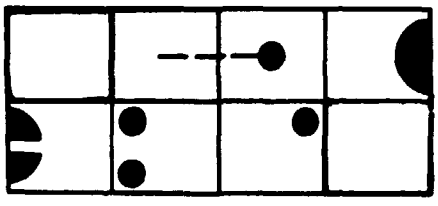
UNIVERSIDADE FEDERAL DE MINAS GERAIS

ESCOLA DE ENGENHARIA



APLICAÇÃO DA METODOLOGIA DA ÁRVORE DE FALHAS NA ANÁLISE DE RISCO EM SISTEMAS COMPLEXOS

AUTOR: Vanderley de Vasconcelos

ORIENTADOR: Walkirio R.A. Lavorato

DEPARTAMENTO DE ENGENHARIA NUCLEAR

CURSO DE PÓS-GRADUAÇÃO EM CIÊNCIAS E TÉCNICAS NUCLEARES

UNIVERSIDADE FEDERAL DE MINAS GERAIS

APLICAÇÃO DA METODOLOGIA DA ÁRVORE DE FALHAS NA ANÁLISE DE RISCO EM SISTEMAS COMPLEXOS

Autor: VANDERLEY DE VASCONCELOS

Orientador: Walkirio R.A. Lavorato

Dissertação apresentada ao Curso de Pós-Graduação em Ciências e Técnicas Nucleares da UFMG, como parte dos requisitos necessários para obtenção do grau de Mestre em Ciências (M.Sc.)

Belo Horizonte - Brasil
Dezembro / 1984

TÍTULO DA DISSERTAÇÃO : Aplicação da Metodologia da Árvore de Falhas na Análise de Risco em Sistemas Complexos.

NOME DO AUTOR : Vanderley de Vasconcelos

Dissertação defendida e aprovada pela banca examinadora, constituída dos Senhores:

Antônio Fabiano de Paiva, M.Sc.

Flavio Soares de Menezes, M.Sc.

Orientador: Walkirio Ronaldo de Andrada Lavorato, M.Sc.

Área de Concentração: Tecnologia das Centrais Nucleares

Belo Horizonte, 06 de maio de 1985
(Data de defesa de Tese)

Este trabalho foi realizado nas instalações do Centro de Desenvolvimento da Tecnologia Nuclear - NUCLEBRÁS, e constitui uma tarefa do programa de atividades do Departamento de Radioproteção e Apoio ao Licenciamento.

Dedico este trabalho
ao meu pai e à Carla

AGRADECIMENTOS

Ao Engº Walkírio R. A. Lavorato, meu orientador, pela contribuição, estímulo e compreensão.

Aos Srs. Virgílio Mattos de Andrade e Silva, José Olympio Nardelli Monteiro de Castro, Ricardo Brant Pinheiro, Luiz Augusto de Queiroz e Oliveira e Ivan Padrão de V. Paiva, por haverem permitido a realização deste trabalho.

Aos colegas da Divisão de Apoio ao Licenciamento, em especial ao Flávio Soares de Menezes, Antônio Carlos Lopes da Costa e Celso Pinto Coelho, pelas revisões, críticas e sugestões.

Ao pessoal da Divisão de Sistemas e Componentes, em especial ao Carlos V. G. Azevedo, Fernando Avelar Esteves, Said Choucair, Roberto Antônio da Silva, Valdir Mendonça de Lima, Alexandros A. Maraslis e Fernando de P. Cortezzi, pelo apoio e informações prestadas.

Ao pessoal da Divisão de Computação, em especial à Maria Aparecida de O. Castro, José Rodrigues Batista, Getúlio A. Ramos Júnior e Enedina Maria A. Oliveira, pela intensa colaboração nos aspectos de computação envolvidos no trabalho.

Ao pessoal da Seção de Documentação Técnica pelo eficiente atendimento.

Ao pessoal da Divisão de Formação e Treinamento do CDTN e da Secretaria do CCTN/UFMG, pelo apoio prestado.

Ao Dr. Luis Lederman da CNEN, pelo fornecimento da cópia dos códigos PREP e KITT.

À Sra. Márcia Valéria L. S. Fagundes, pelo paciente trabalho de datilografia, e ao Sr. Maurício Vieira de Carvalho, pelos serviços de desenho.

Ao pessoal do setor xerox/gráfica do CDTN, pelos serviços de impressão.

A todos aqueles que, direta ou indiretamente, contribuíram na elaboração deste trabalho, meus sinceros agradecimentos.

SUMÁRIO

RESUMO

O processo de avaliação de risco em instalações com um grande número de componentes envolve a determinação da probabilidade de ocorrência de acidentes ou outros eventos indesejáveis, o que só é possível através de técnicas dedutivas, como a Análise da Árvore de Falhas. Este trabalho se propõe a descrever a metodologia da árvore de falhas e a utilizá-la na avaliação de risco de tais instalações complexas.

Na descrição da metodologia, procurou-se fornecer todas as suas informações básicas, ressaltando seus aspectos mais importantes como, por exemplo, construção das árvores de falhas, técnicas de avaliação e sua utilização para a avaliação de risco e de confiabilidade de um sistema.

Tópicos como falhas de modo comum, erros humanos, fontes de dados utilizadas e avaliação das incertezas dos resultados, pela sua importância, foram tratados isoladamente, cada um em um capítulo.

Para a aplicação da metodologia tornou-se necessária a implantação de códigos de computador, normalmente utilizados para este tipo de análise. Foram escolhidos os códigos PREP, KITT e SAMPLE, escritos em FORTRAN IV, por sua disponibilidade e por terem sido utilizados em trabalhos importantes da área nuclear, tal como no Wash-1400.

Com estes códigos, avaliou-se a probabilidade de ocorrência de pressão excessiva no circuito principal do Circuito de Testes de Componentes - CTC, do CDTN. Os resultados qualitativos e quantitativos obtidos servirão como subsídio para a elaboração dos procedimentos de operação, teste e manutenção do CTC.

ABSTRACT

The task of risk assessment of facilities with a large number of components involves the estimate of the probability of occurrence of accidents or other undesired events, which can only be carried out by using deductive techniques, like Fault Tree Analysis. This study intends to describe the fault tree methodology and apply it to risk assessment of such complex facilities.

In the methodology description, it has been attempted to provide all the pertinent basic information, pointing out its more important aspects like, for instance, fault tree construction, evaluation techniques and their use in risk and reliability assessment of a system.

In view of their importance, topics like common mode failures, human errors, data bases used in the calculations, and uncertainty evaluation of the results, will be discussed separately, each one in a chapter.

For the purpose of applying the methodology, it was necessary to implement computer codes normally used for this kind of analysis. The computer codes PREP, KITT and SAMPLE, written in FORTRAN IV, were chosen, due to their availability and to the fact that they have been used in important studies of the nuclear area, like Wash-1400.

With these codes, the probability of occurence of excessive pressure in the main system of the component test loop - CTC, of CDTN, was evaluated. The qualitative and quantitative results thereof will be useful as a subsidy to the elaboration of procedures for CTC related to operating, testing and maintenance.

LISTA DE TABELAS

LISTA DE FIGURAS

1 INTRODUÇÃO

A análise de riscos, em sistemas com um grande número de componentes, é uma tarefa que envolve um considerável dispêndio de tempo e esforço. Para auxiliar nesta tarefa, tem sido largamente utilizada, na área nuclear, a metodologia da árvore de falhas, para a determinação da probabilidade de ocorrência de acidentes ou outros eventos indesejáveis.

Mesmo com a utilização desta metodologia sistemática, esta tarefa não seria possível sem o auxílio de um computador digital. Apenas a título de ilustração, para avaliação de um sistema com 100 componentes seria necessária a realização de cerca de 10^{10} avaliações parciais, levando em conta apenas os modos de falha mais simples (considerando falha simultânea de até 5 componentes).

Este trabalho tem como objetivos básicos a descrição da metodologia da árvore de falhas, a implantação e familiarização com os códigos de computador PREP, KITT e SAMPLE escritos em FORTRAN IV, tradicionalmente utilizados para a implementação da referida metodologia.

Na descrição da metodologia, procurou-se tornar este trabalho o mais completo possível, cobrindo-se todos os seus aspectos importantes, tais como os fundamentos básicos, os processos de construção das árvores de falhas, a simbologia utilizada, as técnicas de avaliação e as características de confiabilidade. Tópicos como falhas de modo comum, erros humanos e avaliação das incertezas dos resultados, pela sua importância, foram tratados isoladamente, cada um em um capítulo. Não foram revistos nem os conceitos de estatística nem os princípios da álgebra de Boole, devido à extensa bibliografia já existente sobre estes assuntos.

Os códigos PREP e KITT, por problemas de capacidade de memória, não puderam ser implantados no computador CDC 6600, que está li

gado ao terminal do Centro de Desenvolvimento da Tecnologia Nuclear - CDTN. A sua implantação se deu ro computador IBM 4341, utilizando-se o computador CDC 6600 como veículo de entrada e saída de dados. Isto, aliado ao excessivo tempo de processamento das árvores de falhas no computador, ao volume de dados de entrada e ao tempo necessário para corrigi-los, resultou numa demora muito grande para rodar cada caso analisado de árvore de falhas. Já o código SAMPLE, utilizado para avaliação das incertezas dos resultados quantitativos, pôde ser implantado no computador CDC 6600, evitando-se assim, os problemas acima mencionados.

Para ganhar familiarização com os referidos códigos e com a metodologia, escolheu-se a avaliação da probabilidade de ocorrência de pressão excessiva no circuito principal, do circuito de testes de componentes - CTC, do CDTN. Esta escolha se deu, principalmente, pela disponibilidade de informações, pela complexidade do sistema e visando obter subsídios para avaliação dos aspectos de segurança envolvidos no CTC, dos critérios de projeto e dos procedimentos de operação, teste e manutenção.

São apresentadas, em capítulo à parte, as fontes de dados utilizadas, onde é ainda sugerido um processo de codificação dos eventos analisados na árvore de falhas.

Por fim, convêm ressaltar que, com o exemplo de aplicação apresentado, não foram mostradas todas as potencialidades da metodologia da árvore de falhas, principalmente no que diz respeito à avaliação das características de confiabilidade de sistemas complexos, levando-se em conta uma análise temporal, considerando taxas de falhas e de reparos, que variam no decorrer do tempo. Isto poderá ser feito em outra oportunidade, quando o problema que estiver sendo analisado conduzir naturalmente o trabalho para o campo da avaliação das características de confiabilidade do sistema.

2 HISTÓRICO

O conceito de Análise de Árvore de Falhas foi desenvolvido nos EUA, pela "Bell Telephone" e em 1961 esta técnica foi utilizada para a avaliação da segurança do sistema de controle de lançamento dos mísseis Minuteman. No Simpósio de Segurança em 1965, patrocinado pela Universidade de Washington e pela "Boeing Company", foram apresentados diversos trabalhos relativos ao desenvolvimento e aplicação da metodologia da árvore de falhas |19|. A apresentação destes trabalhos marcou o início de um largo interesse de aplicação da metodologia nos EUA, como uma ferramenta de análise de confiabilidade em reatores nucleares. No entanto, os primeiros resultados não corresponderam às expectativas, principalmente devido à inexperiência dos técnicos da área nuclear com a metodologia e à ausência de dados estatísticos de falhas dos sistemas e componentes |25|.

No início de 1970 foram realizados grandes progressos na metodologia, no sentido de se obterem informações completas de confiabilidade de sistemas relativamente complexos. Foram grandes também os avanços na área de coleta e avaliação de dados de taxas de falhas.

Entretanto, o marco fundamental da evolução da tecnologia ocorreu em 1972, quando um grupo de 60 técnicos e cientistas, dirigidos pelo Prof. Norman C. Rasmussen, iniciou o Estudo de Segurança de Reatores (Wash-1400) |48|. Este estudo analisou os riscos envolvidos na operação dos reatores a água leve, existentes, em construção e em projeto, definindo risco da seguinte forma:

$$\text{RISCO}\left[\frac{\text{Conseqüência}}{\text{unid. tempo}}\right] = \text{FREQÜÊNCIA}\left[\frac{\text{evento}}{\text{unid. tempo}}\right] \times \text{MAGNITUDE}\left[\frac{\text{conseqüência}}{\text{evento}}\right]$$

Como os sistemas de segurança dos reatores são normalmente projetados para terem alta confiabilidade, os eventos de interesse na análise de risco são eventos raros. Foi então necessária a

utilização da metodologia da árvore de falhas para a obtenção da freqüência de ocorrência destes eventos, a partir de dados de falhas dos componentes individuais. O relatório final, publicado em 1975, contém 11 apêndices, num total de mais de 2000 páginas, e custou aproximadamente 5 milhões de dolares. Foi comentado por 61 organizações americanas e internacionais, antes de sua redação final, e poucas alterações foram feitas nos resultados quantitativos.

Em 1978, devido a muitas críticas que vinha recebendo, a NRC contratou um grupo para a revisão do Estudo de Segurança dos Reatores, o que resultou no Relatório Lewis, que identificou os pontos fracos daquele trabalho, basicamente relativos à incerteza dos resultados quantitativos e à apresentação dos resultados |24|.

A partir de 1979 deu-se início, nos EUA, a uma série de Avaliações Probabilísticas de Risco ("Probabilistic Risk Assessments"), específicas para várias centrais nucleares |14|. A Avaliação Probabilística de Risco (APR) é uma tentativa de quantificar as probabilidades e conseqüências associadas com o mau-funcionamento e acidentes, aplicando técnicas probabilísticas (como a árvore de falhas) e métodos de avaliação de conseqüência, julgados aceitáveis pelos técnicos.

O Programa de Aplicação da Metodologia do Estudo de Segurança dos Reatores ("Reactor Safety Study Methodology Application Program - RSSMAP"), que inicialmente estimou a freqüência de ocorrência de acidentes em um reator sem considerar suas conseqüências, evoluiu para o Programa Provisório de Avaliação da Confiabilidade ("Interim Reliability Evaluation Program - IREP"), que selecionou 8 centrais e fez para cada uma delas uma APR mais completa. As APRs das centrais nucleares de Big Rock Point, Zion, Limerick e Indian Point foram realizadas por interesse dos respectivos proprietários.

Em 1981, o Instituto de Pesquisa de Energia Elétrica ("Electric Power Research Institute") realizou um estudo demonstrando que a contribuição para o risco total, do ciclo do elemento combustível é somente 1% do risco de acidentes em centrais nucleares |60|.

Após o acidente de TMI-2 ("Three Mile Island - 2"), em 1979, concluiu-se que se tivesse sido realizada uma APR para esta central, pelo menos um dos eventos que levou à seqüência de acidentes teria sido identificado e seguramente algumas correções teriam sido feitas |35|. Desde então a NRC ("Nuclear Regulatory Commission") passou a estudar as Metas de Segurança ("Safety Goals"), com a finalidade de utilizar a metodologia das árvores de falhas, para assistir ao processo de licenciamento nas tomadas de decisão e para melhorar a compreensão pelo público dos critérios aplicados para a estimativa de risco. Em 10 de janeiro de 1983, a NRC aprovou as metas de segurança que estão sendo usadas num período de 2 anos de experiência. O proprietário da instalação deverá demonstrar, através de uma APR, que a probabilidade de ocorrência de um acidente que resulta numa fusão em grande escala no núcleo é inferior a 10^{-4} por ano de operação. Após o período de experiência, a NRC irá avaliar os resultados obtidos e recomendar procedimentos para a implementação futura das metas de segurança, na regulamentação e licenciamento das centrais nucleares |14|.

Nos outros países desenvolvidos na área nuclear, a metodologia da árvore de falhas tem sido utilizada apenas como uma ferramenta para auxiliar nas fases de projeto, construção e operação das instalações nucleares.

A Alemanha realizou um Estudo de Risco para suas centrais, aplicando os mesmos métodos do Wash-1400. Apesar das diferenças conceituais entre os reatores alemães e americanos e entre as densidades demográficas dos dois países, os resultados do Estudo de Risco Alemão foram semelhantes aos do Wash-1400 |6|. Uma versão interessante da metodologia da árvore de falhas é utilizada

na Itália, através da chamada Metodologia Semiprobabilística. É um método simples, aplicável a qualquer estágio do projeto, que utiliza não valores específicos de dados de falhas para componentes e sistemas, mas sim níveis de qualidade, definidos de acordo com o conhecimento que o analista tem do sistema (critérios de projeto, tecnologia de construção, controle de fabricação, métodos de instalação, inspeções periódicas e procedimentos de manutenção)[16].

No Brasil, a Comissão Nacional de Energia Nuclear (CNEN) está trabalhando na determinação da probabilidade de fusão do núcleo do reator Angra-1, através do seu departamento de reatores, utilizando a metodologia da árvore de falhas. A maior dificuldade encontrada neste trabalho é que até hoje não se dispõe de um banco de dados de falhas, envolvendo equipamentos nacionais, equipamentos importados trabalhando sob condições nacionais, e mesmo dados de desempenho de trabalhadores nacionais.

3 FUNDAMENTOS DA ANÁLISE DA ÁRVORE DE FALHAS

O termo da lingua inglesa correspondente a falha ("failure") refere-se, geralmente, às ocorrências anormais básicas de um componente, devido ao seu próprio mau-funcionamento. O termo correspondente a falta ("fault") refere-se às ocorrências anormais de um componente, devido tanto à sua própria falha quanto à falha de outros componentes situados a montante no sistema. No entanto, na lingua portuguesa, não existe uma distinção muito clara entre os termos falta e falha, de forma que, neste trabalho, eles serão considerados equivalentes, sem prejuízo para o contexto. A expressão árvore de falhas será adotada por ser aquela que vem recebendo a preferência dos técnicos brasileiros envolvidos na área.

3.1 Modelo de Falhas e Modelo de Sucessos

A operação de um sistema pode ser considerada sob dois aspectos: podem-se enumerar seus caminhos de falha ou seus caminhos de sucesso. Embora a primeira tendência seja selecionar uma visão otimista do sistema, i.e., o espaço de sucessos, isto não é necessariamente o mais vantajoso. Uma vantagem do espaço de falhas é a facilidade da definição de falha em relação à definição de sucesso. Um evento é normalmente constituído de vários outros eventos e o sucesso do evento seria a ocorrência simultânea de todos os eventos. Às vezes, a falha de um dos eventos não invalida o sucesso do sistema, o que torna a identificação do espaço de sucessos bastante difícil. Outra desvantagem do espaço de sucessos é que o sucesso tende a ser associado com a eficiência do sistema, características de produção e outras variáveis contínuas, que não são facilmente modeladas em termos de eventos discretos. Por outro lado, os eventos falhas, particularmente a falha total de um sistema, são fáceis de modelar. Outra vantagem do espaço de falhas é que ele é normalmente bem menor que o espaço de sucessos, i.e., o sistema pode falhar por uma quantidade de caminhos menor do que pode operar com sucesso. É portanto, mais eficiente se fazer uma análise do comporta

mento de um sistema, tomando como base o espaço de falhas.

3.2 Evento Indesejável

A Análise da Árvore de Falhas é uma técnica dedutiva, por meio da qual são identificadas as causas prováveis de um evento indesejável específico de um sistema. O evento indesejável constitui o evento topo no diagrama da árvore de falhas e é geralmente a falha total do sistema. Uma escolha cuidadosa do evento topo é importante, pois se é muito geral, torna a análise muito complexa e se é muito específico, o analista não obtém uma visão global do sistema. Às vezes o evento topo é simplesmente definido como a maior falha de interesse do sistema.

3.3 Elementos Básicos de uma Árvore de Falhas

A árvore de falhas é um modelo gráfico das várias combinações paralelas e seqüenciais de falhas que resultam na ocorrência de um evento indesejável pré-definido.

As falhas podem ser os eventos associados com as falhas dos componentes, erros humanos, ou quaisquer outros eventos pertinentes que podem levar aos eventos indesejáveis. A árvore de falhas, portanto, não é um modelo de todas as possíveis falhas do sistema, mas sim um modelo que inclui somente as falhas que contribuem para a ocorrência de um evento topo específico. Além disso, ela inclui apenas as causas mais prováveis.

A árvore de falhas não é também, um modelo quantitativo, mas sim um modelo qualitativo que pode ser analisado quantitativamente, e freqüentemente o é. O modelo é constituído pela disposição de portas lógicas booleanas[1], que mostram as relações

---

(1) Relativo a Boole, matemático inglês do século passado e introdutor da matemática no estudo da lógica.

necessárias entre os eventos,para permitir a ocorrência de um evento situado num nível mais alto da árvore de falhas. Os eventos em níveis mais altos são as saídas das portas e os em níveis mais baixos são as entradas.

Um componente de um sistema é um constituinte básico, cuja falha é considerada falha primária, durante a construção da árvore. Conseqüentemente, os componentes de um sistema podem variar, de acordo com o evento topo a ser analisado ou com o detalhe que o analista deseja incluir na árvore de falhas. Alguns componentes têm diversos estados de operação, nenhum dos quais é, necessariamente, um estado de falha. Por exemplo, os contatos de um relé podem estar abertos ou fechados, sem que o relé esteja num estado de falha. A descrição destes estados é chamada de configuração do componente.

A construção da árvore de falhas é o desenvolvimento lógico do evento topo. No processo de construção, cada evento falha é desenvolvido até que seja encontrado um evento primário. Um evento falha é uma situação que resulta de uma interação lógica das falhas primárias. O desenvolvimento de qualquer evento falha resulta num ramo da árvore de falhas. O evento que está sendo desenvolvido é chamado de evento base do ramo. O ramo estará completamente desenvolvido somente quando todos seus eventos estiverem desenvolvidos em eventos primários. Todos os eventos em um ramo estarão no domínio do evento base.

Uma porta da árvore de falhas é composta de duas partes:

a) O símbolo lógico booleano, que relaciona as entradas da porta com seu evento de saída;

b) A descrição do evento de saída.

Uma porta é equivalente a outra porta se, e somente se, o símbolo lógico, a descrição do evento de saída, e as condições limites associadas com o evento de saída são idênticas. Estas condi

ções limites modificam um evento e são impostas pelo analista ou são geradas pelos eventos falhas que ocorreram previamente.

3.4 Componentes Passivos e Ativos

Um componente passivo contribui de uma maneira mais ou menos estática para o funcionamento do sistema. Ele pode atuar como transmissor de energia de um local para outro (fio, barramento, linha de vapor, etc.) ou atuar como transmissor de cargas (estrutura).

Um componente ativo contribui de uma maneira mais dinâmica para a operação do sistema, modificando de alguma forma o seu funcionamento. Uma válvula que abre e fecha modifica a vazão de fluido num sistema e uma chave tem efeito similar num sistema elétrico.

Um componente passivo pode ser considerado como um transmissor de sinal, da saída de um componente ativo para a entrada de um outro componente ativo. A falha de um componente passivo irá resultar na não transmissão, ou transmissão parcial do sinal, enquanto que a falha de um componente ativo irá originar ou modificar um sinal. As taxas de falhas dos componentes passivos são, geralmente de 2 a 3 ordens de grandeza, menores que as dos componentes ativos.

3.5 Falhas Primárias, Secundárias e de Comando

Uma falha primária é qualquer falha que ocorre num componente que está trabalhando sob condições para as quais ele foi projetado. Um exemplo de falha primária é a ruptura de um tanque a uma pressão inferior ou igual à pressão de projeto, devido a problemas de solda.

Uma falha secundária é qualquer falha que ocorre num componente

que está trabalhando sob condições para as quais ele não foi projetado. Um exemplo de falha secundária é a ruptura de um tanque a uma pressão superior à de projeto.

Uma falha de comando envolve a operação adequada de um componente, mas em instante ou local errado. Um exemplo de falha de comando é o desligamento desnecessário de um disjuntor, provocado por um sinal incorreto do circuito de comando.

3.6 Causa Imediata

No processo de construção da árvore de falhas, o analista define o sistema (determina seus limites) e seleciona um modo de falha do sistema para análise subseqüente (evento topo). A próxima etapa é a determinação das causas imediatas, necessárias e suficientes para a ocorrência do evento topo. Estas causas não são necessariamente as causas básicas do evento, mas sim os mecanismos imediatos que levam ao evento. Cada uma destas causas deve ser tratada como um evento sub-topo e desenvolvido em suas causas imediatas, até quando for alcançado o limite de resolução da árvore, i.e., quando todas as causas imediatas forem eventos básicos.

3.7 Procedimentos Gerais da Análise da Árvore de Falhas

O limite de resolução da árvore de falhas é determinado pela necessidade do analista e pela disponibilidade de informações. Definida a resolução, o analista tem a opção de fazer a avaliação da árvore de falhas. A própria árvore pode ser o objetivo final, para se ter um maior entendimento do funcionamento do sistema.

Uma análise mais profunda da árvore de falhas pode levar aos modos de falha do sistema, o que é feito através de uma análise qualitativa. Além disso, podem ser obtidas informações probabi

lísticas de falha para o evento topo, tomando como base as informações das probabilidades de falha dos eventos básicos.

As quatro etapas seguintes estão normalmente presentes na análise da árvore de falhas:

a) Definição do Sistema

A definição do sistema compreende a aquisição de informações detalhadas sobre o funcionamento do sistema e o estabelecimento dos limites analíticos do modelo. Para cada problema que estiver sendo analisado, devem ser obtidas as seguintes informações:

- condições iniciais para todos os componentes que têm mais de um estado de operação;
- limite de resolução, i.e., qual nível do sistema que deverá ser considerado básico para a análise;
- eventos que têm probabilidade nula ou unitária;
- outras hipóteses simplificadoras adotadas.

b) Construção da Árvore de Falhas

Consiste em se fazer uma representação lógica booleana, associada com o modelo de falhas ou sucessos de um aspecto particular de um sistema. Existem poucas publicações disponíveis na literatura a respeito de métodos de construção de árvores de falhas. Algumas apresentam métodos para construção de modelos apenas para sistemas elétricos [20] e outras para sistemas mais gerais [61]. Este item será estudado com mais detalhes no próximo capítulo.

c) Avaliação Qualitativa

Consiste na obtenção dos modos de falha para um determinado evento topo de um sistema. A obtenção desses modos de falha pode ser feita deterministicamente ou probabilisticamente pelo método de Monte Carlo. Quando determinada pelo método de Monte Carlo, existe a desvantagem de se ter sempre a dúvida

se todos os modos de falha foram obtidos. Esta etapa envolve um dispêndio muito grande de tempo e esforço.

d) Avaliação Quantitativa

É a área que tem recebido maior esforço de pesquisa e desenvolvimento, desde o aparecimento da metodologia da árvore de falhas. Basicamente têm sido utilizados 3 métodos para este fim:

. simulação direta;
. método de Monte Carlo;
. solução analítica direta.

O método da simulação direta consiste em utilizar um computador analógico ou híbrido para simular a lógica da árvore de falhas. Este método, devido ao seu custo e tempo excessivos, não é muito utilizado.

O método de Monte Carlo é o mais simples em princípio e consiste das seguintes etapas:

. atribuição de dados de taxas de falhas e taxas de reparos, quando existentes, para os eventos primários;
. representação da árvore de falhas num computador digital, para fornecer os resultados quantitativos.

Ao realizar estas etapas, o computador simula a árvore de falhas e, utilizando os dados de entrada, seleciona aleatoriamente os parâmetros das distribuições de probabilidade atribuídas e testa a ocorrência ou não do evento topo, dentro de um determinado período de tempo. Cada teste é uma tentativa e é realizado um grande número de vezes, até que seja realizada a avaliação quantitativa.

O método da solução analítica direta consiste em obter, através de propriedades da álgebra booleana, equações booleanas mais simples para a árvore de falhas que está sendo analisada e, através das leis da probabilidade, fazer a avaliação

quantitativa da árvore de falhas |32|. Com o advento da teoria da árvore cinética, em 1970, as soluções analíticas das árvores de falhas complexas, para árvores cujas taxas de falhas são funções do tempo e com possibilidade de reparos, puderam ser realizadas com pouco tempo de processamento em computadores digitais |56|.

Esses métodos serão analisados com mais detalhes no Capítulo 5.

4 CONSTRUÇÃO DA ÁRVORE DE FALHAS

Uma das maiores dificuldades do processo de construção das árvores de falhas é a sua dependência do analista, no que diz respeito à sua astúcia, habilidade e conhecimento profundo da metodologia e do sistema que está sendo analisado. Já existem atualmente códigos de computação disponíveis para a construção automática das árvores de falhas |1, 20|. No entanto, esta construção automatizada nunca poderá substituir a construção manual, pois uma das principais vantagens da técnica da árvore de falhas é que o analista é forçado a compreender o sistema, e muitas vezes os pontos fracos do sistema são identificados enquanto a árvore está sendo construída. Uma árvore de falhas construída automatiçamente pelo computador pode ser um bom ponto de partida para uma análise mais profunda, incluindo efeitos humanos e ambientais, e poderia liberar o analista para aspectos mais sutis da análise.

4.1 Simbologia Utilizada nas Árvores de Falhas

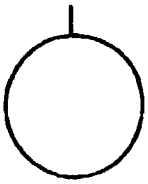
Segundo padrões mais ou menos aceitos internacionalmente, os símbolos das árvores de falhas são divididos em três categorias: símbolos de eventos, símbolos lógicos e símbolos de transferência |27|.

4.1.1 Símbolos de Eventos

a) Retângulo

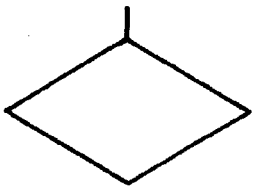
O retângulo identifica um evento que resulta da combinação de eventos falhas, através da porta lógica a ele associada. Se for omitido, resulta em árvores mais compactas, mas de difícil compreensão, até mesmo por quem as elaborou.

b) Círculo



O círculo descreve um evento falha básico, um evento primário, que não necessita mais ser desenvolvido. Aos eventos assim identificados são atribuídos valores de probabilidades de falha, obtidos de tratamento estatístico de dados empíricos, que podem ser utilizados para a avaliação da probabilidade de ocorrência do evento topo.

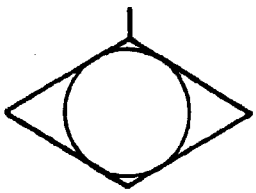
c) Losango



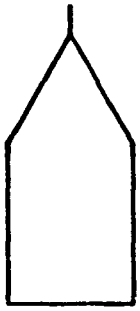
O losango descreve um evento falha, que numa determinada árvore é considerado básico. No entanto, ele pode ser desenvolvido em eventos falhas mais básicos. A razão mais comum do seu não desenvolvimento é a sua baixa conseqüência ou a inexistência de informações para obter a probabilidade de ocorrência de seus eventos básicos.

Círculos e losangos representam, portanto, as falhas primárias numa árvore de falhas.

d) Círculo inscrito num Losango



O círculo inscrito num losango indica que existe uma subárvore, que foi avaliada separadamente e cujos resultados quantitativos foram inseridos no local onde se encontra este símbolo na árvore de falhas, como se fossem dados de eventos básicos.



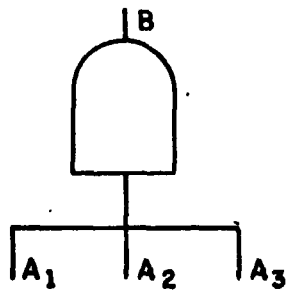
e) Casa ("HOUSE")

É usada como uma chave, para incluir ou eliminar partes da árvore de falhas. Quando houver alguma parte da árvore que não se aplica a determinadas situações, isto deve ser indicado dentro deste símbolo.

Dos símbolos de eventos mostrados, aqueles que representam as situações mais comuns são o círculo, o retângulo e o losango.

