TESE
477

EDMÉA PIRES DE OLIVEIRA BORGES

ANÁLISE DE CONFIABILIDADE EM SISTEMAS COMPLEXOS E DE ALTA SEGURANÇA

Escola Federal de Engenharia
Biblioteca MAUÁ
Itajubá

ORIENTADOR: RENATO DE AQUINO FARIA NUNES

CO-ORIENTADOR: IRANY DE ANDRADE AZEVEDO

TRABALHO DE DISSERTAÇÃO APRESENTADO À ESCOLA FEDERAL DE ENGENHARIA DE ITAJUBÁ COMO PARTE DOS REQUISITOS PARA OBTENÇÃO DO TÍTULO DE MESTRE EM ENGENHARIA ELÉTRICA.

CLASS. 621.311.1.004.15(043.2)
CUTT. B 732 a
TOMEO 477

Ministério da Educação e Cultura
ESCOLA FEDERAL DE ENGENHARIA DE ITAJUBÁ

A N E X O I

PRONUNCIAMENTO DA COMISSÃO EXAMINADORA

A Comissão Examinadora, abaixo assinada, nomeada por Portaria nº 148 de 22/05/87, considerando o resultado do Julgamento da Prova de Defesa Pública da Dissertação de Mestrado Intitulada: "Análise de Confiabilidade em Sistemas Complexos e de Alta Segurança",

apresenta pronunciamento no sentido de que a Comissão de Pós-Graduação da Escola Federal de Engenharia de Itajubá solicite à DDD (Divisão de Divulgação e Documentação) a expedição do título de Mestre em Engenharia Elétrica na Área de Concentração de Sistemas de Potência satisfeitas as demais exigências regimentais à EDMÉA PIRES DE OLIVEIRA BORGES.

Itajubá, 23 de maio de 1987.

1º Examinador
Dr. André Leite Alckmin
RHODIA S.A.

2º Examinador
Prof. Irany de Andrade Azevedo
EFEI

3º Examinador
Prof. Renato de Aquino Faria Nunes
EFEI

Ministério da Educação e Cultura
ESCOLA FEDERAL DE ENGENHARIA DE ITAJUBÁ

A N E X O II

FOLHA DE JULGAMENTO DA COMISSÃO EXAMINADORA

Título da Dissertação: "Análise de Confiabilidade em Sistemas Complexos e de Alta Segurança".

Autor: EDMÉA PIRES DE OLIVEIRA BORGES

JULGAMENTO

EXAMINADORES	CONCEITO	RUBRICA
1º	A	
2º	A	
3º	A	

Resultado médio: Conceito A, ou seja Aprovada

Observações:

Itajubá, 23 de maio de 1987.

1º Examinador
Dr. André Leite Alckmin
RHODIA S.A.

2º Examinador
Prof. Irany de Andrade Azevedo
EFEI

3º Examinador
Prof. Renato de Aquino Faria Nunes
EFEI

AGRADECIMENTOS

- Ao meu esposo pelo apoio, incentivo e compreensão constantes e, especialmente, para a realização deste trabalho.
- Aos professores Renato de Aquino Faria Nunes e Irany de Andrade Azevedo pelo trabalho de orientação e acima de tudo, pela amizade e cooperação.
- Aos professores e funcionários da EFEI pela atenção e competência.
- A Regina Maria Santos Grilo pelo execelente trabalho de datilografia.
- Ao amigo Gilberto Marino pelo apoio no desenvolvimento do programa "ÁRVORE".
- Aos colegas engenheiros que colaboraram para o desenvolvimento da Análise de Falhas.
- Ao amigo Daniel Oliva pela ótima qualidade dos desenhos.
- A todos aqueles que de alguma maneira colaboraram para a realização deste trabalho.

RESUMO

Este trabalho, foi desenvolvido com o objetivo de selecionar técnicas apropriadas para análise de confiabilidade de sistemas complexos, que favoreçam também a análise de segurança.

Foram estudados e analisados comparativamente vários métodos julgados relevantes, dois dos quais, pelas suas características, foram escolhidos como mais apropriados para a análise de confiabilidade do tipo de sistema a ser estudado.

Estes dois métodos, a **Análise de Modos de Falha e seus Efeitos** e o **Método das Árvores de Falhas**, complementares pela sua natureza, são então descritos detalhadamente.

Foi desenvolvido e implementado um algorítmo eficiente destinado a efetuar a análise quantitativa de Árvores de Falhas. O programa correspondente encontra-se implementado e sua aplicação tem-se mostrado bastante encorajadora.

Finalmente, os métodos escolhidos foram aplicados a um sistema-teste real e os principais resultados obtidos encontram-se detalhadamente descritos e criticamente analisados.

ÍNDICE

CAPÍTULO 1 - INTRODUÇÃO

1.1 - Descrição Geral do Problema..... 01

1.2 - Evolução da Metodologia..... 02

1.3 - Estrutura da Dissertação..... 06

CAPÍTULO 2 - ANÁLISE DE METODOLOGIAS

2.1 - Descrição Geral..... 08

2.1.1 - Análise Qualitativa..... 09

2.1.2 - Análise Quantitativa..... 11

2.2 - Métodos Baseados na Determinação de Sucesso..... 12

2.2.1 - Diagrama de Blocos de Confiabilidade..... 13

2.2.1.1 - Método de Decomposição por Aplicação do Teorema da Probabilidade Total. 18

2.2.1.2 - Método dos Mapas de Karnaugh..... 19

2.2.2 - Diagrama de Fluxos de Sinal..... 20

2.3 - Métodos Baseados na Determinação das Condições de Falha..... 21

2.3.1 - Análise Preliminar de Risco..... 21

2.3.2 - Análise de Modos de Falha e seus Efeitos..... 22

2.3.3 - Análise de Criticidade..... 23

2.3.4 - Árvore de Falhas..... 24

2.3.5 - Diagrama de Dependências..... 25

2.3.6 - Árvore de Eventos..... 28
2.3.7 - Conjuntos Mínimos de Corte..... 32
2.4 - Análise Comparativa..... 33
2.5 - Escolha dos Métodos..... 37

CAPÍTULO 3 - MÉTODO DAS ÁRVORES DE FALHAS

3.1 - Introdução..... 39
3.2 - Principais Características do Método..... 39
3.3 - Geração das Árvores de Falhas..... 40
3.3.1 - Análise de Modos de Falha e seus Efeitos..... 46
3.3.1.1 - Aspectos Relevantes.... 46
3.3.1.2 - Etapas de Construção... 48
3.3.1.3 - Um Modelo..... 49
3.4 - Análise Quantitativa..... 52
3.4.1 - Função Confiabilidade..... 52
3.4.2 - Função de Estrutura..... 57
3.4.3 - Função de Probabilidade..... 59
3.4.4 - Aproximação do Evento Raro..... 60
3.4.5 - Avaliação da Árvore de Falhas através de seus Cortes Mínimos... 62
3.4.6 - Avaliação da Árvore de Falhas através do Cálculo das Probabilidades dos Eventos Intermediários. 66
3.4.7 - Árvore de Falhas com Eventos Repetidos..... 71
3.4.8 - Método Monte Carlo de Simulação.. 71
3.4.8.1 - Considerações sobre Aplicações do Metodo às Árvores de Falhas..... 72

- 3.4.8.2 - Aspectos Particulares do Método..... 73
3.4.9 - Determinação de Taxas de Falha de Eventos Intermediários e do Evento Topo de Árvore de Falhas. 74
3.4.9.1 - Portões OU..... 75
3.4.9.2 - Portões E..... 76
3.4.10- Sensibilidades..... 77
3.5 - Análise do Sistema Elétrico de Emergência de uma Aeronave..... 80
3.5.1 - Descrição do Funcionamento do Sistema..... 80
3.5.2 - Análise de Modos de Falha e seus Efeitos..... 81
3.5.3 - Construção da Árvore de Falhas. 82
3.5.4 - Cálculo da Probabilidade de Ocorrência do Evento Topo..... 83
3.5.5 - Cálculo da Taxa de Ocorrência do Evento Topo..... 85
3.5.6 - Análise de Sensibilidades..... 86

CAPÍTULO 4 - APLICAÇÃO DA METODOLOGIA

4.1 - Introdução..... 90
4.2 - Descrição do Sistema..... 90
4.2.1 - Características do Sub-Sistema AC..... 96
4.2.1.1 - Condições Normais de Operação em Vôo..... 96

4.2.1.2 - Condição de Falha de um Gerador..... 96
4.2.1.3 - Aspectos Operacionais 97
4.2.2 - Características do Sub-sistema DC..... 98
4.2.2.1 - Condições Normais de Operação em Vôo..... 99
4.2.2.2 - Condições de Falha... 99
4.2.2.3 - Aspectos Operacionais 100
4.3 - Análise de Modos de Falha e seus Efeitos do Sistema de Geração de Potência Elétrica..... 101
4.4 - Desenvolvimento das Árvores de Falhas do Sistema..... 148
4.4.1 - Caracterização da Missão Típica..... 148
4.4.2 - Estabelecimento do Evento Topo. 150
4.4.3 - Análise da Confiabilidade da Missão..... 150
4.5 - Avaliação da Probabilidade de Falha da Missão..... 160
4.6 - Análise de Sensibilidades..... 167

CAPÍTULO 5 - CONCLUSÕES..... 174

BIBLIOGRAFIA..... 180

APÊNDICE A - PROGRAMA ÁRVORE

A.1 - Introdução..... 189

A.2 - Descrição..... 189
A.3 - Manual do Usuário..... 195
A.3.1 - Informações Gerais..... 195
A.3.2 - Entrada do Programa..... 196
A.3.2.1 - Descrição de Entrada da Estrutura da Árvore - 1º Conjunto de Dados..... 196
A.3.2.2 - Descrição de Entrada de Valores Associados aos Eventos - 2º Conjunto de Dados..... 196
A.4 - Exemplo Típico..... 199

APÊNDICE B - REQUISITOS DE CONFIABILIDADE USUAIS PARA HOMOLOGAÇÃO DE AERONAVES CIVIS..... 208

CAPÍTULO I

INTRODUÇÃO

1.1 - DESCRIÇÃO GERAL DO PROBLEMA

O avanço tecnológico atual tem forçado uma competição de mercado cada vez maior e mais diversificada.

Isto faz com que os novos produtos desenvolvidos estejam sujeitos a comprovação de requisitos estabelecidos como indispensáveis.

Em se tratando de sistemas caros ou cuja falha implique em riscos, um dos requisitos básicos é a confiabilidade. Na indústria aeronáutica, para demonstrar requisitos de confiabilidade, várias metodologias têm sido empregadas, sendo que é preferida a análise de riscos com o objetivo de minimizar sua probabilidade de ocorrência. O mesmo pode ser sentido na área nuclear, química, de armamentos e sistemas de potência elétrica.

Neste trabalho, pretendeu-se desenvolver uma metodologia de análise de confiabilidade que permita o acompanhamento do projeto desde sua concepção, favorecendo uma melhor escolha de alternativas, evoluindo com o projeto,entrando em fase de testes econtinuando através de coleta de dados para comprovação dos resultados da análise que demonstrou teóricamente cumprimento dos requisitos. Além disso, permita levantar informações importantes para o planejamento de manutenção preventiva e corretiva para garantir os níveis de confiabilidade desejados e favoreça a análise de segurança.

O método foi aplicado ao sistema elétrico de uma

aeronave, por ser um exemplo bastante completo e onde os requisitos de segurança severos obrigam a análise detalhada dos sistemas envolvidos.

1.2 - EVOLUÇÃO DA METODOLOGIA

No início deste século, os problemas relativos a confiabilidade eram tratados de maneira intuitiva. Após projetados, os equipamentos eram submetidos a testes e, quando necessário, eram reprojetados. Além de dispendiosa, esta técnica teve que ser abandonada com a evolução industrial. O lançamento de projetos novos, complexos e caros, exigia uma nova técnica de análise de confiabilidade que permitisse quantificar seu desempenho de maneira objetiva e rápida, dimuinuindo o número de insucessos e tornando o produto competitivo no mercado.

Inicialmente, eram feitas comparações de qualidade. Na indústria aeronáutica, com o aumento das unidades em operação, as informações sobre o número de falhas levou, na década de 30, à idéia de se expressar a confiabilidade em termo de um número médio de falhas para aviões.

Na década de 40, alguns requisitos fixavam a taxa de acidentes em 1 em 100 000 horas de vôo. Alguns tipos diferentes de expressões foram aparecendo.

A teoria matemática da confiabilidade tem crescido das demandas da tecnologia moderna e particularmente das experiências da 2ª. Guerra Mundial com sistemas militares complexos.

O trabalho realizado com o desenvolvimento de mísseis também foi de grande importância para o desenvolvimento da teoria da confiabilidade.

Excetuando a informática e ciências do ambiente, nenhum outro braço da ciência desenvolveu-se tão drasticamente nas últimas décadas como a análise de confiabilidade, segurança e risco. No início da década de 1960 as análises de segurança eram feitas em bases empíricas; somente em alguns setores das indústrias aeroespacial e armamentista era usada a palavra confiabilidade. O termo análise de risco era virtualmente desconhecido.

Desde 1970, particularmente na Europa, uma tecnologia inteiramente nova surgiu para resolver problemas associados a qualidade do produto, restrição ambiental e para satisfazer às exigências de autoridades governamentais que passaram a interferir em projetos, construção e operação de sistemas. A evolução dessa tecnologia tem sido lenta e difícil porque a literatura é complexa e algumas técnicas não são familiares a muitos engenheiros. A diversidade de aplicações e de métodos representa às vezes obstáculos para inovações. Um método que tem sido bastante explorado em várias aplicações é o de Árvore de Falhas.

Esta técnica foi desenvolvida originalmente por Watson, H.A., da Bell Telephone Laboratories em 1961 para analisar o sistema de controle de lançamento do Missil Minuteman [1].

Mais tarde, Haasl, D.F. da Companhia Boeing utilizou o método em seus estudos, divulgando-os no "System Safety Symposium - 1965", sob o título "Advanced Concepts in Fault Tree Analysis".

A partir daí, o processo ganhou boa aceitação e passou a ser explorado por profissionais de outras áreas, conforme exemplificado a seguir.

- Um estudo bastante completo e pioneiro na área de energia nuclear - Estudo de Segurança de Reatores-foi denominado WASH - 1400 ou "Rasmussen Report", em homenagem ao coordenador do trabalho. Embora tenha sido publicado em 1975 e seja aplicável a reatores operando em 1972, é até hoje usado como referência para análises de risco de reatores nucleares [38]. Neste estudo foram aplicadas as técnicas de Análise de Modos de Falha e seus Efeitos, Árvore de Falhas, Árvore de Eventos, que são ferramentas eficientes para análise de risco.
- Na análise de confiabilidade de capacitores série em sistemas de potência [2] foi empregado o método de Árvore de Falhas para cálculo da probabilidade de ocorrência dos eventos indesejados. Ainda nesta aplicação foi utilizada a Análise de Modos de Falhas e seus Efeitos- FMEA- como análise complementar do sistema, de forma a garantir que todos os componentes e modos de falha tenham sido considerados. Os autores ainda sugerem utilizar a árvore de falhas para análise de sensibilidades de forma a escolher taxas de falha aceitáveis para componentes.
- Lapp and Powers sugeriram um algorítmo para composição de árvore de falhas em computador, aplicando-o a um sistema de processamento químico. Este algorítmo gerou muitas críticas e debates [3,4, por exemplo] que levaram os autores a aprofundar alguns pontos em [5]. Outro exemplo é apresentado por Taylor, em [6].
- Pau e Weber apresentam a aplicação da técnica de Árvore de Falhas ao controle de qualidade, baseados na analogia entre componentes falhados (em confiabilidade) e medidas fora de tolerância [7].
- Outros campos de aplicação foram surgindo, como é o caso de

Árvore de Falhas aplicada a análise de um Sistema Elétrico de Potência - Sistema de Distribuição [8].

- A metodologia de Árvore de Falhas foi proposta para estudos de melhoramento da disponibilidade de Sistemas Elétricos de Potência, na "Southern Company Services - Birmingham, Alabama" [9]. Primeiramente, para identificar áreas carentes de melhoramento e após, para determinar que mudanças ou combinações de mudanças deveriam ser aplicadas para alcançar a disponibilidade desejada para cada sistema.
- Outra aplicação interessante foi apresentada em [10] , a Sistemas de Proteção. O autor chama a atenção para um problema importante e que merece mais atenção: os dados relativos aos modos de falha.

Em consequência da diversidade de aplicações, a metodologia foi sendo aprimorada e novas propostas surgiram para avaliação de resultados e implementação computacional.

Alguns algorítmos baseiam-se na determinação dos conjuntos mínimos de corte, seguindo duas lógicas: do topo para a base [11,12] ou da base para o topo [13].

Um dos algorítmos mais conhecidos, orientado do topo para a base, foi proposto por Fussel e Vesely [11], reduzindo o tempo de execução em relação aos algorítmos conhecidos até então, que passou a ser aproximadamente função linear da quantidade e da ordem dos conjuntos de corte.

Um algorítmo opcional consiste na determinação dos parâmetros relativos aos eventos intermediários, combinando-os segundo a lógica da árvore até atingir o evento topo. É este processo que está desenvolvido neste trabalho e que demonstra ser eficiente e de tempo de execução bastante reduzido. Uma des

crição deste mesmo processamento pode ser encontrado em [14].

Normalmente, a lógica da árvore de falhas é descrita utilizando Álgebra Booleana - como nos algorítmos descritos anteriormente - entretanto, existem trabalhos propondo uma alternativa a esta sistemática, visando analisar sistemas não-coerentes [15].

Outros trabalhos propõem a extensão da aplicação da análise por Árvore de Falhas a sistemas de mais de dois estados [16] e sujeitos a reparos [17,18,19].

1.3 - ESTRUTURA DA DISSERTAÇÃO

Este trabalho foi desenvolvido com o objetivo de selecionar técnicas apropriadas para análise de confiabilidade de sistemas complexos, que favoreçam também a análise de segurança.

No Capítulo 2, são descritas algumas metodologias comumente encontradas em aplicações típicas. Esses métodos seguem basicamente uma lógica positiva ou negativa, a medida que pesquisam a confiabilidade de sistemas a partir da probabilidade de sucesso ou de falha dos seus componentes. Os métodos selecionados foram: Método de Diagrama de Blocos de Confiabilidade, Diagrama de Fluxos de Sinal - os que seguem a lógica positiva; Análise Preliminar de Risco, Análise de Modos de Falha e seus Efeitos, Análise de Criticidade, Árvore de Falhas, Diagrama de Dependências , Árvore de Eventos, Conjuntos Mínimos de Corte - os que seguem a lógica negativa.

Pelas características favoráveis apresentadas, foi feita a escolha dos métodos: Análise de Modos de Falha e seus Efeitos e Árvore de Falhas.

A partir da escolha, são apresentados no Capítulo 3, maiores detalhes sobre os métodos e sua aplicação.

Um formulário típico para a Análise de Modos de Falha e seus Efeitos foi apresentado como modelo. Um sistema exemplo foi desenvolvido para ilustrar o método, assim como para análise de sensibilidades e cálculo da taxa de falha de eventos intermediários.

O sistema selecionado para aplicação das metodologias, encontra-se descrito no Capítulo 4. Após descrição do sistema, pode ser encontrada uma Análise de Modos de Falha e seus Efeitos detalhada até o nível de informações disponíveis e até onde houve interesse em detalhar para conhecimento do sistema. Procurou-se incluir todos os modos possíveis de falha de cada componente.

Uma missão típica foi descrita para que as Árvores de Falhas pudessem ser geradas.

Utilizando o programa ÁRVORE, desenvolvido para esta aplicação, foi determinada a probabilidade de ocorrência do evento topo e realizada a análise de sensibilidades.

Finalmente, no Capítulo 5 apresentam-se conclusões do estudo proposto, considerações e sugestões para aplicações futuras.

O apêndice A descreve o manual de utilização do programa ARVORE, no qual se inclui também um fluxograma detalhado do algorítmo utilizado.

No apêndice B foram apresentadas informações adicionais acerca de Análise de Riscos.

CAPÍTULO 2

ANÁLISE DE METODOLOGIAS

2.1 - DESCRIÇÃO GERAL

Em estudos de confiabilidade e no estabelecimento de metas de confiabilidade, existe uma diferença entre sistemas que estão sujeitos somente a uma interrupção de serviço e que podem ser operados assim que a parte falhada for substituída e aqueles em que uma falha ou uma combinação de falhas podem causar sua perda total. A perda do sistema não envolve somente fatores de ordem econômica, mas pode ter como consequência perda de vidas, como nos casos de acidentes com aeronaves e usinas nucleares ou de interrupção do fornecimento de energia elétrica a consumidores especiais (hospitais, por exemplo).

Em virtude dessas diferenças, e de acordo com a complexidade do sistema, diferentes métodos de análise de confiabilidade podem ser empregados.

A escolha do método a ser aplicado a um sistema específico, depende do nível de detalhes que se deseja atingir e do estágio de desenvolvimento do sistema.

Em se tratando de análise inicial para escolha de um,entre vários projetos alternativos, pode ser interessante comparar a eficiência dos sistemas de uma forma geral sem muitos detalhes. Neste caso; o método de diagrama de blocos [20] poderá ser uma boa escolha.

Para sistemas em que é exigida minimização de sua criticidade, uma análise de segurança deverá ser desenvolvida.

Alguns métodos de análise de confiabilidade [27, 38] favorecem a análise de risco e sensibilidades. Esses métodos são gerais e podem ser aplicados normalmente a sistemas complexos.

Para analisar sistemas semelhantes aosque são propostos neste trabalho, é conveniente selecionar um método para cálculo de segurança e confiabilidade que torne possível um detalhamento profundo dos modos de falha potenciais e suas consequências sobre o sistema.

Dois aspectos da análise de confiabilidade de sistemas podem ser considerados: o qualitativo e o quantitativo.

2.1.1 - ANÁLISE QUALITATIVA

É usada para identificar as possíveis falhas e indicar as ações apropriadas (mudanças de projeto, procedimentos administrativos, etc.) que reduzirão a frequência ou consequências de tais falhas.

A análise qualitativa pode ser realizada com um ou mais dos seguintes objetivos [20]:

- Identificar pontos fracos ou desbalanceamentos no projeto.
- Auxiliar a avaliação sistemática da segurança total da instalação.
- Documentar e estabelecer a importância relativa de todas as falhas identificadas.
- Desenvolver disciplina e objetividade, por parte do projetista de sistemas, relativos à segurança.
- Fornecer uma compilação sistemática de dados como um passo preliminar para facilitar análises quantitativas.

Esse tipo de análise deve ser parte integral do processo normal de projeto de sistema . O projetista é o mais qualificado para identificar os modos particulares de falha e seus graus de importância, mas deve ser imaginado que o projetista pode negligenciar, nessa análise sistemática, aqueles modos de falha que são considerados sem importância durante a fase executiva do processo original de projeto. Portanto, sua análise sistemática deve ser revisada e verificada por pessoa qualificada e que não esteja diretamente envolvida no projeto.

O analista de confiabilidade deve fornecer métodos, dados e serviço de análise aos grupos de projeto, além de participar da análise.

Os passos gerais na análise qualitativa da confiabilidade do sistema são:

- Identificar falhas significativas e suas consequências.
- Dispor a informação acima na forma de tabelas, diagramas, árvores de falhas ou outro formato.
- Verificar os pontos frágeis e críticos do sistema e resolver os problemas identificados.

Cada um desses passos requer diferentes tipos de documentação, métodos e pessoal.

Os modos de falha são identificados não somente pelo pessoal de projeto e operação, mas por todos envolvidos no projeto; no entanto cabe, em geral, ao engenheiro de projeto documentar esses modos.

2.1.2 - ANÁLISE QUANTITATIVA

A análise quantitativa representa o sistema através de um modelo matemático, dotado de objetivos de confiabilidade, disponibilidade e segurança, bem como os compatibiliza com os objetivos globais do sistema. A análise fornece um modelo apropriado para representar o sistema que facilitará as aplicações das técnicas da engenharia de confiabilidade durante os estágios de projeto, produção e operação [20].

Essa análise ajuda o projetista a minimizar a complexidade do sistema, a estar ciente das características dos componentes selecionados e a desenvolver um projeto confiável. O projetista considera as taxas e modos de falha dos componentes que ele seleciona e verifica a sua identificação sob condições de falha, para determinar ações apropriadas no sistema, sobre o operador ou ambas.

O modelo matemático gerado pode ser usado em análises de sensibilidades. Assim, pode-se identificar ítens críticos no projeto e estabelecer a credibilidade da análise. A importância relativa de cada taxa de falha dos componentes na previsão da confiabilidade e da disponibilidade para o sistema pode também ser determinada.

Os métodos de análise de confiabilidade de sistemas baseiam-se na identificação das condições de sucesso ou falha dos elementos componentes de tal forma que, convenientemente combinados, resultem no sucesso ou na falha do sistema.

Os primeiros são usados, de preferência, quando se deseja apenas avaliar a confiabilidade do sistema como um todo, sendo mais gerais.

O estudo de confiabilidade considerando as falhas, impõe que se detalhe o sistema em profundidade, possibilitando ainda análises de criticidade e segurança do sistema.

O objetivo principal dos estudos de criticidade e segurança é identificar as relações de causa entre os eventos básicos, sejam humanos, de componentes ou ambientais, que resultem em falha do sistema e encontrar maneiras para diminuir seu impacto através de modificações ou melhoramentos do projeto original.

2.2 - MÉTODOS BASEADOS NA DETERMINAÇÃO DAS CONDIÇÕES DE SUCESSO

Durante a fase inicial de desenvolvimento de um novo sistema, o projetista defronta-se com uma questão básica: a de desenvolver um sistema sujeito a certos requisitos de desempenho, que se traduzem usualmente pela exigência de cumprir funções pré-especificadas com um número mínimo de falhas.

Normalmente existem várias alternativas de projeto que satisfazem os requisitos de desempenho e, antes da decisão entre vários projetos, uma análise preliminar de confiabilidade pode ajudar na decisão.

Os métodos de determinação de sucessos são bastante utilizados nesta fase.

Quando se trata de desenvolvimentos complexos, um programa efetivo de controle deve acompanhar a evolução do projeto e estender-se às fases de teste e produção.

2.2.1 - DIAGRAMAS DE BLOCOS DE CONFIABILIDADE [20]

São diagramas de associação de sucessos que representam graficamente a lógica do sistema.

São desenvolvidos através da análise de relacionamento funcional entre os componentes. O relacionamento de eventos é expresso pela maneira como os blocos são conectados no diagrama.

O procedimento geral para construir um diagrama de blocos é o seguinte:

- Definir a missão de forma que completá-la representa o sucesso do sistema.
  Se o sistema tem mais que uma missão, cada uma deve ser considerada, individualmente.
- Construir o diagrama, utilizando informações sobre o sistema que podem ser obtidas através de algum procedimento sistemático como a Análise de Modos de Falha e seus Efeitos, Diagramas Funcionais, etc.
- Investigar o diagrama e assegurar-se de que todos os caminhos levando ao sucesso foram incluídos.

O diagrama corresponde rigorosamente ao Diagrama Funcional do Sistema e permite uma compreensão visual do funcionamento normal do sistema.

A avaliação da confiabilidade do sistema é feita, a partir dos dados de confiabilidade dos elementos que o compõem, segundo a lógica do diagrama.

São considerados dois estados possíveis de desempenho dos componentes e sistemas: funcionamento e não funcionamento.

A indicação do estado de um sistema pode ser fornecida por uma variável binária ϕ, dependente das variáveis indicadoras dos componentes [24,37].

$\phi = \phi(\vec{x})$ é chamada função de estrutura do sistema

onde:

$(\vec{x}) = (x_1, x_2 \ldots x_n)$ representa a combinação dos estados dos componentes que podem ser

$\begin{cases} 1 \text{ quando o componente funciona} \\ 0 \text{ quando o componente não funciona} \end{cases}$

Quando o funcionamento do sistema depende do funcionamento de todos os componentes, eles estarão agrupados em série e sua função de estrutura é

$$\phi = x_1 x_2 \ldots x_n$$

$$= \prod_{i=1}^{n} x_i$$

$$= \min(x_1, x_2, \ldots, x_n).$$

Estas são associações do tipo E.

Quando o funcionamento do sistema ocorre se pelo menos um dos componentes funcionar, eles estarão agrupados em paralelo e sua função de estrutura é

$$\phi = 1-(1-x_1)(1-x_2)\ldots(1-x_n)$$

$$= 1 - \prod_{i=1}^{n} (1-x_i)$$

$$= \coprod_{i=1}^{n} x_i$$

$$= \max(x_1, x_2, \ldots, x_n)$$

Estas associações são do tipo OU.

Para determinação da função de estrutura de um sistema com várias associações mistas (série-paralelo), podemos usar o Método da Decomposição Modular que consiste em decompor o sistema em subsistemas do tipo série ou paralelo (módulos), determinando suas funções de estrutura. Em seguida, pode-se determinar a função de estrutura do sistema combinando as funções de estrutura dos módulos.

A determinaçao da confiabilidade do sistema equivale a determinação da probabilidade de sucesso do sistema, a partir das probabilidades dos estados funcionais dos seus componentes.

$$P(\phi=1) = 1.P(\phi=1) + 0 \cdot P(\phi=0) = E(\phi)$$

Sendo $E(\phi)$ o valor esperado ou média de ϕ, isto é, consideramos que ϕ somente poderá assumir os valores 0 ou 1.

Deste modo, temos que, calcular a probabilidade de funcionamento do sistema $[P(\phi=1)]$ equivale a calcular a média de ϕ, ou seja, o desempenho médio do sistema.

Para os sistemas série e paralelo, resulta:

$$\begin{aligned} R_s &= P(\phi=1) \\ &= r_1 . r_2 \ldots r_n \\ &= \prod_{i=1}^{n} r_i \end{aligned}$$

$$\begin{aligned} R_p &= P(\phi=1) \\ &= 1-(1-r_1)(1-r_2)\ldots(1-r_n) \\ &= \coprod_{i=1}^{n} r_i \end{aligned}$$

onde:

R_s = confiabilidade do sistema série

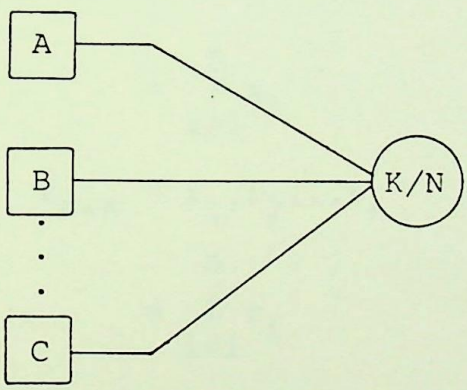
R_p = confiabilidade do sistema paralelo

r_i = confiabilidade do componente i

Além dos sistemas formados por combinações em série ou paralelo, existem outras lógicas permitidas. É o caso dos sistemas k-em-N.

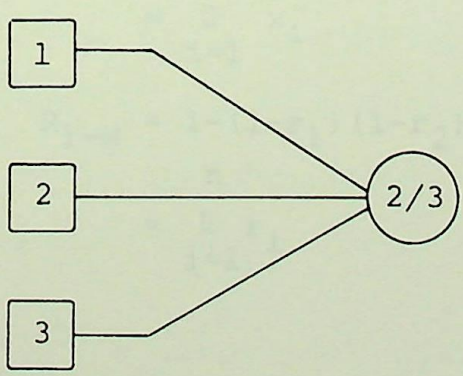
Um sistema k em N é constituído de N componentes e que o seu funcionamento é satisfatório quando pelo menos k componentes funcionam. Esta lógica é muito usada em sistemas de alarme onde se exige que vários sinais confirmem uma situação de perigo real.

Sua possível representação é:



Estes sistemas podem ser transformados nos sistemas série ou paralelo, de maneira conveniente.

Por exemplo, um sistema 2 - em - 3



Sua função de estrutura é:

$$\phi = x_1x_2+x_1x_3+x_2x_3-x_1^2x_2x_3-x_1x_2^2x_3-x_1x_2x_3^2+x_1^2x_2^2x_3^2$$

Por redução booleana,

$$\phi = x_1x_2+x_1x_3+x_2x_3-2x_1x_2x_3$$

Daí, podemos obter a função de confiabilidade

$$R_{2-3} = r_1r_2+r_1r_3+r_2r_3-2r_1r_2r_3$$

Constata-se agora facilmente que os sistemas série e paralelo se enquadram como casos particulares do sistema K em N.

O sistema N em N é o sistema série.

$$\phi_{N-N} = x_1.x_2\ldots x_n$$

$$= \prod_{i=1}^{n} x_i$$

$$R_{N-N} = r_1.r_2\ldots r_n$$

$$= \prod_{i=1}^{n} r_i$$

O sistema 1 em N é o sistema paralelo.

$$\phi_{1-N} = 1-(1-x_1)(1-x_2)\ldots(1-x_n)$$

$$= \coprod_{i=1}^{n} x_i$$

$$R_{1-N} = 1-(1-r_1)(1-r_2)\ldots(1-r_n)$$

$$= \coprod_{i=1}^{n} r_i$$

A análise pelo método de Diagrama de Blocos de Confiabilidade pode requerer outros modelos para representação lógica de funcionamento de sistemas particulares.

Como exemplo, cita-se o caso de componentes redundantes, porém, em reserva, de modo que somente entrarão em operação no caso de falha do componente efetivamente em serviço. Detalhes da análise de confiabilidade desse tipo de sistema podem ser encontrados nas referências [26,38].

2.2.1.1 - MÉTODO DE DECOMPOSIÇÃO POR APLICAÇÃO DO TEOREMA DA PROBABILIDADE TOTAL [26]

Alguns sistemas possuem características próprias que não permitem representação direta por combinação de associações série, paralelo ou reserva. Nestes casos, um recurso bastante utilizado para procura da solução utiliza o teorema da probabilidade total.

$$P(A) = \sum_{i=1}^{n} P(A|B_i).P(B_i)$$

Este procedimento pode ser repetido várias vezes até que se obtenha associações série-paralelo.

Pode-se então escrever a expressão equivalente e determinar a probabilidade de sucesso ou falha do sistema.

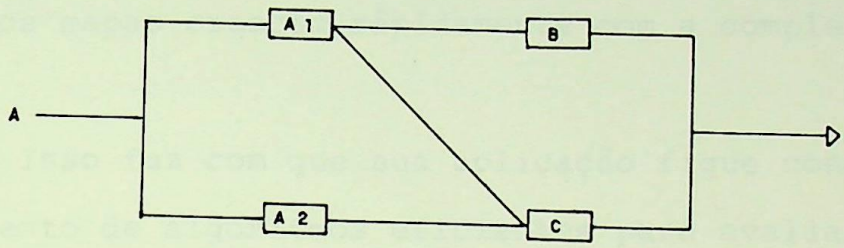
Para que o método possa ser aplicado é necessário que os eventos B_i, que são efetivamente, condições convenientemente escolhidas pelo analista, sejam mutuamente exclusivos e totalmente exaustivos.

2.2.1.2 - MÉTODO DOS MAPAS DE KARNAUGH

É uma outra metodologia aplicável à solução de combinações de eventos em formas mais complexas que a combinação série - paralelo.

Um exemplo simples pode ilustrar o método.

Seja o sistema abaixo representado.



Atribui-se ao estado de funcionamento o valor 1 e ao estado de falha o valor 0.

As combinações de eventos que permitem que um sinal de A alcance B podem ser representadas pelo mapa de Karnaugh:

		A1 , A2			
		00	01	11	10
	00	0	0	0	0
	01	0	1	1	1
B,C	11	0	1	1	1
	10	0	0	1	1

Agrupando as situações de sucesso em blocos disjuntos no mapa, pode-se escrever a função de sucesso

$$S = \left[A_2 \cap C\right] \cup \left[A_1 \cap \overline{A_2} \cap C\right] \cup \left[A_1 \cap B \cap \overline{C}\right]$$

a função de probabilidade de sucesso

$$P(S) = P(A_2).P(C) + P(A_1).P(\overline{A_2}).P(C) + P(A_1).P(B).P(\overline{C})$$

ou confiabilidade do sistema.

$$R = P(S) = R_{A_2}.R_C + R_{A_1}.Q_{A_2}.R_C + R_{A_1}.R_B.Q_C$$

Este método é equivalente ao método dos caminhos mínimos utilizando o mapa de sucesso ou falha para facilitar a seleção dos caminhos mínimos entre todos os caminhos possíveis. As dimensões dos mapas crescem rápidamente com a complexidade dos sistemas.

Isso faz com que sua aplicação fique condicionada ao desenvolvimento de algorítmos eficientes para avaliação das condições de sucesso e eliminação de componentes repetidos.

2.2.2 - *DIAGRAMA DE FLUXOS DE SINAL* [35,38]

Aplica-se a sistemas simples, sendo algumas vezes preferido ao Diagrama de Blocos por apresentar analogia com a teoria de circuitos e outras disciplinas da engenharia.

Um Diagrama de Fluxos de Sinal consiste na representação do sistema através de nós interligados por braços. Cada dois nós interligados por um braço representam um componente e seus sinais de entrada e de saída.

Os Diagramas de Fluxos de Sinal são resolvidos de forma análoga aos Diagramas de Blocos; os braços em série são associações do tipo E e os braços em paralelo são associações do tipo OU.

2.3 - MÉTODOS BASEADOS NA DETERMINAÇÃO DAS CONDIÇÕES DE FALHA

Esses métodos, também chamados Estudos de Risco , além de possibilitarem a avaliação da Confiabilidade de Sistemas, favorecem a Análise de Segurança e de Sensibilidades.

2.3.1 - ANÁLISE PRELIMINAR DE RISCO [22]

De acordo com critérios de risco-benefício, pode-se proceder ao melhoramento do sistema, se este não obedecer aos níveis de segurança desejados.

A fase inicial de um estudo de risco em um sistema envolve:

- Identificação de situações de risco.
- Identificação das partes do sistema que possam levar à ocorrência de risco.
- Limitação dos fatores de influência a considerar nos estudos de risco.

Frequentemente, após ser identificado o risco, é necessário para uma análise de segurança do sistema,proceder-se a uma avaliação quantitativa do problema.

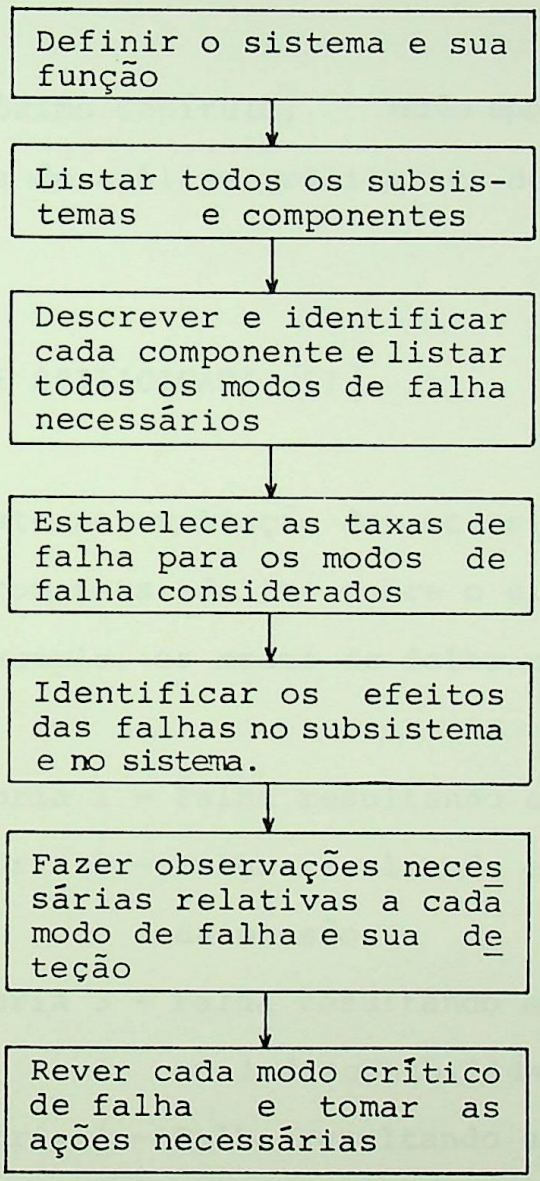
Obtidos os resultados, os riscos são classificados por ordem de criticidade . Pode ser conveniente eliminar aqueles de efeitos mais críticos através de melhoramentos nos sistemas.

O método de Árvore de Falhas é amplamente utilizado como extensão da Análise de Risco, que é qualitativa.

2.3.2 - ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS - FMEA

É um método de análise indutiva de sistemas. Consiste em identificar os modos potenciais de falha de cada componente e pesquisar seus possíveis efeitos sobre o sistema.

A rotina da análise pode ser orientada de acordo com o fluxograma abaixo [39].



As informações desta análise de falhas deverão ser dispostas em forma de tabelas, de modo a facilitar sua organi

zação e utilização.

Por ser um procedimento sistemático, muitas vezes evidencia modos de falha com consequências críticas ou prejuízo no desempenho do sistema, que ficariam despercebidos durante o processo normal de desenvolvimento do sistema.

É usada na escolha de projetos alternativos, em estudos para melhoramentos do sistema, assim como fornece informações valiosas para estabelecimento de tarefas de manutenção preventiva.

No próximo Capítulo, serão apresentados mais detalhes sobre esta técnica de análise qualitativa de confiabilidade de sistemas.

2.3.3 - ANÁLISE DE CRITICIDADE [27]

Consiste na avaliação dos modos de falha de componentes de acordo com seus efeitos sobre o sistema.

Por exemplo, os modos de falha podem ser classificados como:

Categoria 1 - Falha resultando em perigo de vida

Categoria 2 - Falha resultando em falha potencial da missão

Categoria 3 - Falha resultando em atraso potencial ou indisponibilidade operacional

Categoria 4 - Falha resultando em excessiva manutenção não programada.

Trata-se de um método de análise qualitativa que seleciona os modos de falha como mais críticos, analisando seus efeitos e consequências.

Pode ser um passo após a análise de falhas e como tal incorporar-se à mesma que, neste, caso será denomimada Análise de Modos de Falha e seus Efeitos e Análise de Criticidade.

Esta análise é importante para identificar:

- Que itens requerem estudo intensivo para eliminação do risco , segurança do projeto, redução da taxa de falha ou redução dos danos.
- Que itens requerem especial atenção durante a produção, alto controle de qualidade e monitoramento constante.
- Requisitos especiais a serem incluídos nas especificações para os fornecedores relativamente a projeto, desempenho,confiabilidade, segurança ou garantia de qualidade.
- Padrões de aceitação a serem estabelecidos para componentes recebidos de subcontratos e parâmetros que devem ser testados intensivamente.
- Onde deverão ser empregados procedimentos especiais, equipamentos de proteção, equipamentos de monitoramento ou sistemas de alarme.
- Onde devem ser aplicados recursos e esforços para prevenção de acidentes de forma mais efetiva. Isto é especialmente importante, visto que cada programa está, geralmente, limitado pela disponibilidade de recursos.

2.3.4 - ÁRVORE DE FALHAS

É um método para análise detalhada de sistemas complexos que, por sua característica gráfica, facilita a visualização de combinação de modos de falha dos componentes que possam comprometer o

desempenho do sistema. Esta característica faz do método um elemento importante para substanciar escolha entre projetos, assim como evidenciar possíveis áreas críticas que necessitem ações corretivas.

Após estabelecido o evento topo, que representa a falha do sistema; a estrutura da árvore vai sendo determinada combinando todos os possíveis modos de falha de componentes que possam resultar neste evento topo ou indesejado.

Dois tipos básicos de relacionamento entre eventos são utilizados. Quando é necessário ocorrer ao menos um entre vários eventos para indisponibilidade de um componente, eles são relacionados pela lógica OU. No caso em que é necessário ocorrer todo um conjunto de eventos para indisponibilidade do componente, eles são relacionados pela lógica E. Existem outros tipos de associações que, entretanto, fogem ao objetivo deste trabalho [2].

Desenvolvida a Árvore de Falhas, a probabilidade de ocorrência do evento topo pode ser determinada, utilizando-se, por exemplo Álgebra de Boole e técnicas dos conjuntos mínimos de corte.

Este método será desenvolvido com mais detalhes no capítulo seguinte.

2.3.5 - DIAGRAMA DE DEPENDÊNCIAS [22]

É um diagrama de blocos esquematicamente mais simples que a árvore de falhas, no qual cada bloco define, por exemplo, uma falha de uma parte de um sistema e as condições relativas a ela e, quando necessário, especifica a frequência de ocorrência. Os blocos são arranjados em série e paralelo re

presentando através de associações E e OU.

