecidas e que sejam embasadas em dados de falhas de equipamentos.

Impulsionada pelos avanços tecnológicos que surgiram durante a Segunda Guerra Mundial e pelo desenvolvimento de equipamentos mais complexos, a engenharia de confiabilidade começou a destacar-se, e por volta dos anos 50, diversas fontes de dados sobre falhas de componentes começaram a ser publicadas.

Fragola [55] menciona que, nesta época, a partir de testes de ciclo de vida e de campo realizados em equipamentos, renomadas empresas como a *Radio Corporation of American* (RCA), *General Electric* (GE) e *Motorola* publicaram manuais compilados de dados de falhas.

Fragola [55] também destaca que o *Martin Titan Handbook* [56], em 1959, foi a primeira fonte de informação em confiabilidade amplamente divulgada, contendo dados genéricos de taxa de falhas de componentes elétricos, eletrônicos e mecânicos. Entretanto, os dados não faziam nenhuma menção a fatores de ajuste ou intervalos de confiança para os valores propostos. Um dos legados desta publicação foi a consagração da distribuição exponencial nos cálculos de probabilidade de falha dos equipamentos, a utilização da taxa de falha constante e a notação de falhas/ 10^6 horas.

O *Titan Handbook* [56] subsidiou o surgimento de diversos outros programas, dando origem a uma segunda geração de banco de dados de confiabilidade. Muitos desses foram impulsionados pelas demandas militares que se iniciaram nos anos 60, resultando em um vasto número de publicações, onde se destacam: *MIL-Handbook-217* [57], *Failure Rate Data Bank – FARADA* [58] e *RADC Non-Electronic Reliability Notebook* [59]. A título de exemplo, por volta dos anos 70, o FARADA já tinha mais de 400 integrantes associados, entre membros da indústria, instalações de manutenção/reparo e laboratórios do governo. A segunda geração foi marcada também pelo uso de limites de confiança baseados na distribuição χ^2 (chi-quadrado) o que propagou erros nos dados, pois as populações de equipamentos eram claramente heterogêneas.

Nos anos 70 e 80 deu-se início à terceira geração de banco de dados. Nesta geração os bancos de dados apresentaram faixas de valores para as estimativas de valores médios, o que facilitou a identificação das subpopulações heterogêneas. As taxas de falhas foram

subdivididas em: falhas em operação e falhas em demanda. Os modos de falha foram divididos em: catastróficos, degradados e incipientes. O modo de falha degradado descreve os casos onde houve perda da capacidade funcional do sistema, porém o equipamento continua em operação acima do nível mínimo aceitável. E o modo de falha incipiente ocorre quando não houve perda da função, mas existem indicações que a perda da função ocorreria caso não tivessem sido realizados os reparos e manutenções necessários.

Fruto desta terceira geração de banco de dados, a norma IEEE-500 (1984) [60] foi concebida para coletar, codificar e apresentar os dados de falhas de equipamentos nos diferentes contextos onde eles ocorrem, corrigindo alguns erros da geração anterior. Informações dos equipamentos, tais como tipo de aplicação (uso funcional ou serviço), tipo de ambiente (externo ou interno), tipo de operação (manual, elétrico ou hidráulico) e dimensões, foram incorporadas aos bancos de dados.

Em 1989, a fim de tornar os dados de componentes genéricos amplamente disponíveis, a AIEA compilou dados de confiabilidade de componentes de várias fontes da literatura no documento IAEA-TECDOC-508 [61]. A Base de dados de confiabilidade de componentes da AIEA continha mais de 1000 registros, categorizados em 100 grupos de componentes e derivados de 21 fontes da literatura. Para criar um banco de dados genéricos, os 100 grupos de componentes da base foram agrupados em 20 tipos genéricos, por exemplo, todos os transformadores foram considerados um único tipo. Também foram selecionados os modos de falha, tais como: falha na partida, na operação, na abertura e no fechamento. Então foram plotados gráficos para cada grupo para os diferentes modos de falhas, a fim de se avaliar a dispersão (intervalo) dos dados das taxas de falha. A maioria das fontes de dados usadas para a base de dados da AIEA foram estudos de APS ou fontes que forneceram informações para estudos de APS, destaca-se dentre as 21 fontes: WASH-1400 [7], EPRI-NP-2433 [62], IEEE 500 [60] e NUREG/CR-2815 [9].

Mais recentemente, a U.S.NRC tem disponibilizado um arcabouço de publicações que aborda os resultados da experiência operacional de reatores americanos (<https://nrcoe.inl.gov/>) [17]. Este banco de dados está sob a gestão do *Idaho National Laboratory* (INL) e inclui dados atualizados provenientes da indústria nuclear americana. Originalmente, os dados de desempenho dos equipamentos e sistemas eram publicados no documento NUREG/CR-6928 [63], cuja última edição foi em 2007 e, desde então, têm sido atualizados periodicamente e disponibilizados no website <https://nrcoe.inl.gov/> [17]. Vale destacar que, segundo a NUREG/CR-6928 [63], a distribuição lognormal que foi amplamente utilizada em vários estudos no passado e, inclusive no relatório WASH-1400

[7], como modelo de distribuição de incerteza para a probabilidade de ocorrência de eventos básicos, passou a ser substituída pelas distribuições gama e beta para probabilidades relacionadas ao tempo de operação e probabilidades de falha na demanda, respectivamente.

No que diz respeito aos reatores nucleares de pesquisa, a necessidade de um banco de dados de confiabilidade específico para essa classe de instalação tem sido discutida desde meados da década de 1980. Em 1997, a AIEA publicou o documento IAEA-TECDOC-930 [64] como resultado de um projeto de pesquisa coordenado por essa organização, trazendo dados genéricos de confiabilidade de componentes de diversos tipos de reatores de pesquisa. Mais recentemente, em 2020, foi publicado o documento IAEA-TECDOC-1922 [65], que além de atualizar os dados de confiabilidade de componentes do documento IAEA-TECDOC-930 [64], expandiu o escopo da base de dados e abordou questões relacionadas à preparação e aplicação de dados, reuniu informações sobre eventos iniciadores, falhas de causa comum e confiabilidade de sistemas digitais de controle.

2.3.3 Análise de confiabilidade humana

Para se obter uma medida mais precisa da confiabilidade de um sistema ou do risco associado a uma instalação, fatores humanos devem ser considerados. A análise de projetos de sistemas, procedimentos operacionais e relatórios pós-acidente mostram que o erro humano pode ser um iniciador imediato de acidente ou pode agravar a situação de um acidente. Se as probabilidades de erro humano (*Human Error Probabilities*, HEPs) não forem incorporadas à análise, os resultados da confiabilidade do sistema e da segurança da instalação ficam incompletos e muitas vezes subestimados. No entanto, para que HEPs sejam estimadas, é preciso compreender e modelar o comportamento humano, o que representa um grande desafio. A literatura mostra não haver um forte consenso sobre a melhor forma de modelar todos os tipos de ações humanas e, assim, quantificar as HEPs. As suposições, mecanismos e abordagens usados por qualquer modelo humano específico não podem ser aplicados a todas as atividades humanas [66]. Desta maneira, modelos dedicados devem ser desenvolvidos, contudo esses modelos, em geral, partem de conhecimentos prévios [67].

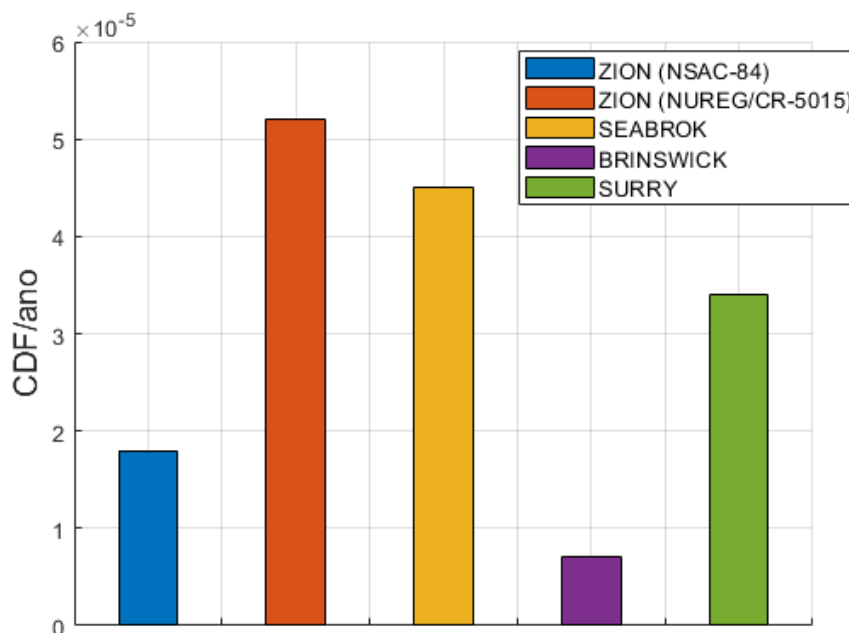
Os acidentes em Three Mile Island e Chernobyl mostram claramente como os erros humanos podem derrotar os sistemas de segurança e desempenhar um papel dominante na progressão dos acidentes. Frente à importância do assunto e motivada pelo acidente em TMI, a U.S.NRC emitiu o guia NUREG/CR-1278 [68] que contém métodos, modelos e estimativas de HEPs para plantas nucleares de potência.

Em especial, como resultado da avaliação de segurança de plantas nucleares americanas em baixa potência e em modo de desligamento, a emissão do documento NUREG-1449 [69] conduziu a um aumento das preocupações a respeito da confiabilidade humana para estes modos de operação. Este assunto deu origem a um projeto de pesquisa realizado por *Brookhaven National Laboratory* e *Sandia National Commission* para identificar aspectos únicos de desempenho humano durante as condições de baixa potência e desligamento da planta. Este projeto resultou na publicação NUREG/CR-6093 [70], a qual documenta os resultados da análise da experiência operacional em baixa potência e no modo de desligamento, além de descrever um plano aprimorado do programa de Análise de Confiabilidade Humana.

2.3.4 Avaliação probabilística de segurança para modos de baixa potência e desligamento

O relatório NUREG-1449 [69] apresenta um compilado de estudos de avaliação probabilística de segurança para plantas nucleares de potência no modo de desligamento e em paradas para troca de combustíveis, ressaltando que, até a data desta publicação, este modo de operação não havia sido extensivamente estudado e não havia um bom entendimento sobre o assunto, se comparado aos estudos para operação em potência. Os estudos citados nos itens 2.3.4.1 a 2.3.4.5 contêm estimativas de frequência de dano ao núcleo, conforme ilustrado na Figura 4. Vale ressaltar que as estimativas de CDF calculadas em cada estudo são diretamente dependentes das operações conduzidas nas paradas de desligamento, do nível de detalhe dos modelos (ex.: erro humano, manutenções/testes, eventos internos/externos e falhas de causa comum) e do refinamento do banco de dados de confiabilidade.

Figura 4 – Resultados de Análises Probabilísticas de Segurança (APS) para o modo de desligamento de plantas americanas.



Fonte: Adaptado NUREG-1449 [69].

2.3.4.1 NSAC-84

NSAC-84 [71] foi um estudo extensivo de APS, completado em 1981, da planta nuclear Zion. Árvores de falhas foram desenvolvidas para considerar as mudanças das condições da planta durante o modo de desligamento. Nesse estudo, erros humanos foram também considerados. Os eventos iniciadores considerados no estudo foram perda do Sistema de Remoção de Calor Residual, Acidente de Perda de Refrigerante (*Loss of Coolant Accident*, LOCA) e Sobrepressurização a frio. Um banco de dados específico foi desenvolvido para a planta de Zion e usado na quantificação das árvores de falhas.

O estudo estimou um CDF de 1,8E-5/ano para a planta no modo de desligamento. A perda do Sistema de Remoção de Calor Residual (SRCR) foi o evento iniciador com maior contribuição, 56% do CDF total. Destacaram-se no estudo as falhas durante a operação de redução de inventário do sistema de resfriamento (*midloop*³), incluindo erros do operador e indisponibilidade de equipamentos, que totalizaram 61% do CDF total. Falhas do operador durante operações com *midloop* contabilizaram sozinhas 44% do CDF total.

³ O nível da água do sistema de resfriamento do reator é mantido abaixo do topo da perna quente do primário.

2.3.4.2 NUREG/CR-5015

O documento NUREG/CR-5015 [72] foi emitido em resposta às preocupações relativas à perda do Sistema de Remoção de Calor Residual para reatores de água pressurizada (*Pressurized Water Reactor, PWR*), abordado no estudo NSAC-84 [71]. O NUREG/CR-5015 utilizou a metodologia de NSAC-84 (baseado nas configurações da planta ZION) com algumas modificações, que incluíram a perda do Sistema Elétrico Externo (*Loss Of Offsite Power, LOOP*) como evento iniciador, utilizando uma base de dados genérica para este evento, baseada em experiências de reatores PWR no período compreendido entre 1976 e 1986.

O CDF estimado foi de $5,2E-5$ /ano para a planta no modo de desligamento. As contribuições dos eventos iniciadores para o CDF total da planta foram: Perda do SRCR - 82%; perda do Sistema Elétrico Externo - 10%; e Acidente de Perda de Refrigerante - 8%. Os resultados apresentados em NUREG/CR-5015 corroboram com aqueles encontrados em NSAC-84 sobre a dominância do risco provocado por fatores humanos durante operações com *midloop*.

2.3.4.3 Seabrook

Segundo a NUREG-1449 [69], as informações foram coletadas de várias apresentações realizadas para a U.S.NRC sobre o licenciamento da usina nuclear de Seabrook. O estudo acrescentou a APS de nível 3 da planta, onde foram examinadas as probabilidades de ocorrência de dano ao núcleo durante os estados da planta em desligado a quente, desligado a frio e troca de combustíveis. Os termos fonte e as consequências para o público também foram consideradas. Este estudo utilizou a metodologia usada em NSAC-84 [71], entretanto incluiu incêndio e inundação como eventos iniciadores, além de realizar a análise de incerteza dos resultados.

Para a planta no modo de desligamento, foi estimado um CDF total de $4,5E-5$ /ano e 71% do CDF ocorreram durante a condição de *midloop*.

2.3.4.4 Brunswick (NSAC-83)

O estudo realizado para a planta de Brunswick [73] avaliou o desempenho e a disponibilidade do Sistema de Remoção de Calor Residual (SRCR) no modo de desligamento, considerando uma variedade de cenários que desafiavam o correto

funcionamento desse sistema. A falha do SRCR, considerada como um evento que pode levar a um dano ao núcleo, apresentou probabilidade de ocorrência estimada em $7,0E-6$ /ano. O modo de falha comum dos trocadores de calor do SRCR foi destacado como um dos eventos com maior contribuição para o acidente.

2.3.4.5 Surry

Foi realizado um estudo de APS da planta nuclear Surry no modo de desligamento e em baixa potência [74, 75], que foi dividido em duas fases. A Fase 1 consistiu em um estudo de triagem para determinar quais sequências de acidentes seriam analisadas com mais detalhes. Na Fase 2 foi realizada uma análise detalhada das sequências de acidentes dominantes identificadas na Fase 1. A APS propriamente dita foi realizada em duas partes: uma análise das frequências de acidentes (nível 1), seguida por uma análise da progressão dos acidentes e das consequências (níveis 2/3).

A Fase 2 teve como principais objetivos: (1) estimar as frequências de acidentes severos que poderiam ser iniciadas durante a operação em *midloop*; (2) comparar as frequências estimadas de danos ao núcleo, sequências de acidentes e outros resultados qualitativos e quantitativos deste estudo com os de acidentes iniciados durante a operação da planta em potência; e (3) demonstrar metodologias para análise de sequências de acidentes para plantas em modos de operação diferentes da plena potência.

A abordagem foi usada para definir diferentes estados de operação da planta, dentro de cada tipo de parada (interrupção). As paradas foram agrupadas em quatro tipos: recarga / troca de combustíveis; manutenção com o inventário de refrigerante drenado; manutenção sem drenagem do inventário de refrigerante e utilizando o SRCR; e manutenção sem drenagem do inventário de refrigerante e sem o uso do SRCR. Durante a parada de troca de combustíveis, 15 estados operacionais foram utilizados para definir as atividades da planta.

O CDF estimado para a planta de Surry em modo de desligamento e baixa potência foi de $3,4E-5$ /ano. O erro do operador para mitigar o acidente apresentou a maior contribuição para o cálculo da frequência de dano ao núcleo. Foi destacada, também, a contribuição de eventos de incêndio para a frequência de dano ao núcleo durante operações em condição de *midloop*, que foi estimada em $2,03E-5$ /ano.

2.4 Projeto de instalações nucleares baseado em informação do risco

Nos EUA, o desenvolvimento de projetos baseados em informação do risco teve

início quando a U.S.NRC emitiu uma declaração de política, revisada em 1995, sobre o uso da APS na tomada de decisões, conforme apresentado em 60FR-42622 [48], incluindo uma visão mais positiva sobre o papel que os resultados dessa análise deveriam ter no apoio às decisões regulatórias. Os eventos que mais favoreceram investimentos significativos em APS por parte das operadoras de instalações nucleares, durante esse período, foram a emissão do *Regulatory Guide* 1.174 [49], de guias regulatórios específicos associados ao *Regulatory Guide* 1.174 e do plano padrão de revisão (*Standard Review Plan*). Pela primeira vez, a U.S.NRC forneceu em seus guias regulatórios critérios claros para a revisão/alteração de atividades e características de projeto em plantas nucleares de potência, utilizando a informação sobre o risco associado à instalação para subsidiar seu licenciamento, incluindo critérios quantitativos de aceitação do risco baseados em CDF ou LERF. Antes da publicação desses guias, as tentativas da indústria em apresentar argumentos baseados em risco para obter alguma isenção na regulamentação ou relaxamento em alguns requisitos eram muito difíceis de serem aceitas e revisadas pela U.S.NRC [76].

Alguns trabalhos acadêmicos têm sido desenvolvidos sob a égide de informação do risco para otimização de projetos, principalmente quando se trata de projetos com algum tipo de característica especial. Dentre estes, destacam-se alguns trabalhos como o de Mizuno et al. [77] que apresentou um estudo de APS Nível 1 para eventos internos aplicado ao projeto do reator *IRIS – International Reactor Innovative and Secure*, para operação em potência. Este reator apresenta características inovadoras com um arranjo integrado que possui, inclusive, bombas de circulação do refrigerante do núcleo dentro do vaso de pressão do reator. Segundo o autor, o arranjo integrado elimina tubulações, resultando em uma configuração econômica e que praticamente elimina a possibilidade de acidentes mais severos como o LOCA. O foco do trabalho documentado em [77] foi avaliar as características de projeto do IRIS, em sua fase conceitual, subsidiando o projeto e seu pré-licenciamento. Foram realizadas alterações em um projeto base e avaliados os CDFs para as novas configurações. Adicionalmente, foram realizadas combinações entre as diferentes configurações até se obter um projeto otimizado com uma baixa métrica de risco. O projeto base inicial estava associado a um CDF de $1,98E-6$ /ano e o projeto otimizado apresentou um CDF de $1,21E-8$ /ano.

Outro trabalho importante, que segue a mesma linha de pesquisa, foi desenvolvido por Deng et al. em [78]. Neste trabalho, foi aplicada uma APS Nível 1 para eventos internos com reator em potência, ao projeto de um reator modular pequeno do tipo multipropósito denominado ACP100 – *Advanced China Power*. O autor ressalta que a APS comprovou ter

vantagens únicas na demonstração do nível de segurança global da instalação, avaliando o equilíbrio e identificando as vulnerabilidades no projeto, referindo-se a um projeto com informação do risco (*Risk-Informed Design*). No trabalho, foram propostas alterações no projeto original que melhoraram o CDF da instalação de $1,47E-7$ /ano para $6,78E-8$ /ano. Destacam-se, também, as análises de importância dos eventos iniciadores, assim como a baixa contribuição da perda do sistema elétrico externo para o acidente de dano ao núcleo, contribuindo com apenas 0,03% no projeto original.

Em [79], Oh e Hwang utilizaram a abordagem de otimização de projeto baseado em informação do risco. Foi desenvolvido um modelo de APS para um reator japonês, tecnologia APR+ com características de segurança avançada, incluindo sistema passivo de reposição de água e quatro diesel geradores de emergência. O trabalho parte da premissa que, em potência, a frequência de dano ao núcleo para a planta APR+ tem um decréscimo significativo em relação à planta base APR1400. Entretanto, em baixa potência e no modo desligamento não houve melhoras substanciais do risco. O trabalho ressalta que a planta apresenta 15 estados distintos durante as paradas para troca de combustíveis, sendo que os estados números 4 e 12 apresentam dois subestados cada um. Então, o estudo aplica a metodologia de APS para a planta APR+ no modo desligado, durante a troca de combustíveis, e apresenta alternativas de projeto para minimizar o risco para a planta. O CDF é considerado como métrica de risco, que apresenta diferentes valores dependendo do estado da planta. São identificados, também, diferentes eventos iniciadores que dependem do estado da planta. O risco é quantificado através do método dos cortes mínimos (*cutsets*). Por fim, é realizada uma análise de sensibilidade para as alternativas de projeto.

Em [80], Ahmed et al. aplicaram a metodologia de APS em um reator de pesquisa de potência zero chamado AGN-201K. O trabalho destaca a dificuldade de se obter um banco de dados de confiabilidade de componentes de reatores de pesquisa e, por este motivo, foram utilizados dados genéricos de componentes e equipamentos de plantas nucleares de potência. No estudo, foram identificados os componentes críticos para a segurança da instalação, foram propostas melhorias para o sistema de proteção do reator, além da realização de análises de sensibilidade das taxas de falha dos componentes modelados. Por se tratar de um reator de potência zero, o escopo da APS envolveu o conceito de falha do sistema de proteção, pois o conceito de acidente de dano ao núcleo não se mostrava aplicável a esse caso.

Em [81], Kowal e Torabi realizaram um estudo da confiabilidade de diferentes arquiteturas do sistema elétrico de um reator de teste de alta temperatura resfriado a gás

(*HTTR - High Temperature Gas-cooled Reactors*). O objetivo do trabalho foi avaliar a frequência de interrupções inesperadas devido à falha do sistema elétrico da planta. A análise foi realizada aplicando-se a técnica de Análise de Modos de Falha e Efeitos (*Failure Mode and Effect Analysis*, FMEA). Primeiramente, foi considerada a arquitetura do sistema elétrico comercial padrão e sugeridas quatro modificações que pudessem melhorar a confiabilidade do fornecimento de energia. O projeto inicial do sistema elétrico previa o fornecimento de energia para a planta por apenas uma LT. Então, foram propostas quatro modificações para o novo projeto: (1) adição de uma segunda LT; (2) adição de um disjuntor de interligação entre os barramentos de distribuição em energia de baixa tensão; (3) adição de um disjuntor de interligação entre os barramentos de emergência; e (4) adição de um inversor para o sistema de energia ininterrupta. Adicionalmente, foram realizadas análises relativas às incertezas das taxas de falha dos componentes modelados, além de ter sido examinado o impacto do envelhecimento dos componentes para a confiabilidade do sistema elétrico.

3 METODOLOGIA

A importância dos sistemas elétricos para a segurança das instalações nucleares, evidenciada principalmente após o acidente da Usina Nuclear de Fukushima Daiichi, assim como o surgimento de novas tecnologias e diversificação da funcionalidade/aplicação dos reatores nucleares têm demandado ferramentas de análise de segurança que possam auxiliar na escolha de projetos otimizados e no licenciamento das instalações.

Adicionalmente, a realização da avaliação de segurança dos sistemas elétricos de instalações nucleares no âmbito de uma avaliação integrada, depende da análise de todos os sistemas de segurança da instalação, incluindo os sistemas de suporte e suas interfaces. Devido à elevada quantidade de componentes, estruturas, sistemas e interações a serem avaliadas, faz-se necessário a utilização de ferramentas robustas de análise. Assim, na metodologia proposta neste trabalho, adotaram-se os conceitos da APS Nível 1 e os métodos de análise implementados no programa computacional CAFTA [82] para modelagem e análise dos sistemas de uma instalação nuclear, tomando por base a frequência de dano ao núcleo (*Core Damage Frequency*, CDF) como medida de risco.

Diante da importância do assunto e complexidade das análises, este capítulo é iniciado com um embasamento teórico das principais técnicas e conceitos de APS, o qual subsidia o entendimento e desenvolvimento da metodologia. Em seguida, são apresentadas as principais técnicas de modelagem do CAFTA [82], a fonte de dados de confiabilidade consultada para os componentes a serem modelados e o método de avaliação probabilística de segurança proposto para projetos de sistemas elétricos de instalações nucleares. Por fim, o passo a passo para aplicação da metodologia proposta é apresentado, considerando um modelo simplificado de um sistema elétrico CA.

3.1 Fundamentos da análise probabilística de segurança de instalações nucleares

As consequências das falhas de sistemas complexos, como os das usinas nucleares, são significativas e podem causar efeitos adversos para o público, ao meio ambiente e à economia da região. A Análise Probabilística de Risco, também conhecida como Análise Probabilística de Segurança (APS), consiste em uma metodologia baseada em técnicas sistemáticas para se identificar cenários de eventos de falha que possam ter consequências

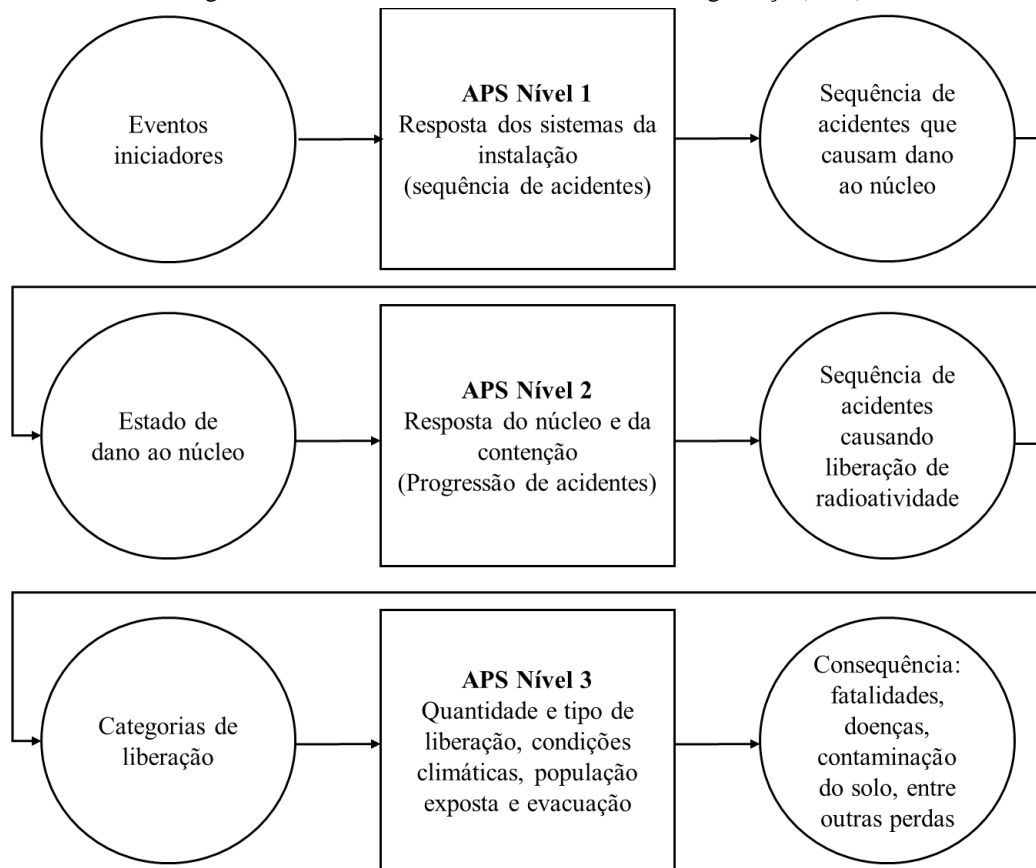
indesejáveis significativas na instalação e, em seguida, quantificar as frequências e consequências desses cenários para se obter estimativas de risco. Inicialmente, a APS de instalações nucleares foi desenvolvida para se estimar a probabilidade de resultados adversos, como danos ao núcleo do reator e liberação de material radioativo para o meio ambiente. Recentemente, a metodologia de APS tornou-se uma ferramenta aplicável a todo o ciclo de vida da instalação, para auxiliar nas fases de licenciamento, projeto, fabricação, construção, operação, manutenção, segurança e descomissionamento. Hoje, um espectro amplo de organizações nos setores de defesa, energia, aeroespacial, saúde e segurança contam com a metodologia da APS para tomar decisões referentes ao ciclo de vida, regulamentações e políticas com base em informações sobre riscos e que sejam proporcionais aos riscos de sistemas de engenharia complexos [66].

3.1.1 Níveis da APS de uma instalação nuclear

A APS é geralmente dividida em três níveis, conforme Figura 5:

- Nível 1: estima a frequência de acidentes que causam dano ao núcleo do reator, comumente chamada de frequência de dano ao núcleo (*Core Damage Frequency, CDF*);
- Nível 2: caracteriza o material radioativo que possa ser liberado e estima a frequência de liberação para o ambiente externo em caso de acidente, considerando os acidentes de dano ao núcleo identificados no Nível 1 da APS; e
- Nível 3: tem, como ponto de partida, o acidente de liberação de radioatividade calculado no Nível 2 da APS, estimando as consequências em termos de fatalidades ou danos aos indivíduos do público e as consequências indesejáveis ao meio ambiente.

Figura 5 – Níveis da Análise Probabilística de Segurança (APS).



Fonte: Modarres e Kim [66].

3.1.2 Elementos básicos da APS

Em uma APS, são avaliados os riscos associados a sistemas de engenharia complexos, delineando um grande número de cenários de eventos que levam a consequências indesejáveis definidas pelo analista. Em geral, um cenário de eventos consiste nos seguintes elementos [66]:

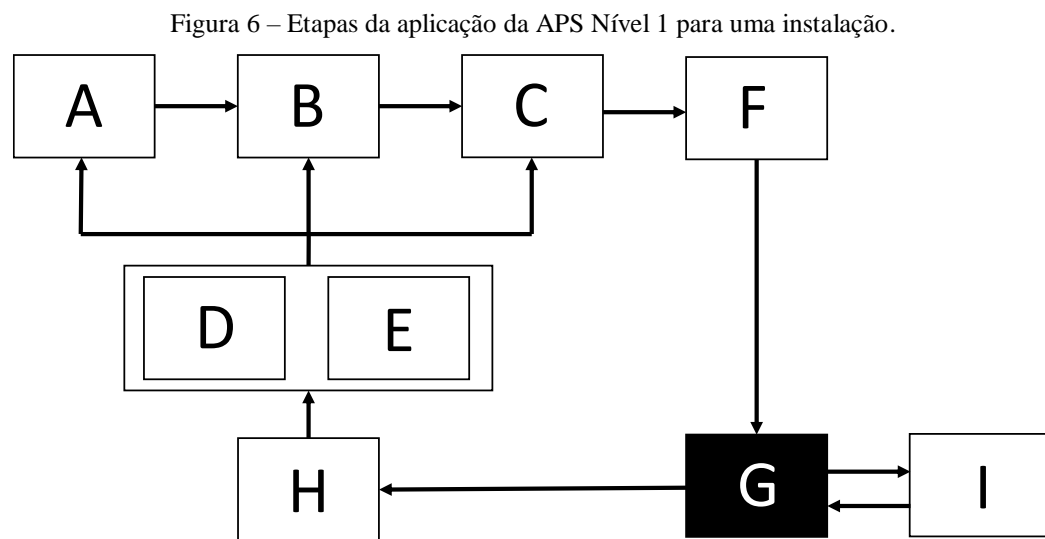
- Evento Iniciador: Um evento que desencadeia uma condição anormal nos sistemas e que, se não for respondido corretamente, pode levar a consequências indesejáveis;
- Eventos de hardware (componentes/equipamentos): Falha ou indisponibilidade dos componentes de hardware dos sistemas;
- Eventos de software (programa ou sistema de processamento de dados): Falha ou indisponibilidade dos componentes de software dos sistemas;
- Eventos de erro humano: Erros dos operadores ou de outros membros do corpo técnico da planta; e
- Eventos de não recuperação: Falha na recuperação dos componentes que

apresentaram falha ou estavam indisponíveis.

Se um evento iniciador ocorre internamente à planta ou por um motivo relacionado aos sistemas da planta, é chamado de evento interno, e a APS para eventos internos é referida como APS de eventos internos. Se for causado por um motivo externo à planta ou fora dos sistemas da planta, é chamado de evento externo, e a APS para eventos externos é referida como uma APS de eventos externos (por exemplo, APS Sísmica). Adicionalmente, a APS recebe uma classificação em relação ao estado operacional da planta quando ocorre o evento iniciador, podendo ser uma APS para a planta em potência ou APS para a planta em baixa potência e em modo de desligamento.

3.1.3 Etapas para se conduzir a APS Nível 1

A Figura 6 mostra as etapas para se realizar a APS Nível 1 em uma instalação. Cada etapa é discutida em detalhes nas seções seguintes.



Fonte: Adaptado Modarres e Kim [66].

Onde:

- [A] Identificação dos eventos iniciadores;
- [B] Delineamento da sequência de acidentes (árvore de eventos);
- [C] Análise dos sistemas – modelo lógico (árvore de falhas);
- [D] Banco de dados de confiabilidade;
- [E] Análise de confiabilidade humana;
- [F] Integração do modelo e quantificação;
- [G] Interpretação dos resultados;
- [H] Análise de sensibilidade; e
- [I] Classificação de importância.

3.1.3.1 Identificação dos eventos iniciadores

Os eventos iniciadores são os primeiros eventos que tiram a instalação nuclear de sua condição normal de operação e têm o potencial de dar início a um cenário de eventos que levam a uma exposição ao perigo. Na APS Nível 1, são eventos ou condições anormais que, se não forem respondidos de forma correta e oportuna, podem resultar em danos ao núcleo do reator. Durante a operação normal da planta, falhas de equipamentos, eventos naturais ou outros eventos que podem ocorrer externamente à planta, como um incêndio externo ou uma inundação, podem fazer com que ela entre em um estado não usual ou transitório. Quando um transiente tem início, há duas possibilidades. Em primeiro lugar, o estado da planta pode ser tal que nenhuma outra função seja necessária para mantê-la em uma condição segura. Aqui, o termo seguro refere-se a um estado em que a chance de evoluir a uma condição perigosa é insignificante. Neste caso, barreiras inerentes ou atuadas de modo passivo previnem qualquer exposição ao perigo. A segunda possibilidade é um estado em que certas funções de segurança/proteção, realizadas por meio de atuações dos sistemas ou ações humanas, são necessárias para evitar a exposição ao perigo. As análises probabilísticas de segurança abordam, em especial, a segunda classe de eventos [66].

Um dos principais métodos para se identificar eventos iniciadores é desenvolver um diagrama de blocos funcional dos sistemas envolvidos na operação normal da instalação. Cada função pode então ser decomposta em sistemas, subsistemas e componentes que, individualmente ou em combinação, realizam essas funções. O diagrama de blocos funcional é usado para rastrear o efeito de eventos de falha que levam à perda das funções de segurança.

3.1.3.2 Delineamento das sequências de acidente

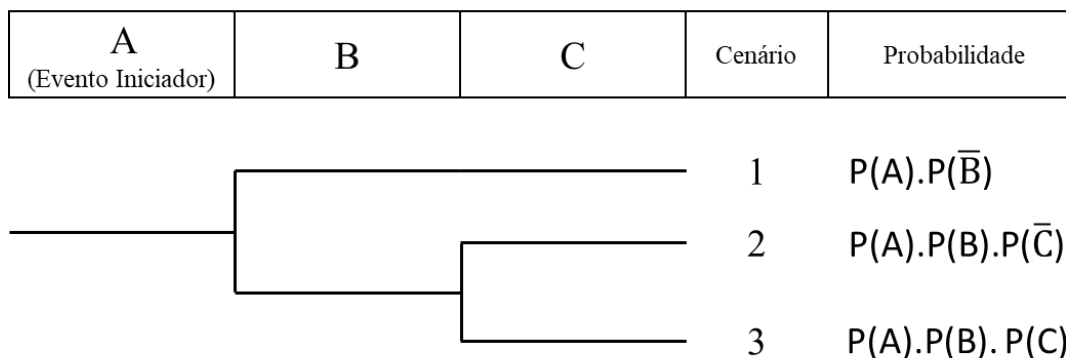
O objetivo desta etapa da APS é desenvolver um conjunto completo de cenários após a ocorrência de cada evento iniciador. Os cenários que descrevem a resposta funcional da instalação aos eventos iniciadores são exibidos em árvores de eventos. A árvore de eventos reflete os cenários de eventos específicos (em termos de perda de barreiras, erros humanos, falhas de sistemas de proteção ou mitigação). Exemplos de sistemas de mitigação em plantas nucleares de potência são os sistemas de resfriamento de emergência do núcleo e sistemas de resfriamento da contenção. Um exemplo de sistema de proteção é o sistema de desligamento do reator. Portanto, uma árvore de eventos delinea totalmente a resposta geral da planta a um evento iniciador e serve como ferramenta principal para análises adicionais na APS. O seguinte procedimento deve ser seguido nesta etapa da APS [66]:

- Identificação das funções de mitigação para cada evento iniciador;
- Identificação das ações humanas e dos sistemas/equipamentos associados a cada função, juntamente com as circunstâncias específicas de sucesso ou falha; e
- Desenvolvimento de uma árvore de eventos para cada evento iniciador, delineando as condições de sucesso, condições de falha, introduzindo fenômenos de progressão de eventos e efeitos finais (ou seja, resultados ou perdas consequentes) de cada cenário. No caso da APS Nível 1, o estado final de uma sequência pode ser o dano ao núcleo do reator ou a mitigação bem sucedida do acidente.

3.1.3.2.1 Árvores de eventos

As árvores de eventos envolvem eventos cronologicamente próximos desenvolvidos da esquerda para a direita a partir do evento iniciador. Os pontos de ramificações das árvores de eventos marcam a ocorrência dos eventos subsequentes e se eles têm sucesso (ramo superior) ou se falham (ramo inferior) na missão. A Figura 7 ilustra uma árvore de eventos típica. Nesta árvore de eventos, a coluna cenário identifica os possíveis cenários após a ocorrência do evento iniciador e dos eventos subsequentes, a coluna seguinte, a probabilidade de ocorrência de cada um dos cenários identificados.

Figura 7 – Exemplo ilustrativo de uma árvore de eventos.



Fonte: Adaptado Marcelo Martins [83].

Na Figura 7 foi considerado que os eventos são independentes, onde $P(X)$ representa a probabilidade do evento X falhar e $P(\bar{X})$ a probabilidade de X não falhar, sendo $P(\bar{X})=1-P(X)$.

3.1.3.3 Análise de sistemas

Modelos lógicos dos sistemas da planta, tais como árvores de falhas, podem ser

usados para estimar a frequência de falhas dos eventos considerados no desenvolvimento das árvores de eventos. As árvores de falhas permitem que sejam obtidas expressões booleanas que representam sua lógica binária, com base em operadores booleanos, tais como OR e AND. A probabilidade de falha do evento topo da árvore de falhas pode, então, ser quantificada a partir da expressão booleana que representa o conjunto de cortes mínimos desse evento. Essas árvores de falhas mostram, também, as combinações importantes de falhas de hardware (componentes/equipamentos), erros humanos ou falhas de software que causam as falhas dos eventos principais correspondentes.

