AUTARQUIA ASSOCIADA À UNIVERSIDADE DE SÃO PAULO

ANÁLISE DA CONFIABILIDADE DO SISTEMA DE SUPRIMENTO DE ENERGIA ELÉTRICA DE EMERGÊNCIA DE UM REATOR NUCLEAR DE PEQUENO PORTE

GERSON BONFIETTI

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

Orientador:
Dr. José Messias de Oliveira Neto

São Paulo
2003

87

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

ANÁLISE DA CONFIABILIDADE DO SISTEMA DE SUPRIMENTO DE ENERGIA ELÉTRICA DE EMERGÊNCIA DE UM REATOR NUCLEAR DE PEQUENO PORTE

GERSON BONFIETTI

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

Orientador :
Dr. José Messias de Oliveira Neto

São Paulo
2003

COMISSÃO NACIONAL DE ENERGIA NUCLEAR/SP-IPEN

ANÁLISE DA CONFIABILIDADE DO SISTEMA DE SUPRIMENTO DE ENERGIA ELÉTRICA DE EMERGÊNCIA DE UM REATOR NUCLEAR DE PEQUENO PORTE

Gerson Bonfietti

RESUMO

O presente trabalho analisa o sistema de suprimento de energia elétrica de emergência de um reator nuclear de pequeno porte. São consideradas três configurações típicas e analisadas as suas confiabilidades.

O método utilizado na avaliação da confiabilidade usa a árvore de falhas como ferramenta principal de análise.

É feita uma revisão bibliográfica sobre a confiabilidade dos diesel geradores de emergência e uma discussão sobre a posição regulatória aplicável ao desenvolvimento de sistemas elétricos.

A influência de falhas de modo comum na confiabilidade é analisada utilizando-se o método do fator beta.

São consideradas as influências de ações do operador atribuindo-se probabilidades de falha humana.

Através de uma análise paramétrica é mostrada a forte dependência da segurança do reator a eventos de perda do suprimento externo de energia, bem como a sensível alteração da confiabilidade do sistema quando se passa a considerar a contribuição de falhas de modo comum.

COMISSÃO NACIONAL DE ENERGIA NUCLEAR/SP-IPEN

SMALL NUCLEAR POWER REACTOR
EMERGENCY ELECTRIC POWER SUPPLY SYSTEM RELIABILITY
COMPARATIVE ANALYSIS

Gerson Bonfietti

ABSTRACT

This work presents an analysis of the reliability of the emergency power supply system of a small size nuclear power reactor. Three different configurations are investigated and their reliability analyzed.

The fault tree method is used as the main tool of analysis.

The work includes a bibliographical review of emergency diesel generator reliability and a discussion of the design requirements applicable to emergency electrical systems.

The influence of common cause failure influences is considered using the beta factor model.

The operator action is considered using human failure probabilities.

A parametric analysis shows the strong dependence between the reactor safety and the loss of offsite electric power supply.

It is also shown that common cause failures can be a major contributor to the system reliability.

SUMÁRIO

1 – INTRODUÇÃO 9
1.1 – Objetivos do Trabalho 11
1.1.1 – O Diesel Gerador de Emergência 12
1.2 – Organização do Trabalho 17
2 – HISTÓRICO DA CONFIABILIDADE DAS FONTES DE EMERGÊNCIA 18
3 – POSIÇÃO REGULATÓRIA 31
3.1 – Geral 31
3.2 - Requisitos 33
3.2.1 – CFR-50 33
3.2.2 - BNL 50831-II 35
3.2.3 - 50-SG-D7 - Agência Internacional de Energia Atômica 36
3.2.4 – ABNT-NBR 8671 41
3.2.5 - CNEN 43
3.3 – Observações sobre a Base Normativa 44
4 – MÉTODO DE AVALIAÇÃO DA CONFIABILIDADE 46
4.1 – Considerações Gerais 46
4.2 – Árvore de Falhas 47
4.2.1 – Fundamentos 47
4.2.2 – Elementos Básicos de uma Árvore de Falhas 48
4.2.3 – Cortes Mínimos 49
4.2.4 – Falhas Dependentes 51
4.3 - Subsídios para Avaliação da Confiabilidade 57
4.3.1 - Familiarização com o Sistema 57
4.3.2 – Confiabilidade Humana 57
4.3.3 – Banco de Dados 60
4.3.4 – Códigos Computacionais 60
5 – ESTUDO DE ALTERNATIVAS 62
5.1 - Geral 62
5.2 – O Sistema Analisado 62
5.2.1 - O Sistema Elétrico Externo 64
5.2.2 - O Sistema Elétrico Local 68
5.2.2.1 - Subestação Principal 68
5.2.2.2 – Cabine Primária 70
5.2.2.3 – Subestação de Emergência - 4 DG 70
5.2.2.4 – Subestação de Emergência - 3 DG 73
5.2.2.5 – Subestação de Emergência - 2 DG 75
5.3 – Base de dados 77
5.3.1 – Equipamentos e Componentes 77
5.3.2 – Confiabilidade Humana 77
5.3.3 – Eventos Dependentes 81

COMISSÃO NACIONAL DE ENERGIA NUCLEAR/SP-IPEN

5.4 – Desenvolvimento das Árvores de Falhas 81
5.4.1 – Definição do Evento Topo 81
5.4.2 – Construção das Árvores de Falhas 82
5.4.2.1 – Árvore de Falhas para a Configuração com 4 Diesel Geradores. 82
5.4.2.2 – Árvore de Falhas para a Configuração com 3 Diesel Geradores. 82
5.4.2.3 – Árvore de Falhas para a Configuração com 2 Diesel Geradores. 82
5.6 – Análise de Desempenho do Sistema Elétrico 94
5.6.1 - Geral 94
5.6.2 – Avaliação do Desempenho 96
5.7 – Análise Paramétrica 96
5.7.1 – Alimentação Externa 98
5.7.2 – Transferência Automática/Manual 98
5.7.2 – Contribuição das Falhas de Modo Comum 98
6 – CONCLUSÕES E RECOMENDAÇÕES 102
7 - REFERÊNCIAS 104
ANEXO A – Falhas dos Diesel Geradores por Demanda por Planta 107
ANEXO B – Símbolos Empregados na Árvore de Falhas 109
ANEXO C -Roteiro para Análise de Falhas de Modo Comum 111
ANEXO D – Valores Recomendados para o Fator Beta 112
ANEXO E – Interrupções de Energia da Linha de Transmissão 113
ANEXO F – Histograma das interrupções da Linha de Transmissão 117
ANEXO G – Diagrama Lógico - Configuração com 3 Diesel Geradores 119
ANEXO H – Diagrama Lógico - Configuração com 2 Diesel Geradores 122

LISTA DE TABELAS

1.1 – Definição dos estados da planta	14
2.1 – Contribuição dos subsistemas dos diesel geradores	22
2.2 - Contribuição dos componentes dos subsistemas dos diesel geradores	23
2.3 – Sumário das falhas de modo comum dos diesel geradores	29
3.1 – Limites de tempo para restabelecimento do suprimento externo	42
4.1 – Tipos de eventos dependentes	52
4.2 – Exemplos de falhas humanas que causaram indisponibilidade dos diesel geradores	59
5.1 – Freqüência anual de perda da alimentação externa – CPFL	66
5.2 - Freqüência anual de perda da alimentação externa de algumas usinas	67
5.3 – Dados de falha dos componentes do sistema elétrico	78
5.4 - Dados de falha dos componentes dos sistemas auxiliares dos diesel geradores	79
5.5 – Lógica da árvore de falhas para a configuração com 4 diesel geradores	88
5.6 – Resumo dos casos estudados	95
5.7 – Cortes mínimos obtidos para as configurações estudadas	97
5.8 – Cortes mínimos obtidos com dados da linha de alimentação de ANGRA I	99
5.9 – Freqüências anuais de perda de alimentação elétrica para transferência automática e manual	101
5.10 – Freqüência anual de perda de alimentação elétrica para diferentes valores do fator beta	101

LISTA DE FIGURAS

1.1 – Esquema ilustrativo dos estados da planta	13
1.2 – Passos para avaliação probabilística de segurança	13
1.3 – Diagrama ilustrativo do diesel gerador e seus subsistemas	15
2.1 – Número médio de demandas por diesel gerador	21
2.2 – Comparação de falhas por demanda NUREG 4347 x GL 84-15	25
2.3 – Distribuição dos eventos de falha de modo comum	29
2.4 - Distribuição dos eventos de falha de modo comum por subsistema	30
2.5 - Distribuição por subsistema para ação humana como causa raiz	30
3.1 – Diagrama unifilar típico de uma central nuclear	32
3.2 – Sistemas típicos de suprimento de energia elétrica	39
4.1 – Características de falhas do componente	50
4.2 – Estrutura fundamental da árvore de falhas	50
4.3 – Elementos físicos de um evento dependente	52
4.4 – Distribuição de falhas agrupadas por causa raiz	54
4.5 - Distribuição de falhas agrupadas por fator de acoplamento	54
5.1 – Diagrama de blocos do sistema elétrico	63
5.2 – Histograma do número de interrupções de energia	66
5.3 – Evolução do número de interrupções de energia	67
5.4 – Diagrama unifilar da subestação principal	69
5.5 - Diagrama unifilar da cabine primária e da subestação de emergência – 4 DG	72
5.6 – Subestação de emergência com 3 DG	74
5.7 - Subestação de emergência com 2 DG	76
5.8 – Probabilidade de falha humana	80
5.9 – Árvore de falhas para a configuração 4 DG	83
5.10 - Árvore de falhas esquemática para a configuração 3 DG	92
5.11 - Árvore de falhas esquemática para a configuração 2 DG	93

COMISSÃO NACIONAL DE ENERGIA NUCLEAR/SP-IPEN

ANÁLISE COMPARATIVA DA CONFIABILIDADE DE SISTEMAS DE SUPRIMENTO DE ENERGIA ELÉTRICA DE EMERGÊNCIA DE UMA CENTRAL NUCLEAR DE PEQUENO PORTE

1 – INTRODUÇÃO

As centrais nucleares requerem energia elétrica em corrente alternada para executar suas funções de segurança em condições normais de operação e durante ou após a ocorrência de um acidente.

Até o final da década de 60, o foco principal da segurança de reatores nucleares era predominantemente voltada para o núcleo do reator. Após a publicação do estudo efetuado por Rasmunssen e seus colaboradores em 1975, as atenções sobre os problemas de segurança deslocaram-se para os sistemas periféricos das centrais nucleares /1/. Rasmunssen mostra que um dos tipos mais sérios de acidente, num reator tipo PWR – Pressurized Water Reactor, ocorreria se num determinado momento e por um período de tempo de vários minutos, houvesse falha total do suprimento de energia elétrica à central.

Em geral, o sistema elétrico de uma central nuclear é similar ao sistema elétrico de uma central térmica convencional, exceto pela maior preocupação com o suprimento de energia elétrica das cargas necessárias para a operação segura do reator.

A necessidade de fontes de energia independentes e redundantes tem origem nas características que envolvem a operação de reatores nucleares.

O calor do decaimento radioativo, gerado logo após o desligamento do reator, deve ser removido de modo a evitar que o calor gerado eleve a temperatura do núcleo do reator a níveis não permitidos, que poderiam danificar o combustível nuclear.

Acidentes, como a perda de refrigerante ou a falha das bombas de refrigeração do circuito primário, criam a necessidade de fornecimento de refrigeração de emergência provido por bombas e válvulas acionadas por motores que dependem da disponibilidade de eletricidade para a sua operação.

A fonte principal de energia elétrica de uma central nuclear é composta por linhas de transmissão. Na ocorrência de acidentes coincidentes com a perda das linhas de transmissão um sistema de emergência local, em geral composto

COMISSÃO NACIONAL DE ENERGIA NUCLEAR/SP-IPEN

por diesel geradores, tem a função de prover a energia elétrica necessária aos sistemas de segurança e equipamentos necessários para manter o reator numa condição segura.

A autoridade regulatória nuclear exige que seja estudado o comportamento previsto de uma central nuclear em situações normais, transitórias e de acidentes postulados, de modo a se determinar as margens de segurança previstas e a adequação de itens e sistemas para prevenir acidentes e atenuar as conseqüências dos acidentes que possam ocorrer.

Também devem ser objeto de atenção os acidentes com baixa probabilidade de ocorrência, visto que os mesmos podem ser mais severos do que aqueles considerados no projeto.

As condições consideradas neste trabalho, para a avaliação da confiabilidade do sistema elétrico, pertencem ao grupo de acidentes severos, uma vez que a perda do suprimento de energia elétrica em corrente alternada dos barramentos de segurança pode conduzir a um cenário de múltiplas falhas.

Acidentes severos são aqueles associados a cenários de múltiplas falhas, além daqueles considerados na base de projeto, que podem envolver danos substanciais ao núcleo do reator e/ou liberações de produtos radioativos em quantidades que possam afetar a saúde do público e do meio ambiente /2/.

Os estados de uma central nuclear podem ser representados conforme mostrado na Figura 1.1.

Segundo o Safety Series 50-SG-D7 /2/, uma central nuclear pode se enquadrar em duas condições possíveis, a saber: "*Estados Operacionais*" e "*Acidentes*". A condição de "*Estados Operacionais*" pode ser entendida como a operação da central em condições normais e em condições de pequenos desvios das condições normais de operação. A condição de "*Acidentes*" caracteriza que a central opera com desvios das condições normais de operação onde liberações de material radioativo são mantidas dentro dos limites aceitáveis.

Dentro da condição de "Acidentes", a ocorrência de acidentes severos está associada à probabilidade da ocorrência simultânea de múltiplas falhas de sistemas e barreiras de segurança, tornando remota a chance desses cenários considerados "*além-base-de-projeto*". Sua baixa probabilidade não significa que os mesmos não possam ocorrer, devendo-se, portanto, prover medidas ou procedimentos para gerenciar seu curso e mitigar suas conseqüências.

Uma descrição sucinta de cada um dos estados possíveis para uma central nuclear é apresentada na Tabela 1.1 /2/.

A meta, consistente com o objetivo de segurança técnica, para as plantas existentes é que a ocorrência de acidentes com danos severos ao núcleo tenham uma probabilidade de no máximo 10E-04 eventos por ano de operação. A implementação de todos os princípios de segurança, para plantas futuras, devem levar a uma melhora na meta, de forma que a mesma não seja superior a 10E-05 eventos por ano /3/.

Cada central nuclear possui sistemas, componentes e procedimentos que contribuem mais significativamente para a redução do risco de acidentes severos.

A falta de suprimentos de energia adequados, com conseqüente incapacidade dos sistemas de executar as funções de segurança necessárias, pode levar a planta a um cenário de acidente, podendo resultar em liberações inaceitáveis de radioatividade.

Nessa condição, os diesel geradores de emergência desempenham papel de fundamental importância, tendo sido objeto de vários estudos visando melhorar suas características de confiabilidade.

1.1 – Objetivos do Trabalho

Este trabalho tem por objetivo analisar os requisitos aplicáveis para o desenvolvimento de sistemas elétricos de centrais nucleares do tipo PWR, e fazer uma avaliação dos requisitos de confiabilidade do sistema elétrico de um reator nuclear de pequeno porte focando, principalmente, a alimentação externa e o suprimento de energia elétrica em corrente alternada de emergência das cargas relacionadas com a segurança.

Um processo de avaliação probabilística de segurança é realizado em níveis, conforme mostrado na Figura 1.2 /4/. Cada um dos níveis tem objetivos específicos e o resultado da análise desses níveis é uma medida do potencial de risco.

Para a avaliação do sistema diesel de emergência é empregada a técnica da análise através da Árvore de Falhas, utilizada na Avaliação Probabilística de Segurança - Nível 1 /4/, com o objetivo de determinar as freqüências de ocorrência dos eventos indesejáveis.

Foram estudadas três alternativas para a configuração do sistema elétrico de emergência em corrente alternada.

Partiu-se de uma configuração típica, em termos de fontes locais de emergência a qual contempla um diesel gerador dedicado a cada barramento de segurança. Para avaliar a melhora na confiabilidade do sistema elétrico, a segunda alternativa acrescenta um terceiro diesel gerador na configuração anterior, que pode ser conectado a qualquer um dos barramentos de segurança. Pela mesma razão, a terceira alternativa contempla dois diesel geradores dedicados a cada barramento de segurança.

Como fonte externa de energia foi adotada uma linha de transmissão genérica em 88 kV da CPFL – Companhia Piratininga de Força e Luz. Foram obtidos, dados históricos sobre as interrupções do fornecimento de energia sofridos pela linha adotada. Os dados obtidos são comparados a dados do sistema elétrico externo de outras centrais nucleares de modo a avaliar a qualidade do suprimento de energia considerado.

Uma vez tendo a confiabilidade da linha de transmissão, é avaliada a confiabilidade de cada uma das três configurações propostas para o sistema de geração de energia elétrica de emergência em corrente alternada.

1.1.1 – O Diesel Gerador de Emergência

A principal diferença entre as três configurações analisadas é o arranjo adotado para os diesel geradores de emergência. Para melhor avaliar a sua contribuição na confiabilidade do sistema elétrico, o diesel gerador é definido como sendo a combinação do motor diesel e componentes de exaustão, gerador elétrico, excitatriz, disjuntor de saída, sistemas de óleo lubrificante, sistema de resfriamento, sistema de óleo combustível, sistema de ar comprimido de partida e lógica e controle. A Figura 1.3 mostra um diagrama esquemático representativo do diesel gerador sendo apresentado a seguir, uma breve descrição dos principais subsistemas que o compõe.

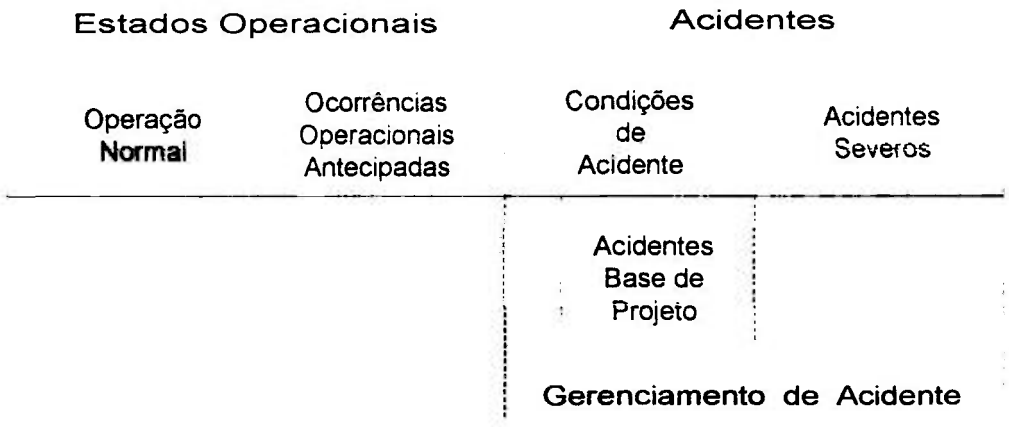


Figura 1.1 Esquema ilustrativo dos estados da planta
Fonte: Safety Series 50-SG-D7 /2/

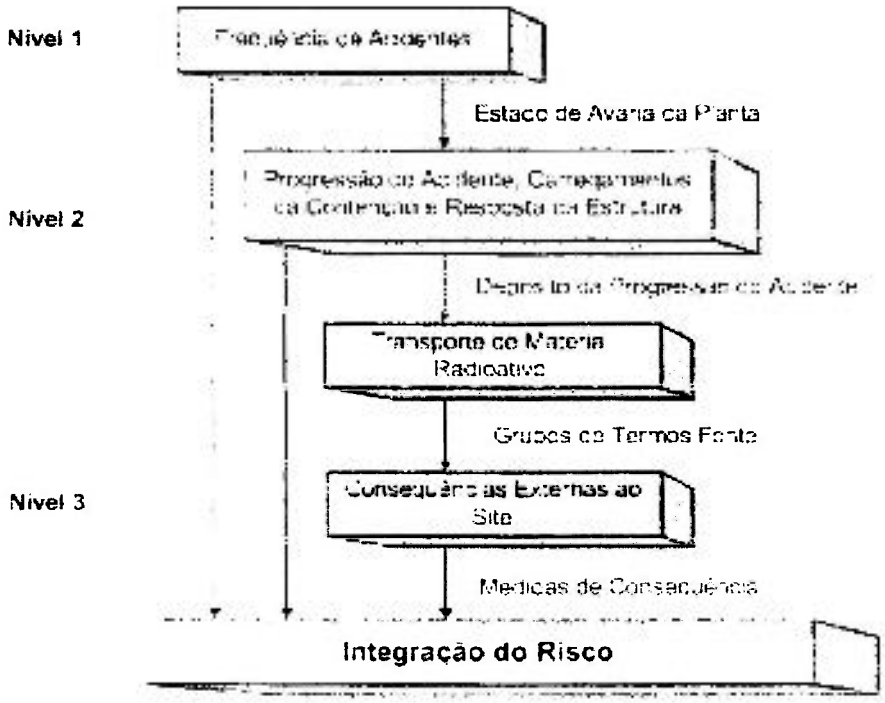


Figura 1.2 Principais passos para o processo de Avaliação Probabilística de Segurança /4/.

Tabela 1.1 – Definição dos estados da planta

Estados Operacionais	Estados definidos na Operação Normal e nas Ocorrências Operacionais Antecipadas.
Operação Normal	Operação da central dentro das condições e limites operacionais especificados.
Ocorrências Operacionais Antecipadas	Todo desvio das condições normais de operação, cuja ocorrência é esperada algumas vezes durante a vida da central, que não causa danos significantes aos itens relacionados com a segurança.
Condições de Acidente	Desvios dos estados operacionais nos quais as liberações de material radioativo são mantidas dentro dos limites aceitáveis por características de projeto apropriadas. Os desvios não incluem Acidentes Severos.
Acidentes Postulados ou Acidentes Base de Projeto	Acidentes considerados como de ocorrência admissível para fins de análise, visando o estabelecimento das condições de segurança capazes de impedir ou minimizar eventuais conseqüências.
Acidentes Severos	Acidentes associados a cenários de múltiplas falhas, além daqueles considerados na base de projeto, que podem envolver danos substanciais ao núcleo do reator e/ou liberações de produtos radioativos em quantidades que possam afetar a saúde do público e do meio ambiente.
Gerenciamento de Acidentes	Execução de uma seqüência de ações: • Durante a evolução da seqüência de um evento, antes que a base de projeto da central seja excedida; • Durante Acidentes Severos sem degradação do núcleo; ou • Depois que uma degradação do núcleo tenha ocorrido para conduzir a central a um estado controlado seguro e mitigar quaisquer conseqüências do acidente.

Fonte: Safety Series 50-SG-D7 /2/

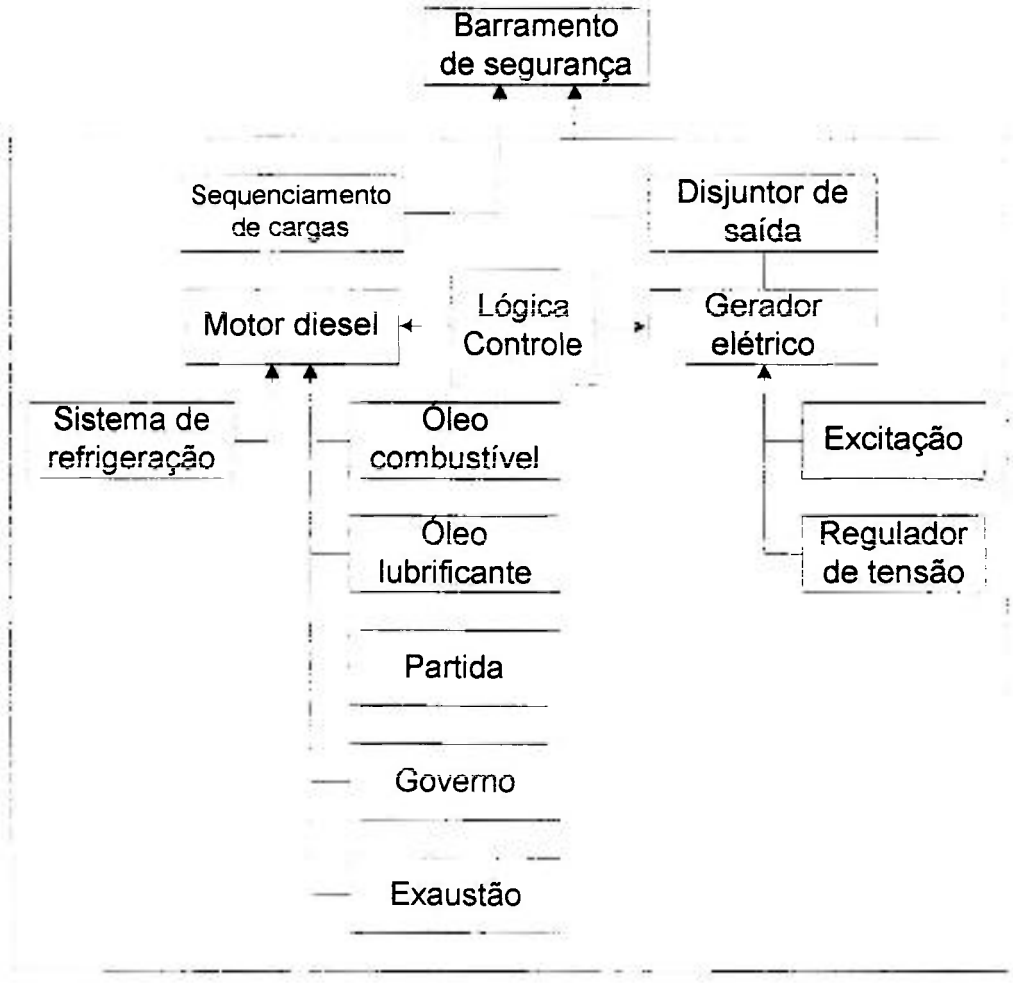


Figura 1.3 – Diagrama representativo do diesel gerador e seus subsistemas

1.1.1.1 – Disjuntor de Saída

O disjuntor inclui o disjuntor de saída principal e o dispositivo de sequenciamento de cargas, o qual controla a ordem e o tempo no qual as cargas de emergência são conectadas ao barramento de segurança.

1.1.1.2 – Sistema de Refrigeração

É um circuito fechado de água dedicado ao motor diesel, tendo tipicamente como meio de resfriamento, a água de serviço de emergência da central. As bombas, trocadores de calor e válvulas são parte desse sistema.

1.1.1.3 – Motor Diesel

O motor diesel é o bloco do motor e todas as partes internas e o governador. O governador mantém a velocidade correta do motor controlando a quantidade de óleo combustível direcionada aos injetores.

1.1.1.4 – Óleo Combustível

Provê o óleo combustível de tanques externos de armazenamento para os tanques diários de cada motor diesel. Os tanques externos têm capacidade para vários dias de operação. Os tanques diários têm, tipicamente, capacidade para 4 a 6 horas de operação.

1.1.1.5 – Gerador

O gerador é composto pela carcaça do gerador, rotor, enrolamentos, excitatriz e regulador de tensão. A função desses componentes é fornecer energia elétrica ao barramento de segurança.

1.1.1.6 – Lógica e Controle

Tem a função de partir, parar, prover o controle operacional e proteger o diesel gerador. Os controles, para diesel geradores, são uma composição de dispositivos elétricos e pneumáticos, dependendo do fabricante.

A avaliação feita ilustra a aplicabilidade da técnica da árvore de falhas como ferramenta de auxílio para o desenvolvimento de sistemas, quantificando as probabilidades de perda das fontes de energia elétrica e identificando os componentes que mais contribuem para a perda de alimentação elétrica em corrente alternada contribuindo, dessa forma, para nortear decisões de projeto quanto ao número de redundâncias e arquitetura do sistema.

1.2 – Organização do Trabalho

O trabalho encontra-se estruturado em sete capítulos. O Capítulo 1 faz uma breve introdução do problema de perda do suprimento de energia elétrica em centrais nucleares e descreve os objetivos do trabalho.

O Capítulo 2 apresenta uma revisão bibliográfica sobre os estudos de confiabilidade de sistemas elétricos anteriormente realizados focando, principalmente, os eventos de perda de alimentação elétrica.

O Capítulo 3 discute as recomendações, diretrizes e guias de projeto, emitidas principalmente por entidades americanas, aplicáveis ao desenvolvimento de projetos de sistemas elétricos de centrais nucleares.

O Capítulo 4 aborda de forma sucinta a utilização da técnica da árvore de falhas como ferramenta para a avaliação da confiabilidade de sistemas e equipamentos. É feita uma explicação resumida da técnica, dos parâmetros que podem ter influência nos resultados e de como proceder para considerar a contribuição de falhas de modo comum na elaboração de uma árvore de falhas.

O Capítulo 5 apresenta um estudo de caso focando o sistema elétrico de uma central nuclear de pequeno porte. A confiabilidade desse sistema é analisada para três arranjos possíveis para os diesel geradores de emergência.

O Capítulo 6 apresenta as conclusões e recomendações elaboradas a partir dos resultados obtidos.

Finalmente, o Capítulo 7 apresenta as normas, os guias, os códigos de projeto, os relatórios e outros documentos consultados durante a elaboração deste trabalho.

2 – HISTÓRICO DA CONFIABILIDADE DAS FONTES DE EMERGÊNCIA

A confiabilidade das fontes de energia elétrica de emergência em corrente alternada de centrais nucleares tem sido questionada devido ao número razoável de falhas dos diesel geradores de emergência relatadas e devido a um eventual dano que o núcleo do reator poderia sofrer caso os diesel geradores falhassem durante uma emergência.

A antiga Comissão de Energia Atômica dos Estados Unidos dirigiu um estudo, WASH 1400 /1/, publicado em 1975, o qual mostrou que a perda total do fornecimento de energia elétrica em corrente alternada poderia ter uma grande contribuição no risco total de acidentes em centrais nucleares. Nesse trabalho foram analisadas diversas seqüências de acidentes possíveis, sendo as conseqüências de cada acidente avaliadas e comparadas a outros acidentes aos quais está sujeito o homem moderno. A probabilidade de falha do sistema elétrico, do ponto de vista de fornecimento de energia elétrica aos dispositivos de segurança, foi calculada usando-se a técnica de árvore de falhas.

Com o decorrer do tempo e com o conseqüente acúmulo da experiência operacional, foi levantada a suspeita de que a confiabilidade das fontes locais de energia elétrica de emergência em corrente alternada e das fontes externas poderia ser menor da originalmente esperada, aumentando a preocupação com o suprimento de energia elétrica.

Em 1979, a NRC – Nuclear Regulatory Commission, declarou a perda de todas as fontes de energia elétrica – "station blackout", como um problema de segurança não resolvido definindo, em julho de 1980, um plano de ações a serem tomadas para determinar a necessidade de requisitos de segurança adicionais incluindo as tarefas listadas abaixo /5/.

1) Estimar a freqüência de ocorrência da perda de todas as fontes de energia elétrica das centrais nucleares em operação no Estados Unidos:
   a) Estimar a freqüência de perda da alimentação externa de várias centrais; e
   b) Estimar a probabilidade de falha das fontes locais em corrente alternada, na ocorrência de uma perda de alimentação externa.

2) Determinar as respostas da central nuclear e o risco associado com as seqüências de acidentes iniciados no caso de perda de todas as fontes de energia elétrica.

A pedido da NRC, o ORNL – Oak Ridge National Laboratory, desenvolveu uma base técnica para auxiliar a resolver o problema de perda de todo suprimento de energia elétrica culminando com a emissão, em julho de 1983, de um estudo sobre a confiabilidade de sistemas de emergência em corrente alternada de centrais nucleares /6/. Esse documento apresenta o resultado dos estudos de confiabilidade das fontes locais de energia elétrica de emergência em corrente alternada, utilizando dados de um total de 120 diesel geradores cobrindo um período entre 1976 e 1980.

Para a execução dos estudos, 18 plantas tidas como típicas quanto aos sistemas locais de energia elétrica em corrente alternada, e dez projetos genéricos foram selecionados para serem modelados por meio de árvores de falhas.

Detectou-se que muitas plantas em operação não tinham metas de confiabilidade para seus diesel geradores de emergência. Considerando o papel crítico que os mesmos desempenham na mitigação de vários transientes e eventos postulados que podem ocorrer durante a perda da fonte externa de energia, foi ressaltada a necessidade de assegurar e manter a confiabilidade dos diesel geradores em níveis aceitáveis.

Segundo esse estudo, os fatores que contribuem para a confiabilidade dos sistemas locais de energia variam de planta para planta, estando entre os mais importantes:

1. Probabilidade de falha dos diesel geradores, para os quais a média da indústria é $2,5 \times 10^{-2}$ e a faixa varia de $8,0 \times 10^{-3}$ a $1,0 \times 10^{-1}$;
2. Erro humano e falha de modo comum do "*hardware*", para os quais a faixa de indisponibilidade varia de $1,0 \times 10^{-4}$ a $4,2 \times 10^{-3}$;
3. Indisponibilidade devido à manutenção programada durante operação do reator para a qual a média da indústria é $6,0 \times 10^{-3}$ e a faixa varia de 0 a $3,7 \times 10^{-2}$;
4. Tempo de reparo do diesel gerador, para o qual a média é 20 horas e a faixa varia de 4 a 92 horas;

5. Indisponibilidade do sistema de água de serviço da planta, para o qual a probabilidade de falha independente é $2,0 \times 10^{-3}$, a probabilidade de falha de modo comum é $8,0 \times 10^{-5}$ e a indisponibilidade devido à manutenção programada é $2,0 \times 10^{-3}$.

O histograma mostrado na Figura 2.1 sumariza as demandas dos diesel geradores de emergência considerados na NUREG/CR-2989 /6/. O histograma não pretende ser conclusivo, mas sim dar uma idéia do número de demandas experimentadas pelos diesel geradores analisados. Para a contabilizar as demandas, foram consideradas as demandas advindas de testes de rotina, testes especiais, verificação de reparos e atuações devidas à injeção de segurança e subtensão nos barramentos.