4.1.2 Símbolos Lógicos

a) Porta E ("AND")

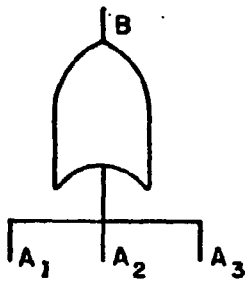


É usada para mostrar que o evento de saída ocorre somente se todos os eventos de entrada ocorrerem. Pode existir qualquer número de entradas, mas apenas uma única saída. Representa uma relação causal entre a entrada e a saída, i.e., as falhas de entrada são a causa da falha de saída. Corresponde aos símbolos booleanos ".", "∧", "&", "() ()" ou "∩". Na figura mostrada ao lado, B irá ocorrer se ocorrerem simultaneamente A_1, A_2 e A_3. A expressão booleana equivalente é:

$$B = A_1 \cdot A_2 \cdot A_3.$$

b) Porta OU ("OR")

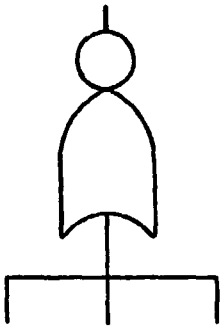
Define uma situação na qual o evento de saída ocorre, se um ou mais eventos de entrada ocorrerem. Ao contrário do que acontece para uma porta E, para uma porta OU as falhas de entrada não são nunca



as causas das falhas de saída. As entradas de uma porta OU são idênticas à saída, mas só que mais especificamente definidas. Corresponde aos símbolos booleanos "+", "U" ou "V". Na figura mostrada ao lado, B irá ocorrer se pelo menos um dos três eventos A_1, A_2 ou A_3 ocorrer. A expressão booleana equivalente é:

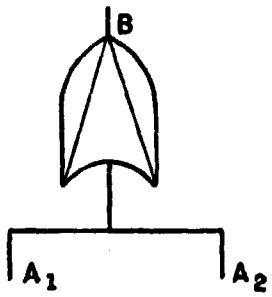
$B = A_1 + A_2 + A_3$.

c) Porta NÃO ("NOT")



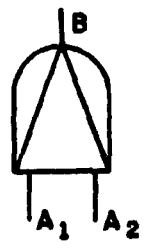
Equivale à negação do evento ou da saída de outra porta lógica a ela acoplada. Por exemplo, o símbolo mostrado ao lado define um outro operador lógico booleano, o NÃO OU ("NOT OR"), onde o pequeno círculo indica a negação da porta OU .

d) Porta OU Exclusiva ("Exclusive OR")



É um caso especial da porta OU, na qual o evento de saída ocorre se somente um dos eventos de entrada ocorrer. Corresponde ao símbolo lógico booleano "⊕". Na maioria das aplicações quantitativas, a diferença de resultados entre a aplicação dos dois tipos de portas OU é tão pequena, que não é geralmente necessária a distinção entre elas.

e) Porta E Prioritária ("Prioritary AND")

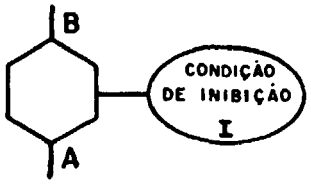


É um caso especial de porta E, no qual o evento de saída ocorre se todos os eventos de entrada ocorrerem numa ordem especificada. Nas aplicações práticas mais comuns também não existe a necessidade

de distinção entre os dois tipos de portas E.

f) Porta Inibição ("Inhibit")

É outro caso especial de porta E, onde a saída é provocada por uma única entrada, mas com alguma condição qualitativa devendo existir para que a entrada provoque a saída. A descrição desta condição, chamada de condição de inibição, deve ser feita dentro de uma elipse, situada à direita da porta. Um exemplo é o caso de certas reações químicas que só ocorrem na presença de catalizador. Neste caso, a inexistência de catalizador seria a condição de inibição. Pode ser usado outro tipo de porta inibição, onde a condição A é necessária, mas não suficiente, para a ocorrência da saída B. Neste caso existe uma probabilidade de ocorrência de B dada a ocorrência de A, que deve ser indicada na elipse.



4.1.3 Símbolos de Transferência

Os triângulos indicam transferência de uma parte da árvore para outra, quando esta se torna demasiadamente grande para ser apresentada como um todo, fazendo ligação entre portas da árvore, mesmo em diferentes folhas de papel. O triângulo com uma linha no vértice indica que o desenvolvimento da árvore continuará em outro lugar, onde houver o triângulo com a linha lateral e com o mesmo número de identificação.

4.2 Regras Básicas para a Construção da Árvore de Falhas

A obediência a certas regras em muito contribui para a obtenção de árvores de falhas claras, objetivas e que representam fielmente o sistema analisado.

Seja por exemplo, a Figura 4.1. É uma árvore de falhas simples, ou talvez uma parte de uma árvore mais complexa. Nela, nenhum dos eventos foi descrito, mas apenas designado pelas letras T, A, B, C e D. Esta não é a forma correta de se construir uma árvore de falhas, pois é necessário descrever exatamente o que tais eventos são, para se ter uma idéia correta da operação do sistema e atingir os objetivos da análise. Esta observação dá origem à

Regra Nº 1:

"Descreva dentro dos retângulos precisamente que falha é e quando ela ocorre".

A condição "que" da regra descreve o estado de operação do componente e a condição "quando" descreve a condição que faz do estado particular do componente uma falha. É importante não condicionar o tamanho da sentença ao tamanho do retângulo que foi desenhado. Se for necessário, deve-se fazer um retângulo maior, pois podem-se abreviar palavras, mas nunca abreviar idéias.

São exemplos de nomes de eventos:

- contatos normalmente fechados de um relé falham em abrir quando uma força eletromotriz é aplicada à bobina;
- motor falha em partir quando é aplicada tensão ao seu estator.

A próxima etapa do procedimento é examinar cada retângulo e fazer a seguinte pergunta:

- Esta falha pode ser devida à falha de um componente?

Esta questão dá origem à

Regra Nº 2:

"Se a resposta é sim, deve-se colocar uma porta OU abaixo do evento e procurar pelos modos de falha primária, secundária e de comando. Se a resposta é não, pode-se colocar uma porta OU, E, Inibição ou nenhuma porta abaixo do evento e procurar pelas causas imediatas da falha".

Geralmente, quando a falha é originada por energia exterior ao componente, deve-se procurar pelas suas causas imediatas.

Regra Nº 3:

"Se o funcionamento normal de um componente propaga a seqüência de uma falha, então deve-se supor que o componente funciona normalmente".

Pode-se imaginar, durante a análise de um sistema, que a propagação de uma determinada seqüência de falhas seria interrompida pela falha de algum componente. No entanto, esta não é a suposição correta. Deve-se admitir que o sistema funciona normalmente, permitindo à propagação da seqüência de falhas em questão.

Regra Nº 4:

"Se o funcionamento normal de um componente atua no sentido de interromper uma seqüência de falhas, deve-se admitir que o componente falha".

Pelas mesmas razões anteriores, esta suposição deve ser feita para permitir a propagação da falha através da árvore.

Regra Nº 5:

"As portas de entrada devem ser eventos falhas perfeitamente de

finidos e não devem estar ligadas diretamente a outras portas".

Uma ligação porta a porta é indicação de uma análise mal elaborada. Se o objetivo da análise é o de se fazer uma avaliação quantitativa (o que não é sempre verdade), pode-se admitir uma ligação porta a porta. No entanto, durante a fase de construção da árvore de falhas este tipo de ligação pode confundir o analista e é normalmente uma indicação que ele não conhece suficientemente o sistema. Uma análise de árvore de falhas só pode ser bem sucedida se o analista tem um conhecimento claro e profundo do sistema que está sendo modelado.

Regra Nº 6:

"Todas as entradas de uma porta devem estar bem definidas antes de se iniciar a análise de qualquer uma delas".

Esta regra estabelece que as árvores devem ser desenvolvidas em níveis, e cada nível deve estar completo antes que qualquer consideração seja feita para níveis mais baixos.

É interessante notar que não existe uma única árvore de falhas correta para um problema específico, mas sim, muitas formas que são equivalentes umas às outras. Certas regras de álgebra booleana podem ser aplicadas para reestruturar a árvore e obter uma forma equivalente mais simples e de fácil compreensão, tornando o processo de avaliação mais simples |53|.

5 TÉCNICAS DE AVALIAÇÃO DA ÁRVORE DE FALHAS

Uma vez construída, a árvore de falhas pode ser avaliada qualitativamente e/ou quantitativamente.

A avaliação qualitativa inclui:

. determinação dos cortes mínimos ("minimal cut sets");
. determinação dos caminhos mínimos ("minimal path sets");
. determinação da importância qualitativa dos componentes e cortes mínimos;
. determinação dos cortes mínimos potencialmente susceptíveis a causas comuns.

A avaliação quantitativa inclui:

. determinação das características de confiabilidade dos componentes, dos cortes mínimos e do sistema;
. determinação da importância quantitativa dos componentes e cortes mínimos;
. avaliação de sensibilidade e de incertezas.

5.1 Avaliação Qualitativa

5.1.1 Determinação dos Cortes Mínimos

Um corte mínimo é o menor conjunto de eventos primários, condições de inibição, eventos falhas não desenvolvidas ou qualquer combinação destes, cuja ocorrência provoca a ocorrência do evento topo. Se um dos eventos do corte mínimo não ocorrer, então o evento topo não irá ocorrer (por meio desta combinação de eventos). Os cortes mínimos representam, portanto, os modos de ocorrência de um evento topo.

Ocorre um corte mínimo de 1ª ordem, quando a falha de um único componente leva à ocorrência do evento topo. A existência de cortes mínimos de 1ª ordem indica geralmente uma freqüência mui

to alta de ocorrência do evento topo. Por outro lado, não são geralmente pesquisados os cortes mínimos de ordens superiores à 5ª ou 6ª (cortes mínimos com mais de 5 ou 6 componentes), devido às suas baixas probabilidades de ocorrência, em relação aos de ordem mais baixa.

Qualquer árvore de falhas terá um número finito de cortes mínimos, os quais são únicos para aquele evento topo. A expressão para o evento topo T pode então ser escrita como:

$$T = M_1 + M_2 + \ldots + M_k,$$

onde M_1, M_2, ..., M_k são os cortes mínimos para o evento topo.

Cada corte mínimo M_i pode ser escrito como:

$M_i = X_1 \cdot X_2 \cdot \ldots \cdot X_m$, onde

X_1, X_2, ..., X_m são os eventos básicos da árvore de falhas. Seja por exemplo a árvore de falhas da Figura 4.1. A expressão para o evento topo é $T = C + A \cdot B$, onde A, B e C são falhas de componentes. Este evento topo tem um corte mínimo de 1ª ordem (C) e um corte mínimo de 2ª ordem (A · B). Estes cortes mínimos são únicos para o evento topo e independentes das diferentes formas equivalentes que a árvore de falhas possa ter.

A determinação dos cortes mínimos pode ser feita deterministicamente, desde que cada componente tenha apenas dois estados. Neste caso, supõe-se a falha dos componentes 1, 2, ..., até n e verifica-se, em cada caso, se ocorre a falha ou o sucesso do evento topo. Identificam-se assim os cortes mínimos de 1ª ordem. Supõe-se em seguida a falha de todas as combinações de 2 componentes e identificam-se os cortes mínimos de 2ª ordem e assim por diante até se obterem todos os cortes mínimos que se deseja analisar.

Para árvores de falhas com mais de 100 componentes, a obtenção

de cortes mínimos de ordem superior a 3, pelo método determinístico, torna-se proibitiva, devido ao enorme tempo de processamento nos computadores digitais. Por isso, a maioria dos códigos de computador utiliza o método de Monte Carlo, gerando apenas os cortes mínimos mais prováveis |29|.

Outro processo de obtenção de cortes mínimos, que pode ser utilizado manualmente, para árvores de falhas menores, ou através de computadores, é o chamado Algorítmo de Vesely-Fussel. O método consiste em, primeiramente atribuir um nome ou código a cada evento da árvore de falhas, a começar pelo evento topo. A seguir, deve-se fazer uma listagem (no processo manual), de uma forma sistemática, dos nomes ou códigos atribuídos aos eventos, da seguinte maneira: se a porta lógica associada ao evento topo é OU, cada entrada deve ser escrita em uma linha; se a porta lógica associada é E, as entradas devem ser escritas na mesma linha; repetindo este procedimento para os eventos listados, de cima para baixo e da esquerda para a direita, os cortes do sistema serão encontrados quando existirem apenas eventos primários; os cortes que não tiverem eventos repetidos serão os cortes mínimos do sistema |8|.

Para ilustrar este método, seja por exemplo, obter os cortes mínimos da árvore mostrada na Figura 5.1.

1. T
2. E1 E2
3. A E2
   E3 E2
4. A E2
   B E2
   C E2
5. A C
   A E4
   B C
   B E4
   C C

C E4

6. A C = AC

A AB = AB

B C = BC

B AB = AB

C C = C

C AB = ABC.

Eliminando os cortes com eventos repetidos, conclui-se que os cortes mínimos são C e AB. Logo, o evento topo pode ser escrito como T = C + AB. A partir desta expressão para o evento topo, pode ser obtida uma árvore de falhas simplificada equivalente à inicial, que coincide com aquela mostrada na Figura 4.1.

5.1.2 Determinação dos Caminhos Mínimos

O evento topo de uma árvore de falhas representa a falha do sistema, que é um evento de grande interesse do ponto de vista da segurança do sistema. Do ponto de vista de confiabilidade, a maior preocupação é em relação às formas de evitar o evento topo. Como existe uma equação booleana para o evento topo, o seu complemento corresponde a uma árvore que é o complemento da original. Esta árvore, chamada de Árvore de Falhas Dual, pode ser obtida diretamente da árvore original, tomando-se o complemento dos eventos primários e substituindo as portas OU por E e vice-versa.

Um corte mínimo da árvore dual é um Caminho Mínimo da árvore original e representa a menor combinação de eventos primários cuja não ocorrência assegura a não ocorrência do evento topo.

A expressão para o evento topo T pode ser escrita como:

$$T' = P_1 + P_2 + \ldots + P_k,$$

onde T' é o complemento de T e P_1, P_2, ..., P_k são os caminhos mínimos da árvore de falhas. Cada caminho mínimo P_i pode ser escrito como:

$$P_i = X_1' \cdot X_2' \cdot \ldots \cdot X_m',$$

onde X_1', X_2', ..., X_m' são os complementos dos eventos básicos da árvore de falhas.

Se os cortes mínimos de uma árvore de falhas já foram determinados, podem-se obter os caminhos mínimos diretamente, bastando para isto achar o complemento da equação do evento topo em função dos cortes mínimos. Para o exemplo do item anterior, onde a expressão para o evento topo era T = C + AB, os caminhos mínimos poderiam ser obtidos da seguinte maneira:

T' = (C + AB)'; achando-se o complemento, resulta:

T' = C' (AB)'; usando-se o teorema de De Morgan para o termo (AB)' |27|:

T' = C' · (A' + B'); usando-se a propriedade distributiva:

T' = C'A' + C'B'.

Esta equação representa as formas de evitar o evento indesejável; logo C'A' e C'B' são os caminhos mínimos para o evento topo.

5.1.3 Importância Qualitativa

Após a obtenção dos cortes mínimos, pode-se ter uma idéia dos contribuintes mais importantes para a falha do sistema, ordenando-se os cortes mínimos de acordo com a sua ordem ou tamanho. Os cortes mínimos de 1ª ordem, quando existem, são geralmente

os mais importantes. Os cortes mínimos de ordem mais alta (5ª, 6ª, etc.) só são importantes quando demonstram susceptibilidade às falhas de modo comum (ver Capítulo 6). Devido às diferenças entre os valores de probabilidades de falha dos componentes individuais, a ordem dos cortes mínimos dá somente uma idéia geral da importância do corte mínimo para a falha do sistema.

obtenção dos cortes mínimos pode servir para certificar se um determinado critério de projeto foi satisfeito. Se, por exemplo, pelo critério de falha única [15], ficar estabelecido que a falha de um único componente não leva à falha do sistema, a inexistência de cortes mínimos de 1ª ordem deve confirmar isto.

Os cortes mínimos servem também para averiguar se tipos específicos de falhas, tais como erros humanos e falhas de componentes ativos podem, individualmente, causar a falha do sistema.

5.2 Avaliação Quantitativa

Após a obtenção dos cortes mínimos, pode ser realizada uma avaliação quantitativa da árvore de falhas. Esta avaliação inclui a determinação das probabilidades de falha de cada componente, de cada corte mínimo e do sistema como um todo. Se as taxas de falhas dos componentes individuais são tratadas como variáveis aleatórias, podem ser utilizadas as técnicas de propagação de variáveis aleatórias na determinação das incertezas dos resultados (ver Capítulo 9).

Serão considerados os modelos de taxas de falhas constantes, sem levar em conta os efeitos de desgaste ou envelhecimento. Os modelos que levam em conta estes fatores são bem mais complicados e só são necessários quando é requerida uma maior precisão dos resultados.

5.2.1 Modelo de Taxa de Falhas por Hora para Componentes Não Reparáveis

Sendo λ a taxa de falhas por hora de um componente, quanto maior o seu tempo de exposição, maior é a sua probabilidade de falha. Este modelo é chamado de Modelo λ.

A probabilidade cumulativa F(t) que o componente sofra sua primeira falha no tempo t, dado que ele está funcionando é:

$$F(t) = 1 - e^{-\lambda t}.$$

F(t) é chamado de Não-Confiabilidade ("Unreliability") do componente e o seu complemento R(t) é chamado de Confiabilidade ("Reliability") do componente:

$$R(t) = 1 - F(t) = e^{-\lambda t}.$$

A função densidade de probabilidade f(t) é a derivada de F(t); assim sendo, o $\lim_{\Delta t \to 0} f(t)\,\Delta t$ é a probabilidade de que não aconteça nenhuma falha do componente até o tempo t, mas aconteça no intervalo de tempo entre t e t + Δt.

Logo, $f(t) = \lambda\, e^{-\lambda t}$.

Para pequenos valores de λ (menores que 10^{-1}), a equação para a não-confiabilidade do componente pode ser escrita como:

$$F(t) \cong \lambda t,$$

com um erro inferior a 5%, do lado conservativo. Este erro é muito pequeno, quando comparado com as incertezas dos valores de λ.

O parâmetro λ utilizado no modelo pode ser a taxa de falhas de um componente de reserva ou a taxa de falhas de um componente em operação. No primeiro caso, o tempo t deve ser o tempo em que o

componente ficou de reserva e, no segundo caso, o tempo t deve ser o tempo de operação.

Para um componente com uma fase de reserva e outra de operação, a probabilidade total de falha do componente até o tempo t será:

$$F_r(t_r) + [1 - F_r(t_r)]\, F_o(t_o) \cong F_r(t_r) + F_o(t_o),$$

onde os índices r e o indicam reserva e operação, respectivamente. A equação indica que, para pequenas probabilidades de falha, as duas não-confiabilidades do componente, em reserva e em operação, podem ser simplesmente somadas.

5.2.2 Modelo de Taxa de Falhas por Hora para Componentes Reparáveis

Quando um componente é reparável, a sua reparação ou substituição não é feita imediatamente após a sua falha e, uma vez iniciada, ela requer algum tempo para ser concluída. A operação de reparo pode ser caracterizada pelo tempo d em que o componente esteve indisponível para a operação. A distribuição cumulativa G(d) do tempo em que o componente esteve indisponível, pode ser definida como a probabilidade que o tempo de indisponibilidade do componente seja menor que d. Esta distribuição é obtida experimentalmente de dados de reparos e substituições.

A Indisponibilidade ("Unavailability") q(t) de um componente pode ser definida como a probabilidade que o componente esteja inoperante no tempo t e incapaz de operar, se ocorrer uma demanda. Se as falhas não são reparáveis, então os componentes estarão inoperantes no tempo t, se e somente se ocorrer uma falha no tempo t. Para estes casos, a indisponibilidade do componente coincide com a sua não-confiabilidade e pode ser dada simplesmente por:

$q(t) = \lambda t$.

Para avaliação de árvore de falhas que contêm apenas este tipo de componente, é necessário apenas o conhecimento dos valores de λ, enquanto que para o caso de conter componentes reparáveis, é necessário também o conhecimento do processo de reparo. Uma suposição otimista que é sempre feita é que, após o reparo, o componente funciona como se fosse um componente novo.

Devem ser considerados dois casos:

. as falhas são monitoradas;
. as falhas não são monitoradas.

Para o caso em que há monitoração, quando ocorre uma falha, um alarme, anunciador, luz ou outro sinal, alerta o operador. Neste caso, a indisponibilidade q_u do componente, será dada por:

$$q_u = \frac{\lambda T_D}{1 + \lambda T_D} \cong \lambda T_D \ ,$$

onde T_D é o tempo médio em que o componente fica inoperante e é obtido experimentalmente pela distribuição G(d). A aproximação da equação provoca um erro < 10%, para $\lambda T_D < 0{,}1$.

Para componentes que não são monitorados, mas testados periodicamente, não é detectada qualquer falha, até que seja realizado um teste (por exemplo, mensalmente). Admite-se que os testes sejam perfeitos, i.e., são detectados 100% das falhas. Para testes periódicos, realizados com um intervalo T, a indisponibilidade cresce de um baixo valor $q(0) = 0$ após um teste, para um alto valor $q(T) = 1 - e^{-\lambda T} \cong \lambda T$, antes que o próximo teste seja realizado. A indisponibilidade média no intervalo de tempo entre os testes é $\lambda T/2$, valor que pode ser aplicado na avaliação da árvore de falhas, admitindo que a demanda de um componente pode ocorrer uniformemente naquele período de tempo. Se o compo

nente falha, então ele permanecerá inoperante até que o defeito seja detectado e o reparo termine. A indisponibilidade total do componente, q_T, será:

$$q_T = (\lambda T/2) + \lambda T_R \ ,$$

onde T_R é o tempo médio de reparo para aquele componente.

Em geral, T_R é pequeno em relação a T, logo

$q_T \cong \lambda T/2$, quando $T_R << T$.

Além da indisponibilidade, uma característica importante dos componentes reparáveis é a Taxa de Ocorrência de Falhas ("Failure Occurrence Rate") W(t), que é definida como a probabilidade de falha do componente no intervalo de tempo entre t e t + Δt. Para os sistemas não reparáveis, cada componente pode falhar uma única vez; logo, neste caso, a função W(t) é igual à função densidade de probabilidade f(t):

$W(t) = \lambda\ e^{-\lambda t} \cong \lambda$, para $\lambda t < 0{,}1$.

Para falhas reparáveis, W(t) é geralmente uma função complexa do tempo. Certos códigos de computador como KITT1 e KITT2 (ver Apêndice B), calculam os valores de W(t) para intervalos de tempo especificados. Contudo, para grandes intervalos de tempo, o valor assintótico de $W(t) \cong \lambda$ é normalmente suficiente para a maioria das aplicações.

Conhecida a função W(t), pode ser calculado o número de falhas do componente no intervalo de tempo entre t_1 e t_2, $n(t_1, t_2)$:

$$n(t_1, t_2) = \int_{t_1}^{t_2} W(t)\ dt.$$

5.2.3 Modelo de Taxa de Falhas por Demanda

Neste modelo, a probabilidade p de falha por demanda é considerada constante e independente do intervalo de tempo entre o instante em que o componente foi testado e o instante em que ocorre a demanda. Este modelo é chamado de Modelo p e é válido quando as falhas são inerentes aos componentes e não são provocadas por mecanismos associados com o tempo de exposição do componente. Por exemplo, o comportamento de um componente novo pode ser inicialmente analisado utilizando-se o modelo p, para levar em conta os defeitos de fabricação e, após os testes operacionais, muitas falhas inerentes aos componentes seriam detectadas e o comportamento do sistema seria melhor representado pelo modelo λ.

Sendo R_d a confiabilidade, q_d a indisponibilidade do componente por demanda e n o número de demandas do componente no tempo t, tem-se:

$$R_d = 1 - q_d = (1 - p)^n \quad \text{ou}$$

$$1 - R_d = q_d \cong np < 0,1.$$

Pelas equações acima, nota-se que as indisponibilidades dos componentes que funcionam sob demanda não dependem explicitamente do tempo, mas sim do número de demandas naquele intervalo de tempo.

5.2.4 Características de Confiabilidade dos Cortes Mínimos

Após a obtenção das características de confiabilidade dos componentes, podem ser obtidas as características de confiabilidade dos cortes mínimos.

Para sistemas de reserva ("standby"), tais como os sistemas de

segurança de reatores nucleares, a característica mais importante é a indisponibilidade Q(t) dos cortes mínimos. $Q_i(t)$ é definida como a probabilidade de que todos os componentes do corte mínimo i estejam inoperantes no tempo t, ou, de outra forma, é a probabilidade que o sistema esteja inoperante no tempo t, devido ao corte mínimo em questão. Dessa forma:

$$Q_i(t) = q_1(t) \cdot q_2(t) \cdot \ldots \cdot q_{n_i}(t),$$

onde $q_1(t)$, $q_2(t)$, ..., $q_{n_i}(t)$ são as indisponibilidades dos componentes do corte mínimo i e n_i é o número de componentes no corte mínimo.

Para sistemas em operação contínua, as características de confiabilidade mais importantes são o número de falhas e a probabilidade de ocorrência de nenhuma falha, num intervalo de tempo especificado. Estas informações podem ser obtidas através da determinação do parâmetro W(t) para o corte mínimo.

Para um corte mínimo i, $W_i(t)\,\Delta t$ representa a probabilidade de falha do sistema no intervalo de tempo entre t e $t + \Delta t$, devido a este corte mínimo em particular. Admitindo independência entre as falhas dos componentes, pode-se escrever:

$$\begin{aligned} W_i(t)\,\Delta t = {} & q_2(t) \cdot q_3(t) \cdot \ldots \cdot q_{n_i}(t) \cdot W_1(t)\,\Delta t + \\ & q_1(t) \cdot q_3(t) \cdot \ldots \cdot q_{n_i}(t) \cdot W_2(t)\,\Delta t + \\ & q_1(t) \cdot q_2(t) \cdot \ldots \cdot q_{n_i}(t) \cdot W_{n_i-1}(t)\,\Delta t \end{aligned}$$

No 2º membro da equação acima, o 1º termo é a probabilidade de que todos os componentes, exceto o nº 1, estejam inoperantes no tempo t e então ocorra a falha do componente nº 1; o 2º termo é a probabilidade de que todos os componentes, exceto o nº 2, estejam inoperantes no tempo t e então ocorra a falha do componente nº 2 e assim por diante. As contribuições das falhas de cada

um dos componentes no intervalo de tempo entre t e t + Δt são somadas, para os n_i componentes do corte mínimo i, para obter-se a taxa de ocorrência total de falhas.

A taxa de ocorrência do corte mínimo, $W_i(t)$, só pode ser obtida pela equação acima, quando todos os componentes têm uma taxa de falhas por hora. Para cortes mínimos cujos componentes operam sob demanda, as seguintes aproximações devem ser feitas:

$$q_d(t) \cong p \cdot n(t) \quad , \text{ e}$$

$$W_d(t) \cong p \cdot k(t) \quad ,$$

onde p é a probabilidade de falha por demanda do componente;

n(t) é o número esperado de demandas no tempo t;

k(t) é a probabilidade de ocorrência de uma demanda por unidade de tempo, no instante t;

e o índice d denota demanda.

Os valores de n(t) e k(t) devem ser obtidos de considerações operacionais dos componentes.

O número esperado de ocorrência do corte mínimo i, $N_i(t_1, t_2)$, no intervalo de tempo entre t_1 e t_2 é:

$$N_i(t_1, t_2) = \int_{t_1}^{t_2} W_i(t)\, dt.$$

Se os componentes do corte mínimo são todos reparáveis e são usados valores constantes para suas indisponibilidades e taxas de ocorrência, então $W_i(t)$ é uma constante W_i e, neste caso, $N_i(t_1, t_2) = (t_2 - t_1)\, W_i$.

Quando os componentes não são reparáveis, $N_i(t_1, t_2)$ é a probabilidade de ocorrência do corte mínimo, no intervalo de tempo entre t_1 e t_2.

Quando alguns componentes são reparáveis, os valores das não-confiabilidades exatas dos cortes mínimos são difíceis de calcular. No entanto, para pequenos valores de probabilidades de falha dos componentes, o valor de $N_i(t_1, t_2)$ pode ser tomado como boa aproximação para a probabilidade de ocorrência do corte mínimo i. Estes valores são fáceis de calcular e são suficientes para a maioria das aplicações.

5.2.5 Características de Confiabilidade do Sistema

Define-se como indisponibilidade $Q_s(t)$ do sistema a probabilidade de que o sistema esteja inoperante no instante t. Considerando desprezível a probabilidade de ocorrência simultânea de 2 ou mais cortes mínimos, pode-se escrever:

$$Q_s(t) = \sum_{i=1}^{N} Q_i(t),$$

onde N é o número de cortes mínimos do sistema.

Esta equação é obtida utilizando-se a aproximação dos eventos raros |10| e pode ser truncada em qualquer valor de N, considerando apenas os cortes mínimos com maior contribuição para a indisponibilidade do sistema.

Para sistemas em operação contínua, a taxa de ocorrência de falhas do sistema, $W_s(t)$, é definida como a probabilidade de falha no intervalo de tempo entre t e $t + \Delta t$. A falha do sistema ocorrerá se e somente se um ou mais cortes mínimos ocorrerem. Pode-se então escrever:

$$W_s(t) = \sum_{i=1}^{N} W_i(t).$$

Sendo $N_s(t_1, t_2)$ o número esperado de falhas do sistema no in

tervalo de tempo entre t_1 e t_2, tem-se:

$$N_S(t_1, t_2) = \int_{t_1}^{t_2} W_S(t)\, dt.$$

Se os componentes são todos reparáveis ou as taxas de falhas são por demanda e são usados valores constantes para as indisponibilidades, o valor de $W_S(t)$ é constante, e então:

$$N_S(t_1, t_2) = (t_2 - t_1)\, W_S.$$

Para $N_S(t_1, t_2) < 0{,}1$, este valor é uma boa aproximação para a não-confiabilidade do sistema.

Estes resultados descritos até agora são válidos somente para falhas independentes e, quando existem dependências, os valores de $Q_S(t)$, $W_S(t)$ e $N_S(t_1, t_2)$ representam apenas valores ótimos de projeto, que são úteis para avaliações relativas, mas não para avaliações absolutas.

5.2.6 Importância dos Cortes Mínimos

A importância dos cortes mínimos e dos componentes pode ser avaliada em relação à indisponibilidade do sistema ou em relação à taxa de ocorrência de falhas do sistema. Em qualquer caso, a importância qualitativa é a relação entre a característica do corte mínimo e a característica do sistema. Para o cálculo da importância do componente, somam-se as características de todos os cortes mínimos que contêm o componente e divide-se o resultado pela característica do sistema.

Sendo $E_i(t)$ a importância do corte mínimo i, no tempo t, e $e_k(t)$ a importância do componente k, no tempo t, ambos em relação à indisponibilidade do sistema, tem-se:

$$E_i(t) = \frac{Q_i(t)}{Q_s(t)} \quad , \text{ e}$$

$$e_k(t) = \frac{\sum_{k \text{ em } i} Q_i(t)}{Q_s(t)}.$$

Em termos de probabilidade condicionada, $E_i(t)$ é aproximadamente a probabilidade de que o sistema esteja inoperante, devido ao corte mínimo i, dado que ele está inoperante, e $e_k(t)$ é a probabilidade de que o sistema esteja inoperante, sendo o componente k uma das causas, dado que o sistema está inoperante.

Sendo $\hat{E}_i(t)$ a importância do corte mínimo i, no tempo t e $\hat{e}_k(t)$ a importância do componente k, no tempo t, ambos em relação à taxa de ocorrência de falhas do sistema, tem-se:

$$\hat{E}_i(t) = \frac{W_i(t)}{W_s(t)} \quad , \text{ e}$$

$$\hat{e}_k(t) = \frac{\sum_{k \text{ em } i} W_i(t)}{W_s(t)}.$$

A interpretação destes resultados é completamente análoga à do caso anterior.

5.2.7 Avaliação da Sensibilidade

Chama-se de avaliação da sensibilidade, a análise do impacto das variações dos dados dos componentes ou do modelo da árvore de falhas, nos resultados quantitativos. Se a indisponibilidade do sistema não muda significativamente com a variação de um determinado parâmetro, então o evento considerado é de pouca im

portância. Com a árvore de falhas simulada num computador digi tal, pode-se realizar um largo espectro de análise de sensibili dade, dependendo das necessidades do analista, através de alte rações de dados de entrada.

6 FALHA DE MODO COMUM (FMC)

6.1 Definição

Falhas de Modo Comum ("Common Mode Failures") são falhas múltiplas, i.e., falhas de mais de um componente, que ocorrem por causa de um único evento. Além da falha simultânea (caso extremo), a causa comum pode levar a uma degradação menos severa dos componentes, aumentando a probabilidade de estarem, em um determinado instante, num estado de falha.

6.2 Histórico

O potencial e as conseqüências das falhas de modo comum foram primeiramente reconhecidos no projeto e operação dos reatores de pesquisa. Em 1957 já era discutida a filosofia de redundância e coincidência para as funções principais de proteção dos reatores, utilizando equipamentos de diferentes tipos para reduzir as falhas de projeto e manutenção comuns. O fenômeno foi chamado inicialmente de falhas sistemáticas e, em 1968, foi chamado de falhas de modo comum pela AEC ("Atomic Energy Commission") |28|.

Em 1973/74 foi realizado, no Wash-1400 |48|, o primeiro estudo que incluiu técnicas de avaliação quantitativa das FMC. A partir de então, todas as avaliações probabilísticas de segurança de centrais nucleares americanas têm demonstrado a importância das FMC |31|. Desenvolveram-se também, ao longo dos anos, códigos de computador específicos para este tipo de análise |18|.

6.3 Mecanismos de Falhas

As FMC podem ser devidas a falhas de engenharia ou falhas externas. Os principais mecanismos que contribuem para estas falhas

são:

a) Deficiências de Projeto

São dependências não detectadas de sistemas ou componentes, de um elemento ou serviço comum. Podem ser também deficiências comuns numa característica de componentes de um certo tipo de um sistema ou subsistema.

Suas causas mais comuns são os erros nos métodos de projeto, erros na administração do projeto, deficiência do projetista, falta de comunicação entre o pessoal envolvido nas várias etapas do projeto, etc.

b) Fatores Ambientais

Condições inadequadas do ambiente da instalação podem levar a FMC. As causas mais comuns são a temperatura alta, a umidade excessiva, a vibração, a corrosão, ruídos, cargas estáticas, a radiação, a sujeira e a poeira.

c) Fenômenos Externos

São fenômenos tais como terremoto, fogo, inundação, tempestade, objetos cadentes, mísseis de máquinas rotativas ou tubulações, vazamentos de vapor, explosões, surtos de tensão, relâmpago, etc.