3.1.3.3.1 Árvores de falhas

A análise de árvores de falhas consiste em uma técnica analítica dedutiva, em que um estado indesejado do sistema é especificado (geralmente um estado que é crítico do ponto de vista de segurança), e o sistema é então analisado no contexto de seu ambiente e operação para encontrar todas as maneiras críveis pelas quais o evento indesejado pode ocorrer. A árvore de falhas é um modelo gráfico das várias combinações paralelas e sequenciais de falhas que resultarão na ocorrência do evento indesejado pré definido. As falhas podem ser eventos associados a falhas funcionais ou estruturais de componentes, erros humanos ou quaisquer outros eventos pertinentes que podem levar ao evento indesejado. Uma árvore de falhas, portanto, descreve as inter-relações lógicas de eventos básicos que levam ao evento indesejado, que é o evento principal da árvore de falhas, chamado Evento Topo [84].

Em geral, desenvolve-se uma árvore de falhas para cada evento principal incluído nos cabeçalhos da árvore de eventos, para os quais não existam dados históricos reais de falhas e com os quais esteja associado um subsistema que consiste em vários componentes ou uma combinação de ações humanas.

- As dependências de um subsistema com outros subsistemas e as dependências entre os componentes devem ser consideradas no modelo de árvore de falhas. As falhas de causa comum (*Common Cause Failures*, CCFs), as quais envolvem falhas dependentes implícitas de vários componentes redundantes, também podem ser modeladas explicitamente nas árvores de falhas e serão discutidas com mais detalhes mais adiante neste capítulo; e
- Todas as causas potenciais e probabilisticamente quantificáveis de falha em termos de equipamentos, software, teste e manutenção ou erro humano devem ser incluídas no modelo de árvore de falhas.

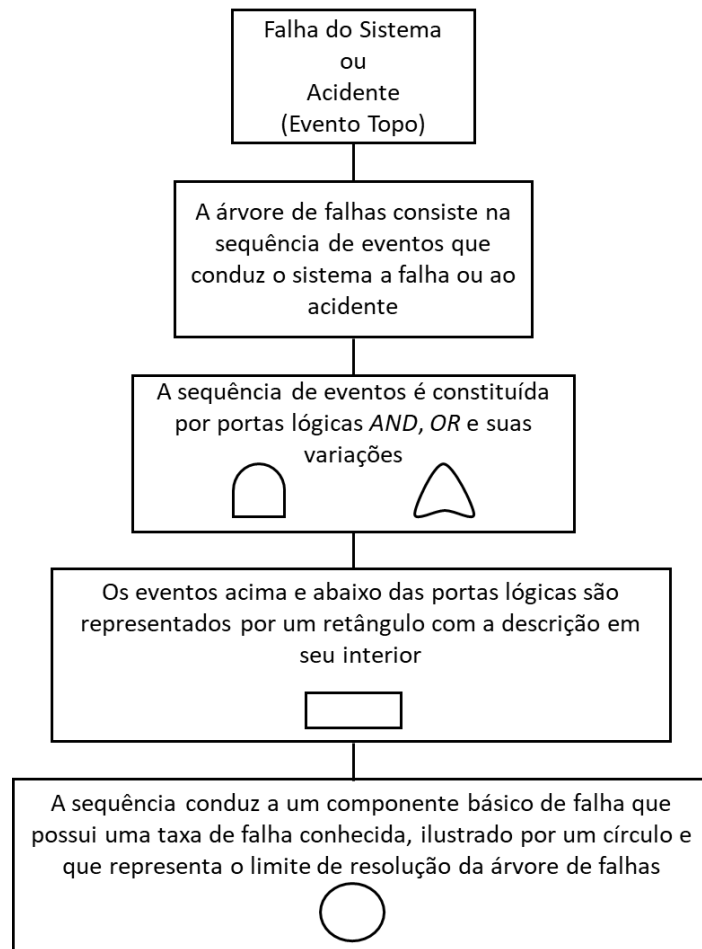
É importante destacar que uma árvore de falhas não é um modelo que requer a inclusão de todas as falhas possíveis do sistema ou todas as causas possíveis para a falha do sistema. Uma árvore de falhas é desenvolvida a partir de um determinado evento topo, que corresponde a algum modo de falha específico do sistema, e a árvore de falhas inclui apenas as falhas que contribuem para este evento topo. Além disso, essas falhas não são exaustivas e cobrem apenas as falhas identificadas, avaliadas pelo analista. Também é importante ressaltar que uma árvore de falhas não é em si um modelo quantitativo. É um modelo qualitativo que pode ser avaliado quantitativamente, o que frequentemente ocorre [84].

Resumidamente, uma árvore de falhas representa uma ferramenta de análise dedutiva, do tipo *top-down*, que pode [85]:

1. Direcionar a análise para identificar as falhas do sistema relevantes para o estudo;
2. Apontar todos os aspectos importantes para a falha do sistema;
3. Fornecer auxílio gráfico para dar visibilidade à gestão do sistema, no que se refere a modificações realizadas no projeto;
4. Fornecer opções para análise qualitativa e quantitativa da confiabilidade do sistema;
5. Permitir que o analista se concentre em uma falha específica do sistema por vez; e
6. Fornecer uma visão sobre o comportamento do sistema.

Uma árvore de falhas é um complexo de entidades conhecidas por "portas" que servem para permitir ou inibir a passagem da lógica de falhas para a parte superior da árvore. As portas mostram as relações de eventos necessárias para a ocorrência de um evento "superior". O evento "superior" é a "saída" da porta; os eventos "inferiores" são as "entradas" para a porta. O símbolo da porta denota o tipo de relacionamento dos eventos de entrada necessários para o evento de saída. Assim, as portas são análogas às chaves em um circuito elétrico ou à configuração de duas válvulas em um *layout* de tubulação [84]. A Figura 8 ilustra a estrutura fundamental de uma árvore de falhas.

Figura 8 – Estrutura fundamental da árvore de falhas de um sistema.

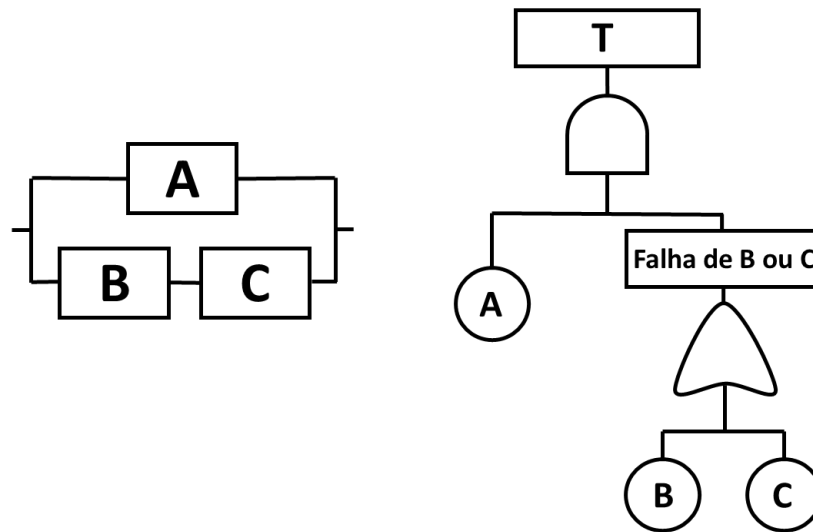


Fonte: Kumamoto e Henley [85].

As portas lógicas *AND* e *OR* possuem equivalência com diagramas de blocos de confiabilidade. A porta *AND* modela os casos de componentes redundantes, sendo portanto equivalente a blocos paralelos; e a porta *OR* modela os casos de componentes em série, no qual a falha de qualquer componente conduz ao evento topo.

A Figura 9 mostra um exemplo simples de árvore de falhas e seu diagrama de blocos de confiabilidade análogo. Nesta figura, o evento topo T da árvore de falhas representa a falha do sistema e os eventos básicos A, B e C representam a falha dos seus respectivos componentes. Assim, para que o evento topo T ocorra é necessária a falha do componente A juntamente com a falha do componente B ou C.

Figura 9 – Exemplo comparativo entre um diagrama de blocos de confiabilidade e uma árvore de falhas de um sistema simplificado.



Fonte: Adaptado Marcelo Martins [83].

Para a avaliação quantitativa que tem como objetivo a determinação da probabilidade de ocorrência do evento topo, o método tradicionalmente utilizado é o método das substituições sucessivas que traduz a árvore de falhas em sua correspondente expressão booleana, através da determinação dos cortes mínimos. Um corte mínimo é um conjunto formado pela menor quantidade de eventos de falha, que caso ocorram simultaneamente, provocam a ocorrência do evento topo. Na Figura 9 existem dois cortes mínimos: $C_1 = \{A, B\}$ e $C_2 = \{A, C\}$.

Desta forma, após determinar todos os cortes mínimos de uma árvore de falhas, a probabilidade de ocorrência do seu evento topo T pode ser definida como sendo a probabilidade de ocorrência destes cortes mínimos:

$$P(T) = P(C_1 \cup C_2 \cup C_3 \cup \dots \cup C_n) \quad (3-1)$$

Onde C_1 a C_n representam todos os possíveis cortes mínimos da árvore de falhas.

Caso os cortes mínimos sejam mutuamente exclusivos entre si, a Equação 3-1 pode ser reescrita como:

$$P(T) = P(C_1) + P(C_2) + P(C_3) + \dots + P(C_n) \quad (3-2)$$

Se os eventos não forem mutuamente exclusivos, a Equação 3-3 irá representar um limite superior da probabilidade de ocorrência do evento topo T (falha do sistema):

$$P(T) \leq P(C_1) + P(C_2) + P(C_3) + \dots + P(C_n) \quad (3-3)$$

Ou o limite inferior da confiabilidade do sistema R_s :

$$R_S = 1 - P(T)$$

$$R_S \geq 1 - P(C_1) + P(C_2) + P(C_3) + \dots + P(C_n) \quad (3-4)$$

Para se determinar a exata confiabilidade do sistema, deve-se usar a Equação 3-1 para probabilidade de falha do sistema, que considera as possíveis intersecções entre os cortes mínimos.

3.1.3.3.2 Falhas de causa comum

A definição de CCF está ligada a uma compreensão da natureza e do significado de eventos dependentes. Considerando os eventos A e B, eles são dependentes quando [86]:

$$\begin{aligned} P[A \cap B] &= P[B|A]P[A] \\ &= P[A|B]P[B] \\ &\neq P[A]P[B] \end{aligned} \quad (3-5)$$

Onde $P[X]$ denota a probabilidade do evento X.

Na presença de dependências, muitas vezes, mas nem sempre, $P[A \cap B] > P[A]P[B]$. Portanto, se A e B representam falha das funções de segurança, a probabilidade real de ambas as falhas será maior que a probabilidade esperada, se essa probabilidade for calculada com base no pressuposto de independência.

As dependências que resultam em falhas podem ser classificadas de várias maneiras. Uma classificação útil para relacionar os dados operacionais às características de confiabilidade dos sistemas é categorizar as dependências com base no fato de serem originadas pelas características físicas e funcionais intrínsecas do sistema ou causadas por fatores externos. Portanto, a dependência pode ser intrínseca ou extrínseca ao sistema.

Uma dependência intrínseca se refere a casos em que o estado funcional de um componente é afetado pelo estado funcional de outro componente. Esses tipos de dependências normalmente se originam da maneira como o sistema é projetado para executar sua função pretendida.

Dependência extrínseca refere-se a casos em que a dependência ou acoplamento não é inerente ou pretendido nas características funcionais do sistema. A fonte e o mecanismo de tais dependências são frequentemente externos ao sistema como a condição ambiental ou a ação humana.

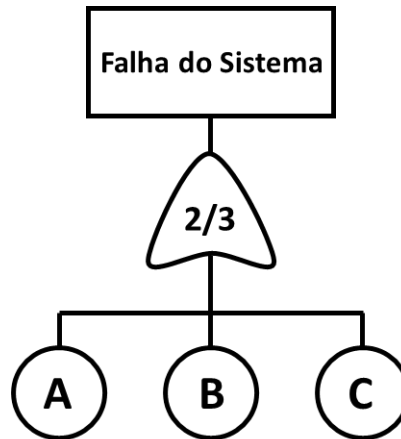
Falhas associadas à ocorrência de uma causa comum são geralmente decorrentes de problemas de projeto, das condições de operação ou de procedimentos de manutenção. Como

exemplo de falhas de causa comum provenientes de projeto, destaca-se a utilização de equipamentos ou sistemas redundantes idênticos adotados como estratégia para se obter a confiabilidade necessária ou especificada em normas de segurança, o que torna fundamental a consideração das possíveis falhas de causa comum.

A. Modelagem da CCF nas árvores de falhas

Para exemplificar a modelagem de CCF na árvore de falhas de um sistema, será adotado um modelo de 3 componentes idênticos (A, B e C), em que é considerado a necessidade de funcionamento de pelo menos 2 para que o sistema tenha sucesso na missão, ou seja, uma configuração 2 de 3. A árvore de falhas da Figura 10 representa o modelo exemplificado:

Figura 10 – Árvore de falhas referente a uma configuração 2 de 3 componentes de um sistema.

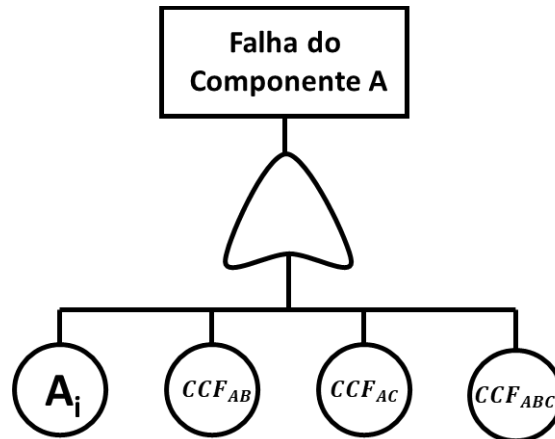


Fonte: NUREG/CR-5485 [87].

Os cortes mínimos do sistema são: $C1=\{A,B\}$; $C2=\{A,C\}$; e $C3=\{B,C\}$.

A árvore de falhas da Figura 10 deve ser expandida considerando os eventos básicos das falhas de causa comum para cada componente. Para o componente A, o evento básico A é substituído pelos eventos mostrados na Figura 11.

Figura 11 – Árvore de falhas expandida em relação às falhas de causa comum associadas ao componente A.



Fonte: NUREG/CR-5485 [87].

Quando todos os componentes são expandidos similarmente, os cortes mínimos do sistema são obtidos: $C1=\{A_i, B_i\}$; $C2=\{A_i, C_i\}$; $C3=\{B_i, C_i\}$; $C4=\{CCF_{AB}\}$; $C5=\{CCF_{AC}\}$; $C6=\{CCF_{BC}\}$; e $C7=\{CCF_{ABC}\}$.

O subíndice i representa falhas individuais dos respectivos componentes e o CCF representa a falha comum dos componentes.

Portanto:

$$\begin{aligned}
 P(\text{falha}) &= P(C1 + C2 + C3 + C4) \\
 P(\text{falha}) &= P(C1) + P(C2) + P(C3) + P(C4) \\
 P(\text{falha}) &= P(A_i)P(B_i) + P(A_i)P(C_i) + P(B_i)P(C_i) + \\
 &P(CCF_{AB}) + P(CCF_{AC}) + P(CCF_{BC}) + P(CCF_{ABC})
 \end{aligned} \tag{3-6}$$

É prática comum nas análises de risco e confiabilidade, assumir a mesma probabilidade para eventos idênticos ou similares envolvendo componentes idênticos ou até mesmo similares [87]. Sendo assim:

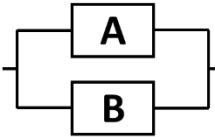
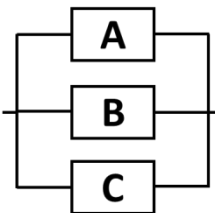
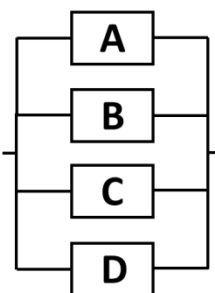
$$\begin{aligned}
 P(A_i) &= P(B_i) = P(C_i) = Q_1 \\
 P(CCF_{AB}) &= P(CCF_{AC}) = P(CCF_{BC}) = Q_2 \\
 P(CCF_{ABC}) &= Q_3
 \end{aligned}$$

Desta forma, a probabilidade de falha pode ser escrita como:

$$P(\text{falha}) = Q_T = 3(Q_1)^2 + 3Q_2 + Q_3 \tag{3-7}$$

A Tabela 2 apresenta de forma resumida o modelo de probabilidade de falha para alguns sistemas redundantes com seus respectivos critérios de sucesso.

Tabela 2 – Modelo de probabilidade de falha para diferentes configurações do sistema.

Diagrama de Blocos	Critério de Sucesso	Modelo de Probabilidade de Falha
	1 de 2	$Q_1^2+Q_2$
	2 de 2	$2Q_1+Q_2$
	1 de 3	$Q_1^3+3Q_1Q_2+Q_3$
	2 de 3	$3Q_1^2+3Q_2+Q_3$
	3 de 3	$3Q_1+3Q_2+Q_3$
	1 de 4	$Q_1^4+3Q_2^2+4Q_1Q_3+Q_4+6 Q_1^2 Q_2$
	2 de 4	$4Q_1^3+12 Q_1Q_2+3Q_2^2+4Q_3+Q_4$
	3 de 4	$6Q_1^3+6Q_2+4Q_3+Q_4$
	4 de 4	$6Q_1+6Q_2+4Q_3+Q_4$

Fonte: NUREG/CR-5485 [87].

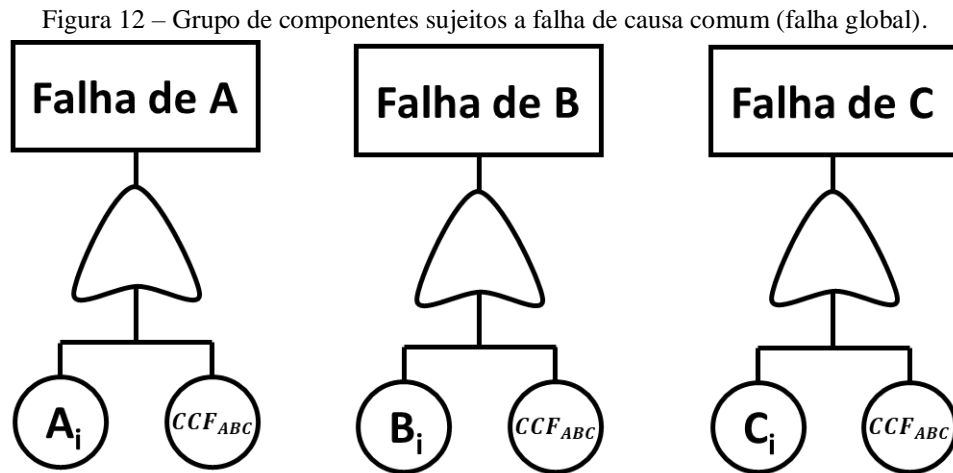
B. Quantificação da probabilidade de CCF

O objetivo básico do método é identificar os fatores de ponderação que ajustam a probabilidade de falha básica de forma que ela represente a probabilidade de falha de causa comum. Em outras palavras, os fatores de ponderação representam a probabilidade, dado que ocorreu uma falha de componente, de outros componentes semelhantes falharem pela mesma causa. Assim, o fator de ponderação pode ser considerado como a razão entre os eventos que falham em vários componentes e o número total de falhas. Além disso, se houver mais de dois componentes sendo tratados, os fatores de ponderação devem ser divididos para abordar as várias combinações potenciais.

Modelo paramétrico global

O documento NUREG/CR-5485 [87] traz uma abordagem conservadora e simplificada para seleção quantitativa de CCF. O procedimento de seleção de CCF é realizado adicionando um evento de falha de causa comum "global" para cada componente. Um evento de causa comum global em um grupo de componentes é aquele em que todos os membros do grupo falham. Como exemplo desta etapa do procedimento, considere um grupo

de componentes de causa comum (*Common Cause Failure Group*, CCCG) composto por três componentes A, B e C, conforme Figura 12:



Fonte: NUREG/CR-5485 [87].

A árvore de falhas é solucionada para obtenção dos cortes mínimos do sistema. Qualquer corte envolvendo as intersecções A_i B_i C_i terá o evento básico CCF_{ABC} . Em grandes sistemas ou sequências de acidente, o produto das falhas independentes A_i B_i C_i é geralmente descartada no processo de truncamento, devido ao seu pequeno valor numérico, enquanto a falha de causa comum CCF_{ABC} é preservada por ser numericamente maior.

Valores numéricos do evento básico CCF podem ser estimados utilizando-se um modelo paramétrico global:

$$P(CCF_{ABC}) = G \times P(A) \quad (3-8)$$

$P(A)$ é a probabilidade de falha total do componente. Na Tabela 3 são apresentados valores globais do fator de causa comum G para configurações de sistemas k-de-n para sucesso.

Tabela 3 – Fator de causa comum para diferentes configurações de sistemas k-de-n

Configuração k de n	Valores de G	
	Teste não simultâneo dos componentes	Teste simultâneo dos componentes
1 de 2	0,05	0,10
2 de 2		
1 de 3	0,03	0,08
2 de 3		
3 de 3	0,07	0,14
1 de 4	0,02	0,07
2 de 4	0,04	0,11

Configuração k de n	Valores de G	
	Teste não simultâneo dos componentes	Teste simultâneo dos componentes
3 de 4	0,08	0,19
4 de 4		

Fonte: NUREG/CR-5485 [87].

Modelo das múltiplas letras gregas

Vários modelos matemáticos estão disponíveis na literatura para representar a contribuição de falhas de causa comum na APS [86, 87]. A abordagem das múltiplas letras gregas (*Multiple Greek Letters*, MGL) apresenta-se como um modelo mais completo, em que os fatores de peso são anexados à probabilidade de falha básica de cada componente, conforme apropriado para as combinações de componentes em avaliação. Para um sistema de dois componentes, o fator é representado pela letra beta (β). Para sistemas de três componentes, o fator beta é combinado com um fator gamma (γ). Esses fatores dependem do número de componentes que estão sendo considerados. Portanto, o valor do fator beta para um caso de dois componentes não é o mesmo que para um caso de três componentes.

Na Tabela 4 são apresentados os fatores do CCF para um dado número de componentes, considerando a combinação de até quatro componentes.

Tabela 4 – Fatores de falha de causa comum para componentes de diferentes configurações de sistema.

Número de componentes	Falha de dois	Falha de três	Falha de quatro
2	β	NA	NA
3	$0,5\beta(1-\gamma)$	$\beta \gamma$	NA
4	$0,33\beta(1-\gamma)$	$0,33\beta \gamma (1-\delta)$	$\beta \gamma \delta$

Fonte: Adaptado NUREG/CR-5485 [87].

Para todos os casos, é aplicado um fator de ponderação $(1-\beta)$ para a estimativa da probabilidade de falha individual dos componentes. A fim de exemplificar a aplicação dos fatores de CCF em termos do MGL, considera-se o caso de um grupo de 3 componentes:

$$Q_1^{(3)} = (1 - \beta)Q_T \quad (3-9)$$

$$Q_2^{(3)} = \frac{1}{2}\beta(1 - \gamma)Q_T \quad (3-10)$$

$$Q_3^{(3)} = \gamma\beta Q_T \quad (3-11)$$

Os valores dos fatores mostrados na Tabela 4 derivam de outras variáveis apresentadas na Tabela 5.

Tabela 5 – Expressões de cálculo dos fatores de causa comum do modelo de múltiplas letras gregas

Número de Componentes	β	γ	δ
2	$2n_2/(n_1+2n_2)$	NA	NA
3	$(2n_2+3n_3)/(n_1+2n_2+3n_3)$	$3n_3/(2n_2+3n_3)$	NA
4	$(2n_2+3n_3+4n_4)/(n_1+2n_2+3n_3+4n_4)$	$(3n_3+4n_4)/(2n_2+3n_3+4n_4)$	$(4n_4)/(3n_3+4n_4)$

Fonte: Adaptado NUREG/CR-5485 [87].

Onde n_k é o número de eventos envolvendo k componentes no estado de falha.

3.1.3.4 Integração dos modelos de árvores de eventos e árvores de falhas e quantificação do risco da instalação

A integração dos modelos de árvores de eventos e árvores de falhas e sua respectiva quantificação pode ser realizada de duas maneiras distintas. A primeira opção consiste na integração de cada evento principal da árvore de eventos com a árvore de falhas correspondente. Neste método, o resultado da probabilidade de ocorrer o acidente é calculado diretamente na árvore de eventos. A segunda maneira consiste em gerar uma árvore de falhas principal (*master*) que integra todas as árvores de falhas que correspondem aos eventos principais da árvore de eventos. Neste segundo método, a árvore de eventos funciona apenas como guia para delineamento dos cenários e a probabilidade de ocorrência do acidente é calculada pela probabilidade de ocorrência do evento topo da árvore de falhas *master*.

3.1.3.5 Análise de sensibilidade

A análise de sensibilidade visa determinar a significância da escolha dos parâmetros, suposições ou outras incertezas do modelo desenvolvido para o cálculo do risco estimado de um sistema ou instalação. Os efeitos das variáveis de entrada e premissas na APS são medidos através da modificação destes dados, multiplicando-os por fatores que podem alcançar várias ordens de magnitude, e observando os resultados do risco estimado pela APS. Qualquer variável ou premissa cuja mudança conduz a uma alteração relativamente significativa na estimativa do risco pode ser considerada “sensível” para a análise. Uma análise de sensibilidade adequada fortalece a qualidade e validade dos resultados da APS. Resumidamente, as etapas envolvidas na análise de sensibilidade são [88]:

1. Identificação dos elementos da APS, incluindo premissas, taxa/probabilidade de falha e parâmetros de modelos, que possam ser sensíveis aos resultados finais do

risco;

2. Alteração dos valores de cada item sensível, em qualquer direção, por fatores que podem variar de 2 a 100. É importante destacar que, a mudança em algumas premissas pode desencadear modificações em vários outros dados de entrada dos modelos. Por exemplo, a alteração da taxa ou probabilidade de falha de um equipamento requer que todos os eventos associados a equipamentos semelhantes sejam alterados; e
3. Cálculo do impacto das alterações realizadas na etapa 2, uma de cada vez, listando os elementos mais sensíveis.

3.1.3.6 Interpretação dos resultados da Análise Probabilística de Segurança

Quando os valores de risco são calculados, eles devem ser interpretados para determinar se alguma revisão é necessária para refinar os resultados e as conclusões. Há dois elementos principais envolvidos no processo de interpretação. A primeira questão é entender se os valores finais e os detalhes dos cenários de acidente são logicamente e quantitativamente significativos. Esta etapa serve para verificar a adequação dos modelos da APS. A segunda questão é caracterizar o papel de cada elemento da planta nos resultados finais. Esta etapa destaca análises adicionais de dados e coleta de informações consideradas necessárias. A etapa de interpretação é um processo contínuo com a aquisição de informações advindas das atividades de quantificação, análise de sensibilidade e análise de importância da APS.

3.1.3.7 Classificação de importância

A classificação dos elementos do sistema em relação ao seu risco ou significância em relação à segurança é um dos resultados mais importantes de uma APS. A classificação de importância consiste em ordenar os elementos do sistema com base em sua contribuição crescente ou decrescente para os valores finais de risco da instalação. As principais medidas de importância utilizadas para classificação de risco em APS são: *Fussell-Vesely*, *Birnbaum*, *Risk Achievement Worth (RAW)* e *Risk Reduction Worth (RRW)*.

As quatro medidas de importância são calculadas a partir da quantificação dos resultados. Os termos utilizados nos cálculos são [89]:

P(topo) Probabilidade de ocorrência do evento topo.

$P(A)$	Probabilidade do evento A (evento de interesse).
$P(\text{topo}/A=1)$	Probabilidade do evento topo ocorrer dado que o evento A sempre ocorre (probabilidade de $A=1$).
$P(\text{topo}/A=0)$	Probabilidade do evento topo ocorrer dado que o evento A nunca ocorre (probabilidade de $A=0$).
$P(C_i)$	Probabilidade do corte mínimo i (o qual contém o evento A).

A medida de importância *Fussel-Vesely* fornece o risco associado a um determinado componente, ou seja, uma medida de quanto o componente contribui para a falha do sistema. A medida de importância *Fussel-Vesely* é expressa como:

$$FV = \frac{P(\text{topo}) - P(\text{topo}/A = 0)}{P(\text{topo})} \quad (3-12)$$

Alternativamente, a medida de importância *Fussel-Vesely* pode ser aproximada em termos da probabilidade de ocorrência do evento A. Esse método de cálculo é utilizado quando os cortes mínimos não contêm negação, sendo expressa por:

$$FV = \sum_{A \text{ em } c_i} \frac{P(c_i)}{P(\text{topo})} \quad (3-13)$$

A medida de importância *Birnbaum* fornece o aumento do risco associado à falha do componente, sendo definida como:

$$\text{Birnbaum} = P(\text{topo}/A = 1) - P(\text{topo}/A = 0) \quad (3-14)$$

A medida de importância *Risk Reduction Worth* é uma medida que fornece o valor da redução do risco quando a indisponibilidade do componente A é reduzida a zero, definida como:

$$\text{Risk Reduction Worth} = \frac{P(\text{topo})}{P(\text{topo}/A = 0)} \quad (3-15)$$

A medida de importância *Risk Achievement Worth* fornece o fator de aumento do risco devido a não disponibilidade do componente A, sendo expressa por:

$$\text{Risk Achievement Worth} = \frac{P(\text{topo}/A = 1)}{P(\text{topo})} \quad (3-16)$$

3.2 Métodos de análise implementados no código computacional CAFTA

3.2.1 Visão Geral do código computacional CAFTA

O CAFTA [82] é um código computacional utilizado para desenvolver modelos de confiabilidade de sistemas complexos, usando a metodologia de árvores de falhas e árvores de eventos. As etapas da modelagem dos sistemas são sintetizadas em:

- Construir um modelo lógico dos sistemas da instalação utilizando árvores de falhas e árvores de eventos;
- Construir o banco de dados de confiabilidade que será considerado na quantificação dos modelos;
- Avaliar as árvores de falhas para obter os cortes mínimos; e
- Revisar e analisar os resultados representados nos cortes mínimos.

A etapa de construção das árvores de falhas ocorre frequentemente em paralelo com a construção do banco de dados de confiabilidade. O banco de dados é requerido para cada evento básico modelado nas árvores de falhas. O evento básico representa a probabilidade de falha ou indisponibilidade de um item do sistema, erros de operação, ações de manutenção ou um evento iniciador ao qual o sistema deve responder. Esta probabilidade de falha é muitas vezes dependente da taxa de falha do evento modelado e do tempo de missão. Por exemplo, a probabilidade de falha de um componente para um determinado tempo de missão pode ser dada com base na distribuição exponencial sendo definida como:

$$P(\text{falha}) = 1 - e^{-\lambda t} \quad (3-17)$$

Onde:

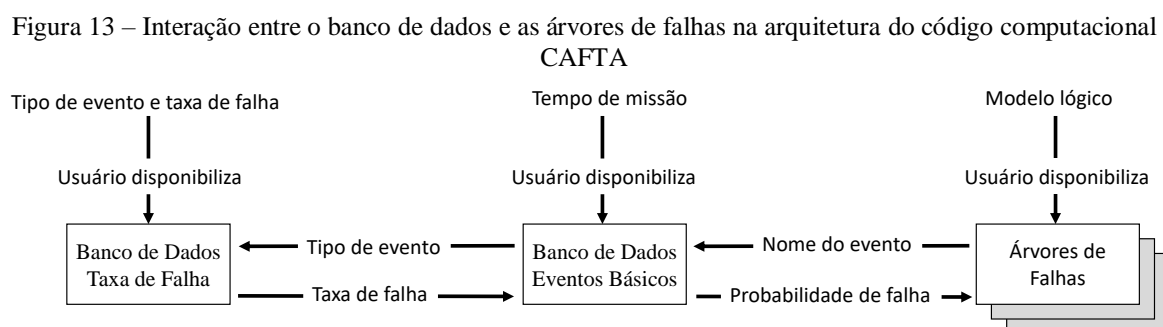
$P(\text{falha})$ = probabilidade de falha do evento básico;

λ = taxa de falha; e

t = tempo operacional requerido (tempo de missão).

Embora a taxa de falha, λ , frequentemente seja a mesma para tipos de eventos similares (ex: falha na operação de motores), a probabilidade de falha pode variar de sistema para sistema devido ao tempo de missão de cada um. Em geral, a taxa de falha é uma função do tipo de evento modelado, enquanto o tempo de missão é uma função de como o componente atua na operação do sistema.

O CAFTA [82] provê um banco de dados de confiabilidade centralizado, subdividido em: (1) Banco de dados de taxa de falha – contém a taxa de falha ou probabilidade de falha sob demanda de cada tipo de evento; e (2) Banco de dados de eventos básicos – contém o nome dos eventos básicos e os parâmetros que dependem do sistema para o cálculo da probabilidade de falha (ex.: tempo de missão). A Figura 13 sintetiza a interação entre o banco de dados de confiabilidade e a árvore de falhas.



Fonte: Manual do CAFTA [89].

Se o tipo de evento não for indicado na modelagem, a taxa de falha deve ser vinculada individualmente a cada evento básico, e isto é feito diretamente na tabela de eventos básicos.

A árvore de falhas pode ser reduzida na forma de cortes mínimos usando o gerador de cortes mínimos (*Cutset Generator*) do programa. Os cortes mínimos fornecem sinais de funcionalidade do sistema, assim como permitem a quantificação da probabilidade do evento topo. Para limitar a quantidade de dados processados, o programa permite truncar os cortes mínimos, negligenciando os que têm probabilidade de ocorrência menor do que o valor de truncamento selecionado.

Após gerados, os cortes mínimos podem ser revisados no editor de cortes mínimos (*Cutset Editor*), sendo possível excluir, incluir ou alterar o valor dos eventos de um corte mínimo, ou até mesmo remover um corte inteiro. Todas essas ferramentas são úteis para realização de estudos de sensibilidade sem ser necessário alterar os modelos lógicos das árvores de falhas. Outra utilização destas ferramentas é quando se tem, por exemplo, eventos excludentes no modelo, como manutenções simultâneas em equipamentos redundantes. Nestes casos, o editor pode ser usado para remover este corte dos resultados, já que a implementação de uma lógica de negação no modelo pode se tornar complexa.

Outra funcionalidade do editor de cortes mínimos é fornecer a medida de importância para os eventos, como a de *Fussel-Vesely*, ordenando os eventos que tiverem maior contribuição para a probabilidade de ocorrência do evento topo.

3.2.2 Definição dos atributos associados aos eventos básicos dos modelos de falha dos sistemas

Ao se criar um evento básico alguns dados devem ser fornecidos. Primeiramente, deve ser definido o método de cálculo para a probabilidade de ocorrência daquele evento. A Tabela 6 sintetiza os métodos padrões de cálculo disponíveis no CAFTA [82].

Tabela 6 – Métodos de cálculo da probabilidade de eventos básicos implementados no código computacional CAFTA.

Método	Fórmula	Descrição	Legenda
0	Prob	Probabilidade direta.	-
1	$\lambda\tau$	Probabilidade de falha durante a missão (aprox. método #3); ou indisponibilidade assintótica, dado reparo (aprox. método #4).	aprox. método #3 λ = taxa de falha em operação τ = tempo de missão (sem reparo) aprox. método #4 λ = taxa de falha em operação τ = tempo médio de reparo
2	$\lambda\tau/2$	Indisponibilidade média entre testes (aprox. método #5).	λ = taxa de falha em <i>standby</i> τ = tempo entre testes
3	$1 - e^{-\lambda\tau}$	Probabilidade de falha durante a missão.	λ = taxa de falha em operação τ = tempo de missão (sem reparo)
4	$\frac{\lambda\tau}{\lambda\tau + 1}$	Indisponibilidade assintótica, dado reparo.	λ = taxa de falha em operação τ = tempo médio de reparo
5	$1 + \frac{1}{\lambda\tau}(e^{-\lambda\tau} - 1)$	Indisponibilidade média entre testes.	λ = taxa de falha em <i>standby</i> τ = tempo entre testes
6	$\frac{\lambda\tau}{\lambda\tau + 1}(1 - e^{-(\lambda + \frac{1}{\tau})T})$	Probabilidade de falha durante a missão com um reparo.	λ = taxa de falha em operação τ = tempo médio do reparo T = tempo de missão

Fonte: Manual do CAFTA [89].

O programa possibilita também que o usuário adicione uma equação para o cálculo da probabilidade diferente das que são fornecidas como padrões.

Escolhido o método de cálculo, o usuário define os valores das variáveis correspondentes à equação (fórmula) daquele método. O evento básico pode também ser associado a um grupo de CCF com uma taxa de falha associada.

Por fim, outro importante dado a ser implementado é a distribuição de incerteza da taxa de falha dos componentes e equipamentos. Os parâmetros a serem definidos dependem dos tipos de distribuição, definidos conforme Tabela 7.

Tabela 7 – Tipos de distribuição de incerteza da taxa de falha considerados no código computacional CAFTA.

Distribuição	Parâmetros de distribuição de incerteza
Beta	Variância
Gama	Variância
Lognormal	90% de intervalo de confiança
Normal	90% de intervalo de confiança
Uniforme	-

Fonte: Manual do CAFTA [89].

Na Figura 14 está ilustrado um exemplo da janela de edição dos dados de um evento básico no código computacional CAFTA [82]. Esta janela de edição é aberta no ambiente da árvore de falhas, no entanto, os dados também podem ser editados diretamente nas tabelas do banco de dados.

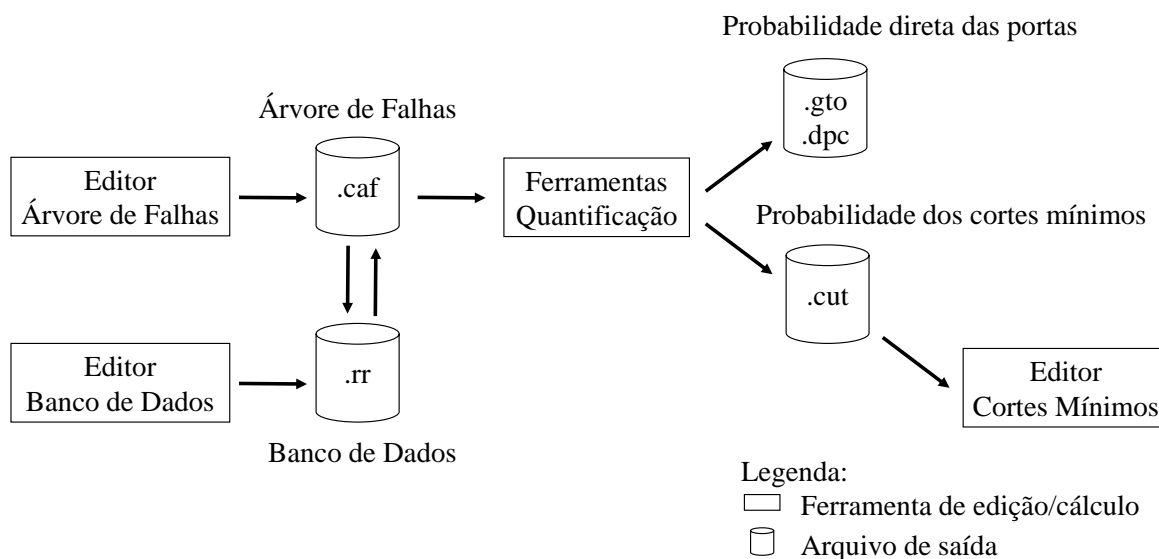
Figura 14 – Janela de edição dos dados de um evento básico apresentada no código computacional CAFTA.

Fonte: Código computacional CAFTA [82].

3.2.3 Quantificação dos modelos de árvore de falhas

Uma vez modelada a árvore de falhas, esta pode ser avaliada de duas maneiras. Pode ser calculada a probabilidade direta de ocorrência para todas as portas da árvore de falhas ou podem ser gerados cortes mínimos para o evento topo escolhido. A Figura 15 ilustra a relação das ferramentas do CAFTA [82] utilizadas no processo de quantificação das probabilidades de falha de um sistema.