Como parte do trabalho desenvolvido na NUREG/CR-2989 /6/, foi também determinada a contribuição de cada um dos subsistemas dos diesel geradores no total das falhas apuradas. Para os subsistemas cujas falhas foram mais significativas, foi sumarizada a contribuição de cada componente. A Tabela 2.1 apresenta a contribuição de cada um dos subsistemas do diesel gerador nas falhas detectadas. Como pode ser observado, a soma das falhas de lógica e controle com as falhas do governador, falhas de água de resfriamento e falhas do disjuntor de saída, totalizam aproximadamente 50 % do total das falhas ocorridas.

Para os subsistemas mais representativos, a Tabela 2.2 faz uma quebra dos mesmos em componentes mostrando a sua contribuição nas falhas observadas.

COMISSÃO NACIONAL DE ENERGIA NUCLEAR/SP-IPEN

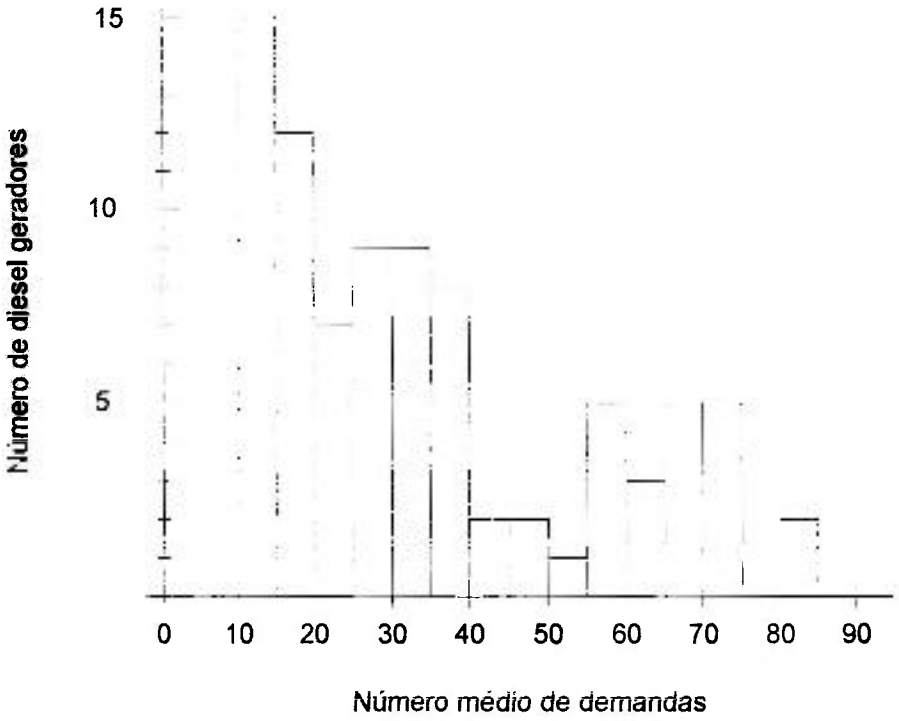


Figura 2.1 – Número médio de demandas por diesel gerador por ano observadas no período de 1976 a 1980 /6/.

Tabela 2.1 - Contribuição dos subsistemas dos diesel geradores nas falhas apuradas

Subsistema	Número de falhas	Porcentagem
Controle e lógica	74	14,7
Governador	62	12,3
Água de resfriamento	60	11,9
Disjuntor de saída e seqüenciador	52	10,3
Ar de partida	46	9,1
Combustível	45	9,0
Desconhecido	35	6,9
Motor diesel	27	5,4
Óleo lubrificante	21	4,2
Excitatriz	19	3,8
Regulador de tensão	14	2,8
Turbo	14	2,8
Ventilação	9	1,8
Humano	7	1,4
Gerador	5	1.0
Exaustão	4	0,8
Partida elétrica	2	0.4
Bateria	2	0,4
Ventilador	2	0.4

Fonte: NUREG 2989 /6/

Tabela 2.2 – Contribuição dos componentes dos subsistemas dos diesel geradores

Componentes de lógica e controle	**Contribuição (%)**
Chaves, relés e fiação	33
Tacômetro	21
Alimentação de controle	12
Geral	34
Componentes do governador	
Sensor e controle	23
Erro de setpoint	20
Óleo contaminado	19
Geral	38
Componentes de água de resfriamento	
Válvulas	25
Entulho	22
Bombas	17
Vazamento tubulação/trocador de calor	14
Geral	22
Disjuntor de saída e seqüenciador	
Relés auxiliares	25
Falha de autofechamento	25
Falha do disjuntor em fechar	22
Falha de controle manual	11
Seqüenciador	11
Geral	6
Componente de Ar de partida	
Válvulas e tubulação	60
Motores a ar	16
Geral	24

Fonte: NUREG 2989 /6/

Uma revisão dos relatórios de ocorrência de falhas gerados pelas centrais licenciadas, para o período de 1976 a 1980, identificou 32 ocorrências de falhas de modo comum atribuídas ao hardware e 88 ocorrências nas quais o erro humano causou a indisponibilidade simultânea de dois ou mais diesel geradores.

A contribuição de falhas humanas é abordada com maiores detalhes no item 4.3.2 deste trabalho.

Levando em conta que, do ponto de vista de segurança, melhorar a confiabilidade dos diesel geradores teria um significante efeito benéfico, a NRC emitiu a Generic Letter 84-15 /7/, em julho de 1984, sugerindo o seguinte:

1) Reduzir o número dos testes periódicos de partida rápida a frio para os diesel geradores de emergência;
2) Solicitar às plantas licenciadas os dados de confiabilidade dos diesel geradores de emergência; e
3) Solicitar às plantas licenciadas o programa, caso existisse, para atingir e manter o nível de confiabilidade dos diesel geradores de emergência.

Todo o esforço despendido no sentido de reduzir os problemas relacionados com os diesel geradores de emergência levou a uma reavaliação dos dados relativos à experiência operacional dos mesmos para o período de 1981 a 1983, resultando na publicação da NUREG 4347 /8/.

O histograma mostrado na Figura 2.2 sumariza os dados de falha de diesel geradores obtidos na reavaliação dos relatórios de ocorrência de falhas e também os dados obtidos como resposta às exigências da Generic Letter 84-15 /7/.

O histograma apresenta os dados separadamente, em termos de porcentagem, porque o período de tempo considerado em cada um dos casos é diferente. Os dados da NUREG 4347 /8/, obtidos através da reavaliação dos relatórios de falhas, vão de 1981 a 1983 enquanto a Generic Letter 84-15 cobriu períodos anteriores a setembro de 1984, nos quais 100 demandas para diesel geradores foram contabilizadas.

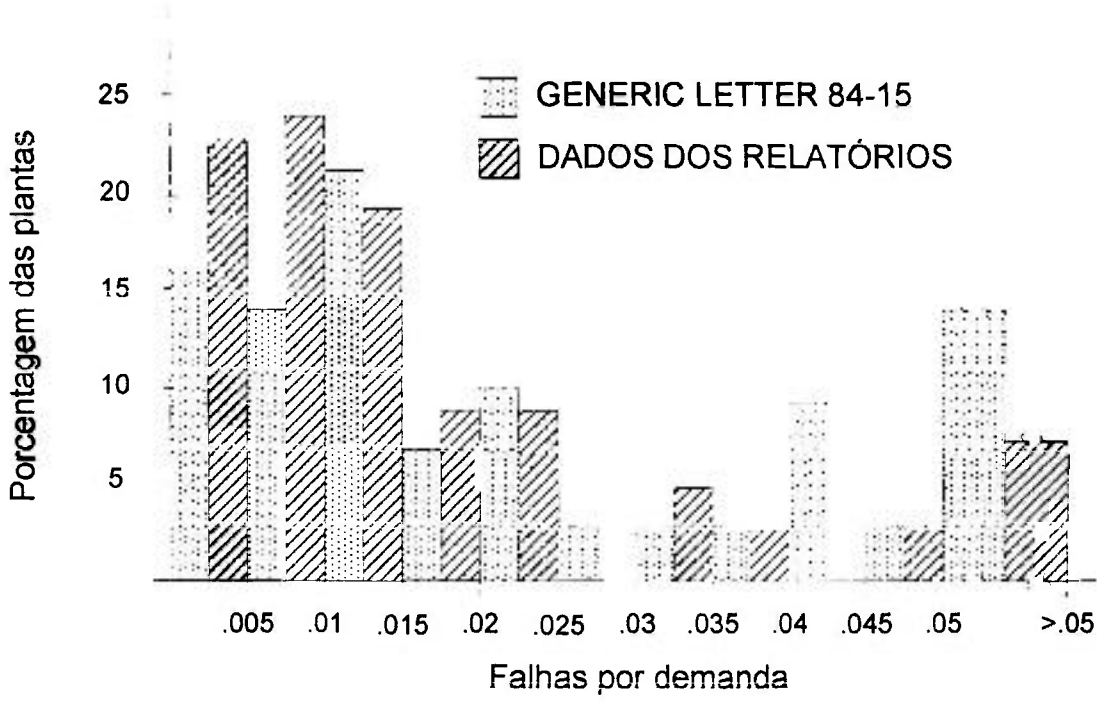


Figura 2.2 - Comparação das falhas por demanda observadas pela NUREG 4347 e Generic Letter 84-15

Fonte: NUREG 4347 /8/

Outro motivo para a não inclusão dos dados deve-se ao fato de que o número de plantas analisadas nos dois casos é diferente e, muitas respostas à Generic Letter 84-15, não descreveram as falhas dos diesel geradores apropriadamente impossibilitando seu uso.

O Anexo A apresenta as falhas por demanda por planta considerados na NUREG 4347 /8/ e na Generic Letter 84-15 /7/.

Em novembro de 1986 foi publicado o relatório da OECD/NEA – "*Loss of Safety System Functions – Pilot Examination of Generic Safety Questions*" /9/ que compila uma série de informações sobre eventos de perda das funções dos sistemas de segurança ocorridos em plantas nucleares dos países membros da Nuclear Energy Agency – NEA.

Duas fontes principais foram utilizadas para compilar as informações pertinentes ao assunto:

- Relatórios dos países membros da NEA que experimentaram eventos de perda de sistemas de segurança; e
- Pesquisa na base de dados da NEA.

Foram consideradas duzentos e oitenta ocorrências das quais cento e noventa e nove são relativas a reatores a água leve e oitenta e uma afetas a reatores a água pesada.

O relatório agrupa os eventos de acordo com os sistemas afetados e os eventos relativos ao suprimento de energia elétrica abordam dois problemas:

- geração de energia elétrica em corrente alternada por grupos diesel geradores de emergência; e
- distribuição de energia elétrica em corrente alternada ou corrente contínua para a instrumentação e controle através dos barramentos vitais.

As falhas de geração de energia elétrica de emergência em corrente alternada por grupos diesel geradores perfazem uma porção considerável dos eventos de perda de sistemas de segurança, tendo sido relatadas quinze ocorrências.

A maior parte dos eventos ocorreu durante a operação em potência e somente três eventos ocorreram durante paradas para troca de combustível.

Nos acidentes ocorridos durante a operação em potência, somente em duas vezes os diesel geradores de emergência foram realmente necessários, nas demais, fontes alternativas de energia estavam disponíveis.

As discussões apontam duas causas principais para a ocorrência de perda de função dos sistemas de segurança devido aos diesel geradores:

- Falha de um diesel gerador enquanto o diesel gerador redundante estava indisponível devido a manutenção; e
- Falha de modo comum dos diesel redundantes.

Sete dos quinze eventos relatados pertencem à primeira categoria, sendo que o diesel gerador em operação falhou cinco vezes devido a uma falha intrínseca e duas vezes por falha humana.

Sete falhas de modo comum dos diesel geradores foram relatadas, tendo as mesmas causado a perda de função dos sistemas de segurança ou contribuído para tal. As falhas observadas foram:

- Trabalhos de modificação executados com documentos errados (listas de cabos e diagramas unifilares/funcionais) tornaram três diesel geradores, do sistema de proteção de segundo nível, inoperáveis. Os diesel geradores falharam em partir na demanda.
- Abertura de chaves erradas, na preparação do teste de partida, (perda do gerador principal e da fonte externa) impediu a partida de quatro diesel geradores.
- Três diesel geradores foram impropriamente borrifados pelo sistema de combate a incêndio.
- Os radiadores dos diesel geradores congelaram devido a adição insuficiente de fluido anti congelante.
- Varas de conexão racharam devido a falha de fabricação.
- Válvulas de verificação defeituosas degradaram a refrigeração do diesel.

Em um dos casos, um diesel disparou devido a uma falha de projeto na lógica de proteção. O mesmo erro estava presente no trem redundante.

Dada a importância dos diesel geradores de emergência como fontes alternativas de energia e a preocupação com a ocorrência de falhas de modo

comum a NEA publicou, em maio de 2000, um relatório que analisa os dados de falha de modo comum visando melhorar o entendimento sobre a ocorrência das mesmas e identificar as medidas que podem ser adotadas para prevenir, ou pelo menos mitigar o efeito das ocorrência de falhas de modo comum em diesel geradores /10/.

Os dados observados cobrem um período que vai de 1982 a 1997 e, dos dados analisados, um total de 106 eventos foram classificados como de falha de modo comum.

A Tabela 2.3 sumariza, por modo de falha, os eventos de falha de modo comum em diesel geradores contemplados no estudo. O grau de falha "*completa*" representa as falhas de modo comum nas quais cada componente falha completamente devido à mesma causa e num pequeno intervalo de tempo. Todos os demais eventos são denominados como "*parcial*". Um subgrupo do grau de falha "*parcial*" é o denominado grau de falha "*quase completa*". Tais eventos são aqueles nos quais todos os componentes falham menos um que fica degradado, sendo que o tempo entre falhas é maior do que o intervalo de inspeção.

As Figuras 2.3 e 2.4 mostram que a falha de modo comum dominante diz respeito ao projeto, manufatura ou construção inadequada e responde por 43 por cento do total dos eventos ocorridos. As figuras mostram, também, que as demais falhas de modo comum estão quase que igualmente distribuídas entre as demais causas.

A Figura 2.5 mostra as falhas por subsistema, considerando a ação humana como causa raiz. Tais ações representam erros de omissão ou operação, ou por parte dos funcionários da central ou por parte dos funcionários de empresas contratadas. Um exemplo típico é a falha em seguir corretamente um procedimento estabelecido. Também estão consideradas ações acidentais, falhas em seguir procedimentos para construção, modificação, manutenção, operação, calibração e teste e treinamento deficiente.

TABELA 2.3 – Sumário das falhas de modo comum dos diesel geradores de emergência.

	Total	Grau de falha observado		
		Parcial	Quase completa	Completa
Falha para rodar	61	46	10	5
Falha para partir	45	22	11	12
Total	106	68	21	17

Fonte: NEA/CSNI/R92000)20 /10/

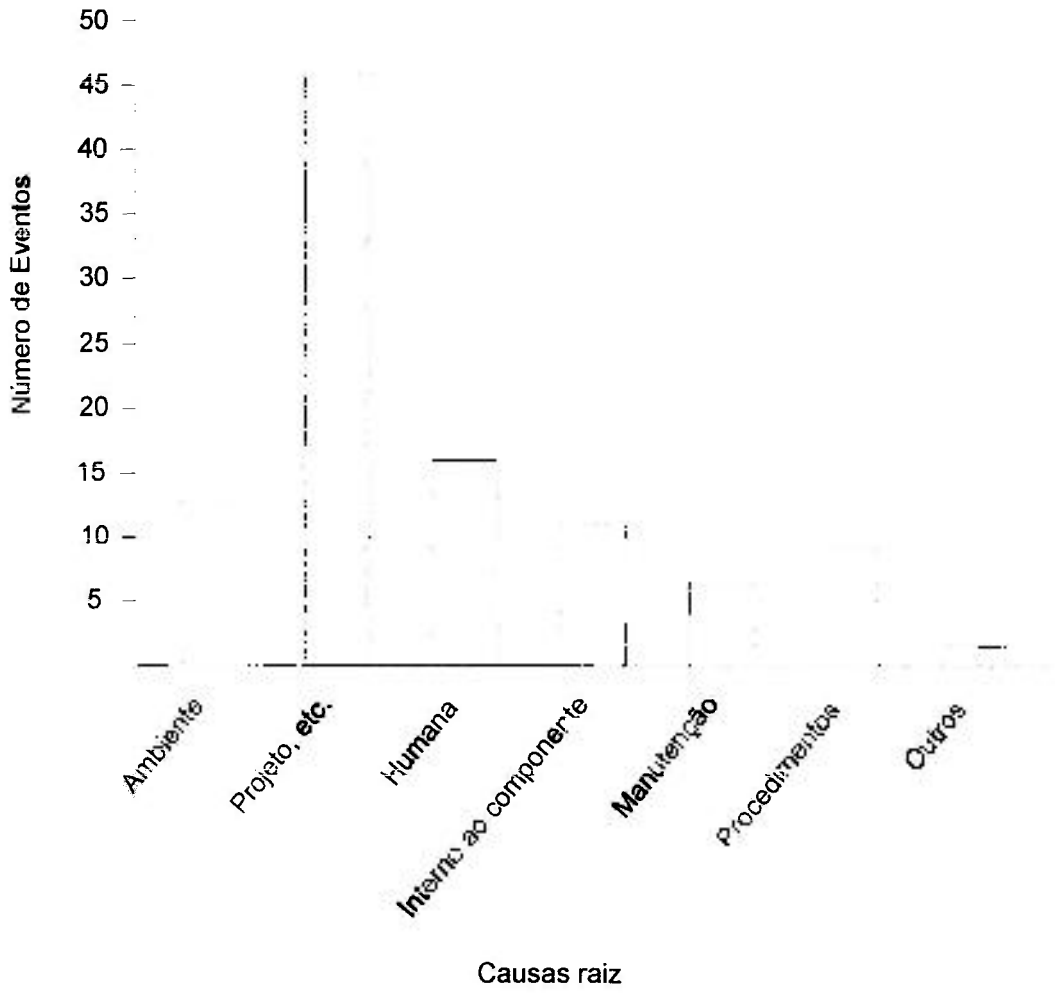


FIGURA 2.3 – Distribuição de eventos de falha de modo comum /10/

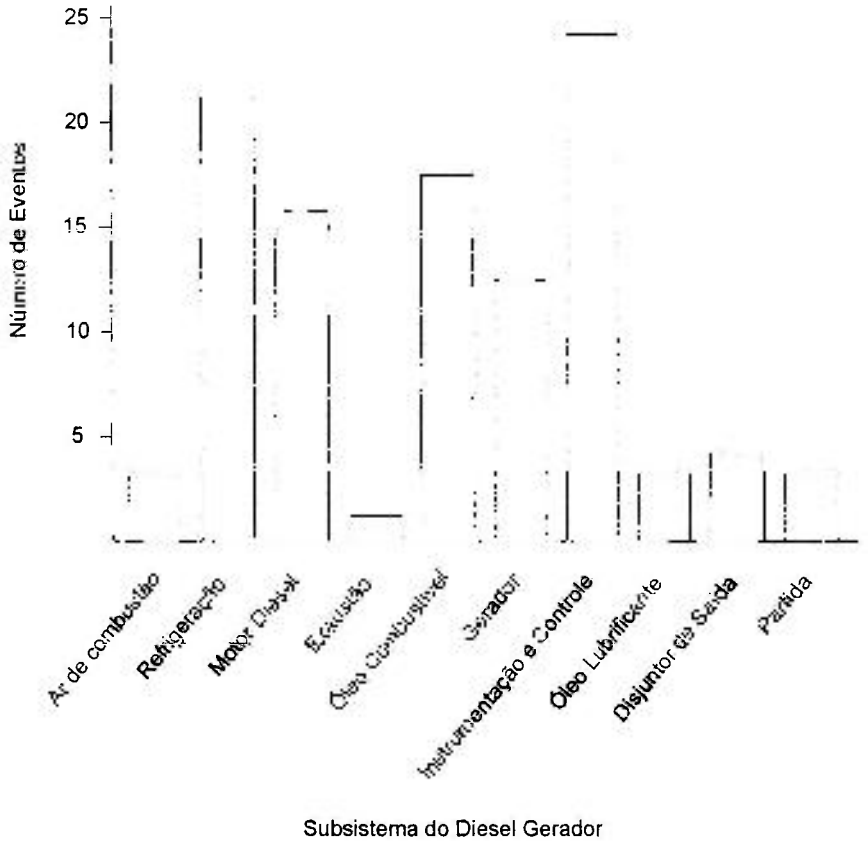


FIGURA 2.4 – Distribuição de eventos de falha de modo comum por subsistema do diesel gerador /10/.

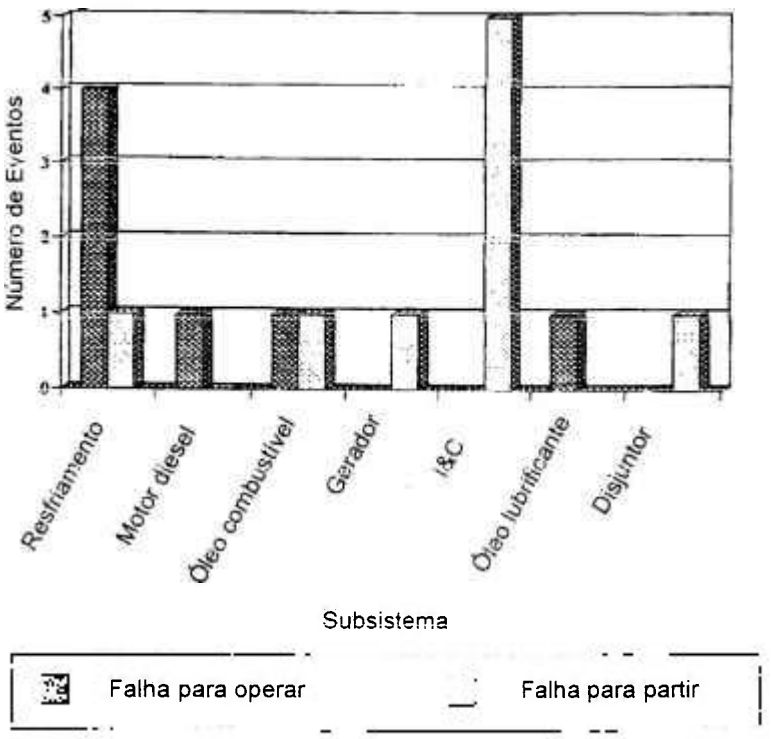


Figura 2.5 Distribuição por subsistema para ação humana como causa raiz /10/

3 – POSIÇÃO REGULATÓRIA

3.1 – Geral

Neste capítulo são abordados os requisitos aplicáveis aos sistemas elétricos de reatores do tipo PWR, sendo discutidos os requisitos do CFR 50 "*Code of Federal Regulations*" /11/, do BNL 50831-II "*Design Guide for Category II Reactors*" /12/ e do 50-SG-D7 "*Emergency Power Systems at Nuclear Power Plants*" /2/.

Tipicamente, durante a operação normal de uma central nuclear, a energia elétrica necessária para a alimentação dos sistemas essenciais e não essenciais provém do gerador principal da central, através de um transformador auxiliar. A energia gerada pela central é entregue à rede de distribuição através do transformador principal. A Figura 3-1 ilustra essa condição, apresentando o diagrama simplificado de uma configuração composta por dois diesel geradores de emergência.

Quando a central não está em operação, as cargas da central são alimentadas pela concessionária através do transformador de partida ou, em alguns casos, pelo transformador principal.

Quase todas as centrais nucleares possuem pelo menos duas fontes de energia elétrica externa para os barramentos de segurança. Em adição, cada central nuclear tem, tipicamente, pelo menos duas fontes locais de energia elétrica de emergência em corrente alternada, normalmente diesel geradores.

Se todas as fontes externas estiverem indisponíveis e houver um problema no gerador principal da central, os barramentos de segurança ficarão desenergizados. Nessa condição, um sinal de falta de tensão comandará a partida automática dos diesel geradores provendo energia elétrica de emergência em corrente alternada para os barramentos de segurança.

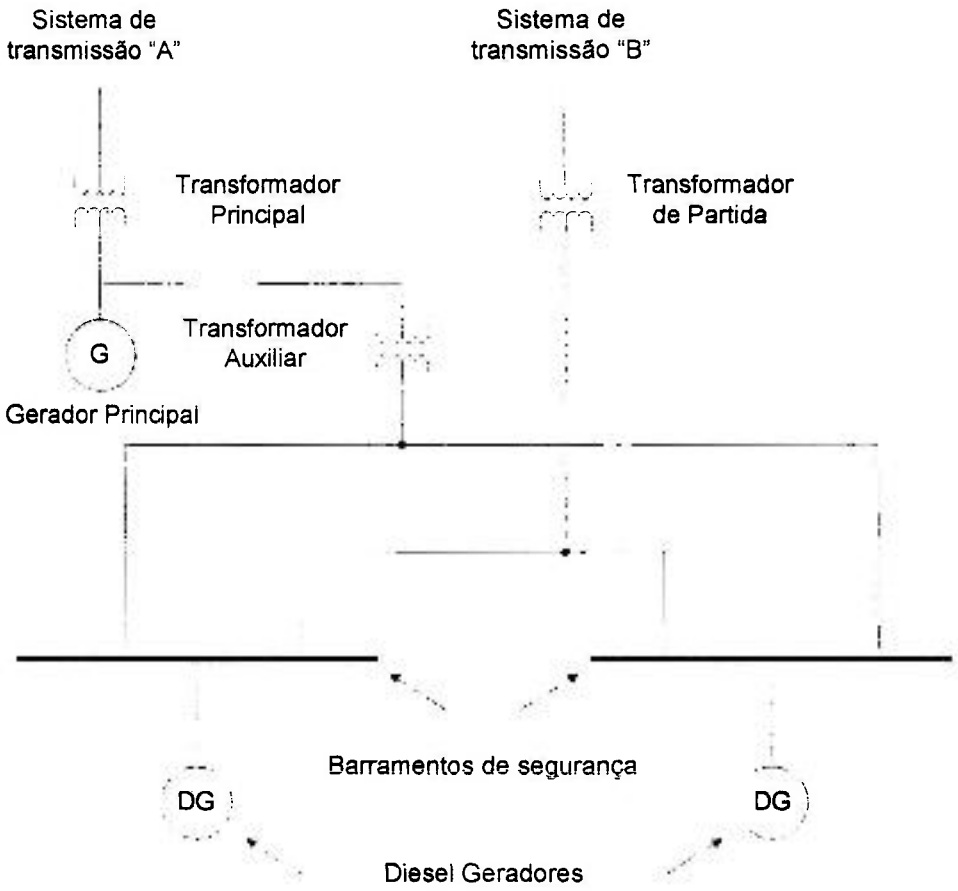


Figura 3-1 Diagrama simplificado do suprimento típico de energia elétrica de emergência em corrente alternada de uma central nuclear /5/

3.2 - Requisitos

O nível de confiabilidade do sistema elétrico de uma central nuclear depende de uma série de fatores. A localização da central, por exemplo, pode dar indicações quanto à sua susceptibilidade a eventos iniciadores postulados naturais e induzidos pelo homem.

De forma a minimizar a ocorrência de acidentes ou condições indesejáveis, o sistema elétrico de uma central nuclear deve atender a uma série de recomendações e diretrizes que se constituem nos requisitos mínimos a serem atendidos para garantir a segurança operacional da central.

3.2.1 – CFR-50

O CFR-50, "*Code of Federal Regulations, Title 10 – Energy, Part 50 – Domestic Licensing of Production and Utilization Facilities*", Apêndice A *[11]* é o documento que define os requisitos mínimos para o direcionamento de projetos de sistemas elétricos de centrais nucleares nos Estados Unidos, de modo que estas possam obter sua licença de operação. Seus requisitos visam, também, determinar procedimentos de projeto, fabricação e testes para todos os sistemas importantes à segurança da central, de modo a minimizar os riscos para a saúde e segurança do público e dos operadores da central.

O 10-CFR-50 em seu critério 17 estabelece que:

1. Um sistema elétrico interno e um sistema elétrico externo devem possibilitar o funcionamento de estruturas, sistemas e componentes importantes para a segurança. O sistema elétrico externo compreende as linhas de transmissão que interligam a instalação nuclear à rede de distribuição de energia da concessionária. O sistema elétrico interno é composto por um subsistema de energia elétrica em corrente alternada, um subsistema de energia elétrica em corrente contínua e um subsistema de energia elétrica em corrente alternada no-break.
2. A função de segurança de cada sistema elétrico, supondo-se que o outro não esteja funcionando, deve ser a de prover meios que assegurem capacidade e dimensionamento suficientes para que:

- O limite aceitável especificado para o combustível e o limite máximo de projeto para a pressão do líquido refrigerante do reator não sejam excedidos devido a ocorrências operacionais esperadas; e
- O resfriamento do reator, a manutenção da integridade da contenção e outras funções vitais sejam mantidas na eventualidade de ocorrência de eventos básicos de projeto.

3. Os sistemas de energia elétrica interno e externo devem possuir características de independência, redundância, e capacidade comprovada para desempenhar as funções de segurança para as quais foram projetados quando da ocorrência de uma falha simples. Os sistemas redundantes devem ser alimentados por circuitos fisicamente independentes, projetados e localizados de modo a minimizar a probabilidade de falhas simultâneas e de acidentes postulados.
4. A energia suprida pelo sistema elétrico externo deve ser fornecida por duas linhas de transmissão fisicamente independentes entre si, projetadas e construídas de modo a minimizar a possibilidade de sua falha simultânea em condições de operação, acidentes postulados ou condições ambientais adversas. Uma subestação comum a ambos circuitos é aceitável. Cada uma das linhas deve ser projetada para estar disponível, em tempo adequado, após a perda de todas as fontes do sistema elétrico interno e da outra linha de transmissão de modo a assegurar que os limites do reator não sejam excedidos. Uma das linhas de transmissão deve ser projetada de modo a estar disponível poucos segundos após a ocorrência de um acidente de perda de refrigerante "*LOCA – Loss of Coolant Accident*" de modo a garantir que o resfriamento do núcleo, a integridade da contenção e outras funções vitais de segurança sejam mantidas.
5. Devem ser tomadas precauções de modo a minimizar a probabilidade de perda de energia elétrica de qualquer um dos suprimentos remanescentes como resultado de, ou coincidente

com, a perda da energia elétrica gerada pelo reator, perda do sistema de elétrico externo, ou a perda de algumas fontes do sistema elétrico interno.

3.2.2 - BNL 50831-II

No caso particular das centrais pertencentes ao DOE – *"Department of Energy"* dos Estados Unidos, o projeto dos sistemas elétricos, além das recomendações do 10-CFR-50, deve seguir as recomendações do "BNL 50831-II *Chapter 8 – Electric Power – "Design Guide for Category II Reactors" - Light and Heavy Water Cooled Reactors, Brookhaven National Laboratory"* /12/, descritas abaixo:

1. Um sistema elétrico classe 1E deve ser providenciado para sistemas e equipamentos classificados, se a eletricidade é requerida para a execução de determinada função de segurança. Os sistemas com alimentação 1E geralmente incluem aqueles necessários para a refrigeração e o desligamento seguro do reator e aqueles que previnem uma emissão descontrolada de radiação.
2. O sistema deve ser projetado com a adequada redundância e separação de componentes redundantes de forma a assegurar a adequada capacidade e o perfeito funcionamento durante um acidente postulado com a adição de uma falha simples no sistema elétrico classe 1E.
3. As porções 1E do sistema elétrico devem ter classificação sísmica devendo ser qualificados em conformidade com as recomendações do BNL 50381-II, Seção 3.10.
4. O sistema deve ser projetado e qualificado para permanecer operacional, nas condições ambientais previstas para o local onde a central está instalada, por um período de tempo suficiente para assegurar que todas as funções de segurança requeridas sejam completadas.
5. As fontes reserva do sistema elétrico interno, as quais fornecem energia classe 1E, devem ser adequadamente separadas (por exemplo; através de transformadores e disjuntores) do sistema elétrico externo, o qual normalmente provê energia elétrica para a

planta, e de outras porções não 1E do sistema elétrico interno da central.

6. As cargas não 1E, as quais podem ser alimentadas a partir de um barramento 1E, devem ser dotadas de dispositivos adequados para assegurar sua desconexão durante emergências.

3.2.3 - 50-SG-D7 - Agência Internacional de Energia Atômica

Em complemento aos Guias e Códigos de Projeto, a Agência Internacional de Energia Atômica – IAEA implantou em 1974, um programa de normas de segurança "NUSS – *Nuclear Safety Standards*" visando dar diretrizes sobre vários aspectos de segurança de reatores nucleares.

Em particular, o Safety Series 50-SG-D7 – *Emergency Power Systems at Nuclear Power Plants* [2] é aplicável a usinas nucleares nas quais a fonte de energia elétrica compreende um suprimento de energia elétrica normal, no caso a concessionária, e um suprimento de energia elétrica de emergência local, estabelecendo considerações e diretrizes gerais que podem ser de grande auxílio na configuração do sistema elétrico.

3.2.3.1 – O Sistema Elétrico Externo

O 50-SG-D7 recomenda que seja executada uma avaliação da rede elétrica da concessionária de forma a verificar as condições de estabilidade da mesma. Onde a estabilidade for baixa, medidas para aumento da estabilidade devem ser consideradas ou, se viável, um local alternativo com uma rede de distribuição de alta estabilidade deve ser selecionado.

A estabilidade da rede é função de vários parâmetros. Eles incluem:

1. o sistema de geração e a reserva de geração durante os períodos de pico e fora de pico;
2. o número e o porte das unidades de geração e suas características;
3. o número e as características das conexões a outros sistemas de distribuição; e
4. o número de linhas de transmissão e suas características, incluindo as características dos relés e disjuntores de proteção.

De particular importância é o fato de que a perda da maior unidade de geração do sistema interligado pode resultar numa instabilidade da rede da

concessionária, levando a um colapso total do sistema tornando indisponível a fonte externa de energia da central em consideração.

É dito que uma conexão simples pode ser aceitável em situações onde a central nuclear contribui com uma grande parte da geração do sistema interligado ou onde a estabilidade da rede é tal que a perda da planta nuclear ocasionaria o colapso da rede. Nessas condições, a inclusão de uma segunda linha pouco acrescentaria à confiabilidade do sistema, sendo necessária a adoção de outras medidas internamente à planta.