Esse diagrama simplificado tem a finalidade de fornecer uma rápida visão da dependência das partes na eficiência do sistema.

Cada bloco do diagrama deve ser desenvolvido posteriormente em outros diagramas de blocos e as probabilidades associadas a cada bloco devem ser acrescentadas de forma que a dependência entre as várias partes do sistema possa ser avaliada rapidamente.

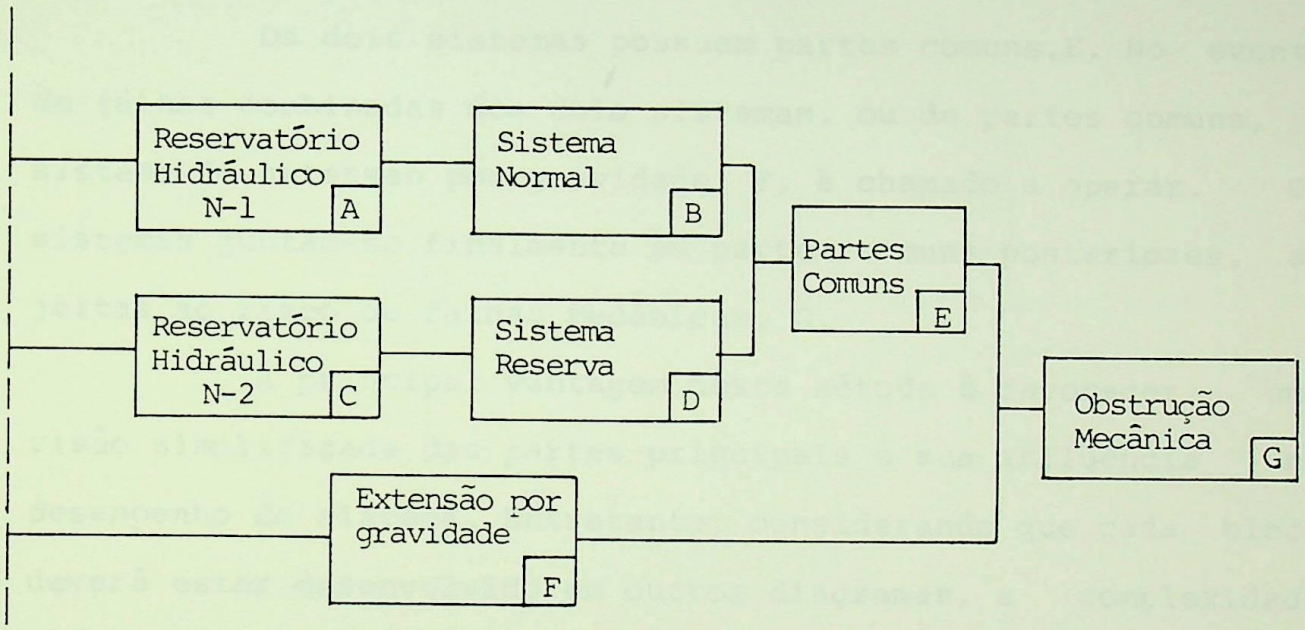


Figura 2.1 - Diagrama de Dependências do Sistema de Acionamento do Trem de Pouso de uma Aeronave.

A figura acima apresenta um exemplo, mostrando uma condição particular de falha de um sistema de acionamento do trem de pouso de nariz de uma aeronave supersônica. A referência no canto inferior direito de cada bloco informa sobre o local onde o bloco poderá ser encontrado mais

detalhado.

O sistema de acionamento em causa tem atuação principal e reserva, supridas por sistemas hidráulicos separados e um abaixamento por gravidade como alternativa.

O diagrama de dependências mostra o sistema de suprimento hidráulico, A, operando o sistema normal, B, havendo um segundo sistema de suprimento hidráulico, C, para operar um sistema de reserva, D. O sistema de reserva somente é chamado a operar no evento de falha do sistema normal.

Os dois sistemas possuem partes comuns,E. No evento de falhas combinadas dos dois sistemas, ou de partes comuns, o sistema de extensão por gravidade, F, é chamado a operar. Os sistemas juntam-se finalmente em partes comuns posteriores, sujeitas ao risco de falhas mecânicas, G.

A principal vantagem deste método é favorecer uma visão simplificada das partes principais e sua influência no desempenho do sistema. Entretanto, considerando que cada bloco deverá estar desenvolvido em outros diagramas, a complexidade da análise não é reduzida.

Utilizando o método de Árvore de Falhas, dispõe-se do mesmo recurso, pois pode-se apresentar as árvores em níveis de profundidade progressivos.

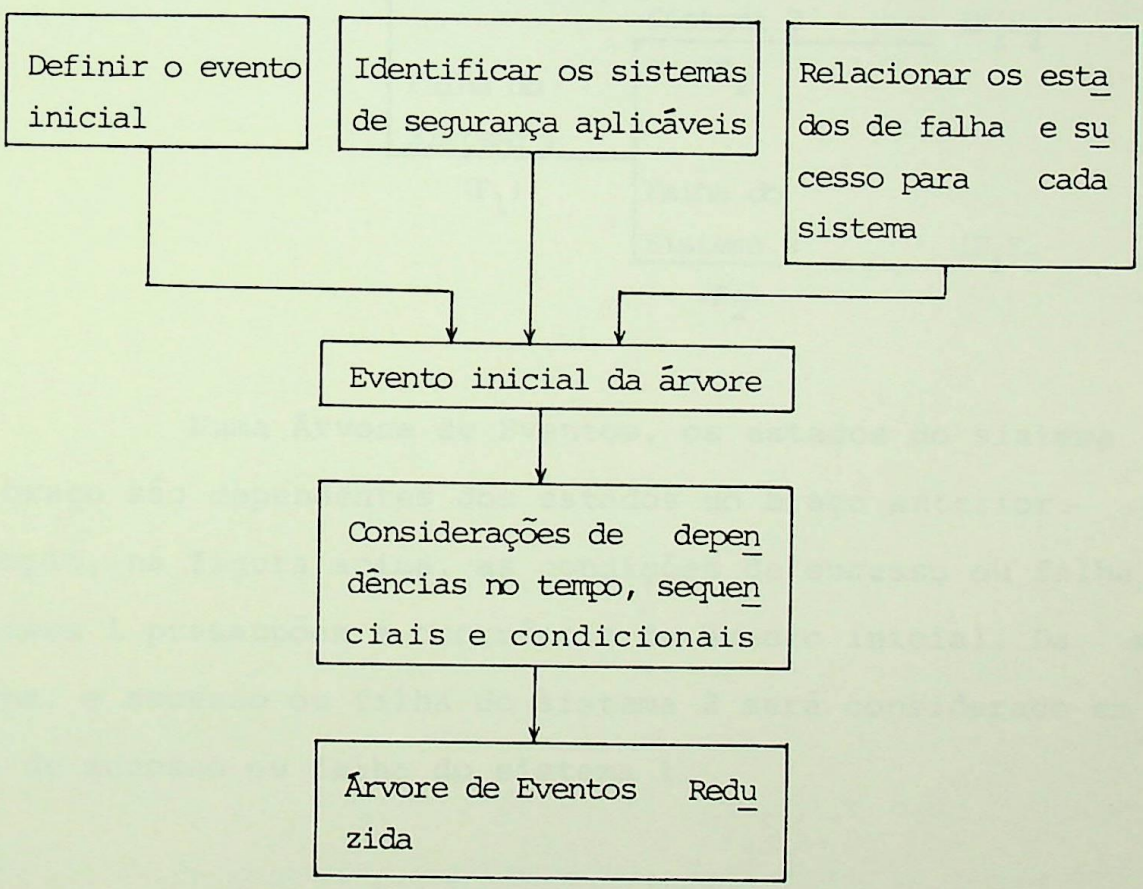
Desta forma, as árvores menos desenvolvidas dão uma visão geral dos principais componentes envolvidos no sistema.

2.3.6 - ÁRVORE DE EVENTOS [27,38]

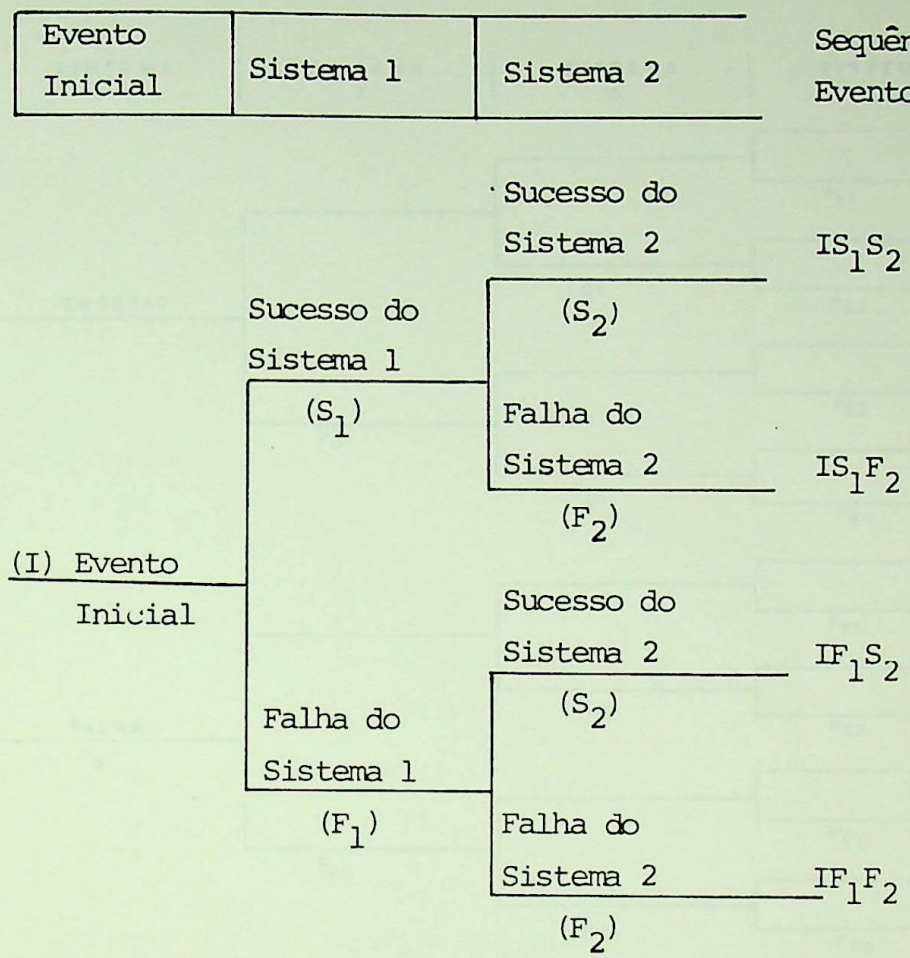
É um método de análise indutiva. A partir de um evento inicial, que pode ser a falha de um componente ou mesmo um acontecimento externo ao sistema, um conjunto de estados de falha e sucesso associados ao evento inicial vai sendo identificado.

Para analisar e avaliar um conjunto de falhas, várias árvores de eventos devem ser construídas.

A sequência de ações para construir uma árvore de eventos pode ser:



EXEMPLO



Numa Árvore de Eventos, os estados do sistema em um braço são dependentes dos estados do braço anterior. Por exemplo, na figura acima, as condições de sucesso ou falha do sistema 1 pressupõem a ocorrência do evento inicial. Da mesma forma, o sucesso ou falha do sistema 2 será considerado em função de sucesso ou falha do sistema 1.

Redução da Arvore de Eventos:

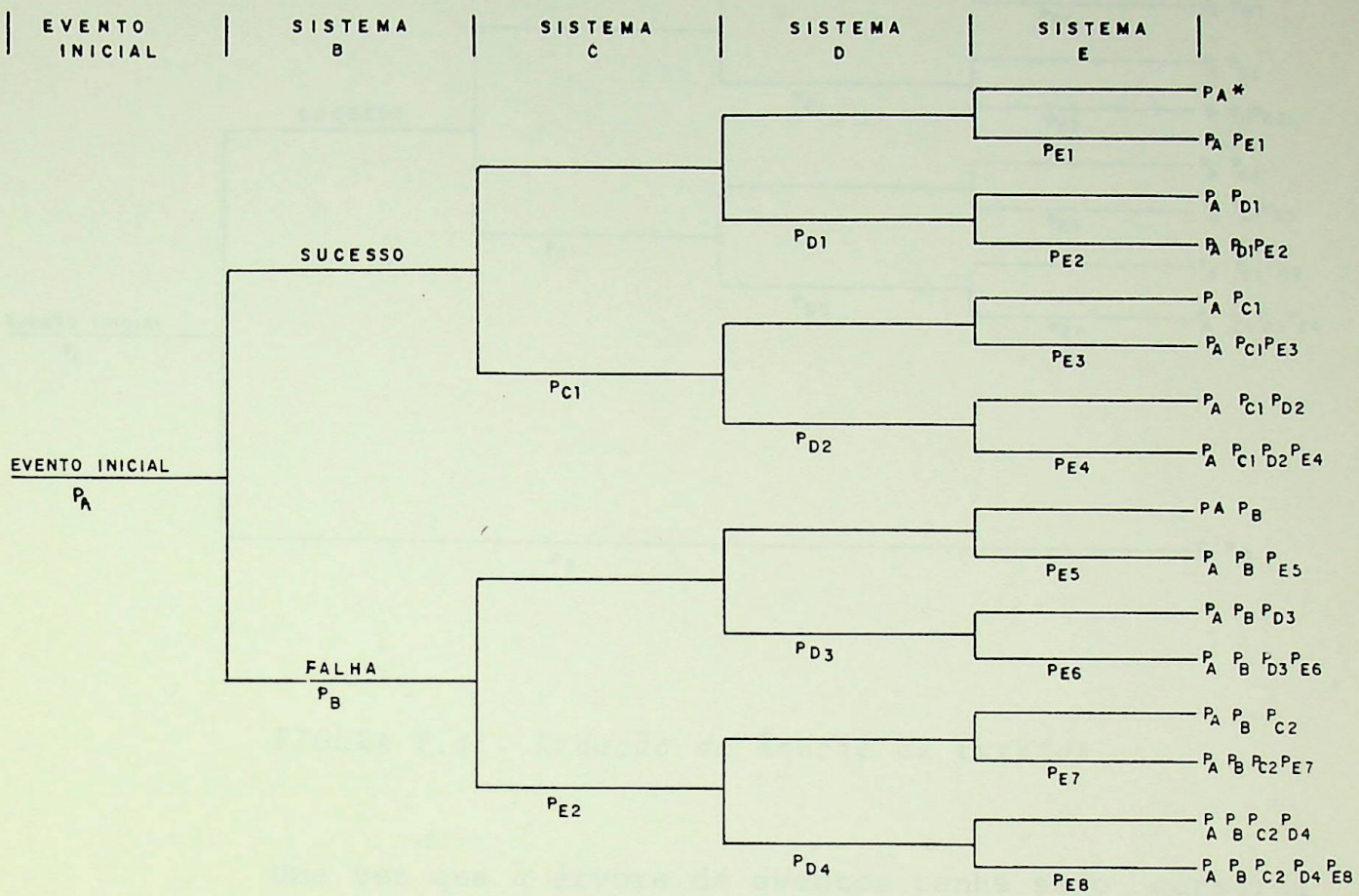


Figura 2.3 - Árvore de Eventos

* Esta é uma aproximação de $P_A(1-P_B)(1-P_{C1})(1-P_{D1})(1-P_{E1})$ no caso em que os valores entre parênteses são muito pequenos.

Na árvore de eventos acima, pode resultar falha do sistema em análise, sempre que o sistema B falhar. Neste caso, os braços que seguem a falha do sistema B são desnecessários e a árvore poderá ser reduzida para a forma a seguir.

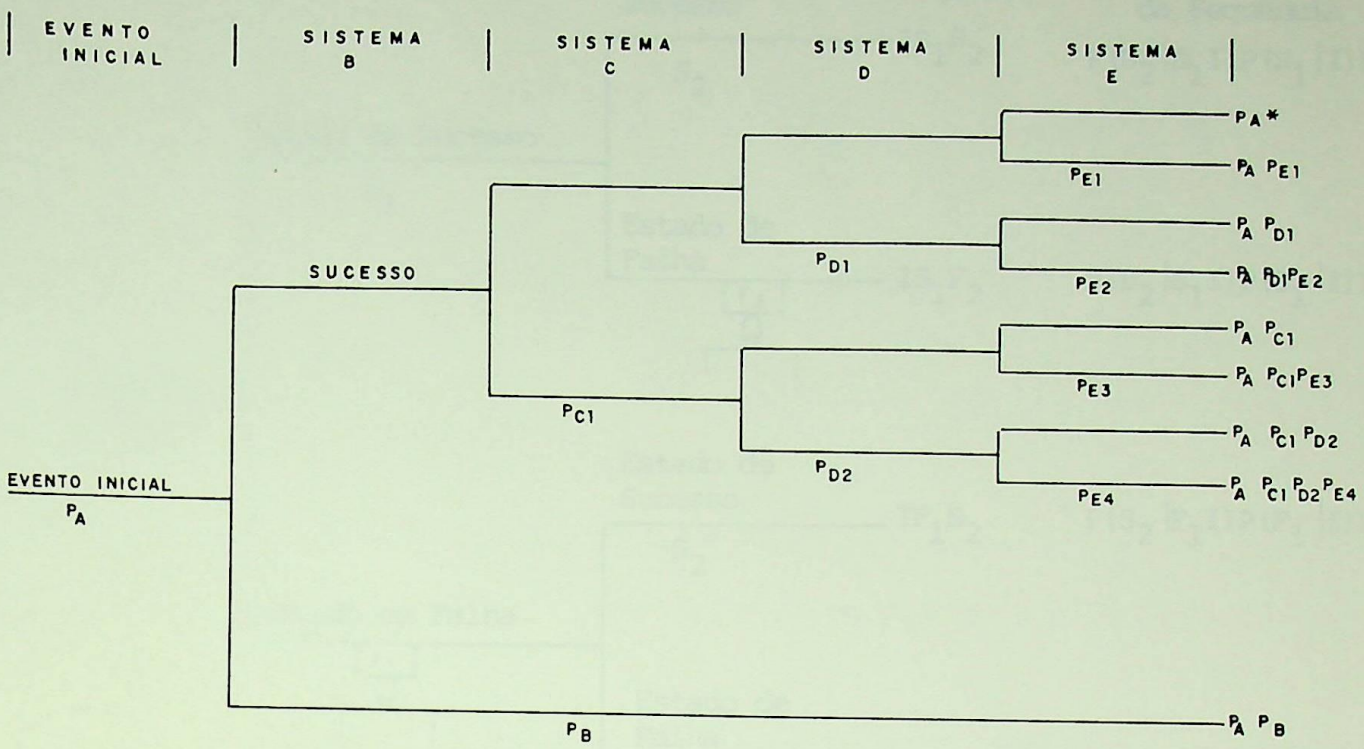
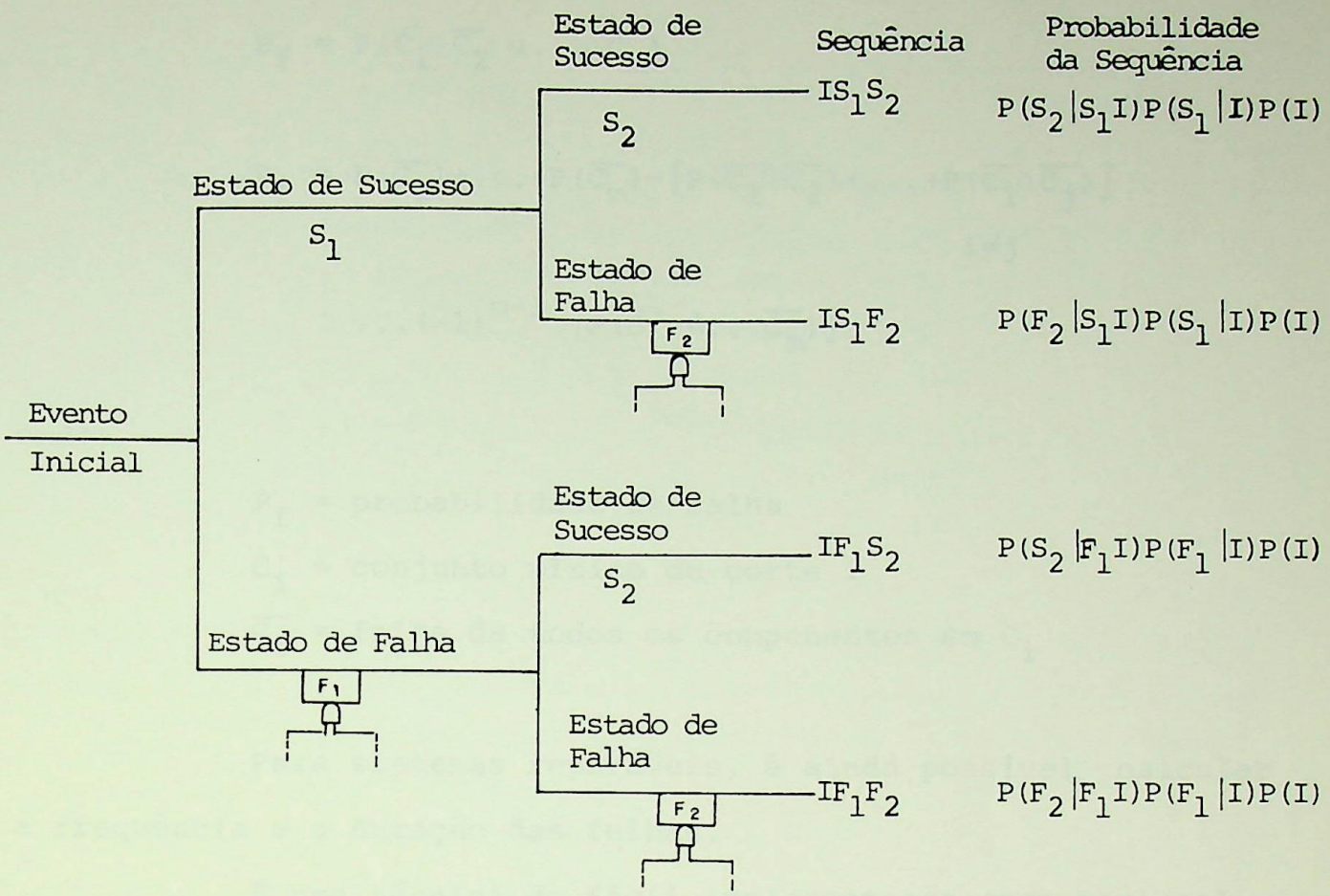


FIGURA 2.4 - Redução da Árvore de Eventos

Uma vez que a árvore de eventos tenha sido construída, de forma que os resultados associados com cada sequência de falhas estejam definidos, pode-se calcular a probabilidade de falha do sistema. Podem ser usadas árvores de falha para calcular as probabilidades condicionais necessárias para cada braço da árvore. Do produto das probabilidades condicionais de cada braço resulta a probabilidade da sequência, conforme pode ser visto na figura da página 32.

Este método aplica-se somente à determinação da probabilidade de ocorrência de associações de eventos sucesso/falha. Não é usualmente dirigido para análise de confiabilidade geral do sistema.



2.3.7 - CONJUNTOS MÍNIMOS DE CORTE (2)

Identificados todos os componentes e sua função no sistema, os conjuntos de corte são formados pelos componentes ou combinação de componentes que, se falharem simultaneamente, levam à falha do sistema.

Destes conjuntos, selecionamos apenas os conjuntos mínimos de corte ou seja, é condição necessária e suficente que todos os componentes de qualquer conjunto de corte falhem para que ocorra falha do sistema.

Uma vez selecionados os conjuntos mínimos de corte, a probabilidade de falha do sistema pode ser determinada da seguinte forma:

$$P_f = P(\overline{C_1} \cup \overline{C_2} \cup \ldots \cup \overline{C_m})$$

$$P_f = P(\overline{C_1}) + \ldots + P(\overline{C_m}) - \left[P(\overline{C_1} \cap \overline{C_2}) + \ldots + P(\overline{C_i} \cap \overline{C_j})\right]_{i \neq j}$$

$$\ldots (-1)^{m-1} \left[P(\overline{C_1} \cap \ldots \overline{C_m})\right]$$

onde,

P_f = probabilidade de falha

C_i = conjunto mínimo de corte i

$\overline{C_i}$ = falha de todos os componentes em C_i

Para sistemas reparáveis, é ainda possível calcular a frequência e a duração das falhas.

É uma técnica de fácil implementação computacional. Porém, para m conjuntos mínimos de corte, o número de termos a ser avaliado é 2^m. Isto pode trazer problemas computacionais , quando o sistema possui muitos componentes.

O método é aplicado para analisar o estado de falha total de componentes, não reunindo informações sobre modos de operação com degradação.

Esta técnica é amplamente utilizada para avaliação quantitativa de árvores de falhas [3,11,71].

2.4 - ANÁLISE COMPARATIVA

A tabela a seguir reune informações básicas sobre os métodos de análise detalhados no texto, de forma a facilitar a escolha do método aplicável a cada sistema e em função dos resultados que se possa desejar.

TABELA 2.1 - Resumo dos Métodos Apresentados e Comparação de Técnicas.

MÉTODO	CARACTERÍSTICAS	VANTAGENS	DESVANTAGENS
Diagrama de Blocos	Associação dos ítens de acordo com a lógica funcional do sistema. Análise qualitativa e quantitativa.	Pode ser aplicado durante a fase inicial de desenvolvimento de sistemas, com informações limitadas. Fácil implementação computacional.	Não permite analisar profundamente os sistemas.
Diagrama de Fluxos de Sinal	Associação dos ítens de acordo com a lógica funcional do sistema. Assemelha-se à representação de circuitos. Análise qualitativa e quantitativa.	Utiliza poucas informações sobre o sistema.	Permite apenas análise de sistemas, sem aprofundamento.
Análise Preliminar de Risco	Análise qualitativa de possíveis situações de risco, inclusive falhas de modo e causa comum.	Favorece a análise e pesquisa de falhas críticas durante fase inicial de projeto.	Aplicação a sistemas que envolvem situações de risco, exigindo análise detalhada.
Análise de Modos de Falha e seus Efeitos	Análise qualitativa. Procedimento sistemático de análise de todos os componentes de um sistema.	Assegura análise profunda do sistema. Reune informações úteis à análise quantitativa de falhas. Necessária para estudar sistemas complexos sujeitos a riscos.	Processo exaustivo de análise de falhas, que consome muito tempo para desenvolvimento e análise.

MÉTODO	CARACTERÍSTICAS	VANTAGENS	DESVANTAGENS
Análise de Criticidade	Análise qualitativa, podendo ser quantificada quando necessário para demonstrar cumprimento de requisitos, por exemplo.	Identifica prioridade de ações de melhoramento do sistema, monitoramento ou padrões de aceitação.	Somente aplicável a sistemas sujeitos a riscos.
Árvore de Falhas	Análise qualitativa detalhada e com características gráficas favoráveis à análise de sistemas. Análise quantitativa que favorece implementação computacional.	Favorece identificação visual de modos de falha e seu relacionamento. Aplica-se tanto a sistemas simples como a sistemas complexos. Pode ser usado para análise de sensibilidades.	Necessita grande quantidade de informações sobre o sistema.
Diagrama de Dependências	Esquematicamente mais simples que as Árvores de Falhas. Relaciona modos de falha sem descer a nível de componentes, para facilitar visualização de dependência entre eles. Análise qualititativa e quantitativa.	Favorece visão simplificada das partes principais do sistema e seu envolvimento.	Necessita grande quantidade de informações sobre o sistema.

MÉTODO	CARACTERÍSTICAS	VANTAGENS	DESVANTAGENS
Árvore de Eventos	Analisa combinação de estados de sucesso e falha de cada componente do sistema. Análise qualitativa e quantitativa.	Considera todas as combinações sucesso e falha no sistema.	Considera somente estados de falha ou sucesso total de componentes no sistema.
Conjuntos Mínimos de Corte	Análise qualitativa e quantitativa.	Identifica condições mínimas de falhas que deverão ser evitadas. Aplicável a todo tipo de sistemas. Pode ser utilizado na quantificação de Árvores de Falhas.	Considera apenas estados de falha total.

2.5 - ESCOLHA DOS MÉTODOS

Dos métodos estudados de análise qualitativa e quantitativa de confiabilidade, os mais profundos e detalhados são o método de Análise de Modos de Falha e seus Efeitos e o método de Árvore de Falhas.

Esses métodos são os mais indicados para análise de sistemas em que o requisito segurança é fundamental, não se podendo negligenciar nenhum detalhe.

Partindo-se do método de Análise de Modos de Falha e seus Efeitos, todos os modos potenciais de falha de cada equipamento devem ser considerados, verificando os possíveis efeitos na operação do sistema. Isso leva o projetista a evitar pontos frágeis em seu sistema e a prever ações de testes e verificações periódicas, assim como funções de proteção e de monitoramento com possíveis alarmes visuais ou sonoros.

Este è um processo de análise qualitativa que reúne informações necessárias sobre o sistema para a construção do modelo matemático para análise quantitativa.

O método de Árvore de Falhas é uma extensão natural da Análise de Modos de Falha e seus Efeitos.

Estabelecido o evento de falha do sistema, num processo do topo para a base, pesquisa-se os eventos e combinações de eventos que resultem em falha do sistema.

Por sua característica gráfica, fornece boa visão do sistema, facilitando a análise dos aspectos críticos. Além disso, é de fácil implementação computacional.

Por todas essas características favoráveis, esses foram os métodos escolhidos para a aplicação proposta neste traba

lho.

São métodos que demandam tempo elevado para aplicação mas, tempo e dinheiro gastos são justificados se consideradas as características de alto risco dos sistemas em análise.

CAPÍTULO 3

MÉTODO DAS ÁRVORES DE FALHAS

3.1 - INTRODUÇÃO

Neste capitulo, são apresentados detalhes do método de Árvore de Falhas para análise de sistemas complexos. As características e técnicas utilizadas na sua geração são descritas, apresentando-se a Análise de Modos de Falhas e seus Efeitos que é um importante instrumento para a avaliação detalhada de sistemas.

São mostradas as formas usuais de análise quantitativa, com descrição do algorítmo adotado.

Um sub-sistema derivado do sistema mais geral analisado no Capítulo 4 é utilizado para ilustrar o método, bem como para análise de sensibilidades e para o cálculo da taxa de falha de eventos intermediários e do evento topo, comparando-se os resultados obtidos.

3.2 - PRINCIPAIS CARACTERÍSTICAS DO MÉTODO

Os aspectos principais desta técnica que podem ser encarados como vantagens são:

- Forçar o analista a procurar exaustivamente eventos de falha de uma maneira dedutiva.
- Fornecer uma visão global de como o sistema pode funcionar mal, permitindo fácil compreensão do sistema por outras pes

soas além do projetista.

- Realçar aspectos críticos do comportamento do sistema.
- Fornecer referência para avaliação de modificações.
- Fornecer base sistemática para a análise quantitativa.

Como desvantagem principal, pode-se considerar o tempo excessivo exigido para uma análise detalhada de sistemas complexos.

3.3 - GERAÇÃO DAS ÁRVORES DE FALHAS

Na literatura especializada, encontra-se pouca informação sobre a construção sistemática de árvores de falhas. Os exemplos encontrados, são frequentemente selecionados para demonstrar o que um algorítmo particular pode fazer, sendo comumente apresentados como produtos acabados, seguidos apenas de explicações sobre seus objetivos e seus detalhes. Contudo, o maior problema da análise de confiabilidade e segurança, é exatamente a construção da árvore.

Desses exemplos pobres em detalhes, pode-se ter a impressão errada de que a análise de confiabilidade consiste principalmente em dominar um conjunto de "software" que gere e avalie a árvore de falhas automáticamente. A confiabilidade resultaria de alguma maneira intuitiva para transformar idéias em árvores de falhas acabadas [21].

O primeiro passo para construção de uma árvore de falhas é a caracterização de falha do sistema, ou do evento topo, que é o objetivo da análise. Todo o cuidado deve ser tomado para definí-lo; além disso, para tornar a árvore compreensível, o analista deve descrever as considerações feitas para definir o sis

tema e a árvore.

Encontra-se aí a primeira dificuldade. Para um mesmo sistema, a situação que representa sua falha pode não ser necessáriamente única.

Alguns sistemas críticos ou indispensáveis para o sucesso de uma determinada missão são projetados para funcionar em situações de emergência com limitações pré-estabelecidas , durante parte do tempo da missão. Dessa forma, é necessário estabelecer o evento topo para situações de possível emergência ou com vários níveis de limitações. Isso ocasiona o desdobramento da árvore principal em sub-árvores ou ramos que, convenientemente agrupados, levarão à análise do sistema e da confiabilidade da missão especificada.

O passo seguinte é identificar as causas diretas da ocorrência do evento topo, ou seja, determinar os eventos contribuintes de ordem mais alta. Estes são também chamados de eventos intermediários.

Existem, pelo menos, quatro possibilidades:

- Nenhuma entrada é recebida pelo equipamento, como sinal para operar.
- O equipamento experimenta alguma falha, de modo que não operará.
- Há um erro humano, tal como falha ao atuar uma chave ou instalação inadequada do equipamento.
- Algum evento externo pode ter ocorrido que impeça a operação do equipamento, tal como falha de causa comum.

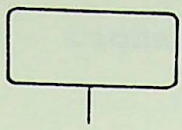
Em continuação, deve-se aprofundar a análise dos eventos de falha de ordem mais alta, buscando os relacionamentos lógicos de eventos de ordem mais baixa que possam causá-los.

Este procedimento deve ser repetido até que sejam atingidos os componentes mais simples do sistema ou até onde as informações estejam disponíveis. Os eventos mais desenvolvidos são denominados eventos básicos.

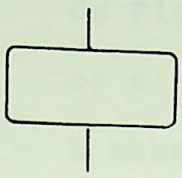
A representação gráfica do relacionamento do evento topo com as de ordem mais baixa que vão sendo identificados é feita utilizando-se símbolos apropriados.

A tabela 3.1 reune os principais e que são largamente utilizados.

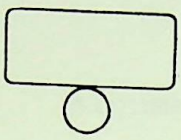
TABELA 3.1 - SIMBOLOGIA USADA NA ÁRVORE DE FALHAS



EVENTO TOPO - ou evento indesejado. Representa a falha do sistema.



EVENTO INTERMEDIÁRIO - Decorre da combinação de outros eventos.



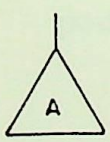
EVENTO BÁSICO - ou mais desenvolvido. Constitue o nível final de desenvolvimento que se pretende atingir na análise da falhas.



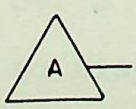
PORTÃO E - Operação interseção de eventos - o evento saída ocorre se e somente se todas as entradas ocorrerem.



PORTÃO OU - Operação união de eventos - o evento saída ocorre se uma ou mais das entradas ocorrerem.



TRIÂNGULO DE ENTRADA - Indica que haverá continuação da árvore onde for encontrado o triângulo de saída correspondente.



TRIÂNGULO DE SAÍDA - Braço de árvore que deverá ser considerado a partir do triângulo de entrada. Usado para evitar repetições do ramo ou para continuar a árvore em folhas seguintes.

Para construção da árvore de falhas de um sistema complicado, é necessário primeiro compreender como o sistema funciona.

Um Diagrama Funcional do Sistema, ou um Diagrama de Fluxo, pode ser usado para retratar os caminhos pelos quais os sinais são transmitidos entre os componentes que constituem o sistema; os Diagramas de Blocos de Confiabilidade são, também, bastante usados.

Um segundo diagrama, o Diagrama Lógico Funcional, é algumas vezes necessário para explicar os relacionamentos dos componentes.

Uma terceira ferramenta, frequentemente usada para explicar os modos de falha do sistema é a Análise de Modos de Falha e seus Efeitos (FMEA).

Duas regras devem ser observadas:

- Somente após o funcionamento do sistema ser completamente compreendido, o analista deve construir a árvore de falhas.
- Para sistemas mais simples, os diagramas lógico e funcional ou a FMEA são desnecessários e a construção da árvore de falhas pode começar imediatamente.

Algumas vezes entretanto, durante o desenvolvimento da FMEA pode ocorrer que, devido à complexidade e/ou o estágio inicial de desenvolvimento do projeto, não seja possível conhecer o efeito de determinado modo de falha de algum equipamento no sistema. Neste caso, a análise de falhas deverá ser acompanhada de ensaios para verificação. É claro que, em se tratando de falhas, isso só é possível no caso de ensaios não destrutivos ou se os mesmos não acarretarem falta de segurança de pessoas

ou se não comprometerem a integridade do ambiente.

Esse foi um dos problemas encontrados durante o desenvolvimento da FMEA do sistema elétrico de uma aeronave, tal como descrito no capítulo seguinte deste trabalho.

Um outro problema relevante é o estabelecimento das taxas de falha para os modos de falha analisados.

Frequentemente, é disponível uma taxa de falha total para o componente. Essa informação, contudo, não é suficiente para um estudo de confiabilidade pelo método das Árvores de Falhas. São necessárias as taxas de falhas para os modos de falha que estão sendo considerados.

Há várias razões para a inexistência dos dados requeridos, que podem ser resumidas em ausência de recursos tanto de pessoas como de dinheiro ou de tempo [29].

Frequentemente, quando os dados se tornam por fim disponíveis, a tecnologia de produção do equipamento evoluiu. E, se algumas mudanças podem ser insignificantes, outras podem afetar consideravelmente os mecanismos de falha, modos de falha, taxas de falha e seu relacionamento com a severidade ambiental. Assim, algumas vezes, bons dados estarão disponíveis para equipamentos obsoletos. A frase "... equipamentos similares..." raramente é aplicável. Por esta razão, os analistas de confiabilidade devem ser realistas e tratar os dados com o ceticismo que eles merecem.

3.3.1 - ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

É um procedimento sistemático para identificar os modos de falha e avaliar suas consequências.

Os objetivos da FMEA são [20] :

- Apoiar a seleção de projetos alternativos com alta confiabilidade e alto potencial de segurança durante a fase inicial.
- Assegurar que todos os modos de falha concebíveis e seus efeitos na operação do sistema sejam considerados.
- Listar falhas potenciais e identificar a abrangência de seus efeitos.
- Desenvolver critérios para o planejamento de testes e para a verificação geral dos sistemas.
- Fornecer bases para o cálculo da confiabilidade quantitativa e para a análise de disponibilidade.
- Fornecer documentação histórica para referência futura e considerações de mudança de projeto.
- Fornecer dados de entrada para estudos de influência mútua entre sistemas.
- Fornecer bases para estabelecer prioridade de ações corretivas.
- Apoiar a avaliação objetiva de requisitos de projetos relativos à redundância, sistemática de deteção ou indicação de falhas e de proteção.

3.3.1.1 - ASPECTOS RELEVANTES

Uma análise completa de confiabilidade requer dados exaustivos de entrada que incluam propriedades materiais, detalhes de projeto e taxas de falha dos componentes. Contudo, não é

necessário esperar até que todos esses dados sejam conhecidos se for limitado inicialmente o escopo da análise à preocupação de como o componente falha e às consequências da falha.

A FMEA pode ser realizada com informações limitadas do projeto porque não é primariamente dependente das taxas de ocorrência ou frequência de falhas.

Pode ser parte integral da avaliação de um projeto e ser periodicamente atualizada para refletir mudanças no projeto ou aplicação . Uma FMEA atualizada tem grande peso nas revisões de projeto, inspeções ou outros pontos de revisão do sistema e tem sido usada como parte do procedimento de seleção de alternativas.

As fases de desenvolvimento de um novo sistema em que a FMEA tem importância são:

- Formulação ou seleção de propostas.
- Projeto preliminar ou esquema básico.
- Complementação de parte detalhada dos projetos.
- Programas de melhoramento de projetos.

As questões básicas a serem respondidas são as seguintes:

- Como pode cada parte, concebivelmente, falhar?
- Que mecanismos podem produzir esses modos de falha?
- Que efeitos podem resultar da ocorrência das falhas?
- A falha torna o sistema inseguro?
- Como são detetadas as falhas?
- Que provisões inerentes são incorporadas ao projeto para compensar a ocorrência das falhas?

3.3.1.2 - ETAPAS DE CONSTRUÇÃO

A profundidade com que se realizam os passos preparatórios é função da complexidade do sistema e da experiência que se tenha como sistemas similares . Cada um dos passos seguintes é essencial, embora a profundidade possa ser variável:

- Definição do sistema e da sua finalidade.
- Descrição da operação do sistema.
- Identificação das categorias das falhas.
- Descrição das condições ambientais.

O sistema deve ser descrito de acordo com sua finalidade.

Estabelecida a função pretendida, devem ser fornecidas as características de projeto. Todos os componentes deverão ser relacionados, definindo exigências técnicas e possíveis interações com outros sistemas.

O ponto importante é que o analista deve conhecer , claramente, o que vai analisar; ele estará então habilitado a definir funções de interação entre componentes e sistemas.

Quanto mais complexo o sistema, maior a necessidade de definí-lo cuidadosamente.

Um diagrama funcional pode ser usado para mostrar as interdependências entre sub-sistemas de forma que os efeitos das falhas possam ser estabelecidos.

Uma vez que o sistema e suas caracteristicas operacionais estejam definidas e compreendidas, a FMEA pode ser desenvolvida. Como estabelecido previamente, a quantidade de informação necessária para alcançar esse ponto é função da complexidade do sistema, da experiência e do conhecimento da pes

soa que realiza esta análise.

3.3.1.3 - UM MODELO [74]

As diretrizes para desenvolver uma FMEA típica podem ser vistas na tabela 3.2, cujas informações são descritas a seguir:

1. Número de Referência - usado para identificar cada modo de falha considerado. Pode ser formado pelo código de diagramas ou de identificação do componente.
2. Tipo de Falha - devem ser indicados todos os modos possíveis de falhas.
3. Condições que Modificam os Efeitos da Falha - se, diferentes condições ambientais, presença de outra falha ou diferentes fases da missão, tornarem diferentes os efeitos de uma falha, essas condições devem ser analisadas individualmente.
4. Efeito da Falha Condicionado pelo Item Anterior - indicar para cada modo de falha, os seus efeitos
   - Sobre a operação do sub-sistema a que pertence.
   - Sobre a operação do sistema, inclusive possíveis interações com outros sub-sistemas.
5. Grau - o objetivo é penalizar o nível de gravidade dos modos de falha que estão sendo descritos.

   São usados os códigos:

   A - Catástrofe quase certa.

   B - Pode haver consequências perigosas, não necessariamente no sub-sistema de interesse.

   C - O acidente pode ser evitado com a intervenção do opera

dor ou do especialista e/ou usando sub-sistemas de reserva eventualmente existentes.

D - Produz efeito sobre a eficácia da missão, mas não necessariamente implica no cancelamento da mesma.

E - Não tem efeito sobre a segurança e sobre a eficácia da missão.

6. Descoberta ou Aviso de Falha - indicar como a falha pode ser descoberta. Se há indicação através de instrumentos, se pode ser percebida pelo comportamento do sistema ou ainda se a falha só pode ser descoberta por especialistas.

7. Ações a Serem Tomadas pelo:

Operador - indicar se alguma ação do operador pode remediar a falha, por exemplo, selecionando um sistema alternativo ou trocando a missão, ou outro tipo de ação.

Especialista - estas informações deverão visar a análise de mantenabilidade. Devem ser informações do tipo:

- remoção e conserto
- reparos
- substituição

8. Taxa de Falha Estimada - indicar os valores estimados para cada modo de falha considerado.

9. Fonte - indicar a fonte de dados utilizados, por exemplo , dados do construtor, dados históricos de outros equipamentos similares.

10. Observações - esta coluna é reservada para quaisquer particularidades que devam ser salientadas.

SISTEMA:

SUBSISTEMA:

EQUIPAMENTO:

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

IDENTIFICAÇÃO DO ITEM:

FUNÇÃO:

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sub-sistema b. No sistema	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA ($x10^{-6}h$)	9. FONTE	10. OBSERVAÇÕES
						Pelo Operador	Pelo Especialista			

TABELA 3.2 - FMEA

3.4 - ANÁLISE QUANTITATIVA

Após construída a árvore de falhas, deseja-se utilizar a informação contida em sua estrutura lógica para quantificar os fenômenos de interesse.

Um valor importante é a probabilidade de ocorrência dos eventos básicos. Estabelecendo-se a função de confiabilidade aplicável, pode-se determinar esse parâmetro.