Figura 15 – Processo de edição usado no CAFTA para quantificação da probabilidade do evento topo da árvore de falhas.



Fonte: Autor.

Probabilidade direta das portas

O arquivo de saída do método de cálculo direto da probabilidade de ocorrência das portas pode ser gerado utilizando-se duas ferramentas do CAFTA [82]. A primeira, chamada GTPROB, gera um arquivo de saída (.gto) que contém o valor mínimo, uma estimativa pontual e o valor máximo para a probabilidade de cada porta da árvore de falhas. A estimativa pontual é a média geométrica dos valores mínimos e máximos. As estimativas pontuais das probabilidades são automaticamente registradas nas portas da árvore de falhas. A segunda ferramenta, *Direct Gate Probability Calculations* (arquivo de saída .dpc) é utilizada para calcular a probabilidade exata do evento topo das portas. Diferentemente do método de cálculo por cortes mínimos, o método de cálculo direto evita a aproximação por eventos raros e aquela associada às lógicas de negação.

Edição do conjunto de cortes mínimos

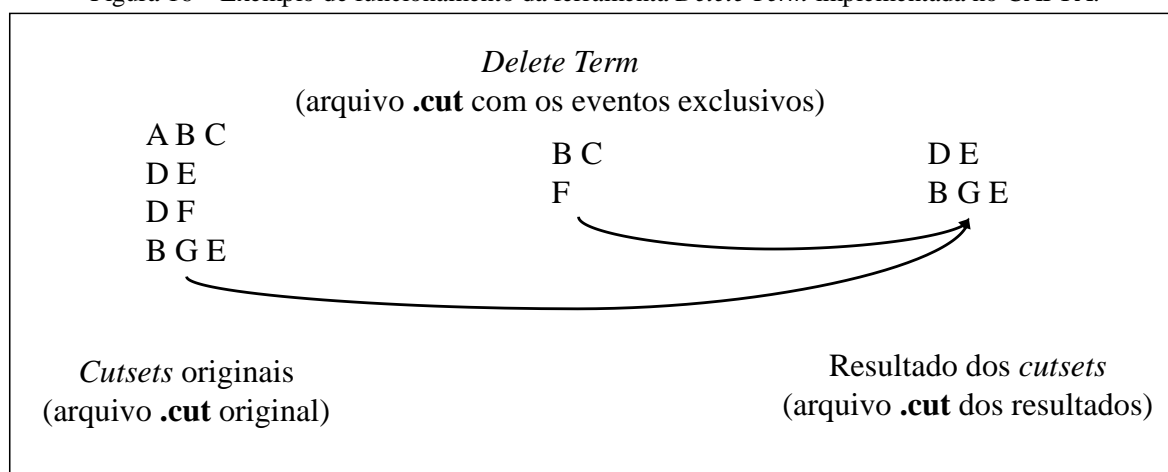
Cada corte mínimo mostrado no arquivo de saída .cut contém a probabilidade de ocorrência e os eventos básicos daquele corte. A probabilidade do corte mínimo é o produto das probabilidades de seus eventos básicos. A probabilidade de ocorrência do evento topo é a soma das probabilidades dos cortes mínimos.

Uma técnica para organizar e facilitar as análises decorrentes do arquivo de saída dos cortes mínimos é atribuir um marcador (evento *flag*), com probabilidade igual a 1.0, em paralelo com um ou mais eventos “porta” resultante da combinação de eventos básicos.

Desta forma, o evento *flag* aparecerá no corte como um evento de estado falho do(s) evento(s) porta, sem contribuir para a probabilidade de ocorrência do corte, possibilitando assim, o cálculo de medidas de importância para eventos que são resultantes de eventos básicos. Cita-se, como exemplo, a utilização de um evento *flag* para o *Station Blackout* que é resultante da falha concomitante do fornecimento de energia pela rede elétrica externa e pelos geradores de emergência.

O *Cutset editor* apresenta muitas ferramentas que auxiliam nas análises, com destaque para a utilidade da ferramenta *Delete Term*. Esta ferramenta realiza a exclusão de cortes mínimos, sendo muitas vezes utilizada para remover os cortes mínimos com eventos mutuamente exclusivos. A remoção de cortes mínimos de um arquivo original é realizada através do carregamento de outro arquivo que possua os cortes mínimos que precisam ser excluídos. A Figura 16 ilustra um exemplo do funcionamento da ferramenta *Delete Term*.

Figura 16 – Exemplo de funcionamento da ferramenta *Delete Term* implementada no CAFTA.



Fonte: Manual do CAFTA [89].

3.3 Seleção dos dados de confiabilidade aplicáveis à avaliação probabilística de sistemas elétricos

O banco de dados de confiabilidade dos componentes, equipamentos e sistemas escolhido como adequado a este trabalho e implementado no CAFTA [82] possui como principal fonte uma base genérica de dados proveniente dos resultados da experiência operacional dos reatores americanos (<https://nrcoe.inl.gov/> [17]).

Na Tabela 39 do anexo A são apresentados os dados de falha dos equipamentos selecionados para as modelagens. Nesta tabela constam informações dos equipamentos, modos de falha, média da taxa de falha e variância da média da taxa de falha.

As taxas de falha do sistema elétrico externo são apresentadas de modo separado

(<https://nrcoe.inl.gov/> [17]) para cada categoria de evento de perda: centrados na planta, centrados na subestação primária/entrada, relacionados à rede e relacionados ao clima. A apresentação dos dados está subdividida, ainda, em operação com o reator crítico e em modo de desligamento. Neste trabalho, adotou-se uma taxa de falha para cada categoria independente do modo de operação do reator, ou seja, a taxa de falha é independente do modo de operação do reator e conseqüentemente da estação climática do ano ao qual esta possa estar vinculada, já que determinados períodos do ano apresentam taxas de falha do sistema elétrico externo maiores. Os valores das taxas de falha do sistema elétrico externo são apresentados na Tabela 40 do anexo A.

Em relação às falhas de causa comum, propõe-se adotar o modelo das múltiplas letras gregas para a estimativa dos parâmetros. Na Tabela 41 do anexo A estão apresentadas as estimativas destes parâmetros dos equipamentos selecionados para as modelagens. Para os casos em que não há dados publicados, foram definidos valores baseados na Tabela 3.

Além disso, considerando um determinado componente, a combinação dos dados da taxa de falha de diferentes fontes ou até mesmo modos de operação, tal como utilizado para o sistema elétrico externo, é realizada através das seguintes expressões [63]:

$$\bar{\alpha} = \frac{1}{N} \sum_{k=1}^N \alpha_k \quad (3-18)$$

$$\bar{\beta} = \frac{1}{N} \sum_{k=1}^N \beta_k \quad (3-19)$$

$$\mu_{\gamma}(\lambda) = \frac{\bar{\alpha}}{\bar{\beta}} \quad (3-20)$$

$$\sigma_{\gamma}^2(\lambda) = \frac{\bar{\alpha}}{\bar{\beta}^2} \quad (3-21)$$

$$\mu_{\beta}(\lambda) = \frac{\bar{\alpha}}{\bar{\alpha} + \bar{\beta}} \quad (3-22)$$

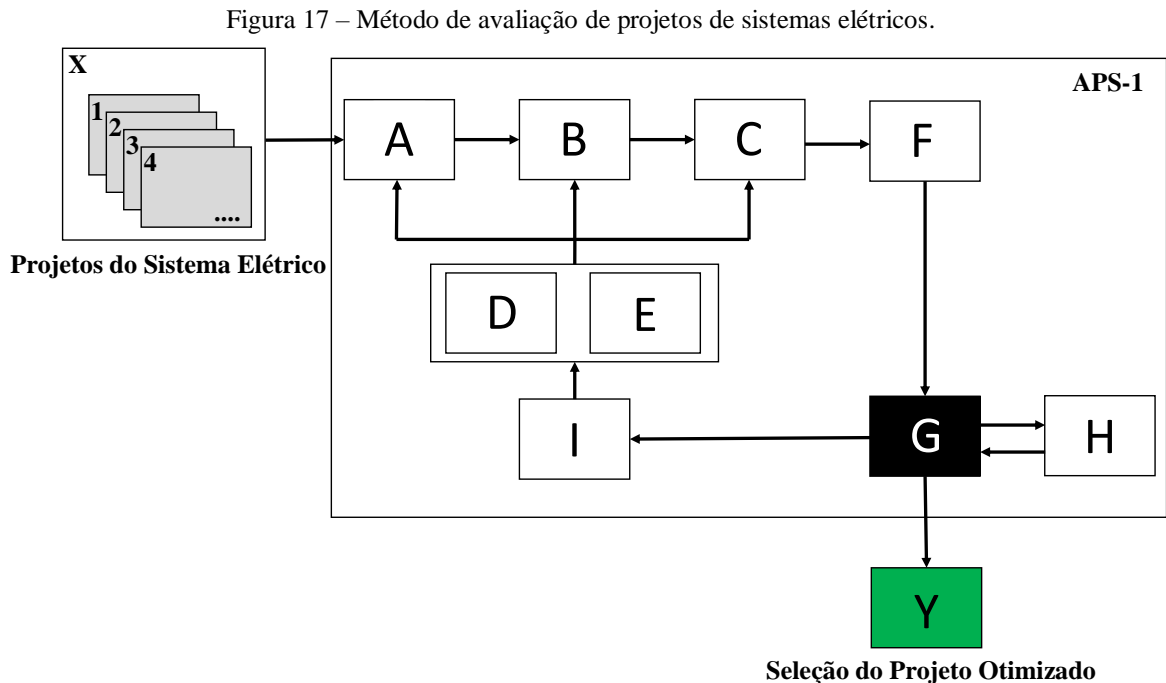
$$\sigma_{\beta}^2(\lambda) = \frac{\bar{\alpha}\bar{\beta}}{(\bar{\alpha} + \bar{\beta})^2(\bar{\alpha} + \bar{\beta} + 1)} \quad (3-23)$$

Deste modo, são primeiramente calculadas as médias aritméticas dos parâmetros alfa e beta das taxas de falha do componente obtidas em fontes de dados diversas, utilizando-se respectivamente as expressões 3-18 e 3-19. Em posse destes dados, são calculadas a média e a variância da taxa de falha do componente através das expressões 3-20 e 3-21 para a distribuição de incerteza gama e 3-22 e 3-23 para a distribuição de incerteza beta.

3.4 Método de avaliação probabilística de projetos de sistemas elétricos

A metodologia de APS nível 1, resumidamente, é focada nos eventos iniciadores que podem causar um acidente de dano ao núcleo ou ao combustível nuclear localizado fora do núcleo, no delineamento das sequências de eventos e na avaliação da probabilidade de ocorrência desse tipo de acidente. Os resultados da APS nível 1 fornecem informações sobre os riscos associados à operação de uma instalação nuclear, constituindo informações imprescindíveis para se efetuar melhorias em relação à segurança nas atividades de projeto, licenciamento e operação dessa instalação. A metodologia para avaliação do projeto do sistema elétrico baseado em informação do risco utiliza os resultados da APS nível 1 para seleção da melhor arquitetura do sistema. Entretanto, para que o projeto com menor risco associado seja o mais adequado àquela instalação, deve-se levar em consideração, também, as especificidades funcionais e operacionais de cada tipo de instalação.

O programa computacional CAFTA [82] pode ser adotado para modelagem e análise dos sistemas da instalação em estudo, tomando como base a medida de risco calculada pela frequência de dano ao núcleo, CDF. A metodologia proposta segue os passos ilustrados na Figura 17.



Fonte: Autor.

Onde:

[X] Alternativas de projeto do sistema elétrico

Propostas de alteração na arquitetura do sistema elétrico, gerando diferentes modelos para a instalação a ser avaliada.

[A] Identificação dos eventos iniciadores

Identificação de eventos internos (falha de sistemas, erros em procedimentos, etc.) ou externos que possam evoluir para um acidente de dano ao núcleo que possam ser considerados eventos iniciadores.

[B] Delineamento das sequências de acidentes (árvore de eventos)

As árvores de eventos são usadas neste estudo para delinear os possíveis caminhos que geram os cenários acidentais.

[C] Análise dos sistemas – modelo lógico (árvore de falhas)

Cada sistema identificado na árvore de eventos que seja requerido para manter as funções de segurança da instalação é analisado em mais detalhes através da árvore de falhas.

[D] Banco de dados de confiabilidade

Levantamento das taxas ou probabilidades de falha dos equipamentos e falhas de causa comum.

[E] Análise de confiabilidade humana

Análise da interação do projetista, operador e técnico em manutenção com os sistemas da instalação. Existem pelo menos dois tipos de erros humanos: ações que ocorrem durante testes e atividades que ocasionam descalibração; e ações que o operador realiza após ocorrer o evento iniciador.

[F] Integração do modelo e quantificação

A integração dos modelos é realizada através de uma árvore de falhas *master* e o cálculo da resposta do sistema aos cenários acidentais é efetuado com base na probabilidade de ocorrência dos eventos.

[G] Interpretação dos resultados

Consiste em um processo contínuo e iterativo com a aquisição de informações das atividades de quantificação e das análises de sensibilidade, incerteza e importância da APS.

[H] Classificação de importância

Para a classificação de importância do risco propõe-se utilizar a medida de *Fussel-Vesely* dos eventos iniciadores, sistemas, modos de falha comum e procedimentos de manutenção e testes.

[I] Análise de sensibilidade

A análise de sensibilidade consiste em recalcular os resultados do modelo para um intervalo de valores numéricos da taxa de falha dos equipamentos ou de premissas adotadas. A análise de sensibilidade pode subsidiar o certame a respeito da classificação de segurança de equipamentos do sistema, haja vista que, equipamentos de classe de segurança nuclear são submetidos a testes e protocolos rígidos de fabricação que aumentam sua confiabilidade quando comparados a outros equipamentos de aplicação apenas industrial.

[Y] Seleção do projeto

Com base nos resultados da APS nível 1 para os diferentes projetos do sistema elétrico é realizada a seleção do projeto do sistema elétrico mais adequado no que diz respeito à segurança para o tipo de instalação avaliada. Assim, foi definida a variável ΔCDF , que significa o percentual de variação relativa do CDF após a atualização do projeto em relação à versão original. O risco associado ao projeto pode ser considerado menor em relação ao projeto original se ΔCDF for negativo, enquanto o risco é maior se ΔCDF for positivo. A equação de ΔCDF é definida por:

$$\Delta CDF = \frac{CDF_{atualizado} - CDF_{original}}{CDF_{original}} \times 100\% \quad (3-24)$$

Ressalta-se que ΔCDF é apenas uma variável de suporte na escolha do projeto, pois não considera aspectos econômicos, a funcionalidade da instalação e a confiabilidade mínima do sistema demandado pelo projeto.

3.5 Procedimento para aplicação do método de avaliação probabilística considerando um modelo hipotético de um sistema elétrico CA simplificado

O modelo de um sistema elétrico CA simplificado, avaliado sob a ótica da metodologia deste trabalho, foi extraído de um sistema elétrico padrão previsto para plantas nucleares de potência e que atende aos requisitos normativos mínimos. A avaliação do modelo simplificado visa enfatizar a importância das fontes de energia elétrica para a instalação e ainda expor em detalhes as etapas da metodologia, levando em conta que modelos mais complexos possuem uma quantidade muito grande de dados que tornaria o detalhamento muito extenso.

Algumas simplificações foram realizadas para a avaliação de um sistema elétrico CA, destacando alguns componentes/sistemas que não foram incluídos no modelo:

- Sistema elétrico CC e sistema CA ininterrupto (fornecem energia para

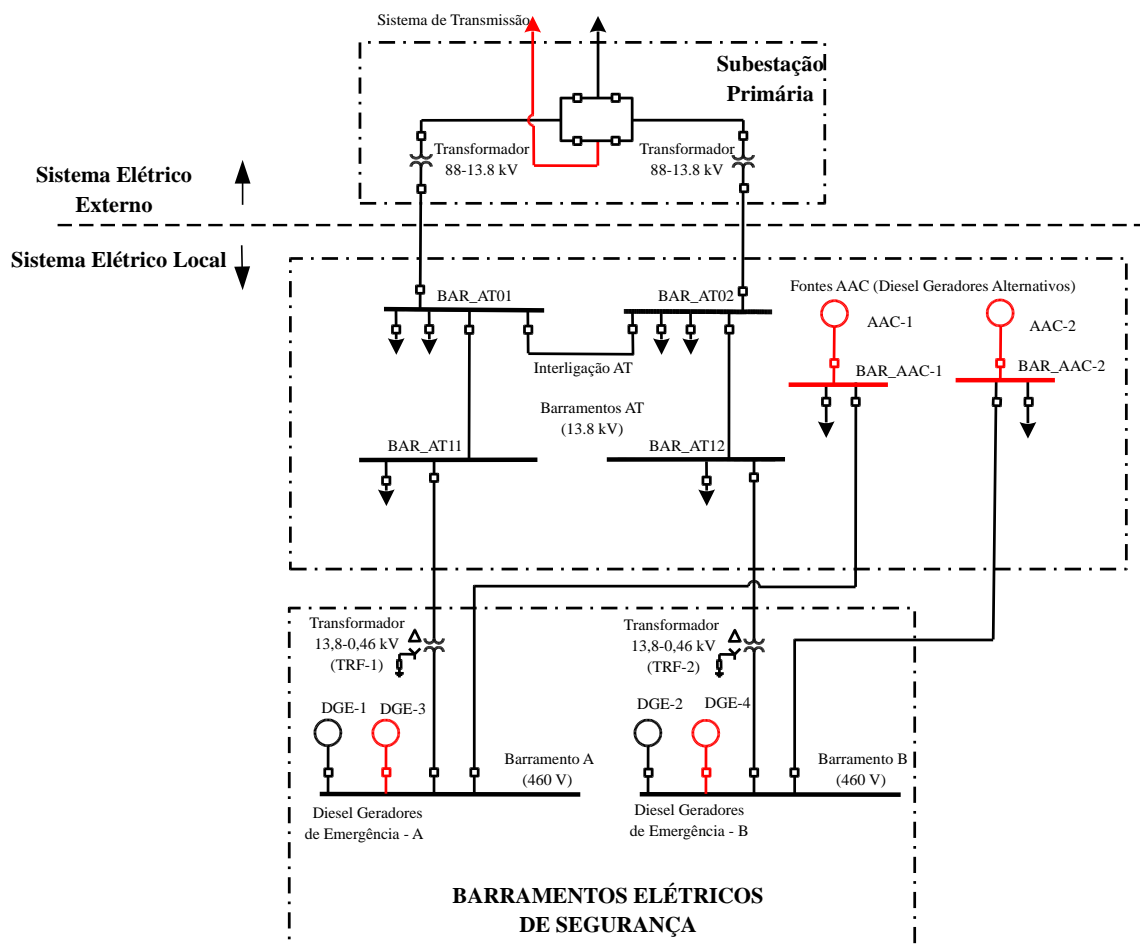
comando e controle de componentes do sistema elétrico CA);

- Sinais de comando, inclusive de partida dos DGEs;
- Relés de subtensão;
- Cabos e conexões;
- Disjuntores (falha de abertura/fechamento e atuação por sinais espúrios); e
- Componentes de interface que possam induzir a falha do sistema elétrico CA.

3.5.1 Alternativas de projeto do sistema elétrico CA simplificado

A Figura 18 ilustra o diagrama unifilar de um sistema elétrico CA simplificado. As marcações em vermelho representam as modificações de projeto que poderão ser avaliadas aplicando-se a metodologia proposta na seção 3.4. O sistema elétrico CA é subdividido em sistema elétrico externo (sistema de transmissão e subestação primária de entrada) e o sistema elétrico local da instalação. As modificações previstas conduziram a quatro projetos diferentes do sistema elétrico CA, conforme a Tabela 8.

Figura 18 – Diagrama ilustrativo do sistema elétrico CA simplificado.



Fonte: Autor.

Tabela 8 – Alternativas de projetos do sistema elétrico CA simplificado.

Projeto	Linhas de transmissão (LTs)	DGEs por barramento de segurança	Fonte AAC por barramento de segurança
A (original)	2	1	1
B	2	1	0
C	1	2	0
D	1	2	1

Fonte: Autor.

3.5.2 Evento iniciador e delineamento das sequências do acidente

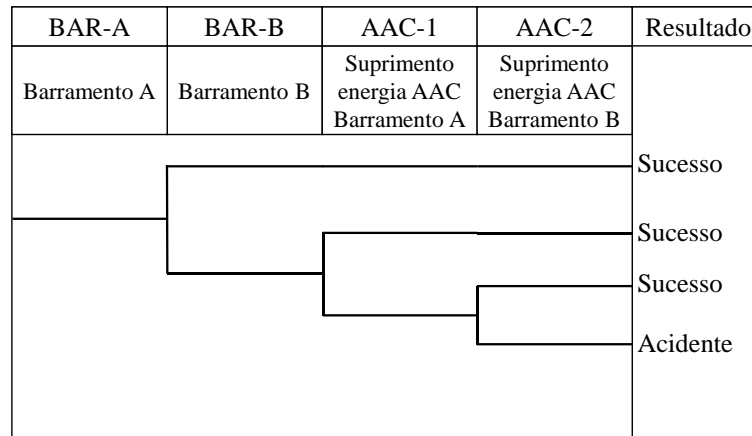
Para o modelo analisado considera-se como acidente a falha completa dos barramentos de segurança, barramentos A e B. A falha dos barramentos pode ser decorrente da falha intrínseca dos barramentos (curto-circuito) ou devido à falha no fornecimento de energia. Ressalta-se que os conceitos de um evento de *Station Blackout* e de fontes AAC utilizados neste modelo são os mesmos daqueles aplicados em instalações nucleares.

Adotou-se como evento iniciador a falha do barramento de segurança A, seja por falha no fornecimento de energia normal/emergência (sistema elétrico externo/DGEs) ou falha do próprio barramento por curto-circuito. A fonte AAC é uma fonte de energia utilizada alternativamente para alimentar os barramentos de segurança durante um evento de *Station Blackout*, ou seja, ela é uma fonte mitigadora aplicada apenas quando há uma falha completa dos dois barramentos de segurança redundantes (A e B).

O barramento de segurança A (Trem A) é a fonte de alimentação das cargas elétricas principais. Enquanto o barramento de segurança B (Trem B) supre as cargas redundantes, justificando o evento iniciador ser a falha do barramento A.

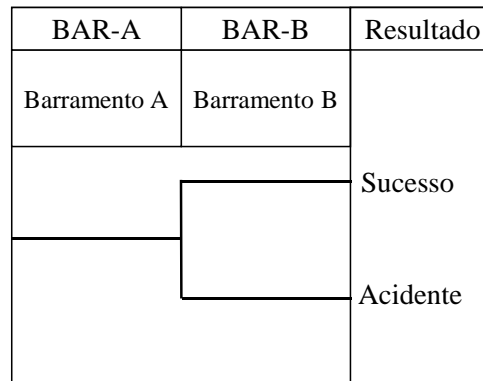
O evento iniciador e os eventos subsequentes identificados nas árvores de eventos da Figura 19 (projetos A e D) e Figura 20 (projetos B e C) são compostos por mais de um evento básico para que se possa adotar a mesma sequência de eventos para os projetos a serem avaliados. Entretanto, a frequência de ocorrência dos eventos principais das árvores de eventos irá mudar conforme a configuração de cada projeto.

Figura 19 – Árvore de eventos para o evento iniciador de perda do barramento de segurança A – alternativas de projeto A e D.



Fonte: Autor.

Figura 20 – Árvore de eventos para o evento iniciador de perda do barramento de segurança A – alternativas de projeto B e C.



Fonte: Autor.

3.5.3 Análise do sistema – modelo lógico

Os cabeçalhos da árvore de eventos, identificados por BAR-A (evento iniciador) e BAR-B, AAC-1 e AAC-2 (eventos subsequentes) possuem um modelo lógico (árvore de falhas) que os representam. Uma árvore de falhas *master* é utilizada para integrar estas árvores de falhas modeladas para os cabeçalhos da árvore de eventos. Nas Figura 44 até Figura 48 do anexo C são apresentadas as árvores de falhas do projeto A (original) que foram modeladas no CAFTA [82].

Um evento marcador (%BAR_A) de probabilidade igual a 1 foi utilizado para identificar o evento iniciador, já que este é um evento macro composto por mais de um evento básico, conforme Figura 48. No entanto, para se obter a probabilidade de ocorrência do evento iniciador é necessário que se realize a quantificação dos cortes mínimos que contém o evento marcador %BAR_A. Adicionalmente, a falha no suprimento normal

juntamente com a falha no suprimento de emergência dos barramentos de segurança A e B são identificadas pelos eventos marcadores %SBO_A e %SBO_B, respectivamente, com probabilidade igual a 1 (ver Figura 44 e Figura 45). Assim, o evento *Station Blackout* é contabilizado pela soma das probabilidades dos cortes mínimos que contêm simultaneamente os eventos %SBO_A e %SBO_B.

Foi assumido que os diesel geradores de emergência (DGEs) e os diesel geradores alternativos (fontes AAC) pertencem a grupos distintos de falha de causa comum e a falha de causa comum entre os dois grupos não foi modelada. Entende-se, também, que a falha em um barramento de segurança devido a um curto-circuito resulta na abertura do disjuntor de proteção do barramento, o que não inviabiliza o alinhamento da fonte AAC ao barramento, após solucionado o problema pelo operador.

3.5.4 Banco de dados de confiabilidade e análise de confiabilidade humana

O banco de dados que supriu as informações para o modelo foi extraído da Tabela 39, Tabela 40 e Tabela 41 do anexo A para taxas de falha de equipamentos, eventos de falha do sistema elétrico externo e falhas de causa comum, respectivamente. Informações adicionais, tais como tempo de missão e indisponibilidade para manutenções/testes, foram incorporadas na modelagem. Desta forma, as seguintes premissas foram adotadas:

- O tempo de missão para os eventos do sistema elétrico externo é de 1 ano;
- O tempo de missão para os componentes do sistema elétrico local é de 24 horas. Assumindo-se que todos os componentes são reparáveis dentro de 24 horas e apenas um barramento de segurança é requerido para que a missão seja bem sucedida, se o trem A (principal) falha, é esperado que ele seja reparado dentro de 24 horas, e o trem B (redundante) é requerido por apenas 24 horas para se ter sucesso na missão. Se o trem redundante falha após 24 horas de operação, então o trem principal estará disponível e poderá ser usado para completar a missão, assumindo-se apenas uma falha por trem de segurança;
- Considera-se que a indisponibilidade mensal devido a testes periódicos dos diesel geradores de emergência (DGEs) e dos diesel geradores alternativos (fonte AAC) é de 7,25 horas (1,00E-2/ano). É assumido que apenas um diesel gerador seja testado por vez, ou seja, os eventos de manutenção/teste dos diesel geradores são mutuamente exclusivos entre si; e
- Na condição de *Station Blackout* é creditado ao operador alinhar a fonte AAC para

suprir energia aos barramentos de segurança. É atribuído um valor de $5,00E-2$ como erro humano nessa tarefa.

A fim de ilustrar o método de edição do banco de dados do modelo, utilizou-se como exemplo o evento básico LOOP2 (eventos centrados na subestação primária) na Figura 21, onde são apresentadas as janelas de edição do banco de dados: evento básico e da taxa de falha associada.

Figura 21 – Janelas de edição do banco de dados do evento básico LOOP2 no programa computacional CAFTA.

The image displays two overlapping windows from the CAFTA software. The top window, titled "Edit Basic Event - LOOP2", has tabs for "Basic Event Data", "User Data", and "Links". It contains the following fields: "Name" (LOOP2), "Display Type" (Basic Event), "Description" (Eventos centrados na subestação primária), "Calc Method" (3 - Mission time, no repair (1-exp(-t))), "Failure Rate" (LOOP2, 1.64E-2 per Year -- Gamma, Variance: 1.45E-5), "Mission Time" (1, Years), and "Calculated probability" (1.6266E-02). The bottom window, titled "Edit Rate Data", has tabs for "Type Code", "Bayes Data", "User Data", and "Links". It contains: "Type Code" (LOOP2), "Description" (LOOP - SWITCHYARD), "Rate" (1.64E-2 per Year), "Dist" (Gamma), "Variance" (1.45E-5), "Equation", and "Notes" fields. Both windows have "OK", "Cancel", and "Help" buttons at the bottom.

Fonte: Código computacional CAFTA [82].

3.5.5 Integração do modelo e quantificação

Conforme mencionado anteriormente, a integração do modelo foi realizada através da árvore de falhas *master*, mostrada na Figura 48 do anexo C. A quantificação do modelo foi realizada através do método de cortes mínimos. Para limitar a quantidade de dados gerados, uma frequência de truncamento de $1E-11$ /ano foi selecionada, onde apenas os cortes mínimos com frequência de ocorrência igual ou superior a este valor são calculados e considerados no resultado.

Os eventos mutuamente exclusivos foram removidos da quantificação dos resultados utilizando-se a ferramenta *Delete Term* do *Cutset Editor*. A árvore de falhas, representada

pela Figura 49 do anexo C, foi modelada para gerar o arquivo com os cortes mínimos com eventos mutuamente exclusivos.

3.5.6 Interpretação dos resultados

Conforme apresentado na Tabela 9, a configuração original do sistema elétrico CA (projeto A) apresentou como medida de risco um CDF de 1,65E-6/ano. Ainda em comparação ao projeto A, foi observado um aumento na medida de risco para os projetos B e C de aproximadamente 8081% e 223,75%, respectivamente. Enquanto, o projeto D apresentou uma diminuição do risco em aproximadamente 96,75%.

Tabela 9 – Resultado do risco para os projetos do sistema elétrico CA.

Projeto	CDF _{TOTAL} (/ano)	Δ CDF _{TOTAL} (%)
A (original)	1,65E-6	-
B	1,35E-4	+8081
C	5,33E-6	+223,75
D	5,35E-8	-96,75

Fonte: Autor.

Os resultados mostram que a ausência das fontes AAC nos projetos B e C acarreta um aumento significativo para a medida de risco do projeto do sistema elétrico CA. Por outro lado, fica também evidenciado que a adição de DGEs no projeto D, em substituição a uma segunda LT, aumenta a confiabilidade do sistema e conseqüentemente diminui consideravelmente o risco de acidente associado ao projeto.

3.5.7 Classificação de importância

Primeiramente foi realizada uma classificação de importância com base na medida de *Fussel Vesely* (F-V) dos cinco eventos básicos que mais contribuíram para o risco de cada um dos quatro projetos analisados. Para os projetos A (Tabela 10) e B (Tabela 11) destacam-se os eventos de falha do sistema elétrico externo centrado na planta (LOOP2) e falhas independentes dos DGEs na partida e após a 1ª hora. No projeto A, destaca-se, ainda, a contribuição elevada de erro humano ao transferir a alimentação dos barramentos de segurança para as fontes AAC. A contribuição da falha das LTs (LOOP3) para o risco da instalação teve baixa relevância tanto no projeto A quanto no B, apresentando F-V de 0,03724 e 0,03809, respectivamente.

Tabela 10 – Eventos básicos do projeto A com maiores contribuições para o risco.

Eventos básicos	Descrição	F-V
LOOP2	Eventos centrados na subestação primária	0,50749
OPERACPN1E001FC	Operador falha para alinhar a fonte AAC-1 ao barramento A / fonte AAC-2 ao barramento B	0,43008
OPERACPN1E002FC		
ACGDG001___DGA	DGE-1 falha após 1ª hora	0,35103
ACGDG002___DGA	DGE-2 falha após 1ª hora	
ACGDG001___DGS	DGE-1 falha na partida	0,30905
ACGDG002___DGS	DGE-2 falha na partida	
LOOP4	Eventos relacionados ao clima	0,23554

Fonte: Código computacional CAFTA [82].

Tabela 11 – Eventos básicos do projeto B com maiores contribuições para o risco

Eventos básicos	Descrição	F-V
LOOP2	Eventos centrados na subestação primária	0,50701
ACGDG001___DGA	DGE-1 falha após 1ª hora	0,35081
ACGDG002___DGA	DGE-2 falha após 1ª hora	
ACGDG001___DGS	DGE-1 falha na partida	0,30888
ACGDG002___DGS	DGE-2 falha na partida	
LOOP4	Eventos relacionados ao clima	0,23537
LOOP1	Eventos centrados na planta	0,21957

Fonte: Código computacional CAFTA [82].

Os eventos básicos que tiveram destaque nos projetos C (Tabela 12) e D (Tabela 13) foram os de falha de causa comum de todos DGEs após a 1ª hora e a falha da LT. O erro humano ao alimentar os sistemas de segurança pelas fontes AAC, também ganhou destaque no projeto D em que estas fontes estão presentes.

Tabela 12 – Eventos básicos do projeto C com maiores contribuições para o risco.

Eventos básicos	Descrição	F-V
AC1EEDGCCF33D13	CCF de todos DGEs após 1ª hora	0,42388
LOOP2	Eventos centrados na subestação primária	0,38826
TL (LOOP3)	Falha da LT	0,26345
AC1EEDGCCF31D03	CCF de todos DGEs na partida	0,25882
LOOP4	Eventos relacionados ao clima	0,1802

Fonte: Código computacional CAFTA [82].

Tabela 13 – Eventos básicos do projeto D com maiores contribuições para o risco.

Eventos básicos	Descrição	F-V
AC1EEDGCCF33D13	CCF de todos DGEs após 1ª hora	0,54489
OPERACPN1E001FC	Operador falha para alinhar a fonte AAC-1 ao barramento A / fonte AAC-2 ao barramento B	0,45193
OPERACPN1E002FC		

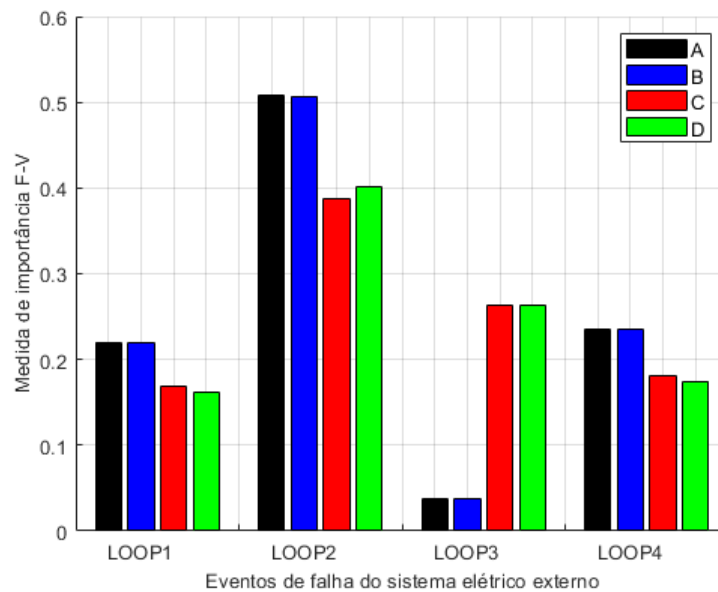
Eventos básicos	Descrição	F-V
LOOP2	Eventos centrados na subestação primária	0,40064
AC1EEDGCCF31D03	CCF de todos DGEs na partida	0,33219
TL (LOOP3)	Falha da LT	0,26318

Fonte: Código computacional CAFTA [82].

Na Figura 22 é representada a medida de importância F-V para os eventos de falha do sistema elétrico, onde: LOOP1 - eventos centrados na planta; LOOP2 - eventos centrados na subestação primária/entrada; LOOP3 - eventos relacionados à rede (sistema de transmissão); e LOOP4 – eventos relacionados ao clima. Destaca-se o aumento da contribuição do LOOP3 para o risco nos projetos C e D, já que estes possuem apenas uma LT em suas configurações.

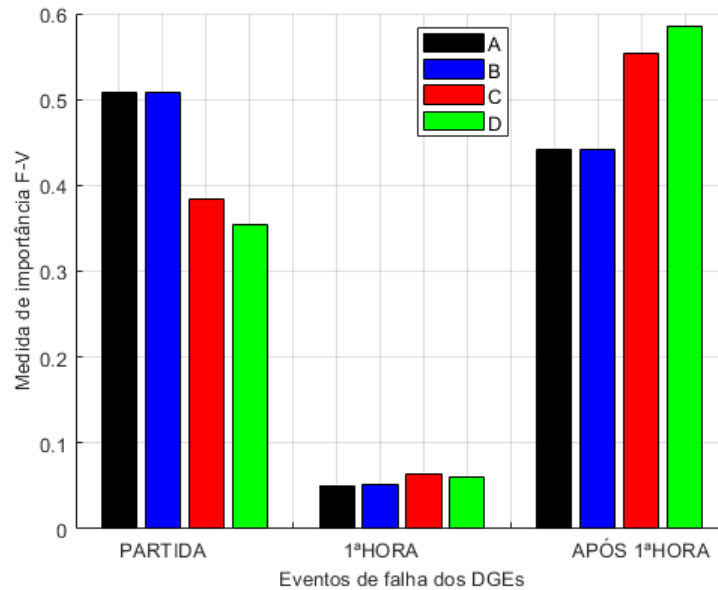
Na Figura 23 é mostrada a contribuição dos eventos relacionados aos DGEs na partida, durante e após a 1ª hora de operação. Os eventos de falha na partida incluem também os eventos de manutenção e testes realizados nos DGEs. Durante a partida dos DGEs, a indisponibilidade por manutenção e testes teve maior contribuição nos projetos A e B (evento básico não consta na Tabela 10 e Tabela 11). Entretanto, durante e após a 1ª hora de operação dos DGEs, a falha de causa comum entre os DGEs foi predominante, com maior contribuição para o risco nos projetos C e D.

Figura 22 – Importância dos eventos básicos de falha do sistema elétrico externo para o risco de cada projeto.



Fonte: Autor.

Figura 23 – Importância dos eventos básicos de falha dos DGEs para o risco de cada projeto.



Fonte: Autor.

3.5.8 Análise de sensibilidade

3.5.8.1 Manutenção/teste simultâneo em diesel geradores

A primeira análise de sensibilidade dos resultados consistiu em desconsiderar a suposição de que não é permitida a manutenção/teste em mais de um diesel gerador ao mesmo tempo. Como resultado, os projetos apresentaram um aumento da medida de risco. Na Tabela 14 são apresentados os resultados, cuja última coluna representa o acréscimo no risco para cada projeto quando comparado aos projetos originais que consideram a premissa de manutenção/teste.

Tabela 14 – Resultado do risco para os projetos do sistema elétrico CA – sem premissa de teste.

Projeto	CDF_{TOTAL} (/ano) (original)	CDF_{TOTAL} (/ano)	ΔCDF_{TOTAL} (%)
A	1,65E-6	1,77E-6	+7,19
B	1,35E-4	1,38E-4	+2,38
C	5,33E-6	5,41E-6	+1,41
D	5,35E-8	5,39E-8	+0,71

Fonte: Autor.

Pode-se verificar nos resultados um aumento mais expressivo do risco para o projeto A (7,19%) e menos expressivo para o projeto D (0,71%), quando se assume a possibilidade de manutenção/teste em mais de um diesel gerador por vez. Os resultados mostram a

importância de um programa de manutenções e testes que atenda requisitos de disponibilidade mínima de fontes de energia de emergência, otimizando desta forma, a confiabilidade/disponibilidade do sistema.

3.5.8.2 Taxa de falha dos DGEs

Para esta análise, são consideradas algumas variações nas taxas de falha dos eventos básicos de todos DGEs, incluindo o evento de indisponibilidade para testes e manutenções. Deste modo, foram consideradas duas situações: (i) as taxas de falha dos eventos associados aos DGEs são 10 vezes maiores do que as taxas originalmente consideradas na análise; e (ii) as taxas de falhas dos DGEs são 10 vezes menores do que inicialmente adotado na análise. Na Tabela 15 é mostrado como resultado da análise de sensibilidade proposta, o impacto das alterações no CDF_{TOTAL} .