Onde a geração da central nuclear é uma pequena porção da geração total e a rede é considerada estável, mesmo depois da perda da planta em questão, a solução preferida é prover pelo menos duas conexões de transmissão entre a planta e a rede. Onde mais de uma linha de transmissão é utilizada para conectar a central à rede, deve-se atentar para a separação adequada das mesmas ou até mesmo a conexão a diferentes partes da rede que sejam relativamente independentes de forma a evitar falhas de modo comum das mesmas.

O uso de mais de duas conexões à rede pode não resultar em aumento de confiabilidade a menos que as conexões possam ser feitas em diferentes pontos da rede. Entretanto, para plantas localizadas longe da rede, pode não ser prático utilizar mais de uma linha de transmissão.

Centrais nucleares alimentadas por uma única linha de transmissão podem ter uma taxa de queda maior devido a um colapso da linha. Isso é particularmente importante em áreas onde a freqüência de descargas elétricas na linha é alta. Em tais casos, ou a central nuclear deve ser projetada para suportar os efeitos das quedas, ou medidas devem ser tomadas para reduzir o número das mesmas, provavelmente acrescentando-se uma linha de transmissão adicional.

3.2.3.2 – O Sistema Elétrico Local

Tipicamente, em condições normais de operação, o suprimento de energia elétrica para os sistemas de uma central nuclear é fornecido pelo próprio gerador da usina.

No caso de indisponibilidade ou do sistema elétrico externo ou do gerador da usina, um sistema elétrico de emergência deve prover a energia necessária para as cargas importantes para a segurança.

3.2.3.2.1 - O Sistema Elétrico de Emergência

Sistemas de energia elétrica de emergência são parte integral dos sistemas de segurança e servem como retaguarda para os sistemas de segurança para o propósito de suprir e distribuir energia elétrica aos sistemas de segurança e a outros itens tidos como importantes para a segurança. Para executar as funções de segurança necessárias para os diferentes eventos iniciadores postulados, os sistemas de segurança são providos numa variedade de formas e arranjos, e com várias combinações de redundância e diversidade.

O propósito dos sistemas de energia elétrica de emergência é prover a planta com a necessária energia em todas as condições relevantes dentro das bases de projeto de forma que a planta possa ser mantida num estado seguro depois da ocorrência de eventos iniciadores postulados, em particular durante a perda do suprimento de energia elétrica externo. Os sistemas de energia elétrica de emergência também podem ser efetivos para algumas condições além da base de projeto.

A Figura 3.2 apresenta um esquema dos sistemas típicos de suprimento de energia elétrica de emergência.

O sistema elétrico de emergência é geralmente subdividido em três tipos de sistemas elétricos, conforme os diferentes requisitos de alimentação das cargas.

Esses sistemas são:

1. Um sistema elétrico de emergência em corrente alternada cujas cargas suportam um pequeno período de interrupção de energia. No caso de perda de energia, o sistema é acionado e carregado obedecendo à prescrição de uma seqüência temporal;
2. Um sistema elétrico de emergência em corrente contínua, cujas cargas não suportam interrupção de energia; e
3. Um sistema elétrico de emergência, tipo no-break, para cargas em corrente alternada que não suportam interrupção de energia.

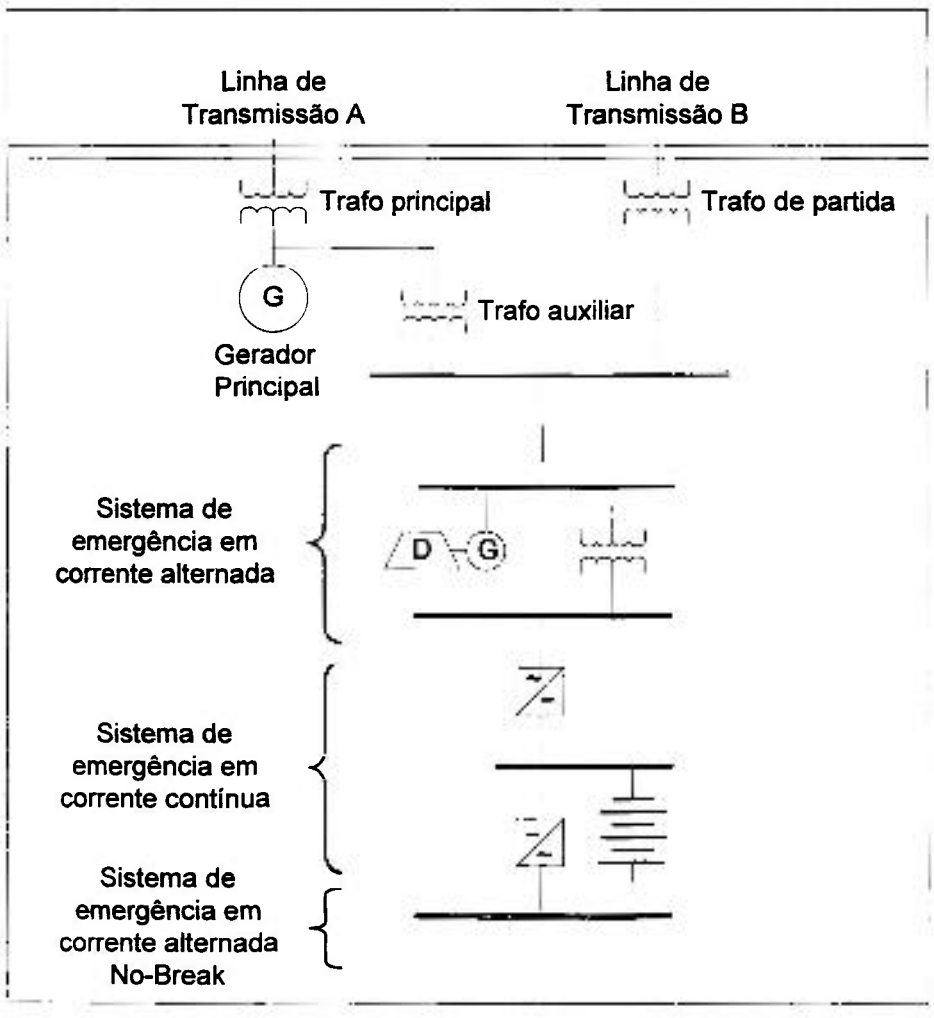


Figura 3.2 – Representação esquemática dos sistemas típicos de suprimento de energia elétrica de emergência /2/.

O sistema elétrico de emergência em corrente alternada deve consistir de uma unidade geradora completa com todos os seus sistemas auxiliares. Tal sistema deve ter capacidade suficiente para partir e alimentar todas as cargas sob ocorrências operacionais antecipadas e em condições de acidente, conforme especificado nas bases de projeto.

Os requisitos a serem atendidos para determinação da capacidade da unidade geradora são:

1. Confiabilidade da partida;
2. Tempo para partir e assumir as cargas na seqüência especificada;
3. Características de performance incluindo operação em vazio, na partida, em carga nominal e operação nos ciclos de sobrecarga; e
4. Capacidade de operação em degraus de cargas em toda faixa de cargas. (manter a tensão e a freqüência dentro dos limites que não degradem a performance das cargas alimentadas, mesmo durante transientes causados pela adição da maior carga ou remoção de carga).

Tipicamente, cada planta nuclear possui internamente, como retaguarda, pelo menos duas fontes de energia elétrica em corrente alternada, normalmente diesel geradores.

Os diesel geradores tem classificação de segurança, provendo energia de emergência confiável aos barramentos elétricos que suprem o sistema de refrigeração de emergência do núcleo e a vários outros equipamentos necessários para o desligamento seguro da planta.

Em geral, o diesel gerador de emergência assegura que a energia elétrica adequada esteja disponível no caso de perda da fonte externa, com ou sem a ocorrência simultânea de um LOCA.

Os diesel geradores de emergência ficam normalmente em espera, esteja a planta operando ou desligada. Um sinal para partida do diesel gerador de emergência é disparado na ocorrência de um acidente de perda de refrigerante ou na perda ou degradação da energia elétrica nos barramentos de segurança.

A energização das cargas do barramento de segurança é feita de forma seqüencial e temporizada permitindo que o diesel gerador possa assumir e manter todas as cargas necessárias nessa condição.

COMISSÃO NACIONAL DE ENERGIA NUCLEAR/IEN

3.2.4 – ABNT-NBR 8671

Em âmbito nacional, a NBR 8671 – Requisitos Gerais de Suprimento de Energia Elétrica para os Sistemas de Segurança de Usinas Nucleoelétricas /13/, fixa os requisitos gerais a serem atendidos no projeto de sistemas de suprimento de energia elétrica para sistemas de segurança.

São feitas as seguintes exigências com relação às possibilidades de suprimento de energia:

1. Possibilidade de suprimento interno de energia através do gerador da central;
2. Duas possibilidades de suprimento externo de energia; e
3. Sistema de suprimento de emergência com geração independente de energia.

É exigido que o suprimento de energia para os sistemas de segurança seja projetado com uma confiabilidade tal que o mesmo não seja o fator determinante para a não disponibilidade dos sistemas a serem supridos.

A NBR 8671 exige que seja assegurado que os diesel geradores de emergência somente sejam necessários no caso de indisponibilidade simultânea do suprimento de energia externo e interno.

Quanto à conexão do sistema elétrico da central à rede da concessionária, a NBR estabelece as condições mínimas mostradas na Tabela 3.1. O disposto na Tabela 3.1 não se aplica se:

1. Para cada uma das possibilidades de suprimento externo, dois transformadores são instalados, sendo um deles dimensionado para suprir as cargas de emergência, ou
2. Puder ser demonstrado que, dentro dos limites permissíveis de tempo, uma possibilidade adicional de suprimento externo para as cargas de emergência possa vir a ser disponível.

Em caso de ocorrência de eventos onde é assumida a falha simultânea por longo período de tempo de todas as alimentações externas, deve ser instalada uma possibilidade de suprimento diferente e independente do sistema de suprimento de emergência, projetada para suprir as cargas de segurança após três dias. /13/

Tabela 3.1 – Limites de tempo para restabelecimento do suprimento externo

Número de possibilidades de suprimento externo	Tempo máximo permitido para restaurar possibilidades de suprimento externo defeituosas	Número mínimo de possibilidades de suprimento externo após medidas de restauração
2	Sem restrições	> 2
1	≤ 14 dias	2
0	≤ 3 dias	1

Fonte: ABNT-NBR-8671 /13/

3.2.5 - CNEN

Tem sido prática da CNEN - Comissão Nacional de Energia Nuclear, na avaliação independente do Relatório de Análise de Segurança, orientar-se pelos requisitos e estrutura da NUREG 0800 "*Standard Review Plan*". O documento em questão, no seu Capítulo 8, estabelece os critérios de aceitação e as diretrizes para os sistemas elétricos.

Além dos requisitos específicos para o projeto de sistemas elétricos contemplados na NBR-8671 /13/ e na NUREG 0800 /14/, a CNEN - Comissão Nacional de Energia Nuclear tem importantes publicações, entre as quais pode-se citar a "NE - 1.04 - Licenciamento de Instalações Nucleares" /15/ e a "NN - 1.16 Garantia da Qualidade para Segurança de Usinas Nucleoelétricas e Outras Instalações" /16/.

A NE – 1.04 estabelece o processo de licenciamento de instalações nucleares aplicado às atividades relacionadas com a localização, a construção e a operação de tais instalações, abrangendo as seguintes etapas:

1. aprovação de local;
2. licença de construção (total ou parcial);
3. autorização para utilização de materiais nucleares
4. autorização para operação inicial
5. de autorização para operação permanente
6. cancelamento da autorização para operação

São apresentadas as informações mínimas que devem estar contidas no relatório preliminar de análise de segurança a ser elaborado visando à emissão da licença de construção, bem como as informações que devem estar contidas no Relatório Final de Análise de Segurança (RFAS), o qual, juntamente com o plano de proteção física, constituem os documentos básicos para a emissão da Autorização para Operação Inicial.

O RFAS deve descrever a instalação, apresentar as bases de projeto, as especificações técnicas, os limites de operação e uma análise de segurança da instalação como um todo, devendo incluir o programa de monitoração ambiental e meteorológica, o programa de garantia da qualidade, o plano de proteção contra incêndio e o plano de emergência, entre outros.

A NN - 1.16 /16/ determina os requisitos a serem adotados para o estabelecimento e implementação de Sistemas de Garantia da Qualidade para usinas nucleoelétricas, instalações nucleares e, conforme aplicável, também para instalações radiativas. Determina a forma segundo a qual os Programas de Garantia da Qualidade devem ser preparados e submetidos à CNEN.

Ela é particularmente aplicável às atividades que influem na qualidade de itens importantes à segurança, desenvolvidos no gerenciamento do empreendimento e em cada um dos seus diversos estágios: escolha de local, projeto, construção, comissionamento, operação e descomissionamento.

3.3 – Observações sobre a Base Normativa

Um grande número de centrais foi construída, principalmente nos Estados Unidos, obedecendo aos guias e códigos de projeto descritos nos itens anteriores.

Uma análise dos guias e códigos aplicáveis ao desenvolvimento de projetos elétricos mostra que todos eles contemplam, de forma mais ou menos abrangente, os principais critérios de projeto, as principais recomendações e condições de contorno a serem observadas.

Um sistema elétrico externo composto por duas linhas de transmissão fisicamente independentes entre si é uma exigência comum.

O 50-SG-D7 /2/ estabelece que uma única linha de transmissão pode ser aceitável nos casos onde a central contribui com uma grande parte da geração do sistema interligado ou onde a estabilidade da rede é tal que a perda da central ocasionaria o colapso da rede. Nestes casos, é recomendado que o sistema elétrico interno seja projetado para suportar os efeitos da perda da alimentação externa.

Os requisitos de redundância e separação física também são comuns a todos os guias códigos. O mesmo se aplica para os requisitos de qualificação de componentes e equipamentos.

A exigência de um sistema elétrico de emergência também é abordada em todos os guias códigos. A ABNT-NBR-8671 /13/ faz uma exigência adicional em caso ocorra a perda simultânea de todas as alimentações externas, por um longo período de tempo.

Nesse caso, é recomendado que haja uma possibilidade de suprimento de energia elétrica diferente e independente do sistema elétrico de emergência, projetada para suprir as cargas de segurança, após três dias.

Essa recomendação exige especial atenção aos requisitos de redundância e segregação das penetrações de cabos e dutos de cabos que conduzem às cargas de segurança, de forma a protegê-las contra a ocorrência de eventos.

Em resumo, os guias e códigos vistos são suficientes para direcionar um projeto elétrico voltado para o atendimento aos requisitos de confiabilidade e disponibilidade.

4 – MÉTODO DE AVALIAÇÃO DA CONFIABILIDADE

4.1 – Considerações Gerais

A confiabilidade de um sistema, item ou componente pode ser definida como sendo a probabilidade de que o mesmo execute a função para a qual foi projetado, por um período de tempo determinado.

Quando se fala em confiabilidade, os sistemas podem ser classificados como *reparáveis* ou *não reparáveis*. Componentes eletrônicos em geral são *não reparáveis,* posto que são sempre substituídos ao apresentarem falhas. Já uma placa de circuito impresso pode ser *reparável* ou *não reparável,* dependendo da política de manutenção adotada.

Sistemas redundantes são normalmente *reparáveis*, uma vez que a unidade redundante mantém o nível operacional do sistema, a despeito de alguma unidade estar sob reparo.

A análise de confiabilidade de um sistema consiste, basicamente, na investigação do potencial de falha do sistema e na avaliação das conseqüências dessas falhas.

Através da análise de confiabilidade é possível obter informações importantes a respeito da performance de sistemas e equipamentos levando à implementação de melhorias, ainda durante a fase de projeto, evitando que eventuais alterações sejam efetuadas no futuro, a um custo bastante alto.

Admite-se que a confiabilidade do sistema seja máxima no instante em que o sistema começa a operar, isto é, admite-se que o sistema esteja funcionando corretamente no início da operação.

O método utilizado neste trabalho, para a análise da confiabilidade, é a técnica da árvore de falhas. Essa técnica tem sido essencial em estudos de análise probabilística de segurança de instalações nucleares e tem apresentado grande aplicabilidade em estudos de análise de risco realizados para as indústrias de processos químicos /1/.

Os principais conceitos empregados neste trabalho são descritos a seguir.

4.2 – Árvore de Falhas

4.2.1 – Fundamentos

A análise através da árvore de falhas foi concebida em 1961, por H. A. Watson dos laboratórios Bell Telephone, atendendo a um contrato com a Força Aérea Americana, para o estudo do sistema de controle de lançamento dos mísseis "Minuteman". Em 1965, durante um simpósio de segurança patrocinado pela Universidade de Washington e pela Boeing Company, vários trabalhos ressaltaram a importância da análise através da árvore de falhas ressaltando seu potencial como ferramenta para o estudo da confiabilidade de sistemas complexos /28/.

Esta técnica permite que sejam identificadas, através de uma investigação lógica e sistemática, as falhas de um sistema que possam desencadear um evento indesejável ou evento catastrófico, além de permitir que seja calculada a probabilidade de ocorrência do evento.

A árvore de falhas pode ter um enfoque apenas qualitativo, como também quantitativo, dependendo da fase de evolução do projeto e do propósito da análise. Se o propósito da análise for o de identificar as falhas que possam ocorrer no sistema, uma avaliação qualitativa será suficiente. Por outro lado, se o propósito for determinar as características de confiabilidade do sistema, como indisponibilidade, confiabilidade, etc., uma avaliação quantitativa é imprescindível.

Na construção de uma árvore de falhas parte-se da definição de um evento de falha indesejável e, através da análise de relações causais, procura-se descobrir as combinações de eventos que levam à ocorrência do evento indesejável. Esses eventos podem estar relacionados com falhas intrínsecas do sistema, também denominadas falhas independentes ou de "hardware", erros humanos ou quaisquer outros eventos pertinentes, que possam conduzir ao evento indesejável ou evento topo.

Os modos, os efeitos e os mecanismos de falhas são importantes na determinação das relações de causa e efeito entre os eventos.

As falhas dos componentes de um sistema são os elementos chave na análise de relações causais e podem ser classificadas como falhas primárias, falhas secundárias ou falhas de comando /17/. A Figura 4.1 ilustra essa classificação.

A falha primária é caracterizada pela falha de um equipamento ou componente em um meio para o qual o mesmo foi qualificado, ou seja, cujas condições de operação não excedem as condições limite de projeto. Um exemplo típico é a falha devido ao desgaste natural. A falha secundária é caracterizada pela solicitação excessiva do equipamento ou componente, fazendo com que as condições de operação ultrapassem os limites de projeto. A ocorrência de tal situação pode ser atribuída aos equipamentos e componentes vizinhos, ao ambiente ou ao pessoal de operação. Uma falha de comando envolve a operação indevida de um equipamento ou componente. Tal ocorrência é característica de sinais inadvertidos ou de ruído eletromagnético.

São descritas nas próximas seções algumas características e conceitos utilizados na elaboração de uma árvore de falhas. Não é objetivo desta dissertação desenvolver em detalhes os aspectos teóricos ligados à quantificação das árvores. O leitor interessado poderá obter essas informações em textos clássicos como Kumamoto /17/ e McCornick /28/.

4.2.2 – Elementos Básicos de uma Árvore de Falhas

A árvore de falhas é estruturada de forma que a seqüência de eventos que leva ao evento topo é representada, abaixo deste, pela combinação de portões lógicos. Os eventos de entrada de cada portão lógico são também eventos de saída de portões lógicos de níveis inferiores, sendo desenvolvidos até se chegar aos eventos terminais da árvore chamados de eventos básicos. Os eventos básicos são os limites de resolução da árvore e são as causas de interesse para a ocorrência do evento indesejável. A Figura 4.2 apresenta a estrutura fundamental da árvore de falhas.

Um portão lógico resume uma relação de causa e efeito. Os eventos causa constituem as diferentes entradas do portão lógico, que tem como saída um único efeito que é o resultado da combinação lógica dos eventos de entrada. O Anexo B mostra os símbolos empregados para a representação dos portões lógicos, eventos e sua descrição.

A elaboração de uma árvore de falhas exige o conhecimento detalhado do sistema a ser analisado, seus componentes, tipos de falhas, possíveis interações entre os componentes do sistema, ações do operador, etc. Na área

nuclear, a NUREG 0492 – Fault Tree Handbook /29/ é uma das referências mais utilizadas para a construção e análise de árvores de falhas.

4.2.3 – Cortes Mínimos

Uma árvore de falhas, além de fornecer uma compreensão detalhada do sistema, permite a identificação das combinações de falhas que levarão à ocorrência do evento topo. Esse processo é conhecido como *análise dos cortes*.

Um corte é definido como um conjunto de eventos cuja ocorrência simultânea acarreta a ocorrência do evento topo. Um corte é dito *mínimo* quando é constituído pelo menor número possível de eventos cuja ocorrência simultânea acarreta a ocorrência do evento topo.

Para árvores de falhas com algumas dezenas de eventos básicos e de portões lógicos, a determinação dos cortes mínimos através da simples análise pode ser difícil. Nestes casos, meios formais de determinação dos cortes mínimos devem ser aplicados, como por exemplo, a Álgebra Booleana.

As árvores de falhas podem ser convertidas em expressões booleanas equivalentes, definindo o evento topo em termos de uma combinação de todos eventos básicos ou não desenvolvidos. Essa expressão pode ser expandida até que se expresse o evento topo como uma soma de todos os cortes mínimos da árvore.

Após a obtenção dos cortes mínimos, uma idéia da importância das falhas pode ser obtida ordenando-se os cortes mínimos de acordo com o seu tamanho. Os cortes mínimos compostos por um único evento básico são listados primeiro, seguidos pelos cortes compostos por dois eventos básicos, seguidos pelos de três, etc /30/.

Medidas de importância proporcionam informações valiosas sobre os eventos que compõe os cortes mínimos de uma árvore de falhas. Componentes com alta importância relativa são candidatos ou a uma monitoração mais rigorosa, de forma a assegurar que o componente não está se degradando, ou a modificações de projeto para aumentar a confiabilidade do mesmo /30/.

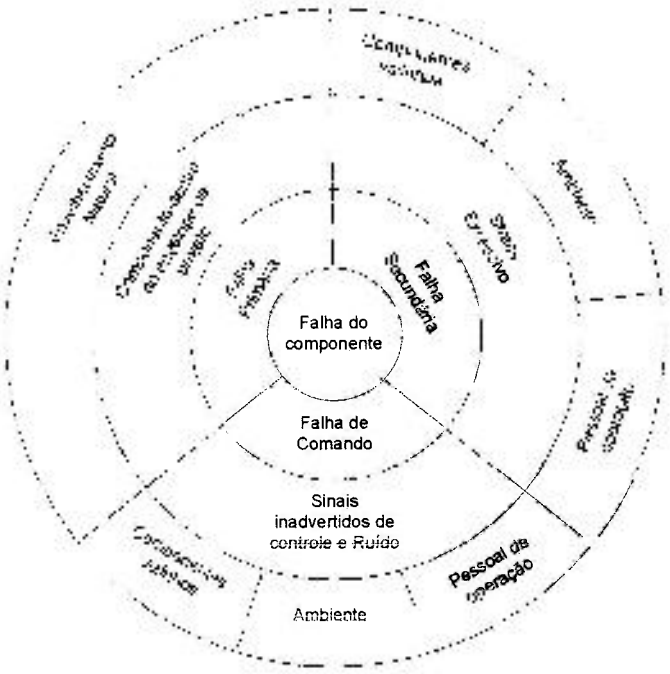


Figura 4.1 Características de falha do componente /17/

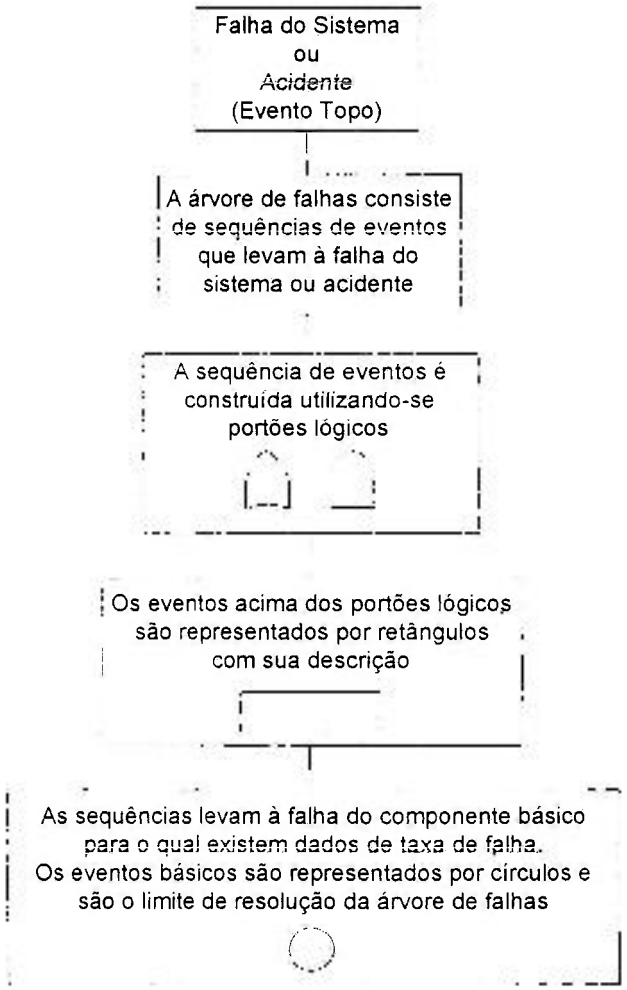


Figura 4.2 Estrutura fundamental da árvore de falhas /17/

COMISSÃO NACIONAL DE ENERGIA NUCLEAR/IPEN

4.2.4 – Falhas Dependentes

Na avaliação de confiabilidade e disponibilidade de sistemas altamente confiáveis, tais como sistemas de segurança de instalações nucleares, é necessário considerar as falhas de modo comum, principalmente em itens redundantes, uma vez que elas podem representar uma porção significativa das falhas, podendo ser dominantes no que diz respeito à probabilidade de falha do sistema.

Algumas definições de falha de modo comum podem ser encontradas na literatura e, de forma simplificada, pode-se defini-la como sendo uma falha dependente na qual dois ou mais componentes em estado de falha existem simultaneamente, ou num pequeno intervalo de tempo, como resultado direto de uma causa comum aos mesmos /18/.

Para compreender e modelar eventos dependentes, é necessário conhecer a causa da falha ou indisponibilidade dos componentes, o que levou à ocorrência de múltiplas falhas ou se existe algo a ser feito para evitar a ocorrência de tais falhas múltiplas /18/. A Tabela 4.1 apresenta os tipos de eventos dependentes, baseado no impacto dos mesmos numa análise probabilística.

Essas questões levam à consideração de três fatores, ilustrados na Figura 4.3. O primeiro é a causa raiz da falha ou indisponibilidade. A causa raiz pode ser entendida como o mecanismo de transição de um *estado disponível* para um *estado com falha* ou *funcionalmente indisponível*. Identificada a causa raiz, o segundo fator a se considerar é o do mecanismo de acoplamento, o que leva a falhas múltiplas do equipamento. O mecanismo de acoplamento explica porque uma causa particular pode afetar vários componentes. O terceiro fator que entra na determinação do potencial de falhas dependentes, incluindo falhas de modo comum, é a existência ou não de defesas, projetadas ou operacionais, contra falhas antecipadas de equipamentos. Algumas práticas adotadas numa política defensiva incluem:

- Controle de projeto;
- Segregação de equipamentos;
- Bons procedimentos de inspeção e teste;
- Bons procedimentos de manutenção;
- Treinamento de pessoal; e
- Controle de qualidade efetivo.

Tabela 4.1 – Tipos de eventos dependentes, baseado no seu impacto

Tipo de evento dependente	Características	Mecanismos de acoplamento	Exemplos de impacto
Evento iniciador de causa comum	Causa um transiente e aumenta a indisponibilidade de um ou mais sistemas de mitigação	Funcional	Perda da alimentação externa
		Espacial	Terremoto
		Humano	Erro de manutenção
Dependência entre sistemas	Causa uma dependência na probabilidade de um evento envolvendo dois ou mais sistemas	Funcional	Sistema de resfriamento falha devido à falha de componente
		Espacial	Fogo causa a perda de equipamentos de dois sistemas
		Humano	Operador causa a perda de dois sistemas
Dependência entre componentes	Causa uma dependência na probabilidade de um evento envolvendo dois ou mais sistemas	Funcional	Bateria perde carga após ser utilizada além de sua capacidade
		Espacial	Fogo causa a perda de bombas redundantes
		Humano	Erro de projeto presente em controle de bombas redundantes

Fonte: NUREG/CR-4780 /18/

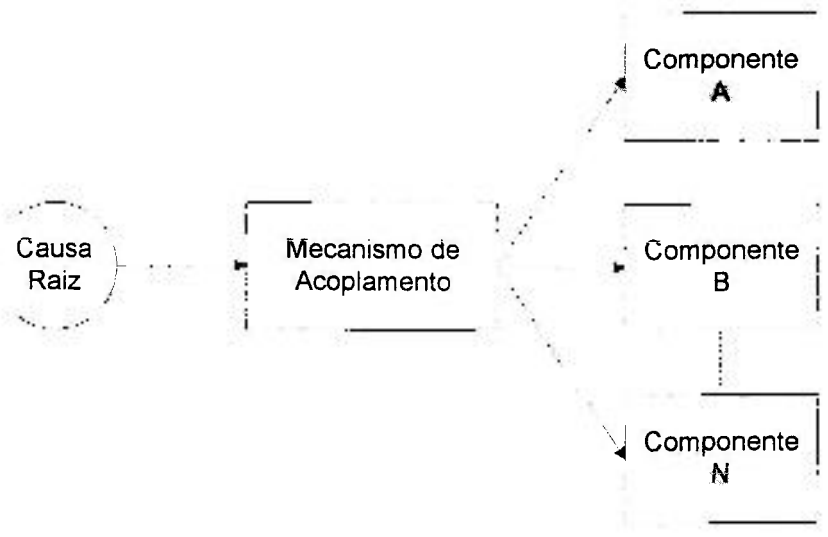


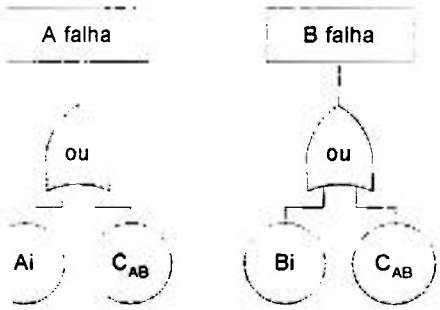
Figura 4.3 – Elementos físicos de um evento dependente /18/

Um estudo realizado pela NEA – "ICDE Report on Collection and Analysis of Common-Cause Failures of Emergency Diesel Generators" /10/, discute os eventos de falha de modo comum ocorridos em diesel geradores de emergência. A Figura 4.4 apresenta a distribuição das falhas de modo comum, agrupadas por causa raiz. Pode-se ver, que a maior contribuição vem das falhas atribuídas ao item *projeto e fabricação*, seguida pelas falhas atribuídas ao *ambiente* e *intervenção humana* /10/. A Figura 4.5 mostra as falhas de modo comum dos diesel geradores agrupadas por mecanismo de acoplamento, evidenciando a maior contribuição do *hardware* nas falhas consideradas.

Do ponto de vista probabilístico, a importância das falhas de modo comum se deve a que sua existência implica que a falha de dois componentes, simbolicamente representados por A e B, não são probabilisticamente independentes e, dessa forma, P(A e B) > P(A).P(B), onde P(A) e P(B) são as probabilidades de falha intrínsecas dos componentes A e B, respectivamente.

A representação de causas dependentes em árvores de falha pode ser feita considerando-se duas ramificações ligadas a um portão lógico. Uma para representar a falha intrínseca do componente e outra para a interação entre eles /18/. Se, portanto, A e B são dois componentes sujeitos a falha de modo comum, os seus eventos básicos da árvore de falhas

são expandidos para incluir o evento C_{AB}, definido como a falha concorrente de A e B devido a modo comum, ficando:



onde Ai e Bi denotam as falhas independentes dos componentes A e B, respectivamente. Esta substituição é feita em todo ponto da árvore de falhas, onde os eventos "A falha" e "B falha" aparecem /18/.

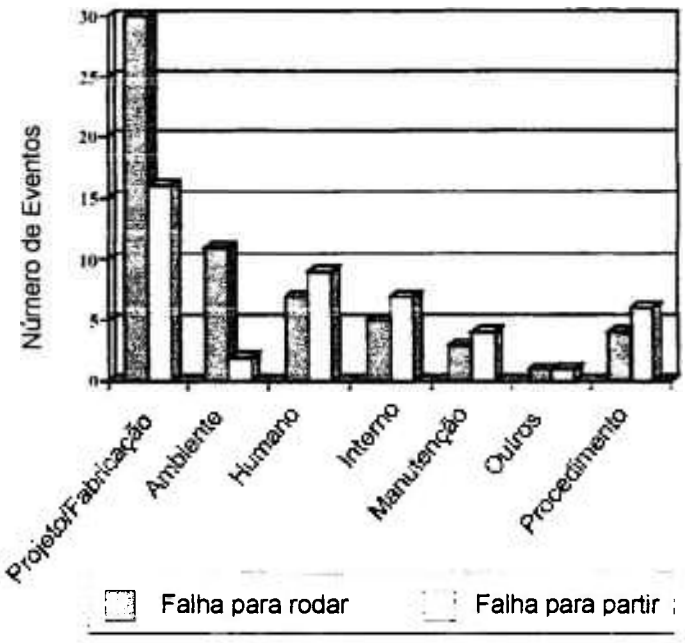


Figura 4.4 Distribuição da falhas ocorridas em diesel geradores de emergência agrupadas por causa raiz /10/.