Identificando a função de estrutura da árvore, pode-se combinar convenientemente as probabilidades de ocorrência dos eventos básicos para determinar a probabilidade de ocorrência do evento topo ou indesejado.

Outros parâmetros poderão ser analisados, tais como as taxas de falha de eventos intermediários e do evento topo.

Um estudo de sensibilidades também pode ser desenvolvido, utilizando-se para tal a estrutura da árvore.

3.4.1 - FUNÇÃO CONFIABILIDADE

Para estabelecer o modelo matemático a ser utilizado na análise de confiabilidade, torna-se necessário calcular a probabilidade de ocorrência de certos eventos ao longo do tempo. A conceituação apresentada a seguir permite estabelecer a fórmula de cálculo de tais probabilidades.

Submetendo-se um número N_o de componentes a teste, deverá haver, após um tempo t, $N_s(t)$ componentes sobreviventes e $N_f(t)$ componentes falhados, sendo que $N_o = N_s(t) + N_f(t)$ permanece constante durante o teste.

A confiabilidade ou probabilidade de sobrevivência é, em qualquer instante durante o teste, calculada por:

$$R(t) = \frac{N_s(t)}{N_o}$$

$$= \frac{N_s(t)}{N_s(t) + N_f(t)}$$

onde:

$N_s(t)$ ou $N_f(t)$ são funções do tempo.

$R(t)$ dá a probabilidade de um componente sobreviver quando operado por um período de tempo t.

Analogamente, pode-se definir a probabilidade de falha

$$Q(t) = \frac{N_f(t)}{N_o}$$

$$= \frac{N_f(t)}{N_s(t) + N_f(t)}$$

É evidente que $R+Q = 1$, pois

$$\frac{N_s(t) + N_f(t)}{N_s(t) + N_f(t)} = 1$$

Os eventos sobrevivência do componente e falha do componente são complementares e são eventos mutuamente exclusivos.

Como $N_s(t) = N_o - N_f(t)$, pode-se escrever

$$R(t) = \frac{N_s(t)}{N_s(t) + (N_f(t)}$$

$$= \frac{N_o - N_f(t)}{N_o}$$

$$= 1 - \frac{N_f(t)}{N_o}$$

Diferenciando, vem

$$\frac{dR}{dt} = \frac{d(1-N_f(t)/N_o)}{dt}$$

$$= - \frac{1}{N_o} \cdot \frac{d\ N_f(t)}{dt}$$

ou

$$\frac{d\ N_f(t)}{dt} = - N_o \frac{dR}{dt}$$

e

$$\frac{d\ N_f(t)}{dt} = \frac{d(N_o - N_s(t))}{dt}$$

$$= \frac{-\ d\ N_s(t)}{dt}$$

O termo $\frac{d\ N_f(t)}{dt}$ pode ser interpretado como o número de componentes que falham em média por unidade de tempo dt, entre o tempo t e t+dt.

Ao fim do tempo t ainda existem $N_s(t)$ componentes em teste; portanto, destes, $dN_f(t)$ componentes falharão em dt.

Normalizando em relação a $N_s(t)$, obtemos o que chamamos de taxa de falha para um componente.

$$\lambda = \frac{1}{N_s(t)} \cdot \frac{d\ N_f(t)}{dt}$$

$$= - \frac{N_o}{N_s(t)} \cdot \frac{dR}{dt}$$

$R = \frac{N_s(t)}{N_o}$ ou $\frac{N_o}{N_s(t)} = \frac{1}{R}$. Substituindo na equação acima

$$\lambda = - \frac{1}{R} \cdot \frac{dR}{dt}$$ que é a expressão mais geral.

Daí, $\lambda dt = - \frac{dR}{R}$

$$\int_o^t \lambda dt = - \int_1^R \frac{dR}{R}$$

$$= - \ell nR$$

ou

$$\ell nR = - \int_o^t \lambda dt$$

Resolvendo para R e conhecendo que em t=0, R=1

$$R(t) = e^{- \int_o^t \lambda dt}$$

Nesta equação, R(t) descreve matemáticamente a confiabilidade de maneira mais geral e aplica-se a qualquer distribuição dos tempos de funcionamento até a falha.

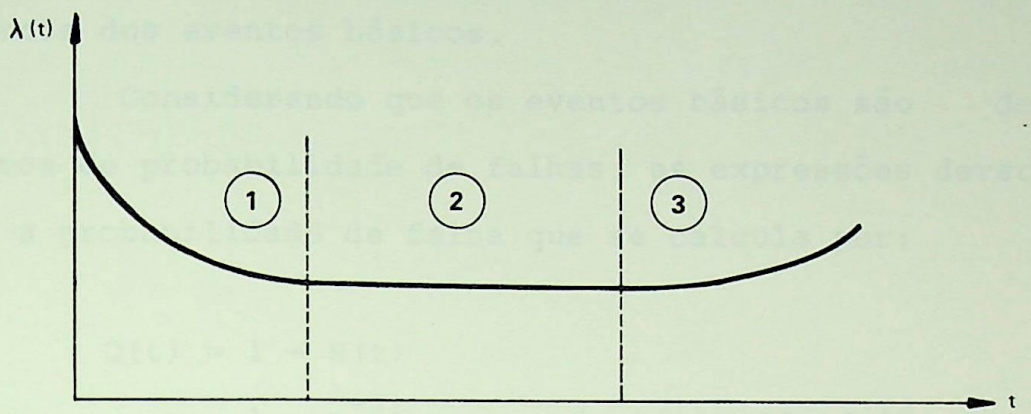
Quando considera-se λ constante, vem:

$$- \int_o^t \lambda \, dt = - \lambda t$$

Resultando na conhecida fórmula

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

Para muitos equipamentos a variação da taxa de falha com o tempo de vida do equipamento é tipicamente descrita pela conhecida CURVA EM BANHEIRA.



Deste comportamento, observa-se três regiões distintas, respectivamente:

1. Mortalidade Infantil
2. Vida Útil
3. Envelhecimento.

Pode-se observar que na região de vida útil a taxa de falha mantém-se aproximadamente constante com o tempo. Se os equipamentos são utilizados nesta faixa de vida útil, pode-se considerá-los como tendo taxa de falha constante.

Isto é conseguido na prática, utilizando testes funcionais para detetar e eliminar os componentes que permanecem no período de mortalidade infantil e substituir aqueles que estão prestes a entrar na região de envelhecimento.

Desta forma, a confiabilidade pode ser calculada utilizando a expressão:

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

3.4.2 - FUNÇÃO DE ESTRUTURA

Foi definida, no ítem anterior, a função de confiabilidade que pode ser usada para determinação da probabilidade de ocorrência dos eventos básicos.

Considerando que os eventos básicos são descritos em termos de probabilidade de falhas, as expressões deverão envolver a probabilidade de falha que se calcula por:

$$Q(t) = 1 - R(t)$$
$$= 1 - e^{-\lambda t}$$ quando a taxa de falha for constante.

A questão agora é a determinação da probabilidade de ocorrência do evento topo de uma árvore de falhas, a partir da probabilidade de ocorrência dos eventos básicos.

Associando ao evento topo uma variável binária $\psi(\vec{y})$, de modo que

$$\psi(\vec{y}) = \begin{cases} 1, \text{ se o evento topo ocorre} \\ 0, \text{ se o evento topo não ocorre} \end{cases}$$

onde

$\vec{Y} = (y_1, y_2, \ldots, y_n)$ é o vetor indicador dos eventos associados ao topo e da mesma forma,

$$y_i = \begin{cases} 1, \text{ se o evento i ocorre} \\ 0, \text{ se o evento i não ocorre} \end{cases}$$

A função $\psi(\vec{y})$ é a função de estrutura da árvore de falhas.

Seja $\phi(x)$ uma função de estrutura de eventos intermediários.

A combinação de eventos básicos através de um portão OU, significa que um evento intermediário ocorre se pelo menos um dos eventos básicos ocorrer. Esta associação resulta na função de estrutura

$$\phi = \coprod_{i=1}^{n} x_i \quad \text{(conforme item 2.2.1)}$$

A combinação de eventos básicos através de um portão E, significa que um evento intermediário ocorre somente se todos os eventos básicos ocorrerem.

Esta associação resulta na função de estrutura

$$\phi(x) = \prod_{i=1}^{n} x_i$$

A função de estrutura de uma árvore de falhas será resultado da combinação lógica dos portões E e OU que a compõem.

A árvore de falhas pode ser representada com seus cortes mínimos, conforme descrito posteriormente, conectados ao evento topo através de um portão OU. Visto que em cada corte mínimo os eventos estão ligados por portões E, a função de estrutura da árvore pode ser escrita

$$\psi(\vec{Y}) = \coprod_{j=1}^{n} \prod_{i \varepsilon k_j} Y_i$$

3.4.3 - FUNÇÃO DE PROBABILIDADE [23,25]

Supondo que o estado do i-ésimo componente, x_i, é aleatório com

$$P(x_i=1) = Q_i$$

$$= E\left[x_i\right] \quad \text{para } i = 1,2,\ldots,n$$

sendo

Q_i a probabilidade do componente i falhar, ou não confiabilidade de x_i

$E[x_i]$ o valor esperado da variável aleatória x_i

Analogamente, a não confiabilidade do sistema é dada por

$$P\left[\phi(x) = 1\right] = h = E\left[\phi(x)\right]$$

Considerando que os componentes são estatisticamente independentes, pode-se representar a não confiabilidade do sistema em função da não confiabilidade dos componentes

$$h = h(Q)$$

sendo

$h(Q)$ a função de não confiabilidade da estrutura ϕ.

Como consequência, para a função de estrutura

$$\phi(x) = \prod_{i=1}^{n} x_i$$

a função de não confiabilidade é

$$h(\mathbf{Q}) = \prod_{i=1}^{n} Q_i$$

Da mesma forma, para a função de estrutura

$$\phi = \coprod_{i=1}^{n} x_i$$

a função de não confiabilidade é

$$h(\mathbf{Q}) = \coprod_{i=1}^{n} Q_i$$

Isto significa que, neste caso, para obter a função de probabilidade, basta substituir na função de estrutura, cada x_i pelo respectivo Q_i. O processo exige que a função de estrutura esteja escrita em sua forma booleana exata, isto é, que não apareçam potências de x_i.

3.4.4 - APROXIMAÇÃO DO EVENTO RARO [37]

Conforme visto, o procedimento geral para a passagem da função de estrutura para a função de probabilidade de ocorrência do evento topo implica na necessidade do desenvolvimento da função de estrutura.

A explicitação de todas as parcelas da função de estrutura de uma árvore torna-se praticamente inviável quando os portões OU contêm grande número de eventos básicos resultando da expressão

$$\phi(x) = x_1+x_2+\ldots+x_n - \Sigma \text{ comb. dois a dois}$$

$$+ \Sigma \text{ comb. três a três} +\ldots+ (-1)^{n-1}$$

$$x_1 . x_2 \ldots x_n$$

Deve-se levar em conta que portões E podem exigir que expressões como esta sejam multiplicadas.

A equação acima quando transformada em expressão probabilística, fornece exatamente o mesmo número de parcelas, ou seja,

$$h(Q) = Q_1+Q_2+\ldots+Q_n - \Sigma \text{ comb. dois a dois} + \ldots$$

Este problema pode ser razoavelmente simplificado se for utilizada a aproximação do evento raro, que consiste em considerar apenas os termos de ordem mais baixa na função de estrutura, desprezando os termos de ordem superior. Considerando que os valores de probabilidade de falha são pequenos, os produtos serão ainda menores que as probabilidades individuais.

Desta forma, para um portão OU com n eventos básicos, tem-se a função de estrutura

$$\phi(x) \simeq \sum_{i=1}^{n} x_i$$

e a função de não confiabilidade equivalente será

$$h(Q) \simeq \sum_{i=1}^{n} Q_i$$

Esta aproximação é tanto melhor quanto menores forem as probabilidades de ocorrência dos eventos básicos (eventos raros), fornecendo valores satisfatórios para $Q<0,1$.

Em qualquer circunstância, a aproximação do evento raro fornece sempre um limite superior para a probabilidade de falha do sistema sendo, portanto, uma aproximação conservativa.

3.4.5 - AVALIAÇÃO DA ÁRVORE DE FALHAS ATRAVÉS DE SEUS CORTES MÍNIMOS

Um algorítmo bastante conhecido e largamente utilizado para avaliação de árvores de falhas foi desenvolvido inicialmente por Jerry Fussel e William Vesely [11] .

Este algorítmo pode ser usado manualmente para árvores de falhas simples e constituídas por poucos elementos. Entretanto, à medida que aumenta a complexidade e o número de portões e eventos, torna-se conveniente ou necessária sua implementação em computador.

Os princípios básicos desse algorítmo são dois. O portão E sempre aumenta o tamanho do conjunto de corte, enquanto o portão OU aumenta o número de conjuntos de corte. Para apresentar o algorítmo é desenvolvido um exemplo que contribui por si mesmo para entender o processamento.

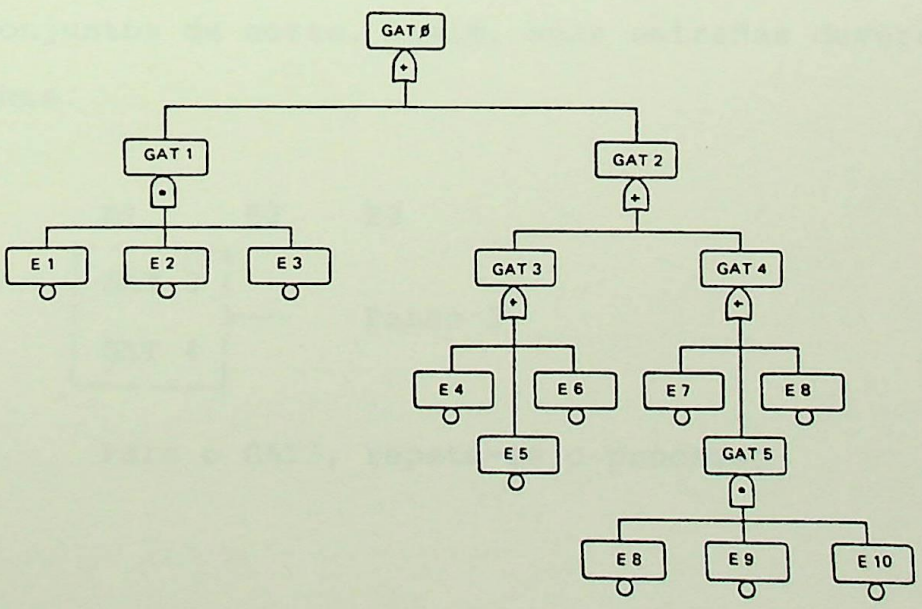
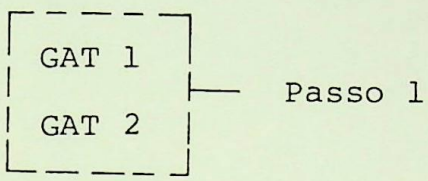


FIGURA 3.1 - Árvore de Falhas

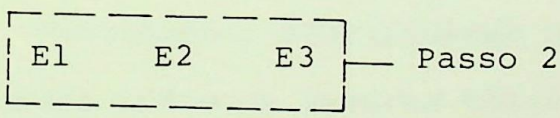
Neste exempo, os eventos intermediários estão sendo representados como portões (GATϕ, GAT1, etc.) e os eventos básicos como numerais precedidos pela letra E. O evento topo foi representado como GATϕ.

Iniciando por GATϕ, verifica-se ser um portão do tipo OU.

Pela lógica do algorítmo ,suas entradas deverão ser escritas em novas linhas. As entradas podem ser novos portões e/ou eventos básicos.

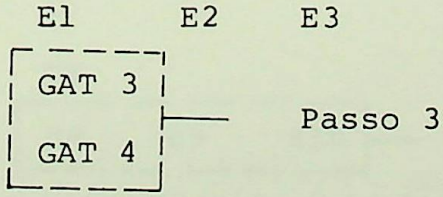


Para continuar a pesquisa da estrutura da árvore , analisando GAT1 , um portão E, deve-se escrever suas entradas como novas colunas.

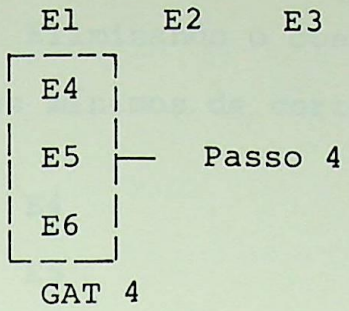


GAT 2

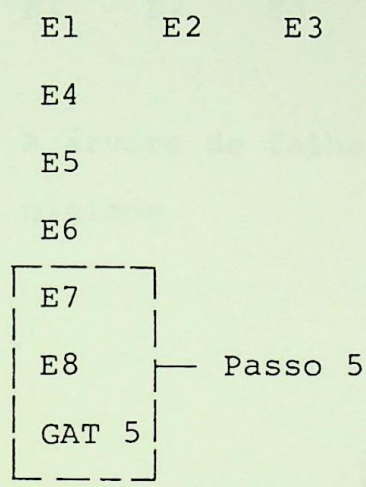
Tendo atingido eventos básicos neste ramo, pode-se pesquisar o próximo portão. O GAT2, do tipo OU, aumenta o número de conjuntos de corte. Assim, suas entradas deverão ser novas linhas.



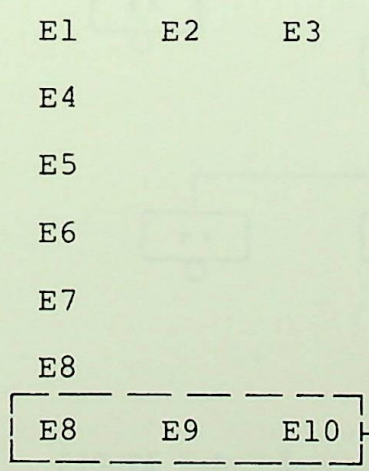
Para o GAT3, repete-se o processo



Novamente, para GAT4



Finalmente, substituindo o portão GAT 5, do tipo E, foram atingidos todos os eventos básicos da árvore, resultando



A combinação de eventos é formada por conjuntos de corte, que não são mínimos porque nesta árvore o evento E8 foi repetido duas vezes.

Eliminando o conjunto de corte não mínimo, obtem-se os conjuntos mínimos de corte.

E4

E5

E6

E7

E8

E1 E2 E3

A árvore de falhas, agora, pode ser representada por seus cortes mínimos

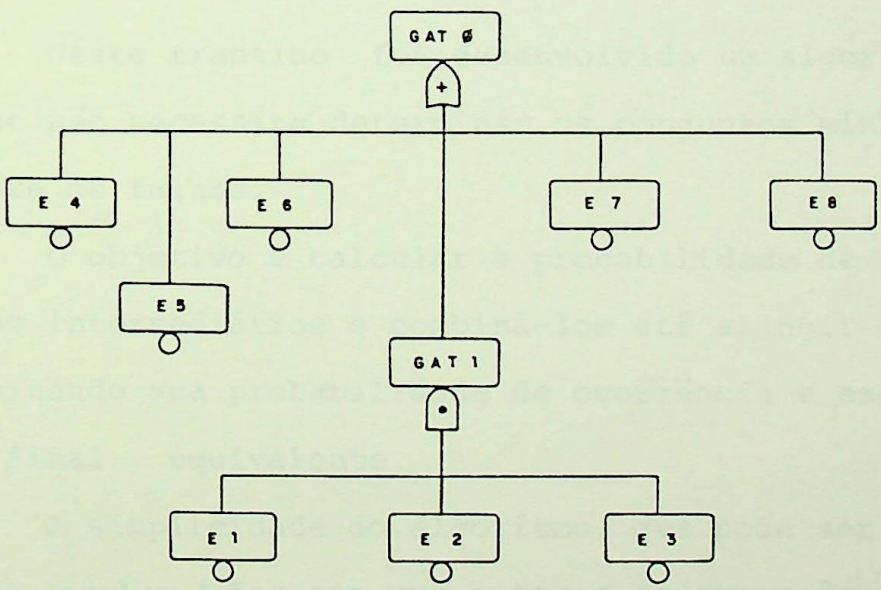


FIGURA 3.2 - Árvore de Falhas Representada por Cortes Mínimos

A árvore de falhas representada por seus cortes mínimos evidencia os eventos críticos que causam diretamente a ocorrência do evento topo.

Comparando as figuras 3.1 e 3.2, pode ser observado que a segunda apresenta-se de forma mais simples e otimizada. Para determinar a probabilidade de ocorrência do evento topo, após terem sido determinados os conjuntos mínimos de corte,é suficiente aplicar a expressão da função de probabilidade:

$$h(Q) = \coprod_{j=1}^{n} \prod_{i \varepsilon k_j} Q_i$$

3.4.6 - AVALIAÇÃO DA ÁRVORE DE FALHAS ATRAVÉS DO CÁLCULO DAS PROBABILIDADES DOS EVENTOS INTERMEDIÁRIOS

Neste trabalho foi desenvolvido um algorítmo alternativo, que não necessita determinar os conjuntos mínimos de corte da árvore de falhas.

O objetivo é calcular a probabilidade de ocorrência dos eventos intermediários e combiná-los até atingir o evento topo, determinando sua probabilidade de ocorrência e escrevendo a expressão final equivalente.

A simplicidade do algorítmo, que pode ser visto com detalhes no Apêndice A faz com que o tempo de execução seja muito pequeno.

Podem-se eleger eventos intermediários como topo para determinar contribuições parciais para a confiabilidade final, assim como desenvolver análises de sensibilidades.

A partir do evento topo, identificam-se todos os por

tões e eventos que estão ligados a ele. Repete-se o processo para cada portão ligado ao evento topo, continuando o processo de "descida" da árvore até que todos os eventos básicos sejam atingidos.

Em seguida operam-se os eventos nos níveis mais baixos da árvore e inicia-se um processo de "subida" operando com os eventos em níveis mais altos. Ao atingir o evento topo, escreve-se a probabilidade de ocorrência do evento topo e a expressão equivalente.

São utilizadas duas matrizes de trabalho. Na primeira são armazenadas informações sobre a lógica da árvore:

- Portão
- Tipo do Portão
- Portão ou Evento Associado
- Probabilidade de Ocorrência dos Eventos Básicos, calculada a partir dos valores de taxa de falha e tempo, utilizando a expressão

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

A segunda matriz é usada para cálculo da expressão resultante da combinaçao lógica de eventos dos vários ramos da árvore.

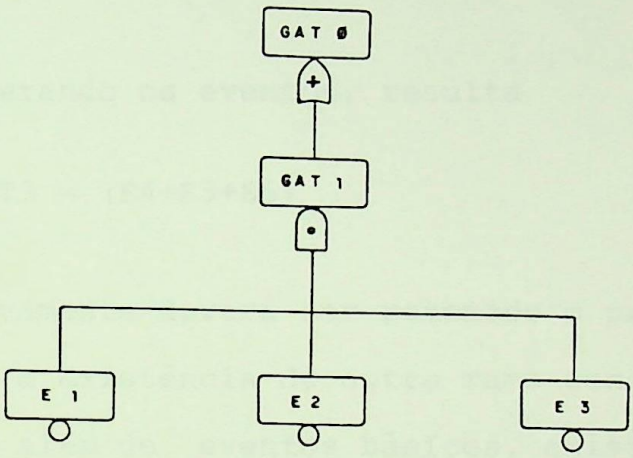
Recorrendo ao exemplo da figura 3.1, já utilizado para ilustrar o método dos cortes mínimos, a primeira matriz contém as seguintes informações:

GATØ	GATØ	GAT1	GAT1	GAT1	GAT2	GAT2	GAT3	GAT3	GAT3
OU	OU	E	E	E	OU	OU	OU	OU	OU
GAT1	GAT2	E1	E2	E3	GAT3	GAT4	E4	E5	E6

GAT4	GAT4	GAT4	GAT5	GAT5	GAT5
OU	OU	OU	E	E	E
GAT5	E7	E8	E8	E9	E10

Através da lógica armazenada anteriormente, é feita a descida por um ramo até o nível mais baixo, armazenando o caminho percorrido na segunda matriz e operando com os eventos.

Isto equivale, por exemplo a identificar o seguinte ramo.

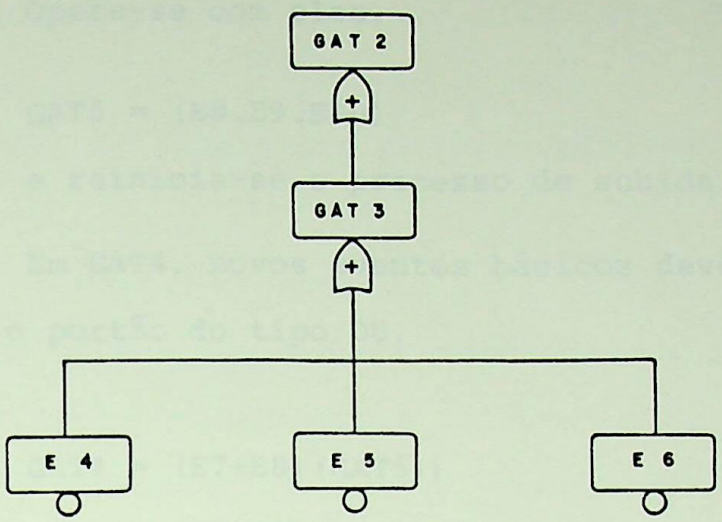


Atingidos os eventos básicos, estes devem ser operados de acordo com o portão GAT1, do tipo E.

GAT1 = (E1.E2.E3)

Subindo um nível no ramo, terá sido atingido o topo e deve ser verificado se existem outros ramos e reiniciar sua descida.

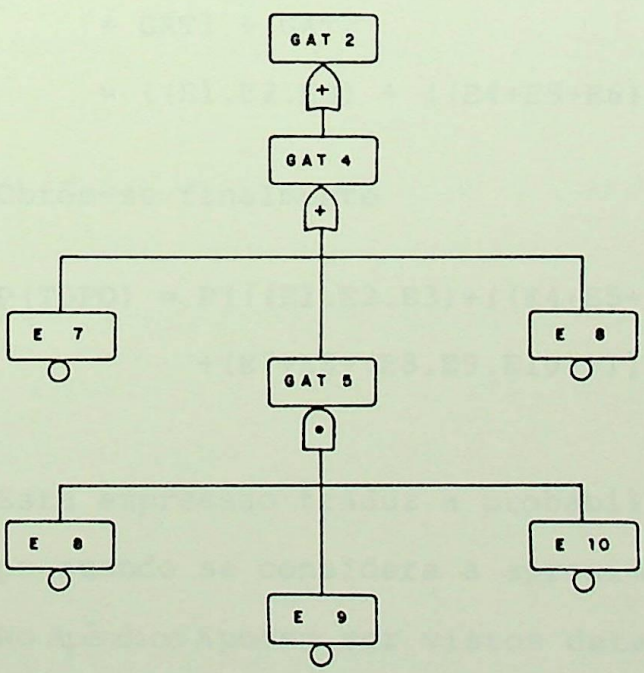
Identificando o GAT2, atinge-se o ramo de GAT3, tipo OU.



Operando os eventos, resulta

GAT3 = (E4+E5+E6)

Novamente deverá ser retomado o processo de subida , verificando-se a existência de outro ramo conectado ao GAT2, que é o GAT4. Como além de eventos básicos, existe outro portão conectado a ele, o processo de descida continua até o GAT5, do tipo E, onde são atingidos os eventos básicos.



Opera-se com eles.

GAT5 = (E8.E9.E10)

e reinicia-se o processo de subida.

Em GAT4, novos eventos básicos devem ser operados,de acordo com o portão do tipo OU.

GAT4 = (E7+E8+(GAT5))

= (E7+E8+(E8.E9.E10))

Reiniciando a subida, verificamos que em GAT2 devem ser combinados GAT3 e GAT4, neste ponto já desenvolvidos

GAT2 = GAT3 + GAT4

= ((E4+E5+E6) + (E7+E8+(E8.E9.E10)))

Em um nível acima, reencontramos o topo, que é um portão OU e agora deve ser operado.

TOPO = GATØ

= GAT1 + GAT2

= ((E1.E2.E3) + ((E4+E5+E6)+(E7+E8+(E8.E9.E10))))

Obtém-se finalmente

P(TOPO) = P(((E1.E2.E3)+((E4+E5+E6)+

+(E7+E8+(E8.E9.E10))))

Esta expressão traduz a probabilidade de ocorrência do evento topo quando se considera a aproximação do evento raro.

No Apêndice A podem ser vistos detalhes do programa "AR

VORE" que segue a metodologia descrita neste ítem.

3.4.7 - ÁRVORE DE FALHAS COM EVENTOS REPETIDOS

É sempre recomendado reduzir a expressão resultante da árvore de falhas com eventos repetidos, aplicando as propriedades de Álgebra Booleana antes de obter os resultados finais.

Entretanto, quando as probabilidades de falha dos eventos básicos são muito pequenas, a inabilidade de remover as dependências não introduz erro significativo no resultado final [70].

Vários autores preocuparam-se com a eliminação de eventos repetidos e com algorítmos que avaliem a árvore de falhas quando são presentes repetições de eventos [63].

3.4.8 - MÉTODO MONTE CARLO DE SIMULAÇÃO

Além dos métodos analíticos de solução de problemas de confiabilidade, o método de simulação apresenta-se como alternativa, valendo-se da característica aleatória da maioria dos problemas da vida real.

O método é definido como a construção de um processo aleatório artificial, através de um modelo probabilístico, possuindo todas as propriedades necessárias para representar, o mais fielmente possível, o sistema real ou o processo que está sendo investigado [34].

Um teste do modelo é repetido várias vezes e cada vez o desempenho do sistema é registrado. Por exemplo, supor a determinação da confiabilidade de um sistema multicomponente após

5 000 horas.

Um modelo para simulação do sistema pode ser desenvolvido e executado 100 vezes. Cada execução é independente e, com efeito, modela o sistema a cada vez. Se, ao fim da execução, 75 dos sistemas sobreviveram além das 5 000 horas, mas 25 falharam antes, podemos concluir que a confiabilidade do sistema durante 5 000 horas é 0,75.

Em geral, simulações Monte Carlo são fáceis de realizar e podem ser aplicadas a sistemas muito grandes ou muito complexos para se resolver por métodos analíticos; o método de Monte Carlo tem sido usado extensivamente para análise de árvores de falhas e diagramas de blocos [27].

3.4.8.1 - CONSIDERAÇÕES SOBRE APLICAÇÕES DO MÉTODO ÀS ÁRVORES DE FALHAS

Geralmente, as árvores de falhas devem simular o desempenho do sistema durante a vida útil do mesmo.

Alguns passos necessários para simular uma árvore de falhas podem ser:

- Obter dados de falha de eventos básicos.
- Representar a árvore de falhas em sua forma matemática, em um computador digital. Pode-se utilizar, por exemplo, a função de estrutura para sua representação.
- Listar as falhas e conjuntos mínimos de corte que levam à ocorrência do evento topo.
- Simular o estado de todos os componentes envolvidos no sistema.
- Determinar os resultados finais desejados [39].

3.4.8.2 - ASPECTOS PARTICULARES DO MÉTODO

Uma das características importantes do método é o de poder-se simular o estado de um componente sujeito a qualquer função de distribuição. Uma vez gerados os números aleatórios, pseudo-aleatórios ou quase-aleatórios uniformemente distribuidos, pode-se modelar eventos e números aleatórios sujeitos a outras distribuições [25].

Outro aspecto favorável é a facilidade com que o número e características dos componentes podem ser modificados.

Os componentes e fatores críticos num sistema podem facilmente ser determinados.

A maioria das técnicas analíticas somente dá como resultado valores esperados, por exemplo, tempo esperado entre falhas. Usando o método de Monte Carlo pode ser obtida a distribuição dos resultados. Esta distribuição é usualmente descrita como um histograma.

Quando são usados valores fixos para as taxas de falhas e outros parâmetros, a probabilidade de falha do sistema é referida como um valor pontual. Contudo, devido a incertezas e variações nas taxas de falhas e outros parâmetros, essas quantidades podem ser tratadas como variáveis aleatórias e, como a probabilidade de falha do sistema é uma função dessas variáveis aleatórias, ela própria é uma variável aleatória. O termo propagação de erro refere-se ao processo de determinação da probabilidade de falha em termos das distribuições dos parâmetros individuais, o que pode ser feito utilizando processos de simulação.

Outra vantagem é que o desenvolvimento e manipulação da técnica Monte Carlo dá aos engenheiros de planejamento alguma "experiência de operação" com o sistema assim como uma penetra

ção na sua estrutura e comportamento funcional.

Por outro lado, o método é dispendioso em termos de tempo e memória computacionais gastos no desenvolvimento e execução dos modelos. Para ter razoável confiança no resultado da simulação, é necessário executar um grande número de simulações significando uma quantidade substancial de tempo de computação.

Para contornar esse problema, algumas vezes são utilizadas técnicas de amostragem restrita [27].

3.4.9 - DETERMINAÇÃO DE TAXAS DE FALHA DE EVENTOS INTERMEDIÁRIOS E DO EVENTO TOPO DE ÁRVORES DE FALHAS [39]

A informação da probabilidade de sucesso e de falha de um sistema algumas vezes não é suficiente por si só, para interpretação de seu desempenho, havendo necessidade de indicadores adicionais. Um desses indicadores é a taxa de falha de eventos intermediários e do evento topo de árvores de falhas.

Alguns requisitos são necessários para validade dos conceitos descritos a seguir:

- Os componentes do sistema, cujos modos de falha constituem os eventos básicos da árvore de falhas, não são reparáveis, pelo menos durante o intervalo de tempo de interesse para a análise a ser desenvolvida.
- Os tempos até a ocorrência dos eventos de falha distribuem-se exponencialmente.
- A árvore de falhas é livre de redundâncias, ou seja, ela não contém eventos repetidos.
- Os eventos básicos representam falhas estatísticamente independentes.

As expressões das taxas de falha para os portões E e OU são desenvolvidas a partir da igualdade:

$$\lambda(t) = - \frac{1}{R(t)} \cdot \frac{dR(t)}{dt} \qquad (1)$$

onde: $\lambda(t)$ = taxa de falha no tempo t

$R(t)$ = Confiabilidade do sistema ou componente

3.4.9.1 - PORTÕES OU

A lógica desta associação corresponde ao sistema série. A confiabilidade do sistema série pode ser obtida da seguinte equação:

$$R_s = \prod_{i=1}^{n} R_i \qquad (2)$$

onde: R_i = Confiabilidade do i-ésimo componente

R_s = Confiabilidade do sistema série

n = número de componentes

Quando os tempos até a ocorrência dos eventos de falha dos componentes se distribuem exponencialmente, tem-se

$$R_s(t) = e^{-(\sum_{i=1}^{n} \lambda_i)t} \qquad (3)$$

onde: λ_i = taxa de falha constante do i-ésimo componente

t = tempo

Substituindo (3) em (1) encontra-se:

$$\lambda_s(t) = \sum_{i=1}^{n} \lambda_i \qquad (4)$$

Ou seja, a taxa de falha de saída de um portão OU é simplesmente a soma das taxas de falha dos eventos de entrada.

3.4.9.2 - PORTÕES E

Um portão E corresponde à lógica da configuração dos sistemas em paralelo. A confiabilidade de um sistema em paralelo pode ser determinada pela expressão:

$$R_p = 1 - \prod_{i=1}^{n} (1-R_i) \qquad (5)$$

onde:

R_p = Confiabilidade do sistema paralelo

n = número de componentes

R_i = Confiabilidade do i-ésimo componente

No caso de taxa de falha constante, a equação acima pode ser escrita como

$$R_p = 1 - \prod_{i=1}^{n} (1-e^{-\lambda it}) \qquad (6)$$

onde: λ_i = taxa de falha constante do i-ésimo componente

t = tempo de interesse

Substituindo (6) em (1), obtém-se o seguinte resultado:

$$\lambda_p(t) = \left[\sum_{j=1}^{n} \lambda_j(Z_j-1)\right]\left[\prod_{j=1}^{n} Z_j-1\right]^{-1} \qquad (7)$$

onde:

$$\frac{1}{z_j} = (1-e^{-\lambda_j t}) \quad \text{para } j=1,2,\ldots,n$$

3.4.10 - SENSIBILIDADES

A definição usual da função de sensibilidade é:

$$S_X^Y = \lim_{\Delta X \to 0} \frac{\frac{\Delta Y}{Y}}{\frac{\Delta X}{X}}$$

Sendo a relação entre a variação normalizada do parâmetro Y e a variação normalizada do parâmetro X.

Se a variação ΔX é infinitamente pequena, tem-se:

$$S_X^Y = \frac{X}{Y} \frac{\partial Y}{\partial X}$$

$$= \frac{\partial(\ell n Y)}{\partial(\ell n X)}$$

Algumas relações úteis podem ser determinadas:

1) $S_X^Y = \dfrac{\partial(\ell n Y)}{\partial(\ell n X)} = 0$ se Y não é função de X

2) Se $Y = CX$, sendo C constante

$$S_X^{CX} = \frac{\partial(\ell n CX)}{\partial(\ell n X)} = \frac{\partial(\ell n C)}{\partial(\ell n X)} + \frac{\partial(\ell n X)}{\partial(\ell n X)} = 1$$

3) $S_X^{1/Y} = \dfrac{(\ell n\ 1/Y)}{(\ell nX)} = \dfrac{\partial(-\ell nY)}{\partial(\ell nX)} = -S_X^Y$

Análogamente

$$S_X^Y = -S_{1/X}^Y$$

4) $S_X^{Y_1 Y_2} = S_X^{Y_1} + S_X^{Y_2}$

5) $S_X^{Y_1/Y_2} = S_X^{Y_1} - S_X^{Y_2}$

6) $S_{X^n}^{Y} = \frac{1}{n} S_X^Y$

7) $S_X^{Y^n} = n\, S_X^Y$

8) $S_X^{Y_1+Y_2} = \dfrac{Y_1 S_X^{Y_1} + Y_2 S_X^{Y_2}}{Y_1 + Y_2}$

9) $S_X^{Cf(X)} = S_X^{f(X)}$

onde C é independente de X e f(X) é uma função de X.

Até aqui, são consideradas mudanças devido a uma variável. Entretanto, muitas vezes, é desejado analisar a mudança que ocorrerá com a variação simultânea de vários parâmetros X_j. A mudança ΔY pode ser obtida da expansão em série de Taylor:

$$\Delta Y = \frac{\partial Y}{\partial X_1}\Delta X_1 + \frac{\partial Y}{\partial X_2}\Delta X_2 + \ldots \frac{\partial Y}{\partial X_m}\Delta X_m + \text{termos de } 2^{a}. \text{ e mais altas ordens}$$

onde:

m é o número de variáveis envolvidas.

Desde que as mudanças ΔX_j nas variáveis sejam pequenas, os termos de ordem igual ou superior a segunda podem ser desprezados.

Desta forma,

$$\Delta Y \simeq \sum_{j=1}^{m} \frac{\partial Y}{\partial X_j} \Delta X_j$$

ou

$$\Delta Y \simeq \sum_{j=1}^{m} \left(\frac{\partial Y}{\partial X_j} \frac{X_j}{Y}\right)\left(\frac{\Delta X_j}{X_j}\right) Y$$

$$= \sum_{j=1}^{m} S_{X_j}^{Y} V_{X_j} Y$$

onde

$V_{X_j} = \dfrac{\Delta X_j}{X_j}$ é a mudança na variável X_j por unidade, também conhecida como variabilidade de X.

Então

$\dfrac{\Delta Y}{Y} = \sum_{j=1}^{m} S_{X_j}^{Y} V_{X_j}$ é a mudança por unidade de Y para a variação simultânea das variáveis X_j

3.5 - ANÁLISE DO SISTEMA ELÉTRICO DE EMERGÊNCIA DE UMA AERONAVE

Com a finalidade de ilustrar a aplicação do método descrito neste capítulo, foi escolhido o sistema elétrico de emergência descrito na figura 3.3, que é um sub-sistema do sistema elétrico completo cujo estudo detalhado se encontra no capítulo seguinte, que é o principal objetivo deste trabalho.

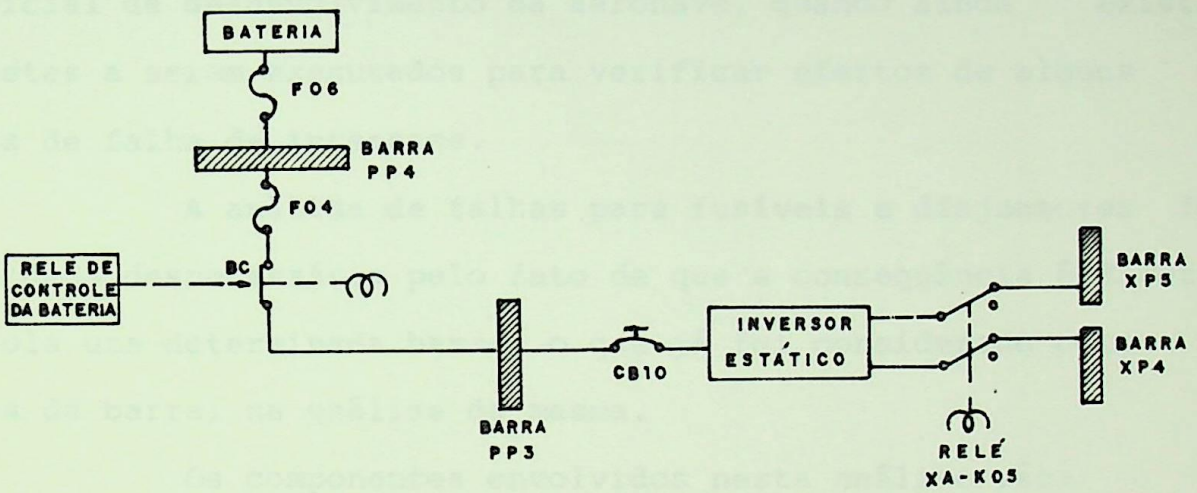


Figura 3.3 - REPRESENTAÇÃO SIMPLIFICADA DO SISTEMA ELÉTRICO DE EMERGÊNCIA

3.5.1 - DESCRIÇÃO DO FUNCIONAMENTO DO SISTEMA

Se ocorrerem modos de falha que representem perda de geração normal, o sistema de emergência deverá ser conectado automáticamente. A desenergização do relé XA-K05, que passa a estar na posição indicada na figura 3.3 e a energização do contator de bateria, que recebe um impulso da bateria através de um re

lé de controle quando este deixa de ser energizado pelo sistema normal, completam a ligação entre as barras PP3 e PP4.

Essas barras terão tensão DC disponível enquanto que o inversor estático suprirá as barras XP4 e XP5 com tensão AC nos níveis estabelecidos.

3.5.2 - ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

A FMEA desenvolvida para o sistema reflete o estágio inicial de desenvolvimento da aeronave, quando ainda existem testes a serem executados para verificar efeitos de alguns modos de falha de interesse.

A análise de falhas para fusíveis e disjuntores foi julgada desnecessária pelo fato de que a consequência é direta: isola uma determinada barra, o que já foi considerado como falha da barra, na análise da mesma.

Os componentes envolvidos nesta análise são:

- Barra de Distribuição AC - XP4
- Barra de Distribuição AC - XP5
- Contator da Bateria
- Relé de Controle do Contator da Bateria
- Chave da Bateria
- Bateria
- Barra de Distribuição DC - PP3
- Barra de Distribuição DC - PP4
- Inversor Estático
- Contator X4 - K05

A Análise de Modos de Falha e seus Efeitos está apresentada nas páginas 108,109,113 a 120 a 122 e 125 a 128.

3.5.3 - CONSTRUÇÃO DA ÁRVORE DE FALHAS

A partir dessas informações, pode ser construída a Árvore de Falhas. Consideram-se falhas simples ou no máximo duplas, devido aos baixos valores das taxas de falha dos componentes envolvidos.