Tais fenômenos são de difícil previsão e podem provocar a falha de diversas linhas de defesa, simultaneamente.

d) Deficiências Funcionais

São sistemas que trabalham da forma que foram projetados, mas são inadequados para as tarefas ou propósitos para os quais estão sendo utilizados.

Podem ser devidas a erros de hipótese sobre o funcionamento da instalação, utilização de componentes inadequados, ou mudança posterior nas características da instalação.

e) Fatores Humanos

São fatores tais como esquecimento, má operação deliberada, respostas inadvertidas, não consideração de fatores humanos no projeto da instalação, etc. Suas causas principais são as falhas de comunicação, inspeções inadequadas, os erros de instalação ou montagem, os erros de teste e manutenção, erros de fabricação ou transporte de equipamentos e erros do operador, no desempenho de suas funções na instalação. As taxas de falhas humanas são mais altas que as maiores taxas de falhas de componentes elétricos e mecânicos (tipicamente por um fator de 100 |53|); e sob condições de alta tensão, como no caso de um acidente, o erro humano pode chegar a 100% dos casos.

6.4 Mecanismos de Defesa

Devido às técnicas de projeto dos sistemas de segurança dos reatores nucleares e aos componentes de alta confiabilidade utilizados, têm sido observadas, até hoje, relativamente poucas falhas nestes sistemas, provocadas por falhas independentes e aleatórias de seus componentes. Em todos os locais onde é utilizado um alto grau de redundância, a confiabilidade do sistema tem sido limitada pelas falhas de modo comum (FMC) |28|.

Diversas práticas podem ser utilizadas como forma de evitar as FMC:

a) Redundância

É a duplicação deliberada de componentes ou sistemas com a

finalidade de melhorar a sua confiabilidade global. No entanto, já ocorreram incidentes nos quais a redundância foi de pouco ou nenhum valor, devido à falha da interconexão entre os sistemas redundantes.

b) Coincidência

É o uso de um determinado número de canais redundantes e independentes, todos obtendo a mesma informação, e conectados de tal forma que nenhuma medida de segurança seja tomada a não ser que um certo número destes canais atue simultaneamente. Embora reduza um pouco a confiabilidade do sistema, a coincidência é necessária para evitar os desligamentos espúrios e para permitir teste e manutenção sem o desligamento da instalação.

c) Diversidade

É o uso de elementos que realizam as mesmas operações básicas, mas totalmente diferentes em projeto, conceito ou método de operação. Esta prática reduz bastante a probabilidade de ocorrência das falhas de modo comum, pois a maior parte destas é de componentes similares. Um bom exemplo de uso de diversidade é a proteção de um vaso de pressão, tanto por uma válvula de segurança, quanto por um disco de ruptura.

Mesmo utilizando diversidade, ainda podem aparecer FMC devidas a erros de especificação, de concepção de projeto e a fatores externos e ambientais.

d) Separação Física

É feita como uma forma de se obter diversidade, mas tem também a vantagem de proteger contra erros de manutenção. No entanto, se não existir independência entre os sistemas, esta prática torna-se inútil.

e) Independência

A falha de um sistema não deve influenciar na falha de outros. É praticamente impossível de ser obtida, pois os componentes estão normalmente no mesmo ambiente, utilizando às vezes a mesma fonte de energia, os mesmos equipamentos adjacentes, sujeitos aos mesmos procedimentos de teste e manutenção, etc.

f) Controle de Qualidade

A existência de um controle de qualidade adequado não só reduz a ocorrência de defeitos de fabricação mas também reduz os erros nas fases de projeto, montagem e operação da instalação.

g) Comunicação

Deve existir uma transmissão correta das informações administrativas e técnicas, bem como uma documentação adequada das informações de projeto. Se isto não ocorrer, os efeitos podem ser sentidos em todos componentes do sistema, aumentando a chance de ocorrência de FMC.

h) Inspeção, Teste e Manutenção

Deve-se ter cuidados especiais ao especificar e realizar as operações de inspeção, teste e manutenção. Tais procedimentos devem pesquisar explicitamente as FMC e estas operações em componentes redundantes devem ser realizadas em épocas diferentes, para reduzir a possibilidade de se cometerem os mesmos erros. Para a instrumentação utilizada para fins de segurança, a redundância dos padrões de calibração é também muito importante.

O número de falhas de modo comum só poderá ser reduzido através de cuidados, prevenção e experiência em projeto e fatores huma

nos, de todo o pessoal envolvido nas fases de projeto, fabricação, montagem, operação e manutenção dos sistemas. As FMC não podem ser previstas, apenas postuladas, mas uma vez reconhecida a possibilidade de ocorrência dessas situações, devem ser iniciados procedimentos corretivos ou ações para minimizar seus efeitos.

6.5 Considerações Regulamentares

De acordo com o critério 21 do 10 CFR 50, de 1961 e revisado em 1971 |15|, as falhas múltiplas que resultam de um único evento devem ser tratadas como falha de um único elemento. Logo, a redundância e independência são exigências de projeto para as centrais nucleares americanas.

Durante a década de 60, a AEC recomendou que fossem realizadas análises de FMC para vários sistemas de controle e segurança de reatores.

Em 1978 o "Code of Federal Regulation" reconheceu, através de uma publicação, que as FMC não estavam ainda bem definidas para o projeto dos sistemas de proteção e controle de reatores |28|. Desde então, as FMC têm sido objeto de constante atenção e suas ocorrências tem sido verificadas nos relatórios de eventos para licenciamento ("Licensing Event Reports") enviados para a NRC.

Atualmente, é dada maior ênfase ao estudo das FMC nas Avaliações Probabilísticas de Risco dos reatores nucleares nas seguintes etapas:

a) Seleção dos eventos iniciadores;

b) Definição das seqüências de acidentes;

c) Análise de falhas dos sistemas (árvores de falhas);

d) Estimativa das probabilidades dos acidentes.

6.6 Pesquisa das Causas das Falhas de Modo Comum

As FMC são mais prováveis de acontecer para componentes em operação intermitente, pois eles podem permanecer no estado de falhapor um longo período de tempo, até o próximo teste ou ativação. Já os componentes em operação contínua permanecem no estado de falha pouco tempo, pois a falta é mais facilmente detectada.

Na pesquisa das FMC, dois problemas principais surgem: a identificação das FMC potenciais e a sensibilidade do sistema à FMC em questão.

Para identificação das FMC, devem ser pesquisadas todas as propriedades dos cortes mínimos que indicam susceptibilidade potencial a causas comuns. Entre elas podem-se destacar:

a) Componentes idênticos em tipo e especificação;

b) Componentes com sensibilidade a falhas do mesmo tipo;

c) Componentes sujeitos aos mesmos procedimentos de teste e manutenção;

d) Componentes de um mesmo fabricante;

e) Componentes situados em um mesmo local;

f) Componentes expostos a um mesmo ambiente possível de acidente;

g) Componentes sobrecarregados ou degradados por uma falha prévia;

h) Falhas que podem ser iniciadas por erros humanos.

Em geral, todos componentes de um sistema podem ser potencialmente acoplados por uma causa ambiental. No entanto, são tantas as incertezas associadas com a ocorrência de eventos externos,

que não se justifica normalmente a sua inclusão na pesquisa das FMC.

A codificação dos eventos pode ajudar na pesquisa das FMC, pois falhas semelhantes podem ser indicadas pelo mesmo símbolo. A codificação que será utilizada neste trabalho é baseada no Wash-1400 |48| e permite este tipo de pesquisa preliminar (por exemplo, as falhas iniciadas por erros humanos são identificadas pela letra X).

A sensibilidade de um sistema a uma FMC de um corte mínimo pode ser determinada na prática, simplesmente atribuindo o mesmo código a todos os eventos do corte mínimo. Se isto alterar significativamente o valor da probabilidade de ocorrência do evento topo, o sistema deverá ser sensível à FMC em questão.

6.7 Avaliação das Falhas de Modo Comum

Os estudos de confiabilidade que consideram independência entre as falhas, não consideram a existência das FMC e podem levar a valores otimistas, i.e., não conservativos, para a probabilidade de falha do sistema.

A avaliação das FMC é uma área ainda em desenvolvimento e muitas dificuldades aparecem, entre elas:

a) Existência de um largo espectro de possibilidade de falhas e de meios de sua detecção;

b) Ausência de meios quantitativos para definição dos Acidentes Bases de Projeto ("Design Basis Accidents");

c) Escassez de dados de FMC de centrais nucleares e utilização de dados tomados de outros sistemas.

Quatro métodos são mais freqüentemente utilizados para a avalia

ção das FMC:

a) Método Explícito

Este método identifica as causas específicas das falhas múltiplas e/ou utiliza modelos específicos para cada interação física ou humana, incorporando estas causas diretamente nas árvores de falhas |18|.

A maior limitação deste método é a ausência dos dados de falhas de modo comum mais freqüentes. Não se pode portanto garantir um estudo completo e os erros associados com a omissão podem ser enormes.

Outra dificuldade do modelo é a incorporação das causas comuns nas árvores de falhas, aumentando consideravelmente o número de cortes que precisam ser processados nos estudos de risco, que normalmente já estão limitados pela capacidade dos computadores utilizados. Um desenvolvimento indiscriminado de uma árvore de falhas em falhas secundárias, sem olhar a probabilidade de ocorrência dos eventos comuns, pode resultar em um número proibitivo de eventos e em um gasto considerável de tempo e esforço.

Seja, por exemplo, um sistema constituído por 3 componentes A, B e C, que podem falhar por causas independentes (eventos A', B' e C') ou por causas dependentes entre os componentes A e B (evento D) e B e C (evento E), conforme Figura 6.1.

Admitindo as probabilidade $P(A') = P(B') = P(C') = 10^{-3}$ e as contribuições de causa comum variando de 0 a 1% da indisponibilidade dos componentes, são analisados 3 casos:

Caso 1

Para este caso, os componentes são considerados independentes e não é considerada a falha do sistema, provocada pela

falha de um único componente (P(C') = 0). Conforme se vê na Tabela 6.1, a indisponibilidade do sistema neste caso será 1×10^{-6}.

Caso 2

Para este caso são consideradas causas comuns entre A e B ainda sem considerar falha do sistema provocada pela falha de um único componente. Admitindo uma contribuição de causa comum equivalente a 1% da indisponibilidade dos componentes ($P(D) = 10^{-5}$), a indisponibilidade do sistema é aumentada por um fator de 10 (ver Tabela 6.1).

De uma maneira geral, pode-se afirmar que sempre que é admitida independência entre sistemas redundantes altamente confiáveis, é necessário certificar se todas as causas das falhas dos subsistemas são independentes, com um nível de confiança muito alto.

Supondo que não se está certo se existe uma causa comum de falha do sistema, a sua indisponibilidade q_s será dada por:

$$q_s = p \cdot q + p_c \cdot q_c ,$$

onde q é a indisponibilidade do sistema, supondo independência; q_c é a indisponibilidade do sistema, supondo a existência de causas comuns e $p = 1 - p_c$ representa o grau de confiança de que não existe causa comum de falha do sistema.

Para manter o erro na estimativa da indisponibilidade do sistema abaixo de um certo valor α, i.e.,

$$\frac{q_s - q}{q_s} \leq \alpha, \qquad \text{deve-se ter:}$$

$$p \geq \frac{(1 - \alpha)\ q_c - q}{(1 - \alpha)\ (q_c - q)} .$$

Assim, para um erro inferior a 10% ($\alpha \leq 0,1$), deve-se estar mais que 98,9% confiante que não existe uma contribuição de causa comum inferior a 1% da indisponibilidade do componente. Para uma contribuição de causa comum de 10%, o nível de confiança requerido aumenta para 99,9%. Este é o caso de sistemas com alto grau de redundância.

Como se pode notar, a precisão da avaliação da indisponibilidade do sistema depende não apenas das falhas dos componentes serem dependentes, mas também do grau de dependência.

Casos 3 e 4

No caso 3, não é considerada a redundância fazendo-se P(A) = 1, o que resulta numa indisponibilidade do sistema de 2×10^{-3}. No caso 4 é considerada uma contribuição de causa comum entre B e C, de 50% de indisponibilidade dos componentes, o que faz com que a indisponibilidade do sistema decresça de 25%.

Normalmente a fração de contribuição de causa comum é menor que 50%, o que faz o efeito da redução da indisponibilidade do sistema série se torne menor. Conseqüentemente, em muitos casos, este tipo de causa comum pode ser ignorado, com um pequeno erro do lado conservativo. Contudo este exemplo serve para ilustrar que a existência de qualquer causa comum, que afeta um conjunto de componentes de um sistema, irá alterar o valor da indisponibilidade do sistema.

b) Técnica da Limitação

Na maioria das vezes é muito difícil saber qual é a contribuição de uma causa comum para a indisponibilidade de um gru

po de componentes. Para este caso, no Wash-1400 |48| foi utilizada a seguinte aproximação:

Se for considerada uma dependência total entre os eventos falhas A_1, A_2, ..., A_n, a probabilidade de falha simultânea $P(A_1 \cdot A_2 \cdot \ldots \cdot A_n)$ deverá ser:

$$P(A_1 \cdot A_2 \cdot \ldots \cdot A_n) \leq \text{MIN}\,[P(A_1), P(A_2), \ldots P(A_n)].$$

Este é portanto o limite superior L_s para

$$P(A_1 \cdot A_2 \cdot \ldots \cdot A_n).$$

Outros documentos utilizam o valor máximo das probabilidades dos eventos individuais como o limite superior L_s |53|. Isto é verdade somente quando a falha de um componente leva à falha dos outros componentes e vice-versa. Se existem causas separadas de falhas para cada componente, então estas informações devem estar contidas nos dados nos quais as probabilidades foram baseadas. Neste caso, a expressão utilizando o valor mínimo das probabilidades é geralmente a mais indicada. Na maioria dos casos práticos, $P(A_1)$, $P(A_2)$, ..., $P(A_n)$, são iguais, principalmente para o caso de componentes redundantes, e a distinção entre os valores máximo e mínimo torna-se irrelevante.

O limite inferior L_i poderá ser obtido, admitindo independência total entre os eventos, ou seja:

$$P(A_1 \cdot A_2 \cdot \ldots \cdot A_n) \geq P(A_1) \cdot P(A_2) \cdot \ldots \cdot P(A_n)$$

Admitindo uma distribuição lognormal para as falhas de modo comum |48|, a mediana M pode ser estimada como:

$$M = \sqrt{L_s \cdot L_i}\ .$$

Seja, por exemplo, utilizar esta técnica de limitação para avaliar a probabilidade de falha de 2 componentes redundantes A e B, com probabilidades de falhas individuais P(A) = P(B) = 10^{-3} e cujos dados de contribuição de causa comum não são bem conhecidos:

L_s = MIN (10^{-3}, 10^{-3}) = 10^{-3}

L_i = P(A) · P(B) = $10^{-3} \cdot 10^{-3} = 10^{-6}$

$M = \sqrt{L_s \cdot L_i} = \sqrt{10^{-3} \cdot 10^{-6}} = 3{,}2 \times 10^{-5}$.

Comparando este resultado com os casos 1 e 2 do método explícito, conclui-se que, para este valor representar a indisponibilidade do sistema, constituído pelos dois componentes redundantes A e B, a contribuição de causa comum deverá ser de aproximadamente 3% da indisponibilidade dos componentes. Para $\alpha \geq 10\%$, deve-se estar 99,6% confiante de que não existe uma causa comum de falha para os dois componentes, para justificar sua omissão.

c) Métodos Paramétricos

Os métodos paramétricos levam em conta os efeitos da FMC através do uso de parâmetros especiais de causa comum. São exemplos destes métodos, o Modelo do Fator β e numerosas variações do Método de Marshal-Olkin, algumas vezes chamado de Modelo de Choque. Uma especialização do modelo de choque, o Modelo de Taxa de Falhas Binomial foi desenvolvido mais recentemente, em 1977 |30|.

Um dos principais problemas encontrados na aplicação dos modelos paramétricos é a ausência de clareza e detalhes necessários para a estimativa dos parâmetros das FMC, nas fontes de dados disponíveis. Isto, combinado ao fato que as FMC de interesse são, na sua maioria, eventos raros, acrescenta vá

rias fontes de incertezas na estimativa dos parâmetros.

O modelo do fator β admite que cada componente ou sistema tem duas contribuições possíveis para suas falhas:

. causa intrínseca (indisponibilidade q_i);

. causa comum (indisponibilidade q_{cc}).

A indisponibilidade q_s do sistema será a soma das duas, i.e.:

$$q_s = q_i + q_{cc}.$$

Definindo β como sendo a probabilidade de falha de um componente ou sistema, devida a uma falha de modo comum, tem-se:

$$\beta = \frac{q_{cc}}{q_s} .$$

Existem levantamentos de valores de β típicos para determinados tipos de componentes; estes variam normalmente entre 0,01 e 0,4 |53|. Estes valores são fáceis de calcular e, em muitos casos, são mais fáceis de obter do que as taxas de falhas básicas, desde que não são necessários dados de tempo de exposição e da população exposta. Estes valores de β podem ser obtidos diretamente dos relatórios de eventos |18|.

Seja, por exemplo, calcular pelo modelo do fator β a probabilidade de falha de dois componentes redundantes. Considerando a existência de falhas de modo comum, a probabilidade de falha do sistema, Q_s, será:

$$Q_s = q_i^2 + q_{cc} , \quad \text{ou}$$

$$Q_s = (1 - \beta)^2 q_s^2 + \beta q_s .$$

Pela tabela 6.2, conclui-se que quando $\beta >> q_s$, a FMC domina

a equação e o erro que se comete em não se considerarem as FMC passa a ser muito maior.

Uma estimativa para os valores de β pode ser obtida, para uma amostra de n componentes, a partir da seguinte fórmula:

$$\beta = \frac{n_c}{n_c + n_i} \quad , \text{ onde}$$

n_c é o número de FMC na amostra e n_i é o número de falhas independentes na amostra.

A maior fonte de incertezas nesta estimativa é o tamanho n da amostra; quanto maior n, maior a precisão do fator β. Interpretando β como uma probabilidade de sucesso (ocorrência de uma FMC numa amostra com falhas dependentes e independentes), a distribuição binomial pode ser usada para estimar a probabilidade L(E/β) de observar n_c falhas de componentes, i.e., a probabilidade da evidência E, dado β:

$$L(E/\beta) = \frac{n!}{n_c!\, n_i!}\ \beta^{n_c}\ (1 - \beta)^{n_i}.$$

O valor desta probabilidade pode ser usado no teorema de Bayes para incorporar os dados coletados no conhecimento"a priori"do valor de β(ver mais detalhes no Capítulo 8).

d) Métodos Computacionais

São modelos que envolvem a utilização de códigos de computador especialmente desenvolvidos para análise das FMC, entre eles:

COMCAN - Desenvolvido pela "Aerojet Nuclear Company", este código tem como dados de entrada os cortes mínimos do siste

ma e os dados de susceptibilidade a causa comum de cada evento básico e, como dados de saída, a lista dos cortes mínimos que são candidatos às FMC. Pelo código, um corte mínimo pode ser um candidato a FMC por um dos dois motivos:

- todos os eventos do corte mínimo são potencialmente afetados pela mesma causa ou condição;
- todos os eventos do corte mínimo compartilham uma susceptibilidade a uma causa comum e, além disso, todos os componentes implicados pelos eventos básicos dos cortes mínimos compartilham um local físico comum, em relação à susceptibilidade a causa comum.

SETS - Este código, através de uma transformação de variável, incorpora a susceptibilidade a causas comuns na equação booleana para o evento topo ou qualquer evento intermediário da árvore de falhas. Um pequeno número de interações permite ao usuário descobrir os cortes mínimos que são candidatos a FMC.

6.8 Comentários

Mesmo existindo informações de falhas em centrais nucleares, nos Relatórios de Eventos para Licenciamento, estes resultados não têm sido utilizados adequadamente para a obtenção de dados de FMC, o que tem dificultado seu processo de avaliação |28|.

Embora a utilização da redundância e da coincidência reduza a probabilidade de falha de um sistema devida à falha aleatória de seus componentes e proporcione meios de realizar testes e manutenção em serviço, ela também introduz o problema das FMC.

A tendência das FMC é aumentar com a complexidade dos sistemas. Esta também é a tendência da preocupação com os fatores humanos, que irão estabelecer um limite para a confiabilidade dos

sistemas. Como os seres humanos são elementos ativos nos sistemas de controle, estes eventos aleatórios mas dependentes continuarão sempre existindo.

Não existem portanto soluções para o problema das falhas de modo comum, existem apenas alternativas para minimizá-las.

7 ERROS HUMANOS

Uma das causas mais importantes de falhas nas instalações nucleares são os erros humanos. Em certas situações, uma avaliação incorreta do estado da instalação pode levar a uma falha funcional de vários componentes, sem a existência de qualquer falha do equipamento propriamente dito.

Desde a ocorrência do acidente na usina nuclear de "Three Mile Island 2", em 1979, a NRC passou a dar uma importância maior ao estudo da confiabilidade humana em centrais nucleares, verificando como os erros humanos contribuem para o risco global e implementando meios para melhorar a segurança dos sistemas [51].

7.1 Tipos de Erros Humanos

Basicamente, são dois os tipos de erros humanos:

a) Erros em seguir procedimento - são mais freqüentes e normalmente menos severos;

b) Erros cognitivos (erros na tomada de decisão) - são menos freqüentes e normalmente mais severos.

Estes tipos de erros são ilustrados na Figura 7.1.

Os erros humanos podem ser mais especificamente agrupados em:

7.1.1 Erros de Comunicação

São erros devidos a informações inadequadas, ausência de diretrizes ou de supervisão, uso de manuais ou procedimentos ultrapassados ou, ainda, mudança de política de pessoal.

7.1.2 Erros de Instalação ou Montagem

São erros devidos a má qualidade de montagem, tais como parafusos frouxos ou excessivamente apertados, conexões incorretas, substituição inadequada de componentes, etc.

7.1.3 Erros de Manutenção

São normalmente erros de descuido, ajuste impróprio de equipamento, má calibração, modificações e reparos, que tornam inoperantes os componentes de um sistema.

7.1.4 Mau-funcionamento de Componentes

São provocados por erros de fabricação, programas de controle de qualidade inadequados, substituição de material, não conformidade com normas ou transporte inadequado de materiais.

7.1.5 Erros do Operador

São erros devidos a ações, ajustes, ou desempenho impróprios do operador. Algumas vezes são deliberados, quando o operador deliberadamente ignora indicações corretas das condições da instalação.

Freqüentemente os erros humanos são também classificados como erros por ação ou por omissão. Porém, tais classificações não são práticas.

7.2 Causas dos Erros Humanos

As causas mais freqüentes das falhas humanas são:

a) Diferença entre as tarefas realizadas pelo trabalhador e o treinamento ou educação recebidos;

b) Diferença entre os procedimentos e a tarefa a ser executada;

c) Influência da organização do trabalho nas características da tarefa a ser executada (conflito entre segurança e produção);

d) Histórico da instalação (incidentes freqüentes);

e) Influência do ambiente social (sentimento de solidão durante os turnos noturnos, etc.);

g) Desempenho individual, fisiológico e psicológico.

Todas estas categorias podem interferir umas com as outras e algumas são difíceis de separar.

7.3 Mecanismos de Defesa

A melhor forma de defesa contra os erros humanos é tornar todos os sistemas de interesse o mais independente possível do operador. Mesmo assim, a presença do homem é indispensável, principalmente em emergências, no diagnóstico de situações complexas, não previstas pelos computadores.

Devido à natureza aleatória das falhas humanas, elas são de difícil previsão. No entanto, algumas medidas podem ser tomadas, visando reduzir sua freqüência:

a) Treinamento adequado, oferecendo condições para os operadores lidarem com situações acidentais (emergências);

b) Existência de pelo menos um operador licenciado em cada turno de operação da instalação;

c) Consideração das conveniências do operador na determinação

dos leiautes dos painéis de controle.

Deve haver uma integração entre os instrumentos de leitura, os indicadores, o controle, os procedimentos e o operador. Por exemplo, os instrumentos de leitura ou sinalizadores críticos devem ocupar posições centrais nos painéis e seus controles associados devem estar localizados num mesmo lado da sala;

d) Consideração, em cada estágio, da possibilidade de ter havido falhas em estágios anteriores (projeto, calibração ou procedimentos).

7.4 Taxas de Falhas Humanas

As taxas de falhas humanas são mais altas (tipicamente por um fator de 100), do que as maiores taxas de falhas dos componentes elétricos ou mecânicos de uma central nuclear. Sob condições de muita tensão emocional, a probabilidade de erro humano pode chegar a 100%. Verifica-se que em reatores BWR, mais de 30% das falhas são devidas a erros humanos e em PWR este número ultrapassa a 50% |53|. Isto comprova a importância das falhas humanas na análise de confiabilidade de sistemas complexos.

Muitas dificuldades surgem na avaliação das taxas de falhas humanas:

a) As taxas de falhas para equipamentos e componentes podem ser determinadas para certas condições e ambientes de trabalho específicos, mas o mesmo não pode ser feito para o elemento humano. Não existe, nem nunca vai existir, um ser humano médio ou típico, cujo desempenho e reações a quaisquer condições operacionais (normal ou anormal), possam ser catalogadas, qualitativamente definido ou quantitativamente determinado;

b) É difícil decidir satisfatoriamente o que é um erro humano. Algumas vezes, o operador não obedece a uma determinada regra, agindo de uma forma diferente, tomando como base a sua experiência. Seja por exemplo, a seguinte situação: O operador deve desligar a instalação quando o nível da variável ultrapassar o nível de alarme. Considerando as três situações ilustradas na Figura 7.2, tem-se:

. No caso 1, o operador permite que a variável ultrapasse várias vezes o nível de alarme, envolvendo, portanto, erros múltiplos;

. No caso 2, o operador comete apenas um erro;

. No caso 3, o operador não comete nenhum erro.

No entanto tais eventos podem levar a conseqüências bastante diferentes para a instalação.

c) As pessoas não erram, a não ser que apareça a oportunidade. A avaliação das taxas de falhas deve portanto levar em conta as duas probabilidades individuais e a probabilidade do trabalhador cometer aquele erro específico;

d) As pessoas tendem a cometer falhas de modo comum, pois quando cometem um erro, normalmente cometem outros. Logo, os erros humanos não são independentes uns dos outros. Isto significa que a probabilidade condicionada de um erro de uma pessoa é a freqüência relativa de ocorrência de um erro específico, dados tanto a oportunidade quanto os erros que o precederam;

e) As pessoas tendem a descobrir seus próprios erros e corrigi-los antes que ocorra algum problema mais sério. Para se obter a probabilidade de erro líquido, a probabilidade absoluta de se cometer um erro (dados a oportunidade e os erros precedentes) deve ser multiplicada pela probabilidade de que o mesmo erro não seja corrigido antes de uma conseqüência de

sastrosa;

f) As probabilidades de erros de operadores trabalhando no mesmo local não são independentes, pois há grande interação entre pessoas que trabalham juntas, que podem inconscientemente reforçar impressões uns dos outros. Isto pode até fazer com que a confiabilidade de dois operadores seja menor que a de um;

g) Há uma menor disponibilidade de informações sobre taxas de falhas humanas que de taxas de falhas de componentes. As linhas aéreas fazem normalmente um levantamento geral do desempenho dos operadores, por exemplo, do número de vezes em que o operador tem que levantar, ir a painéis, etc. No entanto, este procedimento não é usual em outros tipos de indústria.

h) Os dados de outras indústrias não podem ser aplicados diretamente para a área nuclear, devido às diferenças entre as pessoas, treinamento, motivação, procedimentos, etc. Os dados de taxas de falhas obtidos de simuladores de centrais não podem também ser aplicados a casos reais, devido à variação do desempenho dos operadores com o nível de tensão emocional. Um exemplo deste tipo de estudo é a curva da Figura 7.3. A níveis de tensão muito altos, tal quando estivesse ocorrendo a fusão do núcleo do reator e o sistema de refrigeração de emergência não funcionasse, o desempenho do operador seria bem baixo (podendo chegar a 0%). Com baixo nível de tensão, por exemplo, devido a ausência de motivação, o desempenho dos operadores seria também bastante inferior ao máximo.

Levantamentos estatísticos americanos têm demonstrado que manipulações incorretas em válvulas e erros em seguir procedimentos são os tipos mais freqüentes de falhas humanas. A probabilidade de erro na execução de uma tarefa é geralmente alta e varia de 10^{-3} a 10^{-1}. De uma maneira geral, os operadores bem treinados têm uma probabilidade de erro da ordem de 10^{-3} e mal treinados

da ordem de 10^{-1}. Erros na leitura de gráfico são da ordem de 10^{-2} e de resposta a um anunciador (alarme) são da ordem de 10^{-4} |53|.

8 DADOS PARA ANÁLISE DA ÁRVORE DE FALHAS

Durante muitos anos o desenvolvimento da análise probabilística de risco foi bastante lento, principalmente devido à escassez de dados. Estes dados incluem a descrição dos modos de falha, os modelos de representação dos componentes, os dados de taxas de falhas e os dados de taxas de reparos.

As fontes de onde podem ser extraídas estas informações são:

a) Registros de dados de acidentes;

b) Histórico de acidentes;

c) Relatórios de eventos relacionados com a segurança;

d) Banco de dados de taxas de falhas de componentes genéricos;

e) Banco de dados de taxas de falhas de componentes específicos.

Existem registros de dados de acidentes na maioria dos países do mundo. Estes, na forma de narrativa, incluem geralmente alguns dados em relação ao local, ambiente de trabalho, pessoas envolvidas, conseqüências do acidente, etc. Estes registros são feitos normalmente por diferentes pessoas, em diferentes indústrias, que têm pouco ou nenhum conhecimento de como se deve fazer um registro sistemático de um acidente.

A experiência mostra que a maior parte dos equipamentos ou componentes segue a curva em forma de banheira ("bathtub curve") mostrada na Figura 8.1. A infância do componente, que surge devido às falhas de produção, teste ou montagem iniciais, é a região de maior preocupação. Pelo levantamento estatístico de transientes, observa-se que a freqüência de ocorrência de falhas é sempre maior no primeiro ano de vida de uma central nuclear. Passado este período, a taxa de falhas tem uma fase aproximadamente constante, num valor mínimo, que corresponde à vida

útil do componente, até que se inicia a fase de envelhecimento, onde a taxa de falhas começa novamente a aumentar.

Para se fazer qualquer estimativa de taxa de falhas, são necessários dois tipos de informação:

. Número de falhas que ocorreu;

. Número de horas de operação, ou seja, o tempo durante o qual a falha poderia ter ocorrido (tempo de exposição).

Os registros de acidentes raramente fornecem informações do tempo de exposição, sendo portanto difícil de extrair dados de taxas de falhas destes.

Os relatórios de eventos em centrais nucleares se constituem nos bancos de dados mais utilizados, pois possuem uma descrição criteriosa dos modos de falha e dos incidentes que envolvem falhas múltiplas.

Um banco de dados com informações suficientes para análise de árvore de falhas deve conter:

a) Uma distinção clara entre o modo da falha e a causa da falha;

b) Uma classificação do tipo de componente, de forma que os componentes de interesse possam ser facilmente identificados;

c) Registro da forma de obtenção dos dados e do número de informações, nas quais os dados foram baseados;

d) Registro da finalidade do estado de operação normal do componente;

e) Nível de manutenção e teste do componente;

f) Distinção entre o tempo de detecção de uma falha e o tempo de reparo do componente.

Ainda não existe um banco de dados de falhas nacional e um dos subprodutos da utilização da análise probabilística de risco para as instalações nucleares seria a sua criação.

Neste trabalho (Capítulo 10) foram utilizados basicamente 3 bancos de dados genéricos: Wash-1400, IEEE-500 e NUREG/CR-2728.

8.1 Dados do Wash-1400

Os dados do Wash-1400 |48|, coletados em 1974, cobrem uma gama muito grande de componentes de uma central. No entanto, a classificação dos componentes é muito genérica, o que leva a limites de confiança bem amplos, provocando uma incerteza muito grande nos cálculos que utilizam estes dados.

Os dados são fornecidos na forma do 5º e do 95º percentil da distribuição lognormal, associada às taxas de falhas. A variabilidade leva em conta os diferentes fabricantes e diferentes modelos, com diferentes condições de operação e manutenção, bem como as flutuações aleatórias que ocorrem em componentes presumivelmente idênticos.

Como a faixa dos dados de falha varia de 1 a 2 ordens de grandeza, a distribuição natural para este caso é a lognormal, da mesma forma que a distribuição normal é a distribuição natural quando os dados variam por incrementos.

As principais razões para a escolha da distribuição lognornal foram:

a) A forma da distribuição lognormal, em particular a sua inclinação, pode incorporar comportamentos gerais dos dados de taxas de falhas(p. ex., a ocorrência de menores probabilidades para grandes desvios, ou seja, para taxas de falhas anormalmente altas, devido a defeitos em bateladas, condições ambientais desfavoráveis, etc.).

b) Como as taxas de falhas podem ser decompostas em produtos de probabilidades, que representam seus vários mecanismos causais, a distribuição resultante é a lognormal (se $\lambda = p_1 \cdot p_2$, a variável $\log \lambda = \log p_1 + \log p_2$ deve seguir aproximadamente uma distribuição normal).

c) Em 90% dos casos, os dados de taxas de falhas disponíveis são menores que a média. A distribuição lognormal representa bem esta tendência, pois sua média é maior que a sua mediana.