Tabela 15 – Resultado do risco para os projetos do sistema elétrico CA – análise de sensibilidade DGEs.

Projeto	CDF_{TOTAL} (/ano) (original)	$\lambda_{DGE} \times 10$		$\lambda_{DGE} \div 10$	
		CDF_{TOTAL} (/ano)	Fator de Aumento CDF_{TOTAL}	CDF_{TOTAL} (/ano)	Fator de Redução CDF_{TOTAL}
A	1,65E-6	1,40E-4	84,70	3,89E-8	42,38
B	1,35E-4	1,12E-2	83,38	3,34E-6	40,38
C	5,33E-6	4,98E-3	934,61	4,03E-7	13,23
D	5,35E-8	5,90E-5	1102,66	4,40E-9	12,16

Fonte: Autor.

O risco para o projeto C e D é bastante afetado quando se utiliza um fator de aumento igual a 10 para a taxa de falha dos DGEs, este resultado pode ser identificado pela coluna do fator de aumento do CDF_{TOTAL} . Entretanto, nota-se que a medida de risco para o projeto D ainda permanece a menor entre os projetos.

3.5.8.3 Taxa de falha do sistema elétrico externo

Para esta análise, as taxas de falha dos eventos de perda do sistema elétrico externo são, também, multiplicadas e divididas por um fator igual a 10. Na Tabela 16 são mostrados os resultados de aumento e diminuição do risco para os projetos.

Tabela 16 – Resultado do risco para os projetos do sistema elétrico CA – análise de sensibilidade do sistema elétrico externo.

Projeto	CDF _{TOTAL} (/ano) (original)	$\lambda_{LOOP} \times 10$		$\lambda_{LOOP} \div 10$	
		CDF _{TOTAL} (/ano)	Fator de Aumento CDF _{TOTAL}	CDF _{TOTAL} (/ano)	Fator de Redução CDF _{TOTAL}
A	1,65E-6	1,61E-5	9,80	1,63E-7	10,10
B	1,35E-4	1,32E-3	9,79	1,35E-5	9,98
C	5,33E-6	5,06E-5	9,49	5,33E-7	10,01
D	5,35E-8	5,95E-7	11,13	4,42E-9	12,10

Fonte: Autor.

As modificações nas taxas dos eventos de falha do sistema elétrico externo resultam em um fator de aumento/redução do CDF_{TOTAL} ligeiramente maior para o projeto D. Quando comparado à análise de sensibilidade dos DGEs, a análise de sensibilidade para os eventos de perda do sistema elétrico externo possui um menor impacto para os diferentes projetos.

Em resumo, independente das três análises de sensibilidade, entre os quatro projetos, o projeto D apresentou o menor risco para a instalação.

4 INSTALAÇÕES NUCLEARES NÃO CONVENCIONAIS COM APLICAÇÕES NAVAIS EM MODO DE DESLIGAMENTO – OBJETO DE ESTUDO

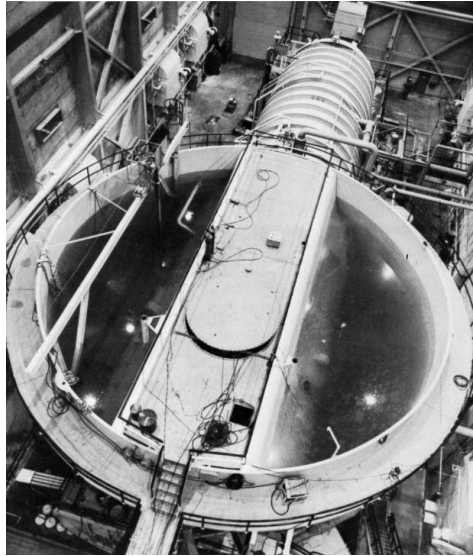
Neste capítulo apresenta-se uma breve descrição das instalações nucleares não convencionais com aplicações navais, enfatizando-se as principais diferenças operacionais entre estas instalações e usinas nucleares comerciais. Em seguida, é realizada uma avaliação de um protótipo em terra da propulsão nuclear em modo de desligamento para troca de combustíveis, abordando as diferentes fases do procedimento de troca de combustíveis e os sistemas envolvidos. Além disso, são estabelecidas as principais suposições de operação dos sistemas que garantem a segurança nuclear da instalação. Os sistemas envolvidos e os requisitos de projeto para um protótipo em terra da propulsão nuclear são similares àqueles utilizados na avaliação de estaleiros de apoio a submarinos nucleares.

4.1 Descrição das instalações nucleares não convencionais com aplicações navais

Protótipos em terra de submarinos com propulsão nuclear e estaleiros que prestam apoio operacional/manutenção a submarinos com propulsão nuclear compõem os dois tipos de instalações nucleares não convencionais com aplicações navais abordados neste trabalho.

Protótipos em terra de submarinos com propulsão nuclear são instalações com reatores de potência. Entretanto, esses reatores possuem características de operação e projeto semelhantes às de um submarino, como por exemplo, os reatores estão inseridos em um casco metálico e operam isolados da rede elétrica externa, assim como nos submarinos. Na Figura 24 é mostrada a seção que contém o reator do protótipo do primeiro submarino nuclear no mundo, o *Nautilus*. Nesta Figura 24, é possível verificar uma piscina de blindagem no entorno da seção do casco onde o reator está localizado. Esta piscina possui a função de blindagem radiológica e de resfriamento do sistema de remoção de calor residual.

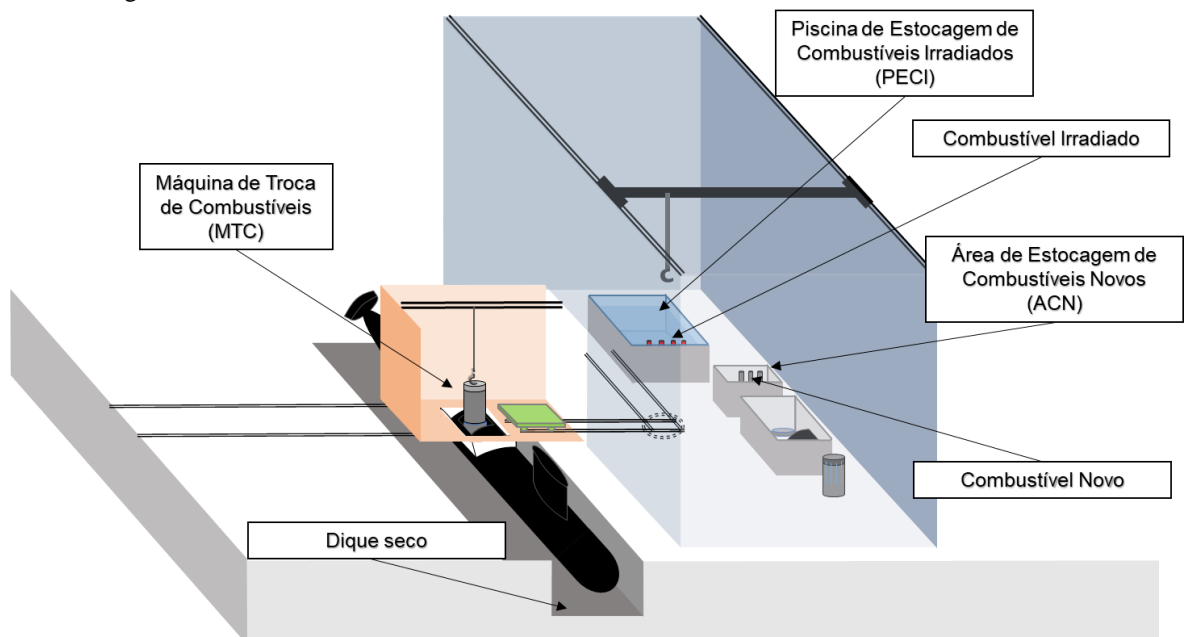
Figura 24 – Protótipo da propulsão nuclear do submarino *Nautilus*



Fonte: [http\ans.org](http://ans.org) [90].

Estaleiros que prestam apoio aos submarinos com propulsão nuclear são instalações sem reatores, entretanto quando um submarino realiza a parada para troca de combustíveis ou manutenções de alto escalão (reator desligado), a garantia da segurança nuclear deixa de pertencer ao submarino e passa a ser responsabilidade do estaleiro. Desta forma, pode-se considerar que o estaleiro é uma instalação que possui reator apenas durante o período de troca de combustíveis ou manutenções de alto escalão do submarino. Na Figura 25 estão representados o estaleiro e as estruturas envolvidas durante a troca de combustíveis do reator de um submarino nuclear.

Figura 25 – Estruturas envolvidas durante a troca de combustíveis de um submarino nuclear.



Fonte: Autor.

As estruturas envolvidas na troca de combustíveis para o protótipo em terra do submarino e para o estaleiro são praticamente as mesmas. Basicamente, o que difere é a estrutura de resfriamento secundário do sistema de remoção de calor residual do reator. No protótipo, esse sistema é representado pela piscina de blindagem e seus componentes (bombas, trocadores de calor e válvulas). No estaleiro, o submarino está no dique seco e não há a presença de água no entorno da seção do reator. Entretanto, um sistema muito similar formado por bombas, trocadores de calor e válvulas também realiza o resfriamento do sistema de remoção de calor residual do reator.

É evidente que o processo da troca de combustíveis do reator nuclear de uma instalação não convencional com aplicações navais apresenta algumas particularidades em relação ao de uma usina nuclear comercial, destacando-se os seguintes aspectos:

Transferência do combustível irradiado (reator – piscina):

A. Usina nuclear comercial

O Vaso de Pressão do Reator (VPR) é inundado, o combustível irradiado é removido do VPR e segue diretamente para a Piscina de Estocagem de Combustíveis Irrradiados (PECI), via um canal de transferência, quando a PECI está localizada fora da contenção, ou por um sistema de comportas, quando a PECI está dentro da contenção.

B. Instalação nuclear não convencional com aplicações navais

O combustível irradiado é removido do VPR por uma Máquina de Transferência de Combustíveis (MTC), sendo descarregado na PECI. A cápsula da MTC, que armazena o combustível durante o processo de transferência para a PECI, é preenchida com água de maneira que o elemento combustível irradiado seja inundado durante todo o transporte.

Periodicidade da troca de combustíveis

A. Usina nuclear comercial

As paradas para troca de combustíveis em reatores do tipo PWR ocorrem geralmente a cada 12 meses.

B. Instalação nuclear não convencional com aplicações navais

As paradas para trocas de combustíveis ocorrem geralmente a cada 36 meses. Esse intervalo de tempo pode variar dependendo do tipo de tecnologia utilizada no reator destas instalações.

Queima do Combustível

A. Usina nuclear comercial

As usinas nucleares de potência operam a uma faixa de potência constante, que de certa forma propiciam uma queima relativamente homogênea do elemento combustível. Desta forma, em uma parada para troca dos combustíveis, é necessária a troca de apenas parte dos elementos combustíveis.

B. Instalação nuclear não convencional com aplicações navais

Os reatores com aplicações navais apresentam características de operação com faixas de potência variáveis (seguidores de carga), resultando em uma queima irregular do elemento combustível. Uma das consequências desta queima irregular é a troca completa do combustível irradiado, por ocasião da parada.

4.1.1 Descrição dos tipos de paradas em modo de desligamento

Tomando como base um reator do tipo PWR, evidenciam-se os três modos de desligamento previstos [91]:

- Tipo A: desligamento para manutenção, religamento sem reduzir o inventário do sistema de resfriamento do reator e não há troca de combustíveis;
- Tipo B: desligamento para manutenção com o inventário do sistema de resfriamento do reator abaixo do normal e religamento sem troca de combustíveis. Em contraste com o tipo A, o inventário é reduzido e as barreiras de pressão são abertas. Durante o período de abertura do tampo do reator, os geradores de vapor não são utilizados para remoção de calor residual; e
- Tipo C: desligamento para troca de combustíveis, que inclui ambas as condições do tipo A e B. Em contraste com os tipos A e B, pode haver uma abundante quantidade de água sobre o combustível (inundação) para descarregamento do combustível irradiado do reator para a piscina de estocagem. Podem existir condições de redução de inventário (*midloop*) em períodos anteriores e posteriores ao abastecimento.

Os tipos de paradas previstas no modo de desligamento e suas principais características são sintetizados na Tabela 17.

Tabela 17 – Tipos de parada para instalações com reator tipo PWR no modo de desligamento.

Tipos de parada	Atividade de troca de combustíveis	Estado de redução do inventário (<i>midloop</i>)	Religamento da planta
A	NÃO	NÃO	SIM
B	NÃO	SIM	SIM
C	SIM	SIM	SIM

Fonte: *US-APWR Design Control Document* [91].

Deve-se observar que a parada do tipo C representa a interrupção na operação para troca de combustíveis no modo de desligamento, que será considerada no estudo de caso da aplicação da metodologia proposta neste trabalho.

4.2 Avaliação do protótipo em terra da propulsão nuclear em modo de desligamento

Conforme abordado na NUREG-1449 [69], o regime de baixa potência e modo de desligamento compreende o período em que o reator está em um estado subcrítico ou está em transição entre a subcriticalidade e a operação em potência limitada a 5% do valor nominal. A NUREG-1449 [69] realiza avaliações apenas para as condições em que o combustível está no Vaso de Pressão do Reator (VPR). A avaliação aborda todos os aspectos do Sistema de Suprimento de Vapor Nuclear (*Nuclear Steam Supply System*, NSSS), a contenção e todos os sistemas que suportam a operação do NSSS. A avaliação não aborda eventos que envolvam o manuseio do combustível fora da contenção, nem o armazenamento do combustível no prédio de armazenamento.

Neste trabalho, a análise não se limitará ao combustível dentro do VPR e se estenderá para seu armazenamento na PEGI durante o período da troca de combustíveis. Sendo assim, a proposta da análise é determinar o risco para a instalação resultante da perda do sistema de remoção de calor residual do primário e do sistema de resfriamento da piscina de estocagem de combustíveis irradiados durante a parada para troca de combustíveis em modo de desligamento. Nesta análise de risco, a contribuição do sistema elétrico da instalação é enfatizada.

A APS nível 1 em modo de desligamento inclui estruturas, sistemas e equipamentos da instalação necessários para manter os parâmetros da planta em um estado estável e seguro durante o procedimento de troca de combustíveis. Isso envolve os seguintes sistemas de linha de frente:

- Sistema de Remoção de Calor Residual (SRCR); e

- Sistema Primário de Resfriamento da Piscina de Estocagem de Combustíveis Irrradiados (SPRP).

Adicionalmente, o Sistema de Água de Segurança (SAS), Sistema de Resfriamento dos Componentes do Primário (SRCP), Sistema Secundário de Resfriamento da Piscina de Combustíveis Irrradiados (SSRP) e Sistemas Elétricos⁴ CA e CC desempenham uma função secundária e de suporte para os sistemas de linha de frente na remoção de calor residual do núcleo.

4.2.1 Configurações da planta em modo de desligamento para troca de combustíveis

Diferentemente de uma APS para a planta em potência, durante o modo de desligamento a configuração da planta muda ao longo do tempo. O combustível não é restrito apenas ao VPR e trens elétricos inteiros podem ser retirados de serviço em simultâneo. Fatores como estes devem ser considerados durante a análise em desligamento. A análise do modo de desligamento para troca de combustíveis inclui: resfriamento do núcleo; preparação e desmontagem do reator; descarga e movimentação do combustível irradiado; movimentação e recarga do combustível novo; manutenções e testes; e preparação para o religamento.

Durante a descarga e movimentação do combustível irradiado, o combustível é removido do VPR e armazenado na PECl. Isto requer modificações na configuração da planta para receber o combustível na PECl. A tampa do VPR e seus internos são removidos para que o combustível possa ser movimentado com segurança para a PECl. Ao longo destes processos, os sistemas necessários para manter o resfriamento do combustível variam.

O SRCR realiza o resfriamento do combustível dentro do VPR, desde o desligamento do reator (após atingir os valores de temperatura e pressão previstos em projeto) até o descarregamento completo de todos os elementos. O Sistema de Resfriamento da Máquina de Troca de Combustíveis (SRMTC) realiza o resfriamento do elemento combustível irradiado no interior da MTC, durante sua movimentação entre o VPR e a PECl. Ao ser descarregado na PECl, o SPRP passa a ser responsável pelo resfriamento do combustível irradiado.

No processo de recarga do reator, o combustível é movimentado via MTC da Área de Estocagem de Combustíveis Novos (ACN) para o VPR. E por último, são realizados os

⁴ Inclui o sistema CA ininterrupto e o sistema de I&C das variáveis do sistema elétrico.

procedimentos para religamento do reator.

É evidente, pelas mudanças nas configurações da planta, que a análise da parada para troca de combustíveis em modo de desligamento não pode ser tratada como um único estado, devendo ser empregada uma abordagem de missão em fases. Sendo assim, são identificadas cinco fases, conforme Tabela 18, com duração de 40 dias, iniciando-se na Fase I com o desligamento do reator e encerrando-se na Fase V com o religamento do reator, já com o combustível novo.

Tabela 18 – Fases do procedimento de troca de combustíveis de um protótipo em terra da propulsão naval.

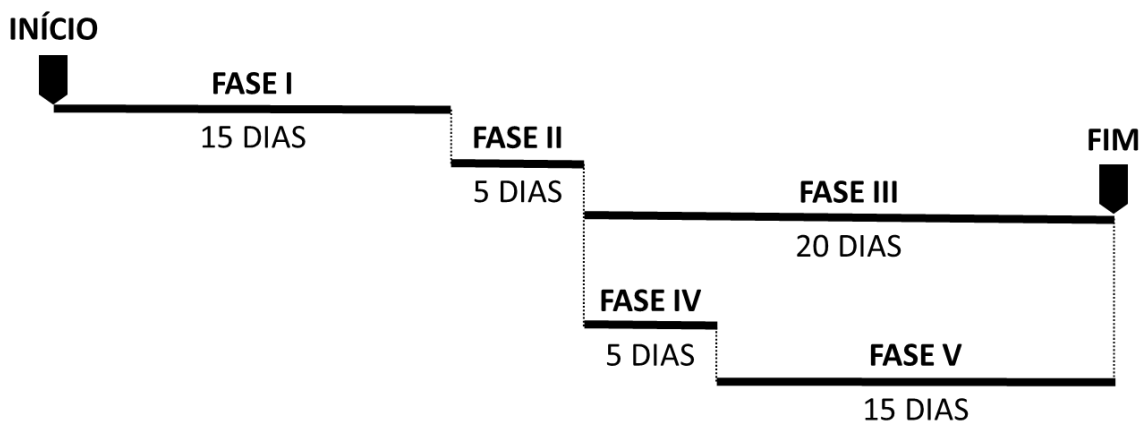
Fase	Descrição	Localização do combustível	Estado do tempo do reator	Sistema primário de resfriamento	Duração (dias)
I	Resfriamento do núcleo	VPR	Posicionado	SRCR	15
II	Descarregamento e movimentação do combustível irradiado	VPR	Removido	SRCR	5
		MTC		SRMTC	
III	Descarregamento completo do combustível	PECI	Removido	SPRP	20
				ACN	
IV	Movimentação e carregamento do combustível novo	MTC	Removido	-	5
		VPR			
V	Preparação para o religamento com combustível novo	VPR	Posicionado	-	15

Fonte: Autor.

Na análise, não é considerado crível um acidente de dano ao núcleo devido à perda do SRMTC, haja vista que, o combustível é movimentado individualmente, um elemento por vez, o tempo de movimentação de cada elemento é limitado há poucas horas e o projeto das MTCs adota sistemas passivos de resfriamento adicionais. Do mesmo modo, não é considerado nenhum acidente de dano ao núcleo para operações que envolvam os combustíveis novos, visto que não há liberação de calor residual.

Desta forma, são analisadas apenas as configurações da planta ao qual é considerado crível um acidente, ou seja, as fases I, II e III, em que os sistemas SRCR e SPRP estão exercendo função de segurança de resfriamento do núcleo no VPR e na PECI, respectivamente. Ressalta-se, ainda, que o tempo de análise da Fase III estende-se até o fim da fase V, término da parada para troca de combustíveis, conforme ilustrado na Figura 26.

Figura 26 – Sequência cronológica das fases de troca de combustíveis.



Fonte: Autor.

A análise de risco para perda do sistema de resfriamento da PEI, considerando o armazenamento do combustível irradiado por longos períodos, não faz parte do escopo deste trabalho. Conforme abordado em [92], este tipo de análise tem ganhado notoriedade após o Acidente de Fukushima Daiichi e deve ser realizada separadamente para a piscina cumprindo a função de estocagem do combustível irradiado por longos períodos.

Fase I

Uma vez iniciada a fase I do modo de desligamento, o SRCR é requerido para remoção do calor residual gerado pelo núcleo do reator. Durante esta fase de resfriamento, o tempo do VPR está posicionado.

A função do SRCR é remover o calor residual gerado pelo núcleo do reator durante as fases I e II do modo de desligamento. Este sistema consiste em dois trens redundantes de equipamentos, sendo que um permanece em *standby* durante a operação normal. Se o calor residual não puder ser efetivamente removido pelo sistema de geração de vapor depois de um *trip* do reator, um dos dois trens do SRCR será atuado. Apenas um trem do SRCR é requerido para remover o calor residual gerado pelo núcleo do reator, deixando o trem secundário em *standby*. O trem redundante será atuado em caso de falha do trem principal.

Fase II

Na fase II, o VPR e a MTC são inundados para a movimentação do combustível irradiado para a PEI. Dado que o tempo do reator é levantado, inicia-se o processo de remoção do combustível. O SRCR é necessário para a remoção do calor residual do combustível no reator; o SRMTC realiza a remoção de calor residual individualmente de

cada elemento combustível no transporte para a PECEI; e o SPRP tem a função de realizar o resfriamento do combustível irradiado descarregado na PECEI.

Fase III

Durante a fase III, o SRCR não é requerido, pois o núcleo do reator está totalmente descarregado e submerso na PECEI. O SPRP é o único sistema responsável pela remoção de calor residual nesta fase, garantindo as condições de segurança da estocagem do combustível irradiado.

Fase IV

Na configuração da fase IV, o combustível novo é movimentado da ACN via MTC para o VPR. Nesta fase, não há calor residual e não é necessária a atuação de nenhum sistema de resfriamento.

Fase V

Na configuração da fase V, o combustível novo está totalmente carregado no VPR. Durante a preparação para o religamento, o tampo do reator é novamente posicionado e tensionado. Nesta fase, também não há calor residual, não sendo necessária a atuação de nenhum sistema de resfriamento.

4.2.2 Descrição dos sistemas envolvidos

Neste item são descritos detalhadamente os sistemas de linha de frente e os sistemas de suporte responsáveis pela remoção de calor residual do núcleo irradiado durante as fases I, II e III. O SRMTC não é descrito, pois não é considerado crível um acidente de dano ao núcleo por falha do sistema durante o transporte dos elementos combustíveis irradiados.

4.2.2.1 Sistema de Remoção de Calor Residual - SRCR

A operação bem-sucedida de um trem do SRCR é necessária e suficiente para fornecer uma remoção adequada de calor residual do núcleo durante as fases I e II. Portanto, uma perda parcial do SRCR não é motivo de preocupação, visto que apenas um trem é necessário para o sucesso. A perda total do SRCR inclui a falha de ambos os trens do SRCR devido a falhas dos próprios componentes do SRCR, a falha dos sistemas de suporte ou a combinação de ambos. São considerados sistemas de suporte do SRCR: SAS; SRCP; e

Sistema Elétrico.

O SRCR tem a circulação do refrigerante realizada pelas bombas (2156-B5/B6) e os trocadores de calor (2156-TC1/TC2). As bombas B5/B6 realizam a sucção da água do circuito de perna quente, passando pelos trocadores de calor TC1/TC2, onde é resfriada, e injetada novamente no VPR através do circuito de perna fria. Os trocadores de calor TC1/TC2 são resfriados pelas bombas de resfriamento 2156-B7/B8, que realizam a troca de calor com a água da piscina de blindagem. A água da piscina de blindagem aquecida pela remoção de calor residual do reator é resfriada pelo SAS. O SRCR está ilustrado na Figura 32 do anexo B.

4.2.2.2 Sistema de Água de Segurança - SAS

O SAS atua como um último dissipador do calor de decaimento removido do combustível e o transfere para o ambiente através de resfriadores evaporativos (5322-RF01A/RF01B). Apenas um trem do SAS é necessário para fornecer o resfriamento da piscina de blindagem. A configuração do SAS é ilustrada na Figura 33 e na Figura 34 do anexo B.

4.2.2.3 Sistema de Resfriamento dos Componentes do Primário - SRCP

O SRCP fornece resfriamento para a vedação e mancais das bombas de circulação do SRCR. O SRCP é composto por dois trens independentes de equipamentos, cada um com sua própria bomba de circulação (2161-B1A/B1B) e trocador de calor (2161-TC1A/TC1B). Os trocadores de calor do SRCP, TC1A/TC1B, são resfriados pelos resfriadores evaporativos do SAS (5322-RF2/RF3), conforme mostrado na Figura 34 do anexo B. Os dois trens do SRCP compartilham um tanque de expansão comum (2161-TQA/B) fornecido a montante das bombas e trocadores de calor.

As bombas de circulação 2156-B5/B6 do SRCR podem ser resfriadas por qualquer um dos trens do SRCP. Apenas um trem do SRCP é necessário para resfriar com sucesso as bombas de circulação do SRCR, deixando o segundo trem em *standby*. O segundo trem será acionado, caso ocorra uma falha do primeiro trem. A configuração do SRCP é mostrada na Figura 35 do anexo B.

4.2.2.4 Sistema Primário de Resfriamento da Piscina de Estocagem de Combustíveis Irrradiados - SPRP

Assim como no caso do SRCR, a operação bem-sucedida de um trem do SPRP é necessária e suficiente para fornecer a remoção adequada de calor residual do núcleo durante as fases II e III. A perda total do SPRP inclui a falha de ambos os trens do SPRP devido a falhas dos próprios componentes do SPRP, falha dos sistemas de suporte ou a combinação de ambos. São considerados sistemas de suporte do SPRP: SSRP e Sistema Elétrico.

O SPRP é composto por dois trens redundantes, sendo necessário e suficiente apenas um para o resfriamento bem sucedido do combustível irradiado. As bombas de circulação (2110-B02A/B02B) e os trocadores de calor (2110-TC02A/TC02B) são responsáveis pela circulação e a remoção de calor residual da água, respectivamente. Depois que a água passa pelo trocador de calor, ela retorna à PECL. Os trocadores de calor do SPRP são resfriados pelos resfriadores evaporativos do SSRP.

É possível realizar a combinação de qualquer uma das duas bombas de circulação com qualquer um dos dois trocadores de calor do SPRP para que seja cumprida a função de segurança. Assim, para resfriar com sucesso os elementos combustíveis da PECL, uma das duas bombas de circulação do SPRP, B02A ou B02B, e um dos dois trocadores de calor do SPRP, TC02A ou TC02B, devem ser bem-sucedidos na missão. Todas as válvulas do sistema são manuais, e a partida e parada das bombas de circulação são feitas manualmente pelo operador, via painel de controle ou localmente. O SPRP é ilustrado na Figura 36 do anexo B.

4.2.2.5 Sistema Secundário de Resfriamento da Piscina de Estocagem de Combustíveis Irrradiados - SSRP

O SSRP é projetado para servir como fonte de água de resfriamento para os trocadores de calor do SPRP. O SSRP consiste em um circuito fechado com bombas de circulação (2120-B01A/B01B), resfriadores evaporativos (2120-RF01A/RF01B) e tanques de expansão (2120-TQ1A/TQ1B), formando dois trens interconectados totalmente redundantes para que cada bomba, tanque de expansão e resfriador evaporativo possam ser compartilhados, conforme mostrado na Figura 37 do anexo B. O sistema SSRP sempre funciona em conjunto com o SPRP e apenas um trem é necessário e suficiente para resfriar com êxito os trocadores de calor do SPRP.

As bombas B01A/B01B circulam a água dos resfriadores evaporativos

RF01A/RF01B através dos dois trocadores de calor do SPRP, fechando o circuito. As mudanças no volume do SSRP são acomodadas pelos tanques de expansão.

4.2.2.6 Sistema Elétrico

O sistema elétrico da instalação é um sistema de suporte, sendo subdividido em sistema elétrico CA, CC e CA ininterrupto. Adicionalmente, existe um sistema de I&C que processa e controla as variáveis do sistema elétrico, como os dados de subtensão dos relés, sinal de partida dos DGEs, e abertura/fechamento de disjuntores.

A falha do sistema elétrico devido à falha de cabos e junções não foi considerada nas modelagens. Um descritivo operacional do sistema elétrico é realizado em 4.2.3.

4.2.2.6.1 Sistema Elétrico CA

O sistema de elétrico CA é um sistema de suporte que interage com todos os sistemas da instalação que requerem energia CA. Isso inclui os sistemas de energia CC, ininterruptos CA ou qualquer sistema que requeira energia CA, como uma bomba motorizada ou uma válvula.

O limite entre o sistema de energia CA e outros sistemas é o barramento ao qual as cargas dos outros sistemas estão ligadas. O sistema de energia CA é modelado até o barramento. A partir deste, qualquer componente elétrico é modelado diretamente nos sistemas que requerem energia. Por exemplo, a modelagem de uma bomba acionada por motor inclui todos os componentes elétricos entre a bomba e o barramento (normalmente o disjuntor de carga e o sistema de controle da bomba). Esses componentes elétricos são considerados parte do sistema onde a bomba reside. No entanto, uma exceção é feita para cargas que são supridas/alimentadas pelos barramentos de segurança, visto que os disjuntores destes barramentos são controlados exclusivamente pelo sistema de controle central da planta no processo de rejeição e religamento de cargas, na falha do sistema elétrico externo e suprimento de energia pelos DGEs. A Figura 38 e a Figura 39 do anexo B mostram o sistema elétrico CA da instalação, sendo em vermelho os equipamentos que poderão ser acrescentados ou removidos dependendo da alternativa de projeto selecionada para a instalação.

4.2.2.6.2 Sistema Elétrico CC

O sistema de energia CC é suprido pelo sistema CA por retificadores. Cada

retificador é conectado a uma bateria como fonte reserva de energia caso haja falha do sistema elétrico CA. O sistema elétrico CC fornece energia para o comando e sinalização de painéis, válvulas solenoides e partida dos DGEs. Além disso, as baterias do sistema elétrico CC são as fontes ininterruptas de energia, através dos inversores, para as cargas CA que não podem sofrer interrupção no suprimento de energia. A Figura 40 e a Figura 41 do anexo B ilustram a configuração do sistema elétrico CC da instalação, sendo em vermelho os equipamentos que poderão ser acrescentados ou removidos dependendo da alternativa de projeto selecionada para a instalação.

4.2.2.6.3 Sistema Elétrico CA Ininterrupto

O sistema elétrico CA ininterrupto pode ser suprido tanto pelo sistema elétrico CA por transformadores quanto pelo sistema elétrico CC por inversores. O sistema elétrico CA ininterrupto supre energia para o sistema de I&C da instalação, responsável por processar os sinais elétricos do sistema e comandar, entre outros, a abertura/fechamento de disjuntores e a partida dos DGEs. A Figura 42 e a Figura 43 do anexo B mostram o sistema elétrico CA ininterrupto do projeto original da instalação.

4.2.3 Descritivo operacional do sistema elétrico

A instalação em modo de desligamento é normalmente suprida pelo sistema elétrico externo. Ocorrendo a falha deste, o sistema de controle detecta a subtensão nos barramentos de segurança CA 460 V e comanda a abertura de todos os disjuntores que suprem as cargas de segurança (rejeição de cargas), além da partida dos DGEs. Quando os DGEs atingem os valores nominais de tensão e frequência, o sistema de controle comanda o fechamento sequenciado dos disjuntores que foram abertos anteriormente, configurando o processo de religamento das cargas. O processo de religamento tem que ser feito sequencialmente, pois o religamento ao mesmo tempo de cargas acima da capacidade dos DGEs ocasiona um desbalanceamento elétrico e os leva a uma condição de falha. Destaca-se, ainda, que os DGEs dos sistemas de segurança redundantes são acionados simultaneamente pelo sistema de controle, independente de assumir carga, em atendimento ao critério de falha única.

Caso haja a falha concomitante da rede elétrica externa e dos DGEs dos dois trens, os barramentos de segurança ficarão sem energia e irá se configurar o cenário de *Station Blackout*. Nesta condição, o operador deverá realizar o alinhamento manual de pelo menos uma fonte AAC para que a energia seja restabelecida para os barramentos de segurança.

Caso haja falha neste suprimento através das fontes AAC, o cenário de dano ao núcleo ocorrerá devido à falta de resfriamento do núcleo irradiado.

Resumidamente, uma carga CA que executa a função de segurança pode ficar sem o suprimento de energia devido a qualquer uma das seguintes falhas:

1. Falha de todas as fontes de energia CA da instalação: sistema elétrico externo, DGEs e fontes AAC;
2. Falha do sistema elétrico externo e falha no fechamento de um ou mais disjuntores que suprem os quadros elétricos das cargas de segurança, por ocasião do religamento sequenciado das cargas; ou
3. Curto-circuito nos barramentos de segurança.

Ressalta-se que, durante a rejeição de cargas, após a falha do sistema elétrico externo, caso algum disjuntor não abra, este poderá causar sobrecarga nos DGEs e conseqüentemente levá-los a uma condição de falha. Outro ponto de destaque é que a falha do suprimento de energia pode ocorrer devido à falha de um componente do circuito de alimentação e não devido à falha da própria fonte, como por exemplo, o sistema elétrico externo pode ficar indisponível caso haja falha de um disjuntor ou de um transformador.

4.2.4 Principais suposições de operação dos sistemas de segurança da instalação em modo de desligamento

São consideradas algumas suposições relacionadas à operação dos sistemas que garantem a segurança nuclear da instalação. Essas suposições serão adotadas na realização da APS nível 1 em modo de desligamento e estão listadas abaixo:

4.2.4.1 Premissas de segurança da operação

Danos ao núcleo poderão ocorrer caso o nível da água não possa ser mantido acima do topo do combustível irradiado ou se uma temperatura superior a 1200 °C for atingida em qualquer ponto do núcleo. Para que essas condições sejam atingidas, estima-se que:

1. Nas fases I, II e III, estando o núcleo irradiado no VPR ou na PECCI, o acidente ocorre caso haja a falha total dos sistemas de resfriamento do núcleo;
2. Não é considerado crível dano ao núcleo pela perda do SRMTC durante a fase II; e
3. Não é assumido nenhum acidente de dano ao núcleo para operações que envolvam o combustível novo, nas fases IV e V.

Na premissa 1, que trata de falha total dos sistemas de resfriamento do núcleo,

presume-se a falha dos trens de segurança redundantes. Esta premissa não considera o tempo para recuperação dos sistemas de segurança, tempo em que o núcleo pode ficar sem resfriamento, consistindo, portanto, em uma abordagem conservadora em relação ao acidente.

As premissas 2 e 3 foram adotadas em concordância com experiências prévias em projetos de instalações nucleares não convencionais com aplicações navais, considerando cálculos termo-hidráulicos e o termo-fonte envolvido.

4.2.4.2 Premissas de operação dos sistemas

- 1 Estima-se que a troca de combustíveis dos reatores das instalações nucleares não convencionais com aplicações navais ocorra a cada 3 anos e tenha duração de 40 dias. Portanto, a frequência anual da instalação em modo de desligamento para troca de combustíveis é de $3,65E-2$ /ano;
- 2 As fases I e V terão duração de 15 dias (cada), as fases II e IV terão duração de 5 dias (cada) e a fase III terá duração de 20 dias. Portanto, a frequência de ocorrência das fases I e V é de $3,75E-1$ /ano, das fases II e IV é de $1,25E-1$ /ano e da fase III é de $5,00E-1$ /ano;
- 3 O tempo de missão para os eventos do sistema elétrico externo é de 1 ano;
- 4 O tempo de missão para os componentes dos sistemas da instalação é de 24 horas. Assumindo-se que todos os componentes são reparáveis dentro de 24 horas e apenas um trem de segurança é requerido para ter sucesso na missão, se o trem A (principal) falha, é esperado que ele seja reparado dentro de 24 horas, e o trem B (redundante) é requerido por apenas 24 horas para se ter sucesso na missão. Se o trem redundante falha depois das 24 horas de operação, então o trem principal estará disponível e poderá ser usado para completar a missão, assumindo-se apenas uma falha por trem de segurança;
- 5 Como o SRCR está no modo *standby* durante a operação da planta em potência, qualquer teste ou manutenção preventiva dos componentes do SRCR será realizada durante o modo de potência da planta. Portanto, eventos de testes e manutenções do SRCR são ignoradas durante o modo de desligamento, com exceção de manutenções corretivas;
- 6 Assume-se uma indisponibilidade de $5,00E-3$ /ano para testes e manutenções de alguns equipamentos do sistema SPRP e dos sistemas de suporte (SAS, SRCP, SSRP

e baterias do sistema elétrico CC);

- 7 Não é previsto que sejam realizados testes e manutenções simultâneas em trens redundantes de sistemas de segurança;

Premissas específicas sobre o sistema elétrico

- 8 Não é considerado crível o evento de abertura dos disjuntores por modo de falha comum devido a sinais espúrios na rede;
- 9 É considerada uma indisponibilidade mensal de 7,25 horas ($1,00E-2$ /ano), devido a testes periódicos dos diesel geradores de emergência (DGEs) e dos diesel geradores alternativos (fonte AAC). É assumido que apenas um diesel gerador seja testado por vez;
- 10 Assume-se que os diesel geradores de emergência e os diesel geradores alternativos pertençam a grupos de falha de causa comum distintos, sendo assim, a falha de causa comum entre os dois grupos não é modelada;
- 11 Na condição de *Station Blackout* é creditado ao operador alinhar a fonte AAC para suprir energia aos barramentos de segurança. É atribuído um valor de $5,00E-2$ como erro humano na operação;
- 12 É assumido que apenas uma bateria do sistema elétrico CC possa ser testada por vez, apresentando indisponibilidade conforme item 6 ($5,00E-3$ /ano); e
- 13 São modelados eventos de falha dos barramentos CA devido a curtos-circuitos, sendo assumido como resultado a abertura do disjuntor para proteção do sistema.

