UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE ELETROTÉCNICA
ESPECIALIZAÇÃO EM ENGENHARIA DA CONFIABILIDADE

THIAGO OLIVA ARY

MÉTODO SISTEMÁTICO DE IDENTIFICAÇÃO DE COMPONENTES E GRUPOS DE CORTE (CUT SETS) CRÍTICOS EM ÁRVORES DE FALHA

MONOGRAFIA DE ESPECIALIZAÇÃO

CURITIBA
2018

THIAGO OLIVA ARY

MÉTODO SISTEMÁTICO DE IDENTIFICAÇÃO DE COMPONENTES E GRUPOS DE CORTE (CUT SETS) CRÍTICOS EM ÁRVORES DE FALHA

Monografia apresentada como requisito parcial à obtenção do título de Especialista em Engenharia da Confiabilidade, do Departamento Acadêmico de Eletrotécnica, da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. Dr. Emerson Rigoni

CURITIBA

2018

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Campus Curitiba
Diretoria de Pesquisa e Pós-Graduação
Departamento Acadêmico de Eletrotécnica
Especialização em Engenharia da Confiabilidade

TERMO DE APROVAÇÃO

MÉTODO SISTEMÁTICO DE IDENTIFICAÇÃO DE COMPONENTES E GRUPOS DE CORTE (CUT SETS) CRÍTICOS EM ÁRVORES DE FALHA

por

THIAGO OLIVA ARY

Esta monografia foi apresentada em 5 de outubro de 2018, como requisito parcial para obtenção do título de Especialista em Engenharia da Confiabilidade, outorgado pela Universidade Tecnológica Federal do Paraná. O aluno foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

Prof. Emerson Rigoni, Dr. Eng.
Professor Orientador - UTFPR

Prof. Carlos Henrique Mariano Dr.
Membro Titular da Banca - UTFPR

Prof. Marcelo Rodrigues Dr.
Membro Titular da Banca - UTFPR

O Termo de Aprovação assinado encontra-se na Coordenação do Curso.

Dedico este trabalho ao meu mentor profissional, Jaures Cardoso Junior, por me ensinar e por me mostrar, de forma natural, que a transmissão do conhecimento é o caminho de maior valor para o ser humano.

AGRADECIMENTOS

Agradeço ao Alberto Ramos de Albuquerque e José Armando da Silva pelo apoio e incentivo durante o decorrer da pós-graduação.

Agradeço ao meu antigo gestor Sergio Rodrigues Pereira que me ofereceu a oportunidade de explorar o campo de conhecimento da engenharia de confiabilidade.

Agradeço ao meu mentor profissional Jaures Cardoso Junior por me guiar e incentivar o meu crescimento intelectual no campo da confiabilidade e segurança de sistemas. Além disso, por transmitir valores essenciais para um ser humano.

Agradeço à minha família que proveu o necessário para a minha base intelectual, física, emocional e espiritual para uma vida de valor.

Agradeço à minha esposa pela paciência, apoio e incentivo. Sua presença enriquece minha vida.

Agradeço a todos os amigos que me auxiliaram a vencer os obstáculos encontrados durante o caminho.

RESUMO

ARY, Thiago Oliva. **Método sistemático de identificação de componentes e grupos de corte (cut sets) críticos em árvores de falha**. 2018. 135 páginas. Monografia (Especialização em Engenharia da Confiabilidade) - Universidade Tecnológica Federal do Paraná. Curitiba, 2018.

Os projetos de sistemas das áreas aeroespacial, nuclear, bélica, ferroviária, possuem padrões de segurança estabelecidos e aceitos pela indústria e sociedade. Para obter a certificação de entidades reguladoras destes setores, estes padrões devem ser seguidos e, posteriormente, auditados pelos órgãos competentes que verificarão o atendimento dos níveis de segurança.

Tão relevante quanto projetar sistemas seguros é o acompanhamento do desempenho dos níveis de segurança durante a operação. As normas e padrões destas indústrias estabelecem atividades de monitoramento do comportamento dos sistemas durante a vida operacional, visando identificar riscos maiores daqueles certificados e atuar na modificação dos sistemas para devolvê-los ao nível inicial de segurança.