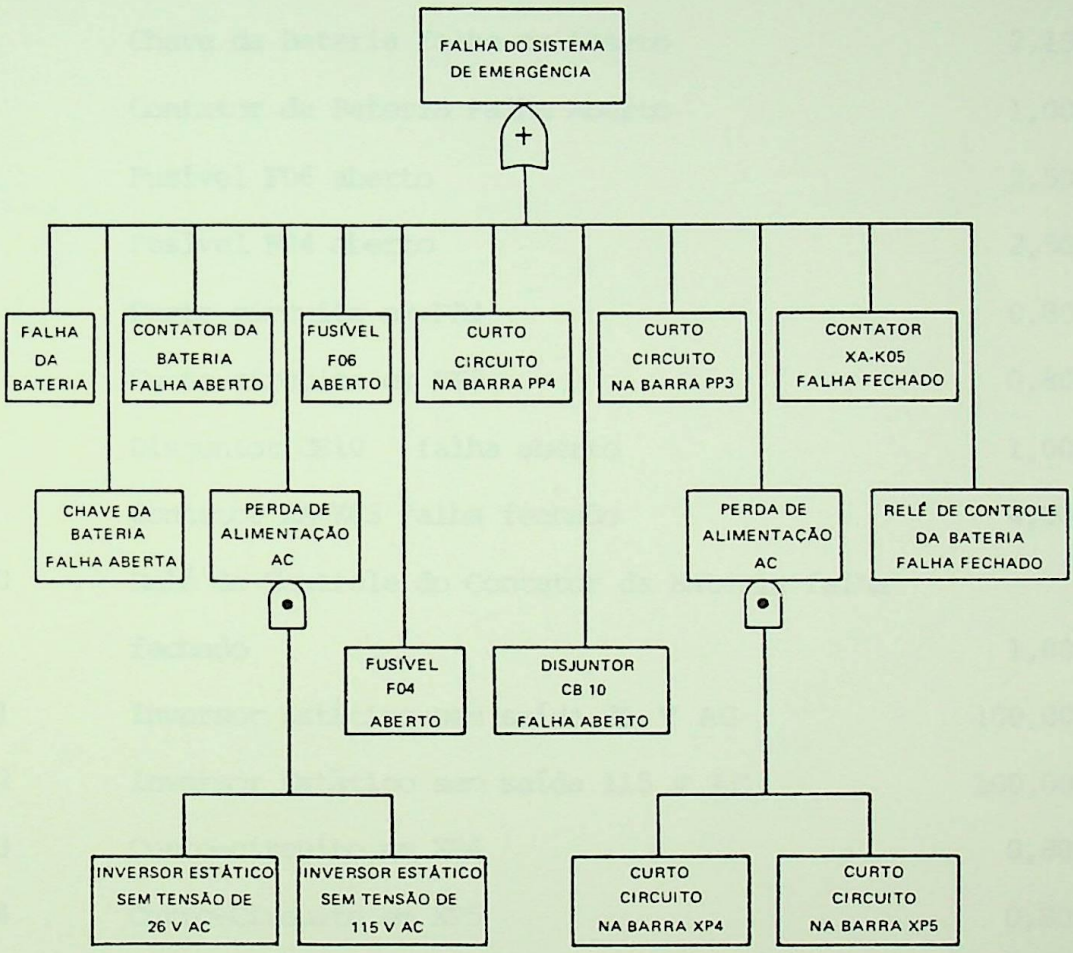


FIGURA 3.4 - Árvore de Falhas do Sistema Elétrico de Emergência

3.5.4 - CÁLCULO DA PROBABILIDADE DE OCORRÊNCIA DO EVENTO TOPO

Para determinar a probabilidade de ocorrência do evento topo foram utilizados os dados descritos na tabela seguinte, e um tempo de exposição igual a 1 hora.

SÍMBOLO	DESCRIÇÃO	TAXA DE FALHA [$\times 10^{-6}$]
E1	Falha da Bateria	6,000
E2	Chave da Bateria Falha em Aberto	2,132
E3	Contator da Bateria Falha Aberto	1,000
E4	Fusível F06 aberto	2,500
E5	Fusível F04 aberto	2,500
E6	Curto-circuito em PP4	0,800
E7	Curto-circuito em PP3	0,800
E8	Disjuntor CB10 falha aberto	1,000
E9	Contator XA-K05 falha fechado	4,000
E10	Relé de Controle do Contator da Bateria falha fechado	1,000
E11	Inversor Estático sem saída 26 V AC	100,000
E12	Inversor Estático sem saída 115 V AC	100,000
E13	Curto-circuito em XP4	0,800
E14	Curto-Circuito em XP5	0,800

Os resultados obtidos, utilizando a metodologia descrita no ítem 3.4.6, estão relacionados à seguir.

```
**********************************************
* EXPRESSAO RESULTANTE DA ARVORE ATRAVES DO  *
*  CALCULO DAS PROBABILIDADES DOS EVENTOS    *
*                INTERMEDIARIOS              *
**********************************************
```

((E11.E12)+(E13.E14)+E1+E2+E3+E4+E5+E6+E7+E8+E9+E10)

A PROBABILIDADE DE OCORRENCIA DO EVENTO TOPO E

I	0.217419629773400-04	I

3.5.5 - CÁLCULO DA TAXA DE OCORRÊNCIA DO EVENTO TOPO

Com a finalidade de fornecer mais informações acerca do sistema, é conveniente determinar a taxa de ocorrência de eventos intermediários e do evento topo.

Foi considerado, novamente, o tempo de exposição de 1 hora.

Evento intermediário corresponde ao portão 1.

$$\lambda_{GAT1}(1) = \frac{\lambda_{11}(Z_{11}-1) + \lambda_{12}(Z_{12}-1)}{Z_{11}Z_{12} - 1}$$

onde:

$$\lambda_{11} = \lambda_{12} = 100\text{x}10^{-6}$$

$$Z_{11} = Z_{12} = \frac{1}{1-e^{-\lambda_{11}t}} = 10\ 000{,}499$$

$$\lambda_{GAT1}(1) = \frac{100\text{x}10^{-6}(10\ 000{,}499)+100\text{x}10^{-6}(10\ 000{,}499)}{100\ 009\ 980{,}6} =$$

$$= 1{,}999 \times 10^{-8}$$

Evento intermediário correspondente ao portão 2

$$\lambda_{GAT2}(1) = \frac{\lambda_{13}(Z_{13}-1) + \lambda_{14}(Z_{14}-1)}{Z_{13}Z_{14}-1}$$

onde

$$\lambda_{13} = \lambda_{14} = 0{,}8 \times 10^{-6}$$

$$Z_{13} = Z_{14} = \frac{1}{1 - e^{-\lambda_{13} t}} = 1\ 250\ 000$$

$$\lambda_{GAT2}(1) = \frac{0{,}8x10^{-6}(1\ 250\ 000)+0{,}8x10^{-6}(1\ 250\ 000)}{1{,}5625 \times 10^{12}} =$$

$$= 1{,}28x10^{-12}$$

$$\lambda_{TOPO} = \Sigma\ \lambda_{parciais}$$

$$\lambda_{TOPO} = (6+2{,}132+1+2{,}5+0{,}8+1+4+1+0{,}02000099805 +$$

$$+0{,}00000128) \times 10^{-6}$$

$$\lambda_{TOPO} = 0{,}2175 \times 10^{-4}$$

Determinando a probabilidade de ocorrência do evento topo $p=e^{-\lambda_{TOPO} t} = 0{,}2175x10^{-4}$, encontra-se um resultado bastante próximo daquele calculado através da árvore de falhas $p = 0{,}2174 \times 10^{-4}$.

3.5.6 - ANÁLISE DE SENSIBILIDADES

Uma das aplicações mais importantes da árvore de falhas é em análise de sensibilidades. Para demonstrar os recursos desta técnica, foi escolhido o sistema elétrico de emergência com sua árvore de falhas simples, de maneira a facilitar conclusões acerca dos resultados.

Utilizou-se em uma primeira aproximação um decréscimo de 10% no valor das taxas de falha, encontrando-se os seguintes resultados:

EVENTOS	Taxas de Falha $[x10^{-6}]$ horas		$\frac{\Delta\lambda}{\lambda}$	Probabilidade de ocorrência do Evento Topo $Q\,[x10^{-4}]$	$\frac{\Delta Q}{Q}$	$S_{\lambda}^{Q} = \frac{\frac{\Delta Q}{Q}}{\frac{\Delta\lambda}{\lambda}}$
	Inicial	Modificada				
-	-	-	-	0,2174	-	-
E1	6,00	5,4	0,1	0,2132	0,019	19%
E2	2,132	1,919	0,1	0,2153	0,010	10%
E3	1,000	0,9	0,1	0,2164	0,004	4%
E4	2,500	2,25	0,1	0,2149	0,011	11%
E5	2,500	2,25	0,1	0,2149	0,011	11%
E6	0,800	0,72	0,1	0,2166	0,004	4%
E7	0,800	0,72	0,1	0,2166	0,004	4%
E8	1,000	0,9	0,1	0,2164	0,004	4%
E9	4,000	3,600	0,1	0,2134	0,016	18%
E10	1,000	0,9	0,1	0,2164	0,004	4%
E11	100,000	90,00	0,1	0,2174	0,000	0%
E12	100,000	90,00	0,1	0,2174	0,000	0%
E13	0,800	0,72	0,1	0,2174	0,000	0%
E14	0,800	0,72	0,1	0,2174	0,000	0%

É interessante observar, por exemplo, que embora os modos de falha E11 e E12 tenham taxas de falha de $100,00x10^{-6}$, a redução desta taxa de falha em 10% produzirá o mesmo efeito na confiabilidade do sistema que a redução de 10% nos modos de falha E13 e E14 que possuem taxa de falha de $0,8 \times 10^{-6}$. Isto pode ser entendido quando analisamos a estrutura da árvore de falhas e verificamos que os modos de falha E11 e E12 são ligados por um portão E, da mesma forma que os eventos E13 e E14 .

Isto significa que formam conjuntos de corte de segunda ordem, com pouca influência sobre a confiabilidade do sistema comparativamente aos demais conjuntos de corte de primeira ordem.

Na verdade esta influência escapa à precisão adotada neste trabalho.

Por outro lado, os eventos ligados ao topo por portões OU, que são conjuntos de corte de primeira ordem, têm grande influência na probabilidade de ocorrência do evento topo, de acordo com a magnitude de sua taxa de falha. Assim, variando a taxa de falha do evento básico E1 de $6x10^{-6}$ para $5,4x10^{-6}$, o sistema sente a variação e responde com uma variação de 19%. Já um evento básico E7 com taxa de falha de $0,8x10^{-6}$, após um decréscimo de 10% neste valor, leva o sistema a uma variação de 4%.

Variando-se na mesma proporção as taxas de falha de mais de um modo de falha, obteve-se:

EVENTOS	PROB. OCORRER EVENTO TOPO $[x10^{-4}]$	$\frac{\Delta Q}{Q} = \sum_{j=1}^{m} S_{\lambda_j}^{Q} V_{\lambda_j}$
E11 e E12	0,2174	0
E13 e E14	0,2174	0
E1 e E2	0,2113	0,029
E7 e E8	0,2156	0,008
E1,E2,E3	0,2103	0,033
E4,E5,E6	0,2116	0,026
TODOS	0,1977	0,087
E1 e E9	0,2094	0,037
E6 e E7	0,2158	0,008

Através desses exemplos, pode-se avaliar a importância da análise de sensibilidades para indicar quais os componentes mais críticos. Para melhorar a confiabilidade do sistema , pode-se substituir aqueles componentes por outros mais confiáveis.

Esta melhoria na confiabilidade do sistema pode ser resultado de uma análise custo-benefício, utilizando-se a análise de sensibilidades para estabelecer prioridade na implementação das modificações.

Outra utilização é encontrada em [2] . Os autores analisam o problema das taxas de falha não disponíveis e adotadas por "uma melhor escolha de engenharia" baseada na experiência ou comparação com similares onde as taxas de falha estiverem disponíveis. Sugerem avaliar sua sensibilidade no resultado da árvore de falhas,variando seu valor; se houver significante influência, torna-se necessário buscar taxas de falha o mais reais possível.

CAPÍTULO 4

APLICAÇÃO DA METODOLOGIA

4.1 - INTRODUÇÃO

Um sistema elétrico de uma aeronave é, quanto à finalidade e guardadas as devidas proporções, muito semelhante aos sistemas elétricos de potência destinados a alimentar grandes centros populacionais. A função de ambos é alimentar as cargas do sistema tão economicamente quanto possível, e com um nível aceitável de continuidade e qualidade de serviço. Por esta razão, os métodos de análise de confiabilidade largamente usados em sistemas aeronáuticos, podem ser estendidos à análise de confiabilidade de grandes sistemas de potência [9] , assim como são usualmente empregados em sistemas nucleares [38] ou químicos [3,4], onde os requisitos de segurança também são elevados.

Os métodos, Análise de Modos de Falha e seus Efeitos e Árvores de Falhas, aplicados ao Sistema de Geração Elétrica de uma Aeronave, estão desenvolvidos neste capítulo e são o resultado da experiência e identificação das dificuldades em problemas relativos ao estágio de desenvolvimento da confiabilidade na área aeronáutica em nosso país. Isto pôde ser comprovado pelo fato de a autora trabalhar junto ao Setor de Eficácia de Sistemas Aeronáuticos na Área de Confiabilidade.

Atualmente, são encontrados na indústria aeronáutica, dois tipos de análises de confiabilidade, isto é,aplicam-se metodologias diferentes para aeronaves civis e militares, em virtude da utilização diversa das duas versões e, consequentemente, sujeitas a requisitos também diferentes.

Para aeronaves civis, os órgãos homologadores exigem que os sistemas sejam analisados qualitativamente pelo método de Análise de Modos de Falha e seus Efeitos e quantitativamente para possíveis situações de risco, pelo método de Árvore de Falhas [Apêndice 2].

Para aeronaves militares, as Forças Aéreas estipulam o nível de confiabilidade que desejam para o cumprimento de uma missão com características bem definidas e, a partir daí, os sistemas são classificados de acordo com seu envolvimento na missão e são estabelecidos os alvos de confiabilidade a serem atingidos para cada um desses sistemas, durante missões de interesse.

Seguindo este critério, para o Sistema de Geração Elétrica, o alvo de confiabilidade a ser atingido é de 0,95.

Para determinar a Confiabilidade da Missão, foi utilizado o Método de Diagrama de Blocos, que, por ser um método de avaliação de sucessos, permite apenas uma análise superficial dos sistemas.

Existem ainda os requisitos de Confiabilidade Básica, referentes às taxas de falhas dos componentes, que deverão ser demonstrados após completar um número de horas de vôo com validade estatística. Essa demonstração requer a implantação de banco de dados, que é outro aspecto de enorme importância na área de confiabilidade e que será discutido no capítulo seguinte.

A partir do conhecimento desta situação,resolveu-se ampliar estas análises, desenvolvendo a Análise de Confiabilidade da Missão pelo método de Árvore de Falhas, ao invés do Dia

grama de Blocos, uma vez que, além de utilizar as informações contidas na Análise de Modos de Falha e seus Efeitos, este método possibilita um estudo mais aprofundado do sistema e favorece a Análise de Riscos e a Análise de Sensibilidades.

A Análise de Sensibilidades, que está sendo utilizada pela primeira vez na indústria aeronáutica nacional, permite avaliar as variações causadas na confiabilidade do sistema quando se alteram as características de seus componentes. Esta informação é importante na escolha de alternativas para melhorar sistemas considerados não satisfatórios, além do tradicional "julgamento de engenharia" aliado ao bom-senso e experiência profissional, que eram, até então, os critérios adotados.

4.2 - DESCRIÇÃO DO SISTEMA

O Sistema Elétrico de Geração a ser analisado neste Capítulo é composto de um sub-sistema principal e de um sub-sistema secundário, que estão esquematicamente representados na figura 4.1.

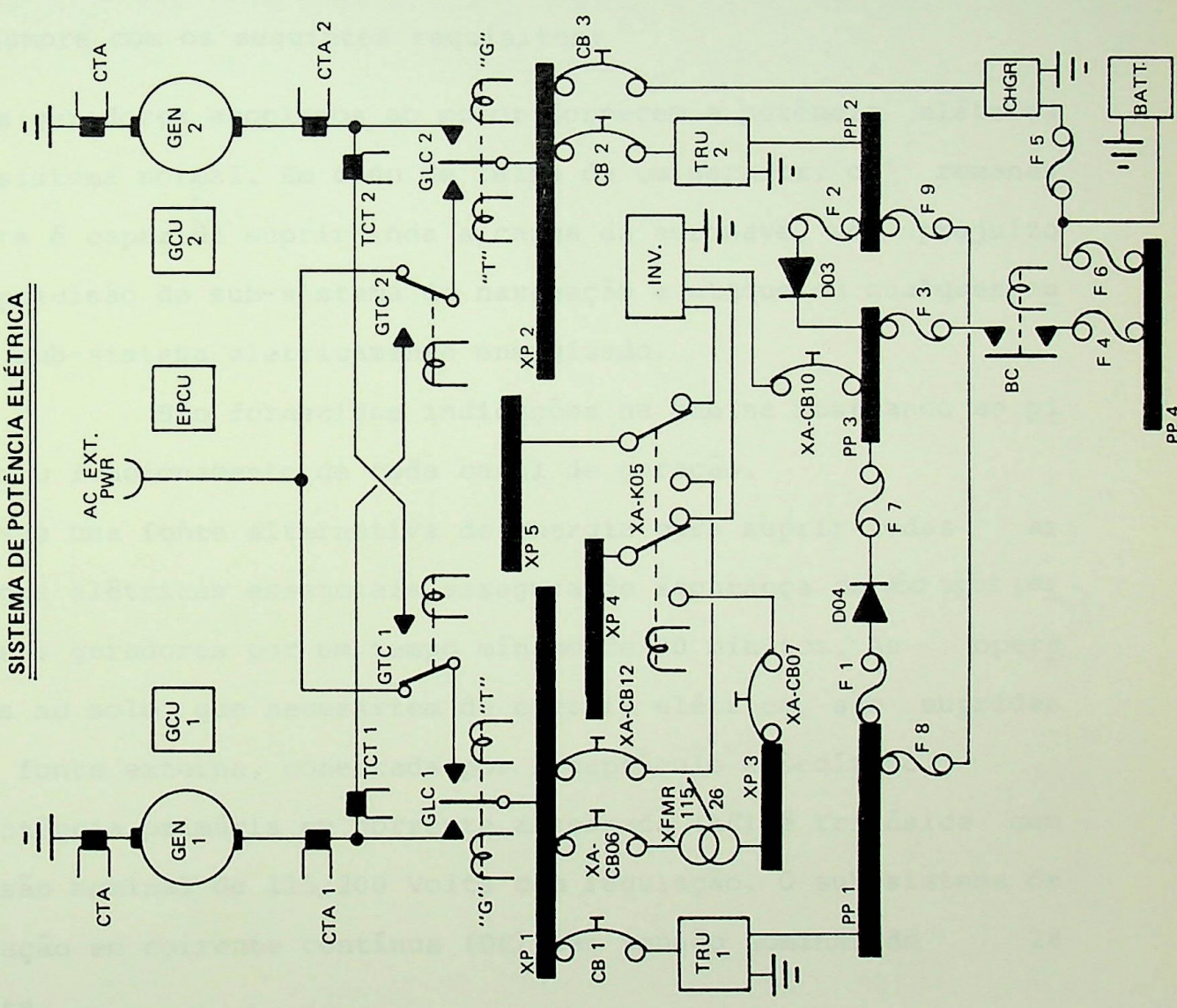


FIGURA 4.1 - Esquema Simplificado do Sistema Elétrico de Geração

O sub-sistema principal envolve geração em corrente alternada e transformação e retificação para utilização em corrente contínua.

Como sub-sistema secundário, existe uma bateria acoplada a um carregador de bateria, além de um inversor que juntos garantem o fornecimento de energia em corrente contínua e corrente alternada, em caso de falha do sistema principal.

O Sistema Elétrico supre todas as exigências de carga elétrica da aeronave durante todas as condições de operação e cumpre com os seguintes requisitos:

Dois geradores acoplados ao motor fornecem a potência elétrica do sistema normal. Em caso de falha de um gerador, o remanescente é capaz de suprir toda a carga da aeronave, sem prejuízo na precisão do sub-sistema de navegação e ataque ou qualquer outro sub-sistema eletricamente energizado.

São fornecidas indicações na cabine mostrando ao piloto o funcionamento de cada canal de geração.

Existe uma fonte alternativa de energia para suprir todas as cargas elétricas essenciais assegurando segurança de vôo após perda dos geradores por um tempo mínimo de 20 minutos. As operações no solo, que necessitem de energia elétrica, são supridas por fonte externa, conectada por receptáculo específico.

A potência primária em corrente alternada (AC) é trifásica com tensão nominal de 115/200 Volts com regulação. O sub-sistema de geração em corrente contínua (DC) tem tensão nominal de 28 volts.

O ponto de aterramento e neutro são capazes de suportar a corrente de curto-circuito do sistema de geração.

A transferência de barras é automática para minimizar a carga do piloto e o risco associado à operação manual. O tempo de chaveamento é reduzido ao mínimo possível.

A confiabilidade e as taxas de falha atribuídas ao sistema elétrico de potência são avaliadas durante as fases de projeto e desenvolvimento, avaliando-se sua influência sobre a confiabilidade total da aeronave.

Como condição de falha simples, somente curto-circuito na barra pode causar perda de cargas exigidas para cumprir a missão. Os sistemas redundantes têm tubulações e fiações fisicamente separados.

4.2.1 - CARACTERÍSTICAS DO SUBSISTEMA AC

Este subsistema é encarregado do suprimento de potência em corrente alternada. É composto de dois canais de geração, cinco barras condutoras e um autotransformador, além dos equipamentos de comando e proteção do sistema.

4.2.1.1 - CONDIÇÕES NORMAIS DE OPERAÇÃO EM VÔO

A potência elétrica gerada é distribuída por duas barras principais de 115/200 V AC (XP1 e XP2), uma barra principal de 26 V AC(XP3), uma barra essencial de 115 V AC (XP5) e uma barra essencial de 26 V AC (XP4).

As barras principais são isoladas uma da outra e diretamente conectadas ao gerador correspondente através de um contator. Um outro contator faz ligação de XP1 com XP5 e de XP1 com XP4, esta última através de um autotransformador.

Cada canal de geração é controlado e protegido por uma Unidade de Controle da Geração (GCU)

4.2.1.2 - CONDIÇÃO DE FALHA DE UM GERADOR

No evento de falha de um canal de geração, existe provisão para transferir toda a carga para a fonte remanescente. Nesta condição , os contatores de linha e de transferência possibilitam a alimentação cruzada entre a barra principal desativada e o gerador sobrevivente.

4.2.1.3 - ASPECTOS OPERACIONAIS

Cada canal de geração é formado por um Gerador de Energia Integrado (IDG), uma Unidade de Controle da Geração (GCU) e por um Conjunto de Transformadores de Corrente (CTA).

Cada GCU deve controlar e monitorar o gerador correspondente, operando os contatores AC para eliminar distúrbios e/ou para isolar faltas.

As funções de proteção abrangem as condições de subtenção, sobretensão, subfrequência, sobrefrequência, sobrecorrente, corrente diferencial e anticiclagem.

Existem duas chaves no painel com as inscrições "ON" e "OFF RESET", para controle de cada canal de geração. Na posição "ON", o gerador entra automaticamente em linha quando suas características elétricas estão dentro dos limites prescritos. Na posição "OFF RESET", o gerador deverá ser desenergizado pela GCU.

A unidade incorpora um Equipamento Interno de Teste (BITE) capaz de identificar mau funcionamento do sistema de geração de potência, de qualquer unidade do canal ou da fiação, independente de ação do piloto. Sua confiabilidade é maior que a confiabilidade de outros componentes do sistema de geração. Possui auto-testes e testes de confiança em toda proteção para minimizar alarmes falsos durante a missão. Uma falha que possa impedir segurança contínua de vôo da aeronave é extremamente improvável.

O BITE permite isolar os equipamentos falhados com 90% de probabilidade de sucesso. Possui a mesma precisão para

deteção e isolamento de falhas intermitentes ou de estado permanente.
A identificação de equipamento falhado permanece armazenada mesmo em caso de falha total do sistema de geração,persistindo até o sistema ser rearmado manualmente. O mostrador e controle para cada canal de geração estão na face frontal da GCU.

O contator de Linha do Gerador (GLC) é usado para conexão da barra principal ao gerador próprio ou ao gerador oposto, em caso de falha do primeiro. Possui dois conjuntos de contatos normalmente abertos ligados por intertravamento mecânico e duas bobinas de operação, de forma que na posição desenergizado ambos os conjuntos de contatos estão obrigatoriamente abertos e a energização de uma bobina faz os contatos correspondentes fecharem enquanto o outro conjunto permanece aberto e vice-versa quando a outra bobina for energizada.

O Contator de Transferência do Gerador (GTC) deve permitir a conexão do suprimento externo de energia quando em repouso e , quando energizado, permitir a transferência de barras entre geradores.

Um autotransformador reduz 115V AC da barra principal XP1 para 26 V AC que suprem a barra principal de 26 V AC XP3.

4.2.2 - CARACTERÍSTICAS DO SUBSISTEMA DC

Este subsistema supre as exigências normais de potência em corrente contínua e, em condição de emergência elétrica, tem condições de suprir as cargas essenciais para garantir

continuidade de vôo até um pouso seguro.

É formado por duas unidades retificadoras e transformadoras, quatro barras condutoras, uma bateria e um carregador de bateria, além dos equipamentos de comando e proteção do sistema.

4.2.2.1 - CONDIÇÕES NORMAIS DE OPERAÇÃO EM VÔO

A potência elétrica em corrente contínua é convertida por duas Unidades Retificadoras e Transformadoras (TRU), que recebem alimentação em corrente alternada das barras principais XP1 e XP2 .

Cada TRU supre a respectiva barra principal PP1 ou PP2, que são interligadas entre si e ligadas em paralelo à barra essencial PP3.

Uma bateria está desconectada das barras principais e essencial do sistema e diretamente conectada à barra de bateria PP4. A bateria é carregada por um carregador de bateria , conectado à barra principal XP2.

4.2.2.2 - CONDIÇÕES DE FALHA

Em caso de falha de uma TRU, a outra tem condições de suprir todas as cargas normais em corrente contínua.

Ocorrendo falha de ambas TRUs, ambas as barras principais DC devem ser desconectadas automaticamente, enquanto a bateria assistida pelo carregador de bateria devem suprir a barra da bateria e a barra essencial.

Se o sistema de potência AC falhar, a bateria deve

suprir a barra de bateria, a barra essencial DC e as barras essenciais de 26 V AC e 115 V AC através de um inversor estático para assegurar o vôo da aeronave com segurança por, ao menos 20 minutos.

Após falha de ambas TRUs ou perda total de potência (ambos geradores AC falhados), a barra essencial é alimentada pela bateria através do contator de bateria.

4.2.2.3 - ASPECTOS OPERACIONAIS

Cada TRU é usada para transformar 115/200 Volts, 400 Hz de suprimento de potência trifásica em 28 V DC, a fim de alimentar as cargas em corrente contínua.

A TRU1 está ligada à XP1 e a TRU2 está ligada à XP2.

A bateria tem como função o fornecimento de potência de emergência no evento de falha total do sistema principal de geração.

O carregador de bateria deve fornecer recarga rápida e correta, evitando sobrecargas e consequente formação de gases na bateria. No caso de falha no suprimento de potência principal DC, o carregador deve assistir à bateria no suprimento das cargas essenciais da aeronave. Toda falha do sistema bateria-carregador de bateria tem indicação luminosa no painel central de alarme, localizado na cabine. O sistema monitora as funções de sobretensão, falta de tensão na saída, falta de tensão na entrada e sobreaquecimento, desativando o carregador quando ocorrer qualquer dessas condições.

Um contator da Bateria (BC) faz conexão entre a barra da bateria e a barra essencial no caso de falha ou de não energização das TRUs.

Um Relê de Controle do Contator da Bateria (BCCR) possibilita fechamento do contator da bateria quando figurar falha do sistema principal de geração DC.

Um Relé Monitor da Barra da Bateria (BBMR) determina acendimento da luz de advertência de falha do sistema de emergência - "BUS FAIL" - no sistema central de alarmes.

4.3 - ANÁLISE DOS MODOS DE FALHA E SEUS EFEITOS DO SISTEMA DE GERAÇÃO DE POTÊNCIA ELÉTRICA

Foram analisados todos os equipamentos que compõem o sistema elétrico, excluindo apenas fiação, que é periodicamente vistoriada para evitar falhas.

Esta análise encontra-se detalhadamente descrita nas páginas 102 a 147.

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

SUBSISTEMA: GERAÇÃO DE POTÊNCIA AC

EQUIPAMENTO: CONTATOR

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

IDENTIFICAÇÃO DO ITEM: XA-K01

FUNÇÃO: CONEXÃO DE GERADOR A BARRA DE DISTRIBUIÇÃO

1. CASO NO.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA [$\times 10^{-6}$h]	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
1	Contatos falham em aberto	Nenhuma	a) Impossibilidade de conexão de potência as barras XP1 e XP3 b) Os equipamentos conectados a XP1 e XP3 perderão alimentação e/ou redundância	D	Teste de B.I.T.E. acusará falha do tipo FPCDB no B.I.T.E da Unidade de Controle da Geração e no Painel Central de Manutenção.	Nenhuma	Substitua a caixa 21A em primeiro nível de manutenção e substitua o contator KA-K01 em segundo nível de manutenção.	2,000		
2	Contatos falham fechados (Bobina G)	a) Respectivo gerador funcionando normal	a) Nenhum b) Perda de redundância	E	Idem	Idem	Idem	3,000		
		b) No caso de necessidade de alimentação cruzada	a) Não se obtém a alimentação cruzada b) Os equipamentos conectados a XP1 e XP3 perderão alimentação e/ou redundância.	B	Idem	Idem	Idem			
3	Contatos falham fechados (Bobina T)	No caso de necessidade de alimentação cruzada	a) Nenhum b) Nenhum	F	Idem	Idem	Idem	3,000		Há necessidade de monitoramento periódico de funcionamento deste contator.

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

SUBSISTEMA: GERAÇÃO DE POTÊNCIA AC

EQUIPAMENTO: CONTATOR

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

IDENTIFICAÇÃO DO ITEM: XA-K02

FUNÇÃO: CONEXÃO DE GERADOR A BARRA DE DISTRIBUIÇÃO

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA [$x10^{-6}h$]	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
1	Contatos falham em aberto	Nenhuma	a) Impossibilidade de conexão de potência à barra XP2. b) Os equipamentos conectados a XP2 perderão alimentação e/ou redundância. Bateria deixará de receber carga durante o vôo.	D	Teste do B.I.T.E. acusará falha do tipo FPCDB no B.I.T.E da Unidade de Controle da Geração e no Painel Central de Manutenção.	Nenhuma	Substitua a caixa 22A em primeiro nível de manutenção e substitua o contator XA-K02 em segundo nível de manutenção.	2,000		
2	Contatos falham fechados (Bobina G)	a) Respectivo gerador funcionando normal	a) Nenhum b) Perda de redundância	E	Idem	Idem	Idem	3,000		
		b) No caso de necessidade de alimentação cruzada	a) Não se obtém a alimentação cruzada. b) Os equipamentos conectados a XP2 perderão alimentação e/ou redundância. Bateria deixará de receber carga durante o vôo.	B	Idem	Idem	Idem			
3	Contatos falham fechados (Bobina T)	No caso de necessidade de alimentação cruzada.	a) Nenhum b) Nenhum	F	Idem	Idem	Idem	3,000		Há necessidade de monitoramento periódico de funcionamento deste contator.

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

SUBSISTEMA: GERAÇÃO DE POTÊNCIA AC

EQUIPAMENTO: CONTATOR

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

IDENTIFICAÇÃO DO ITEM: XA-K03

FUNÇÃO: CONEXÃO DE FONTE EXTERNA À BARRA DE DISTRIBUIÇÃO OU ALIMENTAÇÃO CRUZADA

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA [$\times 10^{-6}$h]	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
1	Contatos falham em aberto	a) Canal de geração operativo sem necessidade de alimentação cruzada.	a) Nenhum. b) Perda de redundância para alimentar as barras XP1 e XP3.	E	Teste do B.I.T.E. acusará falha do tipo FPCDB no B.I.T.E. da Unidade de Controle da Geração e no Painel Central de Manutenção.	Nenhuma.	Substitua a caixa 21A em primeiro nível de manutenção e substitua o contator XA-K03 em segundo nível de manutenção	4,000		
		b) No caso de necessidade de alimentação cruzada.	a) Impossível transferência de alimentação com consequente desenergização de XP1 e XP3. b) Os equipamentos conectados a XP1 e XP3 perderão alimentação e/ou redundância.	D	A indicação GEN OFF # 1 ilumina no painel 4A e AC ilumina no CWP. Teste do B.I.T.E. acusará falha do tipo FPCDB.	Nenhuma.	Idem.			
2	Contatos falham fechados	a) Canal de geração operativo sem necessidade de alimentação cruzada.	a) Nenhum b) Nenhum	F	Teste do B.I.T.E. acusará falha do tipo FPCDB.	Nenhuma	Idem	4,000		
		b) No caso de necessidade de alimentação cruzada.	a) Nenhum b) Nenhum	F	Teste do B.I.T.E acusará falha do tipo FPCDB.	Nenhuma	Idem			

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

SUBSISTEMA: GERAÇÃO DE POTÊNCIA AC

EQUIPAMENTO: CONTATOR

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

IDENTIFICAÇÃO DO ITEM: XA-K04

FUNÇÃO: CONEXÃO DE FONTE EXTERNA A BARRA DE DISTRIBUIÇÃO OU ALIMENTAÇÃO CRUZADA

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA [x10⁻⁶h]	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
1.	Contatos falham em aberto	a) Canal de geração operativo sem necessidade de alimentação cruzada.	a) Nenhum b) Perda de redundância para alimentar a barra XP2	E	Teste do B.I.T.E. acusará falha do tipo FPCD8 no B.I.T.E da Unidade de Controle da Geração e no Painel Central de Manutenção.	Nenhuma	Substitua a cai 22A em primeiro nível de manutenção e substitua o contator XA-K04 em segundo nível de manutenção.	4,000		
		b) No caso de necessidade de alimentação cruzada.	a) Impossível transferência de alimentação com consequente desenergização de XP2. b) Os equipamentos conectados a XP2 perderão alimentação e/ou redundância.	D	A indicação GEN OFF # 2 ilumina no painel 4A e AC ilumina no CWP. Teste do B.I.T.E. acusará falha do tipo FPCD8.	Nenhuma	Idem			
2	Contatos falham fechados	a) Canal de geração operativo sem necessidade de alimentação cruzada	a) Nenhum b) Nenhum	F	Teste do B.I.T.E. acusará falha do tipo FPCD8.	Nenhuma	Idem	4,000		
		b) No caso de necessidade de alimentação cruzada	a) Nenhum b) Nenhum	F	Teste do B.I.T.E. acusará falha do tipo FPCD8.	Nenhuma	Idem			

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

SUBSISTEMA: GERAÇÃO DE POTÊNCIA AC

EQUIPAMENTO: BARRA DE DISTRIBUIÇÃO AC

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

IDENTIFICAÇÃO DO ITEM: XP1 / XP2

FUNÇÃO: BARRA DE DISTRIBUIÇÃO 115VAC

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA [x10⁻⁶h]	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
1	Curto -circuito	Nenhuma	a) Perda das barras XP1/XP2 b) Os equipamentos conectados a XP1/XP2 perdarão alimentação, e/ou redundância	D	A indicação BUS FAIL # 1/BUS FAIL # 2 ilumina no painel 4A e AC ilumina no CWP.	Nenhuma	Substitua a caixa 21A/22A em primeiro nível e verifique os componentes, em segundo nível.	0,800		

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

SUBSISTEMA: GERAÇÃO DE POTÊNCIA AC

EQUIPAMENTO: BARRA DE DISTRIBUIÇÃO AC

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

IDENTIFICAÇÃO DO ITEM: XP3

FUNÇÃO: BARRA DE DISTRIBUIÇÃO DE 26 VAC

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na acronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA [x10⁻⁶h]	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
1	Curto- circuito	a) Disjuntor CB06 atua.	a) Atuação do disjuntor CB06 causa perda de XP3. XP4 e XP5 serão conectados ao inversor estático. b) Perda de redundância a XP4 e XP5. Perda dos equipamentos conectados a XP3.	E	O disjuntor CB06 estará saltado na caixa 21A.	Nenhuma	Checar o sistema	0,800		
		b) Disjuntor CB06 não abre.	a) Possível dano no autotransformador XA-T05 até atuação da Unidade de Controle de Geração nº1 (GCU # 1)	D	A indicação BUS FAIL # 1 ilumina no painel 4A e AC ilumina no CWP.	Nenhuma	Substituir os componentes danificados			

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

SUBSISTEMA: GERAÇÃO DE POTÊNCIA AC

EQUIPAMENTO: BARRA DE DISTRIBUIÇÃO AC

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

IDENTIFICAÇÃO DO ITEM: XP4

FUNÇÃO: BARRA ESSENCIAL DE DISTRIBUIÇÃO DE 26 VAC

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA [x10⁻⁶h]	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
1	Curto-circuito	a) Disjuntor CB07 atua.	a) Atuação do disjuntor CB07 causa perda de XP4 b) Perda dos equipamentos conectados a XP4.	B	O disjuntor CB07 estará saltado na caixa 21A.	Nenhuma	Checar o sistema	0,800		Estamos considerando que o piloto registra falha dos equipamentos conectados a XP4 no livro de bordo. Assim, o pessoal de apoio no solo detetará os problemas.
		b) Disjuntor CB07 não abre.	a) Possível dano aos equipamentos conectados a XP4 até atuação do disjuntor CB06 b) Possível perda dos equipamentos efetados	B	O disjuntor CB06 estará saltado na caixa 21A.	Nenhuma	Substituição de componentes danificados			Idem *

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

SUBSISTEMA: GERAÇÃO DE POTÊNCIA AC

EQUIPAMENTO: BARRA DE DISTRIBUIÇÃO AC

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

IDENTIFICAÇÃO DO ITEM: XP5

FUNÇÃO: BARRA ESSENCIAL DE DISTRIBUIÇÃO DE 115 VAC

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA [$x10^{-6}h$]	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
1	Curto-circuito	a) Disjuntor CB12 atua.	a) Atuação do disjuntor CB12 causa perda de XP5 b) Perda dos equipamentos conectados a XP5.	B	O disjuntor CB12 estará saltado na caixa 21A	Nenhuma	Checar o sistema.	0,800		Estamos considerando que o piloto registre falha dos equipamentos conectados a XP5 no livro de bordo. Assim, o pessoal de apoio no solo detetará os problemas.
		b) Disjuntor CB12 não abre.	a) Possível dano aos equipamentos conectados a XP5 até atuação da GCU # 1. b) Possível perda dos equipamentos afetados.	B	A indicação BUS FAIL # 1 ilumina no painel 4A e AC ilumina no CWP.	Nenhuma	Substituir os componentes danificados.			Idem *

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

SUBSISTEMA: GERAÇÃO DE POTÊNCIA AC

EQUIPAMENTO: AUTOTRANSFORMADOR

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

IDENTIFICAÇÃO DO ITEM: XA-T05

FUNÇÃO: REDUZIR 115 VAC a 26VAC

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA [x10^{-6}h]	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
1	Curto-circuito	a) Disjuntor CB06 atua	a) Atuação do disjuntor CB06 causa perda de XP3. XP4 e XP5 serão conectadas ao inversor estático. b) Perda de redundância a XP4 e XP5. Perda dos equipamentos conectados a XP3.	E	O disjuntor CB06 estará saltado na caixa 21A.	Nenhuma	Substituir o autotransformador e checar o sistema.	1,200		Estamos considerando que o piloto registre falha dos equipamentos conectados a XP3 no livro de bordo, Assim o pessoal de apoio no solo detetará os problemas.
		b) Disjuntor CB06 não abre.	a) O curto-circuito persiste até atuação da GCU # 1. b) Perda dos equipamentos conectados a XP1 e XP3. Perda de redundância a XP4 e XP5.	D	A indicação BUS FAIL # 1 ilumina no painel 4A e AC ilumina no CWP.	Nenhuma	Substituir os componentes danificados.			Idem *
2	Circuito aberto	Nenhuma	a) Perda de XP3. XP4 e XP5 estarão conectadas ao inversor estático. b) Perda de redundância a XP4 e XP5. Perda dos equipamentos conectados a XP3.	E	Nenhuma	Nenhuma	Substitua o autotransformador	1,200		Idem

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

SUBSISTEMA: GERAÇÃO DE POTÊNCIA DC

EQUIPAMENTO: UNIDADE DE TRANSFORMAÇÃO E RETIFICAÇÃO

IDENTIFICAÇÃO DO ITEM: T R U # 1

.FUNÇÃO: TRANSFORMAR 115 VAC em 28 VDC

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA [x10⁻⁶h]	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
1	Sem tensão de saída	a) Falha simples	a) Perda de redundância a PP1 e PP3. b) Nenhum	E	Quando a causa da falha for sobre-aquecimento do TRU # 1, haverá indicação no Painel Central de Manutenção (CMP)	Nenhuma	Substitua o TRU # 1	26,400		
		b) Se o TRU # 2 também falhou	a) Perda de PP1 e PP2. PP3 ficará sendo alimentada pela bateria e carregador de bateria no modo "Tensão Constante". b) O vôo estará restrito devido a perda de PP1 e PP2.	B	A indicação DC ilumina no CWP. Haverá indicação BUS # 1 FAIL e BUS # 2 FAIL no painel 4A. Quando a causa da falha for sobre-aquecimento haverá indicação no CMP.	Desligue cargas não essenciais DC. Pouse tão rápido quanto possível.	Substitua e verifique ambos TRU's.			
		c) Com PP1 desenergizada	a) Perda de redundância a PP2 e PP3. b) Perda dos equipamentos conectados a PP1.	B	A indicação DC ilumina no CWP. BUS # 1 FAIL ilumina no painel 4A. Quando a causa da falha do TRU # 1 for sobreaquecimento, haverá indicação no CMP.	Desligue cargas não essenciais DC; Pouse tão rápido quanto possível.	Verifique os equipamentos danificados e substitua-os			
		d) Com PP2 desenergizada	a) Perda de PP1 e PP2. Perda de redundância a PP3. b) Perda dos equipamentos conectados a PP1 e PP2.	B	A indicação DC ilumina no CWP. BUS # 1 FAIL e BUS # 2 FAIL iluminam no painel 4A. Quando a causa da falha do TRU # 1 for sobreaquecimento, haverá indicação no CMP.	Desligue cargas não essenciais DC. Pouse tão rápido quanto possível.	Verifique os equipamentos danificados e substitua-os			
2	Baixa tensão de saída DC							26,800		*
3	"Ripple" de tensão excessivamente alto							26,800		*

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

SUBSISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA DC

EQUIPAMENTO: UNIDADE DE TRANSFORMAÇÃO E RETIFICAÇÃO

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

IDENTIFICAÇÃO DO ITEM: TRU # 2

FUNÇÃO: TRANSFORMAR 115 VAC EM 28 VDC

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA [x10^{-6}h]	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
1	Sem tensão de saída	a) Falha simples	a) Perda de redundância a PP2 e PP3. b) Nenhum	E	Quando a causa da falha for sobreaquecimento do TRU # 2, haverá indicação no Painel Central de Manutenção (CMP).	Nenhuma	Substitua o TRU # 2	26,400		
		b) Se o TRU # 1 também falhou	a) Perda de PP1 e PP2. PP3 ficará sendo alimentada pela bateria e carregador de bateria no modo "Tensão Constante". b) O vôo estará restrito devido a perda de PP1 e PP2.	B	A indicação DC ilumina no CWP. Haverá indicação BUS # 1 FAIL e BUS # 2 FAIL no painel 4A. Quando a causa da falha for sobre aquecimento, haverá indicação no CMP.	Desligue cargas não essenciais DC. Pouse tão rápido quanto possível.	Substitua e verifique ambos TRU's.			
		c) Com PP2 desenergizada	a) Perda de redundância a PP1 e PP3. b) Perda dos equipamentos conectados a PP2.	B	A indicação DC ilumina no CWP. BUS # 2 FAIL ilumina no painel 4A. Quando a causa da falha do TRU # 2 for sobreaquecimento, haverá indicação no CMP.	Desligue cargas não essenciais DC. Pouse tão rápido quanto possível.	Verifique os equipamentos danificados e substitua-os.			
		d) Com PP1 desenergizada	a) Perda de PP1 e PP2. Perda de redundância a PP3. b) Perda dos equipamentos conectados a PP2.	B	A indicação DC ilumina no CWP. BUS # 1 FAIL e BUS # 2 FAIL iluminam no painel 4A. Quando a causa da falha do TRU # 2 for sobre-aquecimento, haverá indicação no CMP.	Desligue cargas não essenciais DC. Pouse tão rápido quanto possível.	Verifique os equipamentos danificados e substitua-os.			
2	Baixa tensão de saída DC.							26,800		*
3	"Ripple" de tensão excessivamente alto							26,800		*

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

SUBSISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA DC

EQUIPAMENTO: CONTATOR DA BATERIA

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

IDENTIFICAÇÃO DO ITEM: PA - K03

FUNÇÃO: CONECTAR A BARRA DE BATERIA A BARRA ESSENCIAL DC

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA ($x10^{-6}h$)	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
1	Contatos falham fechados	a) Condição normal de geração AC/DC.	a) PP3 será conectada a PP1, PP2 e PP4 ao mesmo tempo. A carga da bateria passará a ocorrer sem controle b) Possibilidade de avalanche térmica	D	A indicação DC ilumina no CWP. SYS FAIL ilumina no painel 4A.	Pouse tão rápido quanto praticável	Substitua o contator da bateria e verifique a bateria	1,000		
		b) Falha total de geração de potência AC ou falha de ambos TRU's	a) Nenhuma b) Nenhuma	C	Nenhuma	Desligue cargas não essenciais DC; Pouse tão rápido quanto possível	Substitua contator da bateria e verifique todo o sistema de geração AC/DC.			
2	Contatos falham em aberto	a) Falha simples	a) Perda de conexão entre PP3 e PP4 durante situação de emergência. b) Perda de redundância a PP3.	E	Nenhuma	Nenhuma	Nenhuma	1,000		Falha dormente. Gostaríamos de sugerir a aplicação periódica do documento TP071A3002 Estágio C, item 4. Esse procedimento pode detectar a falha, evitando situações perigosas.
		b) Falha em ambos TRU's	a) Perda de PP1; PP2 e PP3. Perda de redundância a XP4/XP5. b) Perda do equipamento conectado ao sistema de geração DC e perda de redundância às barras XP4 e XP5.	D.	As indicações TRU # 1 e TRU # 2 iluminam no CWP se a causa da falha dos TRU's for sobreaquecimento.	Pouse tão rápido quanto possível.	Verifique todo o sistema elétrico de geração e execute os reparos necessários			Estamos considerando que o piloto registre falha dos equipamentos conectados às barras em falta, no livro de bordo. Assim, o pessoal de apoio no solo identificará os problemas.
		c) Perda de ambos canais de geração.	a) Perda de XP1, XP2, XP3, XP4, XP5, PP1, PP2 e PP3, restando somente PP4. b) Situação de emergência elétrica restrita a PP4.	A						Falha Múltipla

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

SUBSISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA DC

IDENTIFICAÇÃO DO ITEM: PA - K02

FUNÇÃO: ENERGIZAR O CONTATOR DE BATERIA QUANDO FOREM PERDIDAS PP1 e PP2.