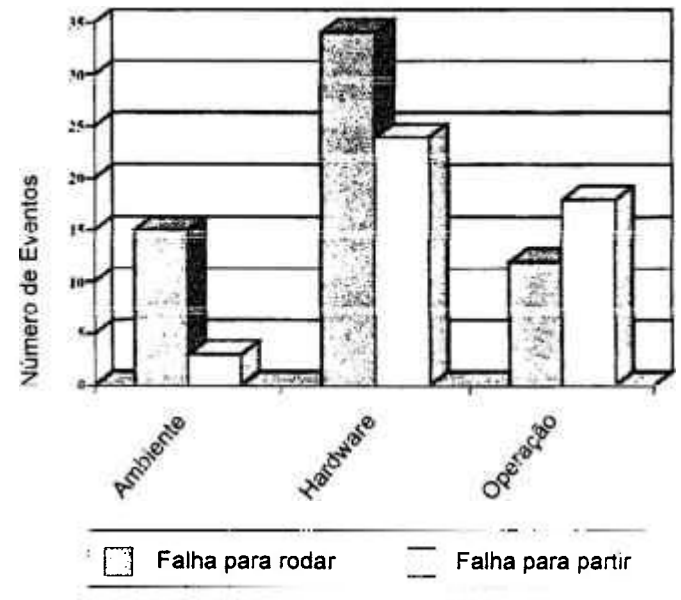


Figura 4.5 Distribuição das falhas ocorridas em diesel geradores de emergência agrupadas por fator de acoplamento /10/.

O ANEXO C mostra o roteiro proposto pela NUREG/CR-4780 /18/, para a avaliação da contribuição das falhas de modo comum. O primeiro passo consiste basicamente na familiarização com o sistema e desenvolvimento de um modelo lógico do sistema estudado. Num segundo passo, devem ser identificados os componentes sujeitos a uma falha de modo comum. Uma vez identificados os componentes sujeitos a falhas de modo comum, deve-se selecionar o modelo probabilístico a ser empregado e estimar os parâmetros a serem utilizados. Por fim, a contribuição das falhas de modo comum é quantificada e avaliada.

Na determinação dos valores numéricos para os eventos básicos de falha de modo comum, pode-se utilizar diferentes modelos probabilísticos.

Os modelos de múltiplos parâmetros são empregados em sistemas com alto grau de redundância e fornecem uma análise mais precisa. Esses modelos envolvem vários parâmetros de forma a quantificar a contribuição específica de vários eventos básicos. Os mais conhecidos são /18/:

- Modelo das múltiplas letras gregas;
- Modelo do fator-alfa; e
- Modelo de taxa de falha binomial.

Os modelos mais simples usam um único parâmetro para calcular a probabilidade de falha devido a modo comum. O mais conhecido e amplamente utilizado é o modelo do fator-beta /18/.

Para uma avaliação preliminar, como é o caso do trabalho proposto nesta dissertação, a utilização do modelo do fator-beta é justificada e fornecerá uma aproximação conservativa da freqüência do evento de modo comum.

Para ilustrar a utilização do fator-beta, consideremos a alternativa da subestação de emergência que utiliza dois diesel geradores em cada barra de segurança, dos quais apenas um é necessário para a operação.

Supondo que a taxa de falha de qualquer dos diesel geradores em operação é λ, a taxa de falha em espera é λ^* e a taxa de reparo de cada um deles é μ. Em adição, sempre que um diesel gerador não estiver em reparo, ele pode falhar randomicamente devido a causas de modo comum.

Os três estados possíveis de tal arranjo são:

0 um diesel está em operação e o outro em espera;

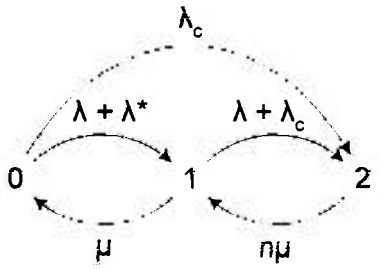
1 um diesel está em reparo e o outro em operação; e

2 ambos diesel estão inoperantes com n unidades em reparo (n=1 ou n=2).

Uma vez que um diesel gerador em operação pode falhar tanto por problemas de operação como por causa de modo comum e, se assumirmos que o diesel gerador não falhará por ambas as razões, a probabilidade de falha de um único diesel gerador, num tempo Δt, será $(\lambda + \lambda_c)\Delta t$, onde λ_c é a taxa de falha do diesel gerador devido a falha de modo comum.

Inicialmente, quando ambos diesel geradores estão em perfeitas condições e apenas um deles está operando, o diesel em operação ou o diesel em espera podem falhar com uma probabilidade combinada de $(\lambda + \lambda^*)\Delta t$, ou ambos podem falhar simultaneamente com probabilidade $\lambda_c \Delta t$.

O diagrama de transição de estados nessa condição fica:



onde se nota que existe uma transição direta entre os estados 0 e 2.

O fator-beta considera que cada falha, independente ou devido a modo comum, é caracterizada por uma distribuição exponencial, para o tempo de ocorrência da primeira falha.

O parâmetro ß é definido como sendo uma fração da taxa de falhas total de uma unidade, atribuída a causa de modo comum, ou seja,

$$\beta = \frac{\lambda_c}{\lambda + \lambda_c}$$

Dessa forma, a probabilidade de ocorrência do evento de modo comum é dada por $P(C_{AB}) = ß.P(A)$ onde, P(A) é a freqüência total de falha randômica a ser utilizada na ausência de qualquer consideração de modo comum.

Estimativas para o fator-beta para diesel geradores e bombas, que podem falhar tanto em demanda como em operação variam, tipicamente, de 0,1 a 0,2 /19/.

Para a estimativa do valor de ß a ser efetivamente utilizado, é fundamental o conhecimento do número de falhas ocorridas no equipamento em estudo, bem como o número de demandas do mesmo.

O ANEXO D apresenta uma classificação de eventos e um sumário da análise efetuada em alguns equipamentos de usinas nucleares mostrando o valor do fator ß considerado. Para o caso de diesel geradores, o valor de ß genérico é 0,05 /18/.

4.3 - Subsídios para Avaliação da Confiabilidade

A avaliação de confiabilidade requer do analista um perfeito conhecimento do sistema em estudo e de todas as relações de causa e efeito que possam vir a ocorrer. Toda a configuração do sistema, sua dinâmica e as interfaces entre sub-sistemas devem ser identificadas através da análise dos documentos que definam suas características de projeto, sua localização física, os detalhes de alimentação de força, tubulações, etc.

4.3.1 - Familiarização com o Sistema

Neste trabalho, o sistema estudado compreende um sistema externo de suprimento de energia, composto por uma linha de transmissão em 88 kV, e um sistema local de suprimento de energia. O sistema local está dividido em duas partes redundantes, física e eletricamente separadas, denominadas trens, de forma a prover a redundância requerida para os sistemas de segurança, sendo composto por transformadores, painéis de distribuição com seus respectivos disjuntores de entrada e de saída, cabos e diesel geradores de emergência.

Os diesel geradores de emergência, por sua vez, são vistos como a sendo a união dos seus principais componentes e sistemas de apoio, conforme mostrado no Capítulo 1.

4.3.2 – Confiabilidade Humana

No caso específico dos diesel geradores, uma revisão dos relatórios de ocorrência de eventos realizada pela NUREG/CR-2989 /6/ detectou 88 eventos

nos quais a falha humana causou ou teve grande peso na indisponibilidade simultânea de dois ou mais diesel geradores.

A Tabela 4.2 apresenta algumas falhas humanas genéricas apontadas como causa dos eventos ocorridos.

A observação desses eventos levou a uma revisão dos procedimentos de inspeção e manutenção de todas as usinas, visando prevenir múltiplas falhas humanas.

Com relação às dependências introduzidas pela ação humana, são feitas duas distinções; aquelas baseadas em processos de comportamento cognitivo e aquelas baseadas em processos de comportamento operacional.

As dependências devido a erros humanos cognitivos resultam em múltiplas falhas dependentes. Dependências devido a erros humanos operacionais incluem erros múltiplos de manutenção, posicionamento e calibração, que resultam em múltiplas falhas dependentes cujos efeitos podem ser imediatamente detectados.

Segundo a NUREG/CR-2815 /20/, a única fonte de informação genérica reconhecida, para erros operacionais, é a NUREG/CR 1278, a qual faz uma série de simplificações advindas principalmente pela falta de reprodutibilidade dos resultados obtidos numa interpretação subjetiva do analista.

Por essas razões, não existem modelos matemáticos para o desenvolvimento das probabilidades individuais de falha humana. Os dados existentes são empiricamente derivados de dados observados /20/.

Tabela 4.2 Falhas humanas genéricas que causaram indisponibilidade dos diesel geradores de emergência

1	Operação inadvertida do sistema de combate a incêndio
2	Disjuntor conectado incorretamente
3	Condutores do governador quebrados e cortados durante manutenção
4	Água no óleo combustível. Trabalhadores cortaram a linha de ventilação abaixo do piso
5	Grupo de manutenção deixa água nos controle de tensão e velocidade
6	Relé de partida comprimido pelo trabalhador
7	Sobrevelocidade do DG devido à ferramenta deixada no armário do injetor depois da manutenção
8	Condutores do neutro do transformador cortados
9	Linhas de ar de partida invertidas
10	Pessoal de construção remove cabos impedindo o fechamento do disjuntor
11	Pessoal de manutenção deixa água no armário de controle causando falha do mesmo
12	Disjuntor não fecha. Pessoal de manutenção entorta dentes de contato durante manutenção
13	Ar no óleo do governador durante manutenção causa variação de velocidade
14	Ar introduzido nas linhas de combustível durante manutenção
15	Trem 1 de água de serviço inabilitado enquanto trem 2 estava em manutenção
16	Pedaço de tecido deixado no filtro de óleo
17	Pré filtro entupido por pedaços de tecido
18	DG indisponíveis. Representante do fabricante desliga alimentação de controle
19	Saco de desumidificador no tanque de combustível do DG
20	Teste de sprinkler joga água no gerador e no regulador
21	DG 1 indisponível devido a manutenção não programada e operadores tiram DG 2 de serviço

Fonte: NUREG/CR 2989

4.3.3 – Banco de Dados

O objetivo de um banco de dados de falhas é fornecer referências atualizadas de falhas de componentes e equipamentos observadas em centrais nucleares ou instalações industriais. Esses dados são utilizados na análise quantitativa da árvore de falhas.

Neste trabalho, as principais referências consultadas para a obtenção das taxas de falhas de equipamentos e componentes foram o IEEE Std 493 – "Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems" /21/; o IEEE-Std 500 – "IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component and Mechanical Equipment Reliability Data for Nuclear Power Generating Stations" /22/; e o EGG-SSRE-8875 – "Generic Component Failure Data Base for Light Water and Liquid Sodium Reactor PRA´s – Informal Report" /23/.

4.3.4 – Códigos Computacionais

A solução de árvores de falhas, ou seja, a obtenção dos cortes mínimos, seqüências de acidentes, etc, é comumente obtida através da utilização de códigos computacionais, por exemplo WAM, FTAP ou SETS. /18/

O desempenho do sistema elétrico e das configurações propostas para a subestação de emergência foi verificado através da utilização do programa SAPHIRE – Systems Analysis Programs for Hands-On Integrated Reliability Evaluations, por ser um programa amplamente utilizado na área nuclear /30/.

O SAPHIRE é um programa voltado para avaliação probabilística de risco auxiliando na identificação, caracterização, quantificação e avaliação de perigos. Ele permite ao usuário criar e analisar árvores de falhas e árvores de eventos utilizando um computador pessoal.

O programa permite que os dados sejam introduzidos tanto no modo gráfico, conforme mostrado na Figura 5.9, ou no modo lógico, conforme mostrado na Tabela 5.5.

O editor lógico do programa é uma ferramenta bastante ágil para a entrada de portões lógicos e eventos básicos permitindo rapidez e clareza na montagem de uma árvore de falhas. Outra vantagem de se trabalhar com o editor lógico é o fato do mesmo permitir a busca e localização de um determinado

portão lógico ou evento básico. Ele também permite que portões lógicos e toda lógica abaixo dele sejam movidos para qualquer outro portão lógico selecionado.

Uma vez feita a entrada dos dados, o programa calcula e apresenta os cortes mínimos e sua importância para a ocorrência do evento topo, conforme mostrado nas Tabelas 5.7 e 5.8.

O programa também permite a realização de análises de incerteza, importância e sensibilidade.

Na análise de incerteza da árvore de falhas, o programa calcula a variação da probabilidade do evento topo da árvore de falhas em função da incerteza das probabilidades de ocorrência dos eventos básicos.

Na análise de importância, o programa calcula a contribuição de determinado evento básico no corte mínimo de interesse.

Para a análise de sensibilidade, o programa permite alterar tanto a lógica da árvore de falhas como as probabilidades dos eventos básicos, guardando tais dados num arquivo específico possibilitando a elaboração de análises comparativas.

5 – ESTUDO DE ALTERNATIVAS

5.1 - Geral

O estudo de caso desenvolvido no presente trabalho visa analisar os índices de confiabilidade para três configurações do sistema elétrico de emergência em corrente alternada de uma central nuclear de pequeno porte através do uso da árvore de falhas.

Uma das configurações é típica, em termos de suprimento de energia elétrica de emergência em corrente alternada, sendo constituída por dois diesel geradores, um para cada barramento de segurança.

A segunda alternativa adiciona um terceiro diesel gerador à alternativa anterior. Esse diesel gerador pode ser conectado a qualquer um dos dois barramentos de segurança.

A terceira alternativa contempla o uso de quatro diesel geradores, sendo dois para cada barramento de segurança.

O estudo ilustra a aplicação da técnica da árvore de falhas como ferramenta para obtenção e comparação de índices de confiabilidade dos diferentes arranjos propostos, tendo sido considerados os efeitos de falhas humanas e falhas de modo comum.

Os resultados obtidos indicam que a configuração com quatro diesel geradores seria a que apresenta os melhores índices de confiabilidade.

A seguir é apresentada uma descrição sucinta do sistema elétrico estudado, levando-se em consideração apenas os fatores e os componentes que afetam diretamente os resultados da análise proposta.

5.2 – O Sistema Analisado

O diagrama de blocos ilustrado na Figura 5.1 mostra como está configurado o sistema em estudo. O sistema é dividido em Sistema Elétrico Externo e Sistema Elétrico Local.

O Sistema Elétrico Externo é composto por uma linha de transmissão em 88 kV, sendo a fonte principal de energia elétrica da central.

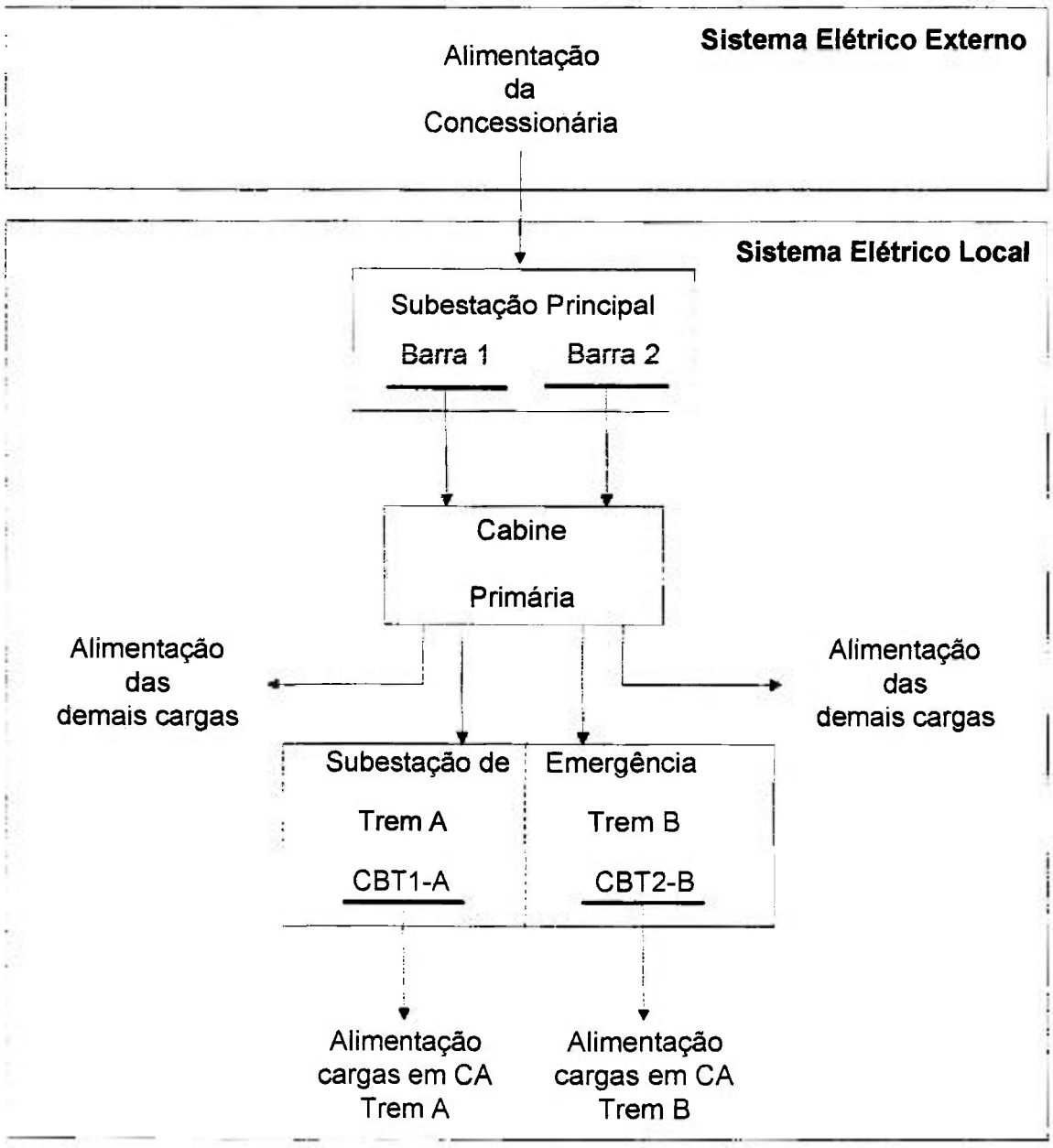


Figura 5.1 – Diagrama de Blocos do Sistema Elétrico

O Sistema Elétrico Local compreende a recepção, transformação e distribuição da energia elétrica recebida da concessionária, bem como a geração e distribuição da energia elétrica de emergência. Para este sistema, são analisadas três configurações possíveis para a Subestação de Emergência. Os detalhes de cada um deles são apresentados nas seções seguintes.

5.2.1 - O Sistema Elétrico Externo

O sistema elétrico externo é a fonte normal de energia elétrica para todas as cargas da planta, sendo constituído por uma linha de transmissão em 88 kV que alimenta a Subestação Principal da planta.

A linha de transmissão comporta os dois circuitos em uma única torre, um de cada lado, na mesma faixa de servidão, sendo que um dos circuitos está normalmente em serviço enquanto o outro é reserva.

O sistema elétrico externo é um componente extremamente importante e tem um grande peso nos índices de confiabilidade da planta estudada.

Para avaliar a sua contribuição procurou-se obter informações sobre interrupções do fornecimento de energia e a duração das mesmas, para linhas de transmissão em 88 kV.

Foi obtido junto à Companhia Piratininga de Força e Luz – CPFL, um conjunto de informações que retrata as interrupções de energia elétrica sofridas por uma linha de transmissão em 88 kV genérica, cobrindo um período entre 1978 a 1991. Esses dados são listados no Anexo E e incluem as datas nas quais ocorreu falta de energia, bem como a duração das mesmas.

A partir da observação dos dados do Anexo E foram calculados alguns índices de confiabilidade. Para o cálculo desses índices, foram admitidas as seguintes hipóteses:

- Distribuição de falhas exponencial (taxa de falhas constante);
- Para a determinação da taxa de falhas da linha, foi contabilizado como falha todo evento onde houve interrupção do fornecimento de energia, independente da sua duração; e
- Adotou-se, conservativamente, que as interrupções com duração 0,00 horas tem, para efeito de cálculo, duração de 0,004 horas. Esta é uma consideração conservativa pois aumenta o tempo de reparo da linha, estando, portanto, a favor da segurança.

Os valores calculados foram:

- Tempo médio entre falhas (MTTF) = 533,81 horas
- Taxa de falhas (λ) = 0,001866 falhas/hora
- Tempo médio de reparo (MTTR) = 0,322 horas
- Desvio Padrão (do MTTR) = 2,053

O valor elevado do desvio padrão, para o tempo médio de reparo (MTTR), é provocado pela presença de alguns valores bastante diferentes da média dos tempos de interrupção apresentados no Anexo E.

O histograma da Figura 5.2 apresenta o número de vezes que a linha considerada sofreu interrupção do fornecimento de energia ao longo do período observado (1978 a 1991), em função da duração das mesmas.

A Figura 5.3 mostra em forma de gráfico, a evolução do número de desligamentos ao longo do período observado. Pode ser observado que a tendência é que, com a consolidação do sistema interligado de distribuição, haja cada vez menos desligamentos. O Anexo F apresenta, por ano, os histogramas dos desligamentos ocorridos e suas durações.

A Tabela 5.1 apresenta a freqüência anual de perda da alimentação externa, em função do tempo de duração da perda. Pode-se concluir que aproximadamente 95 % das interrupções no fornecimento de energia tiveram durações entre 0 e 0,5 horas.

Para efeito de comparação, a Tabela 5.2 apresenta os valores das freqüências anuais de perda da alimentação elétrica externa de algumas usinas nucleares. Comparando-se a freqüência de falhas da linha de transmissão considerada com as apresentadas nessa tabela, constata-se que, para a central nuclear de pequeno porte aqui estudada, a probabilidade de perda do sistema elétrico externo é bem superior.

Isso ocorre porque a planta estudada apresenta uma única alternativa de suprimento externo de energia, enquanto as demais instalações, por serem instalações nucleares de grande porte e por estarem inseridas num sistema interligado de distribuição de energia apresentam, no mínimo, duas alternativas para o suprimento externo de energia elétrica.

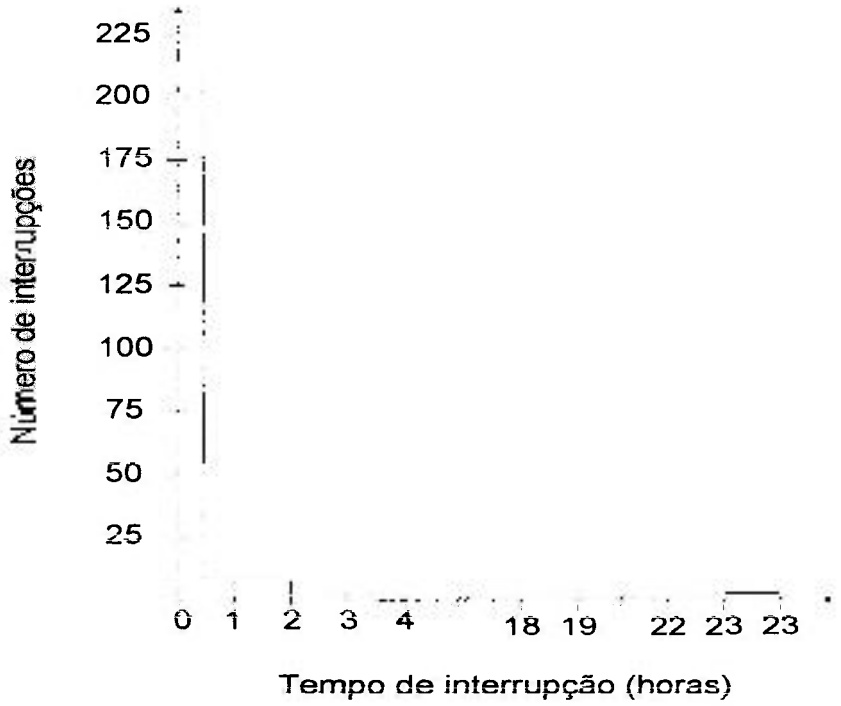


Figura 5.2 – Histograma representativo do número de interrupções de energia da concessionária em função de sua duração, para o período de 1978 a 1991.

Tabela 5.1 – Freqüência anual da perda de alimentação elétrica externa

Duração	Freqüência anual
0 – 0,5	14,70
0,5 – 1	0,50
1 – 2	0,50
2 – 3	0,30
3 – 5	0,10
5 – 8	0
8 – 24	0,20

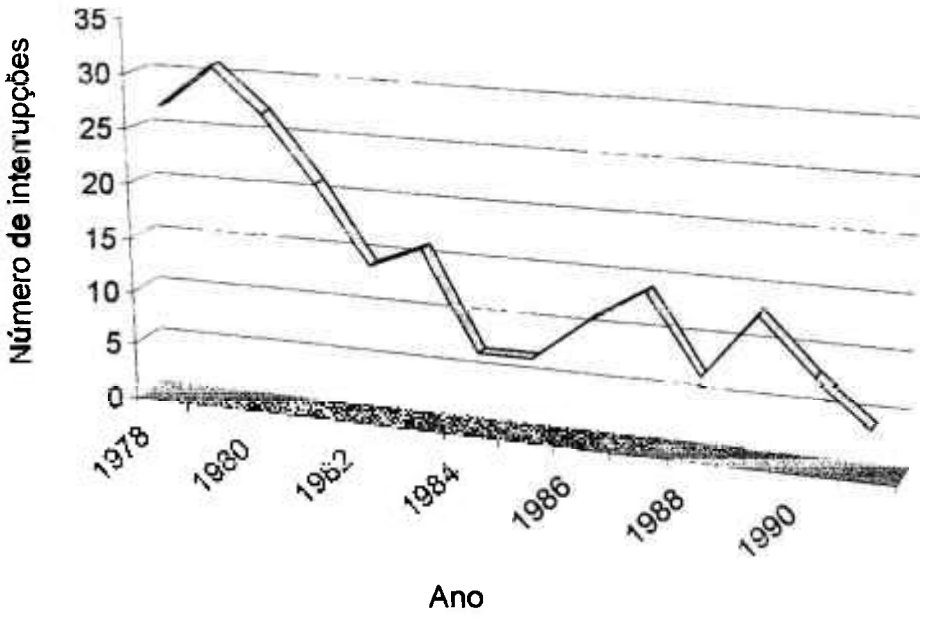


Figura 5.3 – Número de desligamentos da Linha da CPFL
(período de 1978 a 1991).

Tabela 5.2 – Freqüência anual de perda da alimentação elétrica

Usina	Freqüência Anual
APS de Arkansas	0,32
APS de Oconee	0,17
APS de Indian Point	
Unit 2	0,18
Unit 3	0,27
APS de Calvert Cliffs	0,14
APS de Angra I	0,36
Estudo de caso	16,3

Fonte: APS de ANGRA I /24/

O valor elevado da freqüência de perda da alimentação elétrica externa aponta para a necessidade de se ter um sistema de suprimento de energia elétrica de emergência de alta confiabilidade. Isto irá refletir-se na avaliação quantitativa de confiabilidade como é mostrado adiante.

5.2.2 - O Sistema Elétrico Local

O sistema elétrico local tem a função de garantir um suprimento de energia elétrica confiável durante a operação normal, anormal e em emergência para todas as cargas da central.

Para a avaliação da confiabilidade do sistema elétrico local, foram admitidas as seguintes hipóteses:

- Todos os equipamentos e componentes estavam em perfeitas condições e disponíveis no instante inicial da operação;
- Os equipamentos e componentes são monitorados e, em caso de falha, são reparados de imediato, num intervalo de tempo igual ao seu tempo médio de reparo;
- Os equipamentos e componentes, cujo estado de falha é verificado periodicamente, são reparados após o período entre testes;
- Tempo de observação de 1 ano (8760 horas); e

O sistema elétrico local é composto pela subestação principal, cabine primária e subestação de emergência, onde estão localizadas as fontes de energia elétrica de emergência em corrente alternada, no caso diesel geradores.

5.2.2.1 - Subestação Principal

A subestação principal recebe alimentação da concessionária em 88kV. Os transformadores TRAFO 1 e TRAFO 2 abaixam a tensão para 13,8 kV e alimentam os painéis de média tensão BP1 e BP2.

Os painéis de média tensão BP1 e BP2 possuem disjuntores de interligação, normalmente abertos, que possibilitam que um único transformador alimente os dois painéis. A partir dos painéis de média tensão BP1 e BP2 saem dois circuitos, física e eletricamente separados, que alimentam os painéis de média tensão da Cabine Primária.

A Figura 5.4 apresenta o diagrama unifilar simplificado da subestação principal.

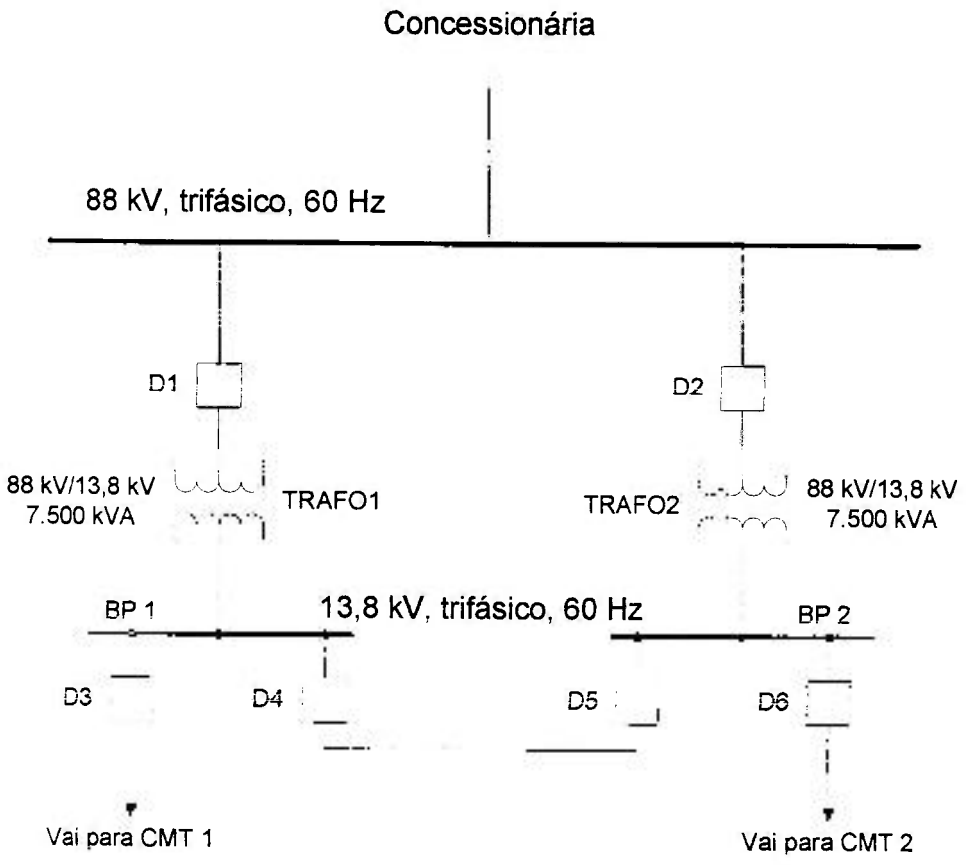


Figura 5.4 – Diagrama unifilar simplificado da Subestação Principal

5.2.2.2 – Cabine Primária

A cabine primária tem a função de distribuir a energia elétrica recebida da subestação principal. Os dois circuitos provenientes da subestação principal alimentam dois painéis de média tensão, CMT1 e CMT2.

Os circuitos que partem do CMT1 e do CMT2 alimentam os painéis de baixa tensão CBT1-A e CBT2-B da subestação de emergência, formando, a partir daí, os trens redundantes A e B, cujos circuitos e equipamentos são física e eletricamente separados.

Os painéis de média tensão da cabine primária CMT1 e CMT2 possuem disjuntores de interligação, normalmente abertos, que possibilitam que um único circuito alimente os dois painéis de baixa tensão.

Em condição normal de operação, cada painel de média tensão CMT1 e CMT2 será alimentado por um circuito independente derivado da subestação principal. Havendo a indisponibilidade de um dos circuitos alimentadores da subestação principal, poderão ser fechados os disjuntores de interligação dos painéis CMT1 e CMT2, restabelecendo o suprimento de energia elétrica do painel desenergizado.

5.2.2.3 – Subestação de Emergência - 4 DG

A partir do CMT1 e do CMT2, a energia elétrica é distribuída por dois trens redundantes sem interconexões chegando aos barramentos de segurança CBT1-A e CBT2-B. Os painéis CBT1-A e CBT2-B são responsáveis pela alimentação das cargas de segurança em corrente alternada, através dos transformadores abaixadores TRF1-A, TRF2-B, TRF3-A e TRF4-B.

Conforme mostrado na Figura 5.5, o painel CBT1-A e todas as suas cargas está associado ao trem A enquanto o painel CBT2-B e todas as suas cargas estão associados ao trem B.

Nenhuma ligação existe entre o trem A e o trem B, sendo os mesmos, portanto, funcionalmente independentes.

Em condição normal de operação, o CBT1-A e o CBT2-B são alimentados pelos transformadores TRF1-A e TRF4-B, respectivamente, enquanto os transformadores TRF2-B e TRF3-A, denominados reserva, estarão permanentemente prontos para operar.

COMISSÃO NACIONAL DE ENERGIA NUCLEAR/SP-IPEN

Em caso de ocorrência de defeito, reparo ou manutenção no transformador principal de um trem, o disjuntor do transformador afetado será aberto e o disjuntor do transformador reserva será fechado, possibilitando o restabelecimento imediato do suprimento de energia elétrica do trem afetado.

No caso da indisponibilidade do suprimento de energia elétrica para os transformadores TRF1-A, TRF2-B, TRF3-A e TRF4-B, os painéis de baixa tensão CBT1-A e CBT2-B serão alimentados pelos grupos diesel geradores de emergência de modo a prover energia elétrica de emergência para as cargas que desempenham função de segurança nuclear.

A cada barramento de segurança CBT1-A e CBT2-B estão associados dois grupos diesel geradores, sendo um principal e outro reserva, com seus respectivos painéis de comando e controle, painéis de sincronismo e sistemas auxiliares.

Os diesel geradores estão sempre prontos para entrar em operação em caso de indisponibilidade do Sistema Elétrico Externo ou no caso de receber um sinal do Sistema de Proteção da Planta (sinal de injeção de segurança para mitigar acidente de perda de refrigerante).

No caso de indisponibilidade do Sistema Elétrico Externo, os quatro grupos partem automaticamente. Após atingirem tensão e freqüência nominal, os diesel geradores principais são carregados seqüencialmente, com as cargas de segurança de seus respectivos painéis, enquanto os diesel geradores reserva retornam ao estado de prontidão.