A evolução dos projetos nas indústrias supracitadas revela um aumento na complexidade e na quantidade de componentes que integram um sistema. Tornar-se-ia inviável monitorar todos os componentes de um sistema complexo tendo como objetivo a segurança. O objetivo deste trabalho é apresentar um método sistemático de identificação de componentes e grupos de corte (*cut sets*) críticos em árvores de falha elaboradas durante o projeto, visando o monitoramento contínuo e o gerenciamento dos riscos.

Para executar o método de identificação de componentes e grupos de corte críticos são utilizadas análises de árvore de falha, medidas de importância de componentes/eventos, método de Pareto, análise de dados de vida, cálculo de *mean time between failure* (MTBF) e *mean time between unscheduled removals* (MTBUR).

A aplicação do método para um conjunto de 6 árvores de falha, possuindo um total de 243 eventos, selecionou 14,81% de eventos críticos (os que mais contribuem para o risco da situação indesejada) para serem continuamente monitorados durante a vida operacional.

Palavras-chave: Árvore de Falhas. Componentes e grupos de corte críticos. Monitoramento e gerenciamento de riscos. Taxa de falha.

ABSTRACT

ARY, Thiago Oliva. **Systematic method of identification of fault tree critical components and cut sets**. 2018. 135 pages. Monografia (Especialização em Engenharia da Confiabilidade) - Universidade Tecnológica Federal do Paraná. Curitiba, 2018.

Systems design is guided by safety standards, which are established and accepted by society. In order to achieve an industry certification, these standards must be followed and, lately, audited by specific organizations that will verify if they comply with the safety goals. This is the case of the following industries: nuclear, aerospace, military, rail.

As relevant as design systems with satisfactory safety levels is the monitoring of the safety performance throughout operational life. Industry standards establish safety levels to be monitored along the product life in order to identify risks higher than those of the design certification and to provide necessary system modifications to return it to initial safety levels.

Design evolution reveals that current systems present an increased complexity and a higher number of components. It is not possible to manage the safety levels monitoring every item of a system. This monograph presents a systematic method to identify critical components and cut sets from the fault trees elaborated during the development phase of a system in order to continuously monitor and manage risk.

This method of identification of critical fault tree components and cut sets is executed using analyzes such as fault tree, importance measures of components and events, Pareto concept, life data analysis, MTBF and MTBUR calculation.

The method applied to a set of 6 fault trees, which contain a total of 243 events, selected 14,81% of the most critical events in order to be monitored during the operational life.

Keywords: Fault tree. Critical components and cut sets. Risk monitoring and management. Failure rate.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS, SIGLAS E ACRÔNIMOS

LISTA DE ABREVIATURAS

Bi	Birnbaum's Importance Measure
STD	Standard
MIL	Military

LISTA DE SIGLAS

AC	Advisory Circular
ARP	Aerospace Recommended Practice
BM	Birnbaum's Importance Measure
CDF	Cumulative Density Function
EB	Evento Básico
FAR	Federal Aviation Regulation
FHA	Functional Hazard Assessment
FMEA	Failure Mode and Effects Analysis
FV	Fussel-Vesely
LDA	Life Data Analysis
MLE	Maximum Likelihood Estimator
MTBF	Mean Time Between Failure
MTBUR	Mean Time Between Unscheduled Removal
MTTF	Mean Time to Failure
PDF	Probability Density Function
RAMS	Reliability, Availability, Maintainability and Safety
RAW	Risk Achievement Worth
RII	Risk Increase Importance
RRI	Risk Reduction Importance
RRW	Risk Reduction Worth
SIL	Safety Integrity Level

LISTA DE ACRÔNIMOS

ATA	Air Transport Association of America
FAA	Federal Aviation Administration
IEC	International Electrotechnical Commission
NASA	National Aeronautics and Space Administration
NUREG	US Nuclear Regulatory Commission Regulation
SAE	Society of Automotive Engineering