Estes itens acima não constituem princípios para uma justificativa da escolha da lognormal como a única distribuição aplicável, mas são apenas considerações"a priori",feitas pelo Wash-1400.

8.2 Dados do IEEE-500

Este documento |33|, de 1977, foi elaborado com a finalidade de se fazer uma tentativa para obter dados de falhas mais detalhados, fazendo o uso do julgamento de engenharia. Os valores registrados foram sintetizados das opiniões de aproximadamente 200 especialistas em dados de falhas. É, conceitualmente, uma aproximação muito boa do ponto de vista do tipo e da apresentação dos dados. O conceito dos modos de falhas são amplamente definidos e desenvolvidos. São fornecidos os dados de falhas por tempo de operação e por demanda, com fatores que levam em conta os efeitos ambientais. Cada especialista registrou um valor baixo (λ_{baixo}), um valor recomendado (λ_{rec}) e um valor alto (λ_{alto}) para a taxa de falhas,sob condições normais, e um valor máximo (λ_{max}), que pode ser aplicado para quaisquer condições. O banco de dados atual compreende apenas componentes elétricos, eletrônicos, sensores e atuadores de válvulas.

O documento não sugere nenhuma distribuição de probabilidades para as taxas de falhas,mas como o método de ponderação utilizado foi a média geométrica, parece razoável adotar-se a distri

buição lognormal também para este caso.

No documento é sugerido o "valor recomendado" como sendo a melhor estimativa. Este valor pode ser interpretado como a mediana da curva lognormal, que é uma medida de tendência central mais representativa que a média, que é muito sensível aos extremos da distribuição. Esta suposição é também conservativa, pois o valor médio da distribuição resultante (ao admitir-se a mediana igual ao valor recomendado), é maior que o valor recomendado.

Os valores máximos e baixos são usados para a obtenção do Fator de Erro ("Error Factor") - FE, pela seguinte equação:

$$FE = \sqrt{\frac{\lambda_{max}}{\lambda_{baixo}}} \quad ,$$

que incorpora, através de λ_{max}, as flutuações devidas a ambientes anormais.

8.3 Dados do NUREG/CR-2728

O documento NUREG/CR-2728 |9|, de 1983, fornece valores de médias, medianas e fatores de erro para as taxas de falhas, para fins de estimativas preliminares de análise probabilística de risco, em centrais nucleares. Para cálculos mais precisos, são recomendados dados de falhas mais específicos para a central.

A mediana e o fator de erro definem uma distribuição lognormal, que descreve as incertezas dos parâmetros de confiabilidade, se se interpretar que o fator de erro define uma região entre o 5º e o 95º percentis.

São listados dados de taxas de falhas por hora e por demanda. Os

dados de taxas de falhas por demanda ($\bar{q}$) foram obtidos da seguinte expressão:

$$\bar{q} = \frac{\lambda T}{2}$$

onde λ é a taxa de falhas por hora, do componente, e T é o número de horas em um mês (supondo um período de testes mensal).

Este valor não deve ser interpretado como a probabilidade real de falha por demanda, que dependeria somente do número de vezes em que ocorre demanda do componente de reserva para operação, e que seria independente do tempo entre testes de operabilidade do componente. Para componentes cujo período entre testes não é substancialmente diferente de 1 mês (por exemplo, até 5 ou 6 meses), o valor da probabilidade de falha por demanda é considerado adequado.

8.4 Especialização de Dados

A especialização ou atualização de dados de falhas consiste na determinação de dados específicos para uma instalação, tendo em vista dados operacionais observados.

O teorema de Bayes é a ferramenta fundamental para a atualização de probabilidades, quando novas evidências tornam-se disponíveis, e pode ser representado pela equação:

$$f(\lambda/E) = \frac{f(\lambda)\ L(E/\lambda)}{\int_0^\infty f(\lambda)\ L(E/\lambda)\ d\lambda}$$

onde, f (λ/E) é a função densidade de probabilidade de λ dada a evidência E (distribuição"a posteriori"); f(λ) é a função densidade de probabilidade antes da evidência E (distribuição"a prio

~~[illegible] é a função de probabilidade (probabilidade da evi~~

dência E dado λ).

Em geral, a avaliação da integral do denominador da equação, não pode ser feita analiticamente e uma solução para este problema é a utilização de valores discretos de probabilidades, substituindo-se a integral por um somatório.

Considerando a ocorrência de eventos independentes, a função de probabilidades terá uma das duas formas, dependendo da situação:

a) Quando a evidência é um número de falhas "r" em "n" tentativas, a distribuição será binomial, ou seja:

$$L\ (E/\lambda) = \frac{n!}{r!\ (n - r)!}\ (\lambda_i)^r\ (1 - \lambda_i)^{n - r}$$

onde λ_i é a freqüência de falhas por demanda;

b) Quando a evidência é da forma "r" falhas num tempo operacional "T", utiliza-se a distribuição de Poisson, ou seja:

$$L\ (E/\lambda) = \frac{(\lambda_i T)^r}{r!}\ \exp\ (-\lambda_i\ T),$$

onde λ_i é a freqüência de falhas por unidade de tempo.

Para a maioria dos problemas de análise de risco, onde os valores de λ_i são muito pequenos, pode-se utilizar a distribuição de Poisson ao invés da binomial, bastando para isto fazer $\lambda_i T = n\ \lambda_i$.

Seja, por exemplo, determinar a distribuição de taxas de falhas de partida de geradores diesel, com uma evidência de r = 5 falhas em n = 227 testes. A freqüência de falhas na partida é dada no Wash-1400 como $\xi_{5\%} = 10^{-2}$ e $\xi_{95\%} = 10^{-1}$, onde $\xi_{5\%}$ e $\xi_{95\%}$ são o 5º e 95º percentis, respectivamente. Com estes valores, de acordo com o Apêndice D, calculam-se os parâmetros da

distribuição lognormal associada:

mediana = $3,2 \times 10^{-2}$;

média = $4,0 \times 10^{-2}$;

variância = 10^{-3}.

Pelas características da evidência, a função de probabilidade deverá ser a binomial e, utilizando valores discretos para a distribuição"a priori",obtêm-se, aplicando o teorema de Bayes, os valores mostrados na Tabela 8.1. A Figura 8.2 mostra graficamente o efeito da evidência na probabilidade"a priori".

A média e a variância do histograma"a posteriori"são 0,025 e $8,2 \times 10^{-5}$, respectivamente. Às vezes é conveniente aproximar o histograma a uma distribuição analítica contínua. Neste exemplo nota-se que o histograma numa escala semi-logarítmica é simétrico, o que sugere que é aplicável uma distribuição lognormal. O efeito da evidência, neste caso, foi o de levar a distribuição das taxas de falhas em direção aos valores inferiores e reduzir a dispersão da sua distribuição, em relação à distribuição "a priori".

8.5 Denominação dos Eventos Primários

A cada evento primário deverá ser atribuído um valor de taxa de falhas,se se deseja fazer uma avaliação quantitativa da árvore de falhas. É sempre conveniente tanto para uma análise qualitativa quanto para uma análise quantitativa, a atribuição de um código de identificação, a cada um dos eventos primários. Esta codificação auxiliará na análise qualitativa, ajudando na pesquisa das falhas de modo comum, desde que ela indique o tipo de componente a que se refere o evento primário e o seu respectivo modo de falha. A existência deste código é também necessária para a avaliação quantitativa automatizada, pois os programas de computador, em geral, requerem que sejam atribuídos nomes de va

riáveis a cada um dos eventos primários.

Será adotada parcialmente a denominação utilizada pelo Wash-1400, pois ela define o tipo de componente e o seu modo de falha. Outra identificação adotada neste documento, a identificação do sistema ao qual o componente pertence, não foi julgada pertinente para os propósitos desta análise.

O nome do evento primário consistirá basicamente de 3 partes:

a) Denominação do componente;

b) Denominação do modo de falha;

c) Numeração do evento primário.

Basicamente, os componentes de uma central nuclear podem ser mecânicos e elétricos. A denominação de cada componente será feita por duas letras, de acordo com as Tabelas 8.2 e 8.3, para componentes mecânicos e elétricos, respectivamente. Por exemplo, RV identifica uma válvula de alívio ("Relief Valve") e TP identifica um transmissor de pressão ("Pressure Transmitter"). A denominação do modo de falha, será feita através de uma letra, de acordo com a Tabela 8.4. Por exemplo, X e R, significam falha operacional ("Operational Fault") e ruptura ("Rupture"), respectivamente. A numeração do evento primário será feita por um número de dois algarismos.

Por exemplo, o evento primário CND 26 identifica a falha de um contato de um relê (CN) em não abrir (D),ordenada com o número 26.

9 TRATAMENTO DAS INCERTEZAS

O tratamento de incertezas na avaliação das árvores de falhas é um dos pontos principais do processo, devido às incertezas e variações dos dados e modelos utilizados.

9.1 Fontes de Incertezas

O uso de valores de probabilidades já implica em incertezas inerentes, na avaliação da probabilidade de ocorrência do evento topo de uma árvore de falhas |44|. As outras fontes de erro do processo podem ser divididas em:

a) Incertezas dos modelos utilizados;

b) Incertezas dos dados utilizados.

9.1.1 Incertezas dos Modelos

Os modelos físicos associados com as árvores de falhas, ou mesmo as próprias árvores de falhas, podem não representar apropriamente o sistema que está sendo analisado. Um problema que estará sempre presente na análise da árvore de falhas é que não se pode garantir que ela foi completamente desenvolvida. É difícil estar-se certo de que todas as trajetórias que levam ao evento topo foram identificadas, ou, alternativamente, que alguns procedimentos conservativos foram adotados, tornando sem importância as possíveis omissões. Apesar da maioria das omissões ser de eventos com baixa probabilidade de ocorrência, esses valores podem ser significativamente aumentados pela existência das FMC.

As limitações específicas das árvores de falhas e que levam a incertezas são:

a) As árvores de falhas se baseiam na suposição binária de que um evento está num estado operacional ou não. Isto pode não ser verdade, como por exemplo no caso de uma válvula que pode estar em um dos três estados: operacional, falha aberta ou falha fechada. Têm sido feitas algumas tentativas de levar em conta este problema, mas não faz parte do escopo deste trabalho este tipo de análise |44|;

b) São enormes as incertezas envolvidas no tratamento quantitativo de falhas secundárias, por exemplo, falhas devidas a eventos externos. Em muitos estudos, como no Wash-1400 |48|, estes eventos não são levados em consideração na análise;

c) A árvore de falhas não é uma representação dinâmica de um sistema, mas sim uma ferramenta de análise combinatorial. Isto faz com que o uso das árvores de falhas para avaliar as características de confiabilidade de um sistema seja, numa certa extensão, aproximado;

d) Em grandes árvores de falhas, os códigos de computador nem sempre conseguem realizar uma análise completa, i.e., que envolva todos os cortes mínimos. Torna-se necessário então fazer uma restrição no número de cortes mínimos considerados (em tamanho ou importância), o que não é conservativo.

9.1.2 Incerteza dos Dados

Os dados utilizados são as probabilidades de ocorrência dos eventos básicos, ou os parâmetros de algum modelo físico que esteja sendo usado. São eles, os dados experimentais de importância direta na análise; os dados extraídos de áreas correlatas de interesse; e opiniões de especialistas. Em cada um destes casos, a teoria estatística é usada para a estimativa dos parâmetros e incertezas associadas. Isto, no entanto, leva a algumas limitações:

a) A estimativa dos dados não é independente dos modelos, o que leva a valores incertos. Por exemplo, na determinação da taxa de falhas de um componente reparável, devem ser feitas muitas suposições sobre a distribuição temporal das falhas e o tempo de reparo;

b) Não se pode garantir que o conjunto de dados utilizados é suficiente. Por exemplo, eles podem ser dependentes de outros fatores, que não foram levados em consideração;

c) A escolha do plano de amostragem para obter os dados pode afetar as estimativas.

9.2 Técnicas de Propagação das Incertezas

O uso de medidas de tendência central (média ou mediana) como dados de taxas de falhas para os eventos básicos de uma árvore de falhas, resulta num valor médio ou mediano de probabilidade para o evento topo. É necessário então ser determinada a distribuição de probabilidade de falha para o evento topo, conhecidas as distribuições para os eventos básicos, para se ter uma idéia da incerteza dos resultados.

São a seguir discutidas as técnicas de propagação das incertezas mais utilizadas.

9.2.1 Método dos Momentos

Dada uma árvore de falhas, o problema da avaliação das incertezas consiste em determinar a distribuição do evento topo, conhecidas as distribuições dos eventos básicos.

Embora não seja largamente utilizado, um dos métodos existentes para a propagação das incertezas é o Método dos Momentos. A

principal desvantagem deste método é que ele não é eficiente para tratamento de erros em árvores de falhas com grande número de eventos básicos.

Chamando de μ a média da variável aleatória $\underline{x}$ e de σ^2 a variância de $\underline{x}$, pode-se escrever:

$\mu = E(x)$, e

$\sigma^2 = E\ (x - \mu)^2$,

onde $E(x)$ e $E(x - \mu)^2$ representam a esperança matemática de $\underline{x}$ e $(x - \mu)^2$, respectivamente.

Utilizando as propriedades dos momentos |4|, pode-se demonstrar que:

a) Se $Y = X_1 + X_2$ então

$\mu_y = \mu_{x_1} + \mu_{x_2}$, e

$\sigma_y^2 = \sigma_{x_1}^2 + \sigma_{x_2}^2$;

b) Se $Y = X_1 \cdot X_2$ então

$\mu_y = \mu_{x_1} \cdot \mu_{x_2}$, e

$\sigma_y^2 = \sigma_{x_1}^2\ \sigma_{x_2}^2 + \mu_{x_1}^2\ \sigma_{x_2}^2 + \mu_{x_2}^2\ \sigma_{x_1}^2$.

Com as relações acima podem ser obtidas expressões para quaisquer combinações de eventos em árvores de falhas.

Este método deve ser utilizado apenas quando os eventos são independentes. Seja, por exemplo, calcular a indisponibilidade Q de um sistema constituído por 2 bombas paralelas e idênticas, com indisponibilidades individuais q e variância σ^2.

Pelo método dos momentos, obtém-se:

$Q = q \cdot q = q^2$, e

$\sigma_Q^2 = \sigma^2 \cdot \sigma^2 + Q^2\ \sigma^2 + q^2\ \sigma^2 = \sigma^4 + 2\ q^2\ \sigma^2$.

No entanto, sabendo que

$$E\ (x - \mu)^2 = \int_{-\infty}^{\infty} (x - \mu)^2\ p\ (x)\ dx,$$

pode-se escrever:

$$E\ (x - \mu)^2 = \int_{-\infty}^{\infty} x^2\ p(x)\ dx - 2\mu \int_{-\infty}^{\infty} x\ p(x)\ dx +$$

$$+ \mu^2 \int_{-\infty}^{\infty} p(x)\ dx$$

$$E\ (x - \mu)^2 = E(x^2) - 2\ [E(x)]^2 + [E(x)]^2$$

$$E\ (x - \mu)^2 = E(x^2) - [E(x)]^2$$

Logo, pela solução exata, deve-se escrever:

$\sigma^2 = Q - q^2$, ou

$Q = \sigma^2 + q^2$,

que é diferente do valor obtido inicialmente ($Q = q^2$).

9.2.2 Método da Integração Direta

Este método consiste fundamentalmente da combinação de distribuições de probabilidades discretas.

Sejam,por exemplo, duas distribuições X e Y cujos pares de valores discretos das probabilidades e das variáveis são (p_i, X_i) e

(q_j, Y_j), respectivamente. O método consistirá então da combinação ponto a ponto dos valores discretos de cada uma delas |38|:

Se $Z = X + Y$, então

$$Z = \{(p_i \cdot q_j), (X_i + Y_j)\}$$

Se $Z = X \cdot Y$, então

$$Z = \{(p_i \cdot q_j), (X_i \cdot Y_j)\}.$$

Na aplicação deste método a mais de duas distribuições, é obtido um número muito grande de pares após cada operação, aumentando bastante o tempo de cálculo mesmo em computadores. Para contornar este problema, uma técnica que pode ser usada na programação é a substituição de pontos por sua média, retornando na etapa seguinte ao mesmo número de pontos inicial.

Enquanto que o Método dos Momentos ajusta para o evento topo uma distribuição que tem uma média e uma variância determinadas, o Método da Integração Direta obtém diretamente uma distribuição para o evento topo, a partir das distribuições para os eventos básicos. Este método é, portanto, mais exato.

9.2.3 Método de Monte Carlo

É a técnica mais utilizada para a propagação das incertezas nas árvores de faltas. A técnica consiste em gerar, por amostragem aleatória das distribuições dos eventos básicos, valores de probabilidade que serão usados para calcular, através da expressão booleana correspondente, um valor pontual de probabilidade para o evento topo. O espalhamento dos valores obtidos dá a incerteza ou variabilidade associada com o resultado.

Este método é análogo à repetição de um experimento um grande

número de vezes, para a determinação do erro dos resultados experimentais. O Método de Monte Carlo pode ser empregado para uma variedade de distribuições e magnitude de erros. Para cada sistema, 1200 tentativas resultam numa precisão de cerca de 1% para a distribuição de probabilidade para o evento topo. A distribuição empírica obtida é caracterizada pela média, mediana e pelo intervalo de confiança (determinado pelos percentis). Para se utilizar os resultados obtidos para avaliações posteriores em outras árvores de falhas, a distribuição do evento topo deve ser ajustada a uma distribuição teórica.

Entre os programas de computador utilizados para se fazer a propagação das incertezas das árvores de falhas, os mais utilizados são o SAMPLE |48|, e o MOCARS |27|. O SAMPLE foi utilizado no Wash-1400 e será descrito mais detalhadamente no Apêndice C.

O Método de Monte Carlo, através de artifícios matemáticos introduzidos nos programas pode incorporar análise de falhas dependentes.

10 EXEMPLO DE APLICAÇÃO DA METODOLOGIA DA ÁRVORE DE FALHAS

Para aplicação da metodologia da árvore de falhas a um sistema já existente, foi escolhido o Circuito de Teste de Componentes - CTC, do CDTN, da NUCLEBRAS. Esta escolha se deu principalmente pelas seguintes razões:

a) O CTC é um sistema relativamente complexo, que envolve componentes elétricos, eletrônicos, mecânicos e de instrumentação, o que torna possível, através da análise de risco de um acidente particular, demonstrar muitas das potencialidades do método;

b) O CTC, por ser um projeto em desenvolvimento no CDTN, tem uma disponibilidade de informações detalhadas, no que diz respeito a diagramas lógicos, fluxogramas de instrumentação, descrição do sistema, memórias de cálculo, etc. Além disso, os contatos verbais com o pessoal envolvido nas diversas etapas do projeto em muito ajuda numa das fases mais importantes do processo, que é o entendimento do sistema;

c) O CTC é um circuito que operará sob condições de pressão, temperatura e vazão, tais que possibilitem testes de componentes de reatores nucleares. Logo, a aplicação da metodologia da árvore de falhas para este sistema dará uma idéia dos problemas envolvidos na análise probabilística de risco destes reatores;

d) A aplicação da metodologia pode fornecer alguns subsídios para a avaliação dos aspectos de segurança envolvidos no CTC, dos critérios de projeto e dos procedimentos de operação, teste e manutenção.

10.1 Descrição do Sistema

O CTC tem como finalidade básica a realização de testes de vál

vulas de centrais nucleares, sob condições similares às de operação. Seus constituintes básicos são os seguintes sistemas:

. Circuito primário;

. Sistema de pressurização;

. Sistema de alimentação;

. Circuito secundário.

Um fluxograma simplificado do circuito, mostrando a instrumentação importante do ponto de vista da segurança, é apresentado na Figura 10.1.

10.1.1 Circuito Principal

É um circuito fechado, com tubulações de aço carbono, que ligam as bombas principais às seções de teste.

As bombas principais denominadas de STC 20/21/22 AP001, podem funcionar individualmente, em série, ou em paralelo, dependendo das posições das válvulas STC 20/21 AA002. Para o circuito operando em série, a vazão máxima do circuito principal será 489 m^3/h e em paralelo será 1.467 m^3/h. O CTC foi projetado para uma temperatura mínima de 80°C, uma temperatura máxima de 218°C e uma pressão máxima de 120 bar.

As válvulas STC 21/22/23 AA001 protegem as bombas contra golpes de aríete, em caso de parada de uma delas (quando ligadas em série).

A seção de testes consiste de 6 derivações em paralelo, e entre seus flanges serão instaladas as válvulas a serem testadas.

A válvula de alívio STC 01 AA006, cuja pressão de abertura corresponde à pressão de projeto do circuito principal, protege o recalque das bombas principais contra golpe de aríete.

O trocador de calor tem a função de remover o calor gerado pelo circuito principal, em operação normal ou em condições de emergência. O calor gerado pelo circuito principal depende do número de bombas principais em funcionamento e do seu ponto de operação.

As válvulas de controle STC 50 AA003/005 e STC 51 AA001 fazem variar as vazões parciais que passam pelo trocador de calor e seu desvio ("by-pass"), permitindo o ajuste da taxa de remoção de calor.

As placas de orifício STC 50 BR001/002 têm a função de evitar grandes variações da pressão diferencial sobre o trocador de calor, por ocasião da mudança da configuração das bombas principais de série para paralelo e vice-versa. Em caso de parada de emergência das bombas principais, o resfriamento é assegurado pela convecção natural, entre o circuito principal e o trocador de calor principal, situado no nível mais alto da instalação.

A linha STC 71 alimenta o chuveiro do pressurizador, quando é necessário reduzir a pressão no circuito principal, para realizar testes a menores pressões, proceder à operação de parada, ou estabilizar a pressão durante transientes.

10.1.2 Sistema de Pressurização

O sistema de pressurização garante o NPSH ("Net Positive Suction Head"), requerido pelas bombas principais, absorve a contração, a expansão, ou os choques hidráulicos do circuito principal, além de auxiliar na operação de enchimento.

O pressurizador é um vaso de pressão com o chuveiro localizado na sua parte superior e as resistências elétricas com termopares para a sua proteção localizados na sua parte inferior. O pressurizador possui ainda as válvulas de segurança STC 81 AA 002/003/004, que estarão isoladas ou não do circuito, de acordo

com a configuração das bombas. Para uma bomba em operação, ou bombas em paralelo, a válvula STC 81 AA002 é que estará em condições de atuação; para 2 bombas em série será a válvula STC 81 AA 003; e para 3 bombas em série será a válvula STC 81 AA004.

A linha de alimentação e acomodação STC 30 estabelece a ligação entre o pressurizador e o circuito principal. Através dela e da linha STC 71 são efetuadas as correções no nível do pressurizador ou compensados os eventuais vazamentos do circuito principal.

10.1.3 Sistema de Alimentação

Este sistema é constituído basicamente pelo tanque de água fria (STC 73 BB001), o tanque de água quente (STC 70 BB001) e a bomba de deslocamento positivo (STC 71 AP001). Este sistema armazena água desmineralizada no tanque de água fria e, através do tanque de água quente e da bomba de deslocamento positivo, promove o enchimento do circuito, bem como compensa as fugas que aí ocorrem.

10.1.4 Circuito Secundário

Tem a função de remover o calor gerado no circuito principal, dissipando-o na atmosfera, através das torres de refrigeração. A água circula através das torres de refrigeração, pela ação combinada da gravidade e da sucção das bombas de circulação SAR 01/02 AP 001. Durante a operação, uma bomba estará operando e a outra de reserva.

10.1.5 Instrumentação

A instrumentação do CTC permite a operação automática durante

os testes e fornece ao operador informações sobre as diversas variáveis de processo, possibilitando, quando necessário, a adoção de procedimentos seguros. Durante todas as fases de operação, a instrumentação age no sentido de evitar que as variáveis ultrapassem os valores estipulados, através de alarmes, ou atuando sobre os componentes do circuito, assegurando a sua integridade.

O nível de água no pressurizador varia com a temperatura. É então necessário o seu controle, para que ele se mantenha constante num determinado ponto de operação. Este controle é feito automaticamente, ligando-se ou desligando-se a bomba STC 71 AP001, através do controlador indicador de nível LIC-30. Uma chave situada no painel de controle (PC) permite a operação manual desta bomba.

O controle de pressão é feito pelo controlador PIC-81, que atua continuamente sobre as resistências do pressurizador e sobre a válvula de chuveiramento STC 31 AA001, quando a pressão cai abaixo de um valor pré-determinado. A monitora de pressão PX-81B tem um ponto de alarme ajustado para a máxima pressão de operação e, quando atuada, impede o comando pelo PIC-81, desligando as resistências.

O controle de temperatura do circuito principal é feito regulando-se a vazão através do trocador de calor principal, por meio das duas válvulas de controle STC 50 AA003/005. Estas válvulas operam independentemente, através do controlador de temperatura TIC-01, e a comutação de uma para outra é feita pelas chaves limites ZSL-50 A/B e ZSH-50 A/B. O controlador TIC-01 possui um contato de valor limite, ajustado para a máxima temperatura de operação, que quando atuado desliga as bombas principais.

As resistências do pressurizador são protegidas contra emersão pelos termopares TE-30D e TE-30E. Os sinais de temperatura são comparados e o maior valor é levado à monitora TX-30D, que des

liga as resistências do pressurizador e as bombas principais, caso a temperatura atinja o valor limite.

A proteção contra vazão mínima no circuito secundário é feita pela chave de vazão FSL-101. Quando a vazão atinge valores inferiores a um mínimo estipulado, esta chave desliga a bomba que estava funcionando e liga a que estava de reserva. Se a vazão continua baixa, a chave de vazão desliga as bombas principais. É feita também a monitoração da temperatura na entrada das torres de refrigeração. Se a temperatura for maior que a máxima especificada, a monitora TX-124 aciona um alarme e envia um sinal para desligamento das bombas principais.

10.1.6 Sistema Elétrico

Os motores das 3 bombas principais, denominados GM13, GM14 e GM15 são alimentados pelo Centro de Controle de Motores de Média Tensão (CCM-MT), na tensão de 4.160 V, através do transformador TM01 de 2.000 kVA. Este transformador é protegido pelo disjuntor principal SA01, que pode ser atuado manualmente pelo operador, através do Botão de Emergência situado no Painel de Controle.

Os motores das 2 bombas do circuito secundário, denominados GM0 e GM02, são alimentados pelo Centro de Controle de Motores de Baixa Tensão (CCM-BT), na tensão de 480 V.

A alimentação da instrumentação e dos anunciadores de alarme é feita através do CCM-BT, através do quadro de alimentação do prédio ou através do gerador diesel de emergência, que deverá entrar em operação, quando houver interrupção no fornecimento de energia elétrica.

As resistências do pressurizador são alimentadas através dos conversores estáticos, que por sua vez são também alimentados

através do CCM-BT.

10.2 Escolha do Evento Topo

Foi escolhido para a análise, o evento topo "Pressão Excessiva no Circuito Principal", por se considerar que este seria o Máximo Acidente Crível para o Circuito de Testes de Componentes. Apesar de não estarem envolvidas substâncias radioativas, ou quaisquer outras substâncias tóxicas que pudessem ser liberadas por um acidente desta natureza, a água a alta pressão e temperatura, liberada por este evento postulado, vaporizar-se-ia imediatamente e poderia causar danos mecânicos consideráveis à instalação.

Admitiu-se que antes do acidente o circuito estaria operando com as 3 bombas do circuito primário em paralelo, por ser esta a configuração crítica, do ponto de vista de vazão, pressão e temperatura |41|.

Admitiu-se também que, sendo a energia elétrica a única fonte de calor do circuito, através das bombas e resistências, o desligamento do disjuntor principal SA01 estabilizaria qualquer transiente de temperatura (e conseqüentemente, de pressão). Nesta situação, o circuito seria refrigerado lentamente, pela convecção natural entre o trocador de calor principal e o circuito secundário.

Não foi considerado o acidente de falta de energia elétrica na instrumentação. Foi considerado que sempre que houvesse indisponibilidade de energia elétrica na instrumentação, isto também ocorreria para o circuito e o transiente estaria sob controle.

De acordo com os critérios de projeto do CTC |41|, somente as vazões inferiores a 10% da vazão de projeto do trocador de calor poderiam, teoricamente, levar a temperatura e pressão no

circuito principal a valores superiores aos de projeto. Por isto, não foram considerados, na análise, os eventos que não são capazes de reduzir suficientemente o valor da vazão, tais como, abertura demasiada das válvulas STC 51 AA001/002, ou entupimento dos filtros da linha do trocador de calor.

Considerou-se que a aspersão do pressurizador teria capacidade para estabilizar um transiente, onde as resistências do pressurizador não fossem desligadas automaticamente pelo circuito de controle.

Não foram considerados os problemas de partida do circuito, considerando-se que o CTC estava em funcionamento normal antes da ocorrência do transiente.

Não foram consideradas também as ocorrências de eventos tais como fogo, abalos sísmicos, inundação, queda de avião, e sabotagem, por se admitir que estes eventos têm probabilidades desprezíveis para a instalação em questão.

10.3 Construção da Árvore de Falhas

Definido o sistema, a próxima etapa da análise é a construção da árvore de falhas. É a etapa mais demorada do processo, pois envolve um conhecimento profundo de todos os sistemas relacionados com o evento topo, i.e., de todos os eventos que poderiam levar a uma pressão excessiva no circuito principal. Por pressão excessiva, entende-se como todos valores superiores às pressões de abertura das válvulas de segurança do pressurizador e de alívio do circuito principal. Portanto, para a ocorrência do evento topo, seria necessária a falha destas duas válvulas, quando ocorressse o aumento de pressão no circuito principal. Seguindo as regras mostradas no Capítulo 4 e discutindo as diversas etapas de construção das árvores de falhas com o pessoal envolvido no projeto do CTC, a árvore de falhas resultante foi

aquela mostrada na Figura 10.2. Às vezes, o objetivo final da análise é a própria árvore de falhas, para compreensão do comportamento do sistema e identificação de seus pontos fracos. No entanto, outras etapas ainda podem ser realizadas no processo de análise da árvore de falhas.

10.4 Avaliação Qualitativa da Árvore de Falhas

Como pode ser notado, a árvore de falhas para o evento "Pressão Excessiva no Circuito Principal do CTC", é relativamente complexa, envolvendo 266 eventos primários e 214 portas lógicas. Para uma árvore deste porte, é impossível uma análise qualitativa sem o auxílio de um computador digital para a obtenção dos cortes mínimos do sistema. Foram então implementados os códigos PREP e KITT |57| e uma descrição resumida dos mesmos, e dos dados de entrada utilizados para a análise, é dada nos Apêndices A e B, respectivamente.

Para apenas 700 tentativas do Método de Monte Carlo no código PREP, foram obtidos 319 cortes mínimos, sendo 51 de 5ª ordem, 143 de 6ª ordem, 59 de 7ª ordem, 22 de 8ª ordem, 12 de 9ª ordem, 5 de 10ª ordem, 5 de 11ª ordem, 20 de 12ª ordem e 2 de 13ª ordem.

A análise de todos estes modos de falha é uma tarefa das mais difíceis. No entanto, os cortes mínimos de ordem mais baixa são, normalmente, os modos de falha mais importantes de um sistema, a não ser que o sistema seja fortemente susceptível a Falhas de Modo Comum.

Uma lista dos 51 cortes mínimos de 5ª ordem obtidos é mostrada na Tabela 10.1 e uma descrição dos eventos primários envolvidos, classificados de acordo com o número de vezes que aparecem nos referidos cortes mínimos, é mostrada na Tabela 10.2.

Como pode ser notado, os eventos mais importantes do ponto de vista da segurança, são aqueles relacionados com:

. a atuação da válvula de segurança do pressurizador;

. a atuação da válvula de alívio do circuito principal;

. o desligamento das bombas principais;

. o desligamento das resistências do pressurizador;

. a atuação da aspersão do pressurizador;

. a abertura inadvertida das válvulas STC 20/21 AA002.

10.5 Avaliação Quantitativa da Árvore de Falhas

Foram utilizados para a avaliação quantitativa os códigos KITT1 e SAMPLE, que por sua vez utilizam os cortes mínimos obtidos pelo código PREP. Os dados de entrada para estes códigos são mostrados resumidamente nos Apêndices A, B e C.

Sem considerar os efeitos das falhas de modo comum, foi obtida uma probabilidade de ocorrência para o evento topo de aproximadamente $6,5 \times 10^{-6}$/ano, com um fator de erro de 20. Levando em consideração as falhas de modo comum entre componentes semelhantes (p.ex., entre as válvulas de alívio e segurança) e entre os eventos dependentes da atuação do operador, foi obtida, pela técnica da limitação (ver Capítulo 9), uma probabilidade de ocorrência de aproximadamente $4,4 \times 10^{-5}$/ano, com um fator de erro de 17.

As distribuições de probabilidade de ocorrência do evento topo, para os dois casos descritos acima, são mostradas nas Figuras 10.3 e 10.4.