5 APLICAÇÃO DO MÉTODO E DISCUSSÃO DOS RESULTADOS

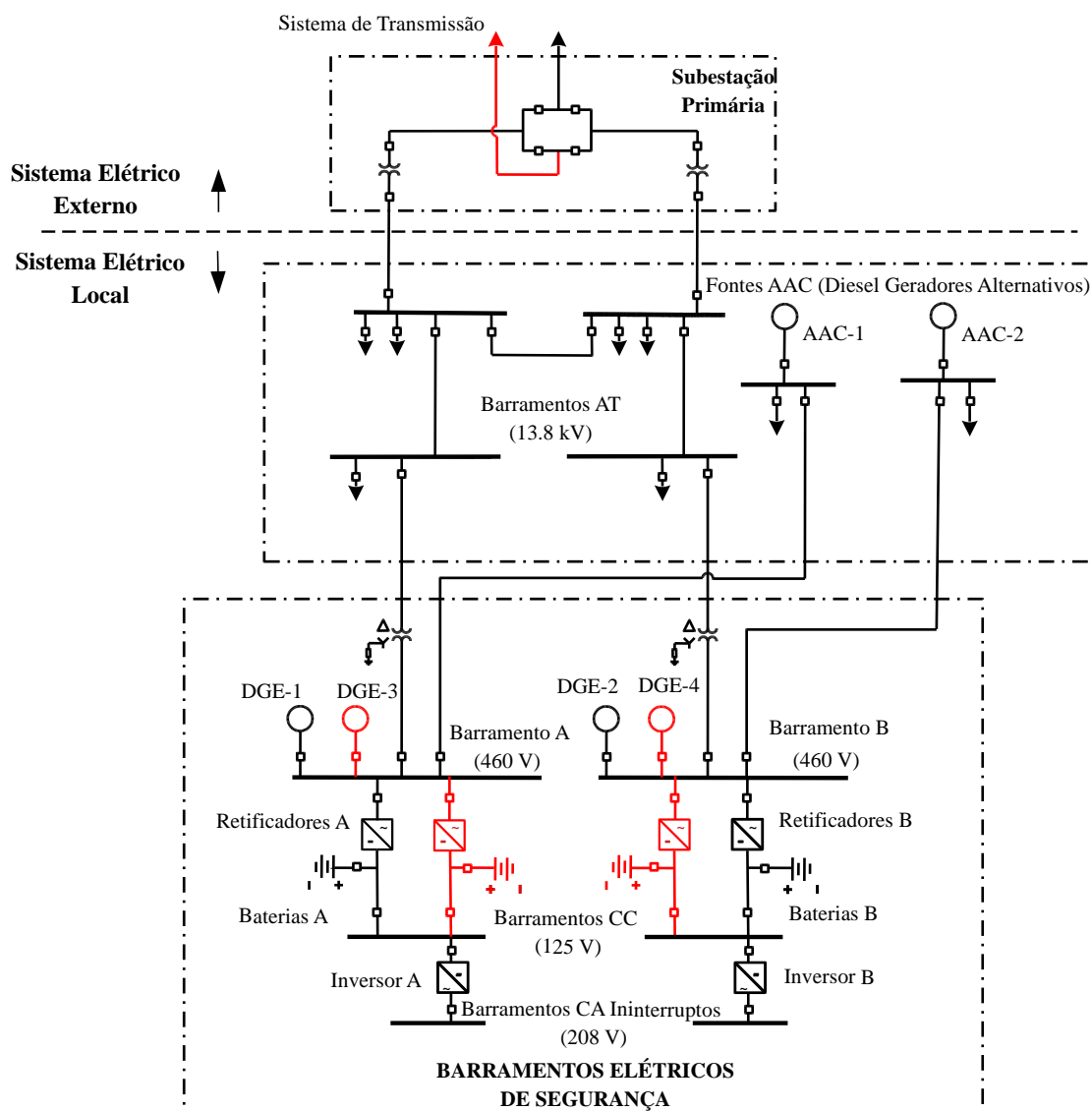
Neste capítulo serão apresentados os resultados e discussões a respeito da aplicação da metodologia para o objeto de estudo descrito no capítulo 4, que consiste na avaliação de segurança de alternativas de projeto de sistemas elétricos de uma instalação nuclear não convencional com aplicações navais, em modo de desligamento, durante a troca de combustíveis, considerando a frequência de dano ao núcleo como principal indicador de risco para a instalação. O modelo implementado no programa computacional CAFTA [82] foi desenvolvido para representar as falhas dos sistemas de um protótipo em terra da propulsão nuclear naval, sendo utilizados dados genéricos para representar as taxas / probabilidades de falha dos equipamentos desses sistemas.

Os sistemas e as suposições adotadas no desenvolvimento do modelo implementado no programa computacional CAFTA [82] foram apresentados na seção 4.2. Assim, o estudo de caso da aplicação da metodologia avalia de forma integrada todos os sistemas responsáveis por garantir a segurança nuclear da instalação, sistemas da linha de frente e de suporte.

São avaliados quatro diferentes projetos do sistema elétrico que suprem energia para a instalação, com alterações tanto no sistema elétrico CA quanto no CC. Adicionalmente, as alterações no modelo podem subsidiar o certame a respeito da necessidade do atendimento ao GDC 17 [3] por instalações nucleares não convencionais com aplicações navais, tendo em vista as particularidades operacionais destas instalações.

Um modelo simplificado do sistema elétrico da instalação estudada é exibido na Figura 27. As modificações de projeto avaliadas no estudo de caso estão destacadas em vermelho. Os diagramas detalhados do sistema elétrico são exibidos da Figura 38 até a Figura 43 do anexo B. As modificações do modelo conduziram a quatro alternativas para o projeto do sistema elétrico, conforme a Tabela 19.

Figura 27 – Sistema elétrico simplificado avaliado no estudo de caso.



Fonte: Autor.

Tabela 19 – Alternativas de projeto do sistema elétrico da instalação estudada.

Projeto	Linhas de transmissão (LTs)	DGEs por barramento de segurança	Retificador/bateria por barramento de segurança
A (original)	2	1	1
B	2	1	2
C	1	2	1
D	1	2	2

Fonte: Autor.

Independente da configuração, em eventos de *Station Blackout* são utilizados dois diesel geradores alternativos adicionais (fontes AAC), dos quais apenas um consegue suprir a demanda de energia das cargas de segurança. Ressalta-se que o sistema elétrico de instalações nucleares não convencionais com aplicações navais atende aos critérios de

redundância, independência, segregação, critério de falha simples, classificação sísmica e qualificação de equipamentos previstos na base normativa de usinas nucleares de potência.

5.1 Eventos iniciadores e delineamento da sequência de acidentes

Existem dois cenários que levam a instalação à condição de dano ao núcleo (acidente):

- %T1: perda completa do SRCR; ou
- %T2: perda completa do SPRP.

No delineamento da sequência de eventos até o acidente, adotaram-se os cenários %T1 e %T2 como eventos iniciadores de probabilidade igual a 1, funcionando assim, apenas como eventos marcadores para organizar os resultados do modelo lógico e simplificar as análises. Na Tabela 20 são listados os possíveis eventos iniciadores para a instalação, mas que são tratados como eventos subsequentes, devido à simplificação adotada. Esses possíveis eventos iniciadores são eventos que englobam várias falhas referentes aos sistemas da linha de frente. Sob uma ótica mais detalhada, sabe-se que existem outros eventos, incluindo eventos associados aos sistemas de suporte, que poderiam ser classificados como eventos iniciadores que levariam à ocorrência destes eventos maiores previstos na Tabela 20, tais como: falha do sistema elétrico externo, falha do sistema elétrico CA e CC, falha de processamento de sinais, falha de equipamentos, entre outros.

Tabela 20 – Possíveis eventos iniciadores.

Cenário	Evento Iniciador
%T1	Falha do trem A do SRCR
%T2	Falha do sistema de bombas do trem A do SPRP; Falha do sistema de trocadores de calor do trem A do SPRP; e Falha do sistema de válvulas comuns do SPRP (tubulação única).

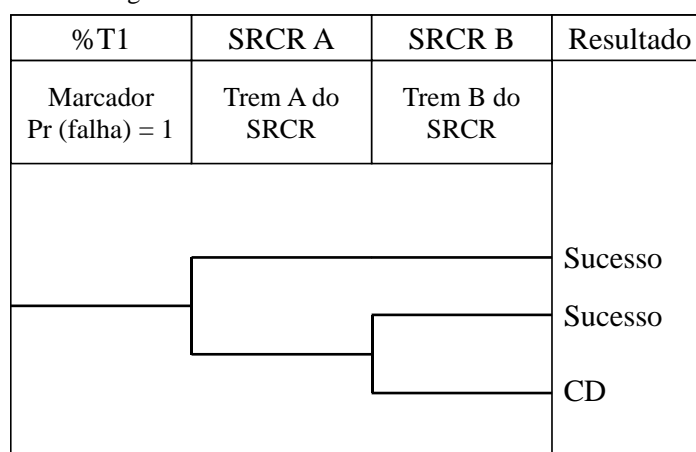
Fonte: Autor.

O SPRP possui uma configuração que permite a combinação entre os sistemas de bombas e trocadores de calor, sendo possível, por exemplo, utilizar o sistema de bombas do trem A e o sistema de trocadores de calor do trem B para realizar a missão de resfriamento do núcleo na PECEI. Para o cenário %T2 adotou-se o sistema de válvulas comuns do SPRP como o primeiro evento subsequente. A falha do sistema de válvulas comuns contribui para o acidente independente da atuação dos outros sistemas, por ser um sistema único (sem redundância) do sistema de resfriamento da PECEI.

Na Figura 28 e na Figura 29 estão representadas as árvores de eventos para os

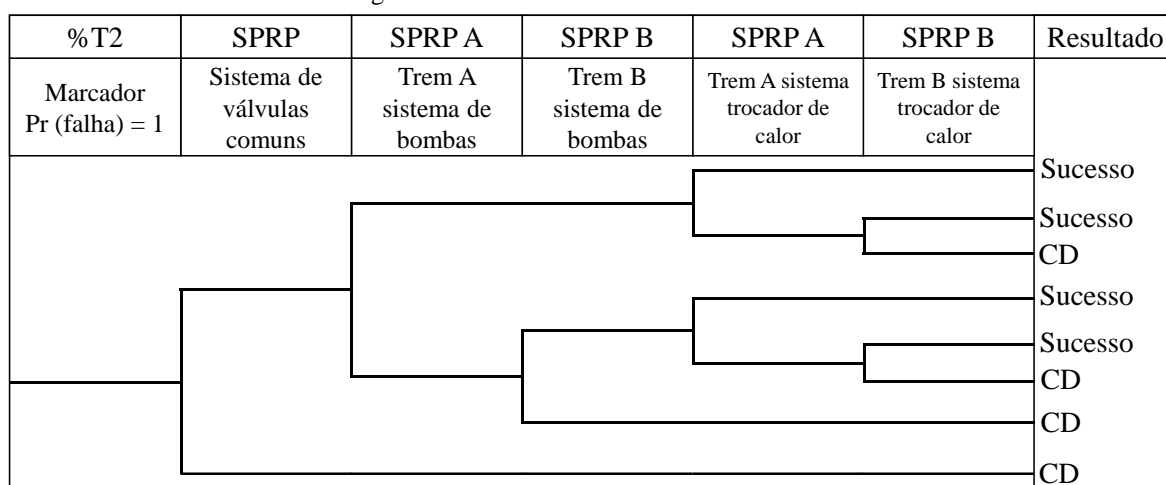
cenários %T1 e %T2, respectivamente. Os eventos principais identificados nestas árvores de eventos são compostos por mais de um evento básico, o que torna possível adotar a mesma sequência de eventos para todas as alternativas de projeto a serem avaliadas. Entretanto, a frequência de ocorrência dos eventos principais da árvore de eventos mudará de acordo com a configuração de cada projeto.

Figura 28 – Árvore de eventos do cenário %T1.



Fonte: Autor.

Figura 29 – Árvore de falhas do cenário %T2.



Fonte: Autor.

CD = *Core Damage*.

5.2 Análise dos sistemas – modelos lógicos

Um modelo de árvore de falhas detalhado foi desenvolvido para cada um dos sistemas requeridos durante o modo de desligamento (sistemas da linha de frente e sistemas de suporte). As dependências entre os sistemas modelados foram implementadas através de *links* gerados pelas árvores de falhas dos sistemas de suporte requeridos para o sucesso da

missão dos sistemas da linha de frente. Desta maneira, árvores de falhas integradas foram desenvolvidas, incluindo todas as dependências. Por fim, uma árvore de falhas *master* foi utilizada para integrar todas as árvores de falhas dos sistemas identificados nos cabeçalhos das árvores de eventos. Eventos de falha de componentes, assim como eventos de testes/manutenções e eventos relacionados a erros humanos, foram incluídos nas árvores de falhas.

No anexo D são apresentados alguns extratos das árvores de falhas modeladas no CAFTA [82]. Na Figura 50 é possível verificar os eventos topo da árvore de falhas *master* que contribuem para o acidente, representados pela falha completa do SRCR ou do SPRP, considerando a indisponibilidade anual da instalação para troca de combustíveis e o tempo de duração de cada fase em que os sistemas são requeridos. Na Figura 51 são mostrados os eventos que levam à falha completa do SRCR. Na Figura 52 são apresentados os eventos que dão origem à falha completa do SPRP. Na Figura 53 estão representados alguns dos eventos que dão origem à falha do sistema elétrico CA (sistema de suporte), que tem destaque nas análises deste trabalho. A falha no suprimento normal de energia (via sistema de transmissão) e no suprimento de emergência (via DGEs) para os barramentos de segurança dos trens A e B são identificados pelos eventos marcadores %SBO_A e %SBO_B, respectivamente, com probabilidade igual a 1. Assim, o evento de *Station Blackout* é contabilizado pela soma das probabilidades dos cortes mínimos que contêm simultaneamente os eventos %SBO_A e %SBO_B.

5.3 Banco de dados de confiabilidade e análise de confiabilidade humana

O banco de dados que supriu as informações para o modelo foi extraído da Tabela 39, Tabela 40 e Tabela 41 do anexo A para taxas de falha de equipamentos, eventos de falha do sistema elétrico externo e falhas de causa comum, respectivamente. Informações adicionais como tempo de missão, indisponibilidade para manutenções/testes e erro humano em operações foram incorporadas na modelagem conforme item 4.2.4.

5.4 Integração do modelo e quantificação

Conforme mencionado anteriormente, a integração dos modelos foi realizada através de *links* das árvores de falhas dos diferentes sistemas e ao final através da construção de uma árvore de falhas *master*, mostrada na Figura 50 do anexo D. O processo de quantificação do modelo foi realizado através do método de cortes mínimos. A combinação da frequência do

evento iniciador com a probabilidade de cada evento básico, em uma sequência específica, fornece a frequência de ocorrência para esta sequência do acidente. Devido ao grande número de combinações possíveis entre os eventos dos ramos das árvores de eventos que são representadas por árvores de falhas, o número total de cortes mínimos que poderiam conduzir ao acidente seria de uma ordem muito elevada. Por este motivo, uma frequência de truncamento de $1E-11$ /ano foi selecionada, onde apenas os cortes mínimos com frequência de ocorrência igual ou superior a este valor são calculados.

Na Tabela 42 do anexo E são apresentados os 20 cortes mínimos que possuem maior contribuição para o acidente. Estes 20 cortes mínimos são os que mais contribuem para o risco da instalação nas quatro alternativas de projeto do sistema elétrico.

5.5 Interpretação dos resultados

Conforme apresentado na Tabela 21, a instalação na configuração original do sistema elétrico (projeto A) apresentou como medida de risco um CDF de $1,29E-5$ /ano. Em comparação com o projeto A, houve uma diminuição no risco (ΔCDF_{TOTAL}) de aproximadamente 1,35%, 2,29% e 3,65% para os projetos B, C e D, respectivamente. A medida de risco associada aos cenários %T1 e %T2 também é apresentada na tabela, considerando que estes cenários de acidente podem ocorrer devido a falhas intrínsecas dos próprios componentes dos sistemas de linha de frente (SRCR ou SPRP), em decorrência da falha dos sistemas de suporte ou, ainda, como consequência da combinação de eventos associados a ambos os tipos de sistemas.

Tabela 21 – Resultados do risco para a instalação medido pela Frequência de Dano ao Núcleo (CDF) considerando as alternativas de projeto do sistema elétrico.

Projeto	CDF _{TOTAL} (/ano)	ΔCDF_{TOTAL} (%)	CDF (/ano)	
			%T1	%T2
A (original)	1,29E-5	-	1,06E-5	2,36E-6
B	1,28E-5	-1,35	1,04E-5	2,34E-6
C	1,26E-5	-2,29	1,04E-5	2,26E-6
D	1,25E-5	-3,65	1,02E-5	2,24E-6

Fonte: Autor.

Fica evidenciado que a perda total do SRCR (%T1) é o cenário que mais contribui para o dano ao núcleo durante a troca de combustíveis em modo de desligamento, independente da alternativa de projeto do sistema elétrico. Analisando os cortes mínimos da Tabela 42 do anexo E, é possível verificar uma contribuição elevada dos eventos básicos de

falha de causa comum dos motores das bombas dos sistemas, assim como dos eventos de indisponibilidade por manutenções e testes. Os eventos básicos do sistema elétrico não aparecem na seleção dos 20 cortes mínimos que mais contribuem para o risco da instalação. Entretanto, tanto para o projeto A quanto para o C, que possuem apenas um conjunto retificador/bateria por trem de segurança, o evento básico da falha do retificador do trem A (RNC-1F-141) compôs o corte mínimo que obteve a 52ª maior contribuição (1,89E-8/ano) para o risco da instalação.

A Tabela 22 e a Tabela 23 apresentam a contribuição dos sistemas da instalação para o acidente de dano ao núcleo e a variação percentual do risco dos sistemas ($\Delta CDF_{\text{SISTEMAS}}$) em relação ao projeto A (original), respectivamente. É possível verificar, comparando os projetos A (original) e D, que houve uma redução de risco associado ao sistema elétrico de 68,48%.

Tabela 22 – Contribuição dos sistemas para a Frequência de Dano ao Núcleo (CDF) da instalação considerando as alternativas de projeto do sistema elétrico.

Sistemas	Descrição	Projetos - CDF (/ano)			
		A (original)	B	C	D
SRCR	Sistema de Remoção de Calor Residual	6,68E-6	6,57E-6	6,63E-6	6,52E-6
SPRP	Sistema Primário de Resfriamento da Piscina de Combustíveis Irradiados	2,28E-6	2,27E-6	2,22E-6	2,21E-6
SRCP	Sistema de Resfriamento de Componentes do Primário	2,10E-6	2,09E-6	2,06E-6	2,04E-6
SAS	Sistema de Água de Segurança	1,80E-6	1,80E-6	1,76E-6	1,75E-6
SSRP	Sistema Secundário de Resfriamento da Piscina de Combustíveis Irradiados	2,90E-10	2,90E-10	2,90E-10	2,90E-10
SE	Sistema Elétrico	1,09E-6	8,06E-7	6,29E-7	3,43E-7

Fonte: Autor.

Tabela 23 – Variação percentual do risco dos sistemas na comparação das alternativas de projeto do sistema elétrico em relação ao projeto A (original).

Sistemas	Projetos		
	$\Delta CDF_{\text{SISTEMAS}}$ (%)		
	B	C	D
SRCR	-1,64	-0,70	-2,41
SPRP	-0,24	-2,45	-2,77
SRCP	-0,46	-2,23	-2,77
SAS	-0,23	-2,47	-2,77
SSRP	0,00	0,00	0,00

Sistemas	Projetos		
	$\Delta CDF_{\text{SISTEMAS}} (\%)$		
	B	C	D
SE	-26,08	-42,25	-68,48

Fonte: Autor.

A Tabela 24 e a Tabela 25 mostram a contribuição dos sistemas elétricos para o acidente de dano ao núcleo e a variação percentual do risco associado às alternativas de projeto dos sistemas elétricos (ΔCDF_{SE}) em relação ao projeto A, respectivamente. Destaca-se que o projeto D, quando comparado ao projeto A, apresentou uma redução de risco associado ao sistema elétrico CA de 67,64% e ao sistema elétrico CC de 80,50%. Pode-se observar, também, que a adição de um conjunto retificador/bateria por barramento de segurança, quando se compara os projetos D e C ou B e A, não apenas contribui para a diminuição do risco associado ao sistema elétrico CC como também para os outros sistemas elétricos. Isso se deve ao fato de que o sistema elétrico CC é a fonte de energia para o sistema elétrico CA ininterrupto e o sistema de I&C, que comanda e controla o sistema elétrico.

Tabela 24 – Contribuição dos sistemas elétricos para o risco da instalação considerando as alternativas de projeto desses sistemas.

Sistemas elétricos	Descrição	Projetos			
		CDF (/ano)			
		A	B	C	D
CA	Sistema Elétrico de Corrente Alternada	8,27E-7	7,32E-7	3,58E-7	2,68E-7
CC	Sistema Elétrico de Corrente Contínua	2,17E-7	4,23E-8	2,19E-7	4,23E-8
CA ⁵ (Ininterrupto)	Sistema Elétrico de Corrente Alternada Ininterrupto	7,62E-9	-	9,99E-9	-
I&C ⁶ (elétrico)	Instrumentação e Controle do Sistema Elétrico	3,85E-8	3,14E-8	4,32E-8	3,37E-8

Fonte: Autor.

Tabela 25 – Variação percentual do risco associado aos sistemas elétricos comparando alternativas de projeto em relação ao projeto A (original).

Sistemas elétricos	Projetos		
	$\Delta CDF_{\text{SE}} (\%)$		
	B	C	D
CA	-11,47	-56,73	-67,64
CC	-80,50	+0,71	-80,50
CA	-100	+31,05	-100

⁵ A falha do sistema elétrico CA inclui o erro humano associado ao alinhamento das fontes AAC aos barramentos de segurança.

⁶ A I&C refere-se aos sistemas de controle, processamento e aquisição de dados elétricos.

Sistemas elétricos	Projetos		
	$\Delta CDF_{SE} (\%)$		
	B	C	D
(Ininterrupto)			
I&C (elétrico)	-18,52	+12,10	-12,60

Fonte: Autor.

Os valores de CDF para o sistema elétrico CA ininterrupto nos projetos B e D são de ordem menor que $1E-11$ /ano, que é a probabilidade de truncamento dos cortes mínimos, por isso não aparecem nos resultados de risco mostrados na Tabela 24.

A Tabela 26 mostra a contribuição do cenário de *Station Blackout* para o risco da instalação em cada alternativa de projeto do sistema elétrico. Neste caso, uma redução de 98,83% é verificada nos projetos C e D quando comparados ao projeto A.

Tabela 26 – Risco da instalação medido pela Frequência de Dano ao Núcleo devido a um evento de *Station Blackout*.

Projeto	$CDF_{SBO} (/ano)$	$\Delta CDF_{SBO} (\%)$
A (original)	7,94 E-8	-
B	7,26E-8	-8,61
C	9,27E-10	-98,83
D	9,27E-10	-98,83

Fonte: Autor.

A falha do sistema elétrico externo poderá iniciar alguns cenários acidentais que não conduzirão, necessariamente, a instalação ao evento de *Station Blackout*. Isso porque, quando a falha da rede elétrica externa é detectada, o sistema de controle comanda a partida dos DGEs e a abertura de todos os disjuntores que alimentam as cargas de segurança (rejeição de cargas). Quando os DGEs atingem seus valores nominais de tensão e frequência, os disjuntores que suprem as cargas devem ser fechados de maneira automática e sequencial. Caso algum disjuntor falhe ao fechar, a carga elétrica associada a este disjuntor que cumpre a função de segurança ficará sem energia, podendo originar um cenário acidental. Nesse cenário não há a falha concomitante da rede elétrica externa e dos DGEs que configuram a ocorrência de um evento de *Station Blackout*. Desta maneira, com relação aos sistemas elétricos, apesar do evento de *Station Blackout* ser o cenário mais crítico e desafiador, que necessita inclusive de intervenções humanas que podem contribuir para o aumento do risco da instalação, a perda do sistema elétrico externo mostra-se como um evento que pode dar origem a outras sequências de acidentes.

Na Tabela 27 é apresentado o risco associado aos eventos de perda do sistema elétrico

externo (LOOP) e ao evento de *Station Blackout*, considerando todas as alternativas de projeto do sistema elétrico. Os resultados mostram que o risco associado à perda do sistema elétrico externo para os projetos com duas LTs (projetos A e B) é maior que àquele dos projetos com apenas uma LT (projetos C e D). Considerando que a probabilidade de falha do sistema elétrico externo seja maior para os sistemas com apenas uma LT, esta falha somente terá relevância para o risco global da instalação quando ocorrer com a falha de componentes do sistema elétrico local, o que restringe o fornecimento de energia para algumas cargas de segurança, podendo originar num cenário acidental.

Tabela 27 - Risco da instalação devido à perda do sistema elétrico externo (LOOP).

Projeto	CDF _{SBO} (/ano)	CDF _{LOOP} (/ano)	Δ CDF _{LOOP} (%)
A (original)	7,94 E-8	5,55E-7	-
B	7,26E-8	4,83E-7	-12,98
C	9,27E-10	2,59E-7	-53,37
D	9,27E-10	1,85E-7	-66,63

Fonte: Autor.

No que lhe concerne, os disjuntores desempenham um papel importante para o risco associado aos sistemas elétricos da instalação. Como foi ilustrado acima, os disjuntores realizam a rejeição das cargas (abrem) e o religamento sequencial das cargas (fecham). A falha ao fechar após o restabelecimento de energia do barramento pelo DGE pode acarretar ausência de energia para uma carga de segurança e, conseqüentemente, levar a instalação uma condição acidental. Por outro lado, durante a rejeição de cargas, se algum disjuntor falha ao abrir, o DGE ao tentar suprir o barramento pode sofrer uma sobrecarga e falhar. A abertura e o fechamento dos disjuntores são comandados pelo sistema de controle que possui como fonte de energia ininterrupta as baterias do sistema elétrico CC. Uma arquitetura do sistema elétrico CC pouco robusta, ou seja, com baixa confiabilidade, pode contribuir para a falha dos disjuntores e, conseqüentemente, aumentar o risco da instalação. Adicionalmente, os disjuntores podem falhar durante a operação por sinal espúrio na rede. A falha por sinal espúrio de um disjuntor do circuito de energia que alimenta uma carga de segurança pode desencadear um cenário acidental, aumentando o risco para a instalação.

5.6 Classificação de importância

Na Tabela 28 são mostrados os oito eventos básicos mais importantes em relação ao CDF calculado para cada alternativa de projeto do sistema elétrico. A medida de importância calculada foi a de *Fussel-Vesely* (F-V). Os eventos aparecem na mesma ordem de

importância para os quatro diferentes projetos. A partir da nona posição da medida de importância de F-V, os eventos básicos começam a diferir para as alternativas de projeto. Destacam-se as falhas de causa comum das bombas dos sistemas da linha de frente e a indisponibilidade por manutenção/teste de componentes dos sistemas de suporte.

Tabela 28 – Eventos básicos com maiores contribuições para o CDF calculado para cada alternativa de projeto do sistema elétrico.

Eventos básicos	Descrição	F-V			
		A	B	C	D
SRC2156CCF03MR1	CCF bombas 2156-B5 e 2156-B6 do SRCR no funcionamento	0,21171	0,21461	0,21668	0,21974
SRA2110CCF02MP1	CCF bombas 2110-B2A e 2110-B2B do SPRP na partida	0,10039	0,10176	0,10274	0,10419
RCP2161CCF03MP1	CCF bombas 2161-B1A e 2161-B1B do SRCP na partida	0,08031	0,08141	0,08219	0,08336
SRC2156CCF02MP1	CCF bombas 2156-B5 e 2156-B6 do SRCR na partida	0,08031	0,08141	0,08219	0,08336
SRC2156CCF08MP1	CCF bombas 2156-B7 e 2156-B8 do SRCR na partida	0,08030	0,08141	0,08219	0,08336
SWS5322_B01A_TM	Indisponibilidade por manutenção ou teste da bomba 5322-B01A do SAS	0,06201	0,06286	0,06347	0,06436
SWS5322_B05A_TM	Indisponibilidade por manutenção ou teste da bomba 5322-B05A do SAS	0,06201	0,06286	0,06347	0,06436
SRC2156TC1__HXP	Falha na conexão do trocador de calor 5156-TC1 do SRCP	0,04323	0,04248	0,04366	0,04285

Fonte: Código computacional CAFTA [82].

A Tabela 29 e a Tabela 30 mostram os dez eventos básicos de falhas do sistema elétrico que possuem as maiores contribuições para o CDF, considerando as alternativas de projeto A e B, respectivamente. Comparando os mesmos eventos básicos do sistema elétrico, é possível verificar que existe uma contribuição ligeiramente maior dos eventos básicos do sistema elétrico para o projeto A. A sequência de importância dos eventos básicos é praticamente a mesma para ambos os projetos, alternando-se apenas os eventos básicos da posição 5 e 6 da análise.

Tabela 29 – Eventos básicos de falhas do sistema elétrico do projeto A com maiores contribuições para o CDF.

Posição	Eventos básicos de falhas do sistema elétrico	Descrição	A
			F-V
1	AC_LOOP2	Perda centrada na subestação primária/entrada	0,02300
2	OPERACPN1E001FC	Operador falha ao alinhar a fonte AAC-1 ao CBT-1F-001	0,01143
3	AC_LOOP4	Perdas relacionadas ao clima	0,00986
4	AC_LOOP1	Perdas centradas na planta	0,00910
5	OPERACPN1E002FC	Operador falha ao alinhar a fonte AAC-2 ao CBT-2F-002	0,00825
6	ACGDG001___DGA	DGE-1 falha após 1ª hora	0,00797
7	ACGDG001___DGS	DGE-1 falha na partida	0,00693
8	ACGDG002___DGA	DGE-2 falha após 1ª hora	0,00570
9	ACGDG04A___DGA	Fonte AAC-1 falha após 1ª hora	0,00525
10	ACGDG002___DGS	DGE-2 falha na partida	0,00493

Fonte: Código computacional CAFTA [82].

Tabela 30 – Eventos básicos de falhas do sistema elétrico do projeto B com maiores contribuições para o CDF.

Posição	Eventos básicos de falhas do sistema elétrico	Descrição	B
			F-V
1	AC_LOOP2	Perda centrada na subestação primária/entrada	0,02027
2	OPERACPN1E001FC	Operador falha ao alinhar a fonte AAC-1 ao CBT-1F-001	0,01054
3	AC_LOOP4	Perdas relacionadas ao clima	0,00870
4	AC_LOOP1	Perdas centradas na planta	0,00803
5	ACGDG001___DGA	DGE-1 falha após 1ª hora	0,00778
6	OPERACPN1E002FC	Operador falha ao alinhar a fonte AAC-2 ao CBT-2F-002	0,00752
7	ACGDG001___DGS	DGE-1 falha na partida	0,00677
8	ACGDG002___DGA	DGE-2 falha após 1ª hora	0,00548
9	ACGDG04A___DGA	Fonte AAC-1 falha após 1ª hora	0,00485
10	ACGDG002___DGS	DGE-2 falha na partida	0,00475

Fonte: Código computacional CAFTA [82].

A Tabela 31 e a Tabela 32 mostram os dez eventos básicos de falhas do sistema elétrico que possuem as maiores contribuições para o CDF, considerando as alternativas de projeto C e D, respectivamente. Evidencia-se a importância da indisponibilidade para testes das baterias no caso do CDF calculado para o projeto C e a contribuição da falha no fechamento de disjuntores no processo de religamento das cargas de segurança, após a perda do sistema elétrico externo, no caso do projeto D.

Tabela 31 – Eventos básicos de falhas do sistema elétrico do projeto C com maiores contribuições para o CDF.

Posição	Eventos básicos de falhas do sistema elétrico	Descrição	C
			F-V
1	AC_LOOP2	Perda centrada na subestação primária/entrada	0,00837
2	AC_LOOP3	Perda relacionada à rede (LT)	0,00544
3	DCRNC141R141IVF	Falha na operação do retificador RNC-1F-141	0,00445
4	AC_LOOP4	Perdas relacionadas ao clima	0,00350
5	AC_LOOP1	Perdas centradas na planta	0,00319
6	OPERACPN1E001FC	Operador falha ao alinhar a fonte AAC-1 ao CBT-1F-001	0,00293
7	DCRNC241R241IVF	Falha na operação do retificador RNC-2F-241	0,00280
8	SPP_002CCF__CU1	CCF trem A e B do CPU em operação	0,00245
9	DCP_BAT141__TM	Indisponibilidade por teste na bateria BAT-1F-141	0,00231
10	ACCBT0015Q1_CBC	Falha no religamento do disjuntor 5Q1 do CBT-1F-001	0,00196

Fonte: Código computacional CAFTA [82].

Tabela 32 – Eventos básicos de falhas do sistema elétrico do projeto D com maiores contribuições para o CDF.

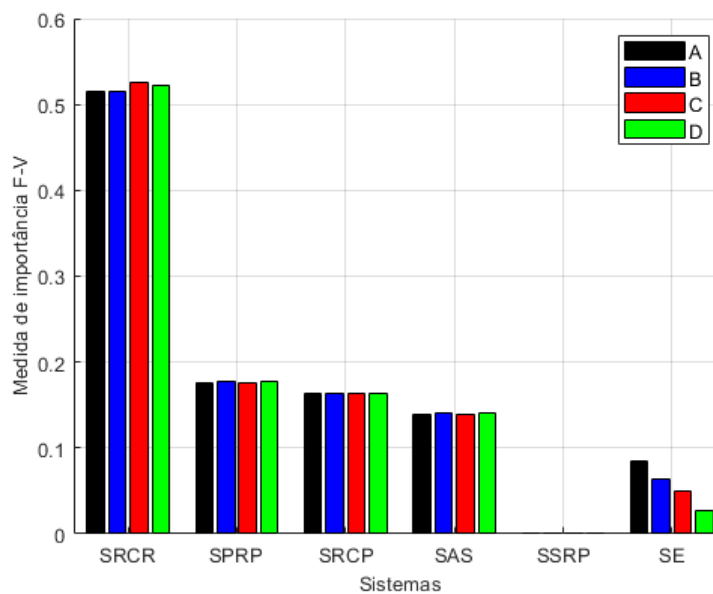
Posição	Eventos básicos de falhas do sistema elétrico	Descrição	D
			F-V
1	AC_LOOP2	Perda centrada na subestação primária/entrada	0,00612
2	AC_LOOP3	Perda relacionada à rede (LT)	0,00395
3	AC_LOOP4	Perdas relacionadas ao clima	0,00251
4	SPP_002CCF__CU1	CCF trem A e B do CPU em operação	0,00249
5	AC_LOOP1	Perdas centradas na planta	0,00229
6	OPERACPN1E001FC	Operador falha ao alinhar a fonte AAC-1 ao CBT-1F-001	0,00220
7	ACCBT0015Q1_CBC	Falha no religamento do disjuntor 5Q1 do CBT-1F-001	0,00186
8	ACCBT0016Q1_CBC	Falha no religamento do disjuntor 6Q1 do CBT-1F-001	0,00140
9	OPERACPN1E002FC	Operador falha ao alinhar a fonte AAC-2 ao CBT-2F-002	0,00139
10	ACCBT0026Q1_CBC	Falha no religamento do disjuntor 6Q1 do CBT-2F-002	0,00112

Fonte: Código computacional CAFTA [82].

A Figura 30 mostra a medida de importância de *Fussel-Vesely* dos sistemas (linha de frente e suporte) da instalação para cada alternativa de projeto do sistema elétrico avaliada. Na Figura 31, o sistema elétrico é detalhado e também é exibida a medida de importância de *Fussel-Vesely* para o risco da instalação considerando cada alternativa de projeto do sistema elétrico. As figuras evidenciam que a contribuição do sistema elétrico para o risco da instalação é menor na alternativa de projeto D do sistema elétrico. Destaca-se, ainda, a baixa contribuição associada aos sistemas elétricos CA e CC. A utilização de um DGE e de um

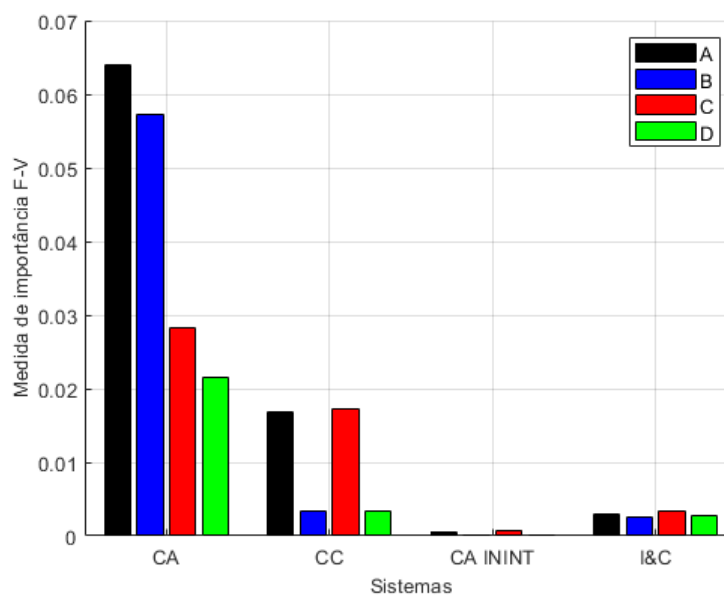
conjunto retificador/bateria adicional por barramento de segurança foi determinante para a redução da contribuição da falha do sistema elétrico para o risco global da instalação.

Figura 30 – Importância dos sistemas para o risco associado a cada alternativa de projeto do sistema elétrico.



Fonte: Autor.

Figura 31 – Importância dos sistemas elétricos para o risco associado a cada alternativa de projeto.



Fonte: Autor.

5.7 Análise de sensibilidade

5.7.1 Manutenção/teste simultâneo de equipamentos do sistema elétrico

A primeira análise de sensibilidade consistiu em remover do modelo as premissas específicas do sistema elétrico estabelecidas nos itens 9 e 12 de 4.2.4.2, as quais restringem a manutenção/teste em mais de um diesel gerador ou bateria em simultâneo. Na Tabela 33, onde são apresentados os resultados do risco total para a instalação, verifica-se que a possibilidade de ocorrer manutenção/teste de um diesel gerador ou bateria em simultâneo teve pouco impacto para o risco, destacando os projetos A e C como os mais afetados. Estes projetos, especificamente, possuem apenas um grupo retificador/bateria por trem de segurança.

Na Tabela 34 é destacado o impacto da manutenção/teste para o evento de *Station Blackout*. Verificou-se um aumento do risco da instalação devido ao evento de *Station Blackout* para os projetos A e B do sistema elétrico no caso em que é permitido efetuar manutenção/teste de um diesel gerador ou bateria em simultâneo. Estes projetos possuem apenas um DGE por trem de segurança.

Tabela 33 – Resultado do risco para a instalação considerando manutenção/teste simultâneo de equipamentos do sistema elétrico para as alternativas de projeto analisadas.

Projeto	CDF _{TOTAL} (/ano) (original)	CDF _{TOTAL} (/ano)	Δ CDF _{TOTAL} (%)
A	1,29E-5	1,30E-5	+0,31
B	1,28E-5	1,28E-5	+0,06
C	1,26E-5	1,27E-5	+0,34
D	1,25E-5	1,25E-5	+0,00

Fonte: Autor.

Tabela 34 – Resultado do risco para a instalação associado ao *Station Blackout* considerando manutenção/teste simultâneo de equipamentos do sistema elétrico para as alternativas de projeto analisadas.

Projeto	CDF _{SBO} (/ano) (original)	CDF _{SBO} (/ano)	Δ CDF _{SBO} (%)
A	7,94E-8	8,27E-8	+4,09
B	7,26E-8	7,58E-8	+4,48
C	9,27E-10	9,27E-10	0,00
D	9,27E-10	9,27E-10	0,00

Fonte: Autor.

Os resultados mostram que o projeto D apresenta uma arquitetura do sistema elétrico bastante robusta, permitindo que manutenções/testes que eventualmente diminuam a

disponibilidade das fontes de energia de emergência não tenham impacto significativo para o risco global associado à instalação.

5.7.2 Taxa de falha dos DGEs

Nesta análise de sensibilidade, variaram-se as taxas de falha associadas aos eventos básicos dos DGEs, incluindo os eventos de indisponibilidade devido a testes e manutenções. A Tabela 35 mostra os resultados da análise considerando uma taxa de falha dez vezes maior do que a originalmente considerada em 5.5 e, também, uma taxa de falha dez vezes menor do que a proposta original. Nas alternativas de projeto A e B do sistema elétrico, o impacto destas variações na taxa de falha dos DGEs para o risco da instalação foi relevante, alcançando, inclusive, valores superiores a 70%, quando as taxas de falha dos DGEs são multiplicadas por um fator igual a 10.

Tabela 35 – Resultado do risco para a instalação considerando variações na taxa de falha dos DGEs para as alternativas de projeto analisadas.

Projeto	CDF _{TOTAL} (/ano)	$\lambda_{DGE} \times 10$		$\lambda_{DGE} \div 10$	
	(original)	CDF _{TOTAL} (/ano)	Δ CDF _{TOTAL} (%)	CDF _{TOTAL} (/ano)	Δ CDF _{TOTAL} (%)
A	1,29E-5	2,22E-5	+71,87	1,26E-5	-2,61
B	1,28E-5	2,19E-5	+71,34	1,24E-5	-2,52
C	1,26E-5	1,75E-5	+38,16	1,26E-5	-0,07
D	1,25E-5	1,71E-5	+37,56	1,25E-5	-0,07

Fonte: Autor.