LISTA DE SÍMBOLOS

t – parâmetro de tempo da distribuição exponencial

λ – parâmetro de taxa de falha da distribuição exponencial

x – variável aleatória contínua

f(x) – função densidade de probabilidade

F(x) – função de probabilidade de falha acumulada ou função de não confiabilidade

R(x) ou R(t) – função de probabilidade de sucesso acumulada ou função confiabilidade

λ(t) – função taxa de falha ou *hazard rate*

β – parâmetro de forma ou inclinação da distribuição Weibull

η – parâmetro de escala ou também chamado de vida característica da distribuição Weibull (representa a chance de que 63,2% dos componentes falhem)

T(t) – tempo total de operação de um componente (equação 16 de MTBF)

r – número de falhas do componente (equação 16 de MTBF)

n – número de falhas do componente (equação 17 de MTBF)

m – número de horas de teste (equação 17 de MTBF)

FV – medida de importância de Fussel-Vesely

F(i) – é o risco apenas daqueles conjuntos de corte que contêm o evento xi

F(x) – é o risco total de todos os conjuntos de corte

F(0) – é o risco total com a probabilidade x_i do evento básico definida como zero “0”

∂/∂x – é a primeira derivada da expressão de risco em relação ao evento básico de interesse (x_i)

SUMÁRIO

1 INTRODUÇÃO

Alguns campos da engenharia requerem níveis adequados e aceitáveis de segurança, como é o caso de sistemas das áreas aeroespacial, nuclear, química, bélica e ferroviária. Para estes setores da indústria, um dos pilares do projeto de sistemas é o atingimento e a comprovação dos níveis de segurança definidos pelos requisitos de certificação e/ou normas específicas.

Para a norma IEC 61508, define-se a existência de dois tipos de certificação:

1. Uma organização pode demonstrar a capacidade genérica para produzir um produto ou sistema (ou seja, mostra que possui os procedimentos e competências necessárias).
2. Um produto ou projeto de sistema específico atende aos requisitos descritos no conteúdo das normas aplicáveis (ou seja, mostra-se que os procedimentos foram implementados).

Estes dois tipos de processos caminham juntos. É preciso que seja evidenciado tanto a capacidade de uma organização elaborar as análises requeridas, quanto a demonstração de atingimento dos níveis de segurança aplicáveis. Com isso, garante-se o cumprimento com os requisitos estipulados pelas normas e legislações, atendendo o anseio da sociedade por produtos e sistemas cada vez mais seguros.

Para a fase de projeto de um sistema, existem normas que padronizam as análises de segurança. Exemplos:

- IEC *International Standard* 61508 (2010): *functional safety of electrical/electronic/programmable electronic safety-related systems*
- IEC *International Standard* 61511: *functional safety – safety instrumented systems for the process industry sector*
- *European Standard* EN 50126: *railway applications – the specification and demonstration of dependability, reliability, maintainability and safety* (RAMS)

- UK *Defense Standard* 00-56 (Issue 3.0): *safety management requirements for defense systems*
- MIL-STD-882 *System Safety*
- ARP 4761 *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Aircraft, Systems, and Equipment*

O trabalho de garantir a segurança de um sistema não se dá apenas na fase de desenvolvimento. Continua durante toda a vida operacional. Assim como existem normas que direcionam as análises durante a concepção de um sistema, há métodos e ferramentas para executar um processo contínuo de avaliação dos níveis de segurança. A norma ARP 5150 - *Safety Assessment of Transport Airplanes in Commercial Service*, por exemplo, oferece um processo sistemático para medir e monitorar a segurança, visando a definição de prioridades e foco dos recursos disponíveis em áreas que proveem o maior potencial para o aumento das margens de segurança na aviação. O documento menciona que a gestão contínua da segurança é uma atividade dedicada a garantir que o risco seja identificado e devidamente eliminado ou controlado. Outra norma, já no campo militar, que versa sobre a gestão dos riscos é a MIL-STD-882E - *System Safety*. Esta fornece um método padrão e genérico para a identificação, classificação e mitigação de riscos e pode ser aplicada para o tratamento de perigos que se aplicam a sistemas / produtos / equipamentos / infraestrutura (incluindo *hardware* e *software*) durante todo o projeto, desenvolvimento, teste, produção, uso e descarte.