Caso o diesel gerador principal falhe em partir ou em assumir as cargas, o diesel gerador reserva é automaticamente conectado ao painel.

Caso os grupos partam em decorrência de um sinal proveniente do Sistema de Proteção, somente serão conectados aos CBT1-A e CBT2-B se houver indisponibilidade simultânea do Sistema Externo de Energia.

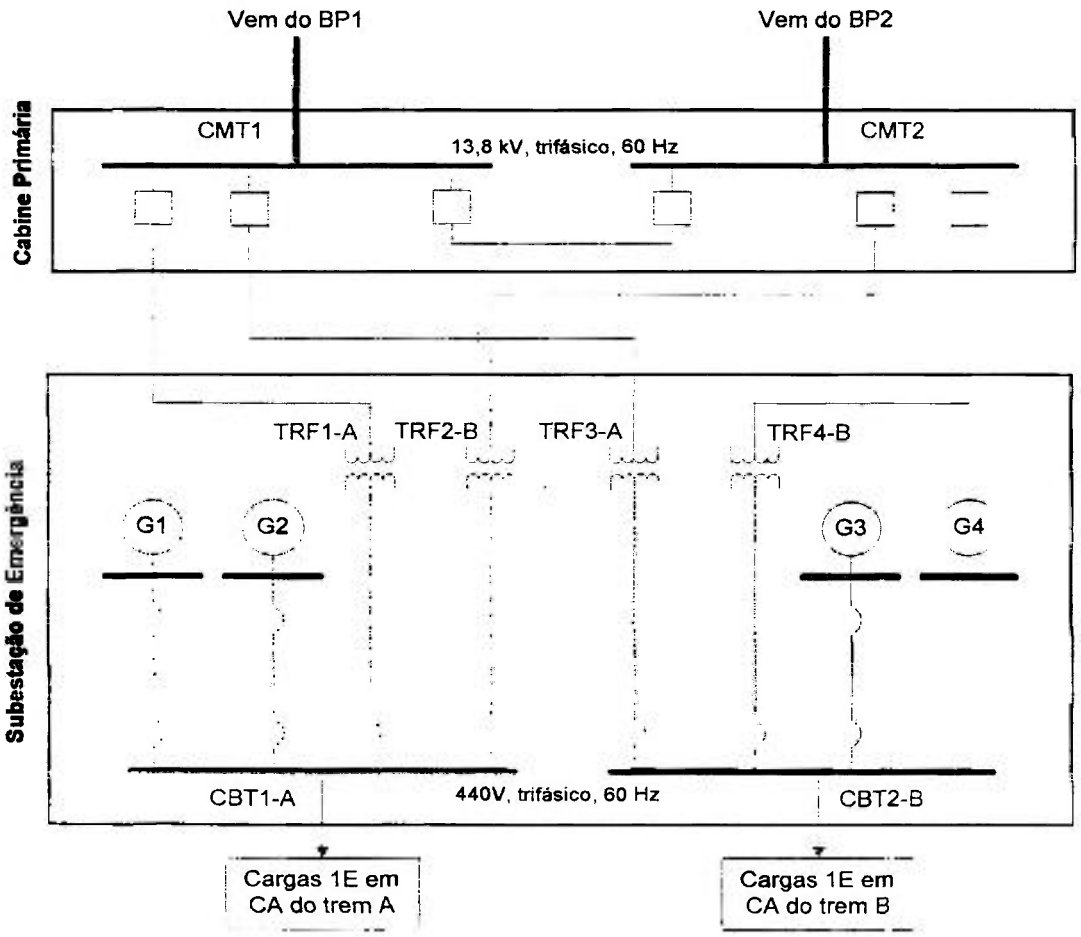


Figura 5.5 Diagrama unifilar simplificado da Cabine Primária e da Subestação de Emergência com 4 Diesel Geradores

5.2.2.4 – Subestação de Emergência - 3 DG

Visando otimizar o uso de diesel geradores considerou-se um arranjo alternativo da subestação de emergência utilizando-se três diesel geradores. Neste caso, cada barramento de segurança CBT1-A e CBT2-B tem dedicado a ele um grupo diesel gerador com seus respectivos painéis de comando e controle, painéis de sincronismo e sistemas auxiliares. O terceiro grupo diesel gerador pode ser conectado tanto ao CBT1-A como ao CBT2-B por meio de uma chave de transferência. A Figura 5.6 ilustra essa situação.

Os diesel geradores estão sempre prontos para entrar em operação, em caso de indisponibilidade do Sistema Elétrico Externo ou no caso de receber um sinal do Sistema de Proteção da Planta (sinal de injeção de segurança para mitigar acidente de perda de refrigerante).

No caso de indisponibilidade do Sistema Elétrico Externo, os três grupos partem automaticamente. Após atingirem tensão e freqüência nominal, os grupos diesel gerador G1 e G2 são carregados, seqüencialmente, com as cargas de segurança do CBT1-A e CBT2-B respectivamente, retornando o grupo diesel gerador G3 ao estado de prontidão.

Caso ocorra a falha do G1 ou do G2, o grupo diesel gerador G3 assume as cargas do CBT1-A ou do CBT2-B.

Caso os grupos partam em decorrência de um sinal proveniente do Sistema de Proteção, somente serão conectados aos CBT1-A e CBT2-B se houver indisponibilidade simultânea do Sistema Externo de Energia.

A conexão do G3 ao CBT1-A ou ao CBT2-B pode ser realizada ou por meio de uma chave de transferência ou manualmente, através da ação de um operador. A utilização de chaves de transferência na indústria, para conexão de geradores de emergência, é bastante conhecida porém, não se tem conhecimento da sua utilização na área nuclear.

A transferência manual, através da atuação de um operador, além de amplamente utilizada é bastante segura, uma vez que se trata da inserção de disjuntores que se encontram extraídos, na presença de um intertravamento que visa impedir que o diesel gerador venha a ser conectado aos dois barramentos de segurança simultaneamente.

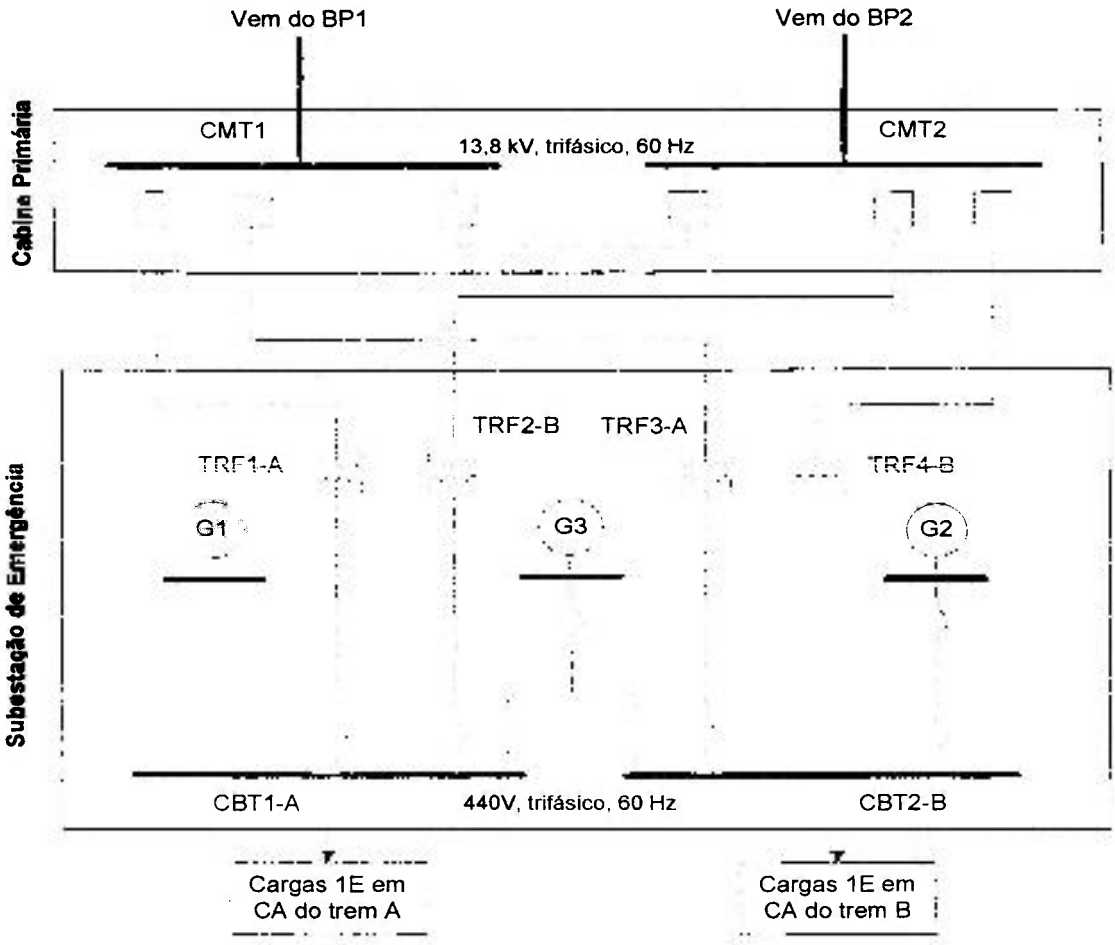


Figura 5.6 Configuração alternativa da Subestação de Emergência com três Diesel Geradores.

5.2.2.5 – Subestação de Emergência - 2 DG

Esta é a configuração típica para os diesel geradores de emergência /5/. Neste caso, cada barramento de segurança CBT1-A e CBT2-B tem dedicado a ele, apenas um grupo diesel gerador com seus respectivos painéis de comando e controle, painéis de sincronismo e sistemas auxiliares. A Figura 5.7 apresenta essa configuração.

Da mesma forma que nas considerações anteriores, os diesel geradores estão sempre prontos para entrar em operação, em caso de indisponibilidade do Sistema Elétrico Externo ou no caso de receber um sinal do Sistema de Proteção da planta.

No caso de indisponibilidade do Sistema Elétrico Externo, os dois grupos partem automaticamente, sendo carregados, seqüencialmente, com as cargas de segurança, após atingirem tensão e freqüência nominal.

Caso os grupos partam em decorrência de um sinal proveniente do Sistema de Proteção, somente serão conectados aos CBT1-A e CBT2-B se houver indisponibilidade simultânea do Sistema Externo de Energia.

Nesta alternativa, a indisponibilidade simultânea da fonte externa e dos diesel geradores apresenta um grande risco para a central.

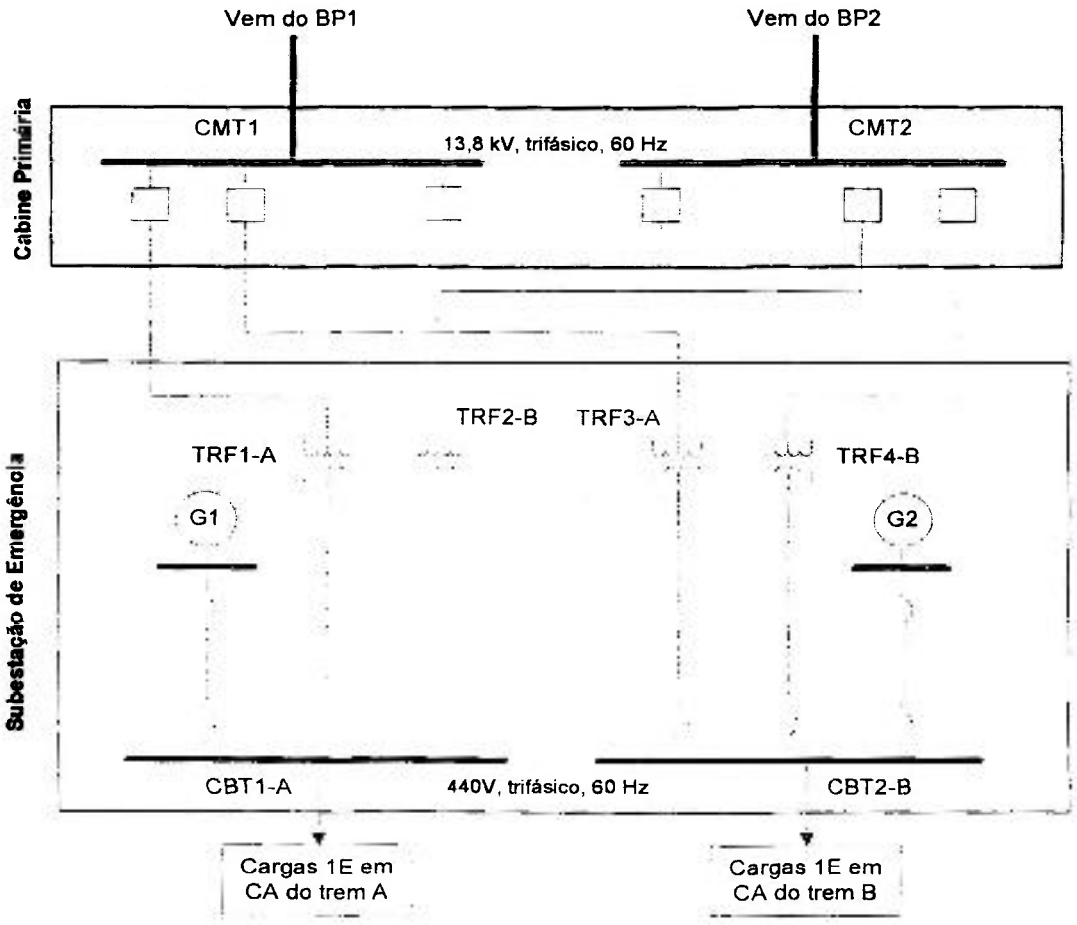


Figura 5.7 Configuração alternativa da Subestação de Emergência com dois Diesel Geradores.

5.3 – Base de dados

5.3.1 – Equipamentos e Componentes

Para os equipamentos e componentes do sistema elétrico local os valores das taxas de falha e dos tempos de reparo foram retirados da IEEE Std-500 – "*IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations*" /22/.

Para tal foi generalizado, de forma conservativa, o uso do modo de falha "*all modes*", que engloba todos os modos de falha possíveis para um determinado equipamento ou componente.

Para os diesel geradores de emergência e seus sistemas auxiliares, as taxas de falha e os tempos de reparo foram retirados da NUREG 2989 /6/.

Os valores considerados para as taxas de falha e tempos de reparo são apresentados nas tabelas 5.3 e 5.4.

5.3.2 – Confiabilidade Humana

Para avaliação da contribuição das falhas humanas foram utilizadas as informações da NUREG/CR-2989 /6/ e da NUREG/CR-2815 /20/.

Ao se fazer considerações sobre a operação manual, deve-se ter em mente que toda operação tem um tempo para ser completada. Esse tempo é função da complexidade da própria operação e também do tempo máximo que os sistemas suportam uma interrupção no fornecimento de energia.

As únicas intervenções humanas consideradas neste trabalho são as afetas à manutenção e testes e transferência manual do G3, caso particular da configuração com 3 DG.

A Figura 5.8 mostra a evolução da probabilidade de ocorrência de erro humano em função do tempo necessário para efetuar uma operação, extraído da NUREG/CR-2815 /20/.

Tabela 5.3 – Dados de falha dos principais componentes do sistema elétrico

Componente	Código do componente	Taxa Falha (Falha/Hora)	Tempo Reparo (horas)	Ref.
Painel de baixa tensão	CBT	$1,19 \times 10^{-6}$	27	IEEE 500
Painel de média tensão	CMT	$4,8 \times 10^{-6}$	13	IEEE 500
Painel de alta tensão	BP	$4,8 \times 10^{-6}$	13	IEEE 500
Operação Diesel	DG-RUN-FAIL	$2,4 \times 10^{-3}$	20	Nureg 2989
Partida Diesel	DG-START-FAIL	$2,5 \times 10^{-2}$	20	Nureg 2989
Transformador AT	TRAFO	$1,24 \times 10^{-6}$	64	IEEE 500
Transformador BT	TRF	$1,65 \times 10^{-7}$	49	IEEE 500
Alimentadores	FEEDER	$1,75 \times 10^{-5}$	3	IEEE 500
Painel de entrada	88 kV-BAR	$4,8 \times 10^{-6}$	13	IEEE 500
Chave transferência	SWITCH	$7,2 \times 10^{-5}$	5	Fabricante
Concessionária	UTILITY	$1,87 \times 10^{-3}$	0,3	Calculado
Falha modo comum DG	CCF	$1,2 \times 10^{-4}$	20	Nureg 2989

Tabela 5.4 Dados de falha dos principais componentes dos sistemas auxiliares dos diesel geradores

Componente	Código do componente	Taxa de Falha (Falha/Hora)
Lógica e controle		
Controle	Control	$8,64 \times 10^{-5}$
Chaves, relés, fiação	Switch-Relay	$2,38 \times 10^{-4}$
Falha genérica	Logic Generic Fail	$2,45 \times 10^{-4}$
Tacômetro	Tach	$1,51 \times 10^{-4}$
Governador		
Falha genérica	Governor-Generic Fail	$2,55 \times 10^{-4}$
Óleo contaminado	Oil	$1,28 \times 10^{-4}$
Sensor e controle	Sensor	$1,55 \times 10^{-4}$
Setpoint	Setpoint	$1,34 \times 10^{-4}$
Resfriamento		
Falha genérica	Cooling Generic Fail	$1,06 \times 10^{-4}$
Entulho	Debris	$1,06 \times 10^{-4}$
Bombas	Pump	$8,16 \times 10^{-5}$
Válvulas	Valve	$1,2 \times 10^{-4}$
Vazamento	Leaking	$6,72 \times 10^{-5}$
Disjuntor e Seqüenciador		
Falha genérica	CB Generic Fail	$1,73 \times 10^{-5}$
Disjuntor	Breaker	$6,34 \times 10^{-5}$
Controle manual	Manual Control	$3,17 \times 10^{-5}$
Relés auxiliares	Relay	$7,2 \times 10^{-5}$
Autofechamento	*Selfclosing*	$7,2 \times 10^{-5}$
Seqüenciador	Sequencer	$3,17 \times 10^{-5}$
Sistema de Partida		
Falha genérica	Start Generic Fail	$5,76 \times 10^{-5}$
Motores a ar	Air Motor	$3,84 \times 10^{-5}$
Válvulas e tubos	Tubing	$1,44 \times 10^{-4}$

Fonte: NUREG/CR-2989 /6/

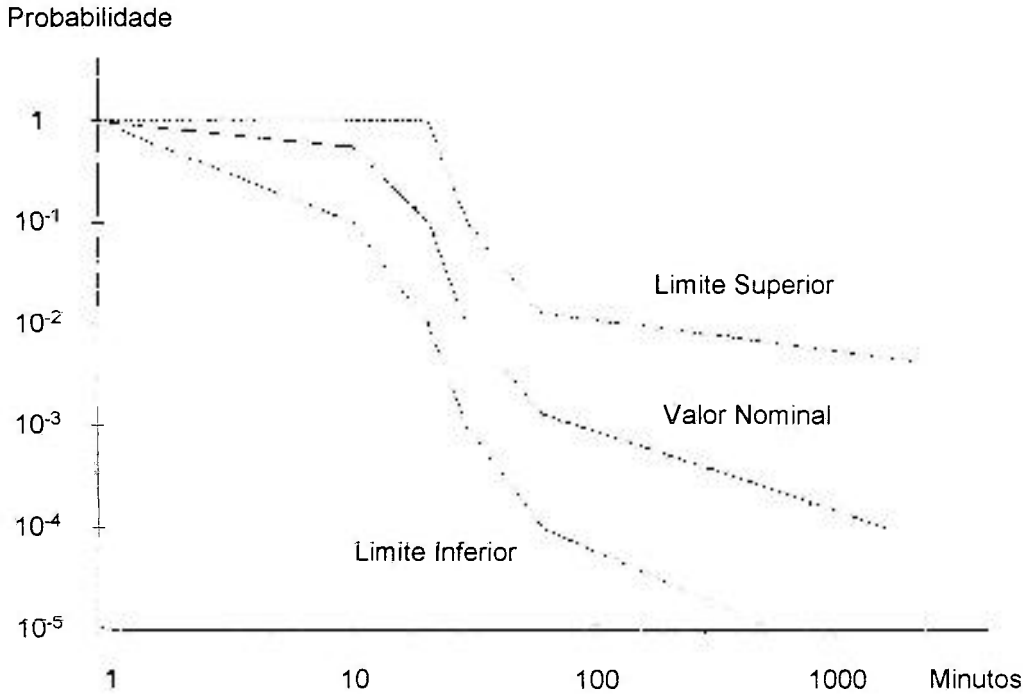


Figura 5.8 Probabilidade de falha humana na resolução de problemas versus tempo para realização da tarefa /20/

COMISSÃO NACIONAL DE ENERGIA NUCLEAR/SP-IPEN

Foi considerado neste trabalho, que o tempo para completar a transferência manualmente pode ser no máximo quatro horas, visto que esse é o tempo da autonomia de um banco de baterias comum.

Se entrarmos com esse valor de quatro horas na Figura 5.8, encontraremos uma probabilidade de falha humana que varia, de modo aproximado, entre 2,0E-02 e 6,0E-04.

Como pode ser observado, a probabilidade de erro humano é tanto maior quanto menor for o tempo para a realização da tarefa. Os limites, inferior e superior, caracterizam o fator de erro a considerar.

A probabilidade de erro humano, considerada para as três configurações possíveis da subestação de emergência, é 6,0 E -04.

5.3.3 – Eventos Dependentes

No caso particular das falhas de modo comum dos diesel geradores de emergência, foram utilizadas as recomendações da NUREG/CR-4780 /18/, utilizando-se o valor de 0,05 para o fator beta (Anexo D). Na análise paramétrica, realizada no item 5.7 desta dissertação, foi estudada a variação da freqüência anual de perda de alimentação elétrica para diferentes valores do fator beta.

5.4 – Desenvolvimento das Árvores de Falhas

O sucesso do sistema elétrico, como um todo, é caracterizado pelo fornecimento de energia elétrica, para todas as cargas da planta, com as condições adequadas de tensão e freqüência.

Para cada uma das alternativas de configuração da subestação de emergência foi construída uma árvore de falhas. As árvores de falha são similares, diferenciando-se somente na forma de considerar a contribuição dos componentes da subestação de emergência.

5.4.1 – Definição do Evento Topo

Para todas as alternativas de configuração da subestação de emergência, a falha do sistema elétrico é caracterizada pela perda do suprimento de energia elétrica em corrente alternada das cargas importantes para a segurança., ficando definido o evento topo *"Cargas 1E em CA não recebem energia"*.

5.4.2 – Construção das Árvores de Falhas

A árvore de falhas contempla os principais componentes do sistema elétrico analisado. Todos os painéis e barramentos considerados na análise englobam seus disjuntores de entrada e de saída.

Os diesel geradores de emergência foram desmembrados nos seus sistemas de apoio e estes, por sua vez, desmembrados nos componentes mais representativos.

Nos itens seguintes são apresentadas as lógicas das árvores de falha das três alternativas estudadas.

5.4.2.1 – Árvore de Falhas para a Configuração com 4 Diesel Geradores

A Figura 5.9 apresenta a árvore de falhas para a configuração com 4 diesel geradores. A Tabela 5.5 apresenta o diagrama lógico dessa árvore de falhas. Esse diagrama é uma saída do código SAPHIRE e mostra uma forma alternativa de se representar o encadeamento lógico dos eventos.

5.4.2.2 – Árvore de Falhas para a Configuração com 3 Diesel Geradores

A árvore de falhas para a configuração com 3 diesel geradores é similar à apresentada na Figura 5.9. A diferença somente aparece quando se postula a falha do G1 ou do G2. Nessa condição, o G3 é conectado ao barramento cujo suprimento de energia foi perdido.

A Figura 5.10 apresenta uma representação esquemática da árvore de falhas realçando a contribuição do DG3.

No Anexo G é mostrado o diagrama lógico gerado pelo código SAPHIRE, para a configuração com 3 diesel geradores.

5.4.2.3 – Árvore de Falhas para a Configuração com 2 Diesel Geradores

Neste caso, a árvore de falhas é uma simplificação da configuração com 4 diesel geradores. Uma vez ocorrida a falha do G1 ou do G2, o barramento ao qual eles estão conectados ficará desenergizado.

Da mesma forma que no item anterior, a Figura 5.11 apresenta uma representação esquemática da árvore de falhas para a configuração com 2 diesel geradores.

O Anexo H mostra o diagrama lógico gerado pelo código SAPHIRE para essa condição.

Figura 5.9 – Árvore de Falhas para a Configuração 4 DG

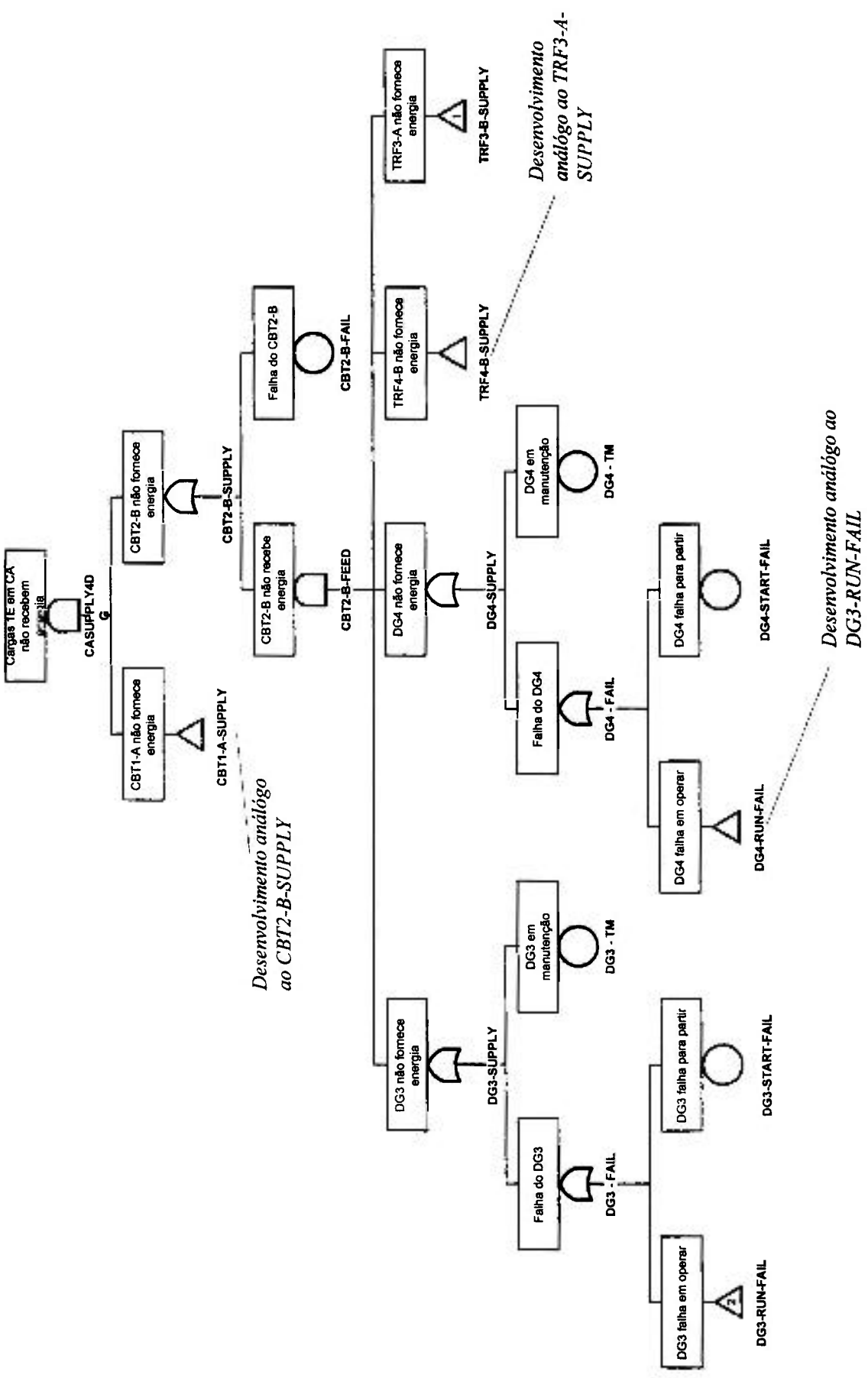


Figura 5.9 – Árvore de Falhas para a Configuração 4 DG (cont.)

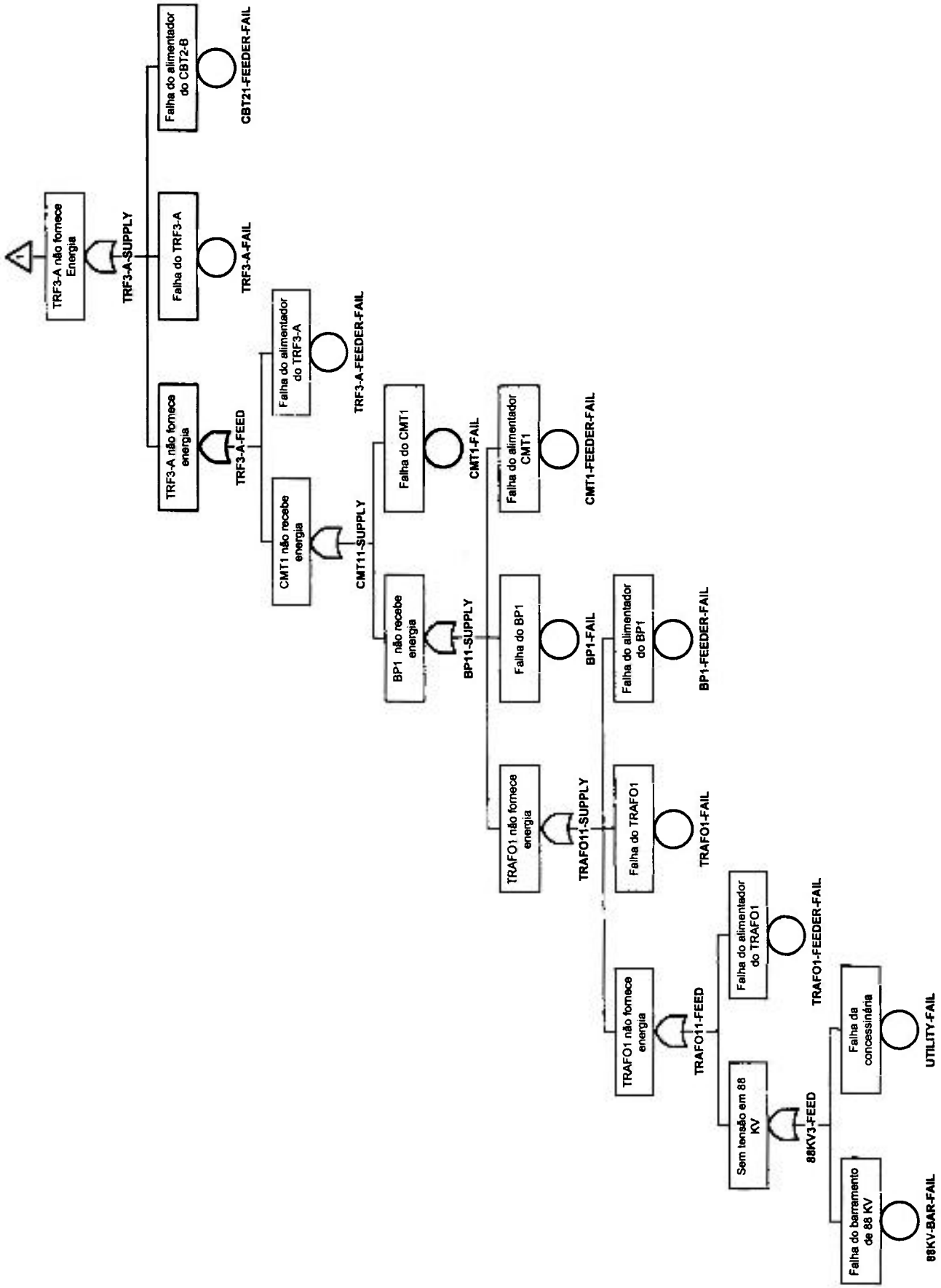


Figura 5.9 – Árvore de Falhas para a Configuração 4 DG (cont.)

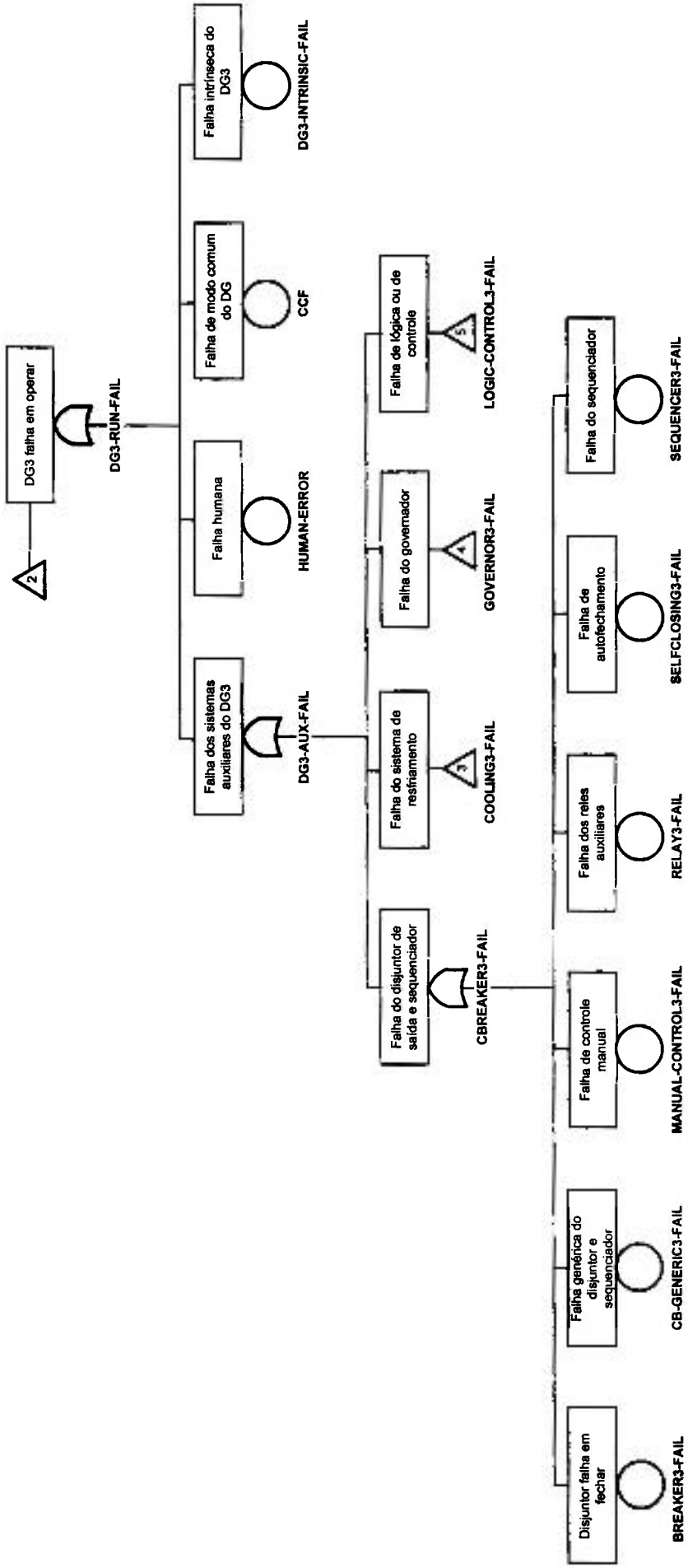


Figura 5.9 – Árvore de Falhas para a Configuração 4 DG (cont.)