Na Tabela 36 são mostrados os resultados do risco associado à instalação em cenários de *Station Blackout*. Pode-se verificar que há um impacto considerável no risco para os projetos C e D do sistema elétrico, quando a taxa de falha dos DGEs é multiplicada pelo fator 10. Entretanto, o risco associado aos eventos de *Station Blackout* para os projetos C e D do sistema elétrico ainda são menores que aqueles dos projetos A e B.

Tabela 36 – Resultado do risco para a instalação associado ao *Station Blackout* considerando variações na taxa de falha dos DGEs para as alternativas de projeto analisadas.

Projeto	CDF _{SBO} (/ano) (original)	$\lambda_{DGE} \times 10$		$\lambda_{DGE} \div 10$	
		CDF _{SBO} (/ano)	Fator de Aumento CDF _{SBO}	CDF _{SBO} (/ano)	Fator de Redução CDF _{SBO}
A	7,94E-8	6,68E-6	84,04	6,13E-10	129,57
B	7,26E-8	6,58E-6	90,60	5,69E-10	127,52
C	9,27E-10	2,65E-6	2854,58	0,00E+0*	-
D	9,27E-10	2,58E-6	2786,20	0,00E+0*	-

Fonte: Autor.

*O valor do risco associado ao evento de *Station Blackout* (CDF_{SBO}) foi menor que 1E-11/ano (frequência de truncamento dos cortes mínimos).

5.7.3 Taxa de falha do sistema elétrico externo

Para esta análise, as taxas de falha atribuídas aos eventos de perda do sistema elétrico externo são, também, multiplicadas e divididas por um fator igual a 10 em relação ao valor originalmente usado na análise. Na Tabela 37 são mostrados os resultados de aumento e diminuição do risco associado à instalação considerando as alternativas de projeto do sistema elétrico. Evidencia-se que há um maior impacto do fator de aumento/redução dos eventos de perda do sistema elétrico externo para os projetos A e B do sistema elétrico da instalação.

Tabela 37 – Resultado do risco para a instalação considerando variações na taxa de falha do sistema elétrico externo para as alternativas de projeto analisadas.

Projeto	CDF _{TOTAL} (/ano) (original)	$\lambda_{LOOP} \times 10$		$\lambda_{LOOP} \div 10$	
		CDF _{TOTAL} (/ano)	Δ CDF _{TOTAL} (%)	CDF _{TOTAL} (/ano)	Δ CDF _{TOTAL} (%)
A	1,29E-5	1,86E-5	+44,14	1,24E-5	-4,01
B	1,28E-5	1,77E-5	+38,77	1,23E-5	-3,53
C	1,26E-5	1,53E-5	+21,21	1,24E-5	-1,93
D	1,25E-5	1,44E-5	+15,64	1,23E-5	-1,40

Fonte: Autor.

Na Tabela 38 são mostrados os resultados do risco para a instalação associados aos cenários de *Station Blackout*. Verifica-se que uma variação na taxa de falha do sistema elétrico externo produz um maior impacto no risco associado ao cenário de *Station Blackout* para as alternativas de projeto C e D do sistema elétrico da instalação. Entretanto, o risco associado ao cenário de *Station Blackout* para os projetos C e D ainda é menor do que o risco associado aos projetos A e B.

Tabela 38 – Resultado do risco para a instalação associado ao *Station Blackout* considerando variações na taxa de falha do sistema elétrico externo para as alternativas de projeto analisadas.

Projeto	CDF _{SBO} (/ano) (original)	$\lambda_{LOOP} \times 10$		$\lambda_{LOOP} \div 10$	
		CDF _{SBO} (/ano)	Fator de Aumento CDF _{SBO}	CDF _{SBO} (/ano)	Fator de Redução CDF _{SBO}
A	7,94E-8	1,13E-6	14,24	2,74E-9	28,98
B	7,26E-8	1,02E-6	14,02	2,70E-9	26,91
C	9,27E-10	4,81E-8	51,86	0,00E+0*	-
D	9,27E-10	2,59E-8	27,94	0,00E+0*	-

Fonte: Autor.

*O valor do risco associado ao evento de *Station Blackout* (CDF_{SBO}) foi menor que 1E-11/ano (frequência de truncamento dos cortes mínimos).

Com base nos resultados da análise de sensibilidade, pode-se inferir que a alternativa de projeto D para o sistema elétrico apresentou medidas de risco menores para a instalação do que as demais alternativas A, B e C. Pode-se dizer que é uma alternativa de projeto para o sistema elétrico que se mostra mais robusta em relação às incertezas nos valores das taxas de falha das principais fontes de energia do sistema elétrico.

6 CONCLUSÕES

Esse trabalho apresentou uma metodologia de aplicação da APS nível 1 como ferramenta de decisão para projetos e licenciamento de sistemas elétricos de instalações nucleares. Foram enfatizadas questões relativas à adequabilidade da atual base normativa de usinas nucleares de potência para instalações nucleares não convencionais, em especial, àquelas com aplicações navais. Foram destacadas, ainda, as principais diferenças operacionais e funcionais entre estes tipos de instalação, assim como, a dependência do sistema elétrico externo por parte das instalações nucleares não convencionais com aplicações navais, para os diferentes modos de operação.

A metodologia de avaliação probabilística de projetos, baseada na Frequência de Dano ao Núcleo (CDF) como métrica de risco, mostrou ser uma importante ferramenta para a seleção da arquitetura e o licenciamento dos projetos. No trabalho foi destacada a importância de uma análise integrada que considere todos os sistemas de uma instalação e não apenas àquele sob avaliação. Através de uma avaliação integrada foi possível verificar o impacto das diferentes arquiteturas do sistema elétrico para o risco de acidente na instalação nuclear, diferentemente de uma análise isolada do desempenho do sistema, em que é possível apenas aferir a confiabilidade e/ou disponibilidade do sistema elétrico para a instalação. O evento de *Station Blackout* foi enfatizado por ser um evento crítico para a instalação, impondo restrições operacionais que dependem, inclusive, de intervenções do operador e, conseqüentemente, podem desencadear em um aumento significativo do risco para a instalação causado por falhas humanas.

Finalmente, os resultados encontrados no estudo de caso da aplicação da metodologia se mostraram de grande valia para a tomada de decisão em projetos e para a demonstração de segurança da instalação em processos de licenciamento. Considerando as especificidades funcionais e operacionais de uma instalação nuclear não convencional com aplicações navais, o descumprimento da exigência de uma segunda LT, prevista na base normativa convencional, pode ser justificado pelo aumento do nível de segurança obtido em uma avaliação probabilística, demonstrado pela incorporação de um diesel gerador de emergência adicional por barramento de segurança no projeto dos sistemas elétricos. Em conformidade

com os resultados, em função das particularidades funcionais, recomenda-se a revisão da base normativa adotada pelas instalações nucleares não convencionais com aplicações navais.

7 TRABALHOS FUTUROS

Para trabalhos futuros sugere-se um estudo de caso com aplicação da metodologia que considere os tempos de recuperação dos sistemas, considerando o tempo ao qual o núcleo pode ficar sem efetivo resfriamento. Sendo assim, será necessário estimar o calor residual do combustível ao longo do tempo. Os tempos de reação proporcionarão uma análise mais detalhada e menos conservadora da que foi realizada neste trabalho. Outro aspecto importante que deve ser estudado em detalhes são os erros humanos em eventos críticos, tais como os eventos de *Station Blackout*, que podem aumentar consideravelmente o risco para a instalação.

A continuação deste trabalho poderá, ainda, ser realizada através da adaptação da metodologia para uma análise probabilística de segurança que avalie os projetos de diferentes sistemas de uma instalação, aplicando-se os três níveis da APS. Sugerem-se, como objeto de estudo, os estaleiros que prestam apoio aos submarinos nucleares, já que estes possuem gerência sobre os reatores apenas em modo de desligamento, podendo ser considerada inclusive uma instalação sem reator quando este estiver em potência (gerência do submarino).

REFERÊNCIAS BIBLIOGRÁFICAS

- 1 Gjorgiev, B.; Volkanovski, A.; Kancev, D.; Cepin, M. Alternative off-site power supply improves nuclear power plant safety. *Annals of Nuclear Energy* **71**, p. 304-312, 2014.
- 2 Khatua, S.; Mukherjee, V. Application of integrated microgrid for strengthening the station blackout power supply in nuclear plant. *Progress in Nuclear Energy* **118**, 2020.
- 3 U.S. NUCLEAR REGULATORY COMMISSION. *Domestic Licensing of Production and Utilization Facilities*. Washington: U.S.NRC, 2017. (10CFR50).
- 4 INTERNATIONAL ATOMIC ENERGY AGENCY. *Design of Electrical Power Systems for Nuclear Power Plants*. Vienna: AIEA, 2016. (Specific Safety Guide No. SSG-34).
- 5 INTERNATIONAL ATOMIC ENERGY AGENCY. *Safety of Nuclear Power Plants: Design*. Vienna: AIEA, 2016. (Specific Safety Requirements No. SSR-2/1).
- 6 COMISSÃO NACIONAL DE ENERGIA NUCLEAR. *Licenciamento de instalações nucleares*. Rio de Janeiro: CNEN, 2002. (Norma CNEN-NE-1.04 / Resolução CNEN 15/02).
- 7 U.S. NUCLEAR REGULATORY COMMISSION. *Reactor Safety Study: an assessment of accident risks in US commercial nuclear power plants*. Idaho: Idaho National Laboratory, 1975. (WASH-1400 (NUREG-75/014)).
- 8 ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT / NUCLEAR ENERGY AGENCY. *Use and Development of Probabilistic Safety Assessment - an overview of the situation at the end of 2010*. OECD Nuclear Energy Agency, 2012. (NEA/CSNI/R(2012)11).
- 9 U.S. NUCLEAR REGULATORY COMMISSION. *Probabilistic Safety Analysis Procedures Guide*. New York: Brookhaven National Laboratory, 1984. (NUREG/CR-2815).

- 10 U.S. NUCLEAR REGULATORY COMMISSION. *PRA Procedures Guide: a guide to the performance of probabilistic risk assessments for nuclear power plants*. Washington: U.S. NRC, 1983. (NUREG/CR-2300).
- 11 NNSA. National Nuclear Security Administration. Disponível em: <<https://www.energy.gov/nnsa/about-nnsa>>. Acesso em: 02 mar. 2020.
- 12 ONS. Operador Nacional do Sistema Elétrico. Disponível em: <<http://www.ons.org.br/Paginas/resultados-da-operacao/qualidade-do-suprimento-paineis.aspx>>. Acesso em: 18 fev. 2020.
- 13 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. *Recommended Practice for Nuclear Power Generating Station Preferred Power Supply Reliability*. New York: IEEE, 2017. (IEEE std 1792).
- 14 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. *Standard for Preferred Power Supply (PPS) for Nuclear Power Generating Stations (NPGS)*. New York: IEEE, 2012. (IEEE std 765).
- 15 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. *Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations*. New York: IEEE, 2020. (IEEE std 308).
- 16 U.S. NUCLEAR REGULATORY COMMISSION. *Reevaluation of Station Blackout Risk at Nuclear Power Plants*. Washington: U.S.NRC, 2005. (NUREG/CR-6890).
- 17 U.S.NRC. U.S. Nuclear Regulatory Commission. *Reactor Operational Experience Results and Databases*. Disponível em: <https://nrcoe.inl.gov/>. Acesso em: 05 jun. 2021.
- 18 Mazzoni S. O. *Electrical Systems for Nuclear Plants*. New Jersey: IEEE Press, 2009, p.26-41.
- 19 U.S. NUCLEAR REGULATORY COMMISSION. *Loss of all alternating current power*. Washington: U.S.NRC, 2021. (10CFR50.63).
- 20 U.S. NUCLEAR REGULATORY COMMISSION. *Application and Testing of Safety-Related Diesel Generators in Nuclear Power Plants*. Washington: U.S.NRC, 2007. (Regulatory Guide 1.9).

- 21 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. *Standard for Criteria for Diesel Generator Units Applied as Standby Power Supplies for Nuclear Power Generating Stations*. New York: IEEE, 2017. (IEEE std 387).
- 22 U.S. NUCLEAR REGULATORY COMMISSION. *Criteria for Power Systems for Nuclear Power Plants*. Washington: U.S.NRC, 2004. (Regulatory Guide 1.32).
- 23 U.S. NUCLEAR REGULATORY COMMISSION. *Application of the Single-Failure Criterion to Safety Systems*. Washington: U.S.NRC, 2003. (Regulatory Guide 1.53).
- 24 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. *Standard for Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems*. New York: IEEE, 2014. (IEEE std 379).
- 25 U.S. NUCLEAR REGULATORY COMMISSION. *Physical Independence of Electric Systems*. Washington: U.S.NRC, 2005. (Regulatory Guide 1.75).
- 26 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. *Standard Criteria for Independence of Class 1E Equipment and Circuits*. New York: IEEE, 2018. (IEEE std 384).
- 27 U.S. NUCLEAR REGULATORY COMMISSION. *Periodic Testing of Electric Power and Protection Systems*. Washington: U.S.NRC, 1995. (Regulatory Guide 1.118).
- 28 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. *Standard for Criteria Surveillance Testing of Nuclear Power Generating Station Safety Systems*. New York: IEEE, 2012. (IEEE std 338).
- 29 U.S. NUCLEAR REGULATORY COMMISSION. *Criteria for Safety Systems*. Washington: U.S.NRC, 1996. (Regulatory Guide 1.153).
- 30 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. *Standard Criteria for Safety Systems for Nuclear Power Generating Station*. New York: IEEE, 2018. (IEEE std 603).
- 31 U.S. NUCLEAR REGULATORY COMMISSION. *Station Blackout*. Washington: U.S.NRC, 1988. (Regulatory Guide 1.155).

- 32 INTERNATIONAL STANDARD. *Nuclear facilities – Electrical equipment important to safety - Qualification*. New York: IEEE, 2016. (IEC/IEEE 60780-323).
- 33 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. *Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Systems and Other Nuclear Facilities*. New York: IEEE, 2016. (IEEE std 352).
- 34 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. *Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Power Generating Stations*. New York: IEEE, 2012. (IEEE std 577).
- 35 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. *Standard for Qualifying Continuous Duty Class 1E Motors for Nuclear Power Generating Station*. New York: IEEE, 2006. (IEEE std 334).
- 36 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. *Standard for Qualifying Electric Cables and Splices for Nuclear Facilities*. New York: IEEE, 2015. (IEEE std 383).
- 37 U.S. DEPARTMENT OF ENERGY. *Facility Safety*. Washington: U.S.DOE, 2019. (DOE O 420.1C chg3).
- 38 U.S. DEPARTMENT OF ENERGY. *Nuclear Reactor Safety Design Criteria*. Washington: U.S.DOE, 1993. (DOE O 5480.30).
- 39 U.S. DEPARTMENT OF ENERGY. *General Design Criteria*. Washington: U.S.DOE, 1989. (DOE O 6430.1A Div 8-16).
- 40 Garrick, B. J.; Christie, R. F. Probabilistic Risk Assessments Practices in the USA for Nuclear Power Plants. *Safety Science*, V. 40, p. 177-201, 2002.
- 41 Frankel E. *Systems reliability and risk analysis*. 2nd ed. Boston: Kluwer Academic Publishers, 2002.
- 42 Green A.; Bourne A. *Reliability technology*. London: Willey, 1972.
- 43 U.S. NUCLEAR REGULATORY COMMISSION. *Individual Plant Examination for Severe Accident Vulnerabilities - 10CFR50.54 (f)*. Washington: U.S.NRC 1988.

(Generic Letter N° 88-20).

- 44 U.S. NUCLEAR REGULATORY COMMISSION. *SECY-89-102 - Implementation of the safety goals*. Washington: U.S.NRC, 1990.
- 45 Keller W.; Modarres M. A historical overview of probabilistic risk assessment development and its use in the nuclear power industry: a tribute to the late Professor Norman Carl Rasmussen. *Reliability Engineering and System Safety*, V. 89, p 271-285, 2005.
- 46 U.S. NUCLEAR REGULATORY COMMISSION. *Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants*. Washington: U.S.NRC 1990. (NUREG-1150).
- 47 Wall, I. B.; Haugh, J. J.; Worlege, D. H. Recent Applications of PSA for Managing Nuclear Power Plant Safety. *Progress in Nuclear Energy*, V. 39, N° 3-4, p 367-425, 2001.
- 48 U.S. NUCLEAR REGULATORY COMMISSION. *Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities – Final Policy Statement*. Washington: U.S.NRC, 1995. (60FR-42622).
- 49 U.S. NUCLEAR REGULATORY COMMISSION. *An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis*. Washington: U.S.NRC, 1998. (Regulatory Guide 1.174).
- 50 U.S. NUCLEAR REGULATORY COMMISSION. *An approach for determining the technical adequacy of probabilistic risk assessment results for risk-informed activities*. Washington: U.S.NRC, 2004. (Regulatory Guide 1.200).
- 51 U.S. NUCLEAR REGULATORY COMMISSION. *Handbook of Parameter Estimation for Probabilistic Risk Assessment*. Washington: U.S.NRC, 2003. (NUREG/CR-6823).
- 52 INTERNATIONAL ATOMIC ENERGY AGENCY. *Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants*. Vienna: IAEA, 2010. (Specific Safety Guide No. SSG-3).
- 53 INTERNATIONAL ATOMIC ENERGY AGENCY. *Development and Application*

- of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants*. Vienna: IAEA, 2010. (Specific Safety Guide No. SSG-4).
- 54 INTERNATIONAL ATOMIC ENERGY AGENCY. *Fundamental Safety Principles*. Vienna: IAEA, 2006. (Safety Fundamentals No. SF-1).
- 55 Fragola J. R. Reliability and risk analysis data base development: an historical perspective. *Reliability Engineering and System Safety*, V. 51, p 125-136, 1996.
- 56 TITAN HANBOOK. *Procedure and data for estimating reliability and maintainability*. Denver: Martin Co, 1959. (Report No. M-N-P-59-21).
- 57 U.S. DEPARTMENT OF DEFENCE. *Reliability Prediction of Electronic Equipment*. Washington, 1965. (MIL-HDBK-217A).
- 58 GOVERNMENT INDUSTRY DATA EXCHANGE PROGRAM. *Summaries of Failure Rate Data*, California: GIDEP, 1960.
- 59 Cottrell, D.F. *RADC Nonelectronic Reliability and Maintainability Notebook*. New York, 1969. (RADC-TR-69-458).
- 60 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. *Guide to the collection and Presentation of Electrical, Electronic, and Sensing Reliability Data for Nuclear Power Generating Station*. New York: IEEE, 1984. (IEEE std 500).
- 61 INTERNATIONAL ATOMIC ENERGY AGENCY. *Survey of Ranges of Component Reliability Data for Use in Probabilistic Safety Assessment*. Vienna: IAEA, 1989. (IAEA-TECDOC-508).
- 62 ELECTRICAL POWER RESEARCH INSTITUTE. *Diesel-Generator Reliability at Nuclear Power Plants: Data and Preliminary Analysis*. California: EPRI, 1982. (EPRI-NP-2433).
- 63 U.S. NUCLEAR REGULATORY COMMISSION. *Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants*. Washington: U.S.NRC, 2007. (NUREG/CR-6928).
- 64 INTERNATIONAL ATOMIC ENERGY AGENCY. *Generic Component Reliability Data for Research Reactor PSA*. Vienna: IAEA, 1997. (IAEA-TECDOC-930).

- 65 INTERNATIONAL ATOMIC ENERGY AGENCY. *Reliability for Research Reactor Probabilistic Safety Assessment*. Vienna: IAEA, 2020. (IAEA-TECDOC-1922).
- 66 Modarres M.; Kim I. S. *Encyclopedia of Nuclear Energy*. V. 2, Section 4. Elsevier, 2021, p. 207-217.
- 67 Maturana, M. C.; Matins, M. R.; Melo, P. F. F. F. Application of a quantitative human performance model to the operational procedure design of a fuel storage pool cooling system. *Reliability Engineering and System Safety* 216, p. 107989, 2021.
- 68 U.S. NUCLEAR REGULATORY COMMISSION. *Handbook of Human Reliability Analysis with Emphasis on Nuclear Plant Applications*. Washington: U.S.NRC, 1983. (NUREG/CR-1278).
- 69 U.S. NUCLEAR REGULATORY COMMISSION. *Shutdown and Low-Power Operation at Commercial Nuclear Power Plants in the United States*. Washington: U.S.NRC, 1993. (NUREG-1449).
- 70 U.S. NUCLEAR REGULATORY COMMISSION. *An Analysis of Operational Experience during Low Power and Shutdown and a Plan for Addressing Human Reliability Assessment Issues*. Washington: U.S.NRC, 1994. (NUREG/CR-6093).
- 71 NUCLEAR SAFETY ANALYSIS CENTER. *Zion Nuclear Plant Residual Heat Removal PRA*. California: EPRI/NSAC, 1985. (NSAC-84).
- 72 U.S. NUCLEAR REGULATORY COMMISSION. *Improved Reliability of Residual Heat Removal Capability in PWRs as Related to Resolution of Generic Issue 99*. Washington: U.S.NRC, 1988. (NUREG/CR-1150).
- 73 NUCLEAR SAFETY ANALYSIS CENTER. *Brunswick Decay Heat Removal Probabilistic Safety Syudy*. California: EPRI/NSAC, 1985. (NSAC-83).
- 74 BROCKHAVEN NATIONAL LABORATORY. *PWR Low Power and Shutdown Accident Frequencies Program – Phase 1: Coarse Screening Analysis*. New York: BNL, 1991.
- 75 BROCKHAVEN NATIONAL LABORATORY. *PWR Low Power and Shutdown*

Accident Frequencies Program – Phase 2: Internal Events. New York: BNL, 1992.

- 76 U.S. NUCLEAR REGULATORY COMMISSION. *Issues and Recommendations for Advancement of PRA Technology in Risk-Informed Decision Making*. Washington: U.S.NRC, 2003. (NUREG/CR-6813).
- 77 Mizuno, Y.; Ninokata, H.; Finnican, D.J. Risk-informed design of IRIS using level-1 probabilistic risk assessment from its conceptual design phase. *Reliability Engineering and System Safety* **87**, p. 201-209, 2005.
- 78 Deng, J.; Xu, Y.; Qiu, Z.; Wu, L.; Wang, X. Research on level 1 PSA and risk-informed design for ACP100. *Annals of Nuclear Energy* **144**, 2020.
- 79 Oh, J. Y.; Hwang, S. W. Risk-informed approach for design optimization during low power and shutdown operation. *Annals of Nuclear Energy* **130**, p. 293-300, 2019.
- 80 Ahmed, I.; Zio, E.; Heo, G. Risk-informed approach to the safety improvement of the reactor protection system of the AGN-201K research reactor. *Nuclear Engineering and Technology* **52**, p. 764-775, 2020.
- 81 Kowal, K.; Torabi, M. Failure mode and reliability study for Electrical Facility of the High Temperature Engineering Test Reactor. *Reliability Engineering and System Safety* **210**, 2021.
- 82 CAFTA, Version 6.0b: Fault Tree Analysis System Software Electric Power Research Institute (EPRI), 2014.
- 83 MARTINS, M. R. *Considerações sobre Análise de Confiabilidade e Risco*. 2013. 900 p. Tese de Livre Docência – Escola Politécnica da Universidade de São Paulo, POLI-USP.
- 84 U.S. NUCLEAR REGULATORY COMMISSION. *Fault Tree Handbook*. Washington: U.S.NRC, 1981. (NUREG-0492).
- 85 Kumamoto H., Henley E. J. *Probabilistic Risk Assessment and Management for Engineers and Scientists*. 2nd Ed. New York: IEEE Press, 1996, p.166-165.
- 86 U.S. NUCLEAR REGULATORY COMMISSION. *Common-Cause Failure Database and Analysis System: Event Data Collection Classification, and Coding*.

Washington: U.S.NRC, 2007. (NUREG/CR-6268).

- 87 U.S. NUCLEAR REGULATORY COMMISSION. *Guidelines on Modeling Common-Cause Failure in Probabilistic Risk Assessment*. Washington: U.S.NRC, 1998. (NUREG/CR-5485).
- 88 Modarres M. *Reliability Engineering and Risk Analysis*. 3th Ed. New York: CRC Press, 2017, p.440.
- 89 ELECTRIC POWER RESEARCH INSTITUTE. **CAFTA Fault Tre Analysis System - Software Manual**. Version 6.0 Demo. California: EPRI, 2013.
- 90 ANS American National Society. Disponível em: <https://www.ans.org/news/article-1635/they-harnessed-the-atom-the-first-navy-prototype-nuclear-plant/>. Acesso em: 10 ago. 2021.
- 91 U.S. NUCLEAR REGULATORY COMMISSION. *US-APWR Design Control Document and Environmental Report*. Chapter 19. Disponível em: <https://www.nrc.gov/reactors/new-reactors/design-cert/apwr/dcd.html>. Acesso em: 27 jan. 2022.
- 92 ELECTRICAL POWER RESEARCH INSTITUTE. *PWR Spent Fuel Pool Risk Assessment Integration Framework and Pilot Plant Application*. California: EPRI, 2014.

ANEXOS

ANEXO A

Tabela 39 – Taxa de falha dos componentes.

Equipamento	Modo de Falha	D ou H	Distribuição	Média	Variância
Barramento elétrico	Falha na operação	H	Gama	2,23E-7	3,38E-14
Bateria	Falha na operação	H	Gama	1,18E-6	8,10E-12
Cartão lógico (CLP)	Falha na operação	H	Gama	1,07E-6	6,08E-12
Chave seletora	Falha ao abrir/fechar	D	Beta	6,61E-6	4,79E-11
CPU	Falha na operação	H	Gama	1,50E-5	3,61E-10
Diesel gerador de emergência	Falha na partida	D	Beta	2,21E-2	7,86E-5
	Falha durante a primeira hora de operação	H	Gama	2,90E-3	5,90E-6
	Falha depois da primeira hora de operação	H	Gama	1,09E-3	1,28E-6
	Falha ao abrir	D	Beta	1,35E-3	4,10E-6
Disjuntor	Falha ao fechar	D	Beta	1,10E-3	1,95E-6
	Sinais espúrios	H	Gama	2,88E-7	5,28E-14
	Falha de conexão	H	Gama	1,38E-7	5,55E-14
Elemento de fluxo	Falha de conexão	H	Gama	1,38E-7	5,55E-14
Filtro	Falha de conexão	H	Gama	1,22E-7	4,76E-14
Inversor	Falha na operação	H	Gama	1,11E-5	9,79E-11
Motor elétrico	Falha na operação	H	Gama	5,96E-6	4,05E-11
Motor da bomba (principal)	Falha na operação	H	Gama	6,27E-6	1,82E-11
	Falha na partida	D	Beta	1,66E-3	1,51E-6
Motor da bomba (reserva)	Falha na partida	D	Beta	1,56E-3	1,33E-6
	Falha durante a primeira hora de operação	H	Gama	9,69E-6	4,31E-11
	Falha depois da primeira hora de operação	H	Gama	7,05E-6	2,80E-11
Relé	Falha na operação	D	Beta	4,13E-4	3,40E-7
Retificador	Falha na operação	H	Gama	2,43E-6	5,32E-12
Sensor de subtensão	Falha na operação	D	Beta	4,13E-4	3,40E-7

Equipamento	Modo de Falha	D ou H	Distribuição	Média	Variância
Sensor/Transmissor (fluxo)	Falha na operação / alto ou baixo	H	Gama	1,38E-7	5,55E-14
Tanque pressurizado	Vazamentos	H	Gama	8,83E-8	1,98E-15
Transformador	Falha na operação	H	Gama	1,09E-6	1,92E-12
Trocador de calor	Falha de conexão	H	Gama	3,60E-6	8,01E-11
Válvula de alívio de segurança	Falha na operação	H	Gama	2,12E-7	1,50E-13
Válvula de retenção	Falha ao abrir	D	Beta	6,07E-5	5,63E-10
Válvula de retenção (reserva)	Falha ao abrir	H	Gama	5,87E-8	1,39E-16
Válvula manual	Falha de conexão	H	Gama	1,75E-8	4,41E-16
	Falha na operação	H	Gama	1,75E-8	4,41E-16
	Falha ao fechar	D	Beta	1,42E-4	1,41E-9
Válvula operada por motor	Falha na operação	H	Gama	1,40E-7	6,86E-15
	Falha ao abrir/fechar	D	Beta	3,89E-3	6,70E-7
Válvula solenóide	Falha na operação	H	Gama	1,21E-7	3,75E-14
	Falha ao abrir	D	Beta	4,23E-4	2,23E-7

Fonte: Adaptado <https://nrcoe.inl.gov/> [17].

Sendo:

D = demanda; e

H = hora.

Tabela 40 – Taxa de falha do sistema elétrico externo.

Categoria do Evento	Distribuição	Média/ano	Variância/ano
Centrado na planta	Gama	7,07E-3	6,25E-6
Centrado na subestação primária/entrada	Gama	1,64E-2	1,45E-5
Relacionado à rede	Gama	1,11E-2	9,77E-6
Relacionado ao clima	Gama	7,58E-3	5,63E-5

Fonte: Adaptado <https://nrcoe.inl.gov/> [17].

Tabela 41 – Taxa de falha de causa comum dos componentes.

Descrição da Falha de Causa Comum	Taxa de falha do CCF	Taxa de falha individual do componente	β (beta)	γ (gama)	δ (delta)
CCF 2 de 2 CLP - operação	2,97E-8	1,07E-6	2,78E-2	-	-
CCF 2 de 4 CLP - operação	4,83E-9				
CCF 3 de 4 CLP - operação	2,94E-9		2,67E-2	4,88E-1	3,61E-1
CCF 4 de 4 CLP - operação	5,03E-9				

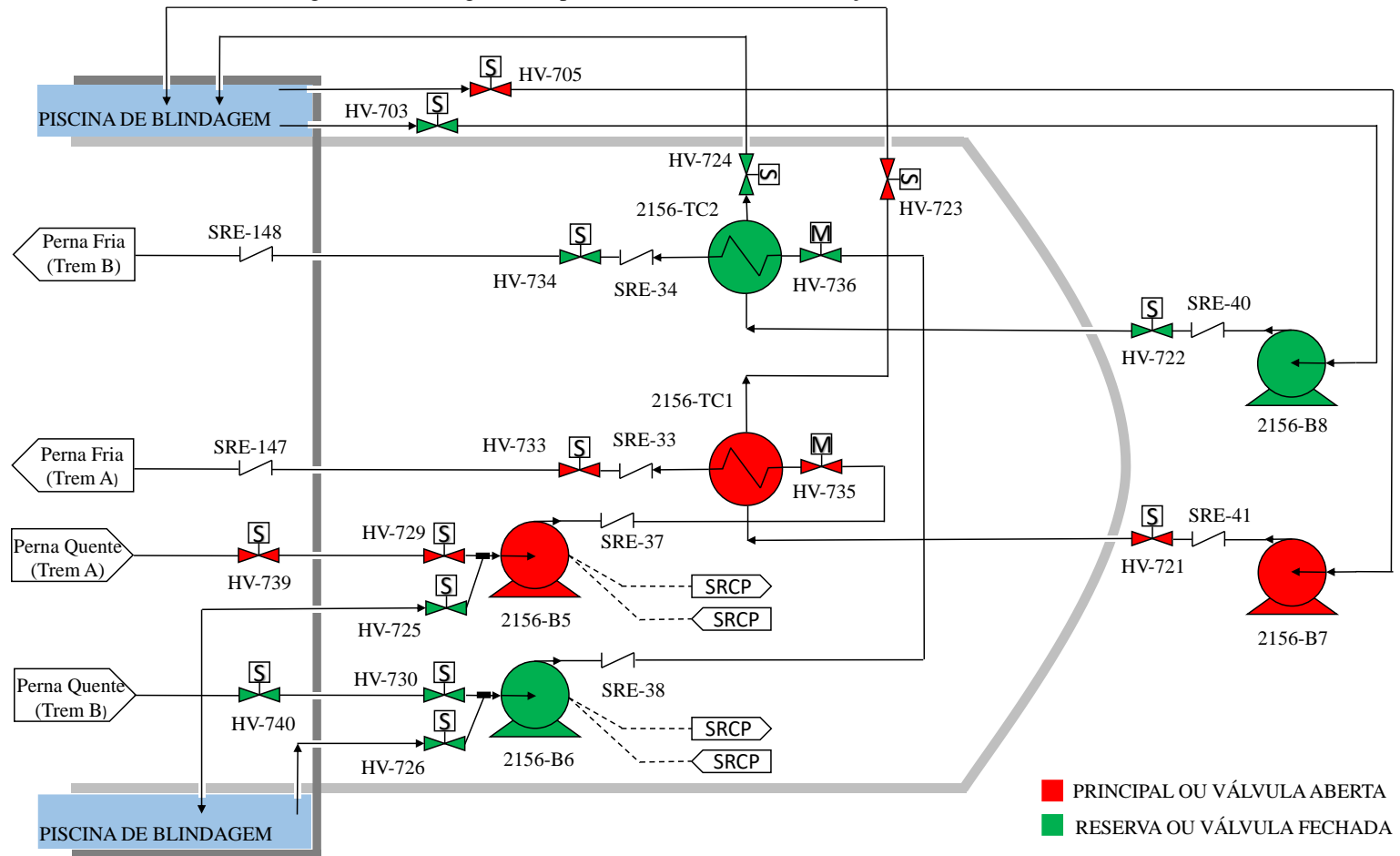
Descrição da Falha de Causa Comum	Taxa de falha do CCF	Taxa de falha individual do componente	β (beta)	γ (gama)	δ (delta)
CCF 2 de 2 CPU - operação	7,50E-7	1,50E-5	5,00E-2	-	-
CCF 2 de 2 disjuntor - fechamento	3,41E-5	1,10E-3	3,10E-2	-	-
CCF 2 de 4 disjuntor - fechamento	4,28E-6				
CCF 3 de 4 disjuntor - fechamento	3,16E-6		2,66E-2	5,56E-1	4,11E-1
CCF 4 de 4 disjuntor - fechamento	6,69E-6				
CCF 2 de 2 DGE - partida	2,54E-4	2,21E-2	1,15E-2	-	-
CCF 2 de 4 DGE - partida	5,71E-5				
CCF 3 de 4 DGE - partida	2,85E-5		1,33E-2	4,09E-1	2,79E-1
CCF 4 de 4 DGE - partida	3,34E-5				
CCF 2 de 2 DGE - operação durante 1ª hora	4,50E-5	2,90E-3	1,55E-2	-	-
CCF 2 de 4 DGE - operação durante 1ª hora	7,89E-6				
CCF 3 de 4 DGE - operação durante 1ª hora	5,02E-6		1,57E-2	4,74E-1	2,93E-1
CCF 4 de 4 DGE - operação durante 1ª hora	6,32E-6				
CCF 2 de 2 DGE - operação depois da 1ª hora	1,69E-5	1,09E-3	1,55E-2	-	-
CCF 2 de 4 DGE - operação depois da 1ª hora	2,97E-6				
CCF 3 de 4 DGE - operação depois da 1ª hora	1,89E-6		1,57E-2	4,74E-1	2,93E-1
CCF 4 de 4 DGE - operação depois da 1ª hora	2,38E-6				
CCF 2 de 2 motor da bomba - partida	5,69E-5	1,66E-3	3,43E-2	-	-
CCF 2 de 2 motor da bomba - operação	1,29E-7	6,27E-6	2,05E-7	-	-
CCF 2 de 2 motor da bomba SRCR (reserva) - operação depois da 1ª hora	3,35E-7	7,05E-6	4,75E-2	-	-
CCF 2 de 4 relé de subtensão- operação	2,66E-6	4,13E-4	3,53E-2	4,47E-1	3,46E-1

Descrição da Falha de Causa Comum	Taxa de falha do CCF	Taxa de falha individual do componente	β (beta)	γ (gama)	δ (delta)
CCF 3 de 4 relé de subtensão - operação	1,41E-6				
CCF 4 de 4 relé de subtensão - operação	2,25E-6				
CCF 2 de 4 aquisição de sinal de subtensão (sensor) - operação	2,66E-6				
CCF 3 de 4 aquisição de sinal de subtensão (sensor) - operação	1,41E-6	4,13E-4	3,53E-2	4,47E-1	3,46E-1
CCF 4 de 4 aquisição de sinal de subtensão (sensor) - operação	2,25E-6				
CCF 2 de 2 válvula de retenção (<i>check valve</i>) - abertura	8,38E-7	6,07E-5	1,38E-2	-	-
CCF 2 de 2 válvula de retenção (<i>check valve</i>) do SRCR (reserva) - abertura	3,04E-8	5,87E-8	5,18E-1	-	-
CCF 2 de 2 trocador de calor - operação	3,37E-7	3,60E-6	9,35E-2	-	-

Fonte: Adaptado <https://nrcoe.inl.gov/> [17].

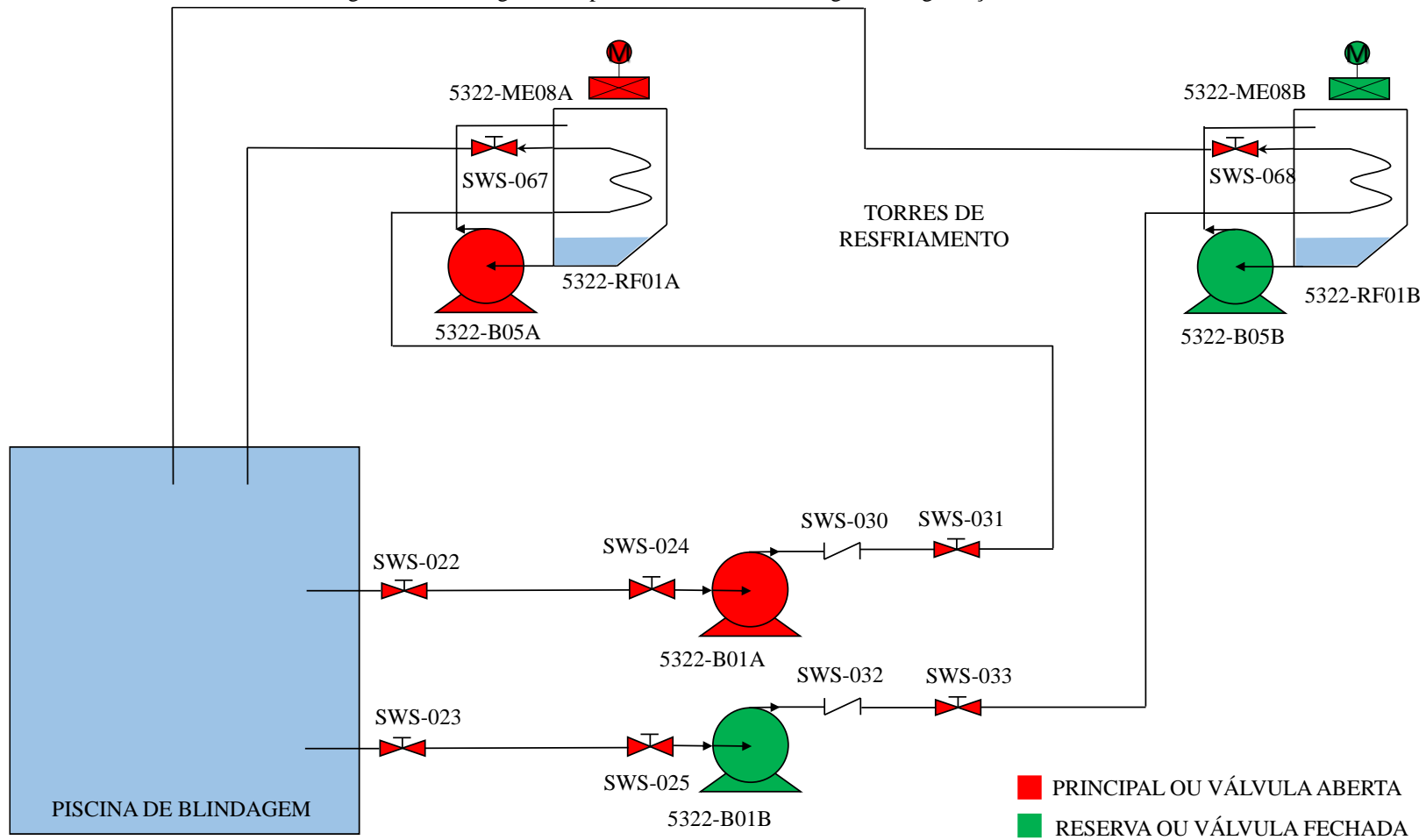
ANEXO B

Figura 32 – Fluxograma de processo do Sistema de Remoção de Calor Residual – SRCR.