Neste cenário de acompanhamento dos níveis de segurança de um produto, existem barreiras que dificultam a execução das análises. A informação do desempenho dos sistemas em campo talvez seja a maior delas. Toda análise de risco quantitativa depende de dados de falha de componentes ou quantidade de eventos para ser executada. No caso de análises de risco elaboradas a partir da ocorrência de um evento ou falha específica, a falta de informação de dados de falha seria o maior entrave. Por outro lado, o acompanhamento sistemático e periódico das taxas de falha de componentes esbarra na limitação de recursos das empresas e na dificuldade de obtenção dos eventos dada a grande quantidade de itens dos sistemas atuais que aumenta sensivelmente o esforço da coleta de informações.

Este trabalho tem o foco na parte de acompanhamento sistemático dos níveis de segurança do produto. Para isso, será proposto um método para identificar

componentes e grupos de corte (*cut sets*) específicos, que sejam mais relevantes em relação ao impacto para a segurança do sistema em estudo. Dessa forma, com um número reduzido de componentes monitorados, pode-se viabilizar a avaliação sistemática e periódica dos riscos de um sistema.

Dentre os vários tipos de análises aplicadas durante o desenvolvimento de sistemas, uma das mais difundidas e utilizadas é a análise de árvore de falhas. No caso da aviação, este método é utilizado após a execução de avaliações funcionais que resumidamente, definem as funções dos sistemas, determinam as condições de falha (maneiras que uma função pode falhar) e classificam a severidade de cada condição de falha baseado em critérios estabelecidos por normas. Para cada condição classificada como catastrófica (que leva a perdas materiais e de vidas), uma árvore de falha deve ser elaborada para avaliar qualitativa e quantitativamente o evento indesejado. Os grupos de corte são identificados após a aplicação de simplificações booleanas e representam as combinações mínimas para que ocorra o evento topo. Todas estas análises são realizadas para se construir um sistema robusto e aderente às demandas normativas.

O método apresentado nesta monografia tem como objetivo criar as bases para realizar avaliações sistemáticas de segurança, tomando crédito dos esforços de engenharia empregados na fase de desenvolvimento de sistemas aeronáuticos. Será focado na identificação dos componentes e grupos de corte das análises de árvore de falhas elaboradas durante o projeto de sistemas de uma aeronave para falhas classificadas como catastróficas.

1.1 FORMULAÇÃO DO PROBLEMA

Um dos maiores desafios no monitoramento contínuo da segurança de sistemas é a coleta de dados de falha. Sem esta informação não é possível elaborar análises de vida dos componentes. O cálculo quantitativo do risco depende das informações de vida. Somado a isso, existe a limitação de recursos de uma organização para monitorar e obter dados de grande quantidade de componentes que compõem os sistemas atuais.

Por um lado, as análises de risco podem ser elaboradas conforme as falhas acontecem. Para esta situação, coletam-se as informações sob demanda e executa-

se a avaliação do caso em questão. Outra maneira de realizar o monitoramento da segurança é através do conhecimento de quais itens devem ser monitorados, realizando-se a coleta e análise sistemática e repetitiva das taxas de falha dos componentes.

Um avião, por exemplo, pode conter mais de uma dezena de sistemas críticos. Para cada um deles, há condições de falha que possuem severidade catastrófica, isto é, podem levar a um acidente: perda material e de vidas. Cada uma das condições de falha catastróficas, em um projeto aeronáutico, é estudada utilizando-se, por exemplo, a análise de árvore de falhas.

O método de árvore de falhas modela as relações lógicas dos modos de falha dos componentes do sistema que podem levar à ocorrência da condição de falha indesejada. Cada árvore de falha pode conter dezenas de componentes. Com isso, assumindo-se dez sistemas críticos, cada um contendo uma média de cinco condições de falha catastróficas e, considerando que para cada condição de falha existe uma árvore de falha composta por vinte componentes, o resultado seria de mil componentes a serem monitorados (assumindo-se que não há repetição de componentes nas árvores de falha).