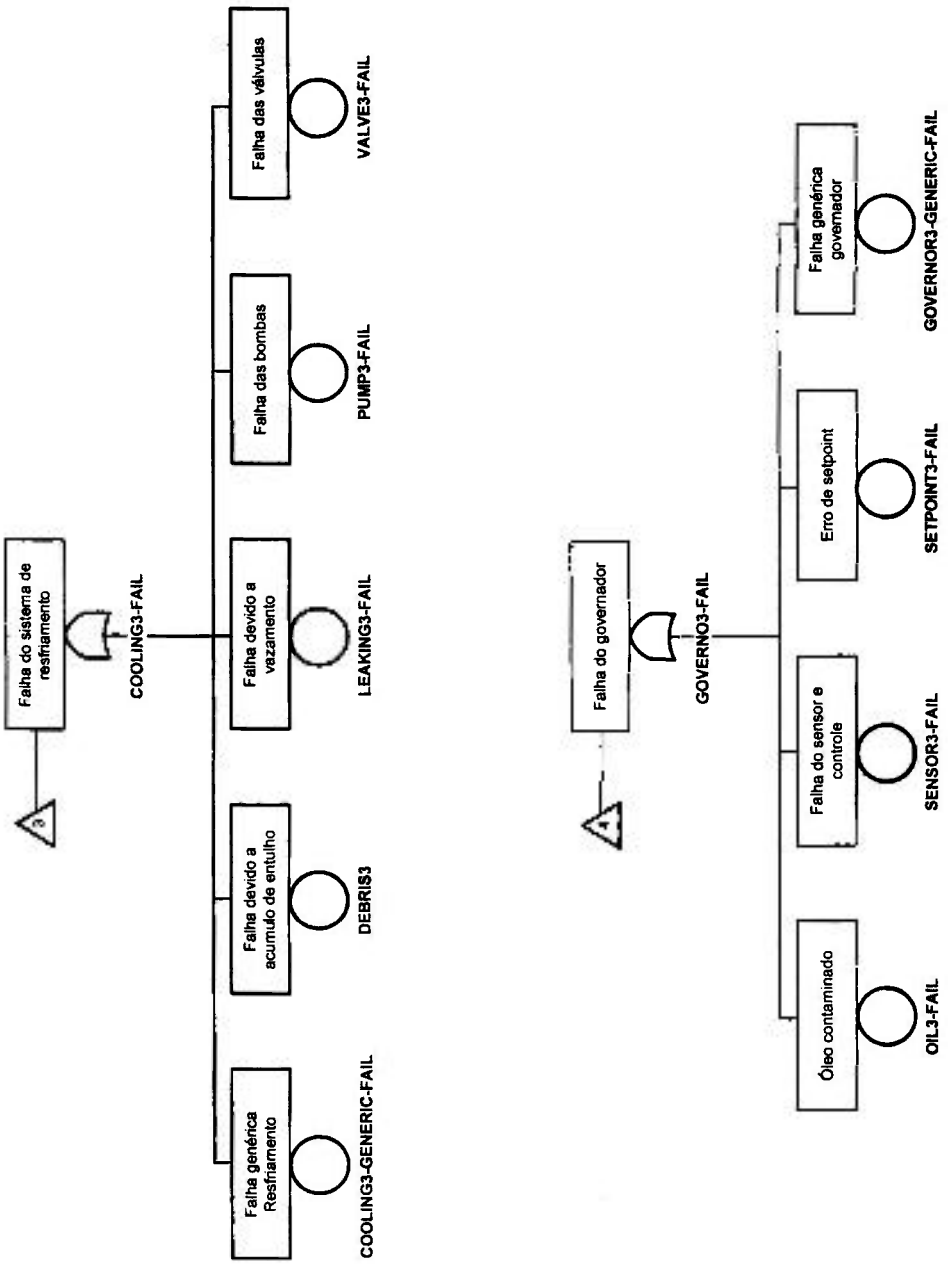


Figura 5.9 – Árvore de Falhas para a Configuração 4 DG (cont.)

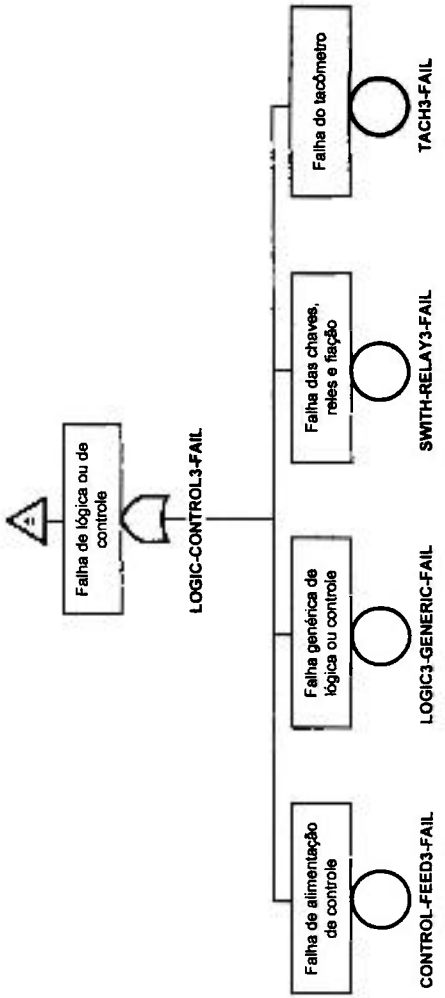
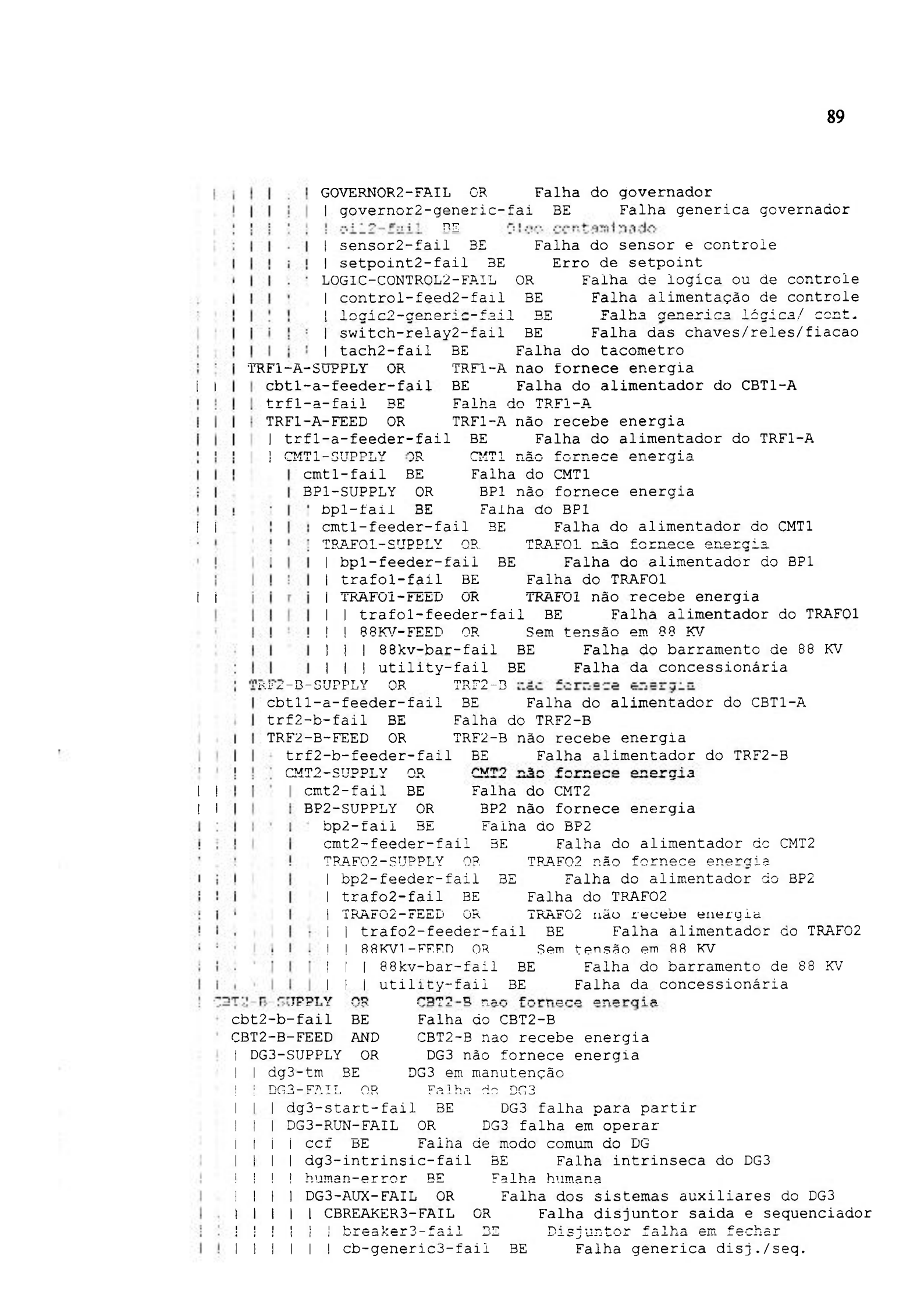


Tabela 5.5 Lógica da Árvore de Falhas para a Configuração 4 DG

```
CASUPPLY4DG  AND     Cargas 1E em CA nao recebem energia
| CBT1-A-SUPPLY  OR      CBT1-A nao fornece energia
| | cbt1-a-fail  BE      Falha do CBT1-A
| | CBT1-A-FEED  AND     CBT1-A nao recebe energia
  | DG1-SUPPLY  OR       DG1 não fornece energia
  | | dg1-t&m  BE        DG1 em manutenção
  | | DG1-FAIL  OR       Falha do DG1
  | | | dg1-start-fail  BE      DG1 falha para partir
  |   DG1-RUN-FAIL  OR      DG1 falha em operar
  |   | ccf  BE       Falha de modo comum do DG
  |   | dg1-intrinsic-fail  BE      Falha intrinseca do DG
  |   | human-error  BE      Falha humana
  |   | DG1-AUX-FAIL  OR      Falha dos sistemas de suporte do DG1
  |   |   | CBREAKER-FAIL  OR      Falha do disj. saída e seq.
  |   |   | | breaker-fail  BE      Disjuntor falha em fechar
  |   |   | | cb-generic-fail  BE      Falha genérica disj. e seq.
  |   |   | | manual-control-fail  BE      Falha de controle manual
  |   |   | | relay-fail  BE      Falha dos relés auxiliares
  |   |   | | selfclosing-fail  BE      Falha de autofechamento
  |   |   | | sequencer-fail  BE      Falha do sequenciador
  |   |   | COOLING-FAIL  OR      Falha do sistema de resfriamento
  |   |   | | cooling-generic-fail  BE      Falha genérica sist. Resf.
  |   |   | | debris  BE      Falha devido a acumulo de entulho
  |   |   | | leaking  BE      Falha devido a vazamento
  |   |   | | pump-fail  BE      Falha das bombas
  |   |   | | valve-fail  BE      Falha das válvulas
  |   |   | GOVERNOR-FAIL  OR      Falha do governador
  |   |   | | governor-generic-fail  BE      Falha genérica governador
  |   |   | | oil-fail  BE      Óleo contaminado
  |   |   | | sensor-fail  BE      Falha do sensor e controle
  |   |   | | setpoint-fail  BE      Erro de setpoint
  |   |   | LOGIC-CONTROL-FAIL  OR      Falha de lógica ou de controle
  |   |   | | control-feed-fail  BE      Falha da alimentação controle
  |   |   | | logic-generic-fail  BE      Falha genérica lógica/controle
  |   |   | | switch-relay-fail  BE      Falha das chaves/reles/fiação
  |   |   | | tach-fail  BE      Falha do tacômetro
  | DG2-SUPPLY  OR      DG2 não fornece energia
  | | dg2-t&m  BE      DG2 em manutenção
  | | DG2-FAIL  OR      Falha do DG2
  |   | dg2-start-fail  BE      DG2 falha para partir
  |   | DG2-RUN-FAIL  OR      DG2 falha em operar
  |   | | ccf  BE      Falha de modo comum do DG
  |   | | dg2-intrinsic-fail  BE      Falha intrinseca do DG2
  |   | | human-error  BE      Falha humana
  |   | | DG2-AUX-FAIL  OR      Falha dos sistemas auxiliares do DG2
  |   | | | CBREAKER2-FAIL  OR      Falha do disj. saida e seq.
  |   | | | | breaker2-fail  BE      Disjuntor falha em fechar
  |   | | | | cb2-generic-fail  BE      Falha generica disj. e seq.
  |   | | | | manual-control2-fail  BE      Falha de controle manual
  |   | | | relay2-fail  BE      Falha dos reles auxiliares
  |   | | | | selfclosing2-fail  BE      Falha de autofechamento
  |   | | | sequencer2-fail  BE      Falha do sequenciador
  |   | | COOLING2-FAIL  OR      Falha do sistema de resfriamento
  |   | | | cooling2-generic-fail  BE      Falha generica sist. Resf.
  |   | | | | debris2-fail  BE      Falha devido acumulo de entulho
  |   | | | | leaking2-fail  BE      Falha devido a vazamento
  |   | | | pump2-fail  BE      Falha das bombas
  |   | | | | valve2-fail  BE      Falha das valvulas
```


GOVERNOR2-FAIL OR Falha do governador
governor2-generic-fai BE Falha generica governador
oil2-fail BE Oleo contaminado
sensor2-fail BE Falha do sensor e controle
setpoint2-fail BE Erro de setpoint
LOGIC-CONTROL2-FAIL OR Falha de logica ou de controle
control-feed2-fail BE Falha alimentação de controle
logic2-generic-fail BE Falha generica lógica/ cont.
switch-relay2-fail BE Falha das chaves/reles/fiacao
tach2-fail BE Falha do tacometro
TRF1-A-SUPPLY OR TRF1-A nao fornece energia
cbt1-a-feeder-fail BE Falha do alimentador do CBT1-A
trf1-a-fail BE Falha do TRF1-A
TRF1-A-FEED OR TRF1-A não recebe energia
trf1-a-feeder-fail BE Falha do alimentador do TRF1-A
CMT1-SUPPLY OR CMT1 não fornece energia
cmt1-fail BE Falha do CMT1
BP1-SUPPLY OR BP1 não fornece energia
bp1-fail BE Falha do BP1
cmt1-feeder-fail BE Falha do alimentador do CMT1
TRAFO1-SUPPLY OR TRAFO1 não fornece energia
bp1-feeder-fail BE Falha do alimentador do BP1
trafo1-fail BE Falha do TRAFO1
TRAFO1-FEED OR TRAFO1 não recebe energia
trafo1-feeder-fail BE Falha alimentador do TRAFO1
88KV-FEED OR Sem tensão em 88 KV
88kv-bar-fail BE Falha do barramento de 88 KV
utility-fail BE Falha da concessionária
TRF2-B-SUPPLY OR TRF2-B nao fornece energia
cbt11-a-feeder-fail BE Falha do alimentador do CBT1-A
trf2-b-fail BE Falha do TRF2-B
TRF2-B-FEED OR TRF2-B não recebe energia
trf2-b-feeder-fail BE Falha alimentador do TRF2-B
CMT2-SUPPLY OR CMT2 não fornece energia
cmt2-fail BE Falha do CMT2
BP2-SUPPLY OR BP2 não fornece energia
bp2-fail BE Falha do BP2
cmt2-feeder-fail BE Falha do alimentador do CMT2
TRAFO2-SUPPLY OR TRAFO2 não fornece energia
bp2-feeder-fail BE Falha do alimentador do BP2
trafo2-fail BE Falha do TRAFO2
TRAFO2-FEED OR TRAFO2 não recebe energia
trafo2-feeder-fail BE Falha alimentador do TRAFO2
88KV1-FEED OR Sem tensão em 88 KV
88kv-bar-fail BE Falha do barramento de 88 KV
utility-fail BE Falha da concessionária
CBT2-B-SUPPLY OR CBT2-B nao fornece energia
cbt2-b-fail BE Falha do CBT2-B
CBT2-B-FEED AND CBT2-B nao recebe energia
DG3-SUPPLY OR DG3 não fornece energia
dg3-tm BE DG3 em manutenção
DG3-FAIL OR Falha do DG3
dg3-start-fail BE DG3 falha para partir
DG3-RUN-FAIL OR DG3 falha em operar
ccf BE Falha de modo comum do DG
dg3-intrinsic-fail BE Falha intrinseca do DG3
human-error BE Falha humana
DG3-AUX-FAIL OR Falha dos sistemas auxiliares do DG3
CBREAKER3-FAIL OR Falha disjuntor saida e sequenciador
breaker3-fail BE Disjuntor falha em fechar
cb-generic3-fail BE Falha generica disj./seq.

```
| | | |   | | manual-control3-fail  BE     Falha de controle manual
|   | |   | | relay3-fail  BE     Falha dos reles auxiliares
|   | |   | | selfclosing3-fail  BE     Falha de autofechamento
|     |   | | sequencer3-fail  BE     Falha do sequenciador
| | | |   | COOLING3-FAIL  OR     Falha do sistema de resfriamento
|   | |   | | cooling3-generic-fail  BE     Falha generica sist. Rest.
|   | |   | | debris3  BE     Falha devido acumulo de entulho
|   | |   | | leaking3-fail  BE     Falha devido a vazamento
|     |   | | pump3-fail  BE     Falha das bombas
|   | |   | | valve3-fail  BE     Falha das valvulas
|   | |   |   GOVERNOR3-FAIL  OR     Falha do governador
|   | |   |   | governor3-generic-fai  BE     Falha generica governador
| | | | | |   oil3-fail  BE     Oleo contaminado
| | | |   | | sensor3-fail  BE     Falha do sensor e controle
| | | |   | | setpoint3-fail  BE     Erro de setpoint
|   | |   | | LOGIC-CONTROL3-FAIL  OR     Falha de logica ou de controle
| | | |   |   control-feed3-fail  BE     Falha alimentacao de controle
|   | |   |   logic3-generic-fail  BE     Falha generica lógica/cont.
|   | |   |   swith-relay3-fail  BE     Falha chaves, reles e fiacao
| | | |   | | tach3-fail  BE     Falha do tacometro
|   | | DG4-SUPPLY  OR     DG4 não fornece energia
|   | |   | dg4-tm  BE     DG4 em manutenção
|   | |   | DG4-FAIL  OR     Falha do DG4
|   | |   | | dg4-start-fail  BE     DG4 falha para partir
|   | |   | | DG4-RUN-FAIL  OR     DG4 falha em operar
| | | | | | | ccf  BE     Falha de modo comum do DG
| | |   | | dg4-intrinsic-fail  BE     Falha intrinseca do DG4
| |     | | human-error  BE     Falha humana
| |     |   DG4-AUX-FAIL  OR     Falha dos sistemas auxiliares do DG4
| | | | |   | CBREAKER4-FAIL  OR     Falha disjuntor saida e sequenciador
| |       |   | | breaker4-fail  BE     Disjuntor falha em fechar
| |       |   | | cb4-generic-fail  BE     Falha generica disj./seq.
| | | | |   | | manual-control4-fail  BE     Falha de controle manual
| |       |   | | relay4-fail  BE     Falha dos reles auxiliares
| |       |   | | selclosing4-fail  BE     Falha de autofechamento
| |       |   | | sequencer4-fail  BE     Falha do sequenciador
| |       |   | COOLING4-FAIL  OR     Falha do sistema de resfriamento
| |       |   | | cooling4-generic-fail  BE     Falha generica sist. Rest.
| |       |   | | debris4-fail  BE     Falha devido a acumulo de entulho
| |       |   | | leaking4-fail  BE     Falha devido a vazamento
| |       |   | | pump4-fail  BE     Falha das bombas
| |       |   | | valve4-fail  BE     Falha das valvulas
| |       |   | GOVERNOR4-FAIL  OR     Falha do governador
| |       |   | | governor4-generic-fai  BE     Falha generica governador
| |       |   | | oil4-fail  BE     Oleo contaminado
| |       |   | | sensor4-fail  BE     Falha do sensor e controle
| |       |   | | setpoint4-fail  BE     Erro de setpoint
| |       |   | LOGIC-CONTROL4-FAIL  OR     Falha de logica ou de controle
| |       |   | | control-feed4-fail  BE     Falha alimentação de controle
| |       |   | | logic4-generic-fail  BE     Falha generica lógica/ cont.
| |       |   | | switch-relay4-fail  BE     Falha das chaves/reles/fiacao
| |       |   | | tach4-fail  BE     Falha do tacometro
| |     TRF3-A-SUPPLY  OR     TRF3-A não fornece energia
| |     | cbt21-feeder-fail  BE     Falha do alimentador do CBT2-B
| |     | trf3-a-fail  BE     Falha do TRF3-A
| |     | TRF3-A-FEED  OR     TRF3-A não recebe energia
| | | | | trf3-a-feeder-fail  BE     Falha do alimentador do TRF3-A
| | | | CMT11-SUPPLY  OR     CMT1 não fornece energia
| | | | | cmt1-fail  BE     Falha do CMT1
| | |   | BP11-SUPPLY  OR     BP1 não fornece energia
| | |   | | bp1-fail  BE     Falha do BP1
```

```
| | | | | | cmt1-feeder-fail  BE      Falha do alimentador do CMT1
| | | | | | TRAFO11-SUPPLY  OR      TRAFO1 não fornece energia
| | | | | | | bp1-feeder-fail  BE      Falha do alimentador do BP1
| | | | | | | trafo1-fail  BE      Falha do TRAFO1
| | | | | | | TRAFO11-FEED  OR      TRAFO1 não recebe energia
| | | | | | | | trafo1-feeder-fail  BE      Falha alimentador do TRAFO1
| | | | | | | | 88KV3-FEED  OR      Sem tensão em 88 KV
| | | | | | | | | 88kv-bar-fail  BE      Falha do barramento de 88 KV
| | | | | | | | | utility-fail  BE      Falha da concessionária
| | | TRF4-B-SUPPLY  OR      TRF4-B não fornece energia
| | | cbt2-b-feeder-fail  BE      Falha do alimentador do CBT2-B
| | | trf4-b-fail  BE      Falha do TRF4-B
| | | TRF4-B-FEED  OR      TRF4-B não recebe energia
| | | | trf4-b-feeder-fail  BE      Falha do alimentador do TRF4-B
| | | | CMT21-SUPPLY  OR      CMT2 não fornece energia
| | | | | cmt2-fail  BE      Falha do CMT2
| | | | | BP21-SUPPLY  OR      BP2 não fornece energia
| | | | | | bp2-fail  BE      Falha do BP2
| | | | | | cmt2-feeder-fail  BE      Falha do alimentador do CMT2
| | | | | | TRAFO21-SUPPLY  OR      TRAFO2 não fornece energia
| | | | | | | bp1-feeder-fail  BE      Falha do alimentador do BP1
| | | | | | | trafo2-fail  BE      Falha do TRAFO2
| | | | | | | TRAFO21-FEED  OR      TRAFO2 não recebe energia
| | | | | | | | trafo2-feeder-fail  BE      Falha alimentador do TRAFO2
| | | | | | | | 88KV2-FEED  OR      Sem tensão em 88 KV
| | | | | | | | | 88kv-bar-fail  BE      Falha do barramento de 88 KV
| | | | | | | | | utility-fail  BE      Falha da concessionária
```

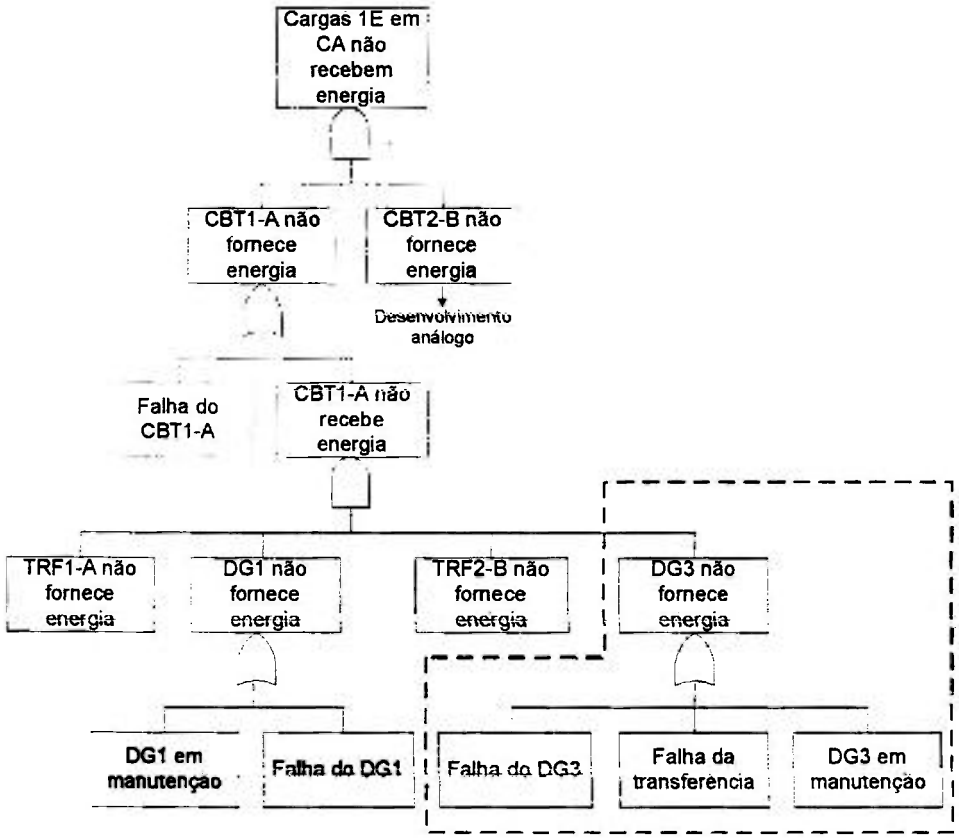


Figura 5.10 - Representação esquemática da árvore de falhas para a configuração com 3 diesel geradores

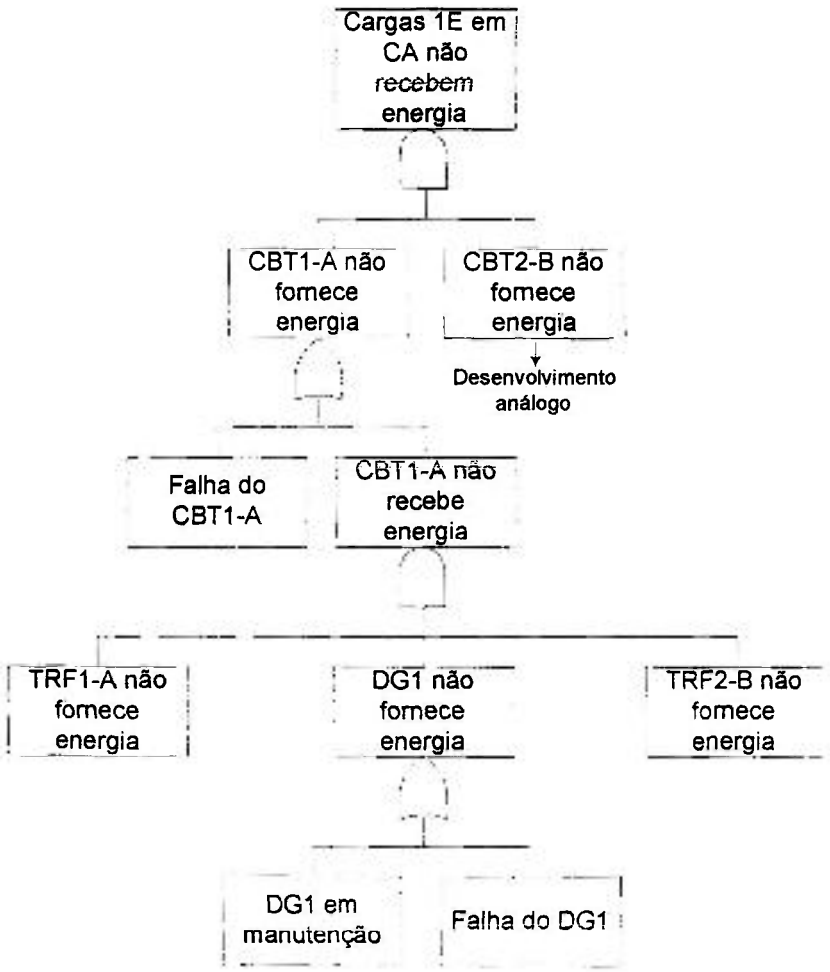


Figura 5.11 Representação esquemática da árvore de falhas para a configuração com 2 diesel geradores

5.6 – Análise de Desempenho do Sistema Elétrico

5.6.1 - Geral

De forma a melhor avaliar a confiabilidade dos arranjos propostos neste estudo, vários casos foram estudados. A Tabela 5.6 mostra um resumo das características de cada caso estudado.

A confiabilidade de cada uma das configurações da subestação de emergência foi estudada considerando o tempo de missão dos diesel geradores em três condições: 0, 10 e 30 horas /6/.

Tendo em vista que a perda da alimentação da concessionária tem grande peso na ocorrência do evento topo estudou-se, para o tempo de missão mais crítico (30 horas), o comportamento de cada uma das três configurações da subestação de emergência considerando, para a fonte externa de suprimento de energia, as mesmas características da linha que alimenta a Central Nuclear Almirante Álvaro Alberto – ANGRA I (freqüência anual de perda de energia igual a 0,36) /24/.

Da mesma forma, para avaliar a contribuição das falhas de modo comum, foram utilizados três valores para o fator beta (0, 0,05, e 0,12) /18/.

Para a configuração da subestação de emergência com 3 DG, foram analisados os casos em que a transferência do diesel gerador é realizada através de uma chave de transferência automática e através da atuação de um operador.

Tabela 5.6 – Resumo dos Casos Estudados

Configuração da Subestação de Emergência	Tempo de missão dos DG	Linha de Transmissão	Fator Beta	Transferência
2 DG	0	CPFL genérica	0,05	
	10	CPFL genérica	0,05	
	30	CPFL genérica	0,05	
	30	CPFL genérica	0	
	30	CPFL genérica	0,12	
	30	Angra I	0,05	
3 DG	0	CPFL genérica	0,05	Automática
	10	CPFL genérica	0,05	Automática
	30	CPFL genérica	0,05	Automática
	30	CPFL genérica	0	Automática
	30	CPFL genérica	0,12	Automática
	30	Angra I	0,05	Automática
	30	CPFL genérica	0,05	Manual
4 DG	0	CPFL genérica	0,05	
	10	CPFL genérica	0,05	
	30	CPFL genérica	0,05	
	30	CPFL genérica	0	
	30	CPFL genérica	0,12	
	30	Angra I	0,05	

5.6.2 – Avaliação do Desempenho

A Tabela 5.7 apresenta os resultados obtidos para as três configurações da subestação de emergência, considerando para os diesel geradores os tempos de missão de 0, 10 e 30 horas. Os resultados mostrados na Tabela 5.7 foram obtidos com os dados da linha de transmissão da CPFL e com fator beta 0,05.

Observa-se que o pior caso, para as três alternativas de configuração da subestação de emergência, ocorre para um tempo de 30 horas. Nessa condição, ao se comparar as três alternativas, nota-se que o corte mínimo *CCF, UTILITY-FAIL* é dominante para todas elas, porém, sua importância aumenta de 15,3% para 60,6% e para 84,9% à medida que aumenta o número de redundâncias dos diesel geradores de dois para três e para quatro, respectivamente.. Conforme comentado anteriormente, o fato da alimentação externa aparecer como corte de grande importância se justifica por se considerar apenas uma linha de transmissão como fonte externa de energia elétrica.

Pela observação dos resultados obtidos, pode-se concluir que a inclusão de mais redundâncias para os diesel geradores proporciona um aumento considerável na confiabilidade do sistema elétrico.

Comparando-se os resultados de freqüência anual apresentados na Tabela 5.7, pode-se verificar que existe uma melhora de aproximadamente 4 vezes quando se passa a utilizar a configuração com três diesel geradores ao invés de dois.

Já uma comparação entre a configuração com 3 DG e a configuração com 4 DG, mostra que a inclusão de um quarto diesel gerador resulta numa melhora de aproximadamente 1,2 vezes na freqüência anual de falhas.

5.7 – Análise Paramétrica

A influência da linha de alimentação externa, das falhas de modo comum e das falhas devido à erros humanos, foi analisada de forma paramétrica, sendo descrita nos itens a seguir.