EQUIPAMENTO: RELÉ DE CONTROLE DO CONTATOR DA BATERIA

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA [x10⁻⁶h]	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
1	Contatos falham abertos.	Falha simples	a) Atuação de K03. PP3 estará conectada a PP1, PP2 e PP4 ao mesmo tempo. A carga da bateria passará a ocorrer sem controle. b) Possibilidade de avalanche térmica.	C	A indicação SYS FAIL ilumina no painel 4A. DC ilumina no CWP.	Desligue a chave de bateria	Substitua o relé.	1,000		
2	Contatos falham fechados	a) Falha simples	a) Impossibilidade da conexão PP3 - PP4 durante situação de emergência. b) Perda de redundância a PP3.	E	Nenhuma	Nenhuma	Substitua o relé	1,000		Falha dormente. Gostaríamos de sugerir a aplicação periódica do documento TP071A3002 - Estágio C, item 4. Esse procedimento pode detetar a falha, evitando situações perigosas.
		b) Ambos TRU's falhados	a) Perda de PP1, PP2 e PP3. Perda de redundância a XP4 e XP5. b) Perda dos equipamentos conectados ao sistema de geração DC e perda de redundância às barras essenciais AC XP4 e XP5.	D	O piloto sente a perda dos equipamentos de navegação e comunicação. Haverá indicação de TRU falhado no CWP em caso de sobreaquecimento.	Pouse tão rápido quanto possível.	Verifique todo o sistema elétrico de geração.			
		c) Ambos canais de geração AC falhados.	a) Perda de XP1, XP2, XP3, XP4, XP5, PP1, PP2 e PP3, restando somente PP4. b) Situação de emergência elétrica restrita a PP4.	A	Haverá indicação de perda do primeiro canal de geração, e após isso, haverá perda de todos instrumentos e indicações.	Pouse tão rápido quanto possível.	Verifique todo o sistema elétrico e execute os reparos necessários.			Falha múltipla

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

SUBSISTEMA: GERAÇÃO DE POTÊNCIA DC

EQUIPAMENTO: CHAVE DA BATERIA

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

IDENTIFICAÇÃO DO ITEM: PA - S01

FUNÇÃO: Tornar possível a conexão entre PP3 e PP4

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA [x10⁻⁶h]	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
1	Falha em aberto	Falha simples	a) Impossibilidade de conexão entre PP3 e PP4 em situação de emergência. b) Perda de redundância a PP3.	E	Nenhuma	Nenhuma	Substituir a chave de bateria	2,132		
2	Falha fechado	Relé K02 falha aberto	a) Atuação de K03. PP3 estará conectada a PP1, PP2 e PP4, ao mesmo tempo. A carga da bateria passará a ocorrer sem controle. b) Possibilidade de avalanche térmica.	D	A indicação SYS FAIL ilumina no painel 4A. DC ilumina no CWP.	Pouse tão cedo quanto praticável.	Substitua a chave de bateria e o relé K02.	0,406		

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

SUBSISTEMA: GERAÇÃO DE POTÊNCIA DC

IDENTIFICAÇÃO DO ITEM: PA - K06

FUNÇÃO: CONEXÃO DE ALIMENTAÇÃO AC AO CARREGADOR DE BATERIA

EQUIPAMENTO: RELÉ

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA [$\times 10^{-6}$h]	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
1	Falha aberto	Falha simples	a) Carregador da bateria desenergizado. Bateria não receberá carga durante o vôo. b) Perda de redundância a PP3.	B	Nenhuma	Nenhuma	Nenhuma	1,000		Falha dormente. Existe previsão de re-projeto para prover indicação de carregador da bateria desenergizado, no CMP. Em consequência, o pessoal de apoio no solo terá informação da falha.
2	Falha fechado	Falha simples	a) Nenhum b) Nenhum	F	Nenhuma	Nenhuma	Nenhuma	1,000		Falha dormente. A aplicação do documento TP071A2004- Estágio B pode detetar a falha.

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

SUBSISTEMA: GERAÇÃO DE POTÊNCIA DC

EQUIPAMENTO: DIODO

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

IDENTIFICAÇÃO DO ITEM: PA - D03/PA - D04

FUNÇÃO: CONEXÃO DE PP2/PP1 a PP3

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA [$x10^{-6}h$]	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
1	Curto - Circuito	a) Falha simples	a) Nenhum b) Nenhum	F	Nenhuma	Nenhuma		0,200		Falha dormente. Gostaríamos de sugerir a aplicação periódica do documento. TP071A3002-Estágio C, item 4. Este procedimento pode mostrar e previnir situações perigosas. *
		b) TRU # 1 e TRU#2 falhados								*
2	Circuito aberto	a) Falha simples	a) Perda de redundância a PP3 b) Nenhum	F	Nenhuma	Nenhuma		0,200		*
		b) Ambos diodos abertos	a) Perda de PP3. Perda do carregador de bateria. b) Perda de equipamentos essenciais conectados a PP3.	B	Indicação indireta pela perda dos equipamentos de navegação e comunicação conectados a PP3.	Pouse tão rápido quanto praticável.	Pesquise falhas e substitua os diodos.			*

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

SUBSISTEMA: GERAÇÃO DE POTÊNCIA DC

EQUIPAMENTO: RELÉ

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

IDENTIFICAÇÃO DO ITEM: PA - K04/PA - K05

FUNÇÃO: INDICAR FALHA DE PP1/PP2 NO CMP E NO PAINEL 4A

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA ($\times 10^{-6}$/h)	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
1	Falha aberto	Nenhuma	a) Falsa indicação BUS # 1 FAIL/BUS#2 FAIL no painel 4A. b) Nenhum	F	Nenhuma	Nenhuma	Pesquisar a falha e substituir K04/K05.	1,000		Indicação falsa pode causar aborto da missão, desnecessáriamente.
2	Falha fechado	a) Falha simples	a) Nenhum b) Nenhum	F	Nenhuma	Nenhuma	Nenhuma	1,000		Falha dormente. Gostaríamos de sugerir a aplicação periódica do documento TP071A3002 - Estágio C, item 4. Este procedimento pode mostrar e previnir situações perigosas.
		b) PP1/PP2 falha	a) Perda de monitoramento de falha de PP1/PP2. b) Perda dos equipamentos conectados a PP1/PP2	B	Nenhuma	Nenhuma	Nenhuma			Idem

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

SUBSISTEMA: GERAÇÃO DE POTÊNCIA DC

EQUIPAMENTO: RELÉ MONITOR DA BARRA DE BATERIA

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

IDENTIFICAÇÃO DO ITEM: PA - K01

FUNÇÃO: INDICAR PERDA DA BARRA DE BATERIA

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
1	Falha aberto	Nenhuma	a) Falsa indicação de BUS FAIL no painel 4A. b) Nenhuma	F	Nenhuma	Nenhuma	Pesquisar a falha e substituir K01	1,000		Falsa indicação pode causar aborto da missão.
2	Falha fechado	a) Falha simples	a) Nenhuma b) Nenhuma	F	Nenhuma	Nenhuma	Pesquisar a falha e substituir K01	1,000		Falha dormente. Gostaríamos de sugerir a aplicação periódica do documento TP071A3002 - Estágio C, item 4. Este procedimento pode mostrar e prevenir situações perigosas
		b) Falha da barra PP4	a) K01 impede indicação de falha de PP4. Perda de redundância a PP3. b) Perda de suprimento de potência de emergência.	E	Nenhuma	Nenhuma	Idem			Idem

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

SUBSISTEMA: GERAÇÃO DE POTÊNCIA DC

EQUIPAMENTO: BATERIA

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

IDENTIFICAÇÃO DO ITEM: PA - BT01

PARTIDA DO GERADOR DE GÁS; SUPRIMENTO DE POTÊNCIA ELÉTRICA

FUNÇÃO: EM SITUAÇÃO DE EMERGÊNCIA.

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA [$\times 10^{-6}$h]	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
1	Termistor curto-circuitado.	Falha simples	a) Carregador de bateria desliga e a bateria não recebe carga. b) Prejuízo ao sistema de emergência elétrica.	E	Nenhuma	Nenhuma		2,000		Gostaríamos de sugerir teste do termistor a cada 150 horas de vôo durante manutenção, como indicado no documento. AP071A5008/A, item 2.2.
2	Termistor aberto	a) Falha simples	a) Carregador de bateria permanece conectado a bateria b) Nenhuma	E	Nenhuma	Nenhuma		2,000		Há previsão de anunciação da falha no CMP.
		b) "Thermoswitch" fechada na condição de modo de carga.	a) Processo ininterrupto de carga com sobretemperatura da bateria e possível dano subsequente. b) Perigo de explosão ou fogo.	A	Não ainda	Nenhuma				Há previsão de inspeção periódica.
		c) "Thermoswitch" fechada na condição de tensão constante.	a) Nenhuma b) Nenhuma	E	Não ainda	Nenhuma				Idem
3	Tensão muito baixa	a) Falha simples	a) Tensão muito baixa em PP4. b) Perda de redundância a PP3.	E	Nenhuma	Nenhuma		2,000		Há previsão de verificação de tensão nas barras a cada 100 horas de vôo.
		b) Perda total de geração AC/DC	a) PP4 não é conectada a PP3. b) Perda total de potência elétrica.	A	Nenhuma	Pouse tão rápido quanto possível	Revisão completa do sistema			Falha múltipla

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

SUBSISTEMA: GERAÇÃO DE POTÊNCIA DC

EQUIPAMENTO: BATERIA

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

IDENTIFICAÇÃO DO ITEM: PA - BT01

FUNÇÃO: PARTIDA DO GERADOR DE GÁS. SUPRIMENTO DE POTÊNCIA ELÉTRICA EM SITUAÇÃO DE EMERGÊNCIA

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA [$x10^{-6}h$]	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
4	Vazamento de eletrólito	Nenhuma	a) Súbito aumento de temperatura da bateria dificultando carga total. b) O sistema de emergência ficará prejudicado.	E	Cheque do nível de eletrólito.	Nenhuma	Inspecionar a bateria a cada 150 horas de vôo ou 6 meses de operação da aeronave. Substituir a bateria.	2,000		
5	"Thermoswitch" aberta	Nenhuma	a) Carregador de bateria desenergizado. A bateria não recebe carga durante o vôo b) Nenhum	E	Nenhuma	Nenhuma		2,000		Há previsão de inspeção periódica.
5	"Thermoswitch" fechada	Falha simples	a) Perda de redundância a proteção de sobre-aquecimento da bateria b) Nenhum	E	Nenhuma	Nenhuma		2,000		Idem
7	Queda de tensão durante a partida	Temperatura muito baixa.	a) Tensão em PP4 abaixo do valor normal. b) Possível perda de partida pela bateria. Possível funcionamento de equipamentos essenciais em condição de sub-tensão se a falha múltipla ocorre.	C	Nenhuma	Nenhuma	Substituir a bateria	2,000		A resistência das células deve ser checada por manutenção programada a cada 150 horas de vôo ou 6 meses de operação da aeronave.
8	Sobre-carga da bateria							2,000		Há previsão de indicação da falha no CMP.
9	"Thermistor" falha de isolamento para terra.							2,000		Idem

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

SUBSISTEMA: GERAÇÃO DE POTÊNCIA DC

EQUIPAMENTO: BATERIA

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

IDENTIFICAÇÃO DO ITEM: PA - BT01

FUNÇÃO: PARTIDA DO GERADOR DE GÁS. SUPRIMENTO DE POTÊNCIA ELÉTRICA EM SITUAÇÃO DE EMERGÊNCIA.

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA ($\times 10^{-6}$h)	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
10	"Thermistor", falha de isolamento para 28 VDC	Falha simples	a) Haverá interrupção no carregamento da bateria b) Nenhuma	E	Nenhuma	Nenhuma	Inspecione a bateria a cada 150 horas de vôo ou 6 meses de operação da aeronave	2,000	Fabricante	

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

SUBSISTEMA: GERAÇÃO DE POTÊNCIA DC

EQUIPAMENTO: BARRA DE DISTRIBUIÇÃO DC

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

IDENTIFICAÇÃO DO ITEM: PP1

FUNÇÃO: BARRA DE DISTRIBUIÇÃO DE 28 VDC

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA [$x10^{-6}h$]	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
1	Curto - circuito	Falha simples	a) Perda da barra. Perda de redundância a PP2 e PP3. b) Perda dos equipamentos conectados a PP1.	D	A indicação BUS # 1 FAIL ilumina no painel 4A. DC ilumina no CWP. Atuação do fusível PA-F08 e/ou PA-F09. Disjuntor PA-CB01 abre, isolando a falha.	Vôo com limitação devido a perda de equipamentos conectados a PP1.	Verificar e substituir os componentes nas caixas 21A/22A.	0,800		

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

SUBSISTEMA: GERAÇÃO DE POTÊNCIA DC

EQUIPAMENTO: BARRA DE DISTRIBUIÇÃO DC

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

IDENTIFICAÇÃO DO ITEM: PP2

FUNÇÃO: BARRA DE DISTRIBUIÇÃO DE 28 VDC

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA [$x10^{-6}h$]	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
1	Curto - circuito	Falha simples	a) Perda da barra PP2. Perda de redundância a PP1 e PP3. b) Perda dos equipamentos conectados a PP2.	D	A indicação BUS # 2 FAIL ilumina no painel 4A. DC ilumina no CWP. Atuação do fusível PA-F09 e/ou F08. Disjuntor PA-CB02 abre, isolando a falha.	Vôo com limitação devido a perda de equipamento conectados a PP2.	Verificar e substituir os componentes nas caixas 21A/ 22A.	0,800		

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

SUBSISTEMA: GERAÇÃO DE POTÊNCIA DC

EQUIPAMENTO: BARRA DE DISTRIBUIÇÃO DC

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

IDENTIFICAÇÃO DO ITEM: PP3

FUNÇÃO: BARRA DE DISTRIBUIÇÃO DE 28 VDC

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA ($\times 10^{-6}$h)	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
1	Curto - circuito	Falha simples	a) Perda da barra PP3. b) Perda dos equipamentos conectados a PP3.	D	Atuação do fusível PA-F01 e/ou PA-F07 e PA-F02 na caixa 22A.	Vôo com limitação devido a perda de equipamentos conectados a PP3.	Verificar e substituir componentes nas caixas 21A e 22A.	0,800		

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

SUBSISTEMA: GERAÇÃO DE POTÊNCIA DC

EQUIPAMENTO: BARRA DE DISTRIBUIÇÃO DC

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

IDENTIFICAÇÃO DO ITEM: PP4

FUNÇÃO: BARRA DE DISTRIBUIÇÃO DA BATERIA

1 CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA ($\times 10^{-6}$h)	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
1	Curto - circuito	Falha simples	a) Perda da barra PP4. Impossibilidade de suprimento de emergência a PP3. Perda do sistema de partida do APU. b) Perda do sistema de potência de emergência.	D	A indicação BUS FAIL ilumina no painel 4A. DC ilumina no CWP. O fusível PA-F06 atua na caixa 23A.	Pouse tão cedo quanto praticável.	Verifique e substitua os componentes na caixa 23A.	0,800		

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

SUBSISTEMA: GERAÇÃO DE POTÊNCIA AC

EQUIPAMENTO: INVERSOR ESTÁTICO

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

IDENTIFICAÇÃO DO ITEM: XA - PS01

FUNÇÃO: SUPRIMENTO DE POTÊNCIA AC EM SITUAÇÃO DE EMERGÊNCIA

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA ($\times 10^{-6}$h)	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
1	Falta tensão de saída 115 VAC	a) Falha simples	a) Perda de redundância a XPS. b) Nenhuma	E	Haverá indicação de Inversor Inoperativo no CMP.	Nenhuma	Substituir o inversor estático.	100,0		Gostaríamos de sugerir a aplicação do documento TP071A2002, Procedimento 8 - após a substituição do inversor estático.
		b) Falta tensão de saída 26 VAC	a) Perda de redundância a XP4 e XPS. b) Nenhuma	E	Idem	Nenhuma	Substituir o inversor estático			Idem
2	Falta tensão de saída 26 VAC	Falha simples	a) Perda de redundância a XP4. b) Nenhuma	E	Nenhuma	Nenhuma	Substituir o inversor estático.	100,0		A aplicação periódica do documento TP071A2002 Procedimento 8 , pode detetar a falha.

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

SUBSISTEMA: GERAÇÃO DE POTÊNCIA AC

EQUIPAMENTO: CONTATOR

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

IDENTIFICAÇÃO DO ITEM: XA - K05

FUNÇÃO: EM SITUAÇÃO NORMAL, CONECTAR XP3 a XP4 e XP1 a XP5. EM SITUAÇÃO DE EMERGÊNCIA, CONECTAR O INVERSOR ESTÁTICO A XP4 e XP5

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA ($x10^{-6}h$)	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
1	Falha aberto	a) Falha simples	a) Inversor estático energiza XP4 e XP5 continuamente. Perda de redundância a XP4 e XP5. b) Nenhum	E	Nenhuma	Nenhuma	Substituir o contator	4,000		A aplicação periódica do documento TP71A2002-Procedimento 8 pode detetar a falha.
		b) Perda de tensão de saída de 26 VAC do inversor estático.	a) Perda de XP4 b) Limitação de vôo devido a perda de equipamentos conectados a XP4.	D	Perda dos equipamentos conectados a XP4.	Vôo com limitação devido a perda de equipamentos conectados a XP4.	Substituir o contator e o inversor estático			
		c) Perda de tensão de saída de 115 VAC do inversor estático	a) Perda de XP5. b) Limitação de vôo devido a perda de equipamentos conectados a XP5.	D	Haverá indicação de inversor inoperativo no CMP. Perda dos equipamentos conectados a XP5.	Vôo com limitação considerando perda dos equipamentos conectados a XP5.	Substituir o contator e o inversor estático.			
		d) Perda de tensão de saída de 26 VAC e 115 VAC do inversor estático	a) Perda de XP4 e XP5. b) Limitação de vôo devido a perda de equipamentos conectados a XP4 e XP5.	D	Haverá indicação de inversor inoperativo no CMP. Perda dos equipamentos conectados XP4 e XP5.	Vôo com limitação considerando perda dos equipamentos conectados a XP4 e XP5.	Substituir o contator e o inversor estático			
2	Falha fechado	a) Falha simples	a) Perda de redundância a XP4 e XP5. b) Nenhum	E	Nenhuma	Nenhuma	Substituir o contator	4,000		Como Ítem 1.a)
		b) XP1 falha	a) Perda de XP4 e XP5 b) Perda de equipamentos conectados a XP4 e XP5, além de XP1 e XP3, devido a falha múltipla.	D	Haverá indicação da perda de XP1 no painel 4A. Perda dos equipamentos conectados a XP4, XP5, XP1 e XP3	Pousar tão rápido quanto possível.	Revisão geral			Falha múltipla

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

SUBSISTEMA: GERAÇÃO DE POTÊNCIA AC

EQUIPAMENTO: CONTATOR

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

IDENTIFICAÇÃO DO ITEM: XA-K05

FUNÇÃO: EM SITUAÇÃO NORMAL, CONECTAR XP3 a XP4 e XP1 a XP5. EM SITUAÇÃO DE EMERGÊNCIA, CONECTAR O INVERSOR ESTÁTICO A XP4 e XP5.

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA ($x10^{-6}$h)	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
		c) XP3 falha	a) Perda de XP4. Perda de redundância a XP5. b) Perda de equipamentos conectados a XP4, além de perda de XP3, devido a falha múltipla.	D	Perda dos equipamentos conectados a XP3 e XP4.	Vôo com limitação devido a perda dos equipamentos conectados a XP3 e XP4.	Substituir o contator. Revisão geral.			

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

SUBSISTEMA: GERAÇÃO DE POTÊNCIA AC

EQUIPAMENTO: CONTATOR

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

IDENTIFICAÇÃO DO ITEM: XA - K06

FUNÇÃO: MONITORAMENTO DE INDICAÇÃO DE FUNCIONAMENTO DO INVERSOR ESTÁTICO NO CMP.

1 CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA ($\times 10^{-6}$/h)	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
1	Falha aberto	a) Falha simples	a) Perda da função de monitoramento. b) Nenhuma	F	Haverá indicação indevida do inversor estático inoperante	Nenhuma	Substituir o contator	4,000		Após possível substituição do inversor estático, a aplicação da TP071A2002 - Procedimento 8 poderá fazer detetar a falha do contator.
		b) Contator XA-K07 falha aberto.	a) Perda da função de monitoramento b) Nenhuma	F	Nenhuma	Nenhuma	Substituir os contatores			Idem
		c) Contator XA-K07 falha fechado.	a) Perda da função de monitoramento. b) Nenhuma	F	Haverá indicação imprópria de inversor inoperativo no CMP.	Nenhuma	Substituir os contatores			Idem
2	Falha fechado	a) Falha simples	a) Perda da função de monitoramento. b) Nenhuma	F	Nenhuma	Nenhuma	Substituir o contator	4,000		Idem
		b) Contator XA-K07 falha aberto	a) Perda da função de monitoramento b) Nenhuma	F	Nenhuma	Nenhuma	Substituir os contatores			Idem
		c) Contator XA-K07 falha fechado	a) Perda da função de monitoramento b) Nenhuma	F	Nenhuma	Nenhuma	Substituir os contatores			Idem

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

SUBSISTEMA: GERAÇÃO DE POTÊNCIA AC

EQUIPAMENTO: CONTATOR

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

IDENTIFICAÇÃO DO ITEM: XA - K07

FUNÇÃO: MONITORAMENTO DE INDICAÇÃO DE FUNCIONAMENTO DO INVERSOR ESTÁTICO NO CMP.

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA ($\times 10^{-6}$h)	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
1	Falha aberto	Falha simples	a) Perda da função de monitoramento b) Nenhuma	F	Nenhuma	Nenhuma	Substituir o contator	4,000		Após possível substituição do inversor estático, a aplicação do documento TP071A2002 - Procedimento 8, pode detetar a falha do contator.
2	Falha fechado	Falha simples	a) Perda da função de monitoramento b) Nenhuma	F	Nenhuma	Nenhuma	Substituir o contator	4,000		Idem

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

SUBSISTEMA: GERAÇÃO DE POTÊNCIA AC

IDENTIFICAÇÃO DO ITEM: CTA

FUNÇÃO: MONITORAR A CORRENTE DA FASE DO GERADOR

EQUIPAMENTO: CONJUNTO TRANSFORMADOR DE CORRENTE DE LINHA

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA ($\times 10^{-6}$h)	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
1	Transformador de corrente aberto ou em curto.	Falha simples	a) A Unidade de Controle da Geração (GCU) sente a falta diferencial. A proteção diferencial desliga o gerador. Perda de saída de um canal de geração. b) Perda de redundância de Geração de Potência AC.	C	As indicações GEN OFF e AC iluminam no painel. O B.I.T.E. operacional indicará FFDR.	Nenhuma	Substituir o CTA	1,000		

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

SUBSISTEMA: GERAÇÃO DE POTÊNCIA AC

IDENTIFICAÇÃO DO ITEM: TCT

FUNÇÃO: MONITORAR A CORRENTE DE FASE DA LINHA DE TRANSFERÊNCIA

EQUIPAMENTO: CONJUNTO TRANSFORMADOR DE LINHA DE TRANSFERÊNCIA

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA [$\times 10^{-6}$h]	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
1	Transformador de corrente aberto ou em curto.	Falha simples	a) Perda da proteção de corrente da linha de transferência. b) Nenhum	E	Nenhuma	Nenhuma	Substituir o TCT	1,000		Falha dormente. Gostaríamos de sugerir a aplicação periódica do documento TP071A2002-Estágio B, para detetar a falha.

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

SUBSISTEMA: GERAÇÃO DE POTÊNCIA AC

EQUIPAMENTO: REGULADOR DE VELOCIDADE

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

IDENTIFICAÇÃO DO ITEM: C S D

FUNÇÃO: CONVERTER A VELOCIDADE VARIÁVEL DO MOTOR EM VELOCIDADE CONSTANTE DE SAÍDA DE 12000 REVOLUÇÕES POR MINUTO.

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA ($\times 10^{-6}$h)	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
1	Potência de entrada não é transmitida.	Nenhuma	a) Perda de um canal de geração elétrica. b) Perda de redundância de geração de potência AC.	C	As indicações GEN OFF e AC iluminam no painel. B.I.T.E. operacional indicará falha do gerador integrado (IDG)	Nenhuma	Substituir o IDG	0,610	AE-7713 Revisão C	
2	Desconexão prematura	Nenhuma	a) Perda de um canal de geração elétrica. b) Perda de redundância de geração de potência AC.	C	As indicações GEN OFF e AC iluminam no painel. B.I.T.E. operacional indicará falha do IDG.	Nenhuma	Substituir o IDG	1,088	Idem	
3	Falha de desconexão	Nenhuma	a) Operação do IDG em temperaturas excessivamente altas pode resultar em dano ao IDG e possível perda de um canal de geração elétrica. b) Perda de redundância de geração de potência AC.	C	As indicações GEN OFF e AC iluminam no painel. B.I.T.E. operacional indicará falha do IDG.	Nenhuma	Substituir o IDG	0,272	Idem	Dano do IDG leva a atuação do circuito de proteção.
4	Unidade Hidráulica Variável - perda de saída da unidade fixa	Nenhuma	a) Possível extensão do dano interno ao mecanismo regulador. Perda de saída regulada e perda de saída elétrica de um canal de geração. b) Perda de redundância de geração de potência AC.	C	As indicações GEN OFF e AC iluminam no painel. B.I.T.E. operacional indicará falha do IDG.	Nenhuma	Substituir o IDG	2,698	Idem	
5	Unidade Hidráulica Variável - degradação na saída da unidade fixa.	Nenhuma	a) Resposta lenta ou irregular ao mecanismo de entrada pode resultar em excessiva flutuação de frequência do canal. Desligamento por sobrefrequência ou subfrequência. Perda de um canal de geração de potência AC. b) Perda de redundância de geração de potência AC	C	As indicações GEN OFF e AC iluminam no painel. B.I.T.E. operacional indicará falha do IDG.	Nenhuma	Substituir o IDG	1,772	Idem	

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

SUBSISTEMA: GERAÇÃO DE POTÊNCIA AC

EQUIPAMENTO: REGULADOR DE VELOCIDADE

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

IDENTIFICAÇÃO DO ITEM: C S D

FUNÇÃO: CONVERTER A VELOCIDADE VARIÁVEL DO MOTOR EM VELOCIDADE CONSTANTE DE SAÍDA DE 12000 REVOLUÇÕES POR MINUTO.

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA ($\times 10^{-6}$h)	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
6	Unidade Hidráulica Fixa. Falta saída ao mecanismo diferencial.	Nenhuma	a) Possível extensão do dano interno ao mecanismo regulador. Perda de saída regulada e perda de saída elétrica de um canal de geração. b) Perda de redundância de geração de potência AC.	C	As indicações GEN OFF e AC iluminam no painel. B.I.T.E. operacional indicará falha do IDG.	Nenhuma	Substitua o IDG	1,962	RE-7713 Revisão C	
7	Unidade Hidráulica Fixa - Degradação na saída do mecanismo diferencial	Nenhuma	a) Resposta lenta ou irregular ao mecanismo de entrada, pode resultar em excessiva flutuação de frequência do canal. Possível desligamento por sobrefrequência ou subfrequência com perda de um canal de geração de potência AC. b) Perda de redundância de geração de potência AC.	C	As indicações GEN OFF e AC iluminam no painel. B.I.T.E. operacional indicará falha do IDG.	Nenhuma	Substitua o IDG	1,308	Idem	
8	Unidade de Mecanismo Diferencial - Nenhuma saída - falha em transmitir potência de entrada recebida da caixa de engrenagem do motor e/ou falha ao transmitir velocidade de entrada compensada das unidades hidráulicas.	Nenhuma	a) Nenhuma saída elétrica de um canal de geração b) Perda de redundância de geração de potência AC.	C	As indicações GEN OFF e AC iluminam no painel. B.I.T.E. operacional indicará falha do IDG.	Nenhuma	Substitua o IDG	5,200	Idem	Dano do IDG leva a atuação do circuito de proteção.
9	Engrenagem de Transmissão - não transfere potência ao regulador e bombas.	Nenhuma	a) Subfrequência na saída do canal de geração. Circuito de proteção contra subfrequência atua. Perda de saída de um canal de geração. b) Perda de redundância de geração de potência AC.	C	As indicações GEN OFF e AC iluminam no painel. B.I.T.E. operacional indicará falha do IDG.	Nenhuma	Substitua o IDG	0,650	Idem	
10	Bomba de pressão - sem pressão de carga	Nenhuma	a) Dano interno ao IDG. Perda da saída de 1 canal de geração. b) Perda de redundância de geração de potência AC	C	As indicações GEN OFF e AC iluminam no painel. BITE operacional indicará falha do IDG	Nenhuma	Substitua o IDG	0,545	Idem	

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

SUBSISTEMA: GERAÇÃO DE POTÊNCIA AC

EQUIPAMENTO: REGULADOR DE VELOCIDADE

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

IDENTIFICAÇÃO DO ITEM: CSD

FUNÇÃO: CONVERTER A VELOCIDADE VARIÁVEL DO MOTOR EM VELOCIDADE CONSTANTE DE SAÍDA DE 12000 REVOLUÇÕES POR MINUTO.

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA [$\times 10^{-6}$h]	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
11	Bomba de pressão - baixa pressão de carga.	Nenhuma	a) Possível dano interno ao IDG. Flutuação de Freqüência na saída abaixo do valor mínimo. Perda de saída de um canal de geração. b) Perda de redundância da geração de potência AC.	C	As indicações GEN OFF e AC iluminam no painel. B.I.T.E. operacional indicará falha do IDG.	Nenhuma	Substitua o IDG	0,545	RE-7713 Revisão C	Dano do IDG leva a atuação do circuito de proteção.
12	Válvula de alívio de carga baixa pressão de carga.	Nenhuma	a) Dano interno à engrenagem. Perda de saída de um canal de geração. b) Perda de redundância da geração de potência AC.	C	As indicações GEN OFF e AC iluminam no painel. B.I.T.E. operacional indicará falha do IDG.	Nenhuma	Substitua o IDG.	0,132	Idem	Idem
13	Válvula de alívio de carga alta pressão de carga.	Nenhuma	a) Alta pressão de carga resultará em desgaste do pino de engrenagem. Perda de saída de um canal de geração. b) Perda de redundância da geração de potência AC.	C	As indicações GEN OFF e AC iluminam no painel. B.I.T.E. operacional indicará IDG falhado.	Nenhuma	Substitua o IDG.	0,088	Idem	Idem
14	Bombas de limpeza - limpeza insuficiente.	Nenhuma	a) IDG acumula óleo resultando em sobretemperatura levando a perda de saída de um canal de geração. b) Perda de redundância da geração de potência AC.	C	As indicações GEN OFF e AC iluminam no painel. B.I.T.E. operacional indicará IDG falhado.	Nenhuma	Substitua o IDG	2,240	Idem	Idem
15	Regulador - falha ao sentir velocidade de saída do CSD.	Nenhuma	a) Regulador assume posição de velocidade muito baixa resultando em abertura por subfreqüência e perda de saída de um canal de geração b) Perda de redundância da geração de potência AC.	C	As indicações GEN OFF e AC iluminam no painel. B.I.T.E. operacional indicará IDG falhado.	Nenhuma	Substitua o IDG	2,314	Idem	Idem

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

SUBSISTEMA: GERAÇÃO DE POTÊNCIA AC

EQUIPAMENTO: REGULADOR DE VELOCIDADE

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

IDENTIFICAÇÃO DO ITEM: CSD

FUNÇÃO: CONVERTER A VELOCIDADE VARIÁVEL DO MOTOR EM VELOCIDADE CONSTANTE DE SAÍDA DE 12.000 REVOLUÇÕES POR MINUTO.

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. FASE	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA [$\times 10^{-6}$h]	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
16	Regulador - falha em medir quantidade apropriada de óleo de ou para o cilindro de controle.	Nenhuma	a) Velocidade de saída do CSD irregular resultando em flutuação de frequência. Perda de um canal de geração por sub ou sobre-frequência. b) Perda de redundância de geração de potência AC.	C	As indicações GEN OFF e AC iluminam no painel. B.I.T.E. operacional indicará IDG falhado.	Nenhuma	Substitua o IDG	9,256	RE-7713 Revisão C	
17	Cilindro de controle - falha manter o ângulo apropriado de oscilação de saída.	Nenhuma	a) Velocidade de saída irregular resultando em flutuação de frequência Abertura por sub ou sobre-frequência. Perda de saída de um canal de geração. b) Perda de redundância de geração de potência AC.	C	As indicações GEN OFF e AC iluminam no painel. B.I.T.E. operacional indicará IDG falhado:	Nenhuma	Substitua o IDG	0,43	Idem	
18	Alojamento - severo vazamento externo de óleo.	Nenhuma	a) Se o vazamento severo ocorre resultando um baixa pressão de carga, pode haver flutuação de frequência na saída abaixo do valor mínimo e dano interno ao CSD. b) Perda do canal afetado.	C	As indicações GEN OFF e AC iluminam no painel. B.I.T.E. operacional indicará IDG falhado.	Nenhuma	Substitua o IDG	0,122	Idem	
19	Alojamento - leve vazamento externo de óleo.	Nenhuma	a) Pequeno vazamento pode resultar em perda de pressurização própria do IDG. Continuação da operação pode causar degradação de componente interno devido a cavitação. b) Sem efeito a curto prazo. Operação continuada pode causar perda do canal afetado.	C	Não detetada Vazamento de óleo pode ser observado pelo pessoal de manutenção.	Nenhuma	Substitua o IDG	0,368	Idem	

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

SUBSISTEMA: GERAÇÃO DE POTÊNCIA AC

EQUIPAMENTO: REGULADOR DE VELOCIDADE

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

IDENTIFICAÇÃO DO ITEM: C S D

FUNÇÃO: CONVERTER A VELOCIDADE VARIÁVEL DO MOTOR EM VELOCIDADE CONSTANTE DE SAÍDA DE 12000 REVOLUÇÕES POR MINUTO.

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA ($\times 10^{-6}$/h)	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
20	Conjunto selado de entrada vazamento externo de óleo.	Nenhuma	a) Nenhum efeito, a menos que ocorra um vazamento severo. Neste caso resulta baixa pressão de carga, podendo a sub ou sobre frequência de saída danificar o CSD. b) Nenhum efeito a menos que vazamento externo severo ocorra.	C	Iluminam as indicações GEN OFF e AC no painel. B.I.T.E. operacional indicará IDG falhado.	Nenhuma	Substitua o IDG.	8,920	RE-7713 Revisão C	
21	Conjunto do filtro de carga - colapso do elemento filtrante.	Nenhuma	a) Nenhum efeito na engrenagem porque o óleo de carga vai desviar do filtro através da válvula de desvio. Operação continuada pode causar dano ao CSD. b) Sem efeito a curto prazo. Operação continuada pode causar dano ao canal afetado.	C	O colapso do filtro pode ser observado pelo pessoal de manutenção.	Nenhuma	Substituir o filtro periódicamente.	0,033	Idem	
22	Conjunto do filtro de carga-vazamento.	Nenhuma	a) Nenhum efeito a menos de severo vazamento. b) Nenhum efeito a menos de severo vazamento.	C	Colapso do elemento filtrante pode ser observado pelo pessoal de manutenção.	Nenhuma	Substituir o filtro periodicamente	0,627	Idem	

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

SUBSISTEMA: GERAÇÃO DE POTÊNCIA AC

EQUIPAMENTO: GERADOR

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

IDENTIFICAÇÃO DO ITEM: G E N

FUNÇÃO: GERADOR DE TENSÃO

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA [$\times 10^{-6}$h]	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
1	Falha na estrutura do magneto ou rotor do Gerador de Imã Permanente (PMG) devido a defeito de material.	Nenhuma	a) Perda de saída do PMG a GCU. Dano ao gerador. Proteção de subtensão atua. Perda de saída de um canal de geração. b) Perda de redundância de geração de potência AC	C	Iluminam as indicações GEN OFF e AC no painel. B.I.T.E. operacional indicará falha do IDG.	Nenhuma	Substitua o IDG	2,000	RE-7713 Revisão C	
2	Enrolamento aberto ou em curto no estator do PMG. Isolamento danificado ou aberto.	Nenhuma	a) Baixa excitação do gerador principal. Proteção de subtensão atua. Perda de saída de um canal de geração. b) Perda de redundância de geração de potência AC.	C	Iluminam as indicações GEN OFF e AC iluminam no painel BITE operacional indicará falha do IDG	Nenhuma	Substitua o IDG	2,000	Idem	
3	Enrolamento aberto ou lado positivo em curto à terra no estator do excitador.	Nenhuma	a) Perda de excitação do gerador principal. Proteção de sub-tensão atua. Perda de saída de um canal de geração. b) Perda de redundância de geração de potência AC.	C	As indicações GEN OFF e AC iluminam no painel. BITE operacional indicará falha de GCU/fiação	Nenhuma	Substituído o GCU, a falha persiste. Substitua o IDG.	1,400	Idem	
4	Lado negativo de enrolamento em curto à terra no estator do excitador	Nenhuma	a) Corrente máxima através do enrolamento do excitador. Proteção de sobretensão atua. Perda de saída de um canal de geração. b) Perda de redundância de geração de potência AC.	C	As indicações GEN OFF iluminam no painel. BITE operacional indicará falha de GCU/fiação	Nenhuma	Idem	0,600	Idem	
5	Enrolamento aberto ou curto-circuitado no rotor do excitador . Isolamento danificado ou aberto.	Nenhuma	a) Perda de excitação do gerador principal. Proteção de subtensão atua. Perda de saída de um canal de geração. b) Perda de redundância de geração de potência AC.	C	Iluminam as indicações GEN OFF e AC no painel. B.I.T.E. operacional indicará falha de IDG.	Nenhuma	Substitua o IDG	2,000	Idem	

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

SUBSISTEMA: GERAÇÃO DE POTÊNCIA AC

IDENTIFICAÇÃO DO ITEM: G E N

FUNÇÃO: GERADOR DE TENSÃO.