O esforço necessário para coletar e analisar os dados de falha para esta quantidade de componentes, somado à revisão dos cálculos das árvores de falha, tornaria inviável um processo sistemático e repetitivo de acompanhamento dos níveis de segurança durante a operação de um modelo de aeronave. Como selecionar uma quantidade reduzida de componentes mais relevantes para a segurança, visando a criação de um processo sistemático e repetitivo de acompanhamento das taxas de falha destes itens para manter os níveis adequados de segurança durante a operação de uma aeronave?

1.2 OBJETIVOS

1.2.1 Objetivo Geral

Elaborar um método de identificação de componentes e grupos de corte críticos em árvores de falha elaboradas durante o projeto de uma aeronave, a fim de tornar possível a implementação de um monitoramento contínuo da segurança e de um gerenciamento sistemático e repetitivo dos riscos.

1.2.2 Objetivos Específicos

Este trabalho deve atender os seguintes objetivos específicos para cumprimento de seu objetivo geral:

- Aplicar o conceito de medida de importância e Pareto para selecionar uma quantidade reduzida de componentes mais relevantes para a segurança do sistema.
- Identificar os grupos de corte mais significativos para a ocorrência do evento topo, a partir da combinação dos componentes mais relevantes, selecionados a partir do método do item anterior.
- Calcular a porcentagem de componentes mais relevantes selecionados para uma árvore de falha.
- Calcular a porcentagem do total de componentes escolhidos das árvores de falha selecionadas em relação ao total de componentes que compõem todas as árvores de falha em estudo.
- Estabelecer os critérios de probabilidade para a elaboração de uma análise de risco.
- Exemplificar a utilização de dados de campo reais e fictícios de componentes selecionados para a realização do monitoramento dos grupos de corte.
- Executar uma análise de risco com as informações de dados de campo mistos (reais e fictícios) de componentes.

1.3 JUSTIFICATIVA

Durante o desenvolvimento do projeto de sistemas, análises são conduzidas, cada indústria respeitando as respectivas regulamentações, para atender os padrões estabelecidos. Muitas horas de engenharia são destinadas a estas atividades. No caso específico da aviação, seguem-se normas como a ARP 4761 - *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Aircraft, Systems, and Equipment*. Conforme mencionado na formulação do problema, a quantidade total de componentes que compõem as análises de árvore de falha pode ultrapassar, facilmente, dez centenas. Se, por um lado, o monitoramento deste montante de itens esbarra na limitação de recursos, por outro lado, pode-se tomar crédito das análises já elaboradas para identificar elementos relevantes e combinações de falha mais significativas, tornando possível a realização de avaliações sistemáticas dos níveis de segurança.

O método de análise de árvores de falha permite modelar as relações lógicas existentes entre os modos de falha dos componentes de um sistema para entender como pode ocorrer a condição de falha indesejada. O resultado da análise pode entregar um entendimento tanto qualitativo quanto quantitativo do evento em estudo. Os grupos de corte (*cut sets*) mostram as combinações mínimas de falhas de componentes que podem levar à ocorrência do evento topo. É possível, por meio desta informação, avaliar as redundâncias, levantar requisitos de independência, entender as fragilidades e compreender como possíveis modificações podem melhorar a robustez do sistema. Na dimensão quantitativa, obtêm-se o valor de probabilidade de falha do evento topo, a probabilidade de falha de cada grupo de corte, exercita-se o intervalo de manutenção de componentes com falhas latentes para mensurar o impacto no evento topo, experimenta-se trocar componentes com taxas de falha distintas e incluir redundâncias, a fim de melhorar o valor da probabilidade do evento topo.

O intuito deste trabalho é utilizar estas informações que são resultado de análises elaboradas durante o desenvolvimento de sistemas aeronáuticos e aplicar métodos como as medidas de importância e o conceito de Pareto para selecionar os componentes e os grupos de corte mais significativos para o monitoramento contínuo. A partir deste ponto, utilizam-se métodos de quantificação de vida e os critérios de segurança para quantificar o risco.