11 CONCLUSÃO

Com a implementação dos códigos PREP, KITT1, KITT2 e SAMPLE no CDTN, torna-se disponível uma ferramenta poderosa para análise de confiabilidade de sistemas complexos. A análise da árvore de falhas, apesar de ser mais conhecida pelos seus resultados quantitativos, é mais útil para identificar, numa maneira sistemática e rigorosa, os modos de falha de um sistema. O grande problema da avaliação quantitativa é que não se pode garantir que os resultados são conservativos, principalmente devido à incerteza dos dados de entrada, à omissão de modos de falha desconhecidos e ao truncamento dos cortes mínimos de ordem mais alta.

A probabilidade de ocorrência do evento topo "Pressão Excessiva no Circuito Principal do CTC" de $4,4 \times 10^{-5}$/ano, obtida no exemplo de aplicação da metodologia, é inferior à meta de segurança de 1×10^{-4}/ano, estabelecida pela NRC para probabilidade de fusão do núcleo de um reator. Apesar do evento analisado não envolver a liberação de quaisquer substâncias radiológicas ou químicas para o ambiente, o baixo valor de probabilidade encontrado não deve ser visto como uma medida absoluta da segurança do sistema, pois na sua obtenção foram utilizados dados genéricos de taxas de falhas dos componentes e algumas simplificações sobre o funcionamento do sistema.

Os resultados da análise, incluindo a árvore de falhas, os cortes mínimos, a susceptibilidade a falhas comuns, e os próprios resultados quantitativos, poderão ser utilizados para reduzir ainda mais a probabilidade de ocorrência do evento topo, através de:

a) Auxílio na elaboração dos procedimentos de operação do circuito, adotando-se princípios que reduzam a chance de ocorrência dos modos de falhas identificados;

b) Auxílio na elaboração dos procedimentos de manutenção, teste

e reparo, adotando-se, por exemplo, separação no tempo e no espaço destas tarefas executadas em componentes de um mesmo corte mínimo;

c) Adoção de padrões redundantes de calibração de instrumentos, reduzindo as falhas de modo comum;

d) Consideração de fatores humanos na elaboração dos procedimentos de operação, manutenção, teste e reparo;

e) Registro de todas as falhas ocorridas não somente daquelas que exigiram reparo ou que tiveram efeito significativo na operação do circuito, mas também das falhas potenciais detectadas pela manutenção;

f) Registro do tempo de funcionamento dos componentes importantes do ponto de vista de segurança, com a finalidade de obter seus dados de taxas de falhas.

REFERÊNCIAS BIBLIOGRÁFICAS

|1| APOSTOLAKIS, G.E. et alii. CAT: a computer code for the automated construction of trees. Los Angeles, California Univ., 1978. 264 p. (EPRI-NP-705).

|2| ___.et alii. Data specialization for plant specific risk studies. Nuclear Engineering and Design, 56 (2): 321-9, 1980.

|3| ___.& CHU, T.L. The unavailability of systems under periodic test and maintenance. Nuclear Technology, 50 (1): 5-15, Aug. 1980.

|4| ___.& LEE, Y.T. Methods for the estimation of confidence bounds for the top-event unavailability of fault trees. Nuclear Engineering and Design, 41(3): 411-9, 1977.

|5| ASEABRÁS INDUSTRIAL LTDA. Centro de controle de motores do CTC+ITCA; diagramas elétricos. São Paulo, s.d.

|6| BIRKHOFER, A. The german risk study for nuclear power plants. IAEA Bulletin, 22 (5/6): 23-33, Oct. 1980.

|7| BORBA, Paulo Roberto. Cálculo das probabilidades de falha de suprimento de energia elétrica dos barramentos de classe IE da usina nuclear de Angra I. São Paulo, Instituto de Energia Atômica, 1978. 53 p. (IEA-DT-099).

|8| CALDAROLA, L. & WICKENHÄUSER, A. The Karlsruhe computer program for the evaluation of the availability and reliability of complex repairable systems. Nuclear Engineering and Design, 43(2): 463-70, Mar. 1977.

|9| CARLSON, D.D. & GALLUP, D.R. Interim reliability evaluation program procedures guide. Albuquerque, NM, Sandia National Labs., 1983. 151 p. (NUREG/CR-2728).

|10| DIXON, Wilfrid J. & MASSEY Jr., Frank J. Introduction to statistical analysis. 3. ed. Tokyo. McGraw-Hill Kogakusha, 1969. 638 p.

|11| DUMMER, G.W.A. & WINTON, R.C. An elementary guide to reliability. Oxford, Pergamon, 1968. 59 p.

|12| EASTERLING, R.G. Methods for statistical uncertainty analysis in PRA's. Albuquerque, NM, Sandia National Labs., 1983. 21 p. (SAND-82-2832C).

|13| ENGEMATIC. Diagrama de intertravamento - CTC+ITCA. São Paulo, 1982.

|14| ERNST, Malcolm L. Use of PRA and safety goals in nuclear power plant regulation. Nuclear Engineering and Design. 75(3): 453-62, June 1983.

|15| E.U.A. Code of Federal Regulations. Title 10. Energy. Part 50. Domestic licensing of production and utilization facilities. Washington, D.C., U.S. Government Printing Office, 1981. p. 342-448.

|16| FELICETTI, F. et alii. Safety analysis. Semiprobabilistic methodology and its applicative development. Roma, Comitato Nazionale Energia Nucleare, 1978. 66 p. (RT/DISP(78)10).

|17| FERNANDES FILHO, T.L. Análise de confiabilidade do sistema de refrigeração e recirculação do ar da contenção de Angra-1. Rio de Janeiro. Comissão Nacional de Energia Nuclear, 1982. 67 p. (CNEN-DR-113/82).

|18| FLEMING, K.N. et alii. On the analysis of dependent failures in risk assessment and reliability evaluation. Nuclear Safety, 24(5): 637-57, Sept./Oct. 1983.

|19| FUSSEL, J.B. Fault tree analysis - concepts and techniques. In: WAITE, H.H. ed. Pressure vessels and piping - design and analysis. New York, American Society of Mechanical Engineers, 1976. v. 4, p 417-31.

|20| ___.Synthetic tree model: a formal methodology for fault tree construction. Idaho Falls, Aerojet Nuclear Co., 1973. 118 p. (ANCR-1098).

|21| ___.& ARENDT, J.S. System reliability engineering methodology: a discussion of the state of the art. Nuclear Safety, 20 (5): 541-50, Sept./Oct. 1979.

|22| GARRICK, B.J. Unified systems safety analysis for nuclear power plants. Los Angeles, University of California, 1968. 318 p. Tese de Ph.D., University of California.

|23| ___.& GEKLER, W.C. Reliability analysis of engineered safeguards. Nuclear Safety, 8 (5): 470-9, Sept./Oct. 1967.

|24| GILBERT, C.P. Nuclear reactor safety - a review of the Rasmussen Report (Wash-1400). Atomic Energy in Australia, 22(2): 1-17, Apr. 1979.

|25| GRIFFIN, C.W. Fault tree as a safety optimization design tool. Canoga Park, Calif., Atomics International, 1973. 20 p. (CONF-730304-3).

|26| GRIFFON, M. A method for analysing incidents due to human errors on nuclear installations. Reliability Engineering. 1(2): 83-8, Oct. 1980.

|27| HAASL, David F. et alii. Fault tree handbook. Washington, D.C., Nuclear Regulatory Commission, 1981. (NUREG-0492).

|28| HAGEN, W.E. Common-mode/common-cause failure: a review. Annals of Nuclear Energy, 7(9): 509-17, 1980.

|29| HAUPTMANNS, Ulrich & YLLERA, Javier. Fault tree evaluation by Monte Carlo simulation. Chemical Engineering, 90(1): 91-7, Jan. 10, 1983.

|30| HEISING, Carolyn D. et alii. Common cause analysis: a review and extension of existing methods. Cambridge, Massachussetts Inst. of Tech., 1982. 372 p. (PB 83-166520).

|31| HICKMAN, J.W. PRA (Probabilistic Risk Assessments) Procedures guide: a guide to the performance of probabilistic risk assessments for nuclear power plants. LaGrange Park, IL., American Nuclear Society, 1983. v. 1. 488 p. (NUREG /CR-2300-V1).

|32| INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. IEEE guide for general principles of reliability analysis of nuclear power generating station protection systems. New York, 1975. 74 p. (IEEE std 352-1975).

|33| ___. IEEE guide to the collection and presentation of electrical, electronic and sensing component reliability data for nuclear-power generating stations. New York, 1977. 543 p. (IEEE std 500-1977).

|34| JOKSIMOVIC, V. & SOLOMON, K.A. Quantitative safety goals through more adequate risk management and risk assessment. Reliability Engineering, 4: 65-84, 1983.

|35| ___.& VESELY, W.E. Use of PRA in evaluating safety of nuclear power. Reliability Engineering, 1(1): 69 - 78, Sept. 1980.

|36| KARIMI, R. et alii. Qualitative and quantitative reliability analysis of safety systems. Cambridge, Massachusetts Institute of Technology, 1980. 288 p. (PB 81-118325).

|37| LELLOUCHE, G.S. Wash-1400: a comparison of experience and prediction. Nuclear Technology, 53(2): 231-33, May 1981.

|38| LLOYD, E. Probability. In: LEDERMANN, W. Handbook of applicable mathematics. New York, John Wiley & Sons, 1980. v. 2.

|39| MAYS, S.E. et alii. Interim reliability evaluation program: analysis of the Browns Ferry, unit 1, nuclear plant. Appendix B - system descriptions and fault trees. Idaho Falls, EG and G Idaho, 1982. 511 p. (NUREG/CR-2802 - App. B).

|40| ___. Appendice C - sequence quantification. Idaho Falls, EG and G Idaho, 1982. 101 p. (NUREG/CR-2802-App. C).

|41| NUCLEBRÁS. Centro de Desenvolvimento da Tecnologia Nuclear. Descrição dos sistemas do circuito de testes de componentes - CTC. 2ª rev. Belo Horizonte, s.d. (NUCLEBRÁS/CDTN-DETR.PD/DISCO.PD).

|42| ___. Diagramas lógicos do CTC. Belo Horizonte, s.d. (NUCLEBRÁS/CDTN-DETR.PD/DISCO.PD).

|43| ___. Fluxogramas de instrumentação do CTC. Belo Horizonte, s.d. (NUCLEBRÁS/CDTN-DETR.PD/DISCO.PD).

|44| PARRY, G.W. & WINTER, P.W. Characterization and evaluation of uncertainty in probabilistic risk analysis. Nuclear Safety, 22(1): 28-42, Jan./Feb. 1981.

|45| PILZ, V. Risk analysis for chemical production processes?- some remarks on meaningful application of available methods and limitations thereof. Angewandte systemanalyse, 2(4): 175-78, 1981.

|46| PRIJATEL, John. Failure analysis of ammonia plant shutdown instrumentation and control. Plant/Operations Progress, 3(1): 25-8, Jan. 1984.

|47| RASMUSON, D.M. et alii. COMCAN II-A: a computer program for automated commom cause failure analysis. Idaho Falls, Idaho National Engineering Lab., 1979. 84 p. (TREE-1361).

|48| RASMUSSEN, Norman C. Reactor safety study: an assessment of accident risks in U.S. commercial nuclear power plants. Washington, D.C., Nuclear Regulatory Commission, 1975. (WASH-1400, NUREG-75/014).

|49| SHAEIWITZ, Joseph A. et alii. Fault tree analysis of sequential systems. Ind. Eng. Chem., Process Des. Dev., 16(4): 529-45, 1977.

|50| SHARMA, D.D. & RAM, K.S. Fault tree analysis of CANDU shut -down system. Nuclear Engineering and Design, 61(2): 265 -76, Nov. 1980.

|51| SHERIDAN, Thomas B. Human error in nuclear power plants. Technology Review, 82(4): 22-33, Feb. 1980.

|52| SILADY, F.A. et alii. HTGR accident and risk assessment. San Diego, California, General Atomic Company, 1982. (GA-A16766).

|53| TAYLOR, J.R. A background to risk analysis. Roskilde, Risoe National Lab., 1979. 4 v. (INIS-mf-6341).

|54| TAYT-SOHN, Lauris C. & OLIVEIRA, Luis Fernando S. Análise da confiabilidade do sistema de água de serviço de Angra I. Rio de Janeiro, Universidade Federal do Rio de Janeiro, 1984. 88 p. (PEN-124).

|55| VASCONCELOS, Vanderley de. Riscos de acidentes em instalações nucleares - métodos de avaliação e análise. Belo Horizonte, Centro de Desenvolvimento da Tecnologia Nuclear, 1980. (Monografia, Curso de Especialização em Tecnologia Nuclear).

|56| VESELY, W.E. Time-dependent methodology for fault tree evaluation. Nuclear Engineering and Design, 13(2): 337-60, Aug..1970.

|57| ___. & NARUM, R.E. PREP and KITT: computer codes for the automatic evaluation of a fault tree. Idaho Falls, Idaho Nuclear Company, 1970. 188 p. (IN-1349).

|58| WADDINGTON, J.G. et alii. The fault tree as a tool in safety analysis in nuclear power plants. Ottawa, Canada Atomic Energy Control Board, 1981. 26 p. (INFO-0036).

|59| WELCH, Bruce L. Deception on nuclear power risks: a call for action. The Bulletin of the Atomic Scientists, 36 (7): 50-54, Sept. 1980.

|60| WILLIAMS, R.F. & LELLOUCHE, G.S. EPRI nuclear fuel-cycle accident risk assessment. Nuclear Safety, 22(3): 300-6, May/June 1981.

Tabela 6.1 - Exemplo da aplicação do método explícito na avaliação das falhas de modo comum |18|

PROBABILIDADE	Caso 1 s/causa comum s/falha de 1 único comp.	Caso 2 c/causa comum a A e B s/falha de 1 único componente	Caso 3 s/redundância s/causa comum	Caso 4 s/redundância c/causa comum a B e C
P(A')	1×10^{-3}	$9,9 \times 10^{-4}$	1	1
P(B')	1×10^{-3}	$9,9 \times 10^{-4}$	1×10^{-3}	5×10^{-4}
P(C')	0	0	1×10^{-3}	5×10^{-4}
P(D)	0	1×10^{-5}	0	0
P(E)	0	0	0	5×10^{-4}
Q	1×10^{-6}	$1,1 \times 10^{-5}$	2×10^{-3}	$1,5 \times 10^{-3}$

Tabela 6.2 - Exemplo da aplicação do método paramétrico na avaliação das falhas de modo comum

q_s	β	P_{FMC}	Q_s (s/FMC)	Q_s (c/FMC)	$\frac{Q_s \text{ (s/FMC)}}{Q_s \text{ (c/FMC)}}$
10^{-1}	0,1	10^{-2}	10^{-2}	$1,8 \times 10^{-2}$	0,56
10^{-2}	0,1	10^{-3}	10^{-4}	$1,1 \times 10^{-3}$	0,10
10^{-3}	0,1	10^{-4}	10^{-6}	$1,0 \times 10^{-4}$	0,01

Tabela 8.1 - Aplicação do teorema de Bayes à probabilidade de falha de geradores diesel em partir [2]

Taxa de Falhas (falha em partir)	Probabilidade "a priori"	Função de probabilidade	Prob."a priori" x função de probabil.	Probabilidade "a posteriori"
0,0087	0,0500	0,0343	0,0017	0,0206
0,0115	0,0587	0,0750	0,0044	0,0529
0,0154	0,0967	0,1320	0,0128	0,1535
0,0205	0,1350	0,1734	0,0234	0,2815
0,0274	0,1596	0,1544	0,0246	0,2963
0,0365	0,1596	0,0820	0,0131	0,1572
0,0487	0,1350	0,0218	0,0029	0,0353
0,0649	0,0967	0,0023	0,0002	0,0027
0,0866	0,0587	0,0001	0,0000	0,0000
0,1155	0,0500	0,0000	0,0000	0,0000
-	1,0000	-	0,0831	1,0000

Tabela 8.2 - Denominação de componentes mecânicos [48]

Acumulador	AC	Unidade de refrigeração	RF
Ventilador	BL	Porta de eclusa	SL
Unidade de acionamento das barras de controle	CD	Caldeira	SP
		Subárvore	ST
Placa de cobertura	FA	Tanque	TK
Amortecedor	DM	Turbina	TB
Diesel	DL	Válvula de retenção	CV
Junta de expansão	XJ	Válvula hidráulica	HU
Filtro	FL	Válvula manual	XV
Cilindro de gás	GB	Válvula a motor	MV
Gaxeta	GK	Válvula pneumática	AV
Trocador de calor	HE	Válvula de alívio	RV
Bocal	NZ	Válvula de segurança	SV
Orifício	OR	Válvula solenóide	KV
Tubulação	PP	Válvula de retenção de parada	DV
Revestimento de tubulação	CP		
Vaso de pressão	PV	Válvula de alívio a vácuo	VV
Bomba	DM	Alívio	VT
Barra de controle do reator	ED	Reservatório	WL

Tabela 8.3 - Denominação de componentes elétricos |48|

Amplificador	AM	Resistência para medição de temperatura	RT
Anunciador	AN		
Bateria	BY	Comparador de sinal	AD
Carregador de Bateria	BC	Chave de restabelecimento	RS
Barramento	BS	Chave de pressão	PS
Cabo	CA	Chave de torque	QS
Disjuntor	CB	Chave de temperatura	TS
Embreagem	CL	Quadro terminal	TM
Chave de Controle	CS	Diodo ou retificador	PE
Bobina	CO	Fusível	FU
Detector	DI	Gerador	GE
Fonte CC	DC	Traçador por aquecimento	HT
Chave de vazão	FS	Botão de teste	SB
Elemento de aquecimento	HG	Sobrecarga térmica	OL
Módulo de entrada	IM	Temporizador	TI
Inversor de estado sólido	IV	Transformador de corrente	CT
Chave de nível	ES	Transformador de Potencial (ou de controle)	OT
Lâmpada	LT		
Chave limite	LS	Transformador de Potência	TR
Chave manual	SW	Transmissor de vazão	TF
Motor	MO	Transmissor de nível	TL
Dispositivo de partida do motor	MS	Transmissor de pressão	TP
Detector de nêutrons	ND	Transmissor de temperatura	TT
Potenciômetro	PT	Fio	WR
Registrador	RC	Alarme	AL
Pára-raios	LA	Evento (quando não está envolvido nenhum componente)	OO
Chave de terra	GS		
Relé	RE		
Contato de uma chave ou de um relé	CN		

Tabela 8.4 - Denominação dos modos de falha [48]

Fechado	C
Desengatado	G
Não fecha	K
Não abre	D
Não parte	A
Engatado	E
Acima do limite	M
Vazamento	L
Perda de função	F
Falha na manutenção	Y
Falta de sinal de entrada	N
Aberto	O
Circuito aberto	B
Falha operacional	X
Sobrecarga	H
Obstruído	P
Ruptura	R
Curto-circuito	Q
Curto para terra	S
Falha de transferência	T

Tabela 10.1 - Cortes mínimos de 5ª ordem para a árvore de falhas do CTC

CORTE MÍNIMO	EVENTOS PRIMÁRIOS				
1	XVX03	SVY01	RVY01	ALX01	CND17
2	CND37	CBD01	XVX02	SVY01	RVY01
3	CND43	CBD01	XVX01	SVY01	RVY01
4	TPF01	SVY01	RVY01	ALX01	CND13
5	CND42	CBD01	XVX01	SVY01	RVY01
6	CND41	CBD01	XVX01	SVY01	RVY01
7	CND40	CBD01	XVX01	SVY01	RVY01
8	CND44	CBD01	XVX01	SVY01	RVY01
9	CND35	CBD01	XVX02	SVY01	RVY01
10	CND45	CBD01	XVX02	SVY01	RVD01
11	CND44	CBD01	XVX02	SVY01	RVY01
12	CND40	CBD01	XVX02	SVY01	RVD01
13	CND39	CBD01	XVX02	SVY01	RVY01
14	CND35	CBD01	XVX01	SVY01	RVY01
15	EPF01	SVY01	RVY01	ALX01	CND17
16	XVX03	SVY01	RVD01	ALX01	CND17
17	CND34	CBD01	XVX01	SVY01	RVY01
18	CND37	CBD01	XVX01	SVY01	RVY01
19	CND39	CBD01	XVX01	SVY01	RVY01
20	IPF02	SVY01	RVY01	ALX01	CND13
21	CND45	CBD01	XVX01	SVY01	RVY01
22	CND36	CBD01	XVX01	SVY01	RVY01
23	CND36	CBD01	XVX02	SVY01	RVY01
24	CND43	CBD01	XVX02	SVY01	RVY01
25	CBD01	XVX03	SVY01	RVY01	CND17
26	CND38	CBD01	XVX02	SVY01	RVY01
27	CND38	CBD01	XVX01	SVY01	RVY01
28	CND42	CBD01	XVX02	SVY01	RVY01
29	CND40	CBD01	XVX02	SVY01	RVY01
30	CND37	CND69	XVX02	SVY01	RVY01
31	CND37	CBD01	XVX02	SVY01	RVD01
32	CND41	CBD01	XVX02	SVY01	RVY01
33	EPF01	SVY01	RVY01	ALX01	CND13
34	CBD01	XVX02	SVY01	RVY01	CND75
35	CND45	CBD01	XVX01	SVY01	RVD01
36	CND45	CBD01	XVX02	SVY01	RVY01
37	CND43	CBD01	XVX02	SVY01	RVD01
38	CBD01	XVX02	SVY01	RVY01	CND72
39	CND34	CBD01	XVX02	SVY01	RVY01
40	CND40	CBD01	XVX02	SVD01	RVY01
41	CBD01	XVX01	SVY01	RVY01	CND75
42	EPF01	SVY01	RVD01	ALX01	CND13
43	CND44	CBD01	XVX02	SVD01	RVD01
44	CND43	CBD01	XVX01	SVY01	RVD01
45	CND38	CBD01	XVX02	SVY01	RVD01
46	CND34	CBD01	XVX01	SVY01	RVD01
47	TPF01	SVY01	RVD01	ALX01	CND13
48	CND38	CBD01	XVX02	SVD01	RVY01
49	CND36	CND69	XVX01	SVY01	RVY01
50	SVY01	RVY01	ALX01	AVD01	CND17
51	CND34	CBD01	XVX02	SVY01	RVD01

Tabela 10.2 - Descrição dos eventos primários envolvidos nos cortes mínimos de 5ª ordem para a árvore de falhas do CTC

ORDEM	EVENTO	DESCRIÇÃO
1	SVY01	Válvula de Segurança STC 81 AA002 com "setpoint" incorreto
2	CBD01	Não desligamento do disjuntor principal SA01
3	RVY01	Válvula de Alívio STC 01 AA006 com "setpoint" incorreto
4	XVX02	Abertura da válvula STC 21 AA002 pelo operador
5	XVX01	Abertura da válvula STC 20 AA002 pelo operador
6	RVD01	Válvula de alívio STC 01 AA006 emperrada
7	ALX01	Erro do operador em responder aos alarmes
8	CND17	Contadores das resistências do pressurizador falham em abrir
9	CND13	Contato da instrumentação não desliga as resistências do Pressurizador
10	CND37	Contato R147/249 falha em desligar bombas principais
11	CND43	Contato R129/266 falha em desligar bombas principais
12	CND40	Contato R148/260 falha em desligar bombas principais
13	CND45	Contato R156A/271 falha em desligar bombas principais
14	CND34	Contato R95/200 falha em desligar bombas principais
15	CND38	Contato R96/215 falha em desligar bombas principais
16	XVX03	Válvula STC 31 AA002 fechada inadvertidamente pelo operador
17	CND44	Contato R154/269 falha em desligar bombas principais
18	EPF01	Falha do sensor de pressão PE 81
19	CND36	Contato R140/248 falha em desligar bombas principais
20	SVD01	Válvula de alívio STC 01 AA006 emperrada
21	TPF01	Falha do transmissor de pressão PT 81
22	CND42	Contato R96/230 falha em desligar bombas principais
23	CND41	Contato R150/262 falha em desligar bombas principais
24	CND35	Contato R107/244 falha em desligar bombas principais
25	CND39	Contato R118/256 falha em desligar bombas principais
26	CND69	Botão de emergência da sala de controle não abre circuito
27	CND75	Contato 3ϕ do contator MC04 não desliga bomba principal
28	IPF02	Falha do controlador indicador de pressão PIC 81
29	CND72	Contato 3ϕ do contator MC02 não desliga bomba principal
30	AVD01	Válvula STC 31 AA001 falha fechada.

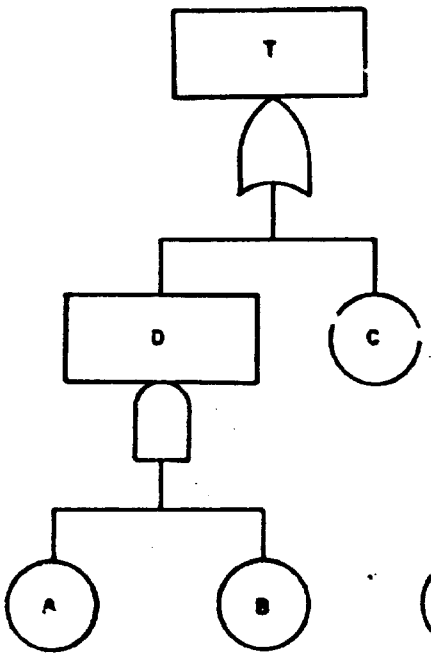


Fig. 4.1 - ÁRVORE DE FALHAS SIMPLIFICADA

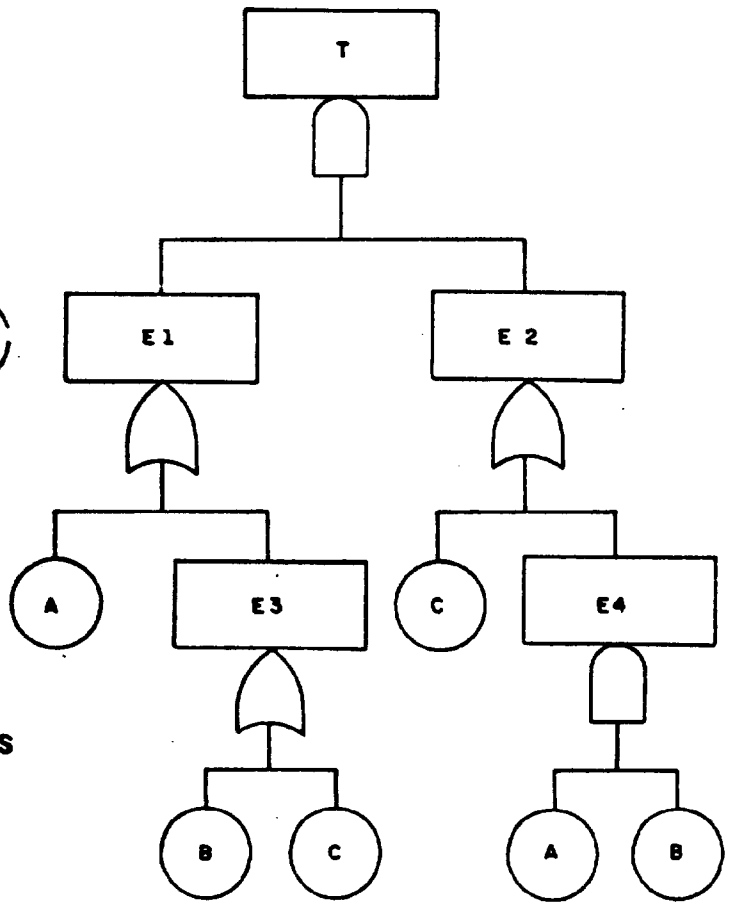


Fig. 5.1 - EXEMPLO DE ÁRVORE DE FALHAS P/ APLICAÇÃO DO ALGORÍTMO DE VESELY - FUSSEL

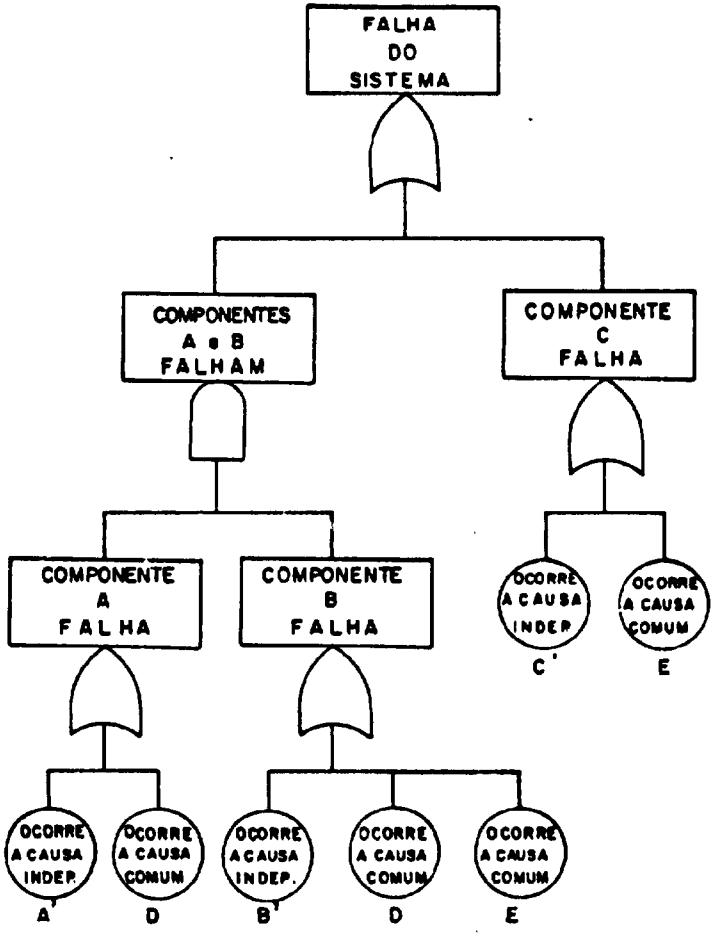


Fig. 6.1 - EXEMPLO DE ÁRVORE DE FALHAS P/ AVALIAÇÃO DE FALHAS DE MODO COMUM PELO MÉTODO EXPLÍCITO [18]

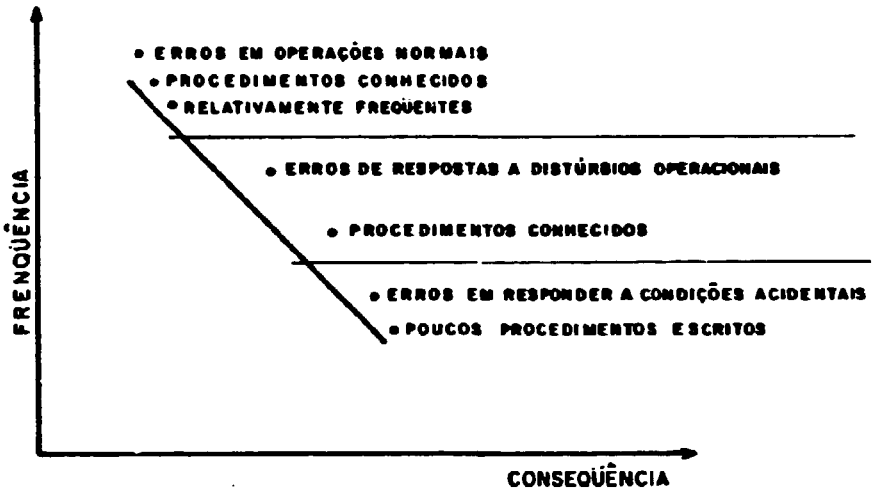


Fig. 7-1 - CLASSIFICAÇÃO DE ERROS DE ACORDO COM SUA FREQÜÊNCIA E CONSEQÜÊNCIA | 73 |

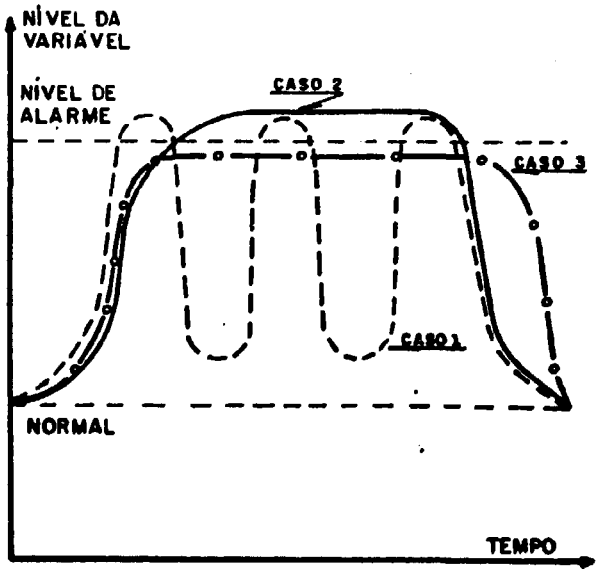


Fig. 7-2 - COMPARAÇÃO DE 3 CURVAS REPRESENTANDO MUDANÇAS HIPOTÉTICAS DE UMA VARIÁVEL DA INSTALAÇÃO, EM RELAÇÃO AO NÍVEL DE ALARME | 5a |