EQUIPAMENTO: GERADOR

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA ($x10^{-6}h$)	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
6	Diodo em curto no retificador	Nenhuma	a) Aumento na corrente do campo do excitador. Reduzida corrente disponível ao campo principal. Capacidade reduzida do canal de geração, possível dano interno ao gerador. Perda de saída de um canal de geração. b) Perda de redundância de geração de potência AC.	C	Iluminam as indicações GEN OFF e AC no painel B.I.T.E. operacional indicará falha do IDG.	Nenhuma	Substitua o IDG	3,000	AE-7713 Revisão C	
7	Diodo aberto	Nenhuma	a) Possível aumento de tensão transiente. Sem efeito significativo na função do gerador. b) Nenhum efeito significativo.	C	Nenhuma	Nenhuma	Nenhum	7,000	Idem	
8	Enrolamento do rotor do gerador principal aberto ou em curto.	Nenhuma	a) Perda de campo do gerador principal. Proteção de subtensão atua . Perda de saída de um canal de geração b) Perda de redundância de geração de potência AC.	C	Iluminam as indicações GEN OFF e AC no painel. B.I.T.E. operacional indicará falha do IDG.	Nenhuma	Substitua o IDG	7,200	Idem	
9	Falha estrutural do rotor do gerador principal	Nenhuma	a) Dano ao gerador. Atuação da proteção de sobre ou sub-tensão . Perda de um canal de geração. b) Perda de redundância de geração de potência AC.	C	Iluminam as indicações GEN OFF e AC no painel. B.I.T.E. operacional indicará falha do IDG.	Nenhuma	Substitua o IDG	0,800	Idem	
10	Transformador de corrente do gerador aberto ou em curto.	Nenhuma	a) A Unidade de Controle da Geração percebe a falta. A proteção diferencial atua. Perda de saída de um canal gerador. b) Perda de redundância de geração de potência AC.	C	Iluminam as indicações GEN OFF e AC no painel . BITE operacional indicará falha do alimentação.	Nenhuma	Substitua o IDG.	1,000	Idem	

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

SUBSISTEMA: GERAÇÃO DE POTÊNCIA AC

EQUIPAMENTO: GERADOR

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

IDENTIFICAÇÃO DO ITEM: GEN

FUNÇÃO: GERADOR DE TENSÃO

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA ($\times 10^{-6}$h)	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
11	Enrolamento do estator do gerador principal aberto.	Nenhuma	a) Perda de tensão de fase. Proteção de subtensão atua. Perda de saída elétrica de um canal de geração. b) Perda de redundância da geração de potência AC	C	Iluminam as indicações GEN OFF e AC no painel. B.I.T.E. operacional indicará falha do IDG.	Nenhuma	Substitua o IDG	1,600	RE- 7713 Revisão C	
12	Estator do gerador principal em curto à terra.	Nenhuma	a) Aumento na corrente de fase. Proteção diferencial atua. Perda de saída elétrica de um canal de geração. b) Perda de redundância da geração de potência AC.	C	Iluminam as indicações GEN OFF e AC no painel. B.I.T.E. operacional indicará falha na alimentação.	Nenhuma	Substitua o IDG	1,200	Idem	
13	Estator do gerador principal em curto entre fases.	Nenhuma	a) Perda de tensão de saída. Proteção diferencial atua. Perda de saída elétrica de um canal de geração. b) Perda de redundância da geração de potência AC.	C	Idem	Nenhuma	Substitua o IDG	1,200	Idem	
14	Resistor supressor aberto	Nenhuma	a) Aumento de interferência eletromagnética. Possível dano ao isolamento do rotor principal e aos diodos. Possível perda de saída elétrica de um canal de geração. b) Perda de redundância da geração de potência AC.	C	Se o gerador falha há indicação GEN OFF e AC no painel B.I.T.E. operacional indicará falha de IDG.	Nenhuma	Substitua o IDG	1,000	Idem	
15	Potência de entrada no eixo do gerador não é transmitida.	Nenhuma	a) Perda de rotação no gerador. Proteção de subfrequência atua. Perda de saída de um canal de geração. b) Perda de redundância da geração AC	C	Iluminam as indicações GEN OFF e AC no painel . B.I.T.E operacional indicará falha do IDG.	Nenhuma	Substitua o IDG	0,200	Idem	

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

SUBSISTEMA: GERAÇÃO DE POTÊNCIA AC

EQUIPAMENTO: GERADOR

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

IDENTIFICAÇÃO DO ITEM: GEN

FUNÇÃO: GERADOR DE TENSÃO

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA [x10⁻⁶h]	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
16	Refrigeração insuficiente do gerador	Nenhuma	a) Falta líquido refrigerante no estator do gerador, levando a degradação de sua vida útil. b) Perda de redundância da geração de potência AC.	C	As indicações GEN OFF e AC iluminam no painel. B.I.T.E. operacional indicará falha do IDG.	Nenhuma	Substitua o IDG	1,400	RE-7713 Revisão C	
17	CSD contaminado	Nenhuma	a) Nenhum efeito na operação do gerador. Dano potencial ao CSD. Potencial perda de saída elétrica de um canal de geração. b) Perda de redundância da geração de potência AC.	C	Idem	Nenhuma	Substitua o IDG	0,400	Idem	
18	Falha do suporte devido a fadiga.	Nenhuma	a) Desalinhamento do gerador. Proteção subtensão atua. Perda de saída elétrica de um canal de geração. b) Perda de redundância da geração de potência AC.	C	Idem	Nenhuma	Substitua o IDG	2,000	Idem	
19	Vazamento externo de óleo	Nenhuma	a) Nenhum efeito a menos de severo vazamento resultando em baixa pressão de carga de CSD, levando a flutuação de frequência ou frequência abaixo do valor mínimo e dano interno ao CSD. b) Nenhum efeito a menos do vazamento severo.	C	Idem	Nenhuma	Substitua o IDG	1,000	Idem	

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

SUBSISTEMA: GERAÇÃO DE POTÊNCIA AC

IDENTIFICAÇÃO DO ITEM: GCU

FUNÇÃO: CONTROLAR E MONITORAR O GERADOR ELIMINANDO DISTÚRBIOS E/OU ISOLANDO FALTAS

EQUIPAMENTO: UNIDADE DE CONTROLE DA GERAÇÃO

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA ($\times 10^{-6}$h)	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
1	Circuito de proteção contra sobre frequência atua indevidamente.	Nenhuma	a) Perda de saída de um canal de geração. b) Perda de redundância de potência AC.	C	As indicações GEN OFF e AC iluminam no painel. Teste de segurança indicará falha da GCU.	Nenhuma	Substitua a GCU	0,307	RE-7713 Revisão C	
2	Circuito de proteção contra sobrefrequência não atua em condição de sobrefrequência.	Nenhuma	a) Perda de proteção contra sobrefrequência em um canal de geração. b) Possível utilização de equipamentos com sobrefrequência em um canal, se ocorrer falha múltipla.	C	Auto-teste indicará falha da GCU.	Nenhuma	Substitua a GCU.	0,307	Idem	
3	Circuito de proteção contra subfrequência atua indevidamente.	Nenhuma	a) Perda de saída de um canal de geração. b) Perda de redundância de potência AC.	C	As indicações GEN OFF e AC iluminam no painel. Auto-teste indicará falha da GCU.	Nenhuma	Substitua a GCU	0,476	Idem	
4.	Circuito de proteção contra subfrequência não atua em condição de subfrequência.	Nenhuma	a) Perda de saída de um canal de geração. b) Possível utilização de equipamentos com subfrequência em um canal, se ocorrer falha múltipla.	C	Auto teste indicará falha da GCU.	Nenhuma	Substitua a GCU	0,476	Idem	
5	Circuito de proteção contra sobretensão atua indevidamente	Nenhuma	a) Perda de saída de um canal de geração. b) Perda de redundância de potência AC.	C	As indicações GEN OFF e AC iluminam no painel. Auto-teste indicará falha da GCU.	Nenhuma	Substitua a GCU	0,483	Idem	
6	Circuito de proteção contra sobretensão não atua em condição de sobretensão.	Nenhuma	a) Perda de proteção contra sobretensão em um canal de geração. b) Possível utilização de equipamentos com sobretensão em um canal, se ocorrer falha múltipla	C	Auto teste indicará falha da GCU.	Nenhuma	Substitua a GCU	0,483	Idem	

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

SUBSISTEMA: GERAÇÃO DE POTÊNCIA AC

IDENTIFICAÇÃO DO ITEM: G C U

FUNÇÃO: CONTROLAR E MONITORAR O GERADOR ELIMINANDO DISTÚRBIOS E/OU ISOLANDO FALTAS.

EQUIPAMENTO: UNIDADE DE CONTROLE DA GERAÇÃO

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA ($x10^{-6}h$)	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
7	Circuito de proteção contra sub tensão atua indevidamente	Nenhuma	a) Perda de saída de um canal de geração b) Perda de redundância de potência AC	C	As indicações GEN OFF e AC iluminam no painel. Auto teste indicará falha da GCU.	Nenhuma	Substitua a GCU	0,368	RE-7713 Revisão C	
8	Circuito de proteção contra sub-tensão não atua em condição de sub-tensão.	Nenhuma	a) Perda de proteção contra sub-tensão em um canal de geração. b) Possível utilização de equipamentos com subtensão em um canal se ocorrer falha múltipla.	C	Auto teste indicará falha da GCU.	Nenhuma	Substitua a GCU	0,368	Idem	
9	Circuito de proteção contra sobrecorrente na linha cruzada atua indevidamente	Nenhuma	a) Perda de possibilidade de um gerador alimentar cargas do outro canal. b) Perda de redundância de geração de potência AC.	C	As indicações GEN OFF e AC iluminam no painel. Auto teste indicará falha da GCU.	Nenhuma	Substitua a GCU	1,133	Idem	
10	Circuito de proteção contra sobrecorrente na linha cruzada não atua em condição de falha por sobrecorrente.	Nenhuma	a) Perda de proteção contra sobre corrente na linha de alimentação cruzada. Possível perda do gerador remanescente. b) Perda de segurança, possível perda de potência AC se uma falha múltipla ocorrer.	C	Auto-teste indicará falha da GCU.	Nenhuma	Substitua a GCU	1,133	Idem	
11	Circuito de proteção diferencial atua indevidamente	Nenhuma	a) Perda de saída de um canal de geração b) Perda de redundância de potência AC.	C	As indicações GEN OFF e AC iluminam no painel. Auto-teste indicará falha da GCU.	Nenhuma	Substitua a GCU	0,206	Idem	
12	Circuito de proteção diferencial não atua em condição de falha diferencial.	Nenhuma	a) Perda de proteção diferencial de um canal de geração .Se ocorrer uma falha, o canal será protegido em retaguarda contra subtensão ou sobrecorrente. b) Possível utilização de equipamentos em situação anormal até que ocorra subtensão.	C	Auto teste indicará falha da GCU	Nenhuma	Substitua a GCU	0,206	Idem	

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA — ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

SUBSISTEMA: GERAÇÃO DE POTÊNCIA AC

EQUIPAMENTO: UNIDADE DE CONTROLE DA GERAÇÃO — IDENTIFICAÇÃO DO ITEM: G C U — FUNÇÃO: CONTROLAR E MONITORAR O GERADOR ELIMINANDO DISTÚRBIOS E/OU ISOLANDO FALTAS

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS: TRIPULAÇÃO	7. AÇÕES A SEREM TOMADAS: APOIO NO SOLO	8. TAXA DE FALHA ($\times 10^{-6}$h)	9. FONTE	10. OBSERVAÇÕES
13	Regulador de tensão de campo não compensa sub-tensão.	Nenhuma	a) Perda de um canal de geração pela atuação da proteção contra sub tensão. b) Perda de redundância de potência elétrica AC.	C	As indicações GEN OFF e AC iluminam no painel. BITE operacional indicará falha da GCU.	Nenhuma	Substitua a GCU	1,16	RE-7713 Revisão C	
14	Regulador de tensão de campo não compensa sobre-tensão.	Nenhuma	a) Proteção de sobretensão causa perda de um canal de geração. b) Perda de redundância de potência elétrica AC.	C	As indicações GEN OFF e AC iluminam no painel. BITE operacional indicará falha da GCU.	Nenhuma	Substitua a GCU	1,16	Idem	
15	Circuito de proteção contra sobrecorrente atua indevidamente.	Nenhuma	a) Perda de saída elétrica de um canal de geração. b) Perda de redundância de potência elétrica AC.	C	As indicações GEN OFF e AC iluminam no painel. BITE operacional indicará falha da GCU.	Nenhuma	Substitua a GCU	1,064	Idem	
16	Circuito de proteção contra sobrecorrente não atua em condição de sobrecorrente	Nenhuma	a) Perda de proteção contra sobracorrente em um canal de geração b) Perda de redundância em segurança	C	Auto-teste indicará falha da GCU.	Nenhuma	Substitua a GCU	1,064	Idem	
17	BITE operacional falha ao detetar unidade falhada	Nenhuma	a) Perda de monitoramento de falha. b) Nenhum	C	Falha indicação de BITE	Nenhuma	Substitua GCU e a outra unidade falhada.	1,563	Idem	
18	BITE operacional falsamente indica uma unidade falhada.	Nenhuma	a) Nenhuma b) Nenhuma	C	Indicação inválida do B.I.T.E.	Nenhuma	Substitua a GCU após substituir a unidade	1,563	Idem	
19	Auto-teste do B.I.T.E. falha ao detetar GCU falhada	Nenhuma	a) Possível perda de saída elétrica de um canal de geração b) Perda de redundância de potência elétrica AC.	C	As indicações GEN OFF e AC iluminam no painel. BITE operacional indicará unidade falhada com reduzida confiança.	Nenhuma	Substitua a unidade e a GCU	2,144	Idem	

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

SUBSISTEMA: GERAÇÃO DE POTÊNCIA AC

IDENTIFICAÇÃO DO ITEM: G C U

FUNÇÃO: CONTROLAR E MONITORAR O GERADOR ELIMINANDO DISTÚRBIOS E/OU ISOLANDO FALTAS

EQUIPAMENTO: UNIDADE DE CONTROLE DA GERAÇÃO

1. CASO Nº.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA ($\times 10^{-6}$h)	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
20	Auto-teste do B.I.T.E. falsamente indica GCU falhada	Nenhuma	a) Nenhum b) Nenhum	C	Indicação inválida do B.I.T.E., acusando falha do GCU	Nenhuma	Substitua a GCU	2,144	RE-7713 Revisão C	
21	Proteção contra curto no PMG atua indevidamente	Nenhuma	a) Perda de saída de um canal de geração b) Perda de redundância de potência AC	C	As indicações GEN OFF e AC iluminam no painel. Auto-teste indicará falha da GCU.	Nenhuma	Substitua a GCU	0,349	Idem	
22	Protução contra curto no PMG falha em condição de curto no PMG	Nenhuma	a) Perda de proteção contra curto no PMG para um canal de guraçãd. Su o curto ocorrer, o canal será protegido por subtensão. Pode ocorrer dano ao transformador da GCU. b) Perda de redundancia em segurança.	C	Auto-teste indicará falha da GCU.	Nunhuma	Substitua a GCU	0,349	Idem	
23	Suprimento de 12V a GCU sem saída ou com valor abaixo do permitido.	Nenhuma	a) Perda de saída de um canal de geração. b) Perda de redundância de potência AC.	C	As indicações GEN OFF e AC iluminam no painel. Auto teste indicará falha da GCU.	Nenhuma	Substitua a GCU	1,005	Idem	
24	Suprimento de 12V a GCU em falha com tensão acima de 18V.	Nenhuma	a) Perda de saída de um canal de geração. Provável dano a unidade de controle. b) Perda de redundância de potência AC.	C	As indicações GEN OFF e AC iluminam no painel. Auto-teste do B.I.T.E. indicará falha da GCU.	Nenhuma	Substitua a GCU	1,005	Idem	
25	Suprimento de 28V da GCU com excessivo "ripple"	Nenhuma	a) Perda de saída de um canal de geração. b) Perda de redundância de potência AC.	C	As indica ções GEN OFF e AC iluminam no painel. Auto-teste indicará falha da GCU.	Nenhuma	Substitua a GCU	0,239	Idem	

SISTEMA: GERAÇÃO DE POTÊNCIA ELÉTRICA

SUBSISTEMA: GERAÇÃO DE POTÊNCIA AC

EQUIPAMENTO: UNIDADE DE CONTROLE DA GERAÇÃO

ANÁLISE DE MODOS DE FALHA E SEUS EFEITOS

IDENTIFICAÇÃO DO ITEM: GCU

FUNÇÃO: CONTROLAR E MONITORAR O GERADOR ELIMINANDO DISTÚRBIO E/OU ISOLANDO FALTAS

1. CASO NR.	2. TIPO DE FALHA	3. CONDIÇÕES QUE MODIFICAM OS EFEITOS DA FALHA.	4. EFEITOS DA FALHA SOB CONDIÇÕES DA COLUNA 3. a. No sistema b. Na aeronave	5. GRAU	6. DETEÇÃO OU AVISO DE FALHA	7. AÇÕES A SEREM TOMADAS		8. TAXA DE FALHA [$x10^{-6}h$]	9. FONTE	10. OBSERVAÇÕES
						TRIPULAÇÃO	APOIO NO SOLO			
26	Falta saída na fonte de suprimento de 28V da GCU	Nenhuma	a) Nenhum efeito. A fonte é redundante. b) Nenhum	C	Somente detetável em testes de aceitação do equipamento	Nenhuma	Substitua a GCU no recebimento	0,0132	RE-7713 Revisão C	
27	Tensão de saída muito alta na fonte de 28V da GCU	Nenhuma	a) Possível perda de um canal de geração se a tensão é alta o suficiente para danificar a unidade. b) Perda de redundância de potência AC	C	As indicações GEN OFF e AC iluminam no painel. Auto-teste indicará falha da GCU	Nenhuma	Substitua a GCU	0,0132	Idem	

4.4 - DESENVOLVIMENTO DAS ÁRVORES DE FALHAS DO SISTEMA

Para que as Árvores de Falhas do Sistema de Geração Elétrica fossem desenvolvidas, foi selecionada uma missão típica teórica, sujeita a exigências próprias e com duração aproximada de noventa minutos.

Considera-se que a missão desenvolve-se em tempo de paz, o que significa maiores exigências para sua realização.

4.4.1 - CARACTERIZAÇÃO DA MISSÃO TÍPICA

Para uma aeronave, as condições estabelecidas e a função a ser desempenhada, que são duas situações a serem perfeitamente determinadas para o estabelecimento da confiabilidade, apresentam aspectos diferentes durante as fases do vôo.

Considerando uma missão típica de aeronave militar, com duração de 1h 30min., a mesma está dividida em 8 fases diferentes, com suas respectivas durações:

Fase 1 - Preparação para decolagem

Inicia-se com a entrada do piloto no avião e termina ao início da rolagem.

Duração: t1 = 6 minutos.

Fase 2 - Decolagem

Inicia-se com o início da rolagem e termina com a retração do trem e dos flapes.

Duração: t2 = 3 minutos.

Fase 3 - Cruzeiro

Inicia-se com a retração do trem e dos flapes e termina ao ser atingido o ponto inicial da área de combate.

Duração: t3 = 30 minutos.

Fase 4 - Penetração

Inicia-se no ponto inicial da área de combate e termina ao ser identificado o alvo.

Duração: t4 = 6 minutos.

Fase 5 - Combate.

Inicia-se com a identificação do alvo e termina com o lançamento do armamento.

Duração: t5 = 5 minutos.

Fase 6 - Fuga

Inicia-se com o lançamento do armamento e termina ao serem atingidas 50 milhas do alvo.

Duração: t6 = 6 minutos.

Fase 7 - Cruzeiro.

Inicia-se a 50 milhas do alvo e termina com a extensão do trem para pouso.

Duração: t7 = 31 minutos.

Fase 8 - Pouso.

Inicia-se com a extensão do trem e termina ao fim da rolagem de regresso.

Duração: t8 = 3 minutos.

4.4.2 - ESTABELECIMENTO DO EVENTO TOPO

O evento topo de uma árvore de falhas representa falha do sistema ao operar. Para o caso em análise, o sistema falhará quando impedir a conclusão de uma missão dentro do tempo e dos requisitos estabelecidos.

Desta forma, Falha da Missão representa:

- o aborto da missão ou o atraso de decolagem superior a cinco minutos.
- a necessidade de recorrer a um procedimento operacional limitado.
- um incidente ou acidente.

4.4.3 - ANÁLISE DA CONFIABILIDADE DA MISSÃO

Para análise da confiabilidade do sistema elétrico durante uma missão, pode-se agrupar as fases estabelecidas no ítem 4.4.1 em três períodos distintos, que são Partida, Vôo e Pouso. Isto porque, alguns modos de falha impedem a decolagem, outros impedem continuação do vôo se ocorrerem após a decolagem e outros podem comprometer a segurança do pouso.

Os períodos e as limitações do sistema são:

Período 1 - Partida.

Coincide com a fase 1 - preparação para decolagem . Durante este período, todo o sistema deverá estar funcionando perfeitamente para ser liberado o vôo . É a situação mais restritiva.

O tempo total de duração é de 6 minutos.

Período 2 - Vôo

Inclui as fases 2 a 7 - decolagem, cruzeiro, penetração, combate, fuga, cruzeiro. Durante este período, deverá haver potência elétrica em todas as barras.

O tempo total de duração é de 81 minutos.

Período 3 - Pouso

Inclui a fase 8 - pouso. Para garantir um pouso seguro, pelo menos o sistema de emergência deverá estar funcionando satisfatoriamente.

O tempo total de duração é de 3 minutos.

Desta forma, foram estabelecidas três árvores de falhas, uma para cada período da missão, com o evento topo representando falha do sistema ao desempenhar a função exigida no período. Uma outra árvore combina os eventos topo de cada uma dessas três árvores e representa o evento topo indesejado que é falha da missão.

As figuras 4.2 a 4.9 representam as árvores de falhas desenvolvidas.

As informações para o desenvolvimento dessas árvores de falhas foram extraídas da Análise de Modos de Falha e seus Efeitos, já apresentada nas páginas 102 a 147.

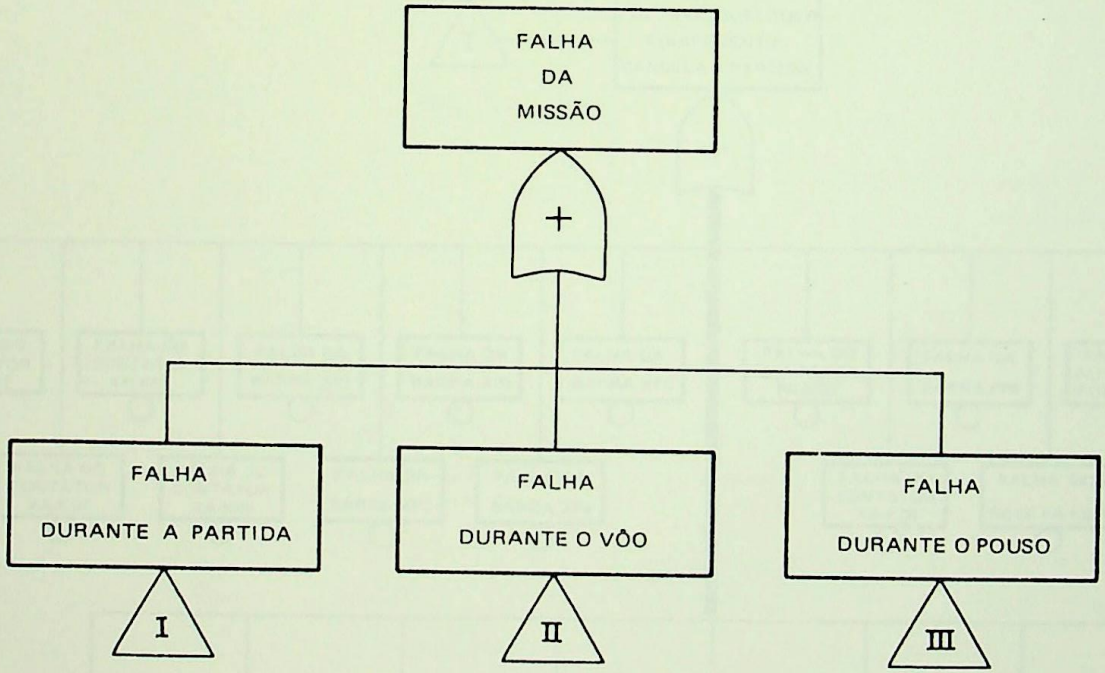


FIGURA 4.2 - Árvore de Falha da Missão

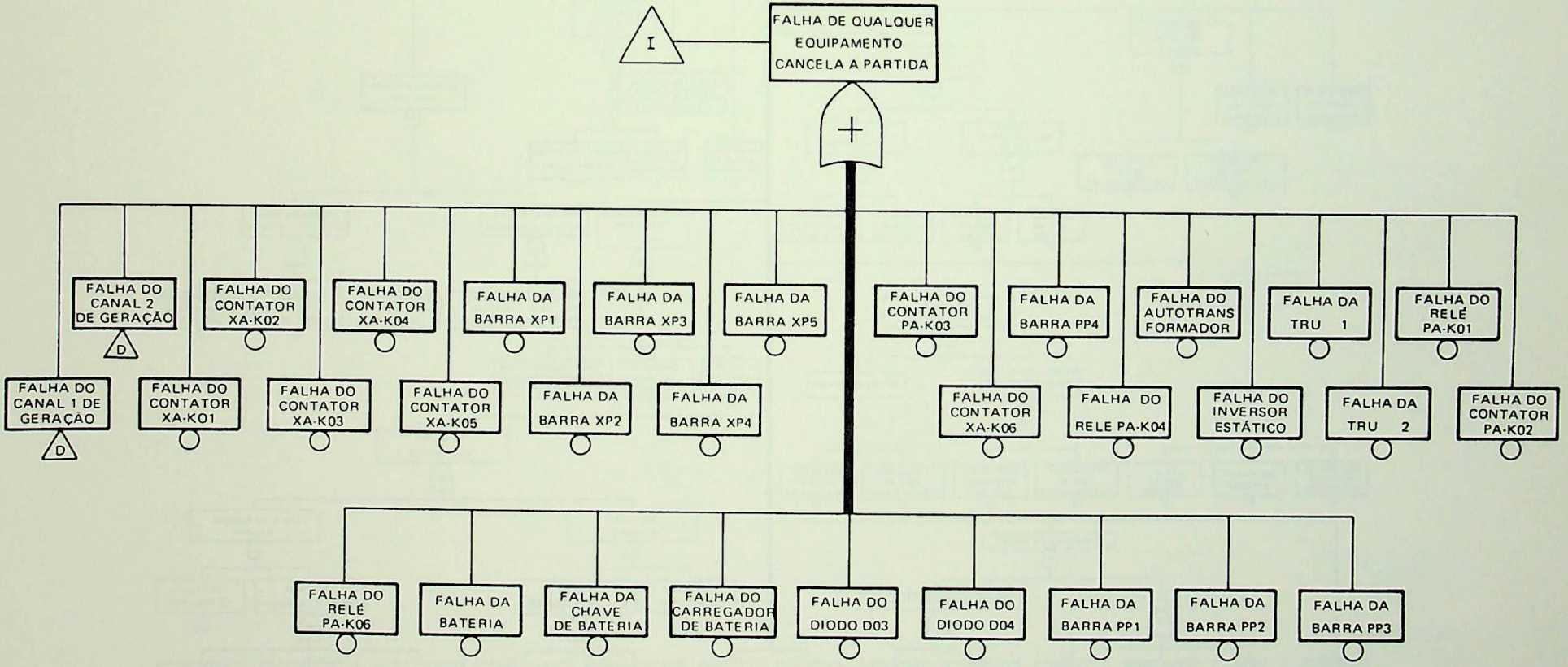


FIGURA 4.3 - Falha Durante a Partida

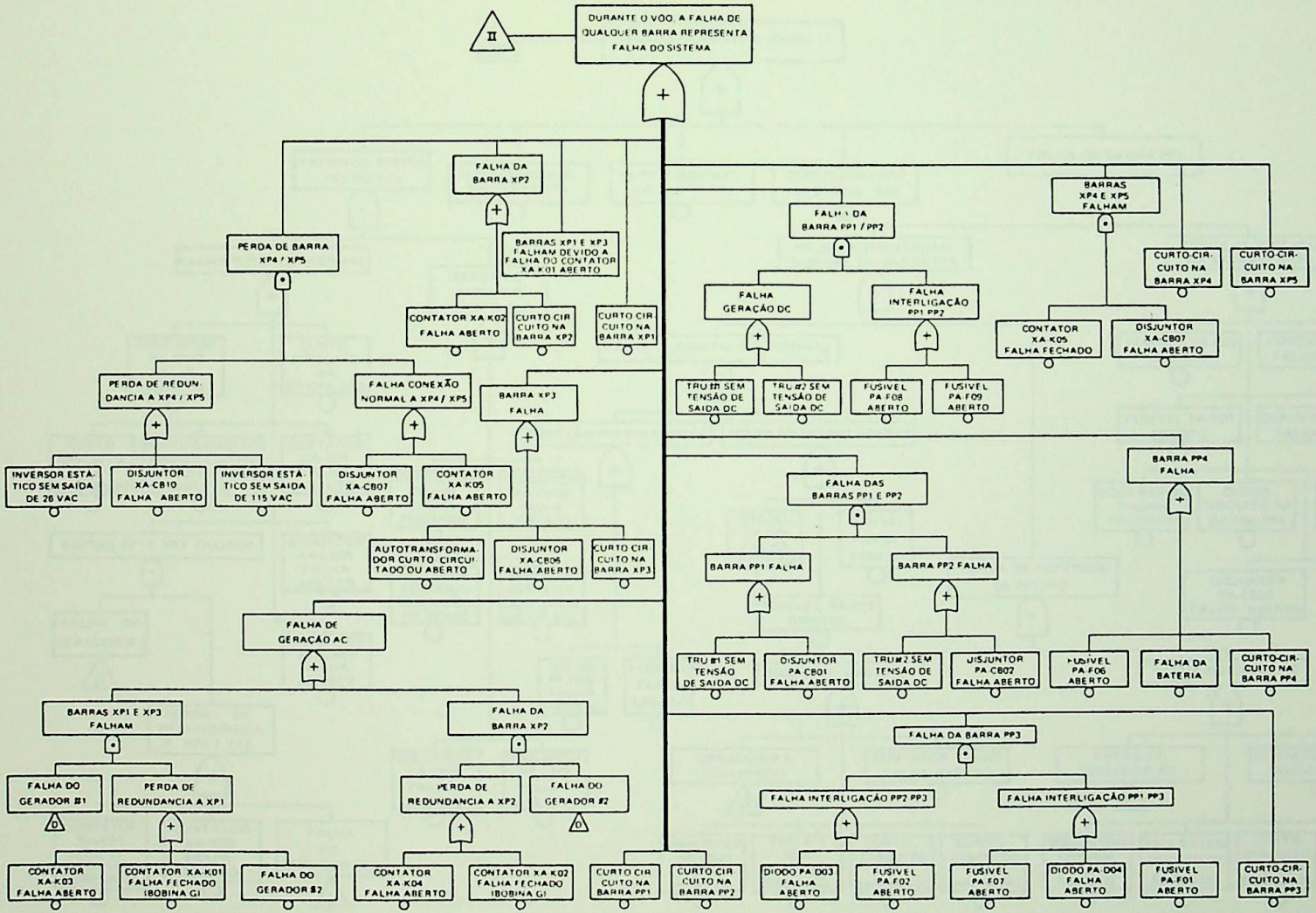


FIGURA 4.4 - Falha Durante o Vôo

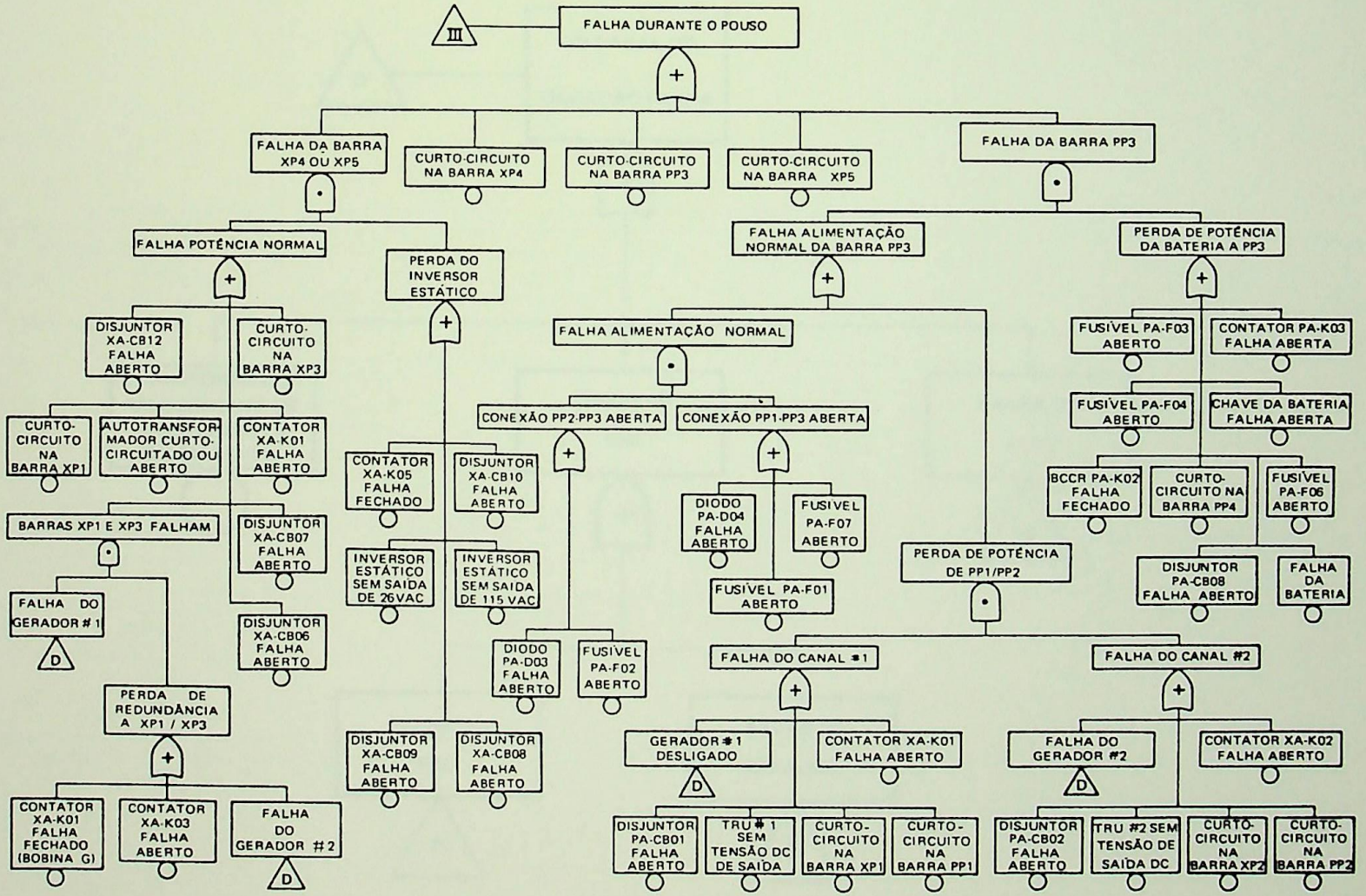


FIGURA 4.5 - Falha Durante o Pouso

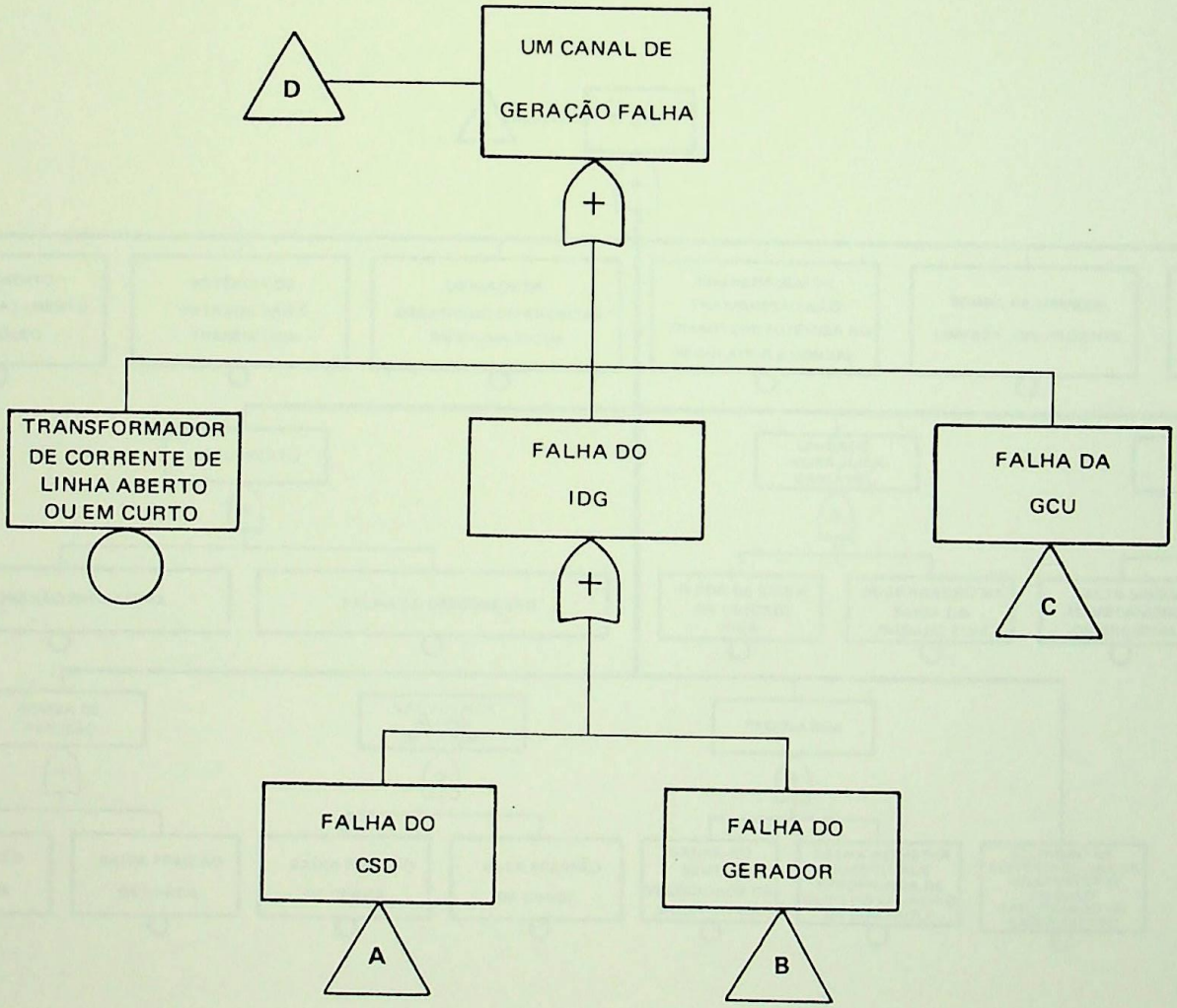


FIGURA 4.6 - Desenvolvimento das Falhas de um Canal de Geração

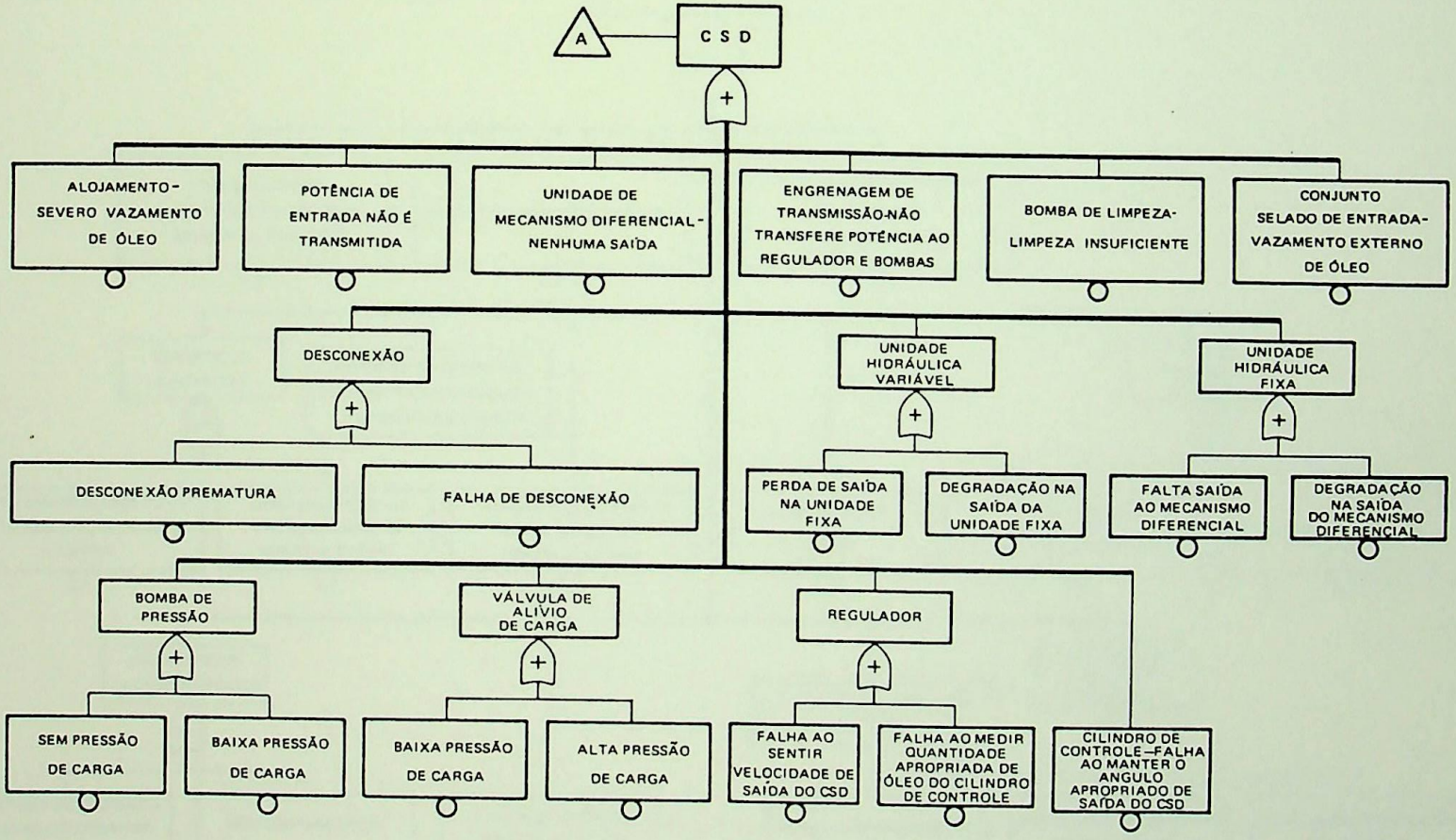


FIGURA 4.7 - Desenvolvimento das Falhas do CSD
(Regulador de Velocidade)

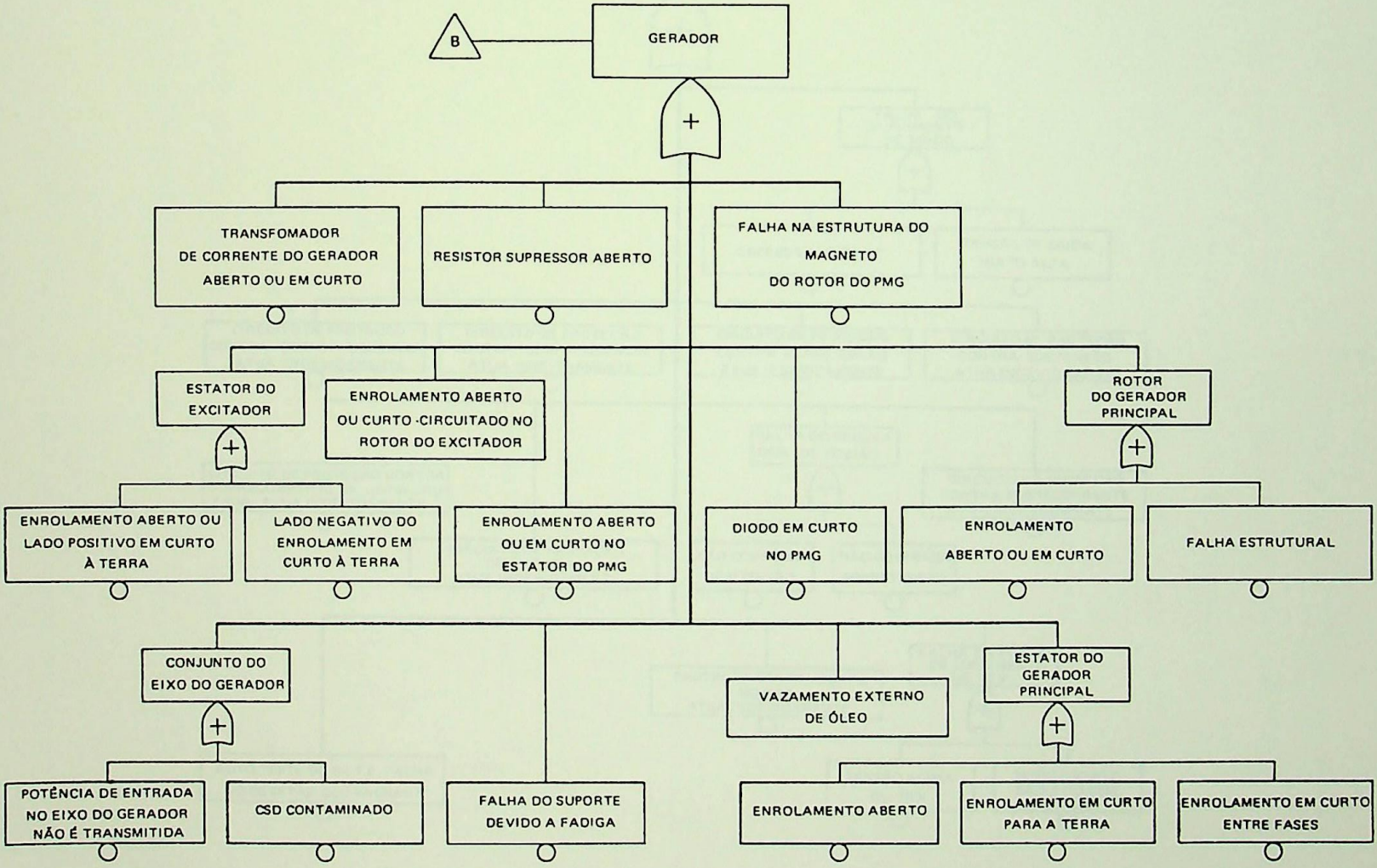


FIGURA 4.8 - Desenvolvimento das Falhas do Gerador

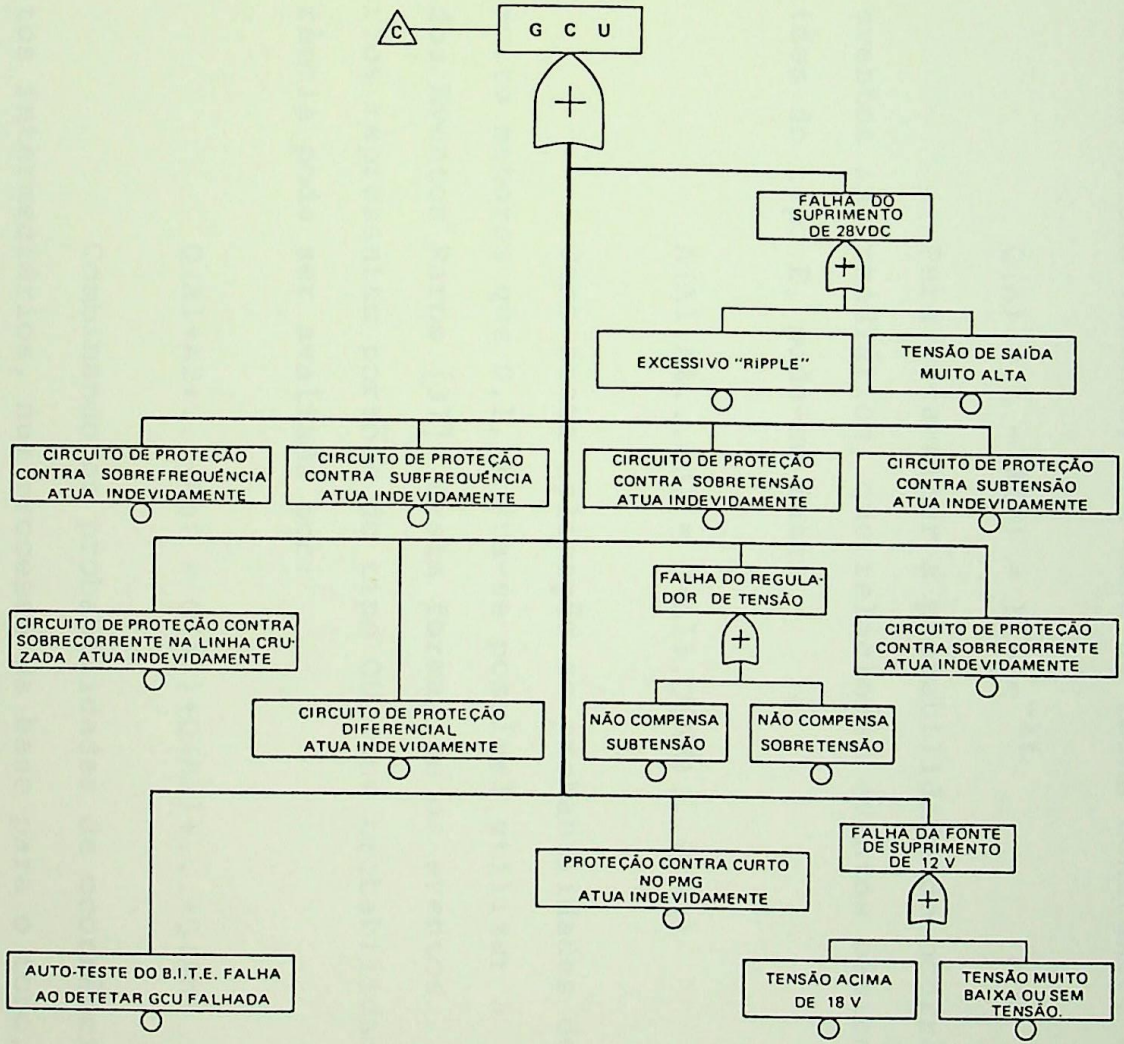


FIGURA 4.9 - Desenvolvimento das Falhas da GCU (Unidade de Controle da Geração)

4.5 - AVALIAÇÃO DA PROBABILIDADE DE FALHA DA MISSÃO

A probabilidade de ocorrência de um evento básico é a probabilidade de falha de um componente ou subsistema durante o tempo de interesse. Então, considerando que os equipamentos falham aleatoriamente, com taxa de falha constante, λ, tem-se

$$Q(A) = 1 - R(t) = 1 - e^{-\lambda t}$$

Para determinar a probabilidade de ocorrência de eventos intermediários, que relacionam eventos básicos por portões do tipo E, pode-se fazer

$$A(A1.A2...An) = Q(A1).Q(A2)...Q(An)$$

Como nesta aplicação as probabilidades de falha são muito menores que 0,1, torna-se possível utilizar a Aproximação dos Eventos Raros [37]. Desta forma, se os eventos intermediários representam portões do tipo OU, sua probabilidade de ocorrência pode ser avaliada por:

$$Q(A1+A2+...+An) = Q(A1)+Q(A2)+...+Q(An)$$

Combinando as probabilidades de ocorrência dos eventos intermediários, num processo da base para o topo, chega-se à expressão final que representa a Probabilidade de Falha da Missão.