Tabela 5.7 Cortes Mínimos obtidos para as configurações estudadas

	Tempo Freqüência Anual	Cortes	(%)
2 DG	0 h 9,53E-07	DG1/DG2-START-FAIL, UTILITY-FAIL	36,8
		CCF, UTILITY-FAIL	16,0
		DG1/DG2-START-FAIL, DG1/DG2-INTRINSIC-FAIL	16,0
		88KV-BAR-FAIL, DG1/DG2-START-FAIL	4,1
		88KV-BAR-FAIL, CCF	1,8
	10 h 2,91E-06	CCF, UTILITY-FAIL	18,2
		DG1/DG2-START-FAIL, DG1/DG2-INTRINSIC-FAIL	18,0
		DG1/DG2-START-FAIL, UTILITY-FAIL	12,1
		DG1/DG2-INTRINSIC-FAIL, UTILITY-FAIL	6,7
		88 KV-BAR-FAIL, CCF	2,0
	30 h 6,81E-06	CCF, UTILITY-FAIL	15,3
		DG1/DG2-START-FAIL, DG1/DG2-INTRINSIC-FAIL, UTILITY-FAIL	15,0
		DG1/DG2-START-FAIL, UTILITY-FAIL	5,2
		88KV-BAR-FAIL, CCF	1,7
		88KV-BAR-FAIL, DG1/DG2-INTRINSIC-FAIL	1,2
3 DG	0 h 2,01E-07	CCF, UTILITY-FAIL	75,7
		88 KV-BAR-FAIL, CCF	8,4
		UTILITY-FAIL, DG1/DG2/DG3-START-FAIL	4,4
		HUMAN-ERROR, UTILITY-FAIL	1,8
	10 h 7,41E-07	CCF, UTILITY-FAIL	71,4
		88 KV-BAR-FAIL, CCF	8,0
		HUMAN-ERROR, UTILITY-FAIL	1,7
		DG1/DG2/DG3-START-FAIL, UTILITY-FAIL	1,2
	30 h 1,72E-06	CCF, UTILITY-FAIL	60,6
		88 KV-BAR-FAIL, CCF	6,8
		DG1/DG2/DG3-INTRINSIC-FAIL, UTILITY-FAIL	1,6
		HUMAN-ERROR, UTILITY-FAIL	1,5
4 DG	0 h 1,75E-07	CCF, UTILITY-FAIL	87,1
		88 KV-BAR-FAIL, CCF	9,7
		HUMAN-ERROR, UTILITY-FAIL	2,1
		CBT1-A-FAIL, CBT2-B-FAIL	0,6
	10 h 6,05E-07	CCF, UTILITY-FAIL	87,5
		88 KV-BAR-FAIL, CCF	9,7
		HUMAN-ERROR, UTILITY-FAIL	2,1
		88 KV-BAR-FAIL, HUMAN-ERROR	0,2
	30 h 1,23E-06	CCF, UTILITY-FAIL	84,9
		88 KV-BAR-FAIL, CCF	9,5
		HUMAN-ERROR, UTILITY-FAIL	2,1
		88 KV-BAR-FAIL, HUMAN-ERROR	0,2

Linha de Transmissão da CPFL, Fator Beta 0,05 e Falha Humana 6,0 E -04

5.7.1 – Alimentação Externa

Para efeito de comparação foi assumido, para a linha de transmissão considerada neste estudo, a mesma freqüência de perda de alimentação elétrica externa da usina de Angra I (0,36 falhas por ano) /24/. Foi calculada a freqüência de perda de alimentação elétrica em corrente alternada para as três configurações do sistema elétrico, para um tempo de missão de 30 horas. Os resultados são mostrados na Tabela 5.8.

Comparando os dados obtidos, nota-se uma melhora na freqüência de perda de alimentação elétrica da ordem de 10 vezes, para as três configurações. Nota-se também que os cortes mínimos dominantes passam a ser, para os três casos, a falha do barramento de alta tensão *88 KV-BAR-FAIL* e a contribuição de falha de modo comum dos diesel geradores *CCF*, com importâncias de 15,5%, 61,8% e 86,1% para 2 DG, 3 DG e 4 DG respectivamente. A perda de alimentação da concessionária passa a ter um peso bastante reduzido, confirmando que a central estudada, pelo fato de possuir apenas uma linha de transmissão como fonte externa de energia, é altamente dependente da mesma.

5.7.2 – Transferência Automática/Manual

Para a avaliação da operação de transferência do G3 para o CBT1-A ou CBT2-B, através da chave de transferência, variou-se a taxa de falha da chave desde 7,2E-05 até 1,0E-03. Da mesma forma, ao considerar a transferência manual, variou-se a probabilidade de falha humana desde 2,0E-02 até 6,0E-04. Em ambos os casos, praticamente não foi detectada uma variação significativa da freqüência anual observada originalmente. A Tabela 5.9 apresenta os resultados obtidos.

5.7.2 – Contribuição das Falhas de Modo Comum

De modo a considerar e representar de forma simples a contribuição das falhas de modo comum, foi adotada uma faixa de valores para o fator ß. Além do valor recomendado, foi considerado um valor pessimista e um valor otimista. /17/

Tabela 5.8 Cortes Mínimos obtidos para as configurações estudadas, com dados da linha de transmissão de Angra I e tempo de missão de 30 horas

	Alimentação Freqüência Anual	Cortes	(%)
2 DG 30 h	LT Angra I 7,51E-07	88 KV-BAR-FAIL, CCF	15,5
		88 KV-BAR-FAIL, DG1/DG2-START-FAIL,DG1/DG2-INTRINSIC-FAIL	15,0
		88 KV-BAR-FAIL, DG1/DG2-INTRINSIC-FAIL	11,0
		88 KV-BAR-FAIL, DG1/DG2-START-FAIL	5,2
		CCF, UTILITY-FAIL	1,5
	LT CPFL 6,81E-06	CCF, UTILITY-FAIL	15,3
		DG1/DG2-START-FAIL, DG1/DG2-INTRINSIC-FAIL, UTILITY-FAIL	15,0
		DG1/DG2-START-FAIL, UTILITY-FAIL	5,2
		88KV-BAR-FAIL, CCF	1,7
		88KV-BAR-FAIL, DG1/DG2-INTRINSIC-FAIL	1,2
3 DG 30 h	LT Angra I 1,88E-07	88 KV-BAR-FAIL, CCF	61,8
		CCF, UTILITY-FAIL	6,1
		DG1/DG2/DG3-INTRINSIC-FAIL, 88 KV-BAR-FAIL	1,6
		88 KV-BAR-FAIL, HUMAN-ERROR	1,5
	LT CPFL 1,72E-06	CCF, UTILITY-FAIL	60,6
		88 KV-BAR-FAIL, CCF	6,8
		DG1/DG2/DG3-INTRINSIC-FAIL, UTILITY-FAIL	1,6
		HUMAN-ERROR, UTILITY-FAIL	1,5
4 DG 30 h	LT Angra I 1,34E-07	88 KV-BAR-FAIL, CCF	86,1
		CCF, UTILITY-FAIL	8,5
		88 KV-BAR-FAIL, HUMAN ERROR	2,1
		CBT1-A-FAIL, CBT2-B-FAIL	0,8
	LT CPFL 1,23E-06	CCF, UTILITY-FAIL	84,9
		88 KV-BAR-FAIL, CCF	9,5
		HUMAN-ERROR, UTILITY-FAIL	2,1
		88 KV-BAR-FAIL, HUMAN-ERROR	0,2

Fator Beta 0,05 e Falha Humana 6,0 E -04

Foram calculadas as freqüências de perda de alimentação elétrica em corrente alternada para os diferentes valores do fator ß, para as três configurações da subestação de emergência, para um tempo de missão de 30 horas. A Tabela 5.10 apresenta os resultados obtidos.

Comparando os resultados obtidos sem a contribuição das falhas de modo comum (fator ß = 0) com os resultados obtidos considerando-se a contribuição das falhas de modo comum (fator ß = 0,05 e fator ß = 0,12) pode ser visto que o fato de se considerar a contribuição das falhas de modo comum é bastante significante. Por outro lado, uma comparação da freqüência total de perda de alimentação elétrica obtida utilizando-se fator ß = 0,05 e fator ß = 0,12 mostra que houve um aumento 1,95 vezes para a configuração com três diesel geradores e 2,3 vezes para a configuração com 4 diesel geradores.

COMISSÃO NACIONAL DE ENERGIA NUCLEAR/SP-IPEN

Tabela 5.9 Freqüências anuais de perda de alimentação elétrica para os casos de transferência automática e manual

Configuração	Transferência	Taxa de falha da chave	Probabilidade de Falha Humana	Freqüência obtida
3 DG 30 horas	Automática	1,0E-03	----------	1,74 E-06
		7,2E-05	----------	1,72 E-06
	Manual	----------	2,0 E-02	1,83 E-06
		----------	6,0 E-04	1,73 E-06

Linha de Transmissão da CPFL e Fator Beta 0,05

Tabela 5.10 Freqüências anuais de perda de alimentação elétrica para diferentes valores do fator ß

Configuração	ß = 0	ß = 0,05 (recomendado)	ß = 0,12 (alto)
2 DG	5,65E-06	6,81E-06	8,45E-06
3 DG	5,61E-07	1,72E-06	3,36E-06
4 DG	6,97E-08	1,23E-06	2,87E-06

Linha de Transmissão da CPFL e Falha Humana 6,0 E -04

6 – CONCLUSÕES E RECOMENDAÇÕES

O objetivo deste trabalho foi estudar o sistema diesel elétrico de emergência de um reator nuclear de pequeno porte. Foram consideradas três configurações típicas e analisadas suas confiabilidades.

A análise dos estudos de confiabilidade das fontes de suprimento de energia elétrica de emergência, anteriormente realizados, aponta para a necessidade de se definir, de forma bastante clara, os requisitos de confiabilidade dos diesel geradores, bem como de ser ter procedimentos de operação e manutenção completos e detalhados e uma equipe de operadores com treinamento adequado.

A confiabilidade foi estudada segundo o método da árvore de falhas e a quantificação feita com o emprego do código SAPHIRE.

Foi possível identificar a melhor configuração em termos de confiabilidade e estudar a influência da linha de transmissão, das falhas de modo comum e das ações do operador.

Os resultados obtidos comprovam que a alimentação externa da central é o item de maior peso. Os cortes mínimos mostram que a falha da alimentação externa está sempre entre os de maior importância enfatizando a forte dependência que a central tem do sistema externo de energia.

É interessante ressaltar que o uso de quatro diesel geradores de emergência compensou a falta de uma segunda linha de alimentação externa, levando o nível de confiabilidade do suprimento de energia elétrica em corrente alternada a níveis aceitáveis.

O presente trabalho deu ênfase ao sistema diesel elétrico abordando para esse sistema, as falhas de modo comum e as falhas humanas. Sistemas como abastecimento de óleo combustível, sistema de ar de partida, e mesmo as intervenções de operadores no restante dos componentes do sistema elétrico não foram estudados e podem ser foco de futuros trabalhos mais detalhados.

Da mesma forma, uma avaliação da contribuição das falhas de modo comum pode ser objeto de um estudo detalhado, empregando-se métodos mais completos como o das múltiplas letras gregas.

Para um trabalho mais abrangente e detalhado, sugere-se um estudo completo do sistema elétrico, conforme descrito no Anexo E, de forma a considerar todos os componentes susceptíveis a falhas de modo comum.

Os resultados do trabalho podem também dar subsídios para futuros estudos de "*station blackout*" ou para análises probabilísticas de segurança visando identificar as seqüências que podem levar à ocorrência de acidentes severos.

7 - REFERÊNCIAS

/1/ United States Nuclear Regulatory Commission. **Reactor Safety Study - An Assessment Of Accident Risks In U.S. Commercial Nuclear Power Plants.** October, 1975 (WASH – 1400/ NUREG – 75/014).

/2/ Safety Series 50-SG-D7 – **Emergency Power Systems at Nuclear Power Plants** - 1988

/3/ Safety Series 75 – INSAG 3 – **Basic Safety Principles for Nuclear Power Plants** - 1988

/4/ United States Nuclear Regulatory Commission. **Severe Accident Risks – An Assesment for Five United States Nuclear Power Plants – Final Summary Report.** December 1990, (NUREG 1150).

/5/ United States Nuclear Regulatory Commission. **Evaluation of Station BlackOut Accidents at Nuclear Power Plants**. June, 1988 (NUREG 1032).

/6/ United States Nuclear Regulatory Commission. **Reliability of Emergency AC Power Systems at Nuclear Power Plants.** July, 1983 (NUREG/CR-2989).

/7/ United States Nuclear Regulatory Commission. **Proposed Staff Actions to Improve and Maintain Diesel Generator Reliability.** July, 1984 (Generic Letter 84-15).

/8/ United States Nuclear Regulatory Commission. **Emergency Diesel Generator Operating Experience, 1981 – 1983**. – October, 1985 (NUREG/CR-4347).

/9/ Nuclear Energy Agency - Committee on The Safety of Nuclear Installations. **Loss of Safety System Functions – "Pilot Examination os Generic Safety Functions".** November, 1986 (CSNI Report n. 127 – Volume I).

/10/ Nuclear Energy Agency - Committee on The Safety of Nuclear Installations **Project Report on Collection and Analysis of Common-Cause Failures of Emergency Diesel Generators.** May, 2000 (NEA/CSNI/R(2000)20).

/11/ United States Nuclear Regulatory Commission - Code of Federal Regulations. **General Design Criteria for Nuclear Power Plants, Title 10 –**

Energy, Part 50 – Domestic Licensing of Production and Utilization Facilities – Appendix A. USA, 1991 (10-CFR-50).

/12/ Brookhaven National Laboratory. **Design Guide for Category II Reactors - Light and Heavy Water Cooled Reactors - Chapter 8 – Electric Power.** (BNL 50831-II).

/13/ Associação Brasileira de Normas Técnicas. **Requisitos Gerais de Suprimento de Energia Elétrica para os Sistemas de Segurança de Usinas Nucleolétricas.** Novembro, 1984 (NBR-8671)

/14/ United States Nuclear Regulatory Commission **Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants – LWR Edition.** July, 1981 (NUREG-0800)

/15/ Comissão Nacional de Energia Nuclear. **Licenciamento de Instalações Nucleares**. Dezembro,1984 (CNEN-NE-1.04).

/16/ Comissão Nacional de Energia Nuclear.CNEN-NN-1.16. ***Garantia da Qualidade para a Segurança de Usinas Nucleolétricas e outras Instalações***. Setembro, 1999 (CNEN-NN-1.16).

/17/ Horomitsu Kumamoto, Ernest J. Henley - ***Probabilistic Risk Assessment and Management for Engineers and Scientists*** – IEEE Press, 1996.

/18/ United States Nuclear Regulatory Commission. **Procedures for Treating Common Cause Failures in Safety and Reliability Studies**. January, 1988 (NUREG/CR-4780).

/19/ American Nuclear Society. K. N. Fleming and P. H. Raabe. **A comparison of three methods for the quantitative analysis of common cause failures in "Probabilistic Analysis of Nuclear Reactor Safety", Vol. 3.** 1978.

/20/ United States Nuclear Regulatory Commission. **Probabilistic Safety Analysis Procedures Guide.** 1984 (NUREG/CR-2815)

/21/ Institute of Electrical and Electronics Engineers IEEE - **Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems** – 1980 (IEEE Std 493).

/22/ Institute of Electrical and Electronics Engineers IEEE **Guide to the Collection and Presentation of Electrical, Electronic, Sensing**

Component and Mechanical Equipment Reliability Data for Nuclear Power Generating Stations. (IEEE Std 500)

/23/ United States Department of Energy – Idaho National Engineering. **Generic Component Failure Data Base for Light Water and Liquid Sodium Reactor PRA´s – Informal Report**. February, 1990 (EGG-SSRE-8875).

/24/ Eletrobrás Termonuclear S.A. – Usina Nuclear de Angra I **Análise Probabilística de Segurança**. Dezembro, 1998.

/25/ Nuclear Energy Agency - *Committee on The Safety of Nuclear Installations*. **Operating Experience Relating to On-Site Electric Power Sources – Proceedings of a Specialist Meeting**. February,1986 (CSNI Report n. 115 – vol. 1).

/26/ United States Nuclear Regulatory Commission. **Enhancements of On-Site Emergency Diesel Generator Reliability**. January, 1979 (NUREG/CR-0660).

/27/ United States Nuclear Regulatory Commission. **Station Blackout Accident Analisys.** April, 1983 (NUREG/CR-3226).

/28/ Norman J. McCornick – **Reliability and Risk Analysis: Methods and Nuclear Power Applications** – Academic Press, 1981.

/29/ United States Nuclear Regulatory Commission. **Fault Tree Handbook.** January, 1981 (NUREG-0492).

/30/ Idaho National Engineering and Environmental Laboratory – INEEL - **Systems Analysis Programs for Hands-On Integrated Reliability Evaluations – SAPHIRE** – Version 5.41

ANEXO A – Falhas dos Diesel Geradores por Demanda por Planta

Nome da Planta	Relatórios 1981 a 1983			Generic Letter 84-15		
	D	F	F/D	D	F	F/D
Arkansas Nuclear 1, 2	208	5	0.024	400	8	0.020
Arnold	153	0	0	200	3	0.015
Beaver Valley 1	99	2	0.020	200	29	0.145
Big Rock Point	333	2	0.006	455	10	0.022
Browns Ferry 1, 2, 3	744	10	0.013	800	11	0.014
Brunswick 1, 2	144	14	0.097	400	16	0.040
Calvert Cliffs 1, 2	1137	13	0.011	300	0	0
Connecticut Yankee	186	2	0.011	---	---	0.01
D. C. Cook 1, 2	303	7	0.023	400	9	0.023
Cooper	160	8	0.050	200	15	0.075
Crystal River 3	186	7	0.038	200	9	0.045
Davis-Besse	234	2	0.009	200	5	0.025
Dresden 2, 3	276	6	0.022	300	13	0.043
J. M. Farley 1, 2	1050	12	0.011	500	7	0.014
J. A. FitzPatrick	249	1	0.004	200	1	0.005
Fort Calhoun	81	1	0.012	189	17	0.090
Fort St. Vrain	186	4	0.022	---	---	---
R. E. Ginna	169	0	0	200	9	0.045
Grand Gulf	154	17	0.110	240	5	0.021
E. I. Hatch 1, 2	837	12	0.014	500	3	0.006
Indian Point 2	561	0	0	851	1	0.001
Indian Point 3	150	0	0	300	0	0
Kewaunee	465	2	0.002	200	11	0.060
LaCrosse	256	2	0.008	200	3	0.015
LaSalle	146	1	0.007	206	1	0.005
McGuire	126	4	0.032	184	7	0.038
Maine Yankee	97	2	0.021	200	14	0.070
Millatone 1, 2	641	5	0.008	---	---	---
Monticello	102	1	0.010	200	0	0
Nine Mile Point	77	1	0:013	200	2	0.010
North Anna 1, 2	384	5	0.013	400	6	0.015
Oyster Creek	267	2	0.007	200	2	0.010

ANEXO A - Falhas dos Diesel Geradores por Demanda por Planta (cont.)

Nome da Planta	LER 1981 a 1983			Generic Letter 84-15		
	D	F	F/D	D	F	F/D
Palisades	78	4	0.051	200	7	0.035
Peach Bottom 1, 2	789	2	0.003	400	1	0.003
Pilgrim	228	2	0.009	200	8	0.040
Point Beach 1, 2	237	1	0.004	200	2	0.010
Prairie Island 1, 2	264	0	0	---	---	---
Quad Cities 1, 2	253	4	0.016	---	---	---
Rancho Seco	111	1	0.009	200	12	0.060
H. B. Robinson	104	2	0.019	200	2	0.010
St. Lucie 1, 2	227	3	0.013	80	1	0.013
Salem 1, 2	474	8	0.017	489	14	0.029
San Onofre 1, 2, 3	575	9	0.016	1121	16	0.014
Sequoyah 1, 2	359	11	0.031	400	3	0.008
V. C. Summer	49	3	0.061	77	1	0.013
Surry 1, 2	157	1	0.006	300	4	0.013
Susquehanna	136	1	0.007	209	4	0.019
Trojan	117	0	0	205	19	0.093
Turkey Point 3. 4	402	4	0.010	200	3	0.015
Vermont Yankee	159	2	0.013	200	4	0.020
Yankee Rowe	189	1	0.005	300	1	0.003
Zion 1, 2	960	9	0.009	500	2	0.024

Onde:

D: Demandas de todos os diesel da planta

F: Falhas de todos os diesel da planta

F/D: Falhas por demanda

Fonte: NUREG 4347 /7/

ANEXO B – Símbolos Empregados na Árvore de Falhas

Portões Lógicos

Portão "OU": representa a operação lógica que define a ocorrência do evento ligado à saída do portão quando pelo menos um de seus eventos de entrada ocorrer.

Portão "E": representa a operação lógica pela qual o evento ligado à saída do portão somente ocorre quando todos os eventos de entrada ocorrerem.

Portão "E PRIORITÁRIO": evento de saída ocorre se e somente se todos os eventos de entrada ocorrerem um a um, da esquerda para a direita.

Portão "K de N": o evento de saída ocorre se K da N entradas ocorrerem.

Portão "INIBIDOR": é um caso especial de portão lógico do tipo "E", onde uma das entradas é um evento inibidor. O evento de saída somente ocorrequando o evento "X" satisfizer a condição imposta pelo evento inibidor.

Portão "NÃO": inverte a lógica, isto é, a saída é o complemento da entrada.

Portão "OU NEGADO": inverte a lógica do portão "OU", isto é, o evento de saída ocorre se e somente se nenhum dos eventos entrada ocorrerem.

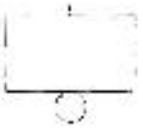
Portão "E NEGADO": inverte a lógica do portão "E", isto é, o evento de saída ocorre se e somente se pelo menos um evento entrada não ocorrer.

ANEXO B – Símbolos Empregados na Árvore de Falhas (cont.)

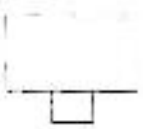
Eventos

Evento TOPO : constitui o ponto inicial da árvore de falhas e representa o evento indesejável principal cujas causas são objeto da análise

Evento INTERMEDIÁRIO : constitui um evento de ligação de portões lógicos e representa um evento causa ou efeito, respectivamente, ao portão ao qual dá entrada e saída



Evento BÁSICO : constitui um ponto terminal numa árvore de falhas onde se atingiu o limite de resolução

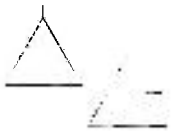


Evento NÃO-DESENVOLVIDO : constitui um ponto terminal numa árvore de falhas e representa um evento cujas causas não são de interesse ou não são possíveis de se avaliar

Evento de ACIONAMENTO ("HOUSE EVENT") : o evento de acionamento constitui um ponto terminal numa árvore de falhas e representa uma chave de acionamento de ramos da árvore

Evento INIBIDOR : constitui um ponto terminal numa árvore de falhas e representa uma condição ou evento de restrição para a ocorrência de um terceiro evento. É usado como entrada de um portão inibidor

Transferidores

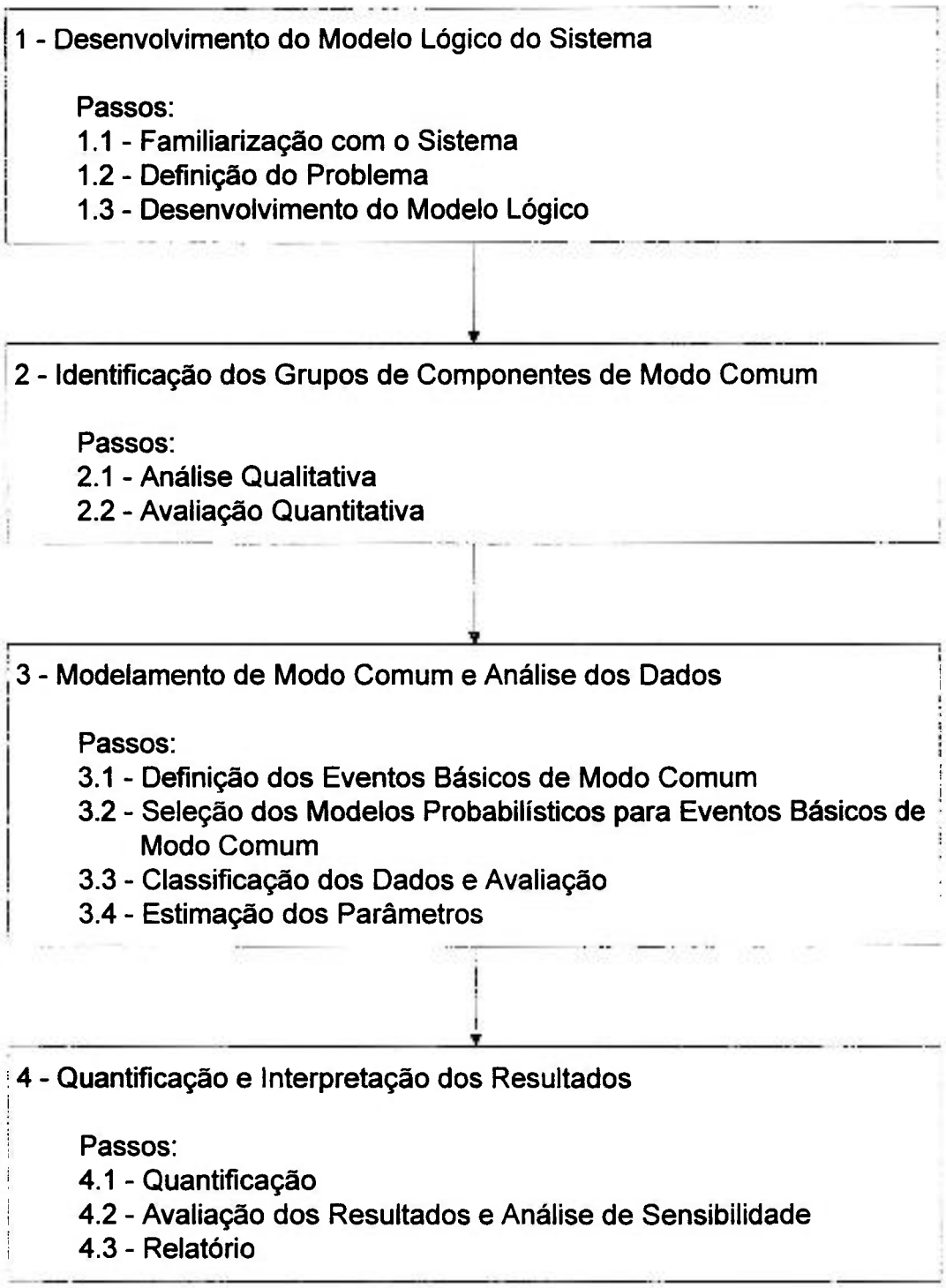


TRANSFERIDORES : utilizados em pares identificados por um determinado número ou letra, indicam que a continuação da árvore num triângulo de saída encontra-se no triângulo de entrada correspondente

TRANSFERIDORES POR SIMILARIDADE : utilizados em pares identificados por um determinado número ou letra, indicam que a continuação da árvore num triângulo de saída é semelhante (mas não idêntica) àquela localizada no triângulo de entrada correspondente

COMISSÃO NACIONAL DE ENERGIA NUCLEAR/SP-IPEN

ANEXO C -Roteiro para Análise de Falhas de Modo Comum



Fonte: NUREG/CR – 4780 /18/

ANEXO D – Valores Recomendados para o Fator Beta

Component	Reactor Years	Number of Events Classified[a]	Event Distribution[b]			Generic Beta Factor
			Independent	Dependent	Generic Common Cause Events	
					Potential / Actual	
Reactor Trip Breakers	583	72	56	16	3 / 8	.19
Diesel Generators	394	674	639	35	8 / 13	.05
Motor-Operated Valves	394	947	842	105	17 / 25	.04
Safety/Relief Valves						
PWR	318	54	30	24	0 / 0	.07
BWR	245	172	136	36	7 / 7	.22
Check Valves	664	254	242	12	3 / 6	.06
Pumps						
Safety Injection	394	112	77	35	2 / 6	.17
RHR	394	117	67	50	2 / 3	.11
Containment Spray	394	48	32	16	1 / 1	.05
Auxiliary Feedwater	394	255	194	61	2 / 3	.03
Service Water	394	203	159	44	2 / 2	.03
Chillers	654	33	27	6	2 / 2	.11
Fans	654	59	49	10	2 / 1	.13
All	-	3,000	2,550	469	62 / 78	.10[c]

[a] Events classified include those having one or more actual or potential component failures or functionally unavailable states.

[b] Independent events are those in category LS (linear, single unit); dependent events are those in the following categories: LM (linear, multiple unit), BSM (branched, single unit, root-caused), and BSC (branched, single unit, component-caused); generic common cause events are a subset of event category BSR that meets screening criteria to be modeled in a systems analysis as a common cause event. Actual common cause events have at least two actual component states.

[c] Average of all component beta factors.

Referência: NUREG/CR-4780 /18/

ANEXO E – Interrupções de Energia da Linha de Transmissão

DATA	DURAÇÃO (h)	DATA	DURAÇÃO (h)
21/1/78 16:53	0,00	4/3/79 15:53	0,04
21/1/78 17:04	0,00	12/3/79 14:00	0,00
21/1/78 17:14	0,00	30/4/79 4:40	22,00
20/2/78 19:20	0,02	3/5/79 17:17	0,00
28/2/78 21:56	0,01	14/5/79 11:54	0,00
25/3/78 18:44	0,02	26/5/79 6:09	0,12
29/3/78 10:00	0,04	29/5/79 13:50	1,04
15/5/78 10:45	0,40	7/6/79 16:07	0,02
18/5/78 3:47	0,01	15/6/79 0:50	0,02
20/5/78 14:24	0,16	1/7/79 14:58	0,02
20/5/78 15:28	0,07	2/7/79 5:14	0,02
8/6/78 20:04	0,20	10/7/79 1:30	0,20
8/6/78 20:24	0,12	10/7/79 1:43	0,02
14/6/78 17:34	0,02	19/7/79 17:20	0,02
15/6/78 8:21	0,08	21/7/79 9:20	0,10
23/6/78 15:24	0,02	22/7/79 4:14	0,06
20/8/78 19:08	0,40	31/7/79 14:18	0,14
1/9/78 15:08	0,02	26/8/79 14:45	0,10
21/9/78 9:16	0,00	26/8/79 15:16	0,72
23/9/78 18:35	0,02	5/9/79 10:32	0,16
26/10/78 7:20	0,14	8/9/79 17:35	0,00
27/10/78 11:55	0,00	8/9/79 17:37	0,00
3/11/78 12:26	0,02	8/9/79 17:38	0,04
15/11/78 9:09	0,02	13/10/79 18:20	0,14
24/11/78 17:14	0,02	19/10/79 10:25	0,00
18/12/78 23:11	0,02	31/10/79 5:42	0,02
30/12/78 18:00	0,02	23/11/79 9:30	0,02
9/1/79 1:05	0,12	27/11/79 17:44	0,02
25/1/79 18:00	0,01	31/12/79 15:34	0,06
27/2/79 13:10	0,00	9/1/80 15:36	0,94

ANEXO E – Interrupções de Energia da Linha de Transmissão (cont.)

DATA	DURAÇÃO (h)	DATA	DURAÇÃO (h)
4/2/80 7:27	0,04	20/2/81 14:53	0,00
15/2/80 16:35	0,02	6/4/81 15:54	0,08
15/2/80 16:37	0,02	10/5/81 12:32	0,02
15/2/80 16:39	0,02	20/6/81 18:56	0,00
15/2/80 16:47	0,02	27/6/81 15:58	0,14
15/2/80 21:40	2,00	14/7/81 17:53	0,02
6/3/80 22:24	0,12	14/7/81 17:59	0,02
8/3/80 16:16	0,28	14/7/81 18:02	0,02
8/3/80 16:46	2,32	3/9/81 20:27	0,01
22/3/80 19:47	0,10	14/9/81 16:42	0,00
14/4/80 19:32	0,02	2/10/81 9:51	0,02
13/5/80 2:08	0,08	15/10/81 18:47	0,12
28/5/80 16:59	0,12	19/10/81 20:29	0,04
7/6/80 17:17	0,02	19/10/81 20:32	0,06
8/6/80 16:52	0,02	31/10/81 17:12	0,02
25/6/80 16:40	0,02	23/11/81 17:05	0,00
2/7/80 12:37	0,28	5/12/81 7:45	0,00
9/8/80 13:58	0,04	5/1/82 22:12	0,02
10/9/80 7:06	0,04	5/1/82 22:36	0,02
20/9/80 18:38	0,84	17/1/82 10:24	0,02
27/9/80 14:38	0,12	2/2/82 16:11	0,00
5/10/80 22:25	0,02	8/2/82 17:15	1,10
8/10/80 3:05	0,10	26/3/82 15:42	0,00
23/10/80 9:53	0,20	17/6/82 10:00	0,20
26/10/80 16:30	0,02	23/8/82 8:30	18,75
22/11/80 18:04	0,36	26/8/82 7:34	0,16
28/11/80 7:35	0,06	27/8/82 18:20	0,04
10/1/81 14:42	0,02	27/9/82 14:56	0,02
21/1/81 7:02	0,02	20/10/82 7:31	0,04
27/1/81 16:22	0,03	26/11/82 21:15	0,04
18/2/81 17:51	0,10	6/12/82 15:25	0,06
20/2/81 14:50	0,02	10/12/82 16:34	0,00

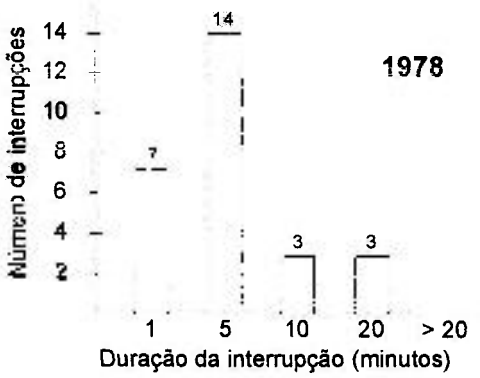
ANEXO E – Interrupções de Energia da Linha de Transmissão (cont.)