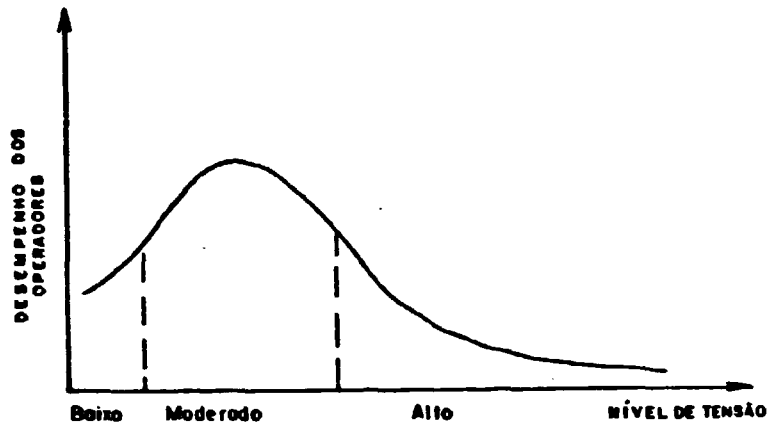


Fig.7.3 - DESEMPENHO DOS OPERADORES EM FUNÇÃO DO NÍVEL DE TENSÃO |53|

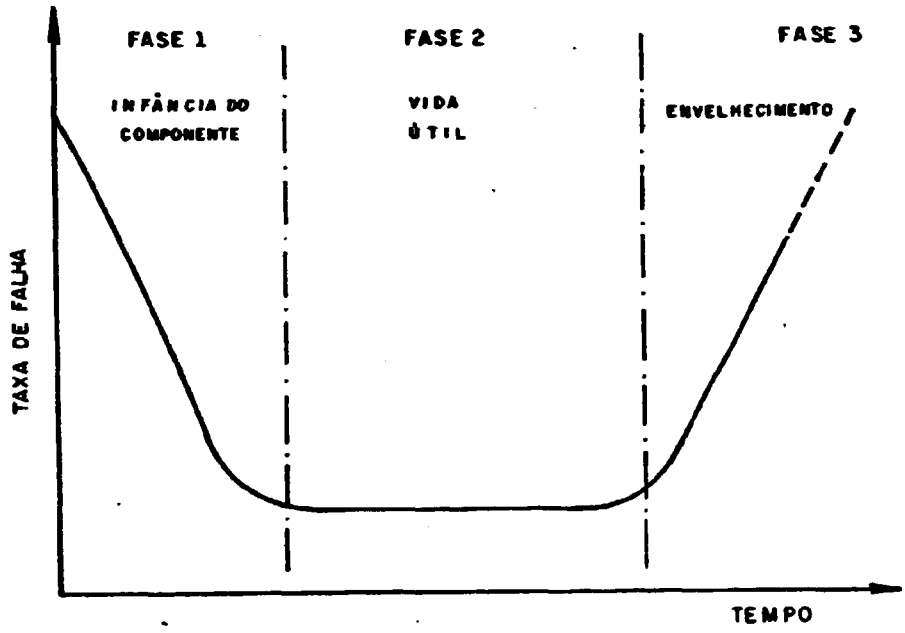


Fig. 8.1 - CARACTERÍSTICAS DA TAXA DE FALHAS |23|

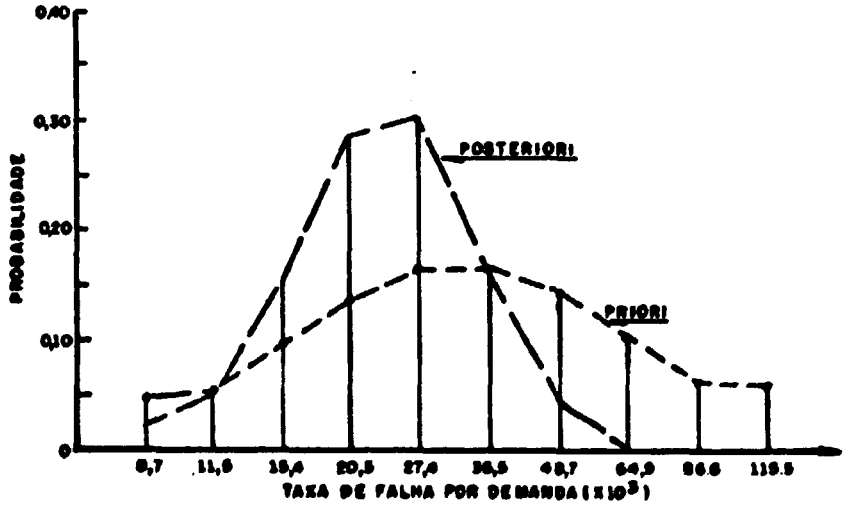


Fig.8.2 - HISTOGRAMAS "A PRIORI" E "A POSTERIORI" PARA FALHA DE PARTIDA DE GERADORES DIESEL |2|

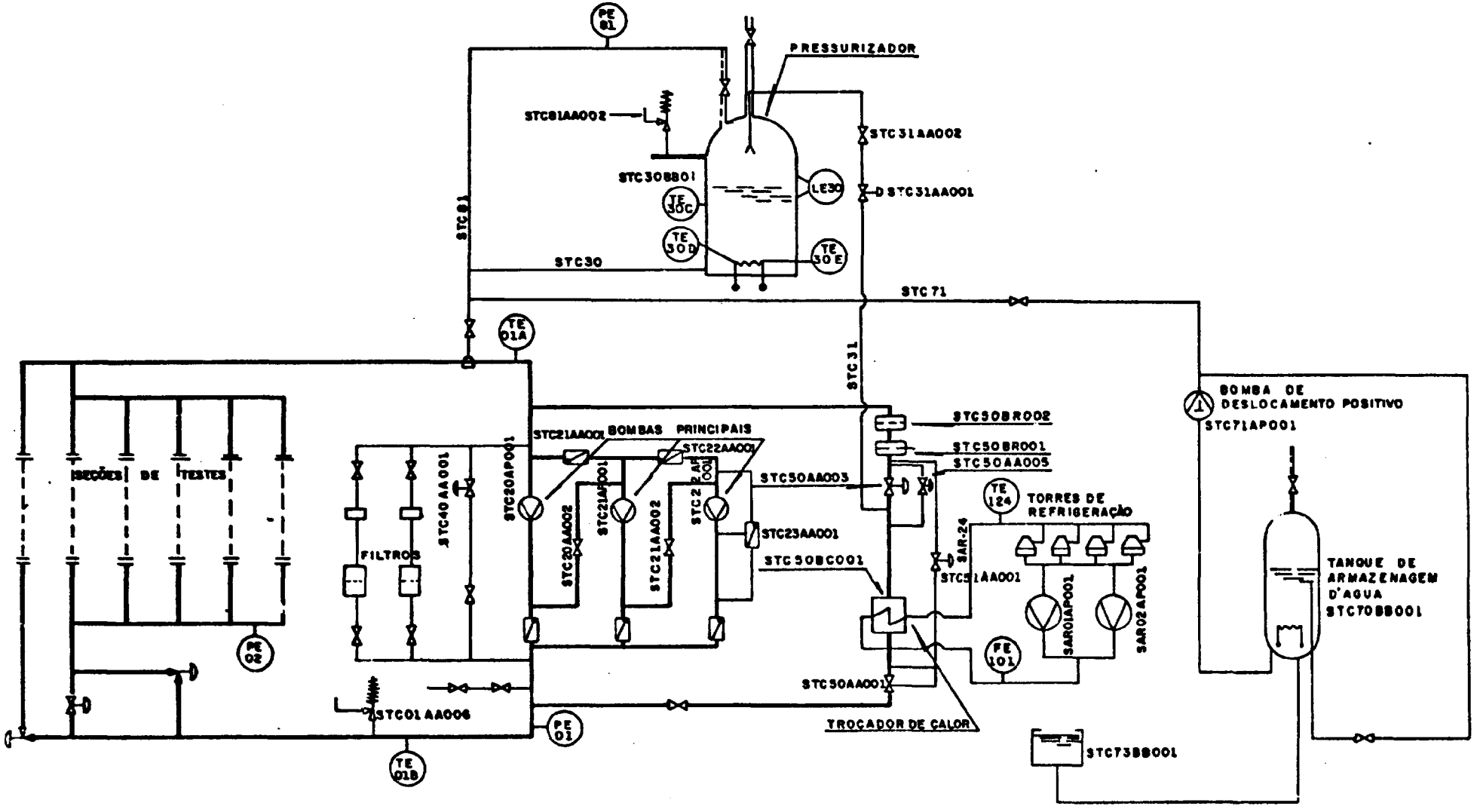
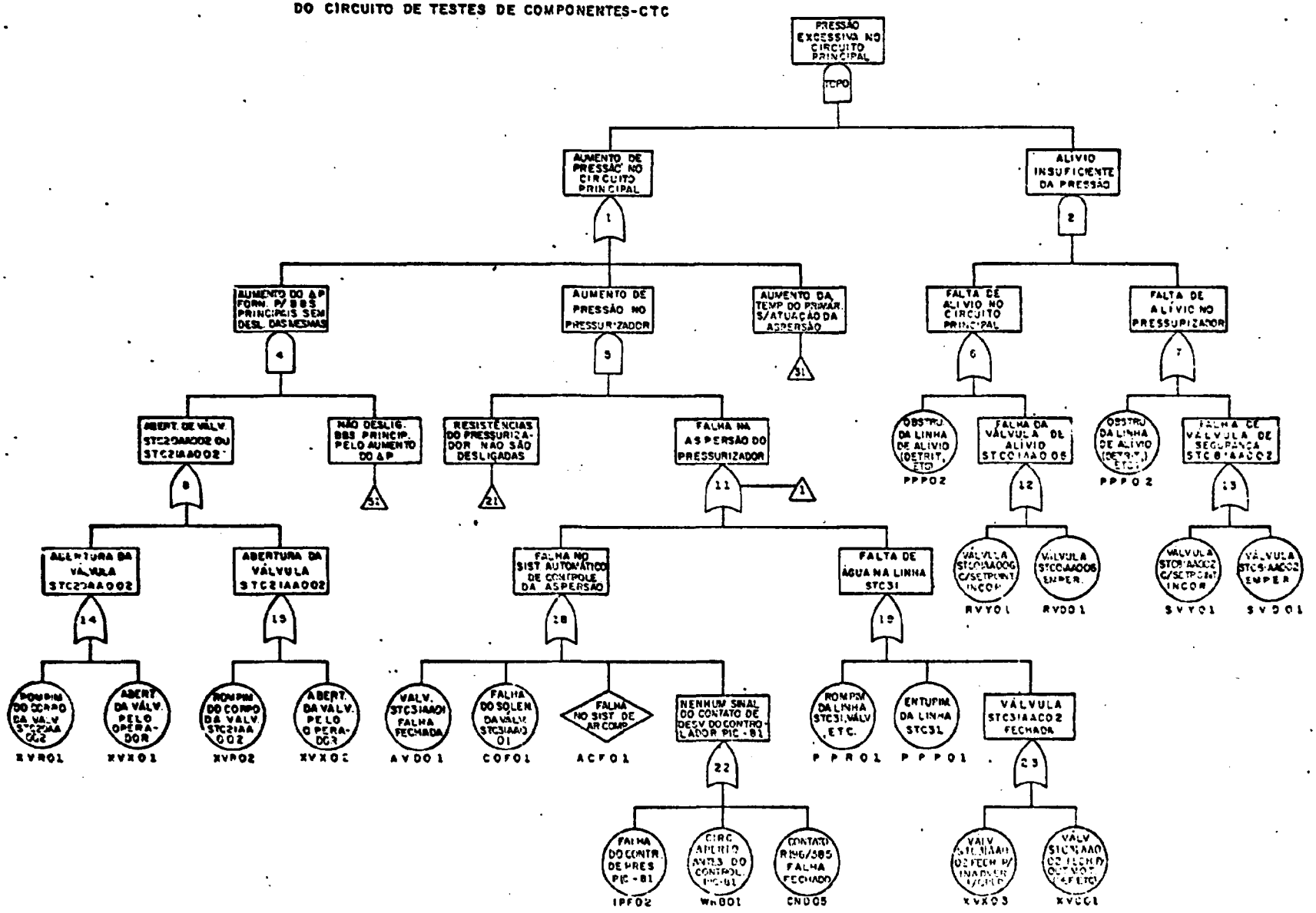
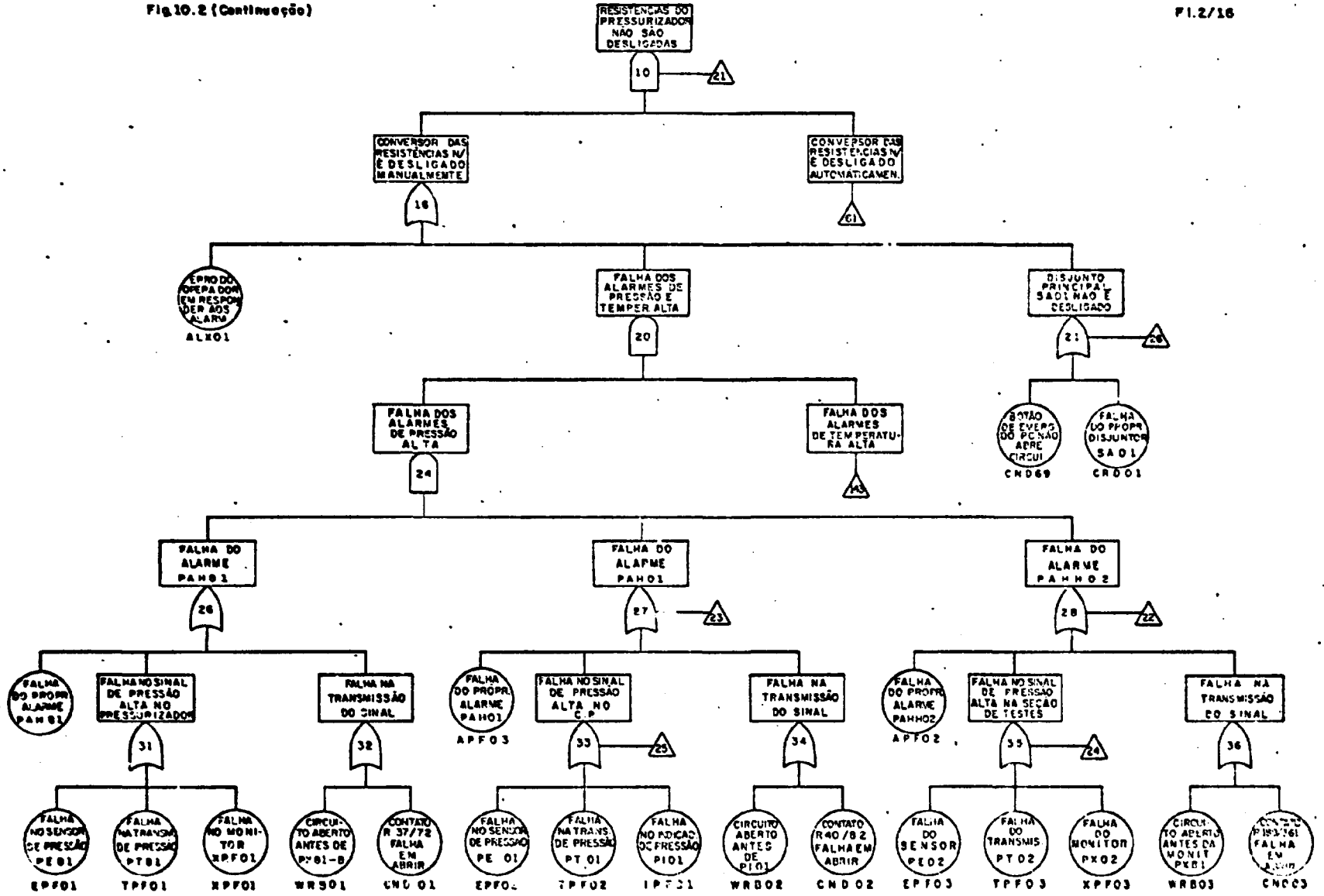


Fig. 10.1 - ASPECTOS DE INTERESSE DO CIRCUITO DE TESTE DE COMPONENTES - C T C |41,43|

Fig. 10.2 – ÁRVORE DE FALHAS PARA PRESSÃO EXCESSIVA NO CIRCUITO PRINCIPAL DO CIRCUITO DE TESTES DE COMPONENTES-CTC

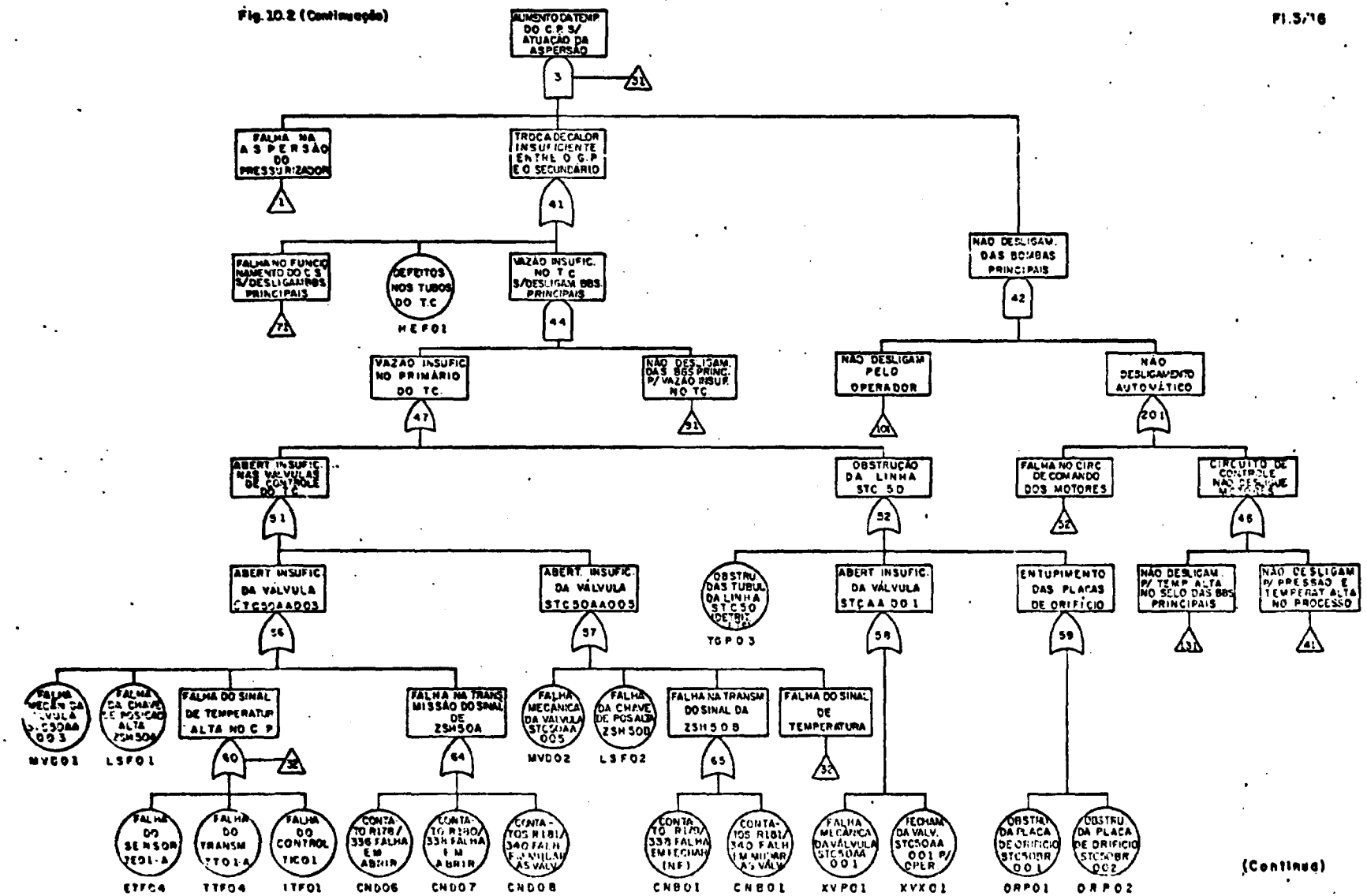


(Continua)


RESISTENCIAS DO PRESSURIZADOR NÃO SÃO DESLIGADAS
10
21
CONVERSOR DAS RESISTÊNCIAS N/ É DESLIGADO MANUALMENTE
16
CONVERSOR DAS RESISTÊNCIAS N/ É DESLIGADO AUTOMATICAMEN.
61
ERRO DO OPERADOR EM RESPONDER AOS ALARM
ALX01
FALHA DOS ALARMES DE PRESSÃO E TEMPER ALTA
20
DISJUNTO PRINCIPAL SA01 NÃO É DESLIGADO
2:
26
FALHA DOS ALARMES DE PRESSÃO ALTA
24
FALHA DOS ALARMES DE TEMPERATURA ALTA
25
BOTÃO DE EMERG DO PC NÃO ABRE CIRCUI
CND69
FALHA DO PROPR DISJUNTOR SA 01
CRD01
FALHA DO ALARME PAH01
26
FALHA DO ALARME PAH01
27
23
FALHA DO ALARME PAHH02
28
22
FALHA DO PROPR ALARME PAH01
FALHA NO SINAL DE PRESSÃO ALTA NO PRESSURIZADOR
31
FALHA NA TRANSMISSÃO DO SINAL
32
FALHA DO PROPR. ALARME PAH01
APF03
FALHA NO SINAL DE PRESSÃO ALTA NO C.P
33
25
FALHA NA TRANSMISSÃO DO SINAL
34
FALHA DO PROPR ALARME PAHH02
APF02
FALHA NO SINAL DE PRESSÃO ALTA NA SEÇÃO DE TESTES
35
24
FALHA NA TRANSMISSÃO DO SINAL
36
FALHA NO SENSOR DE PRESSÃO PE 01
EPF01
FALHA NA TRANSM DE PRESSÃO PT 01
TPF01
FALHA NO MONITOR XPF01
XPF01
CIRCUITO ABERTO ANTES DE PY 01-B
WRB01
CONTATO R 37/72 FALHA EM ABRIR
CND 01
FALHA NO SENSOR DE PRESSÃO PE 01
EPF02
FALHA NA TRANS DE PRESSÃO PT 01
TPF02
FALHA NO INDICAD DE PRESSÃO PI01
IPF01
CIRCUITO ABERTO ANTES DE PI01
WRB02
CONTATO R40 /82 FALHA EM ABRIR
CND 02
FALHA DO SENSOR PE02
EPF03
FALHA DO TRANSMIS PT02
TPF03
FALHA DO MONITOR PX02
XPF03
CIRCUITO ABERTO ANTES DA MONIT PXB1
WRB03
CONTATO P193/761 FALHA EM ABRIR
CND03

(Continua)

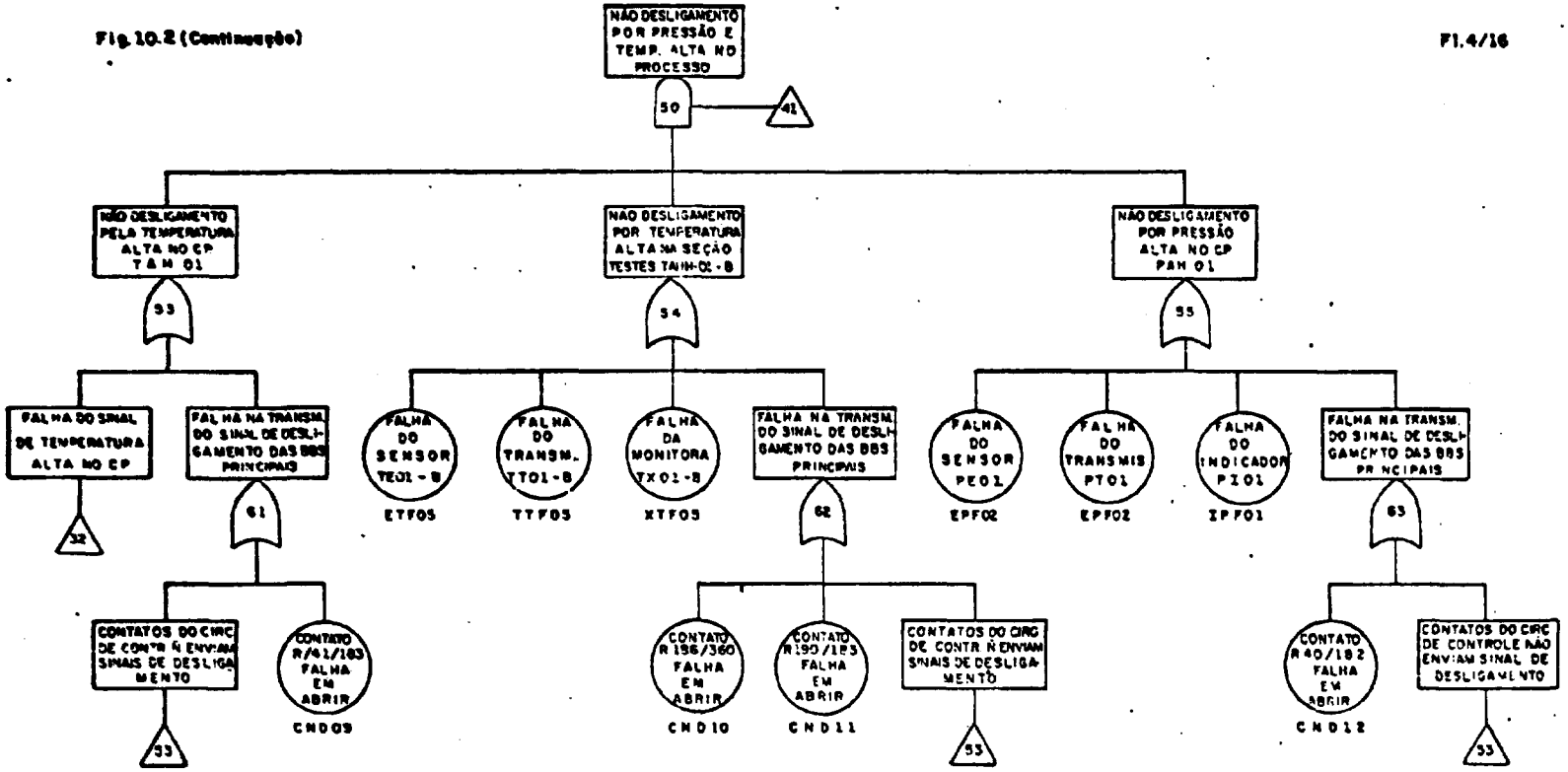
Fig. 10.2 (Continuação)



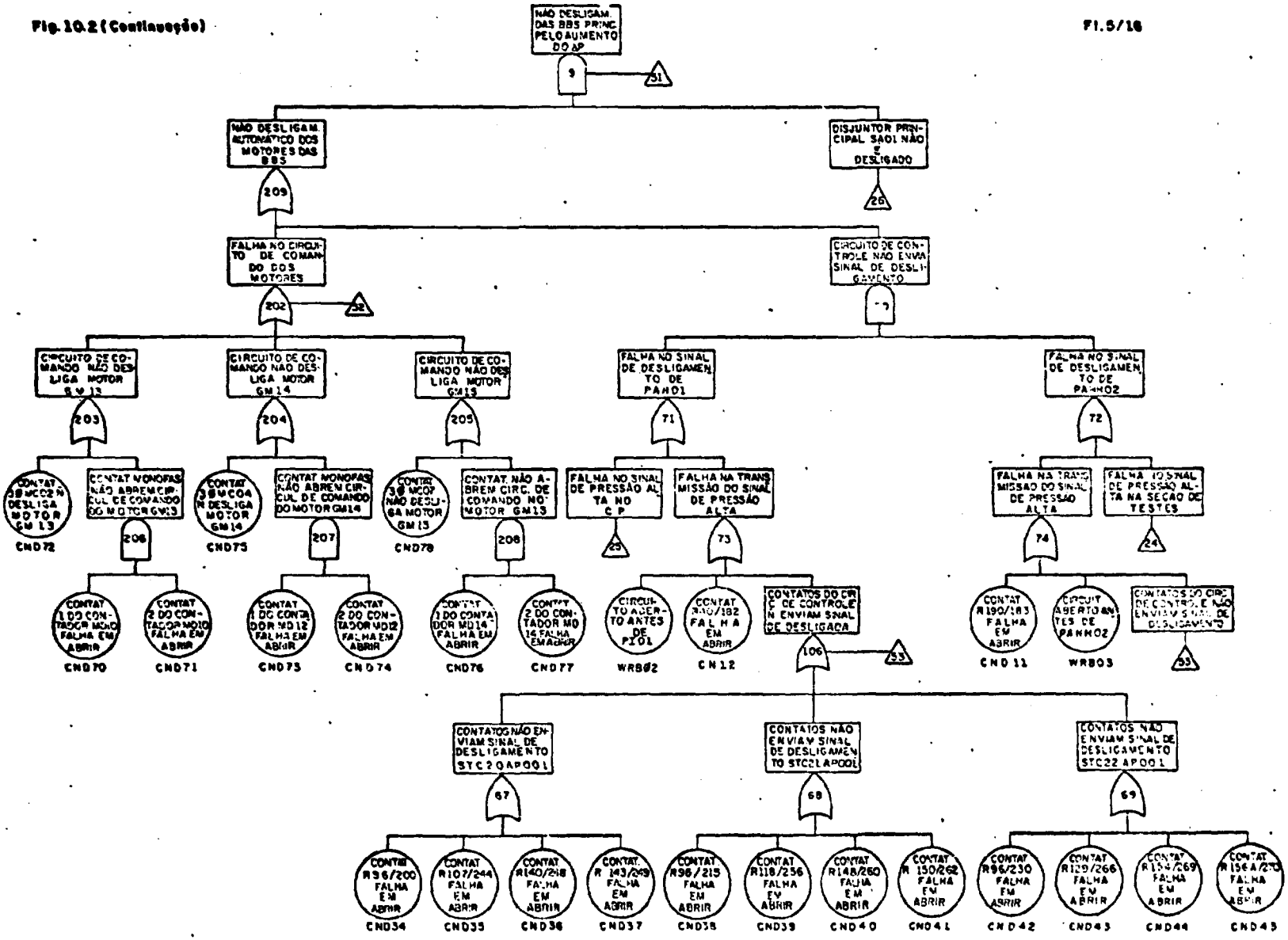
Fl. 5/16

(Continua)

Fig. 10.2 (Continuação)

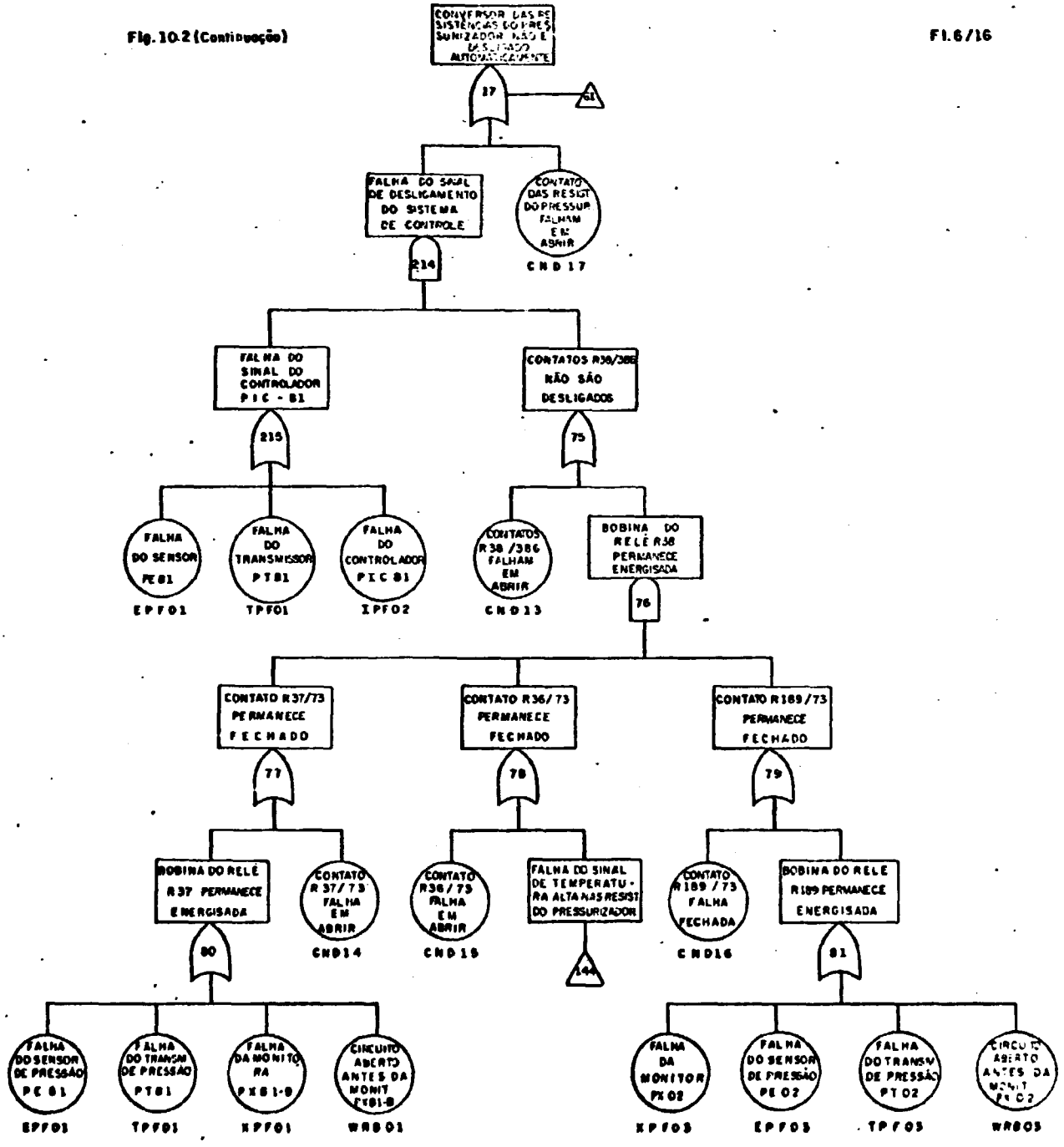


(Continua)