O programa de computador desenvolvido e que utiliza o processo de cálculo descrito, faz imprimir a expressão final que representa a estrutura da árvore de falhas e a probabilidade de ocorrência do Evento Topo.

Para que a estrutura da árvore seja conhecida, o processamento segue o método de explosão escalonada (descrito com detalhes no Apêndice A), que consiste em um processo de descida do topo para a base, registrando os caminhos percorridos.

A tabela 4.10 fornece as taxas de falha dos componentes de cada canal de geração.

As tabelas 4.11 e 4.12 fornecem indicação da simbologia adotada no programa relativamente aos eventos básicos e fornece as taxas de falha por hora de operação.

E V E N T O S	TAXA DE FALHA [$x10^{-6}$ HORAS DE OPERAÇÃO]
Transformadores de corrente aberto ou em curto	1.
CSD - Alojamento - Severo vazamento externo de óleo	.122
CSD - Potência de entrada não é transmitida	.61
CSD - Unidade de mecanismo diferencial - nenhuma saída	5.2
CSD - Engrenagem de transmissão: não transfere potência ao regulador e bombas	.65
CSD - Bombas de limpeza - limpeza insuficiente	2.24
CSD - Conjunto selado de entrada - vazamento externo de óleo	8.92
CDS - Falha de desconexão	.272
CSD - Desconexão prematura	1.088
CSD - Unidade hidráulica variável - perda de saída da unidade fixa	2.658
CSD - Unidade hidráulica variável - degradação na saída da unidade fixa	1.772
CSD - Unidade hidráulica fixa - falta saída ao mecanismo diferencial	1.962
CSD - Unidade hidráulica fixa - degradação na saída do mecanismo diferencial	1.308
CSD - Bomba de pressão - sem pressão de carga	.545
CSD - Bomba de pressão - baixa pressão de carga	.545
CSD - Válvula de alívio de carga - baixa pressão de carga	.132
CSD - Válvula de alívio de carga - alta pressão de carga	.088
CSD - Regulador - falha ao sentir velocidade de saída do CSD	2.314
CSD - Regulador falha em medir quantidade apropriada de óleo ao cilindro de controle	9.256
CSD - Cilindro de controle falha ao manter o ângulo apropriado de oscilação de saída	.43
GEN - Transformador de corrente do gerador aberto ou em curto	1.
GEN - Resistor supressor aberto	1.
GEN - Falha em estrutura do magneto do rotor do PMG	2.
GEN - Enrolamento aberto ou lado positivo em curto a terra no estator do excitador	1.4
GEN - Lado negativo do enrolamento em curto a terra no estator do excitador	.6
GEN - Enrolamento aberto ou curto - circuitado no rotor do excitador	2.
GEN - Enrolamento aberto ou em curto no estator do PMG	2.
GEN - Diodo em curto no retificador	3.
GEN - Enrolamento do rotor do gerador principal aberto ou em curto	7.2
GEN - Falha estrutural do rotor do gerador principal	.8
GEN - Potência de entrada no eixo do gerador não é transmitida	.2
GEN - CSD contaminado	.4
GEN - Falha do suporte devido a fadiga	2.
GEN - Vazamento externo de óleo	1.
GEN - Enrolamento do estator do gerador principal aberto	1.6
GEN - Estator do gerador principal em curto a terra	1.2
GEN - Estator do gerador principal em curto entre fases	1.2
GCU - Suprimento de 28V da GCU com excessivo "ripple"	.239
GCU - Tensão de saída muito alta na fonte de 28V da GCU	.0132
GCU - Circuito de proteção contra sobrefrequência atua indevidamente	.307
GCU - Circuito de proteção contra subfrequência atua indevidamente	.476
GCU - Circuito de proteção contra sobretensão atua indevidamente	.483
GCU - Circuito de proteção contra subtensão atua indevidamente	.368
GCU - Circuito de proteção contra sobrecorrente na linha cruzada atua indevidamente	1.133
GCU - Circuito de proteção diferencial atua indevidamente	.206
GCU - Regulador de tensão de campo não compensa sub-tensão	1.16
GCU - Regulador de tensão de campo não compensa sobre-tensão	1.16
GCU - Circuito de proteção contra sobre-corrente atua indevidamentente	1.064
GCU - Auto-teste do B.I.T.E. falha ao detetar GCU falhada	2.144
GCU - Proteção contra curto no PMG atua indevidamente	.349
GCU - Suprimento de 12V da GCU em falha com tensão acima de 18V	1.005
GCU - Suprimento de 12V da GCU sem saída ou com valor abaixo do permitido	1.005

TABELA 4.10 - TAXAS DE FALHAS DOS COMPONENTES DE CADA CANAL DE GERAÇÃO

E V E N T O S	SIMBOLOGIA ADOTADA	TAXA DE FALHA [$x10^{-6}$ HORAS DE OPERAÇÃO]
Falha do Canal de Geração # 1	E1	80.8242
Falha do Canal de Geração # 2	E2	80.8242
Falha do Contator XA - K01	E3	8.
Falha do Contator XA - K02	E4	8.
Falha do Contator XA - K03	E5	8.
Falha do Contator XA - K04	E6	8.
Falha do Contator XA - K05	E7	8.
Falha da barra XP1	E8	.8
Falha da barra XP2	E9	.8
Falha da barra XP3	E10	.8
Falha da barra XP4	E11	.8
Falha da barra XP5	E12	.8
Falha do contator PA - K03	E13	2.
Falha do contator XA - K06	E14	8.
Falha da barra PP4	E15	.8
Falha do Autotransformador	E16	2.4
Falha do relé PA - K04	E17	2.
Falha do TRU # 1	E18	26.4
Falha do Inversor Estático	E19	200.
Falha do Relé PA - K01	E20	2.
Falha da TRU # 2	E21	26.4
Falha do contator PA - K02	E22	2.
Falha do relé PA - K06	E23	2.
Falha da bateria	E24	6.
Falha da chave da bateria	E25	2.537
Falha do carregador de bateria	E26	60.
Falha do diodo D03	E27	.4
Falha do diodo D04	E28	.4
Falha da barra PP1	E29	.8
Falha da barra PP2	E30	.8
Falha da barra PP3	E31	.8
Contator XA - K01 falha aberto	E32	2.
Curto - circuito na barra XP1	E33	.8
Curto - circuito na barra XP5	E34	.8
Curto - circuito na barra XP4	E35	.8
Curto - circuito na barra PP1	E36	.8
Curto - circuito na barra PP2	E37	.8
Gerador # 2 desligado	E38	80.8242
Contator XA - K04 falha aberto	E39	4.
Contator XA - K02 falha fechado (bobina G)	E40	3.
Contator XA - K02 falha aberto	E41	2.
Curto - circuito na barra XP2	E42	.8
Gerador # 2 desligado	E44	80.8242
Gerador 1 desligado	E45	80.8242
Contator XA - K03 falha aberto	E46	4.
Contator XA - K01 falha fechado (bobina G)	E47	3.
Autotransformador em curto ou aberto	E48	2.4
Disjuntor XA - CB06 falha aberto	E49	1.
Curto - circuito na barra XP3	E50	.8
Disjuntor XA - CB07 falha aberto	E51	1.
Contator XA-K05 falha aberto	E52	4.
Inversor estático sem saída de 26VAC	E53	100.
Inversor estático sem saída de 115VAC	E54	100.
Disjuntor XA - CB10 falha aberto	E55	1.
TRU # 1 sem tensão DC de saída	E56	26.4
TRU # 2 sem tensão DC de saída	E57	26.4
Fusível PA - F08 aberto	E58	2.5
Fusível PA - F09 aberto	E59	2.5
Contator XA - K05 falha fechado	E60	4.
Disjuntor XA - CB02 falha aberto	E61	1.
TRU # 1 sem tensão DC de saída	E62	26.4
Disjuntor PA - CB01 falha aberto	E63	1.
TRU # 2 sem tensão DC de saída	E64	26.4

TABELA 4.11 - TAXAS DE FALHAS RELATIVAS AOS EVENTOS DE FALHA

E V E N T O S	SIMBOLOGIA ADOTADA	TAXA DE FALHA [10^{-6}HORAS DE OPERAÇÃO]
Disjuntor PA - CB02 falha aberto	E65	1.
Fusível PA - F06 aberto	E66	2.5
Falha da bateria	E67	6.
Curto - circuito na barra PP4	E68	.8
Curto - circuito na barra PP3	E69	.8
Diodo PA - D03 falha aberto	E70	.2
Fusível PA - F02 aberto	E71	2.5
Fusível PA - F07 aberto	E72	2.5
Diodo PA - D04 falha aberto	E73	.2
Fusível PA - F01 aberto	E74	2.5
Curto-circuito na barra XP4	E75	.8
Curto-circuito na barra PP3	E76	.8
Curto-circuito na barra XP5	E77	.8
Disjuntor XA-CB06 falha aberto	E78	1.
Disjuntor XA-CB12 falha aberto	E79	1.
Curto-circuito na barra XP3	E80	.8
Curto-circuito na barra XP1	E81	.8
Autotransformador em curto ou aberto	E82	2.4
Contator XA-K01 falha aberto	E83	2.
Disjuntor XA-CB07 falha aberto	E84	1.
Gerador # 1 desligado	E85	80.8242
Contator XA - K01 falha fechado (bobina G)	E86	3.
Contator XA - K03 falha aberto	E87	4.
Gerador # 2 desligado	E88	80.8242
Contator XA - K05 falha fechado	E89	4.
Disjuntor XA - CB10 falha aberto	E90	1.
Inversor Estático sem saída de 26 VAC	E91	100.
Inversor Estático sem saída de 115 VAC	E92	100.
Disjuntor XA - CB09 falha aberto	E93	1.
Disjuntor XA - CB08 falha aberto	E94	1.
Diodo PA - D03 falha aberto	E95	.2
Fusível PA - F02 aberto	E96	2.5
Diodo PA - D04 falha aberto	E97	.2
Fusível PA - F01 aberto	E98	2.5
Fusível PA - F07 aberto	E99	2.5
Gerador # 1 desligado	E100	80.8242
Contator XA - K01 falha aberto	E101	2.
Disjuntor PA - CB01 falha aberto	E102	1.
TRU # 1 sem tensão DC de saída	E103	26.4
Curto-circuito na barra XP1	E104	.8
Curto-circuito na barra PP1	E105	.8
Gerador # 2 desligado	E106	80.8242
Contator XA - K02 falha aberto	E107	2.
Disjuntor PA - CB02 falha aberto	E108	1.
TRU # 2 sem tensão DC de saída	E109	26.4
Curto-circuito na barra XP2	E110	.8
Curto-circuito na barra PP2	E111	.8
Fusível PA - F03 aberto	E112	2.5
Contator PA - K03 falha aberto	E113	4.
Fusível PA - F04 aberto	E114	2.5
Chave da bateria falha aberta	E115	2.132
Relê de controle do contator da bateria PA - K02 falha fechado	E116	1.
Curto-circuito na barra PP4	E117	.8
Fusível PA - F06 aberto	E118	2.5
Disjuntor PA - CB08 falha aberto	E119	1.
Falha da bateria	E120	6.

TABELA 4.12 - TAXAS DE FALHAS RELATIVAS AOS EVENTOS DE FALHA

Os resultados obtidos para o Sistema de Geração Elétrica podem ser vistos na listagem a seguir.

Desta forma, tem-se que a probabilidade do sistema funcionar conforme especificado é

$$P = 1 - Q = 0,9999164$$

que vem demostrar que o valor determinado é melhor do que o especificado no início deste capítulo, de

$$P = 0,95$$

****
* EXPRESSAO RESULTANTE DA ARVORE ATRAVES DO *
* CALCULO DAS PROBABILIDADES DOS EVENTOS *
* INTERMEDIARIOS *
****

((E1+E2+E3+E4+E5+E6+E7+E8+E9+E10+E11+E12+E13+E14+E15+E16+E17+E18+E19+E20+E21+E22+E23+E24+E25+E26+E27+E28+E29+E30+E31)+((
(E53+E54+E55).(E51+E52))+(E41+E42)+((E56+E57).(E58+E59))+(E60.E61)+(E48+E49+E50)+((E62+E63).(E64+E65))+(E66+E67+E68)+(((
E44+E46+E47).E45)+((E39+E40).E38))+((E70+E71).(E72+E73+E74))+E32+E33+E34+E35+E36+E37+E69)+(((((E86+E87+E88).E85)+E78+E79
+E80+E81+E82+E83+E84).(E89+E90+E91+E92+E93+E94))+((((E95+E96).(E97+E98+E99))+((E100+E101+E102+E103+E104+E105).(E106+E107
+E108+E109+E110+E111))).(E112+E113+E114+E115+E116+E117+E118+E119+E120))+E75+E76+E77))

A PROBABILIDADE DE OCORRENCIA DO EVENTO TOPO E

I 0.864608749653600-04 I

4.6 - ANÁLISE DE SENSIBILIDADES

Para verificar a sensibilidade do sistema às variações das taxas de falha dos componentes, foram consideradas, separadamente, as árvores de falhas relativas às fases de Partida, Vôo e Pouso, durante o respectivo tempo de duração da missão.

Pode-se observar que, para a fase de Partida, onde a falha de qualquer componente leva ao cancelamento da missão - o que significa que todos os eventos de falha são conjuntos de corte de primeira ordem - quanto maior a variação, maior é a resposta do sistema a esta variação.

A probabilidade de falha desta fase da missão foi calculada em $0{,}5514 \times 10^{-4}$. Passando a verificar os resultados obtidos na tabela 4.5,notamos que E1, E2, E19 e E26 provocam as maiores variações no sistema. Isto era de se esperar, considerando que estas são as taxas de falha de maior valor.

Para a fase de Vôo, temos os eventos E32, E41, E48, E66 e E67 como mais significativos. De fato, esses eventos representam conjuntos de corte de 1ª. ordem e a influência maior é causada pelo modo de falha de maior taxa de falha. Isso pode ser visto nos resultados da tabela 4.6.

Finalmente, em relação à fase de Pouso, devido a alta redundância do sistema, do pouco tempo envolvido e das pequenas taxas de falha, o sistema praticamente não sente as variações propostas de 10% nas taxas de falha. Apenas os eventos E75, E76 e E77 provocam uma variação sensível no sistema [tabela 4.7].Isto porque são os únicos conjuntos de corte de 1ª. ordem, conforme pode ser visto na figura 4.5.

TABELA 4.5 - ANÁLISE DE SENSIBILIDADES DURANTE A FASE DE PARTIDA

$Q = 0,5514 \times 10^{-4}$

EVENTO	TAXA DE FALHA $[x10^{-6}]$ horas		$\frac{\Delta\lambda}{\lambda}$	PROBABILIDADE DE OCORRÊNCIA DO EVENTO TOPO $Q[x10^{-4}]$	$\frac{\Delta Q}{Q}$	$S_\lambda^Q = \frac{\frac{\Delta Q}{Q}}{\frac{\Delta\lambda}{\lambda}}$
	Inicial	Modificada				
E1	80,8242	72,7418	0,1	0,5433	0,0147	14,69%
E2	80,8242	72,7418	0,1	0,5433	0,0147	14,69%
E3	8,00	7,20	0,1	0,5506	0,0015	1,45%
E4	8,00	7,20	0,1	0,5506	0,0015	1,45%
E5	8,00	7,20	0,1	0,5506	0,0015	1,45%
E6	8,00	7,20	0,1	0,5506	0,0015	1,45%
E7	8,00	7,20	0,1	0,5506	0,0015	1,45%
E8	0,80	0,72	0,1	0,5513	0,0002	0,2%
E9	0,80	0,72	0,1	0,5513	0,0002	0,2%
E10	0,80	0,72	0,1	0,5513	0,0002	0,2%
E11	0,80	0,72	0,1	0,5513	0,0002	0,2%
E12	0,80	0,72	0,1	0,5513	0,0002	0,2%
E13	2,00	1,80	0,1	0,5512	0,0036	0,36%
E14	8,00	7,20	0,1	0,5506	0,0015	1,45%
E15	0,80	0,72	0,1	0,5513	0,0002	0,2%
E16	2,40	2,16	0,1	0,5511	0,0005	0,54%
E17	2,00	1,8	0,1	0,5512	0,0036	0,36%
E18	26,40	23,76	0,1	0,5487	0,0049	4,90%
E19	200,00	180,00	0,1	0,5314	0,0363	36,27%
E20	2,00	1,80	0,1	0,5512	0,0036	0,36%
E21	26,40	23,76	0,1	0,5487	0,0049	4,90%
E22	2,00	1,80	0,1	0,5512	0,0036	0,36%
E23	2,00	1,80	0,1	0,5512	0,0036	0,36%

TABELA 4.5 - ANÁLISE DE SENSIBILIDADES DURANTE A FASE DE PARTIDA

$Q = 0,5514 \times 10^{-4}$

EVENTO	TAXA DE FALHA [x 10^{-6}] horas		$\frac{\Delta\lambda}{\lambda}$	PROBABILIDADE DE OCORRÊNCIA DO EVENTO TOPO Q [x10^{-4}]	$\frac{\Delta Q}{Q}$	$S_{\lambda}^{Q} = \frac{\frac{\Delta Q}{Q}}{\frac{\Delta\lambda}{\lambda}}$
	Inicial	Modificada				
E24	6,00	5,40	0,1	0,5508	0,0011	1,09%
E25	2,537	2,263	0,1	0,5511	0,0005	0,54%
E26	60,00	54,00	0,1	0,5454	0,0109	10,88%
E27	0,40	0,36	0,1	0,5513	0,0002	0,2%
E28	0,40	0,36	0,1	0,5513	0,0002	0,2%
E29	0,80	0,72	0,1	0,5513	0,0002	0,2%
E30	0,80	0,72	0,1	0,5513	0,0002	0,2%
E31	0,80	0,72	0,1	0,5513	0,0002	0,2%

TABELA 4.6 - ANÁLISE DE SENSIBILIDADES DURANTE A FASE DO VOO

$Q = 0,3120 \times 10^{-4}$

EVENTOS	TAXA DE FALHA $[x10^{-6}]$ horas		$\frac{\Delta\lambda}{\lambda}$	PROBABILIDADE DE OCORRÊNCIA DO EVENTO TOPO $Q[x10^{-4}]$	$\frac{\Delta Q}{Q}$	$S_\lambda^Q = \frac{\frac{\Delta Q}{Q}}{\frac{\Delta\lambda}{\lambda}}$
	Inicial	Modificada				
E32	2,00	1,80	0,1	0,3093	0,0087	8,65%
E33	0,80	0,72	0,1	0,3109	0,0035	3,53%
E34	0,80	0,72	0,1	0,3109	0,0035	3,53%
E35	0,80	0,72	0,1	0,3109	0,0035	3,53%
E36	0,80	0,72	0,1	0,3109	0,0035	3,53%
E37	0,80	0,72	0,1	0,3109	0,0035	3,53%
E38	80,8242	72,7418	0,1	0,3120	0	0
E39	4,00	3,60	0,1	0,3120	0	0
E40	3,00	2,70	0,1	0,3120	0	0
E41	2,00	1,80	0,1	0,3093	0,0087	8,65%
E42	0,80	0,72	0,1	0,3109	0,0035	3,53%
E44	80,8242	72,7418	0,1	0,3120	0	0
E45	80,8242	72,7418	0,1	0,3120	0	0
E46	4,00	3,60	0,1	0,3120	0	0
E47	3,00	2,70	0,1	0,3120	0	0
E48	2,40	2,16	0,1	0,3088	0,0103	10,26%
E49	1,00	0,90	0,1	0,3107	0,0013	1,30%
E50	0,80	0,72	0,1	0,3109	0,0035	3,53%
E51	1,00	0,90	0,1	0,3120	0	0
E52	4,00	3,6	0,1	0,3120	0	0
E53	100,00	90,0	0,1	0,3120	0	0
E54	100,00	90,0	0,1	0,3120	0	0
E55	1,0	0,90	0,1	0,3120	0	0

TABELA 4.6 - ANÁLISE DE SENSIBILIDADES DURANTE A FASE DO VÔO

$Q = 0,3120 \times 10^{-4}$

EVENTOS	TAXA DE FALHA $[x10^{-6}]$ horas		$\frac{\Delta\lambda}{\lambda}$	PROBABILIDADE DE OCORRÊNCIA DO EVENTO TOPO $Q[x10^{-4}]$	$\frac{\Delta Q}{Q}$	$S_{\lambda}^{Q} = \frac{\frac{\Delta Q}{Q}}{\frac{\Delta\lambda}{\lambda}}$
	Inicial	Modificada				
E56	26,40	23,76	0,1	0,3120	0	0
E57	26,40	23,76	0,1	0,3120	0	0
E58	2,50	2,25	0,1	0,3120	0	0
E59	2,50	2,25	0,1	0,3120	0	0
E60	4,00	3,60	0,1	0,3120	0	0
E61	1,00	0,9	0,1	0,3120	0	0
E62	26,40	23,76	0,1	0,3120	0	0
E63	1,00	0,90	0,1	0,3120	0	0
E64	26,40	23,76	0,1	0,3120	0	0
E65	1,00	0,90	0,1	0,3120	0	0
E66	2,50	2,25	0,1	0,3087	0,0106	10,58%
E67	6,00	5,40	0,1	0,3039	0,0260	25,96%
E68	0,80	0,72	0,1	0,3109	0,0035	3,53%
E69	0,80	0,72	0,1	0,3109	0,0035	3,53%
E70	0,20	0,18	0,1	0,3120	0	0
E71	2,50	2,25	0,1	0,3120	0	0
E72	2,50	2,25	0,1	0,3120	0	0
E73	0,20	0,18	0,1	0,3120	0	0
E74	2,50	2,25	0,1	0,3120	0	0

TABELA 4.7 - ANÁLISE DE SENSIBILIDADES DURANTE A FASE DE POUSO

$Q = 0,1200 \times 10^{-6}$

EVENTOS	TAXA DE FALHA $[x10^{-6}]$ horas		$\frac{\Delta\lambda}{\lambda}$	PROBABILIDADE DE OCORRÊNCIA DO EVENTO TOPO $Q\ [x10^{-6}]$	$\frac{\Delta Q}{Q}$	$S_\lambda^Q = \frac{\frac{\Delta Q}{Q}}{\frac{\Delta\lambda}{\lambda}}$
	Inicial	Modificada				
E75	0,80	0,72	0,1	0,1160	0,033	33,60%
E76	0,80	0,72	0,1	0,1160	0,033	33,60%
E77	0,80	0,72	0,1	0,1160	0,033	33,60%
E78	1,00	0,90	0,1	0,1200	0	0
E79	1,00	0,90	0,1	0,1200	0	0
E80	0,80	0,72	0,1	0,1200	0	0
E81	0,80	0,72	0,1	0,1200	0	0
E82	2,40	2,16	0,1	0,1200	0	0
E83	2,00	1,80	0,1	0,1200	0	0
E84	1,00	0,90	0,1	0,1200	0	0
E85	80,8242	72,7418	0,1	0,1200	0	0
E86	3,00	2,70	0,1	0,1200	0	0
E87	4,00	3,60	0,1	0,1200	0	0
E88	80,8242	72,7418	0,1	0,1200	0	0
E89	4,00	3,60	0,1	0,1200	0	0
E90	1,00	0,90	0,1	0,1200	0	0
E91	100,00	90,00	0,1	0,1200	0	0
E92	100,00	90,00	0,1	0,1200	0	0
E93	1,00	0,90	0,1	0,1200	0	0
E94	1,00	0,90	0,1	0,1200	0	0
E95	0,20	0,18	0,1	0,1200	0	0
E96	2,50	2,25	0,1	0,1200	0	0
E97	0,20	0,18	0,1	0,1200	0	0
E98	2,50	2,25	0,1	0,1200	0	0

TABELA 4.7 - ANÁLISE DE SENSIBILIDADES DURANTE A FASE DE POUSO

$Q = 0,1200 \times 10^{-6}$

EVENTOS	TAXA DE FALHA [x 10^{-6}] horas		$\frac{\Delta\lambda}{\lambda}$	PROBABILIDADE DE OCORRÊNCIA DO EVENTO TOPO Q[x10^{-6}]	$\frac{\Delta Q}{Q}$	$S_\lambda^Q = \frac{\frac{\Delta Q}{Q}}{\frac{\Delta\lambda}{\lambda}}$
	Inicial	Modificada				
E99	2,50	2,25	0,1	0,1200	0	0
E100	80,8242	72,7418	0,1	0,1200	0	0
E101	2,00	1,80	0,1	0,1200	0	0
E102	1,00	0,90	0,1	0,1200	0	0
E103	26,40	23,76	0,1	0,1200	0	0
E104	0,80	0,72	0,1	0,1200	0	0
E105	0,80	0,72	0,1	0,1200	0	0
E106	80,8242	72,7418	0,1	0,1200	0	0
E107	2,00	1,80	0,1	0,1200	0	0
E108	1,00	0,90	0,1	0,1200	0	0
E109	26,40	23,76	0,1	0,1200	0	0
E110	0,80	0,72	0,1	0,1200	0	0
E111	0,80	0,72	0,1	0,1200	0	0
E112	2,50	2,25	0,1	0,1200	0	0
E113	4,00	3,6	0,1	0,1200	0	0
E114	2,50	2,25	0,1	0,1200	0	0
E115	2,132	1,919	0,1	0,1200	0	0
E116	1,00	0,90	0,1	0,1200	0	0
E117	0,80	0,72	0,1	0,1200	0	0
E118	2,50	2,25	0,1	0,1200	0	0
E119	1,00	0,90	0,1	0,1200	0	0
E120	6,00	5,40	0,1	0,1200	0	0

CAPÍTULO 5

CONCLUSÕES

O desenvolvimento deste trabalho paralelamente à experiência profissional da autora, possibilitou uma visão generalizada do estágio atual da confiabilidade na indústria aeronáutica do país e despertou o interesse em contribuir de alguma forma para seu avanço em direção ao estágio de desenvolvimento já atingido por outros países da Europa e Estados Unidos da América.

Os trabalhos já desenvolvidos nesta área possuem enfoque diferentes para aeronaves civis e militares.

Para aeronaves civis, sujeitas a processos de homologação, existem relatórios para comprovação de exigências do tipo JAR-25 ou FAR-25 (Apêndice 2). Estes estudos visam comprovar desempenho favorável dos diversos sistemas da aeronave. São feitas descrições dos sistemas, Análises de Modos de Falha e seus Efeitos e, quando são detetadas situações de risco, são desenvolvidas análises quantitativas por Árvores de Falhas a fim de classificar o risco dentro de faixas aceitáveis de probabilidade de falha.

Para aeronaves militares, a confiabilidade de uma missão típica foi avaliada pelo método de Diagrama de Blocos , visando atender ao requisito imposto pelas Forças Aéreas.Assim, todos os sistemas foram analisados seguindo a lógica positiva, ou seja, verificando quais as associações de sucessos de componentes levam ao sucesso do sistema.

A partir dessas informações, pesquisou-se várias metodologias de análise de confiabilidade, que estão descritas em capítulos anteriores, de forma a encontrar aquelas que melhor se adaptem aos sistemas aeronáuticos, cujas características predominantes são complexidade e alto risco.

Os métodos estabelecidos para atingir esses objetivos foram Análise de Modos de Falha e seus Efeitos - FMEA - para análise qualitativa e Árvore de Falhas para análise qualitativa e quantitativa.

A FMEA é utilizada para exploração exaustiva dos modos potenciais de falha de todos os componentes e sua consequência no estado operacional do sistema. É um primeiro passo necessário para que nenhum detalhe importante para a análise seja negligenciado. Isto foi constatado durante o desenvolvimento da FMEA do Sistema Elétrico de Geração, que encontra-se no Capítulo 4.

Conforme já citado em capítulos anteriores, a FMEA tem grande importância na fase de projeto e pode ser desenvolvida inicialmente com limitada informação, sendo atualizada periodicamente até ser atingido o nível de informações desejado.

Modos de falha que tenham consequências imprevisíveis no sistema requerem investigações por testes para que as consequências possam ser avaliadas e evitadas. Isto ocorreu várias vezes e os fornecedores de equipamentos foram também solicitados a investigar a possibilidade de ocorrerem alguns modos de falha e suas consequências na operação do componente.

Através das FMEA's dos sistemas, foram localizados pontos vulneráveis que exigiram modificações de projeto que foram implementadas e, quando aplicável, operações de inspeções

e testes foram recomendadas para monitorar o funcionamento do sistema.

O próximo passo foi o estabelecimento das taxas de falha para cada modo de falha da FMEA. Este é um problema que merece atenção especial na busca de solução. Os dados estatísticos de falha de muitos equipamentos não estão disponíveis. Embora havendo interesse em usar dados dos próprios equipamentos sujeitos a solicitações particulares de projeto, muitas vezes os testes de demonstração de confiabilidade não são viáveis por razões de ordem econômica ou mesmo de tempo e pessoal envolvidos. Neste caso, uma alternativa é usar dados de equipamentos similares que foram operados em condições o mais próximo possível da realidade.

Existem publicações [30,31,32] e instituições estrangeiras* que se ocupam da coleta e organização de dados para equipamentos de interesse.

Neste trabalho, foram utilizados todos os recursos citados: dados próprios de alguns componentes, dados de componentes similares e outras vezes as publicações já citadas.

Após desenvolver a FMEA, estando o sistema bem conhecido, pôde-se determinar os modos e combinações de modos de fa

* *Podem ser citadas as organizações:*

- *GIDEP: Government - Industry Data Exchange Program. Corona, Califórnia. 91720. USA.*
- *EXACT: International Exchange of Authenticated Electronic Component Performance Test Data. London N12, ENGLAND.*

lha que levam à falha do sistema.

De acordo com as características da missão, foram determinados os eventos-topo, representando incapacidade do sistema em desempenhar sua função. Pelas características próprias de uma missão aérea, três períodos distintos foram considerados , para satisfazer as exigências que são maiores para liberar a partida, diminuem depois de iniciado o vôo, permitindo-se algumas falhas em sistemas redundantes, desde que não haja limitação operacional e são ainda mais flexíveis para o pouso, desde que não seja comprometida a integridade da aeronave e piloto.

A Árvore de Falhas, por sua característica gráfica , favorece a visualização das condições críticas do sistema sendo, por isso, um bom instrumento para análise qualitativa. É necessário ressaltar que a FMEA e a Árvore de Falhas, como elementos de análise qualitativa não constituem duas alternativas opcionais mas sim complementares. A FMEA presta-se à análise minuciosa dos vários ítens envolvidos no sistema, enquanto que a Árvore de Falhas mostra objetivamente os modos e combinação de modos de falha que são críticos ao sistema.

Para análise quantitativa das Árvores de Falhas foi desenvolvido um algorítmo para determinar a probabilidade de ocorrência do evento topo. Tal algorítmo, que se encontra descrito no Apêndice B foi implementado e vem sendo usado constantemente, demonstrando ser bastante eficiente e rápido.

À medida que o tamanho da árvore cresce, torna-se necessário automatizar o processo de cálculo. A análise de sensibilidades é praticamente inviável se não se dispõe de um algorítmo eficiente.

Neste trabalho, foi desenvolvida uma Análise de Sen

sibilidades, variando a taxa de falha de cada componente em 10% e verificando o efeito desta variação sobre a confiabilidade do sistema. Pôde-se observar maior ou menor variação na confiabilidade do sistema, em função da importância relativa do componente ou dos valores das taxas de falhas para os componentes de mesmo grau de importância. Esses resultados são de utilidade para quantificar um melhoramento desejado e selecionar os componentes que poderão provocar este melhoramento. Desta forma, é possível desenvolver análises de custo e benefício para estabelecer prioridades neste melhoramento.

Uma outra aplicação da análise de sensibilidades refere-se à seleção de componentes para serem realizados testes de demonstração de confiabilidade. A sensibilidade do sistema a pequenas variações na taxa de falha de determinado componente , é um indicador de sua importância e deve ser usada como justificativa para requerer testes de demonstração desses valores.

É bastante evidente a utilidade da análise quantitativa da confiabilidade de sistemas. Ao mesmo tempo que a importância é reconhecida, a constatação da carência de informação de dados é alarmante.

Atualmente, indústria aeronáutica, clientes e operadores estão se organizando para que as informações sejam coletadas e analisadas em Bancos de Dados , visando melhoramento da qualidade, confiabilidade, disponibilidade e mantenabilidade.

Depara-se com um novo trabalho a ser desenvolvido e que consiste numa pesquisa criteriosa para estabelecer as informações necessárias a serem extraídas do Banco de Dados, do treinamento e conscientização de pessoas que irão coletar os dados, de forma a assegurar confiança nos resultados obtidos.

Este trabalho pode ser agrupado em um conjunto maior, reunindo as análises de todos os sub-sistemas, onde se considera também a possibilidade de erro humano desde a concepção, entrando na operação e manutenção do sistema.

Da mesma forma, as possíveis falhas de modo comum em um sistema ou entre sistemas é outro aspecto de grande importância na análise de confiabilidade, que merece um estudo a parte. Os sub-sistemas devem ser analisados quanto a seu projeto e instalação. Deve-se avaliar a eficiência de redundâncias frente a probabilidade de ocorrência de falhas de modo comum.

Além disso, deve-se garantir que canais redundantes sejam fisicamente separados e protegidos de modos de falha que possam tornar indispensaveís vários sistemas ao mesmo tempo.

BIBLIOGRAFIA

[1] LAPP, Steven A. & POWERS, Gary J. *Computer-aided synthesis of fault-trees*. IEEE TRANSACTIONS ON RELIABILITY.Durham, USA. Ralph A. Evans, 2-13, apr. 1977.

[2] BERKOWITZ, D.G; PETERSON, C.A.; POWEL,B.A. - *Study of Series Capacitor Reliability Using Fault Tree Analysis* - BLOOMING TON, IND. - Westinghouse Electric Corporation - 1975.

[3] LAMBERT, Howard E. *Comments on the Lapp-Powers computer-aided synthesis for fault-trees*. IEEE TRANSACTIONS ON RELIABILITY. Durham, USA. Ralph A. Evans, *28*: 6-11, apr. 1979.

[4] YELLMAN, Ted W. - *Comment on "Comments on computer-aided synthesis of Fault Tree"* - IEEE TRANSACTIONS ON RELIABILITY. Durham USA. Ralph A. Evans, *28*: 10-11, apr. 1979.

[5] LAPP, Steven A. & POWERS, Gary J. - *Update of Lapp - Powers Fault - Tree Synthesis Algorithm* - IEEE TRANSACTIONS ON RE LIABILITY. Durham, USA. Ralph A. Evans, *28*:12 - 15, apr.1979.

[6] TAYLOR; J.R. *An Algorithm for fault-tree construction*. IEEE TRANSACTIONS ON RELIABILITY. Durham, USA. Ralph A. Evans,*31*: 137-146, jun. 1982.

[7] PAU, L.F. & WEBER, G.G. - *A Fault Tree Approach to Quality Control by Variables* - IEEE TRANSACTIONS ON RELIABILITY. Dur ham, USA. Ralph A. Evans, *28*: 344-352, dec.1979.

[8] CUMMINGS, Daniel L.; LAPP, Steven, A.; POWERS, Gary, J.-*Fault Tree Synthesis From a Direct Graph Model for a Power Distri bution Network* - IEEE TRANSACTIONS ON RELIABILITY. Durham, USA. Ralph A. Evans, *32*: 140-149, Jun. 1983.

[9] BLAKE, Martin W.; LOFE, James J.; STRINGFELOW, Norman J. *Using fault tree methodologies in availability improvement studies at Southern Company Services*. IEEE TRANSACTIONS ON RELIABILITY. Durham, USA. Ralph A. Evans, *PAS-103*: 656-660 , mar. 1984.

[10] ANDERSON, P.M. - *Reliability Modeling of Protective Systems* IEEE TRANSACTIONS ON RELIABILITY. Durham, USA. Ralph A.Evans, *PAS-103*: 2207-2214, aug. 1984

[11] FUSSEL, J.B. & VESELY, W.E. *A new methodology for obtaining cut sets for fault-trees*. TRANSACTIONS OF THE AMERICAN NUCLEAR SOCIETY. *15*: 262-263, 1972.

[12] KUMAMOTO, H. & HENLEY, ERNEST J. - *Top-Down Algorithm for Obtaining Prime Implicant Sets of Non - Coherent Fault Trees* -IEEE TRANSACTIONS ON RELIABILITY. Durham, USA. Ralph A. Evans, *27*:242-249, oct. 1978.

[13] NAKASHIMA, Kyoichi & HATTORI, Yoshio - *An Efficient Bottom - up Algorithm for Enumerating Minimal Cut Sets of Fault Trees* -IEEE TRANSACTIONS ON RELIABILITY. Durham, USA. Ralph A. Evans, *28*: 353-357, dec. 1979.

[14] FEO, Thomaz, PAFT F77, *Program for the Analysis of Fault Trees* - IEEE TRANSACTIONS ON RELIABILITY. Durham, USA. Ralph A. Evans, *35*: 48-50, apr. 1986

[15] CARGAL, James M. - *An Alternative Fault - Tree Algebra* - IEEE TRANSACTIONS ON RELIABILITY. Durham, USA. Ralph A. Evans,*29*: 269-272, aug. 1980

[16] LOCKS, Michell O. *The fail safe feature of the Lapp & Powers fault tree*. IEEE TRANSACTIONS ON RELIABILITY.Durham, USA. Ralph A. Evans, *29*: 10-11, apr. 1980.

[17] INAGAKI, Toshiyuki & HENLEY, Ernest J. - *Probabilistic Evaluation of Prime Implicants and Top - Events for Non- Coherent Systems* - IEEE TRANSACTIONS ON RELIABILITY. Durham, USA. Ralph A. Evans, *29*: 361-367, Dec. 1980.

[18] OGUNBIYI, ELIZABETH I. & HENLEY, ERNEST J. - *Irredundant Forms and Prime Implicants of a Function with Multistate Variables* - IEEE TRANSACTIONS ON RELIABILITY . Durham, USA . Ralph A. Evans, *30*: 39-42, apr. 1981.

[19] CLAROTTI, C.A. - *Limitations of Minimal Cut - Set Approach in Evaluating Reliability of Systems with Repairable Components* - IEEE TRANSACTIONS ON RELIABILITY. Durham, USA. Ralph A. Evans, *30*: 335-338, oct. 1981

[20] NUCLEAR POWER ENGINEERING COMMITTEE OF THE IEEE POWER ENGINEERING SOCIETY. *IEEE guide for general principles of reliability analysis of nuclear power generating station protection systems*, 1975. (IEEE std 352)

[21] JOLLER, J.M. *Constructing Fault - Tree by Stepwise Refinement*. IEEE TRANSACTIONS ON RELIABILITY. Durham, USA Ralph A. Evans, *31*: 333-338, oct. 1982.

[22] LLOYD,E. & TYE, W. *Systematic Safety*. London, England.Taylor Young Limited, 1982. 159p.

[23] BARLOW, Richard E. & PROSCHAN, Frank. *Mathematical Theory of Reliability*. USA. John Wiley & Sons, Inc., 1965. 255p.

[24] BARLOW, Richard E. & PROSCHAN, Frank. *Statiscal Theory of Reliability and Life Testing - Probability Models*. USA. Holt, Rinehart and Winston, Inc., 1975. 290p.

[25] MANN, Nancy R.; SCHAFER, Ray E.; SINGPURWALLA, Nozer D. *Methods for Statistical Analysis of Reliability and Life Data.* USA. John Wiley & Sons, Inc., 1974. 564p.

[26] BAZOVSKY, Igor. *Reliability Theory and Practice.* USA. Prentice-Hall Inc., 1961. 292p.

[27] HENLEY, Ernest J. & KUMAMOTO, Hirumitsu. *Reliability Engineering and Risk Assessment* - USA. Prentice - Hall, Inc., 1981. 568p.

[28] ANDERSON, R.T. *Reliability Design Handbook* - Rome Air Development Center, NY, 1976. 392 p.

[29] EVANS, Ralph A. O Data, Data! *Wherefore Art Thou Data?* IEEE TRANSACTIONS ON RELIABILITY. Durham, USA. Ralph A. Evans, *31*: 321, oct. 1982.

[30] IEEE *Guide to the Collection and Presentation of Eletrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear - Power Generating Stations* - IEEE Std 500-1984 - *Nuclear Power Engineering Committee of* IEEE *Power Engineering Society* - IEEE, Inc, NY, 1983. 1424 p.

[31] FULTON, Donald W. *Nonelectronic Parts Reliability Data* - Rome Air Development Center, NY, 1978. 245p.

[32] MIL - HDBK - 217D. *Military Handbook - Reliability Prediction of Electronic Equipment* - USA, 1982. 438p.

[33] CAMARGO, C. Celso de B. *Confiabilidade Aplicada a Sistemas de Potência Elétrica* - R.Janeiro, BR. Livros Técnicos e Científicos Editora S.A., 1981. 206p.

[34] BUSLENKO, N.P.; GOLENKO, D.I.; SHREIDER; YuA.; SOBOL', I.M.; SRAGOVICH, V.G. - *The Monte Carlo Method. 2 ed.*; Great Britain. Compton Printing Ltd., Aylesbury, Bucks, 1967. 381p.

[35] KUMAMOTO, H; HENLEY, E.J.; INOUE, K. *Signal - Flow - Based Graphs for Failure Mode Analysis of Systems with Control Loop* IEEE TRANSACTIONS ON RELIABILITY. Durham, USA. Ralph A.Evans, *30*: 110-116, Jun. 1981.