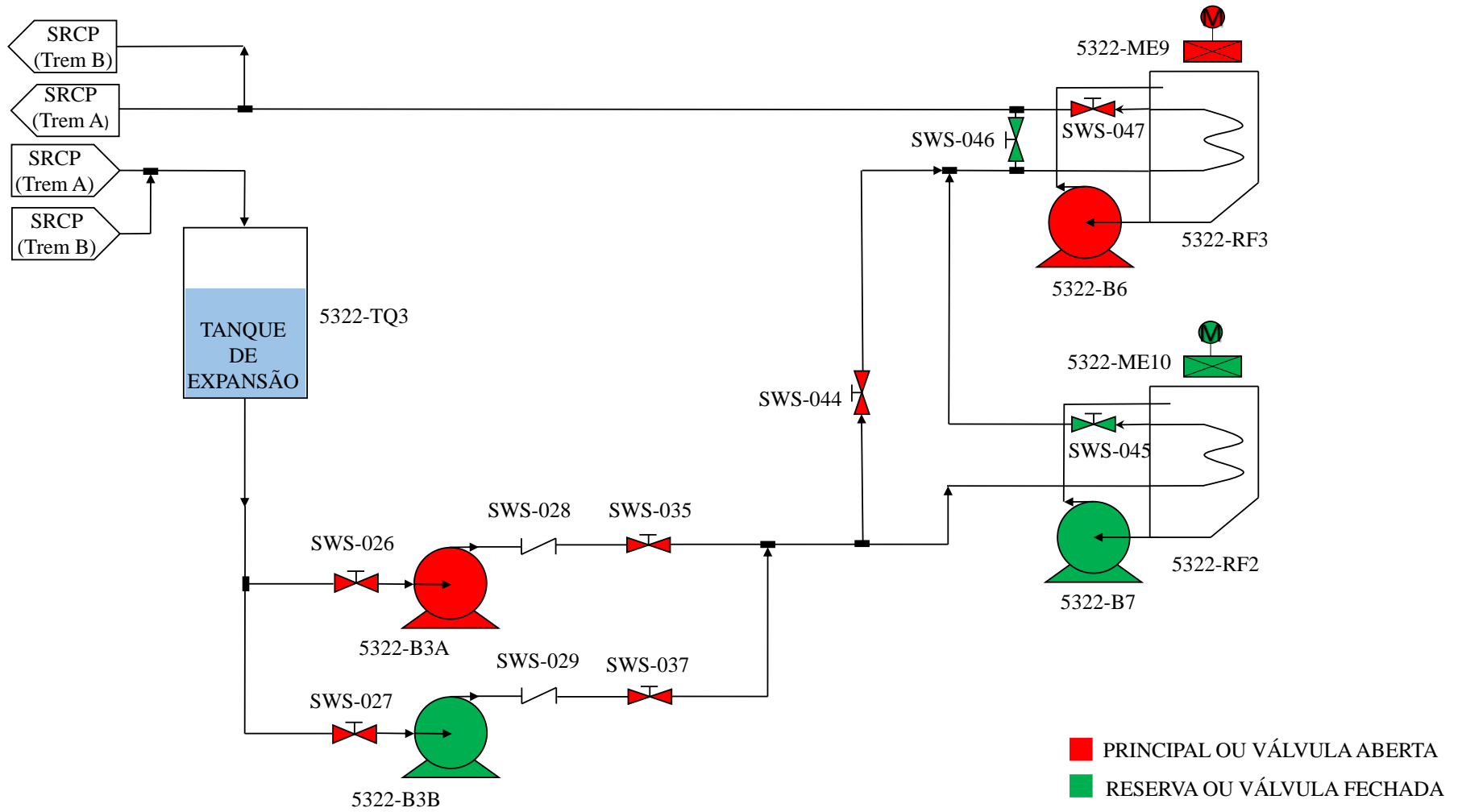
Fonte: Autor.

Figura 33 – Fluxograma de processo do Sistema de Água de Segurança - SAS – Parte 1.



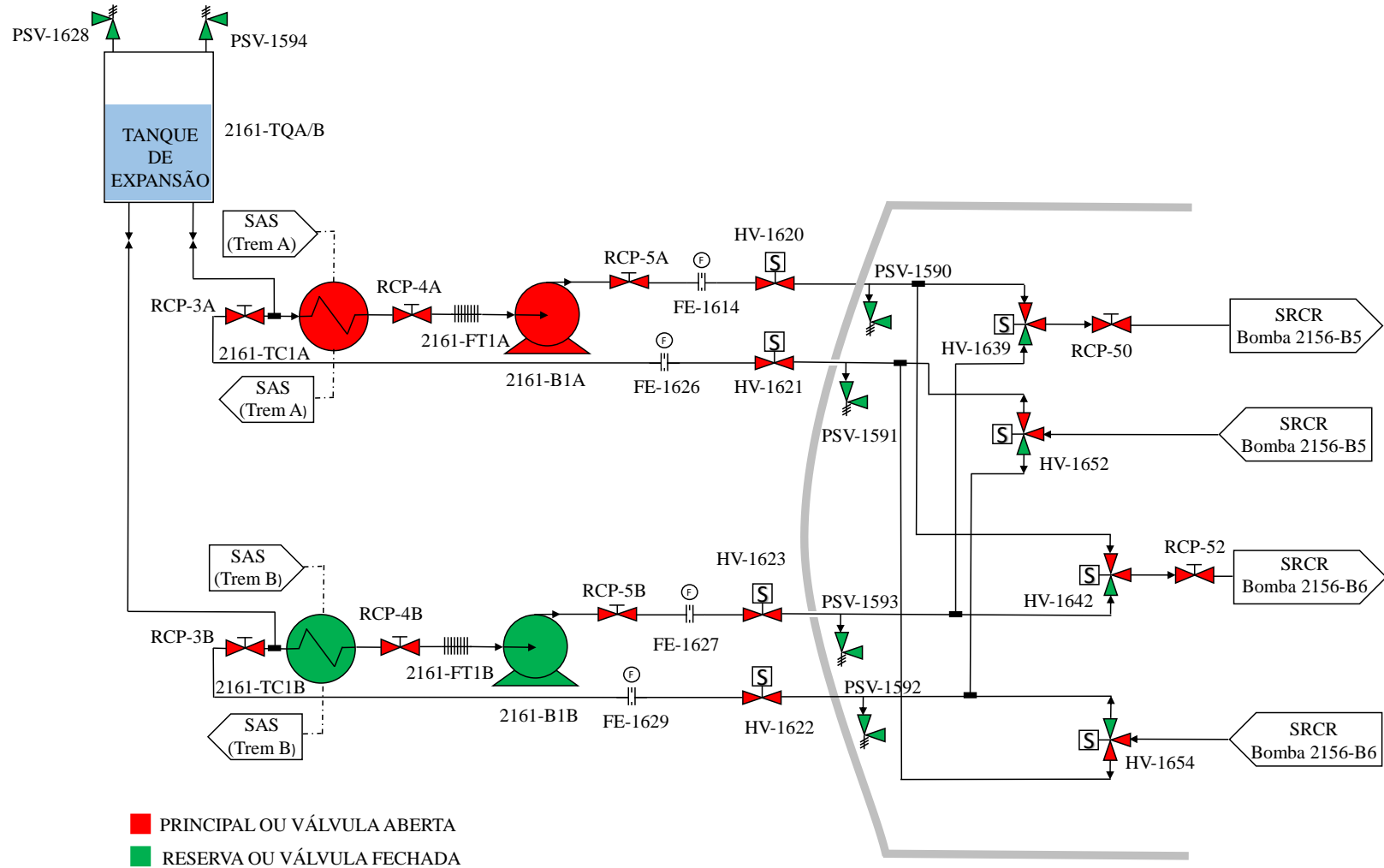
Fonte: Autor.

Figura 34 – Fluxograma de processo do Sistema de Água de Segurança - SAS – Parte 2.



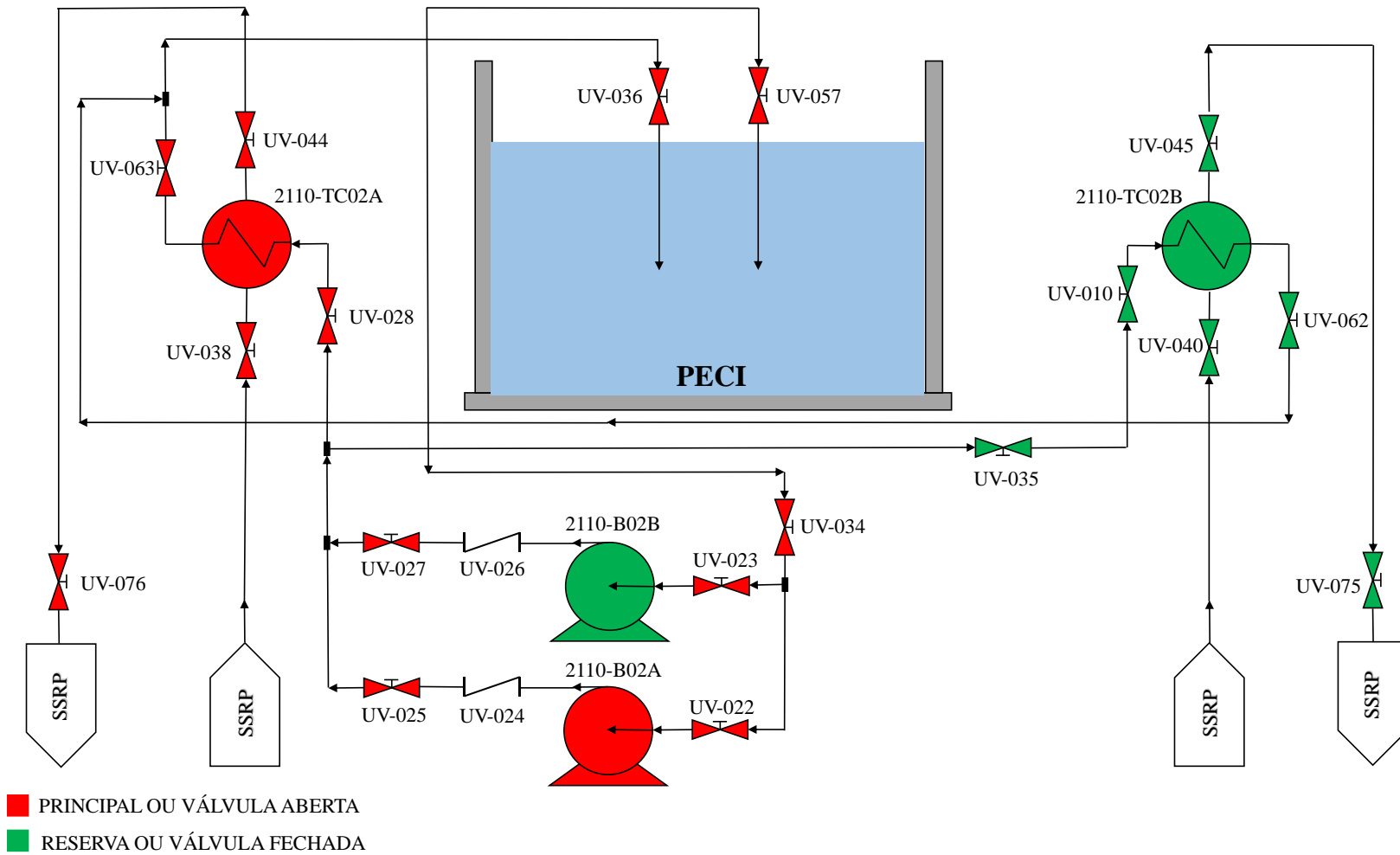
Fonte: Autor.

Figura 35 – Fluxograma de processo do Sistema de Resfriamento de Componentes do Primário – SRCP.



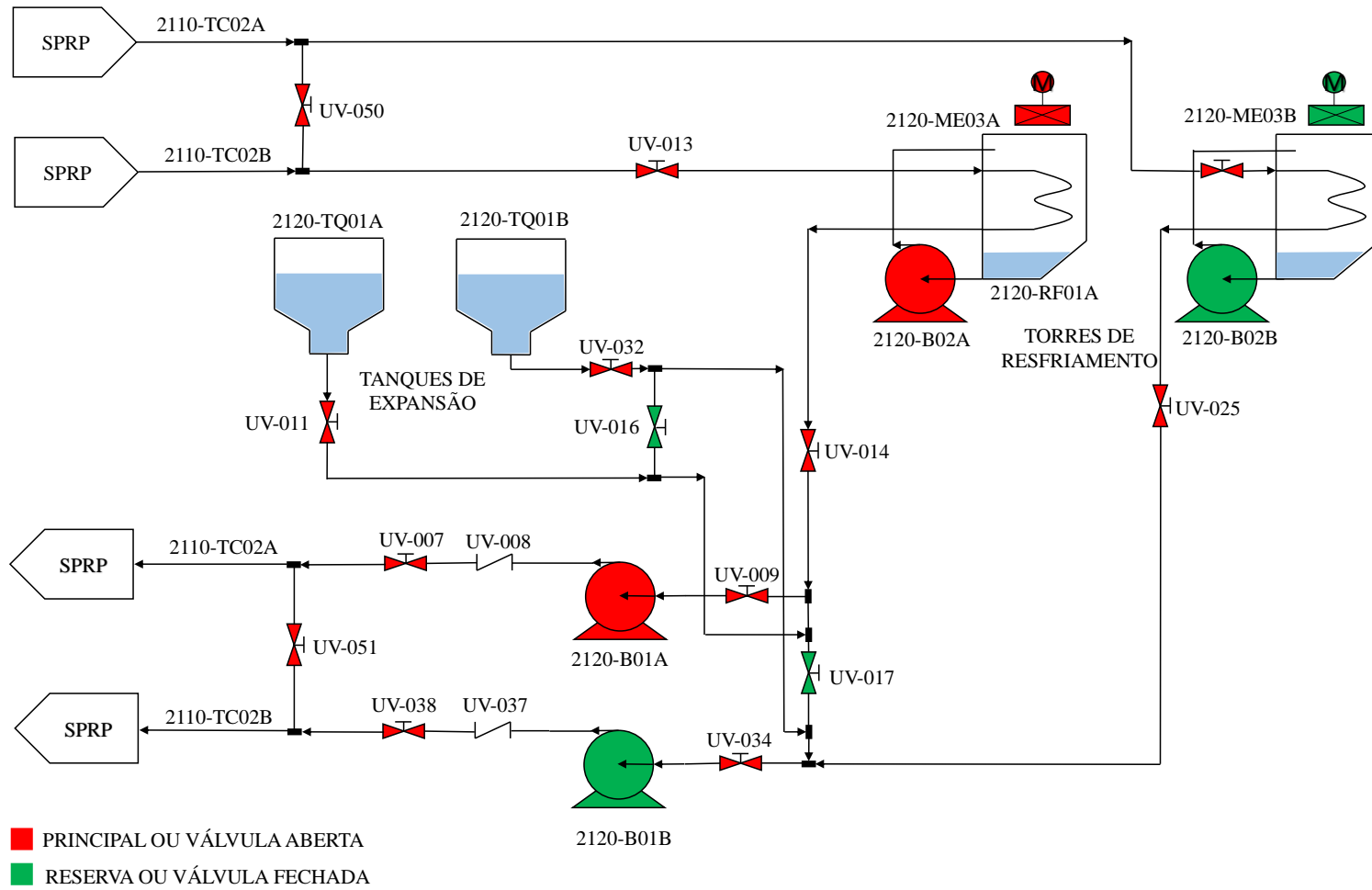
Fonte: Autor.

Figura 36 – Fluxograma de processo do Sistema Primário de Resfriamento da Piscina de Estocagem de Combustíveis Irrradiados – SPRP.



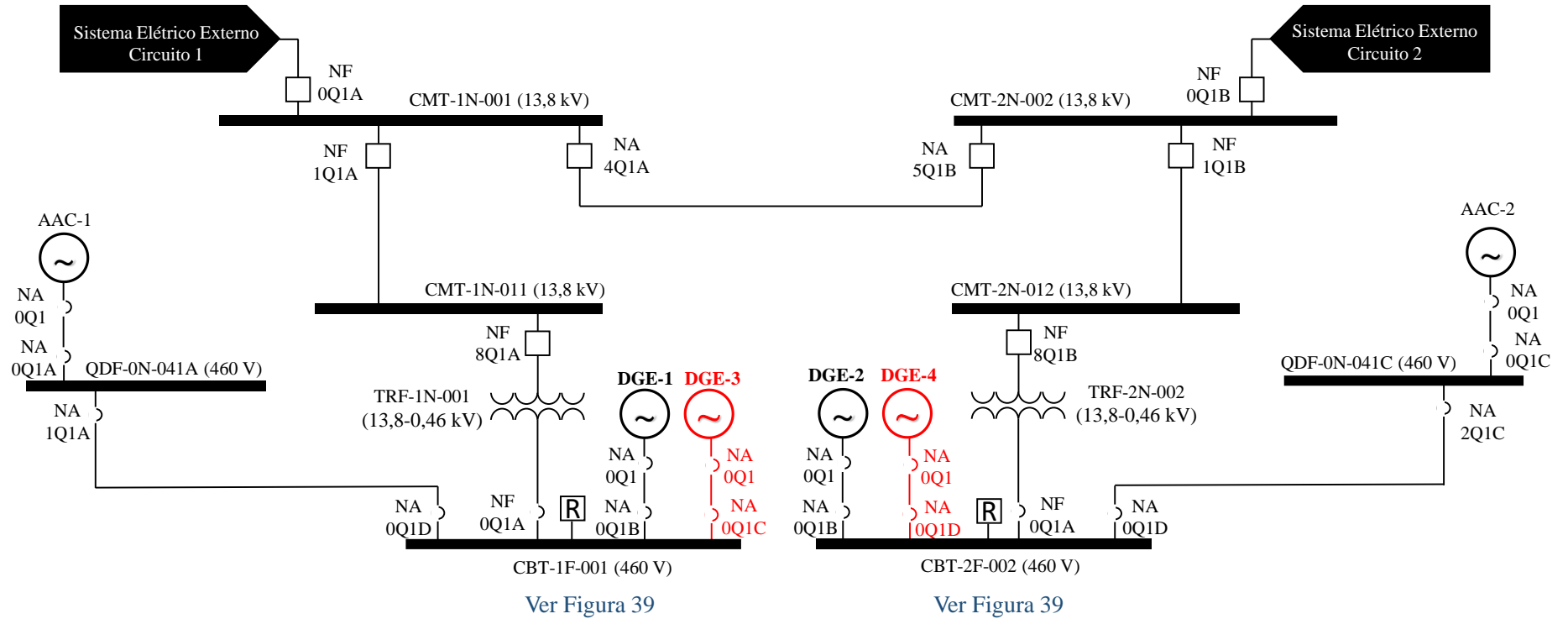
Fonte: Autor.

Figura 37 – Fluxograma de processo do Sistema Secundário de Resfriamento da Piscina de Estocagem de Combustíveis Irrradiados – SSRP.



Fonte: Autor.

Figura 38 – Diagrama unifilar do Sistema Elétrico CA – Parte 1.



- LEGENDA
- NA: NORMALMENTE ABERTO
 - NF: NORMALMENTE FECHADO
 - R: RELÉ DE SUBTENSÃO

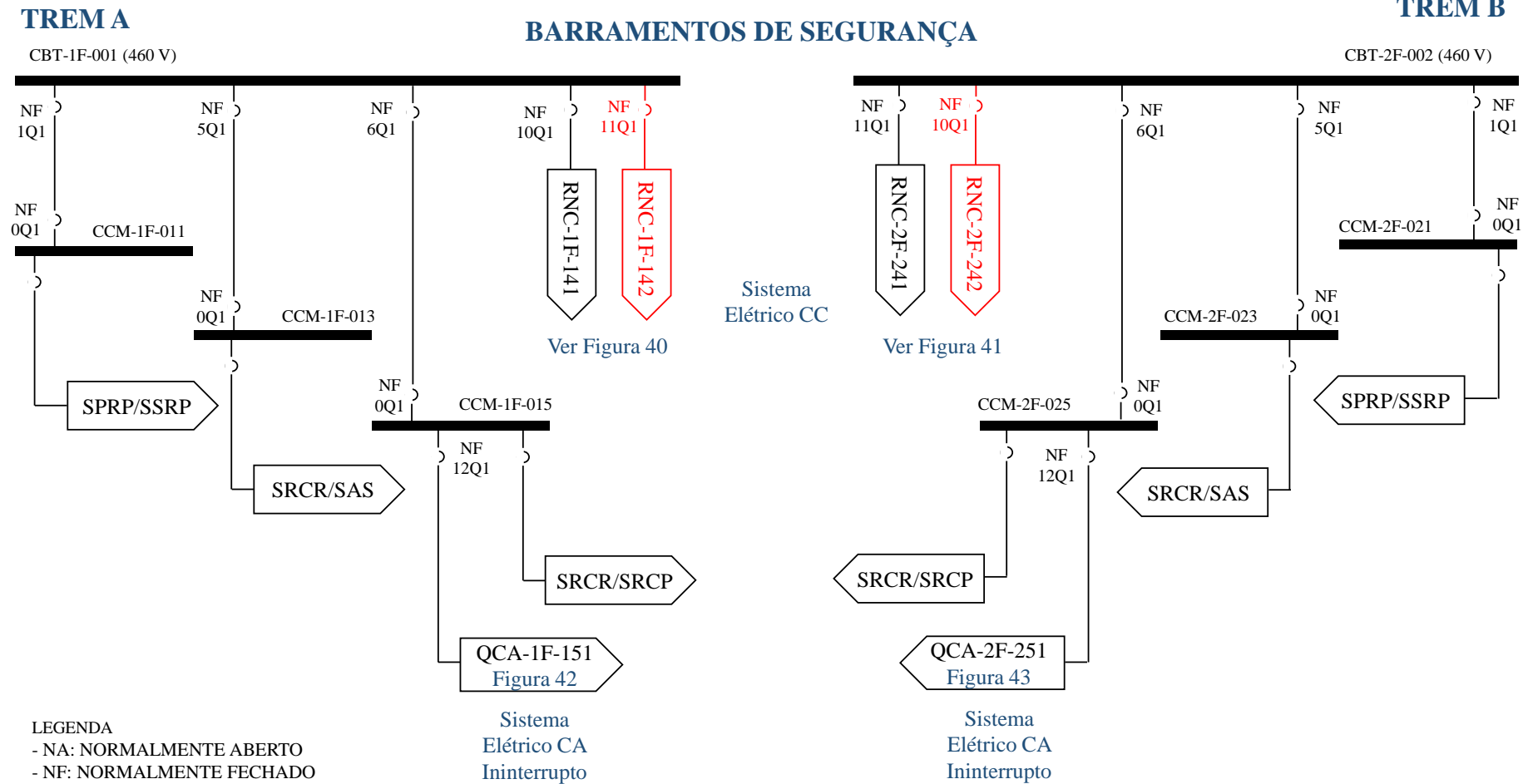
TREM A

TREM B

**BARRAMENTOS DE
SEGURANÇA**

Fonte: Autor.

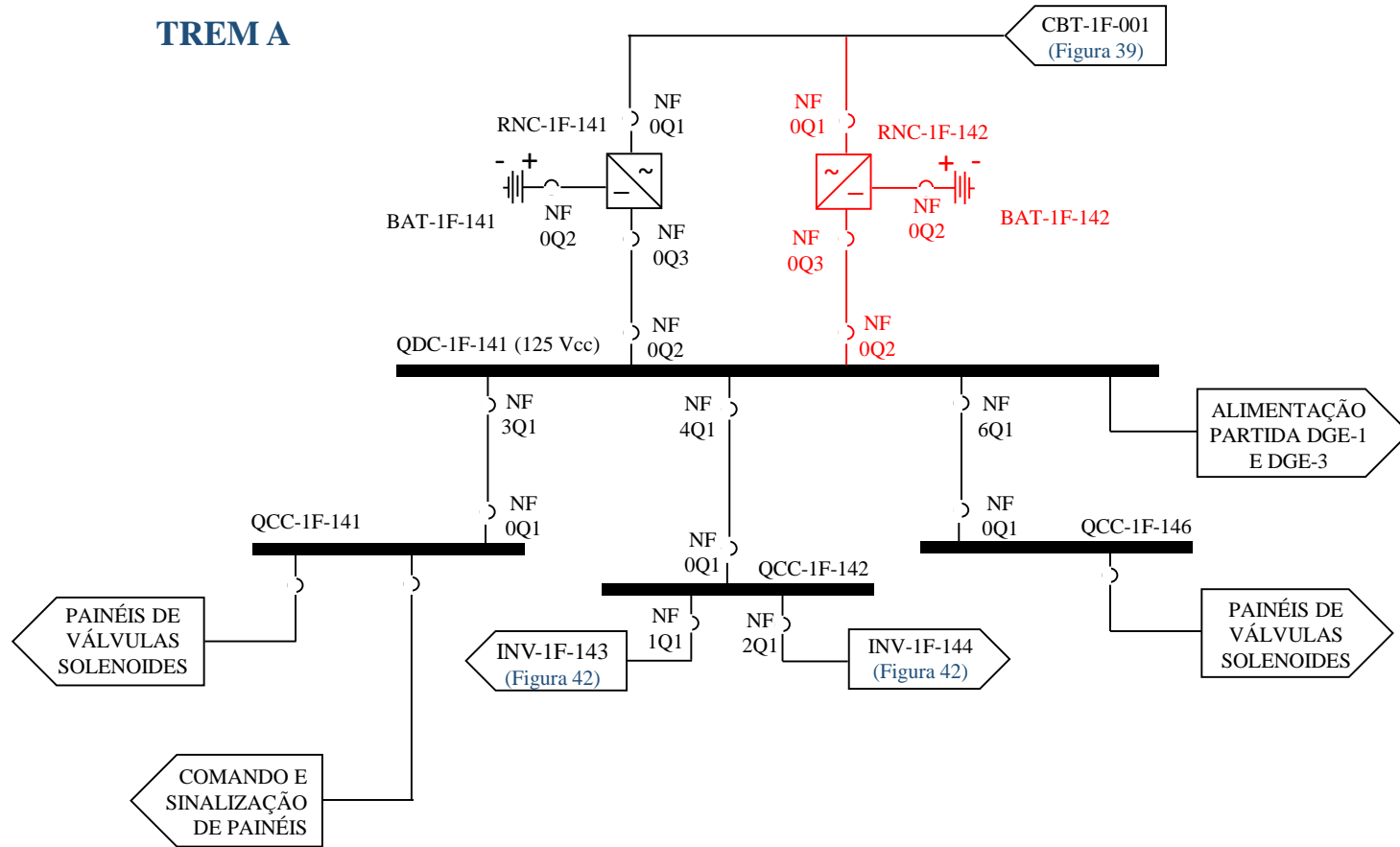
Figura 39 – Diagrama unifilar do Sistema Elétrico CA – Parte 2 (Barramentos de Emergência).



Fonte: Autor.

Figura 40 – Diagrama unifilar do Sistema Elétrico CC – Trem A.

TREM A



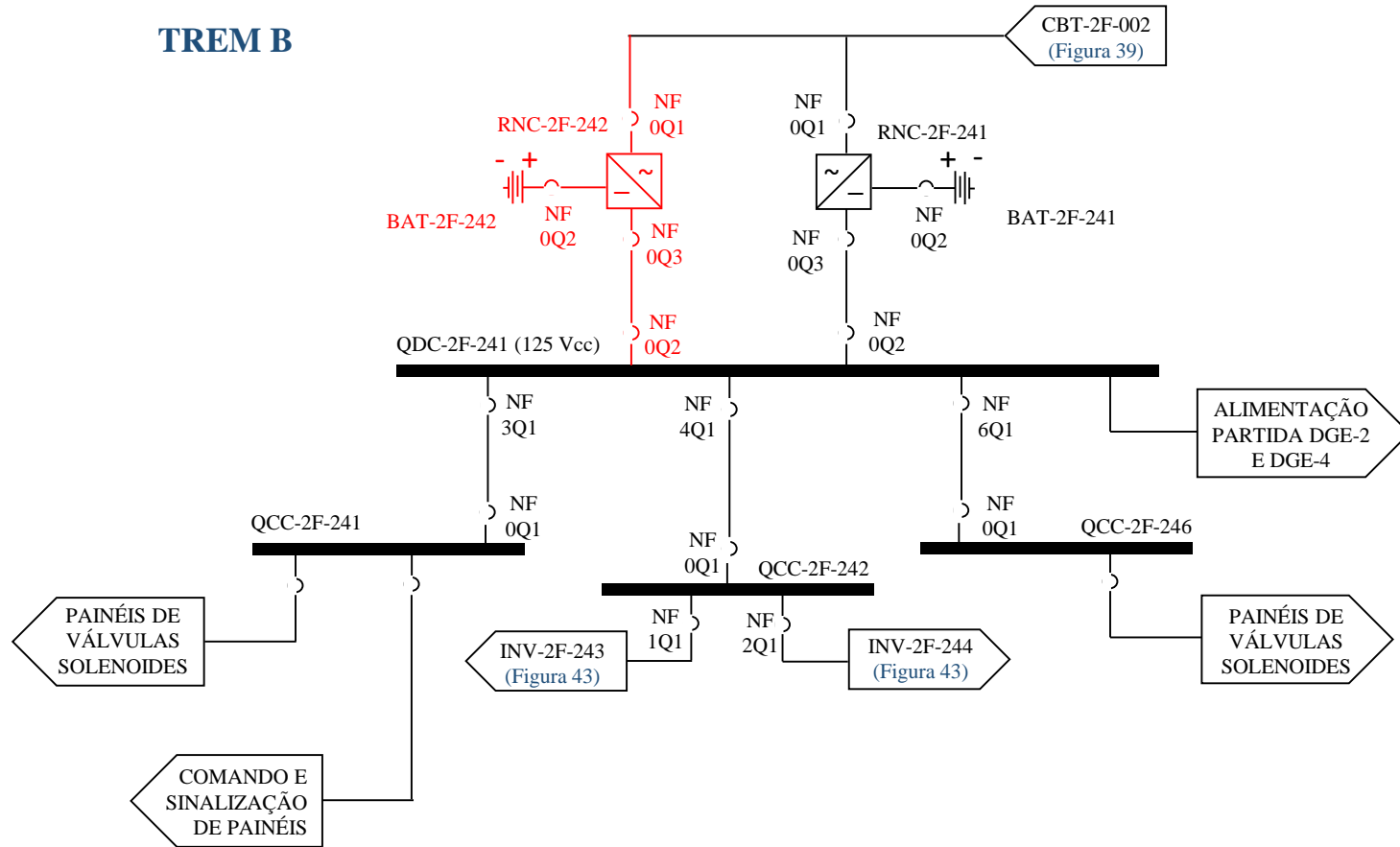
LEGENDA

- NA: NORMALMENTE ABERTO
- NF: NORMALMENTE FECHADO

Fonte: Autor.

Figura 41 – Diagrama unifilar do Sistema Elétrico CC (original) – Trem B.

TREM B



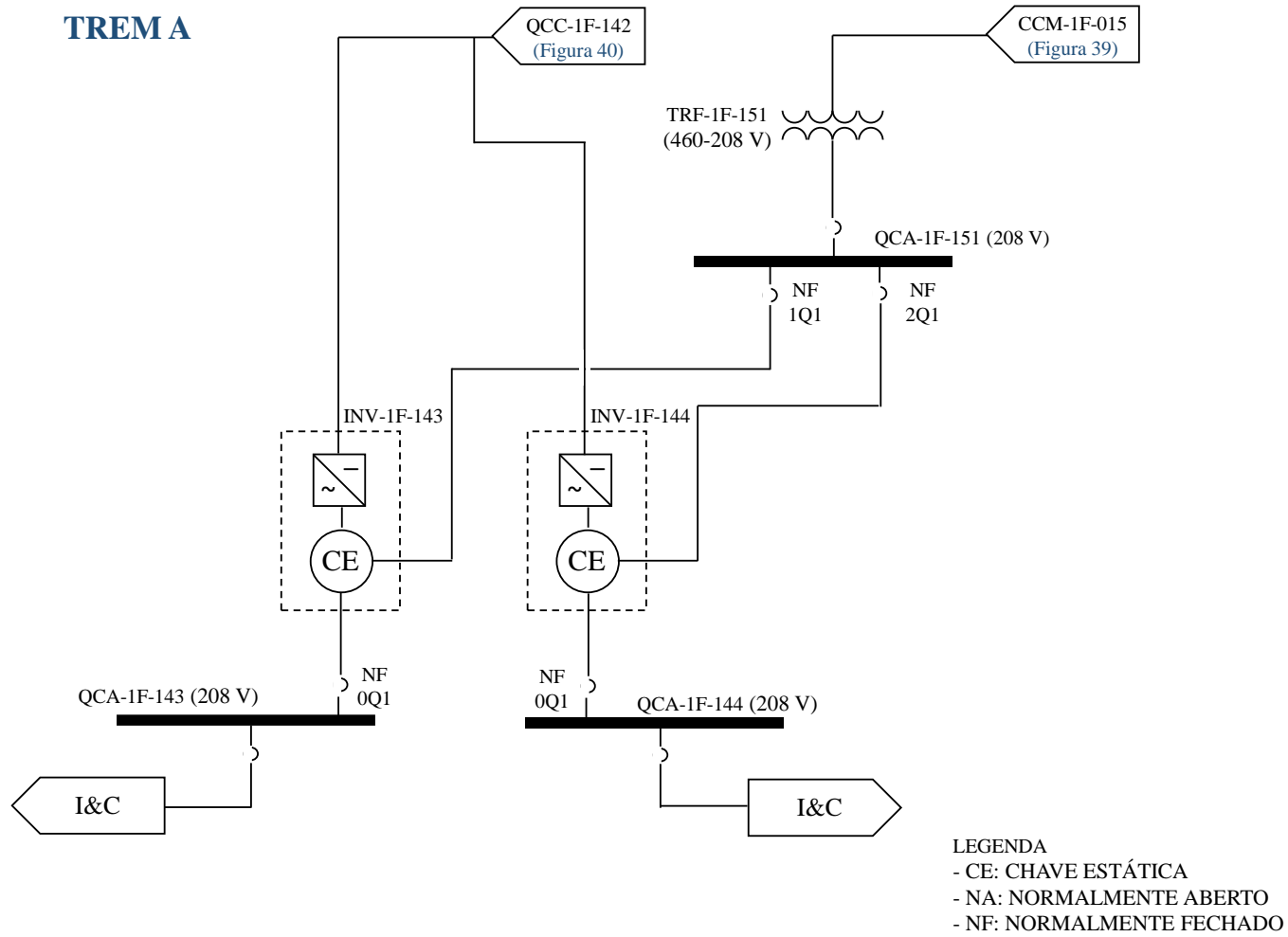
LEGENDA

- NA: NORMALMENTE ABERTO
- NF: NORMALMENTE FECHADO

Fonte: Autor.

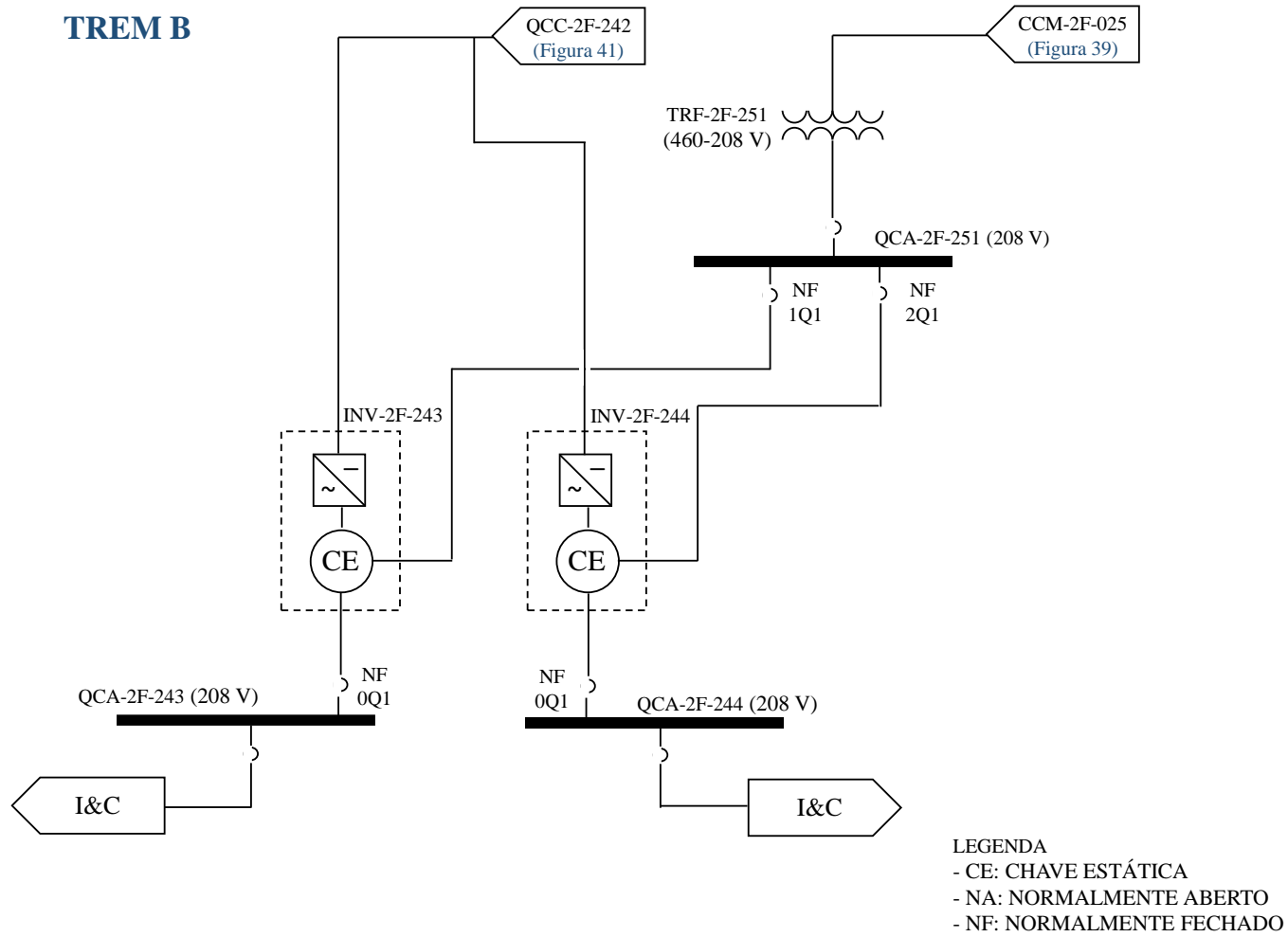
Figura 42 – Diagrama unifilar do Sistema Elétrico CA Ininterrupto – Trem A.