NÃO DESLIGAM. DAS BBS PRINC. PELO AUMENTO DO AP
9
51
NÃO DESLIGAM. AUTOMÁTICO DOS MOTORES DAS BBS
DISJUNTOR PRINCIPAL SAOI NÃO É DESLIGADO
209
26
FALHA NO CIRCUITO DE COMANDO DOS MOTORES
CIRCUITO DE CONTROLE NÃO ENVIA SINAL DE DESLIGAMENTO
202
32
7
CIRCUITO DE COMANDO NÃO DESLIGA MOTOR GM 13
CIRCUITO DE COMANDO NÃO DESLIGA MOTOR GM 14
CIRCUITO DE COMANDO NÃO DESLIGA MOTOR GM 15
FALHA NO SINAL DE DESLIGAMENTO DE PAH01
FALHA NO SINAL DE DESLIGAMENTO DE PAH02
203
204
205
71
72
CONTAT 3ª MCO2 N DESLIGA MOTOR GM 13
CONTAT MONOFAS NÃO ABREM CIRCUL DE COMANDO DO MOTOR GM13
CONTAT 3ª MCO4 N DESLIGA MOTOR GM14
CONTAT MONOFAS NÃO ABREM CIRCUL DE COMANDO DO MOTOR GM14
CONTAT 3ª MCO7 NÃO DESLIGA MOTOR GM 15
CONTAT NÃO ABREM CIRC. DE COMANDO NO MOTOR GM13
FALHA NO SINAL DE PRESSÃO ALTA NO C P
FALHA NA TRANSMISSÃO DO SINAL DE PRESSÃO ALTA
FALHA NA TRANSMISSÃO DO SINAL DE PRESSÃO ALTA
FALHA NO SINAL DE PRESSÃO ALTA NA SEÇÃO DE TESTES
206
207
208
25
73
74
24
CONTAT 1 DO CONTADOR MD0 FALHA EM ABRIR
CONTAT 2 DO CONTADOR MD0 FALHA EM ABRIR
CONTAT 1 DO CONTADOR MD12 FALHA EM ABRIR
CONTAT 2 DO CONTADOR MD12 FALHA EM ABRIR
CONTAT 1 DO CONTADOR MD14 FALHA EM ABRIR
CONTAT 2 DO CONTADOR MD 14 FALHA EM ABRIR
CIRCUITO ABERTO ANTES DE PI01
CONTAT R40/182 FALHA EM ABRIR
CONTATOS DO CIRC DE CONTROLE N ENVIAM SINAL DE DESLIGADA
CONTAT R190/183 FALHA EM ABRIR
CIRCUIT ABERTO ANTES DE PAHM02
CONTATOS DO CIRC DE CONTROLE NÃO ENVIAM SINAL DE DESLIGAMENTO
CND70
CND71
CND73
CND74
CND76
CND77
WRB02
CN12
CND11
WRB03
106
53
93
CONTATOS NÃO ENVIAM SINAL DE DESLIGAMENTO STC20AP001
CONTATOS NÃO ENVIAM SINAL DE DESLIGAMENTO STC21AP001
CONTATOS NÃO ENVIAM SINAL DE DESLIGAMENTO STC22AP001
67
68
69
CONTAT R96/200 FALHA EM ABRIR
CONTAT R107/244 FALHA EM ABRIR
CONTAT R140/248 FALHA EM ABRIR
CONTAT R 143/269 FALHA EM ABRIR
CONTAT R96/215 FALHA EM ABRIR
CONTAT R118/256 FALHA EM ABRIR
CONTAT R148/260 FALHA EM ABRIR
CONTAT R 150/262 FALHA EM ABRIR
CONTAT R96/230 FALHA EM ABRIR
CONTAT R129/266 FALHA EM ABRIR
CONTAT R154/269 FALHA EM ABRIR
CONTAT R156A/270 FALHA EM ABRIR
CND34
CND35
CND36
CND37
CND38
CND39
CND40
CND41
CND42
CND43
CND44
CND45

(Continua)

Fig. 10.2 (Continuação)

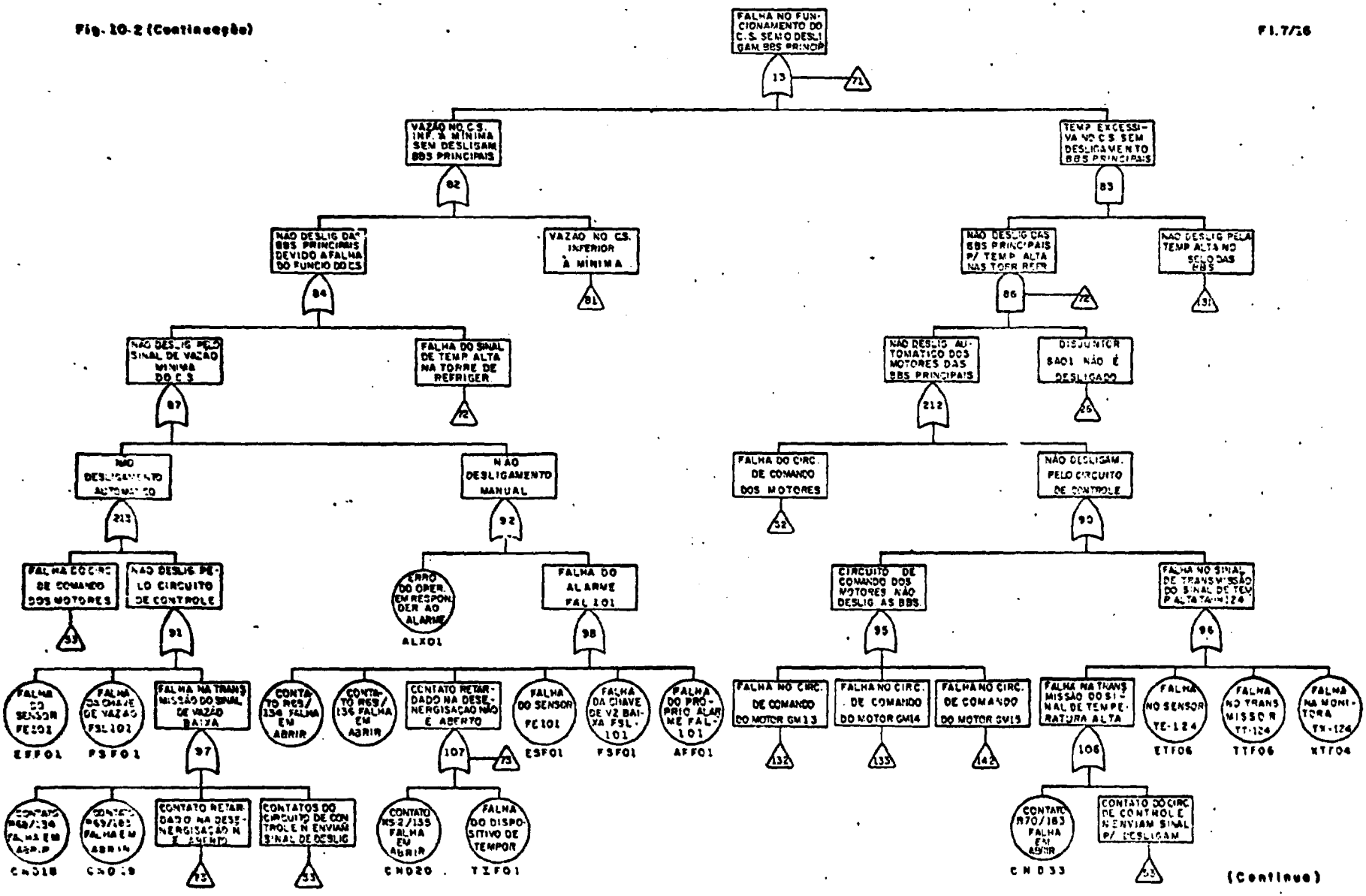


Fl. 6/16

(Continua)

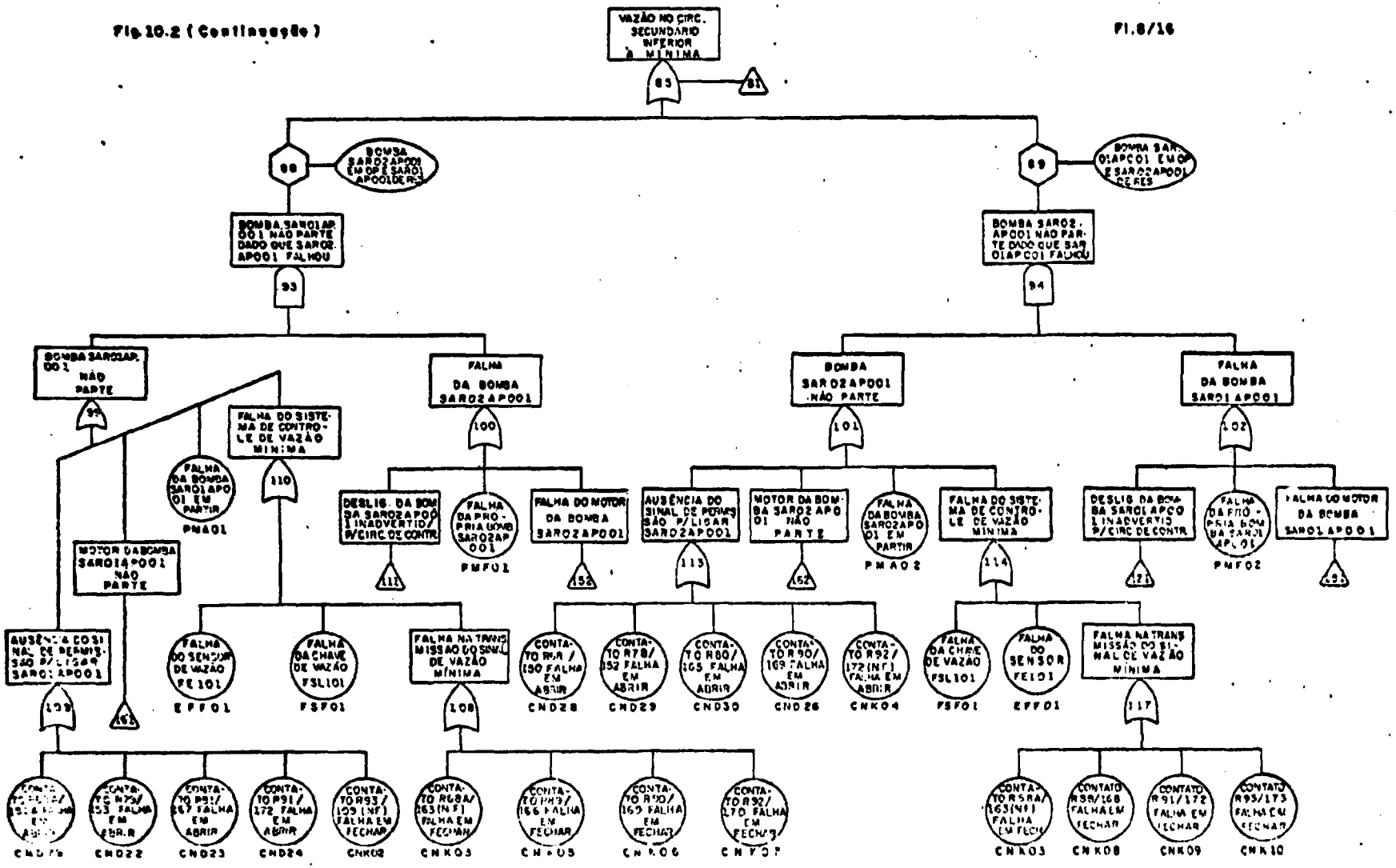
Fig. 10-2 (Continuação)

FT.7/16

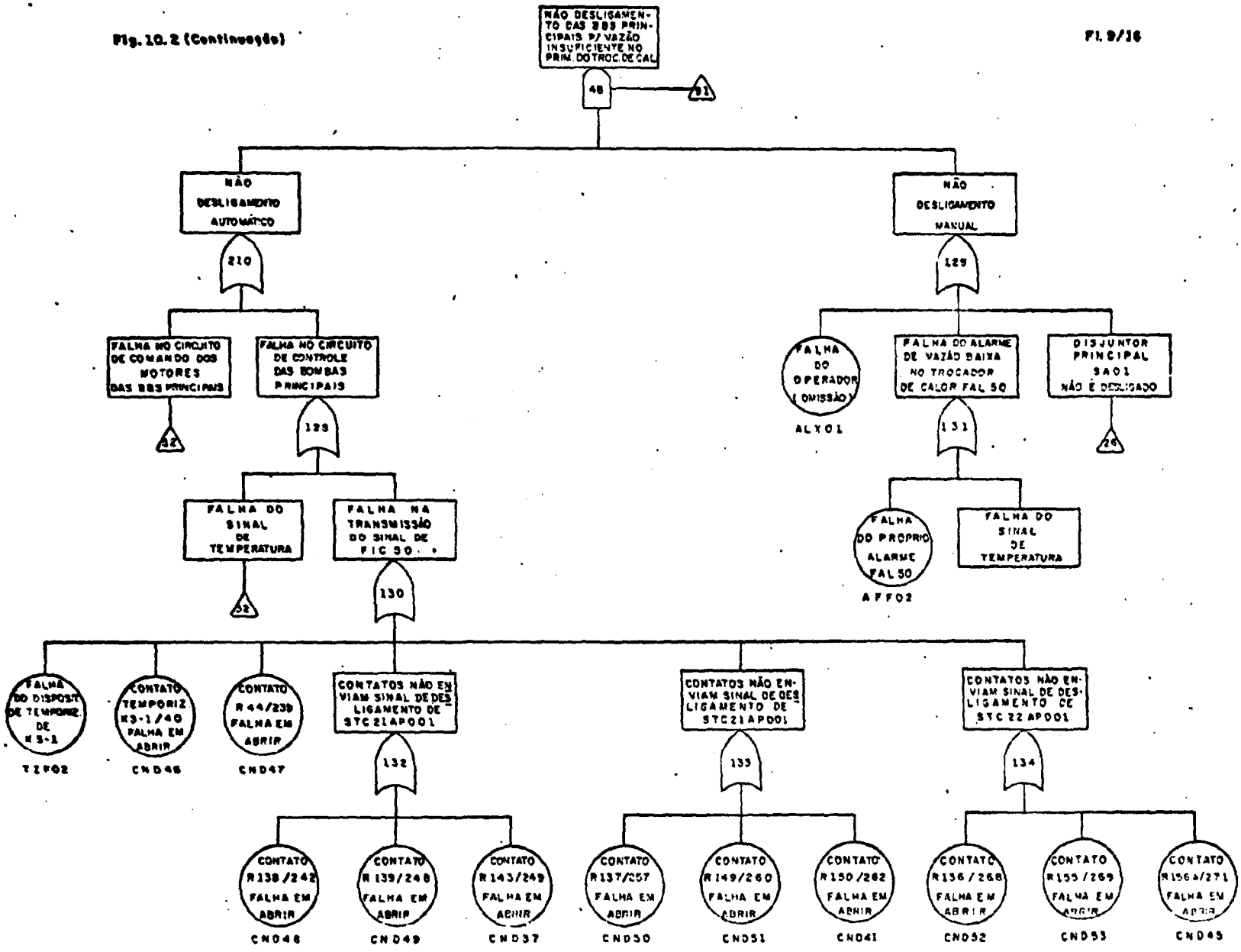


(Continua)

Fig.10.2 (Continuação)

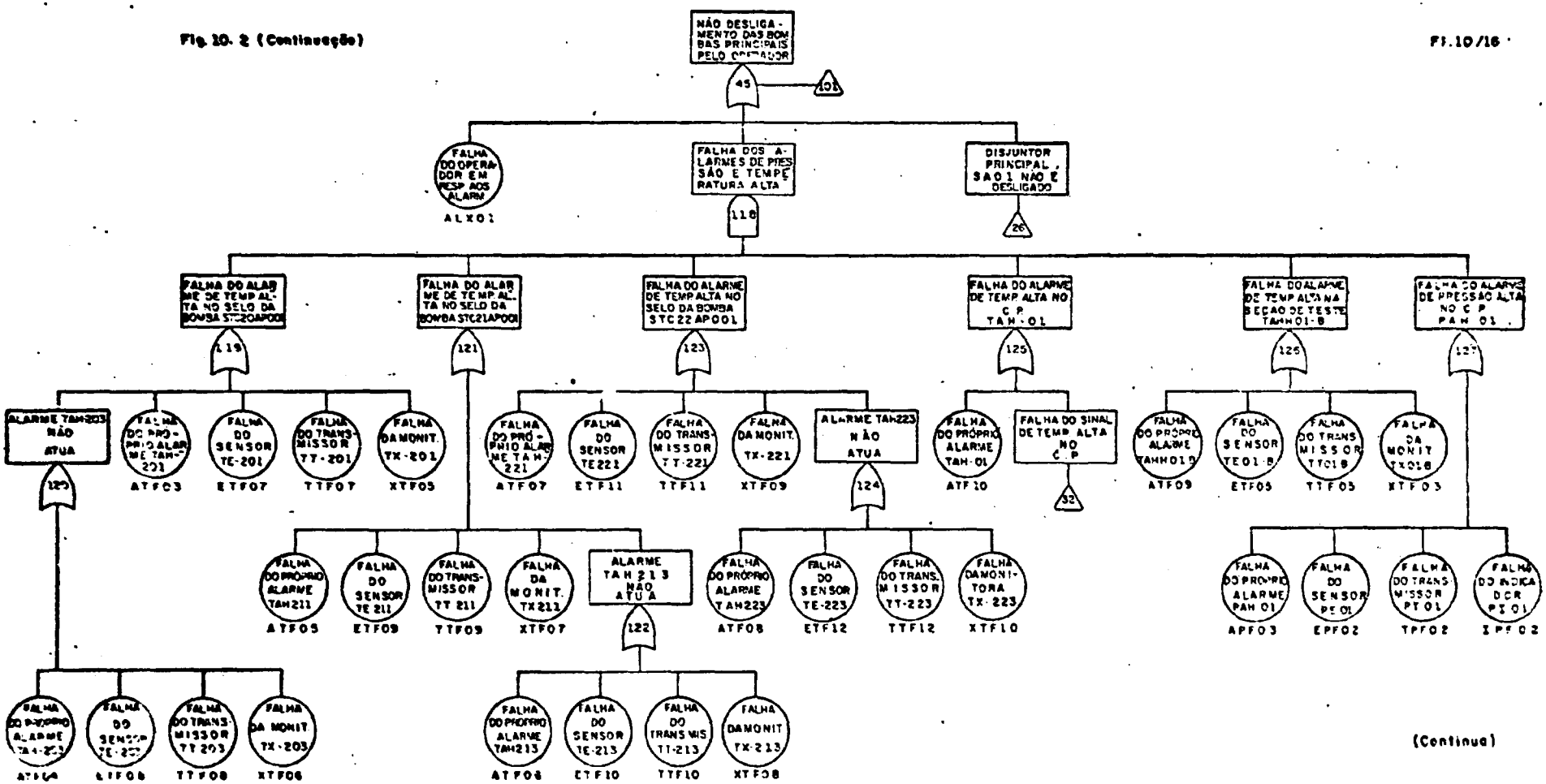


(Continua)


NÃO DESLIGAMENTO DAS BBS PRINCIPAIS P/ VAZÃO INSUFICIENTE NO PRIM. DO TROC. DE CAL
48
91
NÃO DESLIGAMENTO AUTOMÁTICO
210
FALHA NO CIRCUITO DE COMANDO DOS MOTORES DAS BBS PRINCIPAIS
92
FALHA NO CIRCUITO DE CONTROLE DAS BOMBAS PRINCIPAIS
129
FALHA DO SINAL DE TEMPERATURA
52
FALHA NA TRANSMISSÃO DO SINAL DE FIC 90
130
NÃO DESLIGAMENTO MANUAL
129
FALHA DO OPERADOR (OMISSÃO)
ALX01
FALHA DO ALARME DE VAZÃO BAIXA NO TROCADOR DE CALOR FAL 50
131
DISJUNTOR PRINCIPAL SA01 NÃO É DESLIGADO
26
FALHA DO PRÓPRIO ALARME FAL 50
AFF02
FALHA DO SINAL DE TEMPERATURA
FALHA DO DISPOSITIVO DE TEMPORIZAÇÃO DE K3-1
TIF02
CONTATO TEMPORIZ K3-1/40 FALHA EM ABRIR
CND46
CONTATO R44/239 FALHA EM ABRIR
CND47
CONTATOS NÃO ENVIAM SINAL DE DESLIGAMENTO DE STC21AP001
132
CONTATOS NÃO ENVIAM SINAL DE DESLIGAMENTO DE STC21AP001
133
CONTATOS NÃO ENVIAM SINAL DE DESLIGAMENTO DE STC22AP001
134
CONTATO R138/242 FALHA EM ABRIR
CND48
CONTATO R139/248 FALHA EM ABRIR
CND49
CONTATO R143/249 FALHA EM ABRIR
CND37
CONTATO R137/257 FALHA EM ABRIR
CND50
CONTATO R149/260 FALHA EM ABRIR
CND51
CONTATO R150/262 FALHA EM ABRIR
CND41
CONTATO R136/268 FALHA EM ABRIR
CND52
CONTATO R155/269 FALHA EM ABRIR
CND53
CONTATO R156a/271 FALHA EM ABRIR
CND45

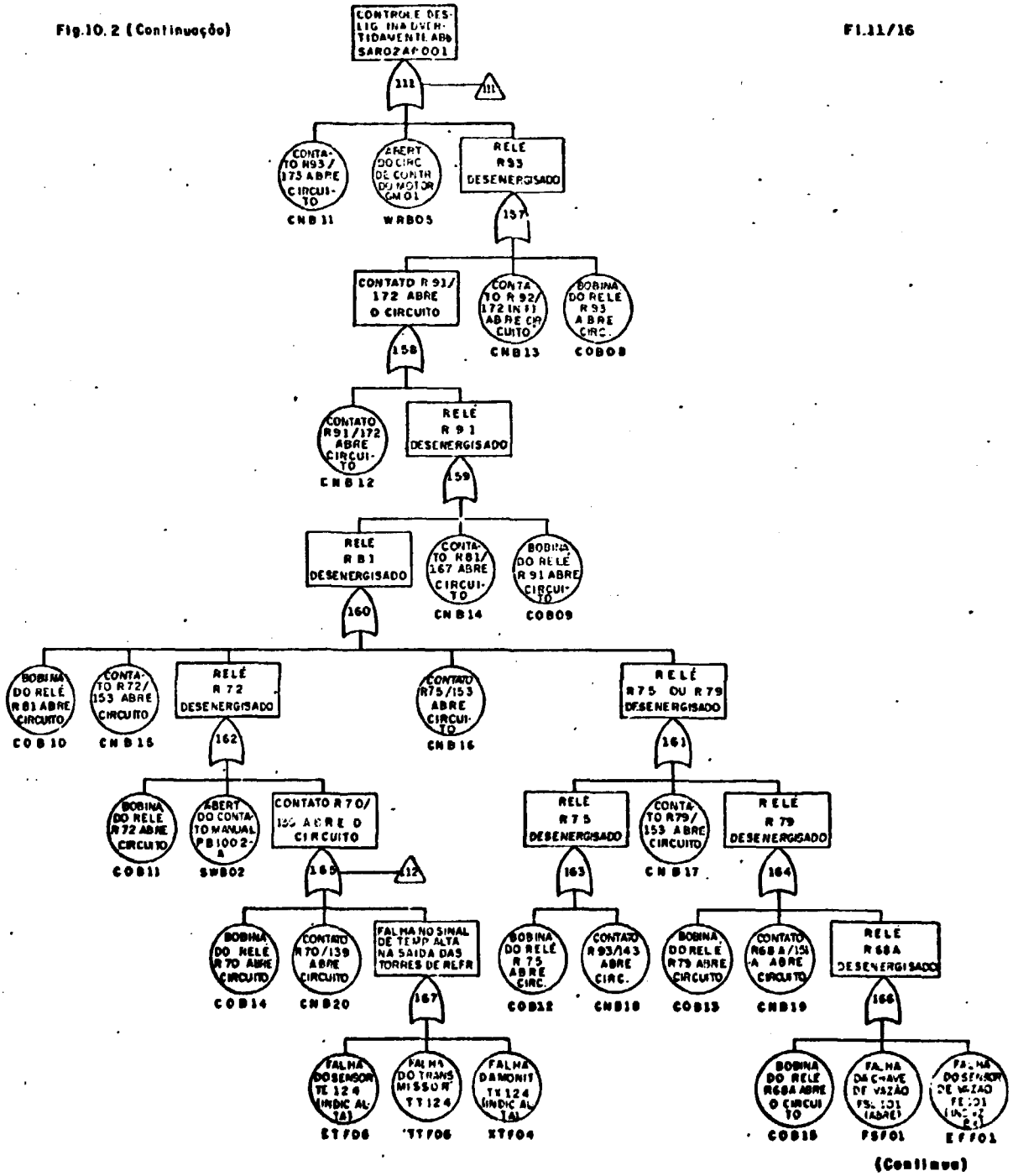
(Continua)

Fig. 10. 2 (Continuação)



(Continua)

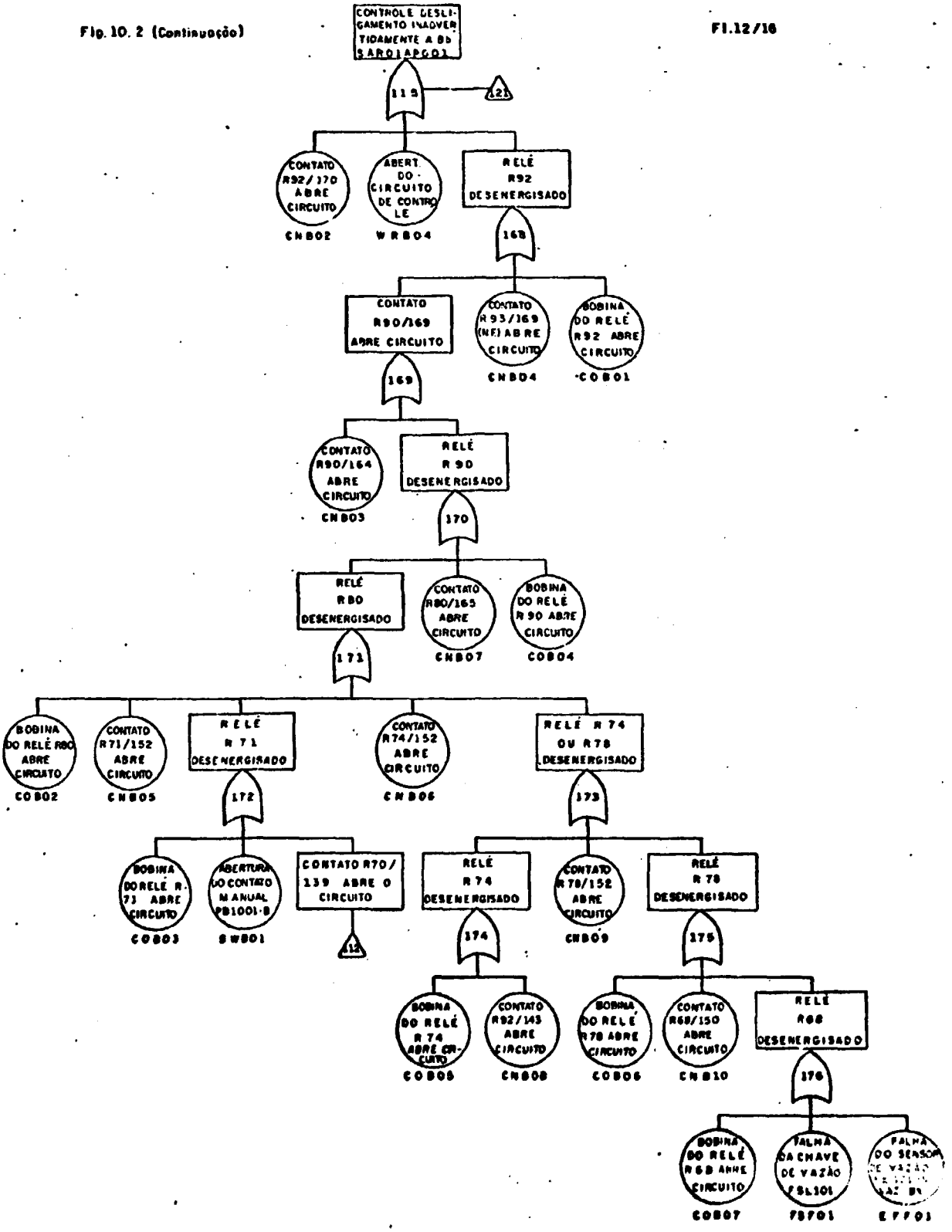
Fig.10.2 (Continuação)



(Continua)

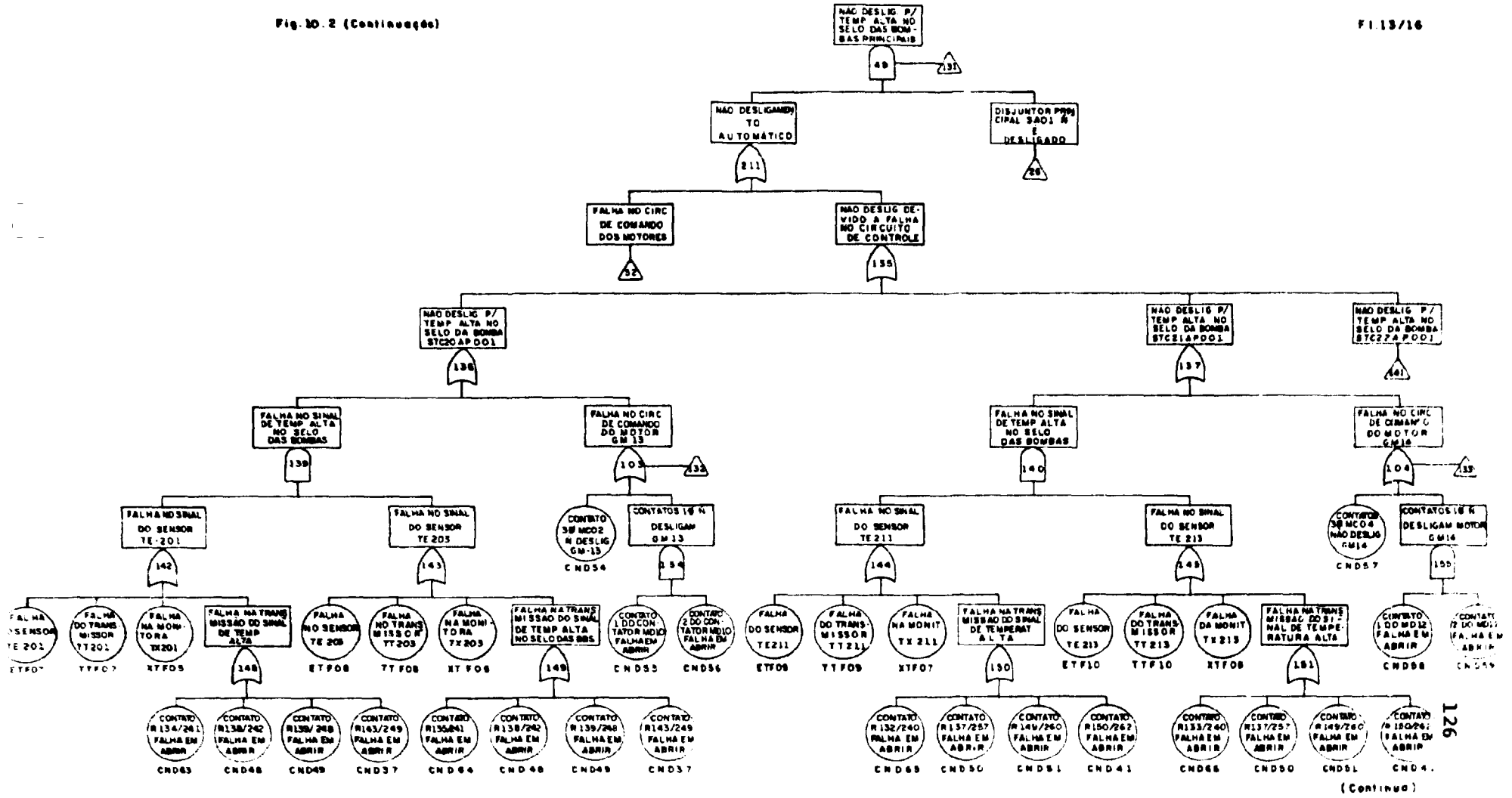
F1.11/16

Fig. 10. 2 (Continuação)