[36] NUNES, Renato A.F. *Confiabilidade de Sistemas de Potência* 1981. 282p.

[37] OLIVEIRA, Luiz F.S.; MELO, Paulo F.F.; FLEMING, Paulo V. *Confiabilidade e Árvores de Falhas*. 1984. 428p.

[38] Mc CORMICK, Norman J. *Reliability and risk analysis*. 1 ed. ; New York, USA. Academic Press, Inc., 1981. 446p.

[39] DHILLON, B.S.; SINGH, Chanan. *Engineering Reliability*. USA. John Wiley & Sons, 1981.

[40] HIGGINS, J. J. & TSOKOS,C.P. *A Quasi-Bayes Estimates of the Failure Intensity of a Reliability - Growth Model* - IEEE TRANSACTIONS ON RELIABILITY. Durham, USA. Ralph A. Evans,*30*: 471-475, Dec. 1981.

[41] AMOIA, V.; BOBBIO,A.; PREMOLI,A.; SANTOMAURO,M.; SARACCO,O.- *Optimum Time - Domain Design of System Reliability* - IEEE TRANSACTIONS ON RELIABILITY - Durham, USA. Ralph A. Evans,*30*: 71-73, Apr. 1981

[42] CHURCHLEY, Andrew R. - *Reliability Techniques in the Service of Industry* - IEEE TRANSACTIONS ON RELIABILITY. Durham, USA. Ralph A. Evans, *30*: 306-308, oct.1981.

[43] SAKAWA, MASATOSHI - *Optimal Reliability Design of a Series-Parallel System by a Large - Scale Multiobjective Optimization Method* - IEEE TRANSACTIONS ON RELIABILITY . Durham, USA. Ralph A. Evans, *30*: 173-174, Jun.1981.

[44] SINGH, C.; *A Matrix Approach to Calculate the Failure Frequency and Related Indices* - MICROELECTRONIC RELIABILITY . GREAT BRITAIN, *19*: 395-398, 1979.

[45] SINGH, C.; *A New Method to Determine the Failure Frequency of a Complex System* - IEEE TRANSACTIONS ON RELIABILITY. Durham, USA. Ralph A. Evans, *23*: 231-239, Oct. 1974.

[46] ANGUS, JOHN E. & SCHAFER, R.E - *Statistical Demonstration of Fault-Isolation Requirements* - IEEE TRANSACTIONS ON RELIABILITY. Durham, USA. Ralph A. Evans, *29*: 116-121, Jun.1980.

[47] SINGH., C. & PATTON, A.D. - *Protection System Reliability Modeling: Unreadiness Probability and Mean Duration of Undetected Faults* - IEEE TRANSACTIONS ON RELIABILITY. Durham, USA . Ralph A. Evans, *29*: 339-340, Oct.1980.

[48] HERRIN, STEPHANIE A. - *Maintainability Applications Using the Matrix FMEA Technique* - IEEE TRANSACTIONS ON RELIABILITY. Durham, USA. Ralph A. Evans, *30*: 212-217, Aug. 1981.

[49] CONNOR,John A. - *I Challenge Your Beliefs About Reliability Part. III: Analitic Practices* - IEEE TRANSACTIONS ON RELIABILITY. Durham, USA. Ralph A. Evans, *31*: 313-315, Aug. 1982.

[50] DUNGLINSON, C & LAMBERT, HOWARD. *Interval reliability for iniciating and enabling events*. IEEE TRANSACTIONS ON RELIABILITY. Durham, USA. Ralph A. Evans, *32*: 150-163, jun. 1982.

[51] STECHER, K. *Fault tree analysis, taking into account causes of common mode failures*. SIEMENS FORSCH. *13*(4), 1984.

[52] ALLAN, R.N.; RONDIRIS, I.L.; FRYER, D.M - *An Efficient Computational Technique for Evaluating the Cut/Tie Sets and Common - Cause Failures of Complex Systems* - IEEE TRANSACTIONS ON RELIABILITY. Durham, USA. Ralph E. Evans, *30*: 101-109, Jun. 1981.

[53] AHMAD, S. Hasamuddin . *A simple technique for computing network reliability*. IEEE TRANSACTIONS ON RELIABILITY. Durham, USA. Ralph A. Evans, *31*: 41-44, apr. 1982.

[54] TAKARAGI, Kazuo; SASAKI, Ryoichi; SHINGAI, Sadanori. *An improved moment - matching algorithm for evaluating top-event probability bounds*. IEEE TRANSACTIONS ON RELIABILITY.Durham, USA. Ralph A. Evans, *31*: 45-48, apr. 1982.

[55] MIL - STD - 1629. *Military Standard - Procedures for Performing a Failure Mode, Effects and Criticality Analysis for Aeronautical Equipment - Department of Defense*, USA, 1980.

[56] HWANG, C.L.; TILLMAN, Frank A.; LEE, M.H. *System reliability evaluation techniques for complex/large systems - a review*. IEEE TRANSACTIONS ON RELIABILITY. Durham, USA. Ralph A.Evans, *30*: 416-423, dec. 1981.

[57] BENNETTS, R.G. *Analysis of reliability block diagrams by Boolean Techniques*. IEEE TRANSACTIONS ON RELIABILITY.Durham, USA. Ralph A. Evans, *31*: 159-166, jun. 1982.

[58] NAKASHIMA, KYOICHI - *Some Properties of Logic - Trees Containing Mutually - Exclusive Primary - Events* - IEEE TRANSACTIONS ON RELIABILITY. Durham, USA. Ralph A. Evans, *28*: 303-308, Oct. 1979.

[59] PEDAR, A. & SARMA, V.V.S. *Phased - mission analysis for evaluating the effectiveness of aerospace computing systems.* IEEE TRANSACTIONS ON RELIABILITY. Durham, USA. Ralph A.Evans, *30*: 429-437, dec. 1981.

[60] AGGARWAL, K.K. - Comments on "*An Efficient Simple Algorithm for Fault Tree Automatic Synthesis from the Reliability Graph*" IEEE TRANSACTIONS ON RELIABILITY. Durham, USA. Ralph A.Evans, *28*: 309-315, oct. 1979.

[61] ARNBORG, STEFAN - *A Simple Event - Definition Notation and Associated Computer Programs* - IEEE TRANSACTIONS ON RELIABILITY. Durham, USA. Ralph A. Evans, *28*: 382-385, dec. 1979

[62] LOCKS, Michell O. *Synthesis of fault trees: an example of noncoherence.* IEEE TRANSACTIONS ON RELIABILITY. Durham, USA. Ralph A. Evans, *28*: 2-5, apr. 1979.

[63] STECHER, Karl - *Evaluation of Large Fault - Trees With Repeated Events Using an Efficient Bottom - Up Algorithm* - IEEE TRANSACTIONS ON RELIABILITY. Durham, USA. Ralph A. Evans, *35*: 51-58, APR. 1986.

[64] WORREL, R.B; STACK, D.W.; HULME, B.L. - *Prime Implicants of Noncoherent Fault Trees* - IEEE TRANSACTIONS ON RELIABILITY . Durham, USA. Ralph A. Evans, *30*: 98-100, Jun. 1981.

[65] KHAN, N.M.; RAJAMANI, K.; BANERJEE, S.K. *A direct method to calculate the frequency and duration of failures for large networks.* IEEE TRANSACTIONS ON RELIABILITY. Durham, USA . Ralph A. Evans, *26*: 318-321, dec. 1977.

[66] CHU, T.L. & APOSTOLAKIS, G. - *Methods for Probabilistic Analysis of Noncoherent Fault Trees* - IEEE TRANSACTIONS ON RELIABILITY. Durham,USA.Ralph A.Evans, *29*:354-360, dec. 1980.

[67] MILLER, H. Gilbert & BRAFF, Ronald. *Impact of the frequency of technician visits on facility failure rate*. IEEE TRANSACTIONS ON RELIABILITY. Durham, USA. Ralph A. Evans, 26: 245-247, oct. 1977.

[68] LOCKS, MITCHELL O. - *Modularizing, Minimizing, and Interpreting the K & H Fault - Tree* - IEEE TRANSACTIONS ON RELIABILITY. Durham, USA. Ralph A. Evans. 30:411-415, dec.1981.

[69] ANDOW, P.K. *Difficulties in fault-tree synthesis for process plant*. IEEE TRANSACTIONS ON RELIABILITY. Durham, USA. Ralph A. Evans, 29: 2-9, apr. 1980.

[70] SCHROEDER; R.J. - *Fault Tree for Reliability Analysis* - PROCEEDINGS OF THE ANNUAL SYMPOSIUM RELIABILITY, IEEE, New York, 1970.

[71] ROSENTHAL, Arnie; *Approaches to Comparing cut-set enumeration algorithms* - IEEE TRANSACTIONS ON RELIABILITY. Durham, USA. Ralph A. Evans, 28: 62-65, apr. 1979.

[72] NANDA, N.K. - *Application of a Boolean Identity for Fault Trees* - IEEE TRANSACTIONS ON RELIABILITY. Durham, USA. Ralph A.Evans, 29: 12, Apr. 1980.

[73] LOCKS, Mitchell O. - *Fault Trees, Prime Implicants, and Noncoherence* - IEEE TRANSACTIONS ON RELIABILITY. Durham, USA . Ralph A. Evans, 29: 130-138, Jun. 1980.

[74] MIL - STD - 785. *Military Standard - Reliability Program for System and Equipment Development and Production - Department of Defense, USA, 1980.*

APÊNDICE A

PROGRAMA ÁRVORE

A.1 - INTRODUÇÃO

Este programa será utilizado para determinar as probabilidades de ocorrência de eventos básicos e combiná-los segundo a lógica de uma árvore de falhas conhecida a fim de obter-se a probabilidade de ocorrência do evento topo estabelecido.

A.2 - DESCRIÇÃO

O presente programa presta-se à determinação da associação lógica eventos-portões numa árvore de falhas calculando a probabilidade de ocorrência do evento topo, de maneira simples, direta e funcional.

Determina e calcula a expressão final da probabilidade de ocorrência do evento topo a partir dos dados de taxas de falha e tempo para cada evento básico da árvore de falhas.

"ÁRVORE" está escrito em Fortran 77 para o Computador IBM/37Ø. Seu algorítmo, que segue o processo de **explosão escalonada** percorre todos os caminhos existentes, partindo do topo, buscando os eventos básicos e operando com eles de acordo com o portão encontrado (OU ou E).

O programa oferece a facilidade de escolha de qualquer portão como topo para cálculo da probabilidade de ocorrência de um evento intermediário desejado.

Pode-se facilmente utilizá-lo para análise de sensibilidades.

A formatação de entrada é simples, não exigindo dados previamente ordenados. O programa incumbe-se de ordená-los.

As figuras A.1, A.2, A.3 e A.4 mostram o fluxograma do programa desenvolvido, batizado de "ÁRVORE".

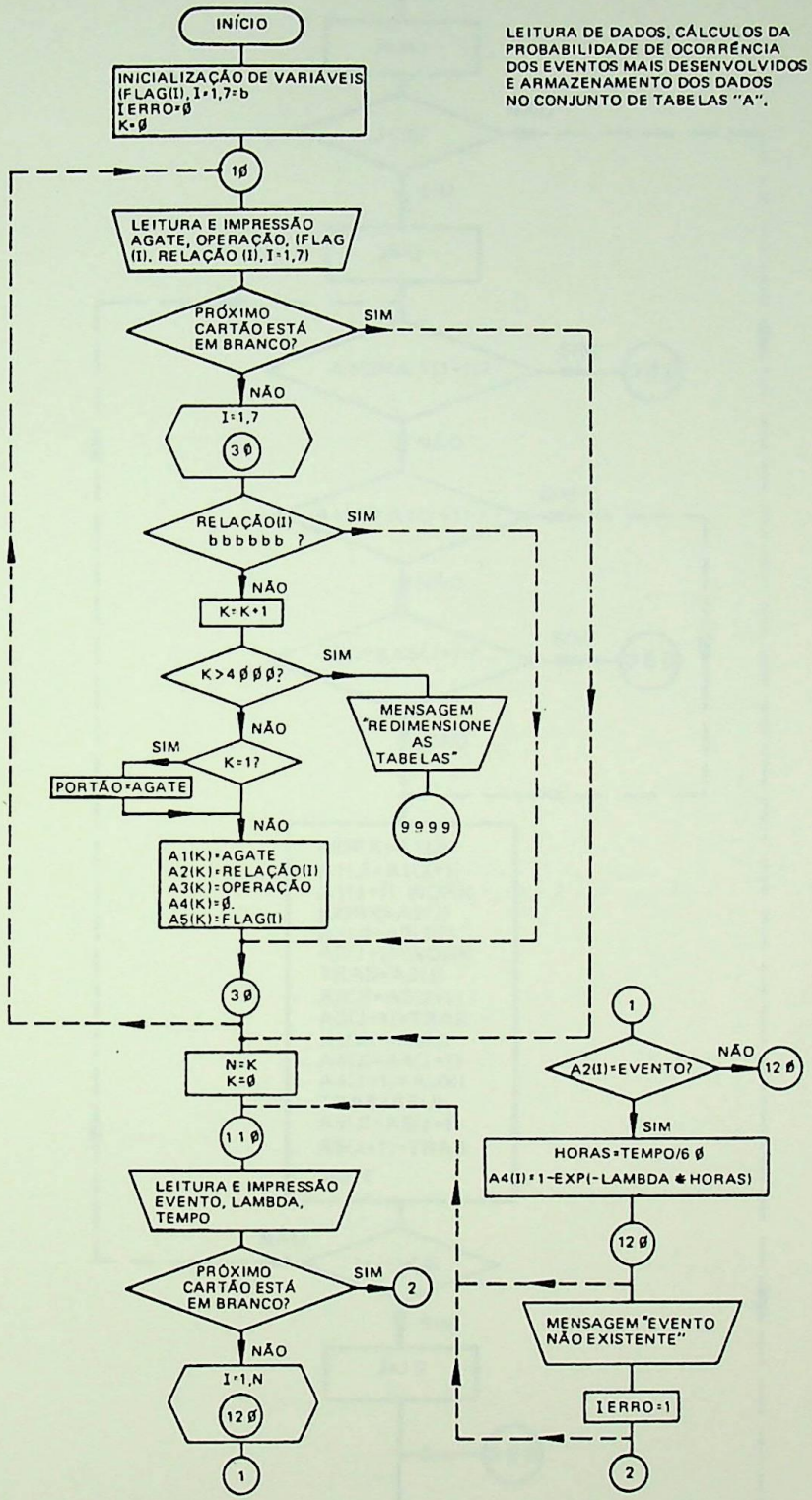
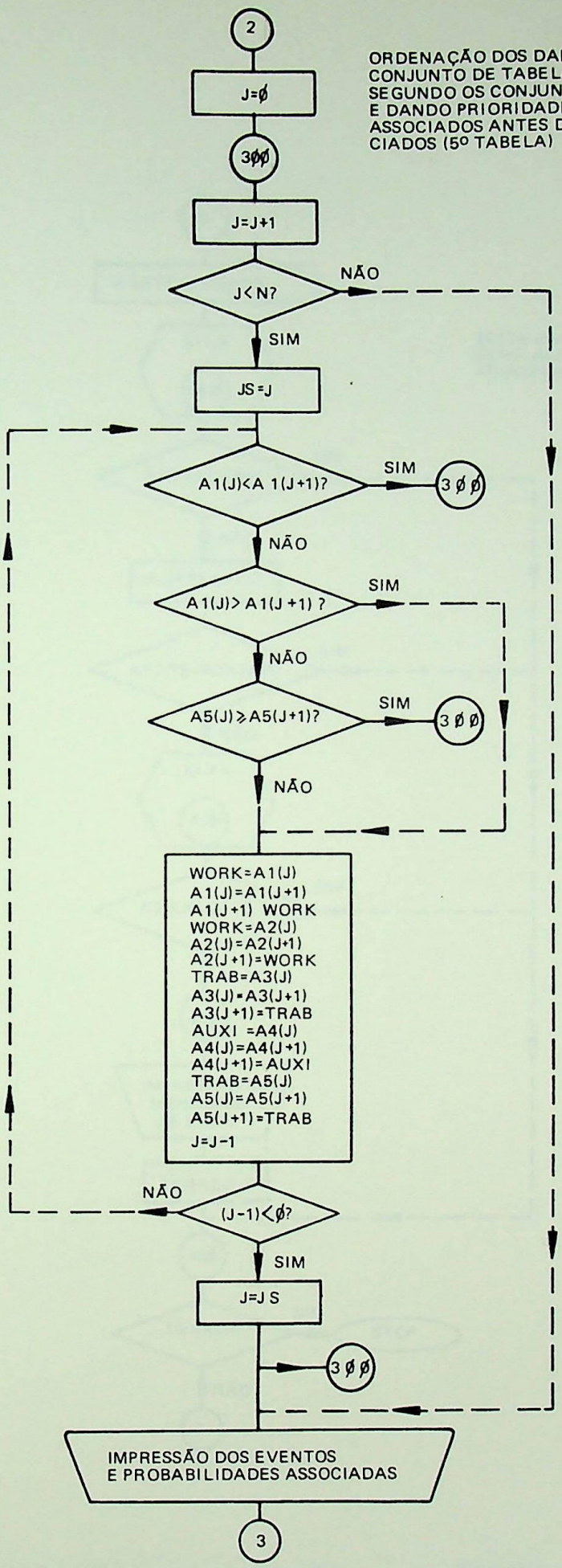


FIGURA A1 - Fluxograma do Programa ÁRVORE



ORDENAÇÃO DOS DADOS CONTIDOS NO CONJUNTO DE TABELAS A, CRESCENTE SEGUNDO OS CONJUNTOS DA 1ºTABELA E DANDO PRIORIDADE AOS CONJUNTOS ASSOCIADOS ANTES DOS EVENTOS ASSOCIADOS (5º TABELA)

FIGURA A2 - Fluxograma do Programa ÁRVORE

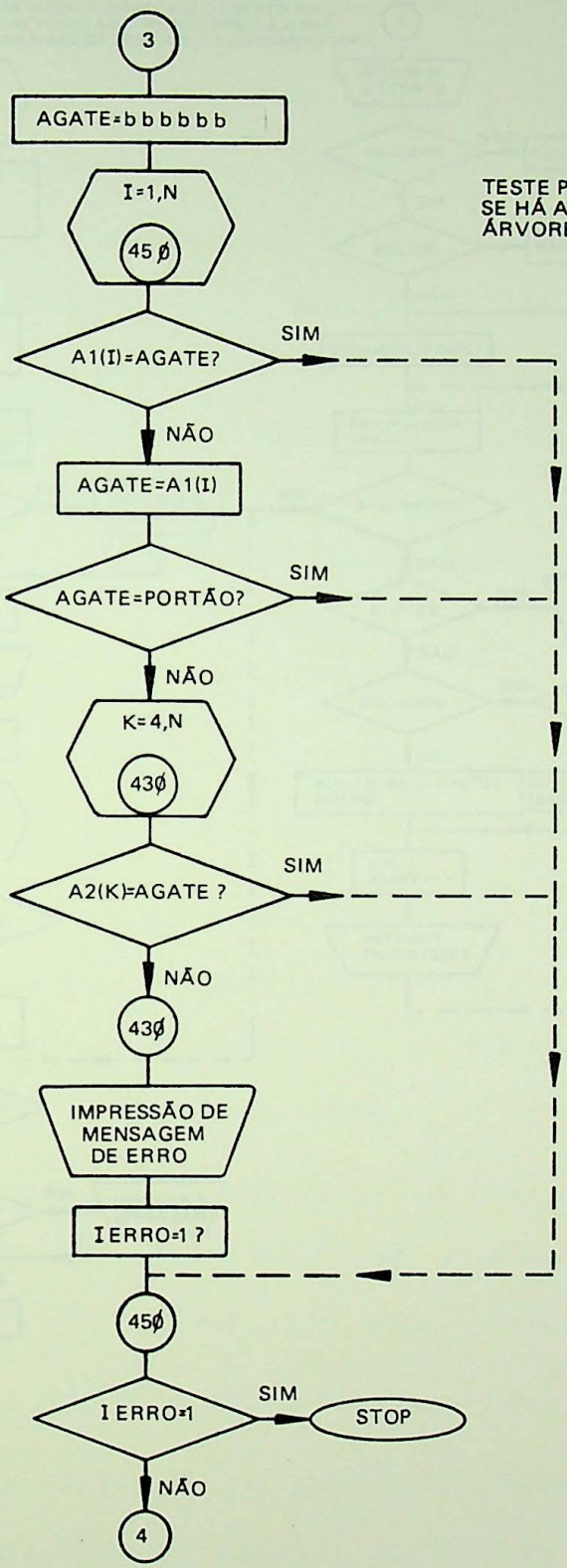


FIGURA A 3 - Fluxograma do Programa ÁRVORE

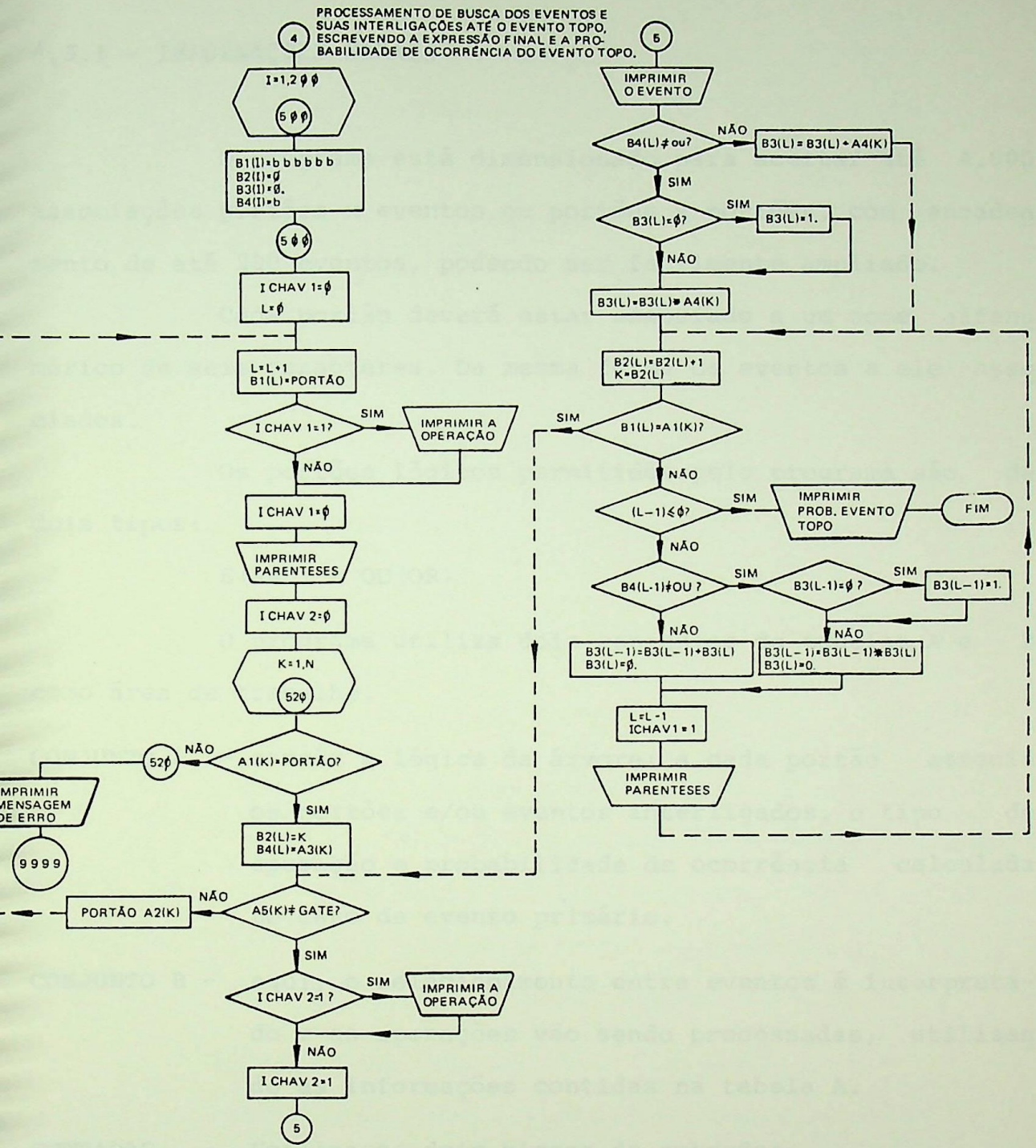


FIGURA A4 - Fluxograma do Programa ÁRVORE

A.3 - MANUAL DO USUÁRIO

A.3.1 - INFORMAÇÕES GERAIS

O programa está dimensionado para aceitar até 4.000 associações portões x eventos ou portões x portões, com encadeamento de até 200 eventos, podendo ser facilmente ampliado.

Cada portão deverá estar associado a um nome alfanumérico de seis caracteres. Da mesma forma os eventos a ele associados.

Os portões lógicos permitidos pelo programa são de dois tipos:

E(AND) e OU(OR)

O programa utiliza dois conjuntos de tabelas A e B como área de trabalho.

CONJUNTO A - contém a lógica da árvore: a cada portão associa os portões e/ou eventos interligados, o tipo de operação e probabilidade de ocorrência calculada no caso de evento primário.

CONJUNTO B - aqui, o relacionamento entre eventos é interpretado e as operações vão sendo processadas, utilizando as informações contidas na tabela A.

ENTRADAS - Utiliza-se dois blocos de entradas.

Entrada 1 - Constam deste bloco os seguintes dados: Nome do portão, tipo de portão, portões e/ou eventos associados.

Entrada 2 - As instruções dadas neste bloco são: tempo da missão e taxas de falha dos eventos básicos.

SAÍDAS - Utiliza-se dois tipos de saída

Saída 1 - O valor encontrado para a probabilidade de ocorrência do evento topo.

Saída 2 - A expressão final encontrada para o cálculo da probabilidade de ocorrência do evento topo.

A.3.2 - ENTRADA DO PROGRAMA

Os dados de entrada devem conter as informações sobre a árvore de falhas.

A.3.2.1 - DESCRIÇÃO DE ENTRADA DA ESTRUTURA DA ÁRVORE - 1º CONJUNTO DE DADOS

OBSERVAÇÃO: O primeiro portão será interpretado como EVENTO TOPO. Logo, coloque em primeiro lugar o "topo" desejado. Não há exigências para os portões seguintes.

Os dados serão lidos no seguinte formato:

FORMAT [A6, A1, 1X, 7(A1, 1X, A6)]

Acompanhe a tabela 1 para introduzir os dados.

A.3.2.2 - DESCRIÇÃO DE ENTRADA DE VALORES ASSOCIADOS AOS EVENTOS - 2º CONJUNTO DE DADOS

Os dados serão lidos no seguinte formato:

FORMAT [A6, D12.4, 1X, F8.3]

Acompanhe a tabela 2 para introduzir os dados.

ENTRADA	CAMPO DE LEITURA (COLUNAS DO CARTÃO)
1. Nome do portão - seis caracteres alfanuméricos	1 a 6
2. Operação - símbolo + ou.	7
3. Espaço em branco	8
4. Flag indicando se o próximo elemento é evento ou portão-carater E ou G.	9
5. Espaço em branco	10
6. Nome do evento e (ou) portão associado - seis caracteres alfanuméricos.	11 a 16
7. Flag indicando se o próximo elemento é evento ou portão-carater E ou G.	17
8. Espaço em branco	18
9. Nome do evento e(ou) portão associado - seis caracteres alfanuméricos.	19 a 24
10. Flag ...	25
.	.
.	.
.	.
.	.

TABELA 1 - DESCRIÇÃO DO 1o. CONJUNTO DE ENTRADA

ENTRADA	CAMPO DE LEITURA (COLUNAS DO CARTÃO)
1. Nome do evento-seis caracteres alfanuméricos	1 a 6
2. Taxa de falha (lambda) doze caracteres obedecendo ao formato exponencial em dupla precisão.	7 a 18
3. Espaço em branco	19
4. Tempo-variável real com 4 inteiros e 3 decimais	20 a 27

TABELA 2 - DESCRIÇÃO DO 2o. CONJUNTO DE ENTRADA

A.4- EXEMPLO TÍPICO

O exemplo descrito a seguir refere-se à árvore de senhada abaixo.

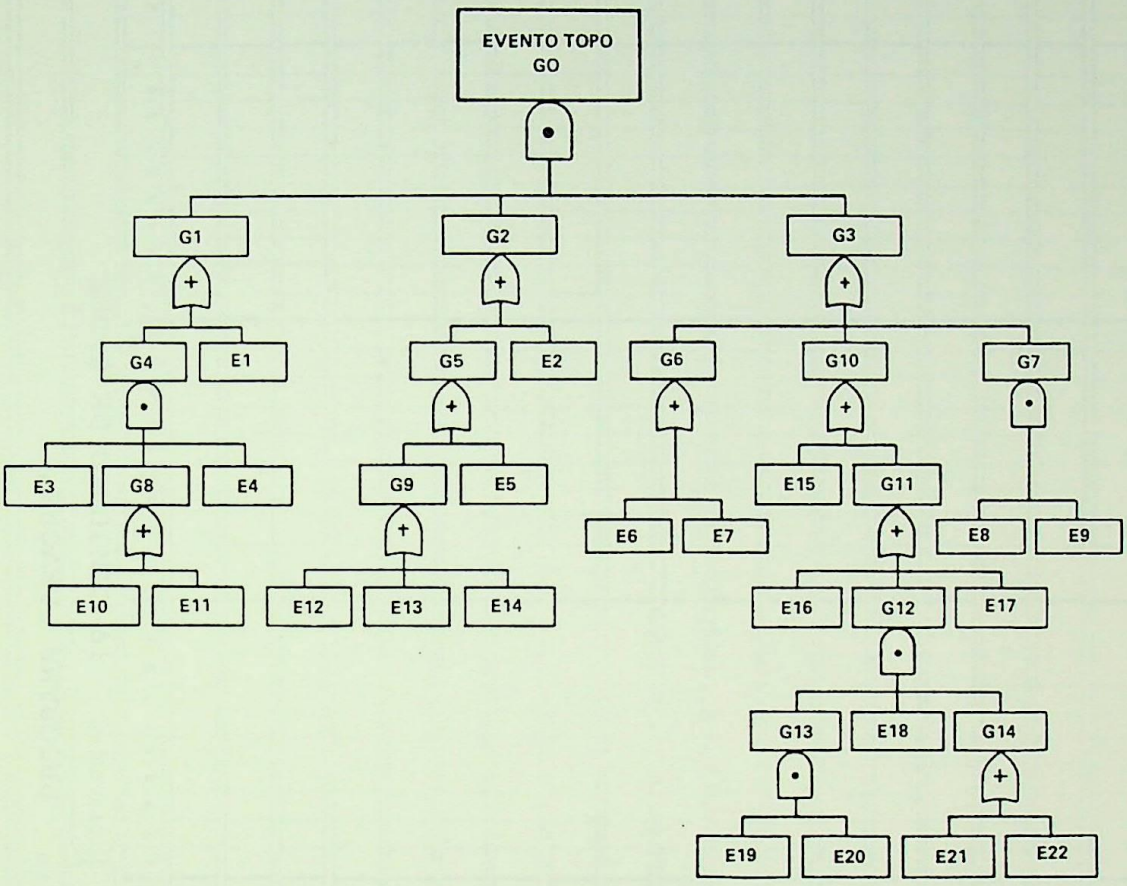


FIGURA 1 - Árvore de Falhas-Exemplo

A seguir, indica-se os dois conjuntos de entrada de dados.

FÔLHA DE CODIFICAÇÃO

DATA / /
PÁGINA 01 DE 01
PROGRAMADOR: _ Nº _

PROGRAMA "DEDARVO3"
APLICAÇÃO PROGRAMA "ARVORE"
IDENTIFICAÇÃO
OBSERVAÇÕES
DESCRIÇÃO 1º CONJUNTO DE DADOS
SIGLA PÁG FÔL.

```
ATOPO  . G G1    G G2    G G3
G10    + E E15   G G11
G13    . E E19   E E20
G5     + G G9    E E5
G2     + E E2    G G5
G11    + E E16   G G12   E E17
G6     + E E6    E E7
G3     + G G10   G G6    G G7
G12    . G G13   E E18   G G14
G7     . E E8    E E9
G1     + G G4    E E1
G14    + E E21   E E22
G9     + E E14   E E12   E E13
G8     + E E11   E E10
G4     . E E3    G G8    E E4
```

-200-

E-9813358

FÔLHA DE CODIFICAÇÃO

DATA / /
PÁGINA 01 DE 02
PROGRAMADOR _ Nº _

PROGRAMA "DEDARVO4"
APLICAÇÃO PROGRAMA "ARVORE"
IDENTIFICAÇÃO
OBSERVAÇÕES
DESCRIÇÃO 2º CONJUNTO DE DADOS
SIGLA PÁG FÔL.

```
E1  .0300D-03  12.
E2  .2520D-04  30.
E3  .1560D-05  06.
E4  .6200D-02  08.
E5  .3400D-03  22.
E6  .0810D-04  18.
E7  .2500D-03  18.
E8  .0303D-03  12.
E9  .3000D-02  30.
E10 .1500D-02  30.
E11 .4000D-03  06.
E12 .4500D-03  12.
E13 .3000D-03  08.
E14 .2500D-02  08.
E15 .1200D-02  22.
E16 .1100D-02  06.
E17 .2000D-03  30.
E18 .5000D-04  06.
E19 .0200D-03  18.
E20 .0300D-02  12.
```


E-9813355

FÔLHA DE CODIFICAÇÃO

DATA / /
PÁGINA 02 DE 02
PROGRAMADOR — Nº —

PROGRAMA "DEDARVO4"
APLICAÇÃO PROGRAMA "ARVORE"
IDENTIFICAÇÃO
OBSERVAÇÕES
DESCRIÇÃO 2º CONJUNTO DE DADOS
SIGLA | PÁG | FÔL.

```
E21     .0200D-02   18.
E22     .2500D-03   08.
```


E-9813355

SAÍDA

Nas páginas seguintes encontra-se a saída com a probabilidade de ocorrência do evento topo escolhido e a expressão utilizada neste cálculo.

****
* ENTRADA DE DADOS E COMENTARIOS *
****

PORTAD	O	C	RELAC	C	RELAC	C	RELAC	C	RELAC	C	RELAC	C	RELAC	C	RELAC
ATOPO	.	G	G1	G	G2	G	G3								
G10	+	E	E15	G	G11										
G13	.	E	E19	E	E20										
G5	+	G	G9	E	E5										
G2	+	E	E2	G	G5										
G11	+	E	E16	G	G12	E	E17								
G6	+	E	E6	E	E7										
G3	+	G	G10	G	G6	G	G7								
G12	.	G	G13	E	E18	G	G14								
G7	.	E	E8	E	E9										
G1	+	G	G4	E	E1										
G14	+	E	E21	E	E22										
G9	+	E	E14	E	E12	E	E13								
G8	+	E	E11	E	E10										
G4	.	E	E3	G	G8	E	E4								

EVENTO	LAMBDA	TEMPO
E1	0.3000D-04	12.000
E10	0.1500D-02	30.000
E11	0.4000D-03	6.000
E12	0.4500D-03	12.000
E13	0.3000D-03	8.000
E14	0.2500D-02	8.000
E15	0.1200D-02	22.000
E16	0.1100D-02	6.000
E17	0.2000D-03	30.000
E18	0.5000D-04	6.000
E19	0.2000D-04	18.000
E2	0.2520D-04	30.000
E20	0.3000D-03	12.000
E21	0.2000D-03	18.000
E22	0.2500D-03	8.000
E3	0.1560D-05	6.000
E4	0.6200D-02	8.000
E5	0.3400D-03	22.000
E6	0.8100D-05	18.000
E7	0.2500D-03	18.000
E8	0.3000D-04	12.000
E9	0.3000D-02	30.000

EVENTO	PROBABILIDADE
E1	0.6000D-05
E15	0.4399D-03
E16	0.1100D-03
E17	0.1000D-03
E18	0.5000D-05
E19	0.6000D-05
E11	0.4000D-04
E10	0.7497D-03
E14	0.3333D-03
E12	0.9000D-04
E13	0.4000D-04
E20	0.6000D-04
E21	0.6000D-04
E22	0.3333D-04
E2	0.1260D-04
E3	0.1560D-06
E4	0.8263D-03
E5	0.1247D-03
E6	0.2430D-05
E7	0.7500D-04
E8	0.6000D-05
E9	0.1499D-02

****
* EXPRESSAO RESULTANTE DA ARVORE ATRAVES DO *
* CALCULO DAS PROBABILIDADES DOS EVENTOS *
* INTERMEDIARIOS *
****

(((((E11+E10).E3.E4)+E1).(((E14+E12+E13)+E5)+E2).(((((E19.E20).(E21+E22).E18)+E16+E17)+E15)+(E6+E7)+(E8.E9)))

A PROBABILIDADE DE OCORRENCIA DO EVENTO TOPO E

0.26206947596941D-11

APÊNDICE B

REQUISITOS USUAIS DE CONFIABILIDADE PARA HOMOLOGAÇÃO DE AERONAVES CIVIS

Conforme já foi mencionado, o método das Árvores de Falhas pode ser aplicado em Análise e Prevenção de Riscos. Toda vez que um evento ou conjunto de eventos possa criar uma situação de risco iminente, é interessante quantificar a situação identificada, comparando-a com requisitos existentes, que possam ajudar no estabelecimento de medidas a adotar.

Na indústria aeronáutica, por exemplo, os riscos são caracterizados de acordo com seus efeitos.

Requisitos de segurança para sistemas aeronáuticos modernos são encontrados nos principais códigos de aeronavegabilidade. Os principais são o JAR-25 (Joint Airworthiness Authorities Steering Commitee by the Civil Aviation Authority - 19 th December 1979), elaborado em conjunto por vários países da Europa, e o FAR-25 elaborado pelos Estados Unidos através da Federal Aviation Regulations. Esses documentos são muito semelhantes e baseados nos mesmos conceitos, relacionando efeitos e ocorrências [22].

Efeitos são os resultados tais como acidentes, incidentes, ou deficiências menores. Ocorrências são causas iniciais como por exemplo falhas de componentes, separadamente ou em combinação, erros humanos, e circunstâncias externas.

É preciso considerar a interação dos componentes dentro do sistema e entre um sistema e outro.

O JAR-25 trata os sistemas como um todo. Pede que

o grau de Severidade do Efeito de todas as ocorrências concebíveis seja considerado.

A intenção final é que os efeitos do tipo catastrófico não devam virtualmente ocorrer durante a vida da frota de aeronaves. Onde os efeitos são menos perigosos, permite-se sua ocorrência mais frequente. O objetivo geral é que a probabilidade de aceitável de um efeito seja inversamente proporcional a sua severidade.

A tabela B.1, a seguir resume a estrutura completa dos requisitos do JAR-25.

Deve ser observado que Acidente Catastrófico não é exatamente o mesmo que Acidente Fatal. Este cobre acidentes em que ao menos uma pessoa venha a morrer.

UmaCatástrofe é um acidente de múltipla fatalidade . É verdade que a definição também inclui perda da aeronave, que pode algumas vezes ser não-fatal, mas na prática usualmente envolve fatalidades.

O Efeito Perigoso deve cobrir sérios incidentes em que o risco de catástrofe é potencialmente alto e também acidentes em que um pequeno número de pessoas possam ser seriamente prejudicadas ou, excepcionalmente, mortas.

O Efeito Maior deve cobrir incidentes em que a tripulação deve continuar o vôo para haver um pouso seguro, apesar das dificuldades em realizá-lo.

Um Efeito Menor é aquele em que a aeronavegabilidade e/ou a carga de trabalho é grandemente afetada. Algum desses pode ser registrado em relatórios de ocorrência.

Para cada categoria de Efeito, a linha central da tabela dá indicações da frequência aceitável de cada efeito. O

fato de tabela cotar probabilidades numéricas não significa que o estabelecimento da segurança deva estar sujeito a uma cotação numérica. Isto depende da simplicidade ou complexidade de um sistema particular.

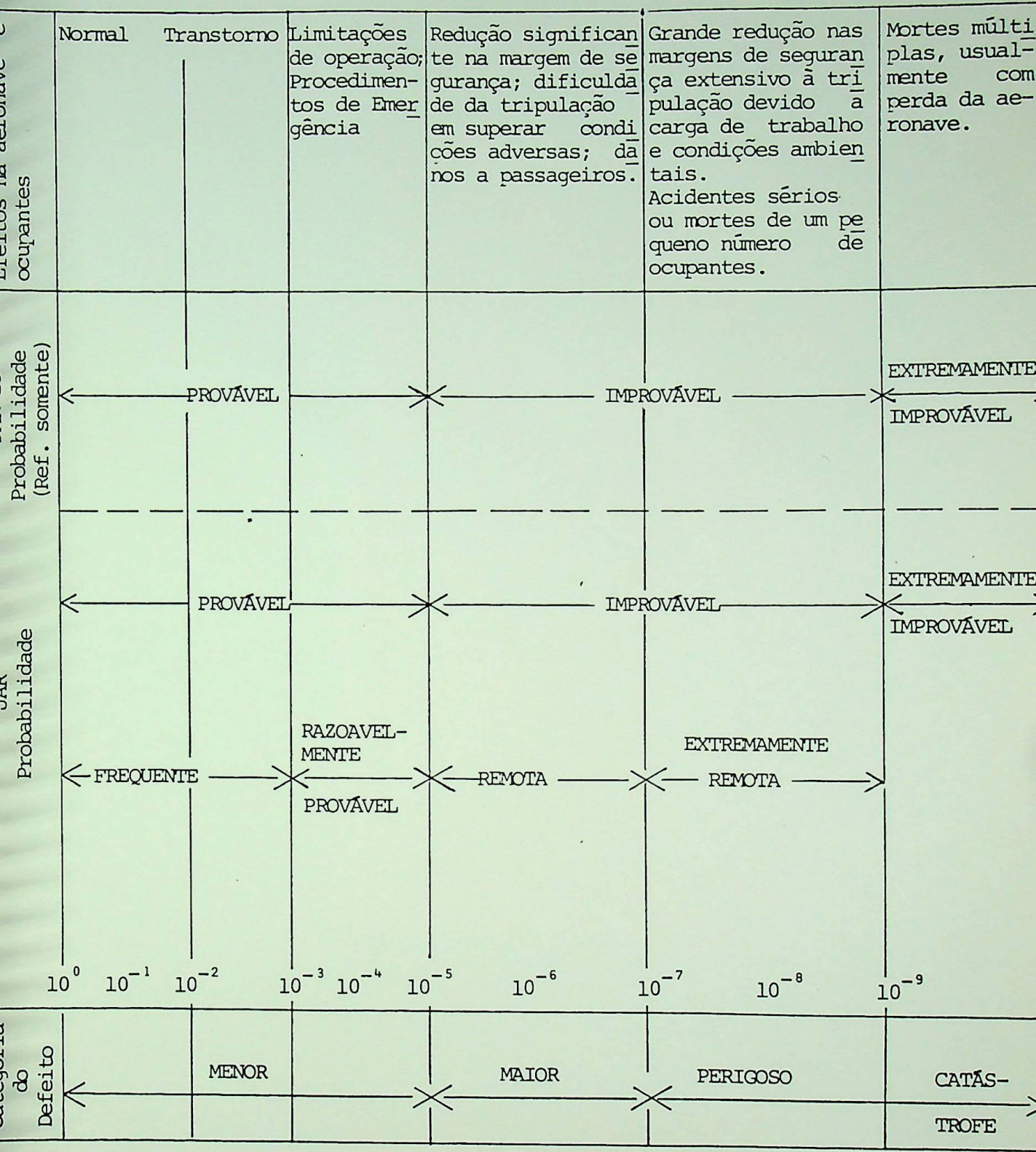


TABELA B.1 - Relacionamento entre probabilidade e severidade de Efeitos.

DATA 31 / 08 / 1987
PROC.
PED. PPG
LIV.
NCr$ DOAÇÃO

621.311.1.004.15(043.2)
B732a
T.477
EFEI / Biblioteca Mauá

Borges, Edméia P. de Oliveira
Análise de confiabilidade em sistemas complexos de alta segurança.

	Nº. Registro	Data Devolu
	Rio - Carlos	26-

EFEI

BIBLIOTECA MAUÁ

Esta publicação deverá ser devolvida dentro do prazo estipulado.

O leitor é responsável pela publicação em seu poder.

EFEI - BIBLIOTECA MAUÁ
8200477
NÃO DANIFIQUE ESTA ETIQUETA