TREMA



Fonte: Autor.

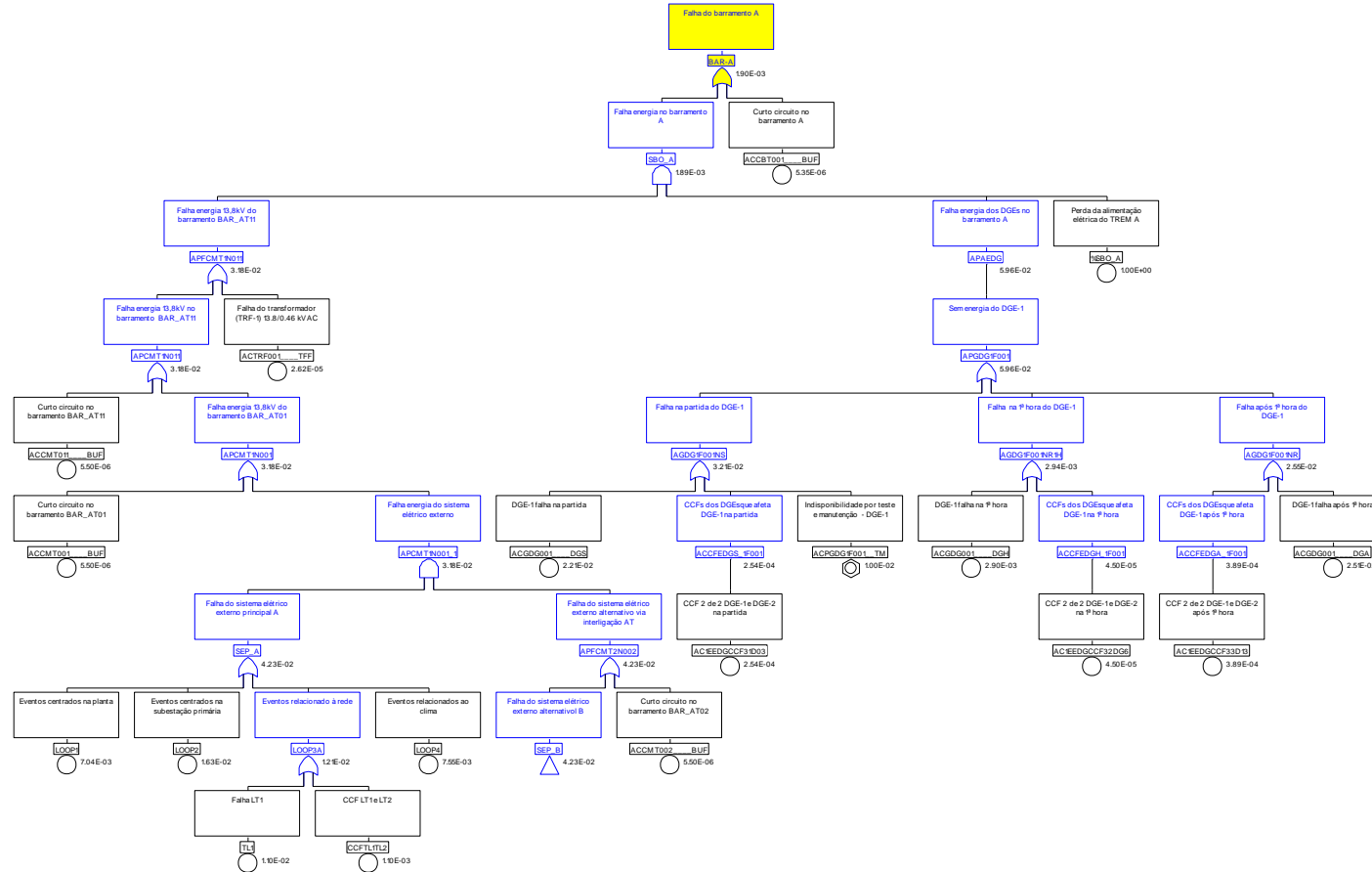
Figura 43 – Diagrama unifilar do Sistema Elétrico CA Ininterrupto – Trem B.



Fonte: Autor.

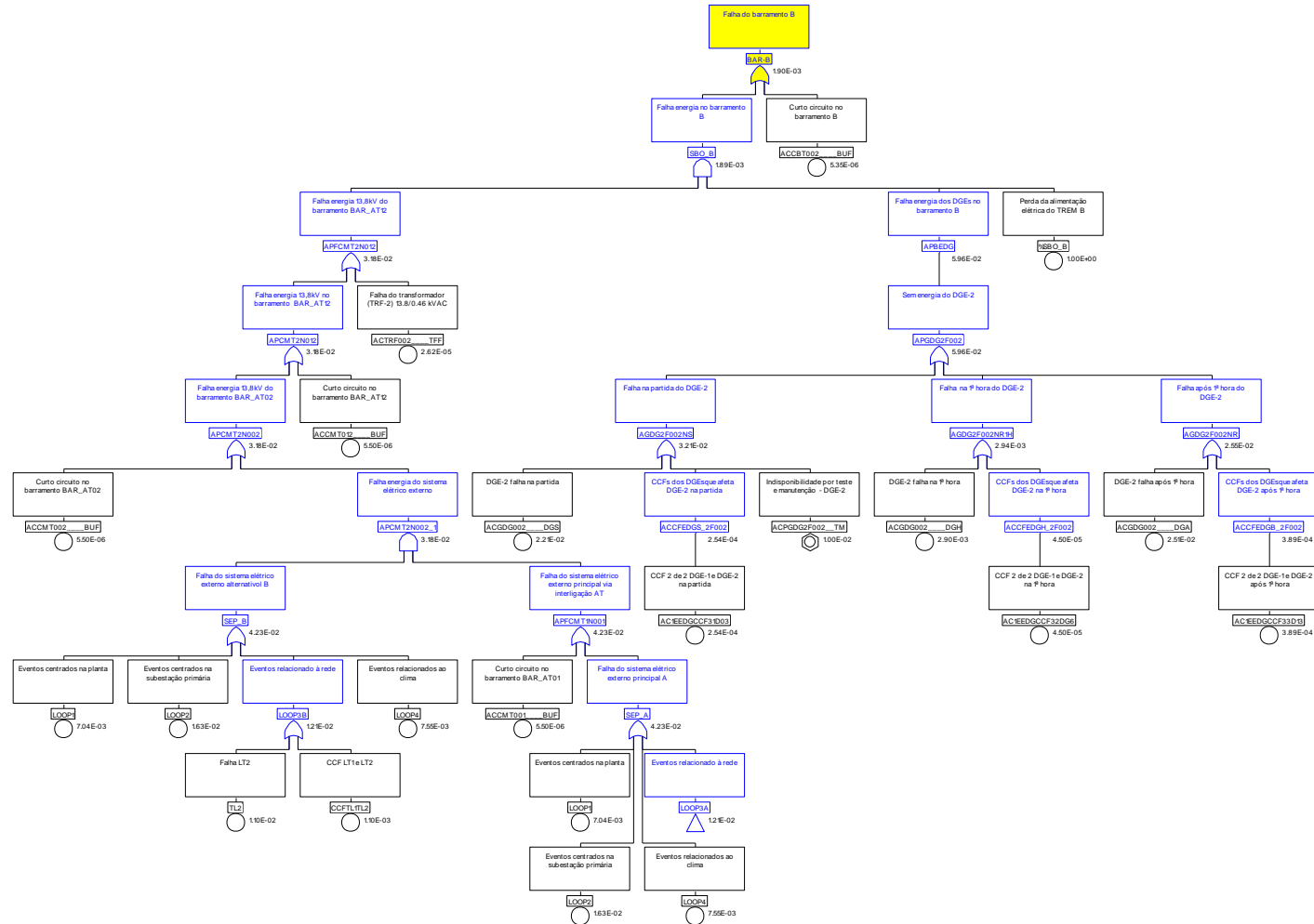
ANEXO C

Figura 44 – Árvore de falhas do evento iniciador BAR-A do projeto A do sistema elétrico.



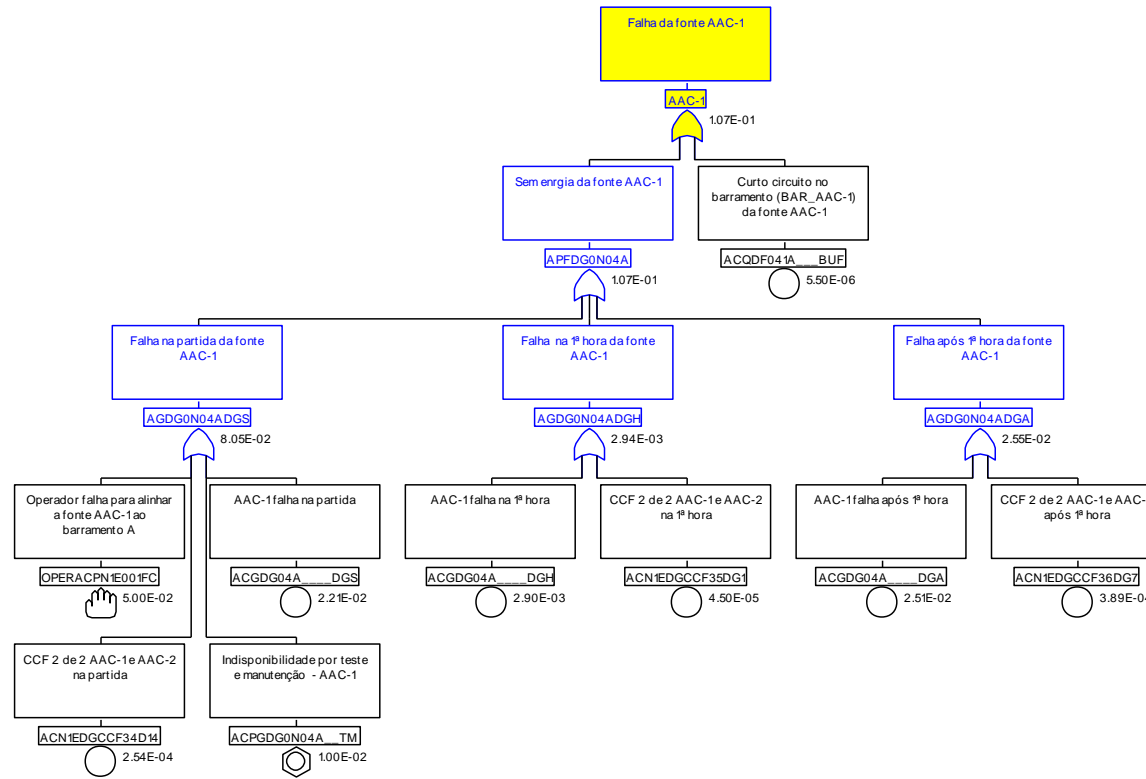
Fonte: Código computacional CAFTA [82].

Figura 45 – Árvore de falhas do evento subsequente BAR-B do projeto A do sistema elétrico.



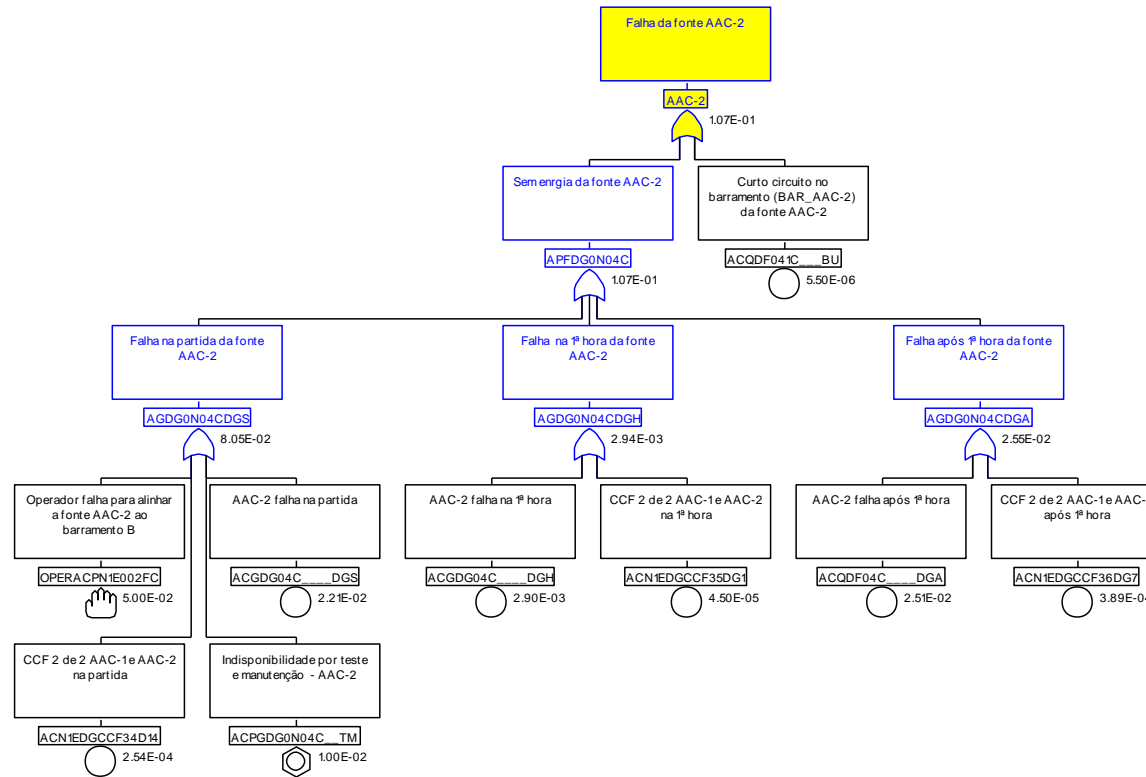
Fonte: Código computacional CAFTA [82].

Figura 46 – Árvore de falhas do evento subsequente AAC-1 do projeto A do sistema elétrico.



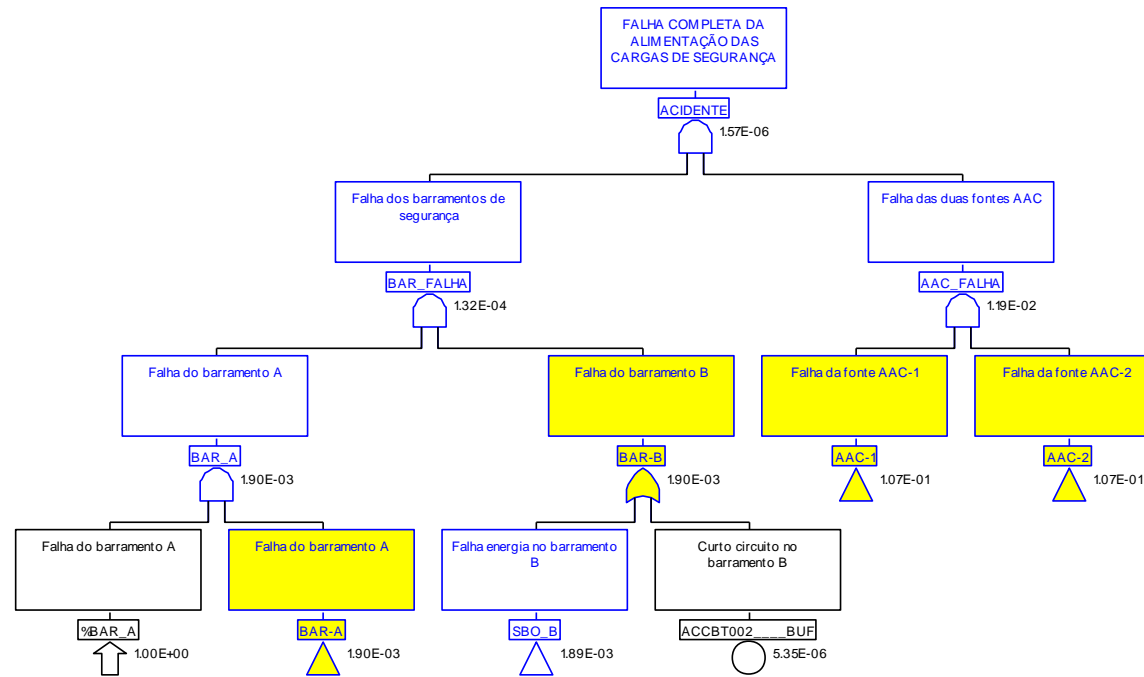
Fonte: Código computacional CAFTA [82].

Figura 47 – Árvore de falhas do evento subsequente AAC-2 do projeto A do sistema elétrico.



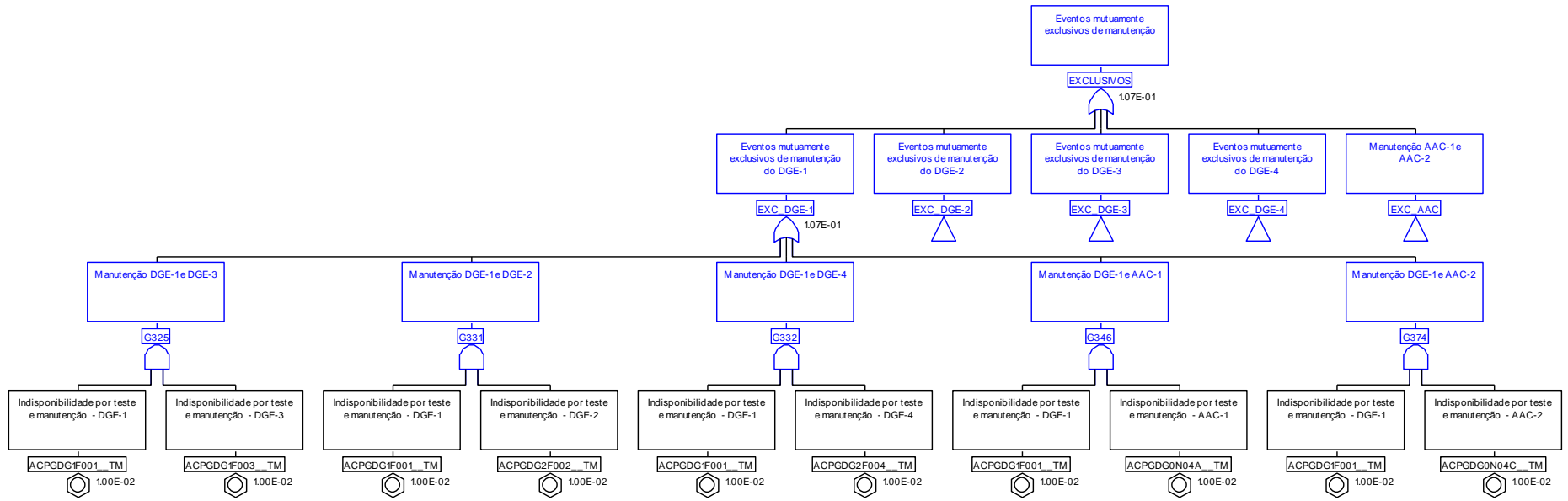
Fonte: Código computacional CAFTA [82].

Figura 48 – Árvore de falhas *master* (integradora) do projeto A do sistema elétrico.



Fonte: Código computacional CAFTA [82].

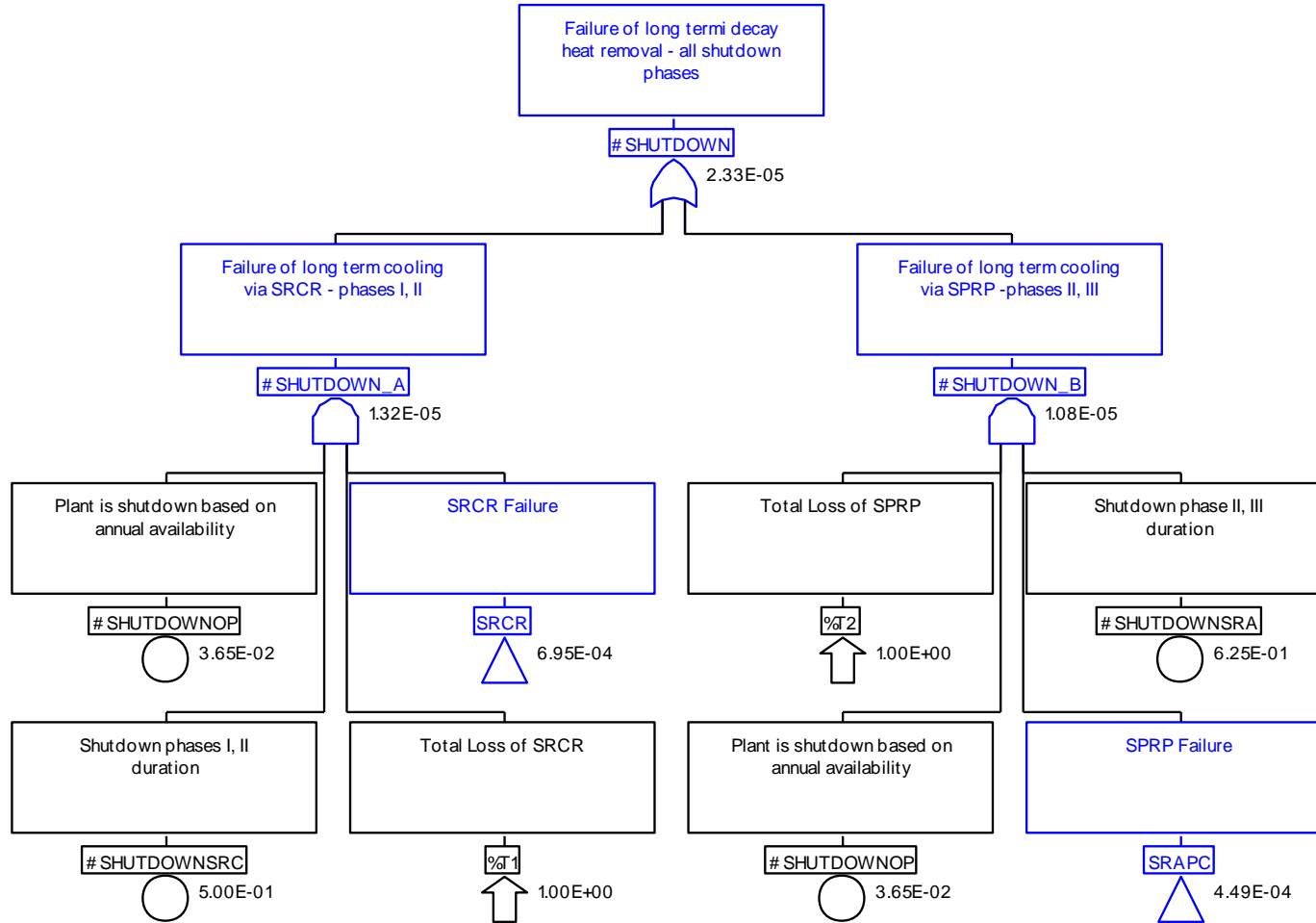
Figura 49 – Árvore de falhas dos eventos mutuamente exclusivos de componentes do sistema elétrico.



Fonte: Código computacional CAFTA [82].

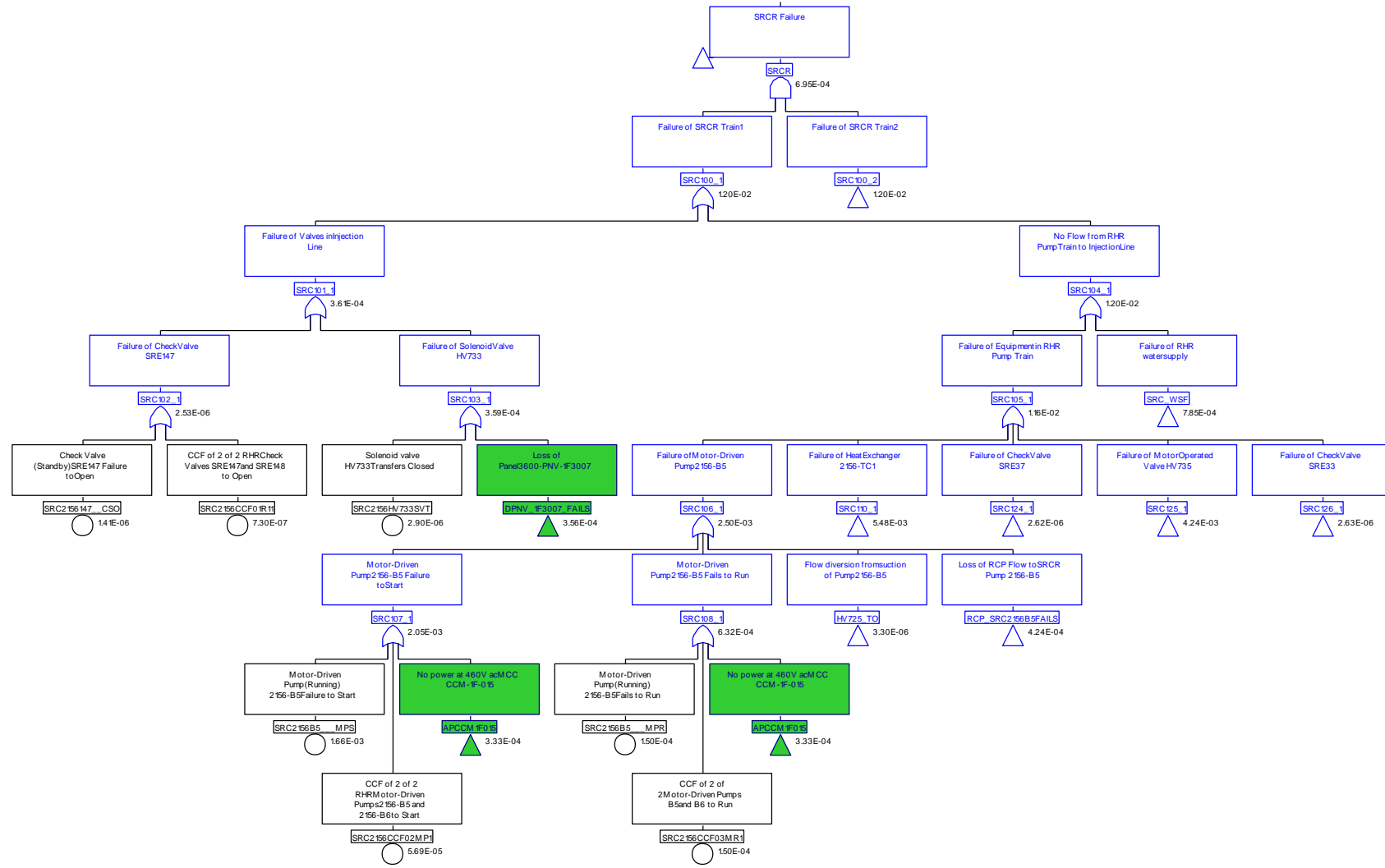
ANEXO D

Figura 50 – Árvore de falhas *master* da instalação em modo de desligamento para o projeto A (original) do sistema elétrico.



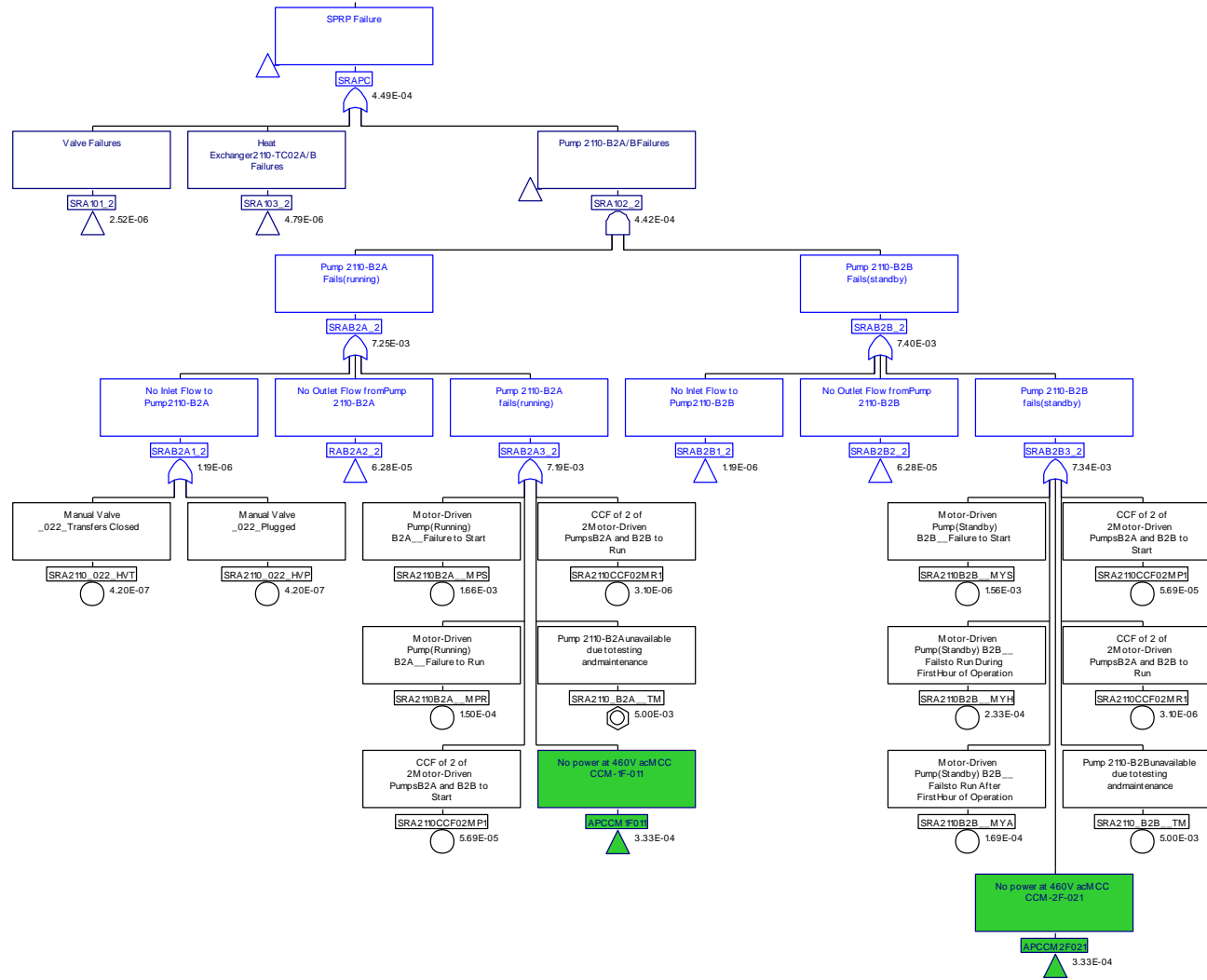
Fonte: Código computacional CAFTA [82].

Figura 51 – Árvore de falhas *master* da instalação em modo de desligamento - Eventos topo do SRCR para o projeto A (original) do sistema elétrico.



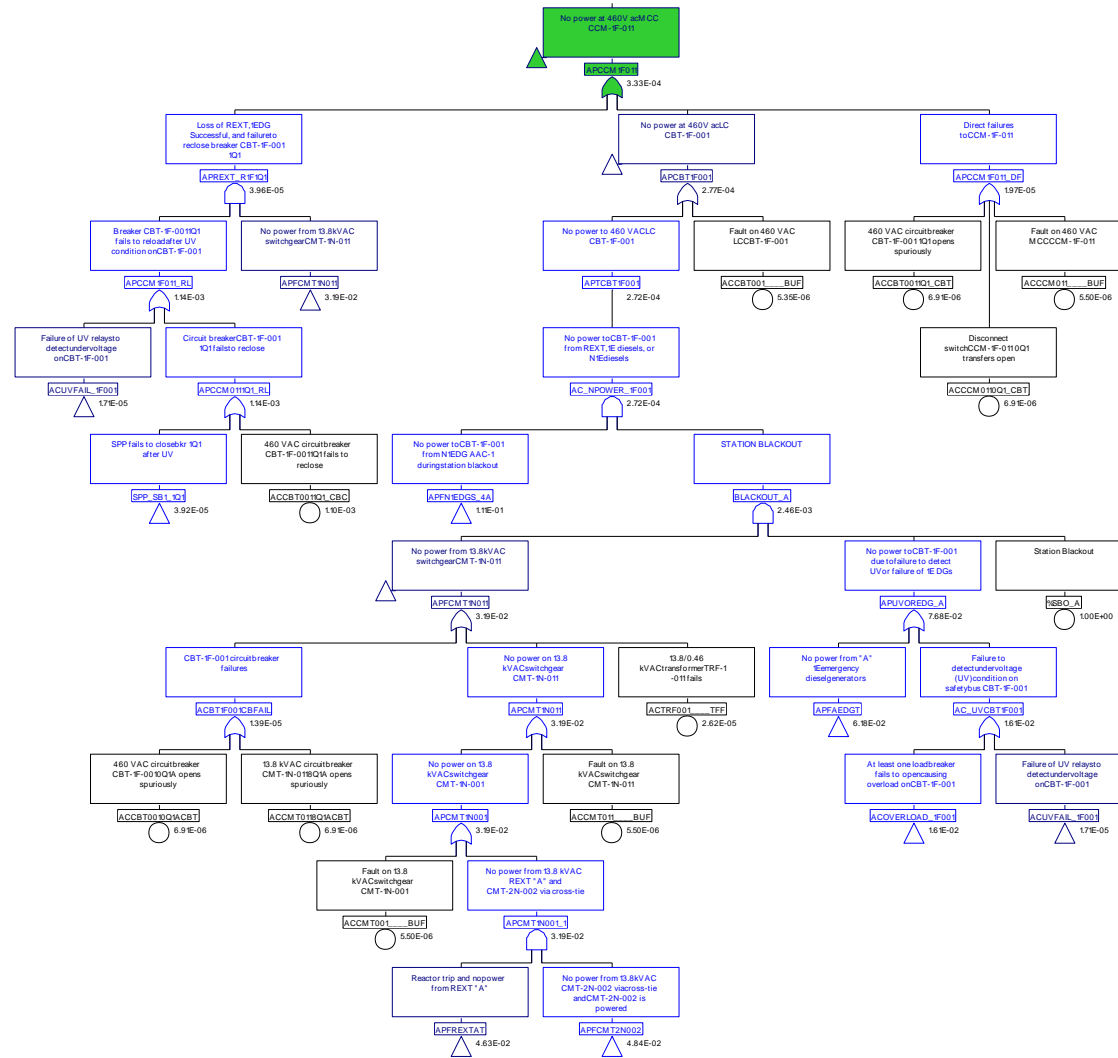
Fonte: Código computacional CAFTA [82].

Figura 52 – Árvore de falhas *master* da instalação em modo de desligamento - Eventos topo do SPRP para o projeto A (original) do sistema elétrico.



Fonte: Código computacional CAFTA [82].

Figura 53 – Exemplo de ramo da árvore de falhas contendo eventos básicos do sistema elétrico CA do projeto A (original).



Fonte: Código computacional CAFTA [82].

ANEXO E

Tabela 42 – Cortes mínimos com maiores contribuições para o risco da instalação para as quatro alternativas de projeto do sistema elétrico.

Corte	Frequência (/ano)	Evento Iniciador (cenário)	Eventos Básicos	Descrição dos Eventos Básicos
1	2,74E-06	%T1	SRC2156CCF03MR1	CCF bombas 2156-B5 e 2156-B6 do SRCR no funcionamento
2	1,30E-06	%T2	SRA2110CCF02MP1	CCF bombas 2110-B2A e 2110-B2B do SPRP na partida
3	1,04E-06	%T1	RCP2161CCF03MP1	CCF bombas 2161-B1A e 2161-B1B do SRCP na partida
4	1,04E-06	%T1	SRC2156CCF02MP1	CCF bombas 2156-B5 e 2156-B6 do SRCR na partida
5	1,04E-06	%T1	SRC2156CCF08MP1	CCF bombas 2156-B7 e 2156-B8 do SRCR na partida
6	4,56E-07	%T1	SWS5322_B01A_TM	Indisponibilidade por manutenção ou teste da bomba 5322-B01A do SAS
			SWS5322_B05B_TM	Indisponibilidade por manutenção ou teste da bomba 5322-B05B do SAS
7	4,56E-07	%T1	SWS5322_B01B_TM	Indisponibilidade por manutenção ou teste da bomba 5322-B01B do SAS
			SWS5322_B05A_TM	Indisponibilidade por manutenção ou teste da bomba 5322-B05A do SAS
8	1,89E-07	%T2	SRA2110B2A__MPS	Falha na partida do motor da bomba 2110-B2A do SPRP
			SRA2110_B2B__TM	Indisponibilidade por manutenção ou teste da bomba 2110-B2B do SPRP
9	1,85E-07	%T2	SRA2110CCF02HP2	CCF conexão dos trocadores de calor 2110-TC2A e 2110-TC2B do SPRP
10	1,84E-07	%T1	SRC2156HV736MVO	Falha ao abrir da válvula motorizada HV736 do SRCP
			SRC2156TC1__HXP	Falha na conexão do trocador de calor 2156-TC1 do SRCR
11	1,78E-07	%T2	SRA2110B2B__MYS	Falha na partida do motor da bomba 2110-B2B do SPRP
			SRA2110_B2A__TM	Indisponibilidade por manutenção ou teste da bomba 2110-B2A do SPRP
12	1,51E-07	%T1	RCP2161B1A__MPS	Falha na partida do motor da bomba 2161-B1A do SRCP
			RCP2161_TRNB_TM	Indisponibilidade por manutenção ou teste do trem B do SRCP
13	1,48E-07	%T1	RCP2161CCF01HP1	CCF conexão dos trocadores de calor 2161-TC1A e 2161-TC1B do SRCP

Corte	Frequência (/ano)	Evento Iniciador (cenário)	Eventos Básicos	Descrição dos Eventos Básicos
14	1,48E-07	%T1	SRC2156CCF05HP1	CCF conexão dos trocadores de calor 2156-TC1 e 2156-TC2 do SRCR
15	1,42E-07	%T1	RCP2161B1B__MYS	Falha na partida do motor da bomba 2161-B1B do SRCP
			RCP2161_TRNA_TM	Indisponibilidade por manutenção ou teste do trem A do SRCP
16	1,42E-07	%T1	SWS5322_B01A_TM	Indisponibilidade por manutenção ou teste da bomba 5322-B01A do SAS
			SWS5322_B05BMYS	Falha na partida do motor da bomba 5322-B05B do SAS
17	1,42E-07	%T1	SWS5322_B01A_TM	Indisponibilidade por manutenção ou teste da bomba 5322-B01A do SAS
			SWS5322_B1B_MYS	Falha na partida do motor da bomba 5322-B01B do SAS
18	1,42E-07	%T1	SWS5322_B05A_TM	Indisponibilidade por manutenção ou teste da bomba 5322-B05A do SAS
			SWS5322_B05BMYS	Falha na partida do motor da bomba 5322-B05B do SAS
19	1,42E-07	%T1	SWS5322_B05A_TM	Indisponibilidade por manutenção ou teste da bomba 5322-B05A do SAS
			SWS5322_B1B_MYS	Falha na partida do motor da bomba 5322-B01B do SAS
20	1,18E-07	%T1	SRC2156B5__MPS	Falha na partida do motor da bomba 2156-B5 do SRCR
			SRC2156HV736MVO	Falha ao abrir da válvula motorizada HV736 do SRCP

Fonte: Código computacional CAFTA [82].

INSTITUTO DE PESQUISAS ENERGÉTICAS E NUCLEARES
Diretoria de Pesquisa, Desenvolvimento e Ensino
Av. Prof. Lineu Prestes, 2242 – Cidade Universitária CEP: 05508-000
Fone/Fax(0XX11) 3133-8908
SÃO PAULO – São Paulo – Brasil <http://www.ipen.br>

O IPEN é uma Autarquia vinculada à Secretaria de Desenvolvimento, associada à Universidade de São Paulo e gerida técnica e administrativamente pela Comissão Nacional de Energia Nuclear, órgão do Ministério da Ciência, Tecnologia, Inovações e Comunicações.