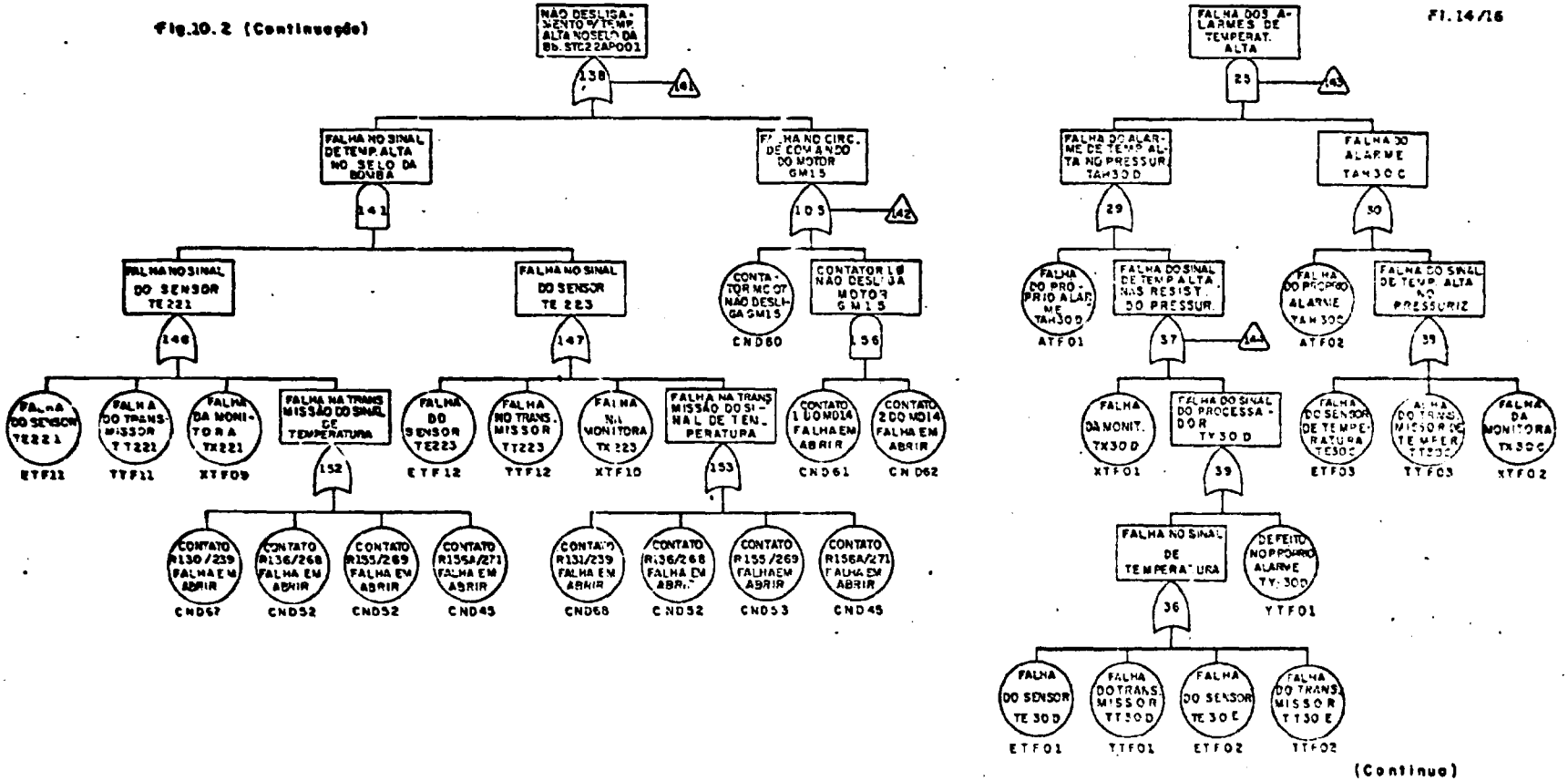
(Continua)

Fig. 10.2 (Continuação)



(Continua)

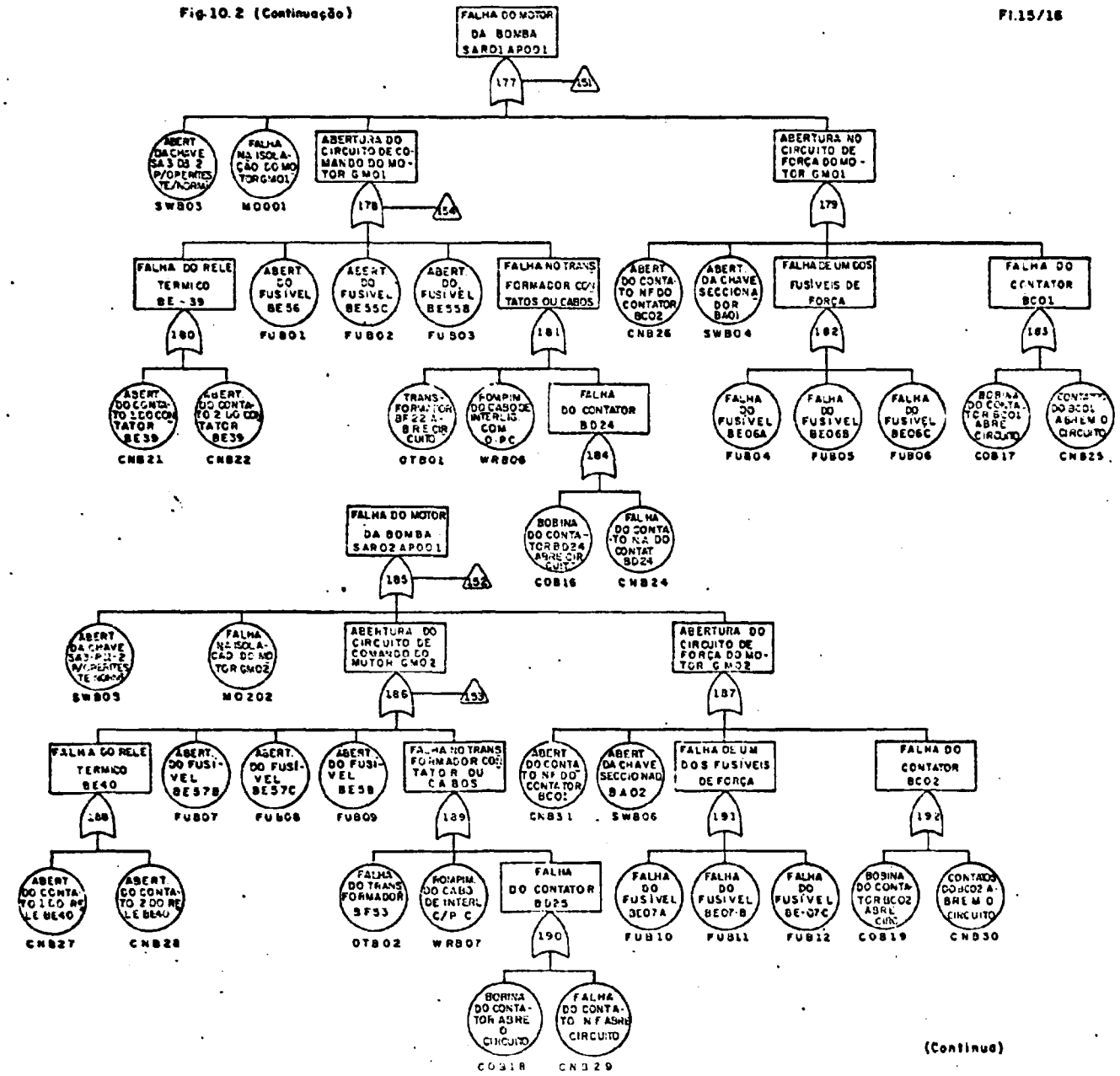
Fig.10.2 (Continuação)



Fl. 14/16

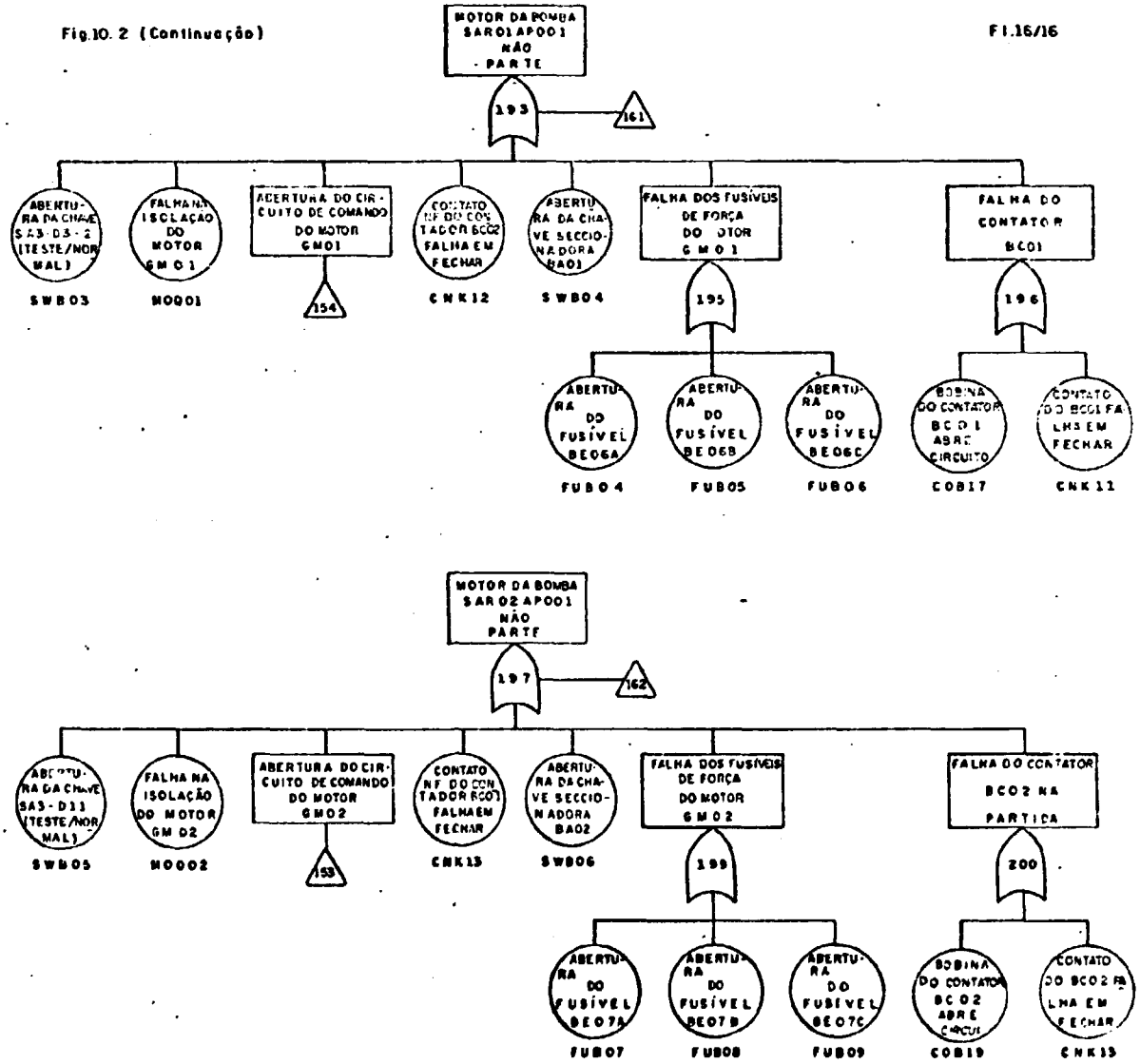
(Continua)

Fig.10.2 (Continuação)



(Continua)

Fig.10. 2 (Continuação)



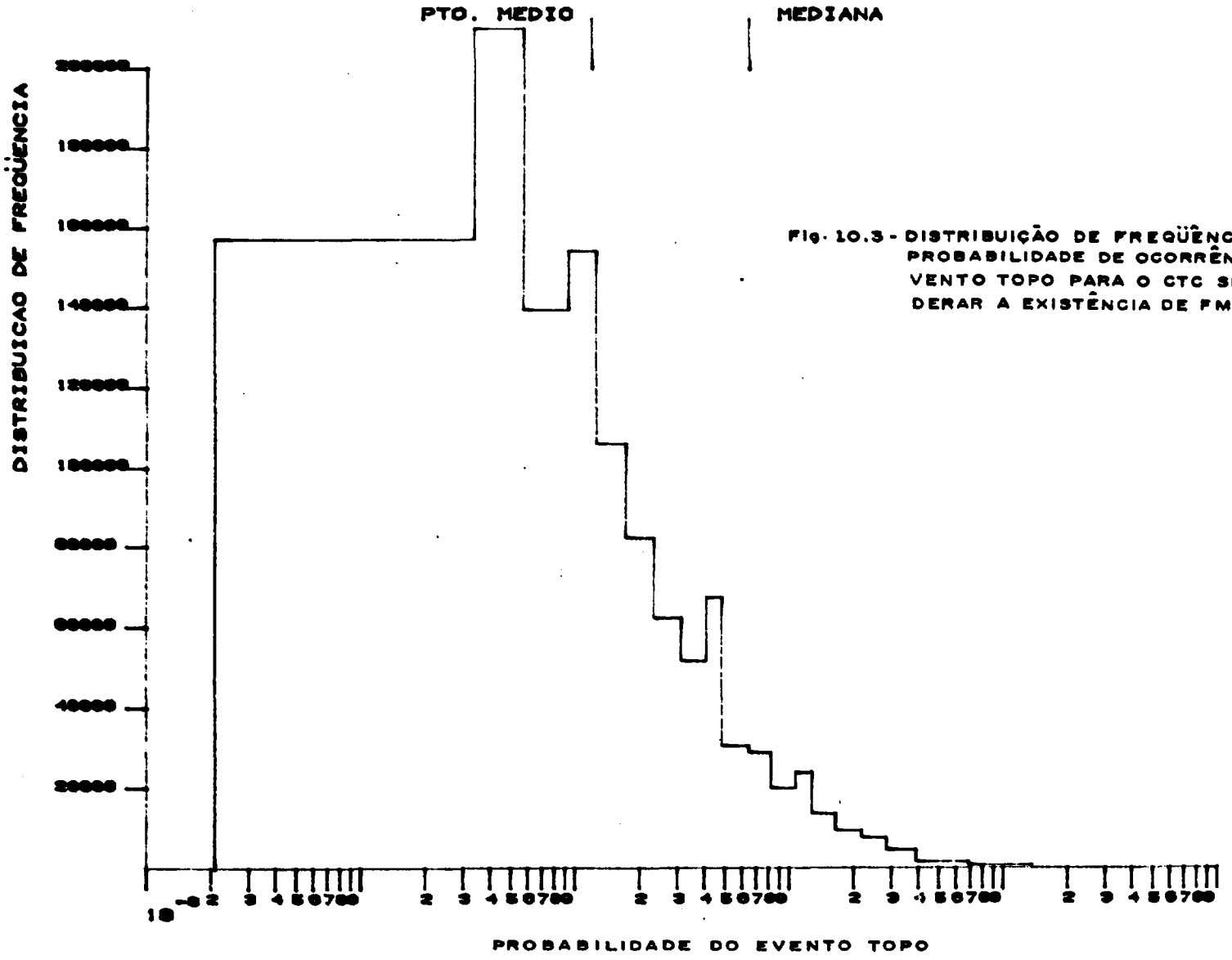


Fig. 10.3 - DISTRIBUIÇÃO DE FREQÜÊNCIA PARA A PROBABILIDADE DE OCORRÊNCIA DO EVENTO TOPO PARA O CTC SEM CONSIDERAR A EXISTÊNCIA DE FMC.

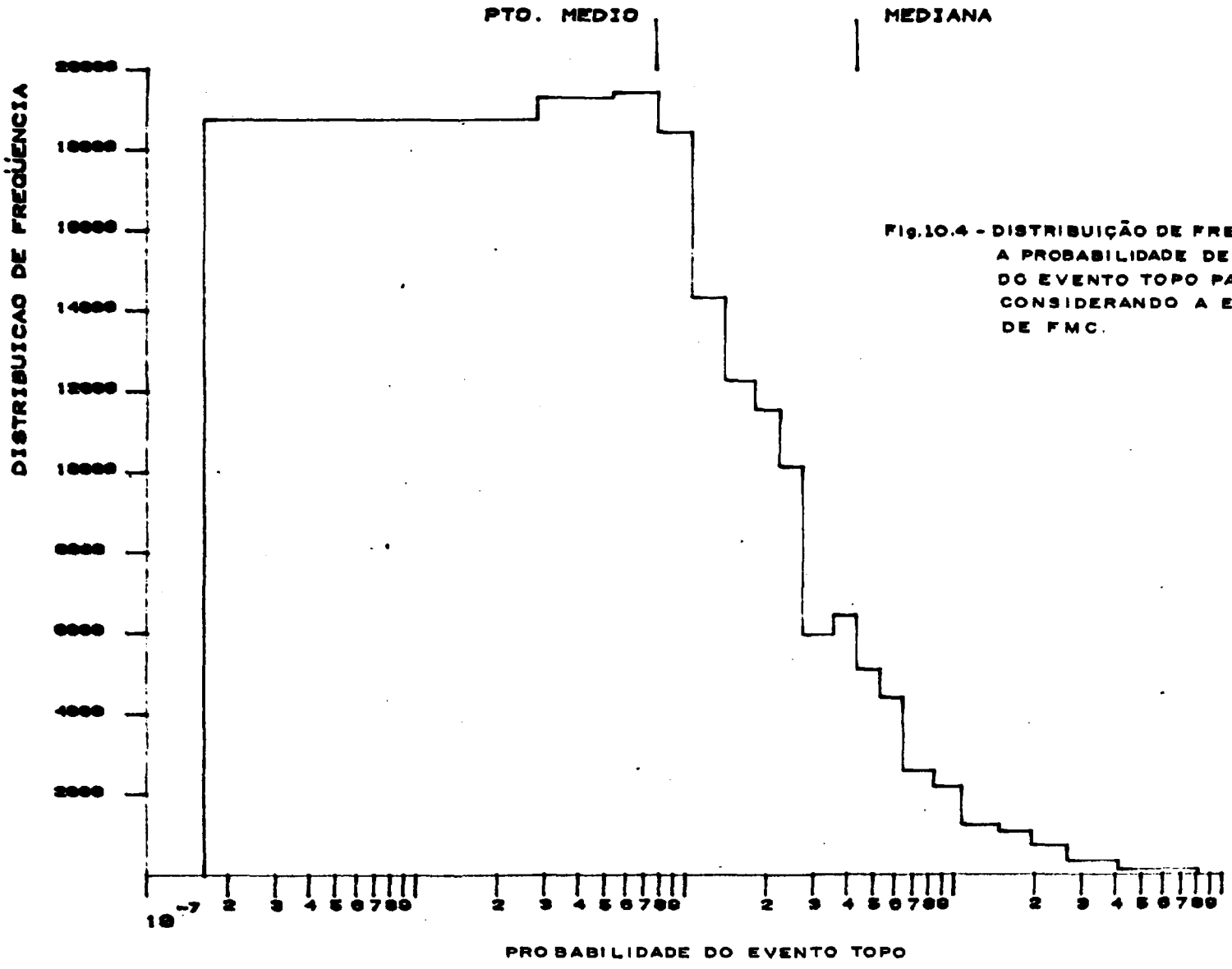


Fig.10.4 - DISTRIBUIÇÃO DE FREQÜÊNCIA P/ A PROBABILIDADE DE OCORRÊNCIA DO EVENTO TOPO PARA O CTC CONSIDERANDO A EXISTÊNCIA DE FMC.

APÊNDICE A

CÓDIGO PREP

Este código, escrito em FORTRAN IV, originalmente para o computador IBM 360/75 e implementado no IBM 4341 da NUCLEBRÁS, obtém os cortes mínimos e os caminhos mínimos de uma árvore de falhas, contendo até 2000 componentes e 2000 portas lógicas. É feita uma crítica minuciosa dos dados de entrada, evitando-se assim a obtenção de informações incorretas.

O código PREP compõe-se basicamente de dois programas: o TREBIL e o MINSET. O dado de entrada para o programa TREBIL é a árvore de falhas num formato que é natural e imediato para o analista. Este programa aceita apenas árvores de falhas com portas E ou OU, sendo que outras portas têm que ser escritas em função destas duas. A porta de inibição pode ser escrita como uma porta E, e a condição de inibição pode ser vista como um componente. O programa gera um equivalente lógico da árvore de falhas, resultando na subrotina TREE, que é compilada junto com as subrotinas de MINSET. MINSET determina os cortes mínimos (ou os caminhos mínimos), por teste determinístico, através da subrotina COMBO, ou pelo método de Monte Carlo, através da subrotina FATE. Em árvores de falhas que contêm mais de 100 componentes, podem-se obter por teste determinístico os cortes mínimos de 1ª, 2ª e possivelmente de 3ª ordem. Neste caso, a obtenção de cortes mínimos de ordem mais alta é impossível, dentro de um tempo razoável de processamento, e deve ser feita através do método de Monte Carlo.

Os cartões de dados para o código PREP são, resumidamente:

1. TITLE CARD

2. {Cartões de Comentários}

3. * b DATA (b = coluna em branco)

4. (Parâmetros de Controle) - Grupo de Dados I

5. END

6. * b TREE

7. (Descrição da Árvore de Falhas) - Grupo de Dados II

8. END

9. * b RATES

10. (Dados de Falhas e de Reparos) - Grupo de Dados III

11. END

Os Grupos de Dados I, II e III, utilizados para a análise da árvore de falhas para o evento topo "Pressão Excessiva no Circuito Principal do CTC", são mostrados resumidamente nas Tabelas A.1 e A.2.

A descrição detalhada do código e dos seus dados de entrada é dada no seu manual de utilização |57|.

Tabela A.1 - Dados de entrada para o código PREP, para a árvore de falhas com o evento topo "Pressão Excessiva no Circuito Principal do CTC"

		GRUPO DE DADOS I
NOME DA VARIÁVEL	VALOR	DESCRIÇÃO
NG	214	Nº de portas lógicas na árvore de falhas.
MIN	0	Indica que será utilizado o método de Monte Carlo.
MCS	1	Indica o tamanho do menor corte mínimo que será obtido.
NREJEC	500	Indica que os 1ºs 500 nºs aleatórios serão rejeitados.
NTR	700	Nº de tentativas do método de Monte Carlo.
IREN	2	Controle de parâmetros da subrotina FATE.
IDEX1	0	Indica que serão obtidos cortes mínimos.
IDEX2	1	Indica que os cortes mínimos serão imprimidos.

	GRUPO DE DADOS II
NOME DA VARIÁVEL	DESCRIÇÃO
GATE(1, J)	Nome da J'ésima porta lógica.
GATE(2, J)	Tipo da J'ésima porta lógica (AND ou OR).
NGG (J)	Número de portas lógicas de entrada para a porta lógica J.
NCC (J)	Número de eventos primários de entrada para a porta lógica J.
	Estes dados são obtidos diretamente da árvore de falhas mostrada na Figura 10.2.

	GRUPO DE DADOS III
NOME DA VARIÁVEL	DESCRIÇÃO
NAM (I)	Nome do I'ésimo evento primário.
LAMBDA (I)	Taxa de ocorrência do I'ésimo evento primário (por 10^6 horas).
TAU (I)	Tempo de reparo para o I'ésimo evento primário (em horas).
	Estas informações são obtidas da Figura 10.2 e da Tabela A.2.

Tabela A.2 - Dados de Taxas de Falhas e Fatores de Erro [9]

DESCRIÇÃO	λ FALHA/H ($x10^{-6}$)	FE
Rompimento de válvula manual	0,1	10
Abertura de válvula manual pelo operador	100	10
Erro do operador em responder a alarmes	28	10
Falha de alarmes	25	2
Falha de instrumentação	1	10
Falha de contato de relé em abrir	0,28	10
Abertura de circuito de controle (fio)	1	10
Válvula pneumática falha fechada	2,8	3
Falha de sistema de ar comprimido	2,8	3
Falha de solenóide de válvula operada a solenóide	2,8	3
Ruptura de tubulação, válvula, flanges, et	0,001	30
Fechamento de válvula manual pelo operador	100	10
Fechamento de válvula manual por defeito	0,001	30
Obstrução de tubulações	0,001	30
Ajuste inadequado de "setpoint" de válvula de alívio	2,8	3
Válvula de alívio falha em abrir	0,28	10
Ajuste inadequado de "setpoint" de válvula de segurança	2,8	3
Válvula de segurança falha em abrir	0,028	3
Válvula operada a motor falha em abrir	2,8	10
Falha de chave de posição	0,28	3
Falha no trocador de calor	0,1	10
Obstrução de placa de orifício	0,84	3
Falha de dispositivo de temporização do relé	5	3
Falha de bomba em partir	2,8	10
Falha de bomba durante funcionamento	10	10
Bobina de relé abre circuito	1	10
Contato de relé abre circuito	0,57	17
Abertura de contato manual por defeito	0,028	10
Abertura da chave manual pelo operador	100	3
Falha na isolação de motor	10	3
Fusível abre imediatamente circuito	1	3
Transformador abre circuito	1	3
Abertura de chave seccionadora por defeito	0,01	10
Disjuntor falha em abrir	2,8	10

APÊNDICE B

CÓDIGO KITT

Este código é uma aplicação da Teoria da Árvore Cinética [56] e foi escrito em FORTRAN IV, originalmente para o computador IBM 360/75 e implementado no IBM 4341 da NUCLEBRÁS. É apresentado em duas versões: o KITT1 e o KITT2. O código KITT1 analisa sistemas com taxas de falhas constantes e que sejam não reparáveis, ou com tempos de reparo constantes. Cada componente pode ter uma única taxa de falhas λ e um único tempo de reparo τ durante todo o tempo de operação. Já o código KITT2 pode analisar também sistemas com componentes que tenham, durante diferentes intervalos de tempo, diferentes características de confiabilidade. Em um intervalo de tempo ou fase, um componente pode ter um valor para λ e outro para τ, enquanto que noutro intervalo de tempo estes dois valores podem ser diferentes. O código KITT2 pode analisar também sistemas que tenham componentes com taxas de reparos constantes μ, ou que tenham diferentes valores de μ, em diferentes fases. Esta capacidade de analisar componentes com diferentes fases permite um estudo do comportamento cinético de um sistema, por exemplo, o estudo da sua confiabilidade quando ele está sob tensão, em um certo período de tempo (maiores valores de λ neste intervalo). O componente pode ter até 50 fases distintas, arbitrariamente espaçadas, e uma vez detalhadas, o comportamento do sistema pode ser investigado.

Em qualquer uma das duas versões, o código obtém as características de confiabilidade para cada componente, cada corte mínimo (ou caminho mínimo) e para o sistema. Estas características englobam:

- probabilidade que esteja num estado de falha no instante t;
- número de falhas que irá ocorrer por unidade de tempo no instante t;

. número de falhas que irá sofrer durante o intervalo de tempo entre 0 e t;

. probabilidade que irá sofrer uma ou mais falhas no intervalo de tempo entre 0 e t.

Quando o topo da árvore representa uma ocorrência de um tipo particular de acidente, ou a falha de um sistema em um dado experimento, a dependência do tempo não tem significado. Deseja-se apenas obter a probabilidade do evento topo, com o conhecimento das probabilidades de ocorrência dos eventos primários. Neste caso deve ser usado o código KITT1, onde cada evento primário deve ser tratado como uma condição de inibição, com probabilidade de ocorrência igual a P_i. Devem ser atribuídos valores de $\lambda_i \leq 0$ e $\tau_i \doteq P_i$ para todos os componentes.

Os cartões de dados para o código KITT1, utilizado para a análise da árvore de falhas, para o evento topo "Pressão Excessiva no Circuito Principal do CTC", são mostrados na Tabela B.1.

A descrição detalhada do código e dos seus dados de entrada é dada no seu manual de utilização [57].

Tabela B.1 - Dados de entrada para o código KITT1, para a árvore falhas com o evento topo "Pressão Excessiva no Circuito Principal do CTC"

NOME DA VARIÁVEL	VALOR	DESCRIÇÃO
		Título - caráter alfanumérico com até 80 caracteres
NPROB	1	Número de problemas que será análisado
NCOMP	30	Número total de componentes nos cortes mínimos (≤ 400)
XLMDA(I)	0	Taxas de falhas por hora para o componente I ($\lambda_i \leq 0$)
TAU(I)	Vários	Tempo de reparo τ_i (ou probabilidade de condição de inibição, para $\lambda_i \leq 0$) - de acordo com a Tabela A.2
ISTOP	1	Indica que não serão obtidas características de confiabilidade do sistema
NTPT	2	Número total de pontos no tempo para obtenção dos resultados
NOUT	1	Indica que não haverá impressão múltipla
DELTA	8760	Indica o espaçamento entre os pontos (em horas)
IPATH	1	Indica que são usados cortes mínimos
NCUT	51	Número de cortes mínimos analisados (≤ 500)
IMAX	5	Número de componentes mais condições de inibição nos cortes mínimos (serão analisados apenas os cortes mínimos de 5ª ordem)
ICUT(K,I)	Vários	Índices dos componentes e condições de inibição no k'ésimo corte mínimo (são obtidos pelo código PREP)

APÊNDICE C

Código SAMPLE

O programa SAMPLE, escrito em FORTRAN IV, originalmente para o computador IBM 360/75, foi implementado no CDC 6600.

O programa utiliza o Método de Monte Carlo para obter a média, a mediana, o desvio padrão, os limites de confiança e a distribuição, para uma função $Y = f(X_1, X_2, \ldots, X_n)$, que representa a equação booleana para o evento topo da árvore de falhas. Dadas a função $Y = f(X_1, X_2, \ldots, X_n)$, as estimativas de probabilidade e dispersão dos eventos primários e uma distribuição específica, o programa obtém uma amostra $x_1, x_2, \ldots, x_n$ da distribuição fornecida e avalia a função correspondente $y = f(x_1, x_2, \ldots, x_n)$. A amostragem é repetida N vezes (N é um parâmetro de entrada) e as estimativas resultantes são classificadas em ordem crescente para a obtenção dos limites de confiança para a estimativa da distribuição de Y.

O programa utiliza apenas uma das três distribuições: a normal, a lognormal ou a loguniforme. Os cortes mínimos da árvore lógica são fornecidos ao computador na forma de uma função em FORTRAN IV, denominada SAMPLE. Pode ser utilizado simultaneamente qualquer número de funções para os cortes mínimos, podendo portanto serem analisadas, simultaneamente, mais de uma árvore de falhas, ou mais de um caso de uma mesma árvore de falhas.

Os grupos de dados utilizados para a análise de incertezas dos resultados da árvore de falhas, com o evento topo "Pressão Excessiva no Circuito Principal do CTC", são dados na Tabela C.1. Este conjunto de dados não leva em conta as Falhas de Modo Comum.

Uma descrição detalhada do código e dos dados de entrada, bem

como uma listagem completa do mesmo é oferecida no Apêndice II, Vol. 1 do Wash-1400 [48].

Tabela C.1 - Dados de entrada para o código SAMPLE, para a árvore de falhas com o evento topo "Pressão Excessiva no Circuito Principal do CTC"

NOME DA VARIÁVEL	VALOR	DESCRIÇÃO
TITLE		Título do problema(até 80 caracteres)
IN	30	Número de variáveis (eventos primários)
IMAX	1200	Número de tentativas do método de Monte Carlo
NPROB	1	Número de problemas analisados
IDIST	L	Indica que será utilizada a distribuição lognormal para as taxas de falhas dos eventos primários
XQ	Vários	Probabilidade de ocorrência do evento primário, no período de interesse (1 ano). São estimados a partir dos valores da Tabela A.2
XD	Vários	Fator de erro para o evento primário (Tabela A.2)
	EXIT	"Flag" do conjunto de dados (último cartão)

APÊNDICE D

Distribuição Lognormal

Se a função densidade de probabilidade de y é a lognormal, a variável lny = x segue uma distribuição normal. Logo,

$$g(y) = \frac{1}{\sqrt{2\pi}\ \sigma}\ e^{-\frac{1}{2}\left(\frac{\ln y - \mu}{\sigma}\right)^2}$$

é a equação para a função densidade de probabilidade de y, onde μ e σ são, respectivamente, a média e o desvio padrão da distribuição normal associada.

São a seguir fornecidos os parâmetros mais utilizados da distribuição lognormal |36|:

Moda = $e^{(\mu - \sigma^2)}$;

Mediana = e^{μ};

Média = $e^{(\mu + \sigma^2/2)}$;

Variância = $(e^{\sigma^2} - 1)\ e^{(2\mu + \sigma^2)}$;

Fator de erro = FE = $\sqrt{\frac{\xi_{95\%}}{\xi_{5\%}}}$;

Percentil de ordem n = $\xi_n = e^{(\mu + \nu_n \sigma)}$,

onde $\xi_{95\%}$ é o 95º percentil da lognormal,

$\xi_{5\%}$ é o 5º percentil da lognormal e

v_n é o percentil de ordem n da normal associada.

A distribuição lognormal representa bem as taxas de falhas da maioria dos componentes elétricos e mecânicos.