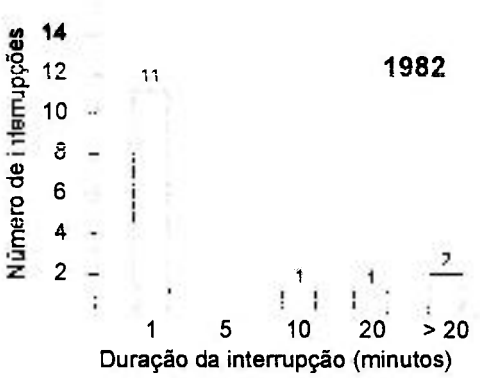
DATA	DURAÇÃO (h)	DATA	DURAÇÃO (h)
10/12/82 16:36	0,00	17/9/85 16:21	0,58
8/1/83 7:12	0,08	17/10/85 13:40	0,24
9/1/83 2:05	0,02	23/11/85 2:45	0,00
9/1/83 2:12	0,04	31/12/85 15:08	0,10
23/2/83 1:47	0,02	25/2/86 15:12	0,00
6/4/83 8:39	0,02	13/3/86 18:51	0,01
16/4/83 15:31	0,04	11/4/86 17:10	0,00
16/4/83 15:38	0,02	17/4/86 12:20	0,06
18/4/83 17:49	0,02	26/4/86 17:57	0,02
18/4/83 17:53	0,02	3/9/86 9:42	0,02
18/4/83 19:42	0,02	14/9/86 0:21	0,06
28/5/83 15:48	0,00	30/11/86 6:42	0,02
6/7/83 15:27	0,02	30/11/86 18:06	0,08
13/9/83 7:52	0,04	21/12/86 3:12	0,04
18/9/83 9:31	0,00	24/12/86 17:10	0,00
29/12/83 20:30	0,00	29/12/86 7:54	0,02
30/12/83 14:45	1,16	3/1/87 15:20	0,00
30/12/83 15:43	23,74	4/1/87 20:13	0,00
17/2/84 15:33	0,00	9/1/87 10:38	0,30
13/3/84 18:10	0,06	16/1/87 17:53	1,59
18/4/84 16:44	3,16	8/3/87 18:33	0,14
17/5/84 22:52	0,01	8/3/87 20:08	0,04
25/6/84 16:14	0,02	27/3/87 10:01	0,04
4/10/84 22:18	0,08	29/3/87 16:05	0,06
29/10/84 16:05	0,04	25/5/87 10:18	0,04
1/12/84 19:05	0,00	19/6/87 7:57	0,66
1/2/85 16:31	0,00	22/6/87 10:08	0,14
14/4/85 12:29	0,28	14/7/87 19:24	0,04
27/8/85 15:59	0,06	14/7/87 19:37	0,30
17/9/85 15:39	0,38	5/8/87 21:08	0,02

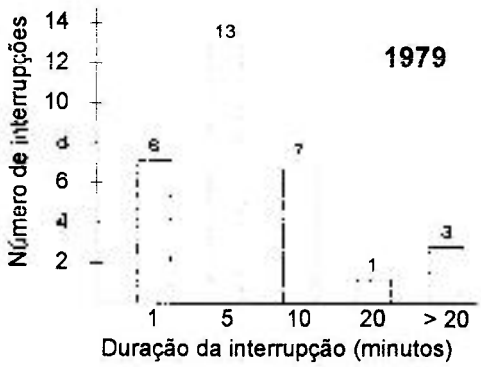
ANEXO E – Interrupções de Energia da Linha de Transmissão (cont.)

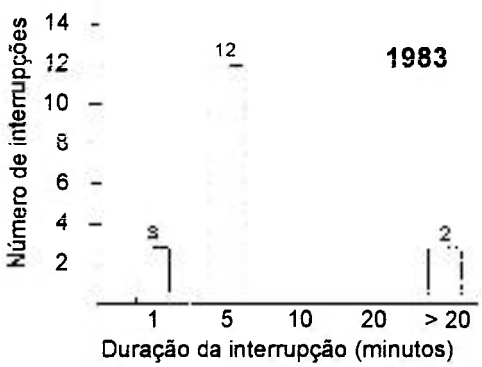
DATA	DURAÇÃO (h)	DATA	DURAÇÃO (h)
6/8/87 10:39	0,02	5/12/90 13:34	0,06
16/3/88 19:05	0,12	1/1/91 15:36	0,00
17/5/88 5:05	0,00	4/2/91 16:45	0,00
17/5/88 5:15	0,00	19/2/91 9:59	0,00
22/5/88 13:18	0,02	29/4/91 10:17	0,02
29/5/88 0:12	0,04	8/7/91 6:24	0,02
29/5/88 0:46	0,04		
28/11/88 14:05	0,06		
23/12/88 16:32	0,00		
5/1/89 15:20	0,02		
11/1/89 3:42	0,04		
12/1/89 5:23	0,02		
28/1/89 21:25	0,02		
29/1/89 8:11	0,04		
1/2/89 4:33	0,16		
28/2/89 17:13	0,04		
4/3/89 18:50	0,04		
28/3/89 14:40	0,08		
12/4/89 8:11	0,18		
8/8/89 15:15	0,16		
9/9/89 1:28	0,00		
26/10/89 12:12	0,00		
3/11/89 12:36	0,04		
22/1/90 18:01	0,05		
1/2/90 16:33	0,00		
8/2/90 6:12	0,20		
9/5/90 15:55	0,36		
5/7/90 17:33	0,00		
14/10/90 22:01	0,08		
23/11/90 17:56	0,00		
30/11/90 15:23	0,02		

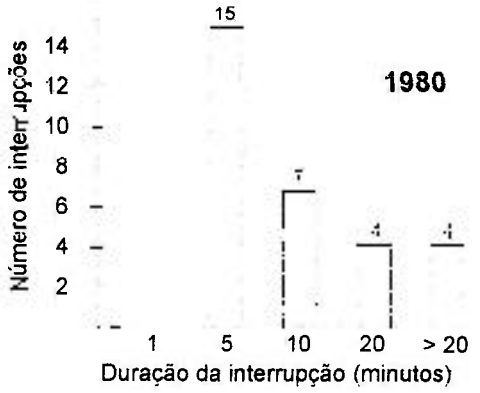
ANEXO F – Histograma das interrupções da Linha de Transmissão

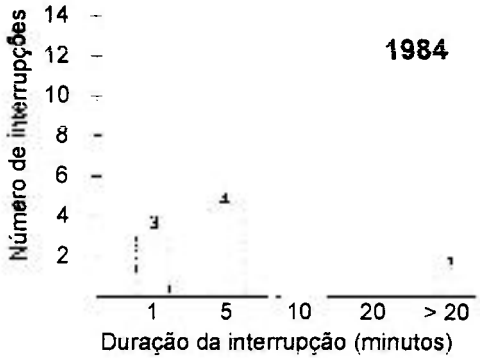


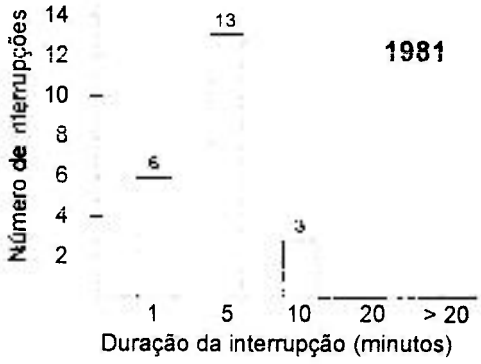


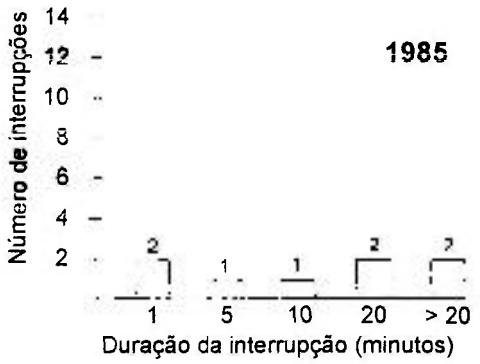




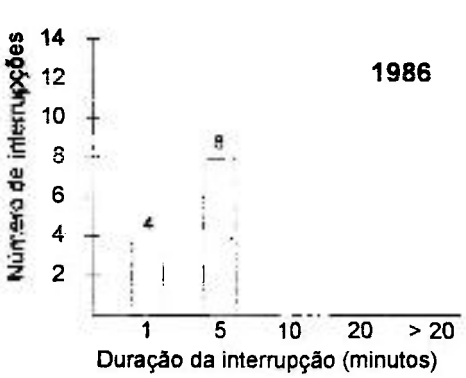


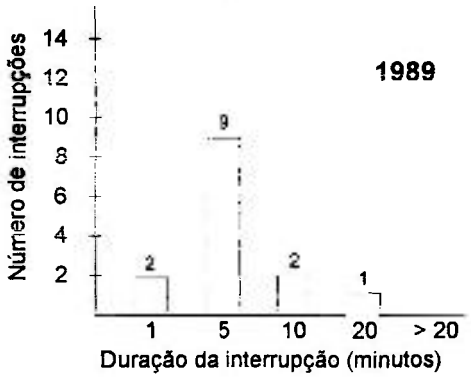


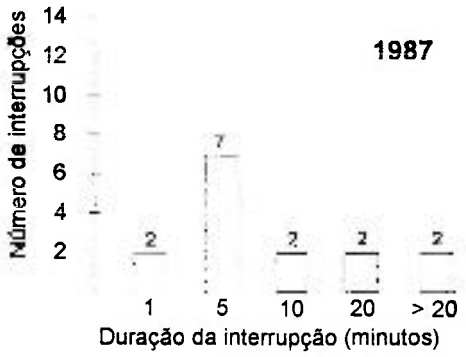


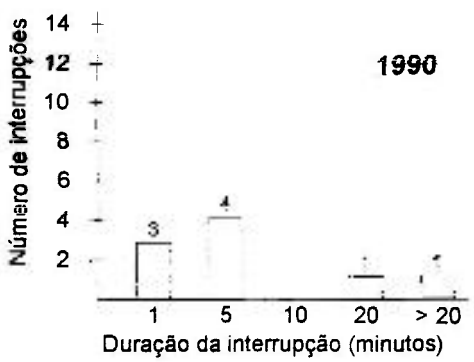


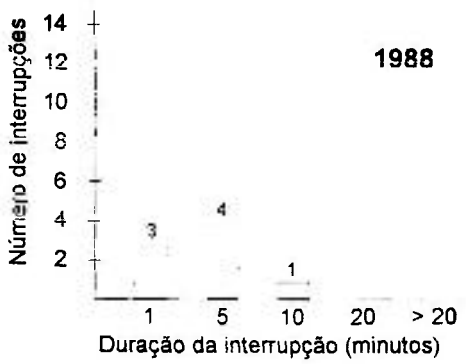
ANEXO F – Histograma das interrupções da Linha de Transmissão (cont.)

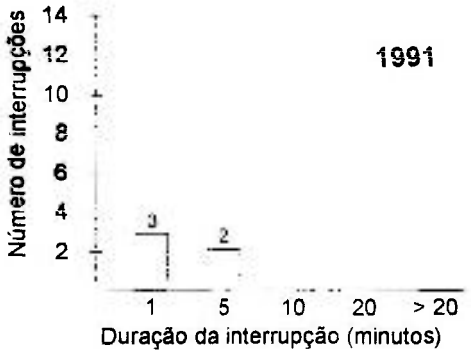








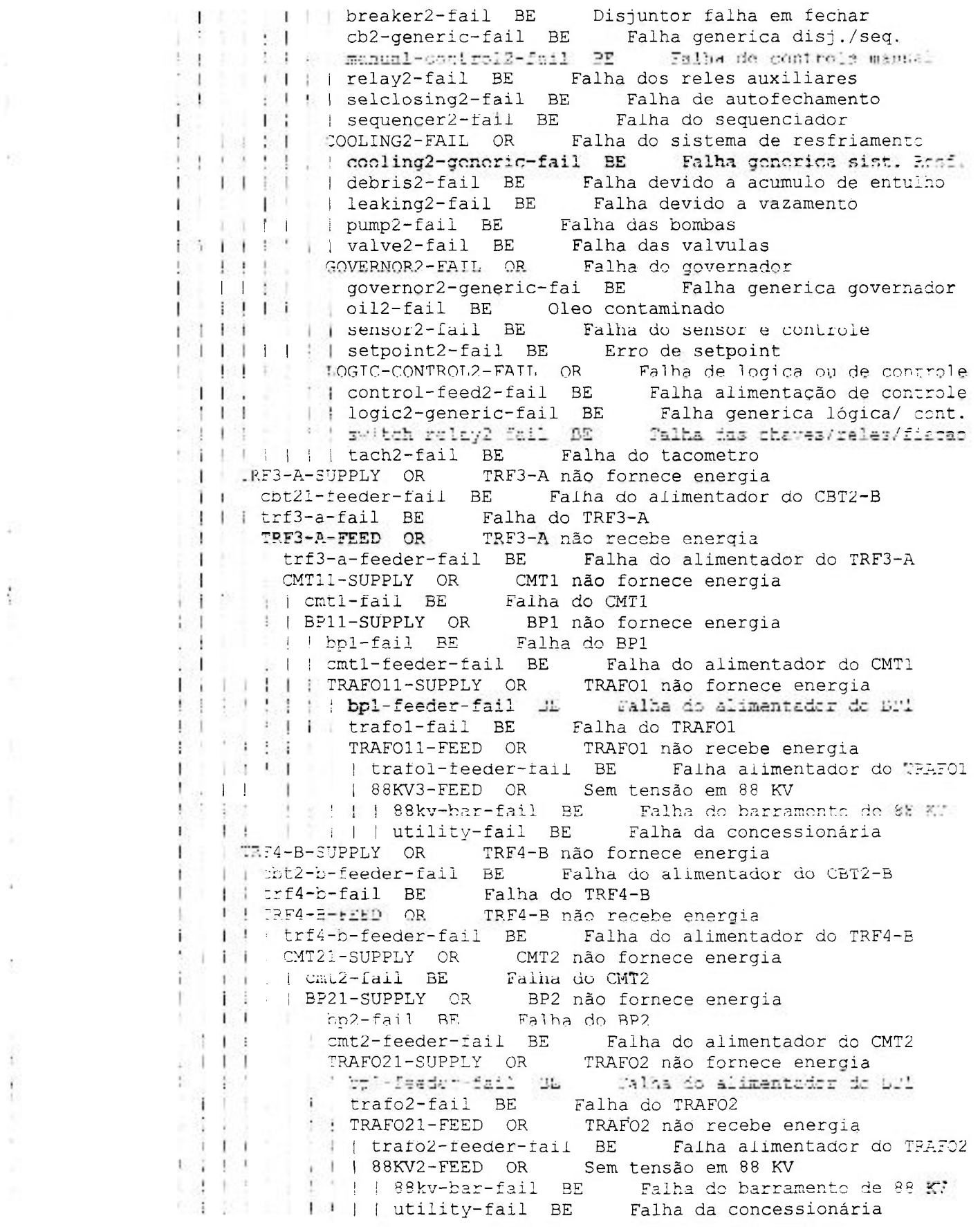




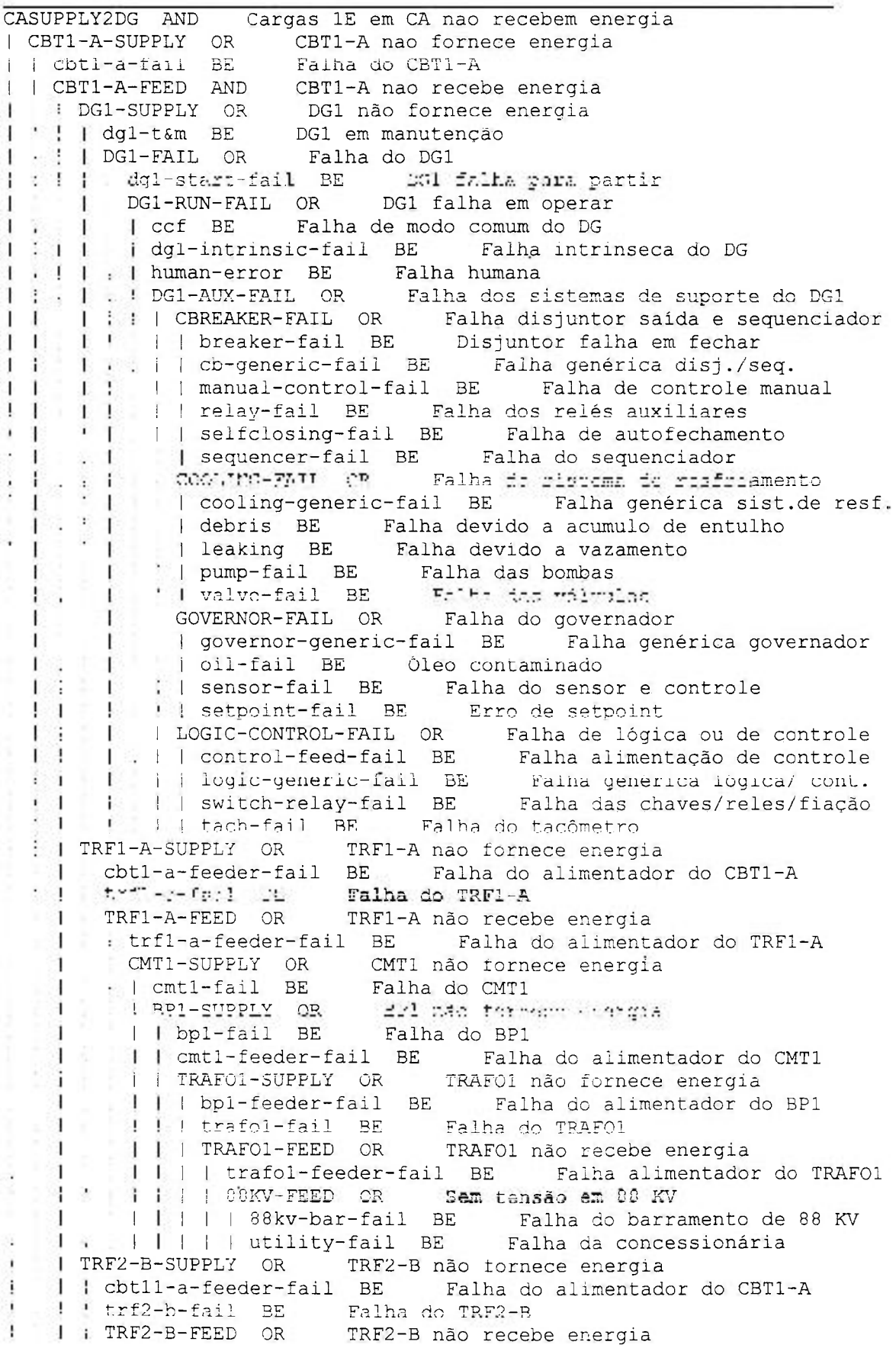
ANEXO G – Diagrama Lógico - Configuração com 3 Diesel Geradores

```
CASUPPLY3DG  AND     Cargas 1E em CA nao recebem energia
  CBT1-A-SUPPLY  OR      CBT1-A nao fornece energia
    cbt1-a-fail  BE      Falha do CBT1-A
    CBT1-A-FEED  AND     CBT1-A nao recebe energia
      DG1-SUPPLY  OR      DG1 não fornece energia
        dg1-t&m  BE      DG1 em manutenção
        DG1-FAIL  OR      Falha do DG1
          dg1-start-fail  BE      DG1 falha para partir
          DG1-RUN-FAIL  OR      DG1 falha em operar
            ccf  BE      Falha de modo comum do DG
            dg1-intrinsic-fail  BE      Falha intrinseca do DG
            human-error  BE      Falha humana
            DG1-AUX-FAIL  OR      Falha dos sistemas de suporte do DG1
              CBREAKER-FAIL  OR      Falha disjuntor saída e sequenciador
                breaker-fail  BE      Disjuntor falha em fechar
                cb-generic-fail  BE      Falha genérica disj./sequenciador
                manual-control-fail  BE      Falha de controle manual
                relay-fail  BE      Falha dos relés auxiliares
                selfclosing-fail  BE      Falha de autofechamento
                sequencer-fail  BE      Falha do sequenciador
              COOLING-FAIL  OR      Falha do sistema de resfriamento
                cooling-generic-fail  BE      Falha genérica sist. Resf.
                debris  BE      Falha devido a acumulo de entulho
                leaking  BE      Falha devido a vazamento
                pump-fail  BE      Falha das bombas
                valve-fail  BE      Falha das válvulas
              GOVERNOR-FAIL  OR      Falha do governador
                governor-generic-fail  BE      Falha genérica governador
                oil-fail  BE      Óleo contaminado
                sensor-fail  BE      Falha do sensor e contrcle
                setpoint-fail  BE      Erro de setpoint
              LOGIC-CONTROL-FAIL  OR      Falha de lógica ou de controle
                control-feed-fail  BE      Falha alimentação de controle
                logic-generic-fail  BE      Falha genérica lógica/ cont.
                switch-relay-fail  BE      Falha das chaves/reles/fiação
                tach-fail  BE      Falha do tacômetro
      DG3-SUPPLY  OR      DG3 não fornece energia
        dg3-tm  BE      DG3 em manutenção
        switch-fail  BE      Falha da chave de transferencia
        DG3-FAIL  OR      Falha do DG3
          dg3-start-fail  BE      DG3 falha para partir
          DG3-RUN-FAIL  OR      DG3 falha em operar
            ccf  BE      Falha de modo comum do DG
            dg3-intrinsic-fail  BE      Falha intrinseca do DG3
            human-error  BE      Falha humana
            DG3-AUX-FAIL  OR      Falha dos sistemas auxiliares do DG3
              CBREAKER3-FAIL  OR      Falha disjuntor saida e sequenciador
                breaker3-fail  BE      Disjuntor falha em fechar
                cb-generic3-fail  BE      Falha generica disj./seq.
                manual-control3-fail  BE      Falha de controle manual
                relay3-fail  BE      Falha dos reles auxiliares
                selfclosing3-fail  BE      Falha de autofechamento
                sequencer3-fail  BE      Falha do sequenciador
              COOLING3-FAIL  OR      Falha do sistema de resfriamento
                cooling3-generic-fail  BE      Falha generica sist. Resf.
                debris3  BE      Falha devido acumulo de entulho
                leaking3-fail  BE      Falha devido a vazamento
                pump3-fail  BE      Falha das bombas
```

```
| | | | | valve3-fail  BE     Falha das valvulas
| | | | | GOVERNOR3-FAIL  OR     Falha do governador
| | | | | governor3-generic-fai  BE     Falha generica governador
| | | | | oil3-fail  BE     Oleo contaminado
| | | | | sensor3-fail  BE     Falha do sensor e controle
| | | | | setpoint3-fail  BE     Erro de setpoint
| | | | | LOGIC-CONTROL3-FAIL  OR     Falha de logica ou de controle
| | | | | control-feed3-fail  BE     Falha alimentacao do controle
| | | | | logic3-generic-fail  BE     Falha generica lógica/ cont.
| | | | | swith-relay3-fail  BE     Falha das chaves/reles/fiacao
| | | | | tach3-fail  BE     Falha do tacometro
| | TRF1-A-SUPPLY  OR     TRF1-A nao fornece energia
| | cbt1-a-feeder-fail  BE     Falha do alimentador do CBT1-A
| | trf1-a-fail  BE     Falha do TRF1-A
| | TRF1-A-FEED  OR     TRF1-A não recebe energia
| | trf1-a-feeder-fail  BE     Falha do alimentador do TRF1-A
| | CMT1-SUPPLY  OR     CMT1 não fornece energia
| | cmt1-fail  BE     Falha do CMT1
| | BP1-SUPPLY  OR     BP1 não fornece energia
| | bp1-fail  BE     Falha do BP1
| | cmt1-feeder-fail  BE     Falha do alimentador do CMT1
| | TRAFO1-SUPPLY  OR     TRAFO1 não fornece energia
| | bp1-feeder-fail  BE     Falha do alimentador do BP1
| | trafo1-fail  BE     Falha do TRAFO1
| | TRAFO1-FEED  OR     TRAFO1 não recebe energia
| | trafo1-feeder-fail  BE     Falha alimentador do TRAFO1
| | 88KV-FEED  OR     Sem tensão em 88 KV
| | 88kv-bar-fail  BE     Falha do barramento de 88 KV
| | utility-fail  BE     Falha da concessionária
| TRF2-B-SUPPLY  OR     TRF2-B não fornece energia
| cbt11-a-feeder-fail  BE     Falha do alimentador do CBT1-A
| trf2-b-fail  BE     Falha do TRF2-B
| TRF2-B-FEED  OR     TRF2-B não recebe energia
| trf2-b-feeder-fail  BE     Falha do alimentador do TRF2-B
| CMT2-SUPPLY  OR     CMT2 não fornece energia
| | cmt2-fail  BE     Falha do CMT2
| | BP2-SUPPLY  OR     BP2 não fornece energia
| | bp2-fail  BE     Falha do BP2
| | cmt2-feeder-fail  BE     Falha do alimentador do CMT2
| | TRAFO2-SUPPLY  OR     TRAFO2 não fornece energia
| | bp2-feeder-fail  BE     Falha do alimentador do BP2
| | trafo2-fail  BE     Falha do TRAFO2
| | TRAFO2-FEED  OR     TRAFO2 não recebe energia
| | trafo2-feeder-fail  BE     Falha alimentador do TRAFO2
| | 88KV1-FEED  OR     Sem tensão em 88 KV
| | 88kv-bar-fail  BE     Falha do barramento de 88 KV
| | utility-fail  BE     Falha da concessionária
CBT2-B-SUPPLY  OR     CBT2-B nao fornece energia
cbt2-b-fail  BE     Falha do CBT2-B
CBT2-B-FEED  AND     CBT2-B nao recebe energia
| DG3-SUPPLY  OR     DG3 não fornece energia (definido acima)
| DG2-SUPPLY  OR     DG2 não fornece energia
| | dg2-tm  BE     DG2 em manutenção
| | DG2-FAIL  OR     Falha do DG2
| | dg2-start-fail  BE     DG2 falha para partir
| | DG2-RUN-FAIL  OR     DG2 falha em operar
| | | ccf  BE     Falha de modo comum do DG
| | | dg2-intrinsic-fail  BE     Falha intrinseca do DG2
| | | human-error  BE     Falha humana
| | | DG2-AUX-FAIL  OR     Falha dos sistemas auxiliares do DG2
| | | CBREAKER2-FAIL  OR     Falha disjuntor saida e sequenciador
```


breaker2-fail BE Disjuntor falha em fechar
cb2-generic-fail BE Falha generica disj./seq.
relay2-fail BE Falha dos reles auxiliares
selclosing2-fail BE Falha de autofechamento
sequencer2-fail BE Falha do sequenciador
COOLING2-FAIL OR Falha do sistema de resfriamento
debris2-fail BE Falha devido a acumulo de entulho
leaking2-fail BE Falha devido a vazamento
pump2-fail BE Falha das bombas
valve2-fail BE Falha das valvulas
GOVERNOR2-FAIL OR Falha do governador
governor2-generic-fai BE Falha generica governador
oil2-fail BE Oleo contaminado
sensor2-fail BE Falha do sensor e controle
setpoint2-fail BE Erro de setpoint
LOGIC-CONTROL2-FAIL OR Falha de logica ou de controle
control-feed2-fail BE Falha alimentação de controle
logic2-generic-fail BE Falha generica lógica/ cont.
tach2-fail BE Falha do tacometro
TRF3-A-SUPPLY OR TRF3-A não fornece energia
cbt21-feeder-fail BE Falha do alimentador do CBT2-B
trf3-a-fail BE Falha do TRF3-A
TRF3-A-FEED OR TRF3-A não recebe energia
trf3-a-feeder-fail BE Falha do alimentador do TRF3-A
CMT11-SUPPLY OR CMT1 não fornece energia
cmt1-fail BE Falha do CMT1
BP11-SUPPLY OR BP1 não fornece energia
bp1-fail BE Falha do BP1
cmt1-feeder-fail BE Falha do alimentador do CMT1
TRAFO11-SUPPLY OR TRAFO1 não fornece energia
trafo1-fail BE Falha do TRAFO1
TRAFO11-FEED OR TRAFO1 não recebe energia
88KV3-FEED OR Sem tensão em 88 KV
utility-fail BE Falha da concessionária
TRF4-B-SUPPLY OR TRF4-B não fornece energia
cbt2-b-feeder-fail BE Falha do alimentador do CBT2-B
trf4-b-fail BE Falha do TRF4-B
trf4-b-feeder-fail BE Falha do alimentador do TRF4-B
CMT21-SUPPLY OR CMT2 não fornece energia
cmt2-fail BE Falha do CMT2
BP21-SUPPLY OR BP2 não fornece energia
bp2-fail BE Falha do BP2
cmt2-feeder-fail BE Falha do alimentador do CMT2
TRAFO21-SUPPLY OR TRAFO2 não fornece energia
trafo2-fail BE Falha do TRAFO2
TRAFO21-FEED OR TRAFO2 não recebe energia
trafo2-feeder-fail BE Falha alimentador do TRAFO2
88KV2-FEED OR Sem tensão em 88 KV
utility-fail BE Falha da concessionária

ANEXO H – Diagrama Lógico - Configuração com 2 Diesel Geradores



```
trf2-b-feeder-fail  BE     Falha do alimentador do TRF2-B
CMT2-SUPPLY  OR     CMT2 não fornece energia
cmt2-fa     BE     Falha do CMT2
BP2-SUPPLY  OR     BP2 não fornece energia
bp2-fail  BE     Falha do BP2
cmt2-feeder-fail  BE     Falha do alimentador do CMT2
TRAFO2-SUPPLY  OR     TRAFO2 não fornece energia
bp2-feeder-fail  BE     Falha do alimentador do BP2
trafo2-fail  BE     Falha do TRAFO2
TRAFO2-FEED  OR     TRAFO2 não recebe energia
trafo2-feeder-fail  BE     Falha alimentador do TRAFO2
88KV1-FEED  OR     Sem tensão em 88 KV
88kv-bar-fail  BE     Falha do barramento de 88 KV
utility-fail  BE     Falha da concessionária
CBT2-B-SUPPLY  OR     CBT2-B nao fornece energia
cbt2-b-fail  BE     Falha do CBT2-B
CBT2-B-FEED  AND     CBT2-B nao recebe energia
DG2-SUPPLY  OR     DG2 não fornece energia
dg2-tm  BE     DG2 em manutenção
DG2-FAIL  OR     Falha do DG2
dg2-start-f     BE     DG2 falha para partir
DG2-RUN-FAIL  OR     DG2 falha em operar
ccf  BE     Falha de modo comum do DG
dg2-intrinsic-fail  BE     Falha intrinseca do DG2
human-error  BE     Falha humana
DG2-AUX-FAIL  OR     Falha dos sistemas auxiliares do DG2
CBREAKER2-FAIL  OR     Falha disjuntor saida e sequenciador
breaker2-fail  BE     Disjuntor falha em fechar
cb-generic2-fail  BE     Falha generica do disj./seq.
manual-control2-fail  BE     Falha de controle manual
relay2-fail  BE     Falha dos reles auxiliares
selfclosing2-fail  BE     Falha de autofechamento
sequencer2-fail  BE     Falha do sequenciador
COOLING2-FAIL  OR     Falha do sistema de resfriamento
cooling2-generic-fail  BE     Falha generica sist. resf.
debris2  BE     Falha devido acumulo de entulho
leaking2-fail  BE     Falha devido a vazamento
pump2-fail  BE     Falha das bombas
valve2-fail  BE     Falha das valvulas
GOVERNOR2-FAIL  OR     Falha do governador
governor2-generic-fai  BE     Falha generica governador
oil2-fail  BE     Oleo contaminado
sensor2-fail  BE     Falha do sensor e controle
setpoint2-fail  BE     Erro de setpoint
LOGIC-CONTROL2-FAIL  OR     Falha de logica ou de controle
control-feed2-fail  BE     Falha alimentacao de controle
logic1 generic-fail  BE     Falha generica lógica/ cont.
swith-relay2-fail  BE     Falha das chaves/reles/fiacao
tach2-fail  BE     Falha do tacometro
TRF2-A-SUPPLY  OR     TRF2-A não fornece energia
cbt21-feeder-fail  BE     Falha do alimentador do CBT2-B
trf2-a-fail  BE     Falha do TRF2-A
TRF2-A-FEED  OR     TRF2-A não recebe energia
trf2-a-feeder-fail  BE     Falha do alimentador do TRF2-A
CMT11-SUPPLY  OR     CMT1 não fornece energia
cmt1-fail  BE     Falha do CMT1
BP11-SUPPLY  OR     BP1 não fornece energia
bp1-fail  BE     Falha do BP1
cmt1-feeder-fail  BE     Falha do alimentador do CMT1
TRAFO11-SUPPLY  OR     TRAFO1 não fornece energia
bp1-feeder-fail  BE     Falha do alimentador do BP1
```

```
trafo1-fail  BE     Falha do TRAFO1
TRAFO11-FEED  OR     TRAFO1 não recebe energia
trafo1-feeder-fail  BE     Falha alimentador do TRAFO1
88KV2-FEED  OR     Sem tensão em 88 KV
88kv-bar-fail  BE     Falha do barramento de 88 KV
utility-fail  BE     Falha da concessionária
TRF4-B-SUPPLY  OR     TRF4-B não fornece energia
cbt2-b-feeder-fail  BE     Falha do alimentador do CBT2-B
trf4-b-fail  BE     Falha do TRF4-B
TRF4-B-FEED  OR     TRF4-B não recebe energia
trf4-b-feeder-fail  BE     Falha do alimentador do TRF4-B
CMT21-SUPPLY  OR     CMT2 não fornece energia
cmt2-fail  BE     Falha do CMT2
BP21-SUPPLY  OR     BP2 não fornece energia
bp2-fail  BE     Falha do BP2
cmt2-feeder-fail  BE     Falha do alimentador do CMT2
TRAFO21-SUPPLY  OR     TRAFO2 não fornece energia
bp1-feeder-fail  BE     Falha do alimentador do BP1
trafo2-fail  BE     Falha do TRAFO2
TRAFO21-FEED  OR     TRAFO2 não recebe energia
trafo2-feeder-fail  BE     Falha alimentador do TRAFO2
88KV2-FEED  OR     Sem tensão em 88 KV
88kv-bar-fail  BE     Falha do barramento de 88 KV
utility-fail  BE     Falha da concessionária
```