1.4 ESTRUTURA DO TRABALHO

O trabalho está dividido em 5 capítulos:

- O Capítulo 1 é composto por apresentação sucinta do tema, formulação do problema, a justificativa da proposição do método de identificação de componentes e grupos de corte críticos e os objetivos gerais e específicos.
- O Capítulo 2 contém as informações que delimitam o tema da pesquisa. Apresenta os objetivos de segurança no projeto de sistemas e risco segundo a norma IEC 61508, explica sucintamente como funciona a regulamentação aeronáutica para o requisito §25.1309, a análise funcional para sistemas e a análise de árvore de falhas, aborda a avaliação de segurança durante a operação de acordo com a ARP 5150, a análise de risco segundo a norma MIL-STD-882E e explica o método de identificação de componentes e grupos de corte críticos em árvores de falha.
- O Capítulo 3 apresenta o referencial teórico e engloba as descrições sobre análise de dados de vida, método de cálculo da métrica MTBF (*Mean Time Between Failures*), método de cálculo da métrica MTBUR (*Mean Time Between Unscheduled Removals*), comparação entre MTTF, MTBF e MTBUR e as medidas de importância Fussell-Vesely (FV), *Risk Reduction Importance* ou *Risk Reduction Worth* (RRW), *Risk Increase Importance* ou *Risk Achievement Worth* (RAW) e Birnbaum's *Importance Measure* (Bi ou BM).
- O Capítulo 4 traz a aplicação do referencial teórico a um conjunto de árvores de falha de um modelo de aeronave. Executa o método em detalhes para uma das seis árvores de falha e apresenta os resultados das análises das medidas de importância para as outras cinco árvores de falha.
- O Capítulo 5 apresenta os resultados obtidos, as dificuldades encontradas e as soluções propostas.

2 TEMA DA PESQUISA

O método proposto neste trabalho será aplicado às árvores de falha de sistemas de um modelo de aeronave. Pretende-se com isso sistematizar o processo de seleção dos componentes mais relevantes para a segurança e a definição dos grupos de corte mais significativos a partir dos componentes selecionados. O tipo de aeronave e o fabricante serão mantidos em sigilo para preservar a fonte das informações.

O *software* utilizado para analisar os grupos de corte e para aplicar as medidas de importância às árvores de falha é o CAFTA.

Neste capítulo serão abordados os seguintes tópicos:

- Objetivos de segurança no projeto de sistemas e risco segundo a IEC 61508.
- Regulamentação da indústria aeronáutica.
- Análise funcional.
- Análise de árvore de falhas.
- Avaliação da segurança durante a operação.
- Análise de risco segundo a norma MIL-STD-882E.
- Método de identificação de componentes e grupos de corte críticos em árvores de falha.

2.1 OBJETIVOS DE SEGURANÇA NO PROJETO DE SISTEMAS E RISCO SEGUNDO A NORMA IEC 61508

Segundo os autores Smith e Simpson (2010) não há risco zero. Isso ocorre porque nenhum item físico tem taxa de falha zero, nenhum ser humano é infalível e nenhum projeto de software pode prever todas as possibilidades operacionais. No entanto, a percepção pública de risco, particularmente após um acidente grave, muitas vezes, volta a clamar pelo ideal de risco zero. Em geral, a maioria das pessoas entende que isso não é praticável, portanto o conceito de definir e aceitar um risco tolerável para qualquer atividade particular prevalece.

De acordo com Smith e Simpson (2010), o grau real de risco considerado tolerável variará de acordo com uma série de fatores como o grau de controle que se tem sobre as circunstâncias, o caráter voluntário ou involuntário do risco, o número de pessoas em risco em qualquer incidente e, assim por diante. Ainda segundo estes autores, explica-se que a tecnologia de segurança cresceu em torno da necessidade de estabelecer níveis de risco e de avaliar se os projetos propostos atendem a esses objetivos, sejam eles instalações fabris, sistemas de transporte, equipamentos médicos ou qualquer outro aplicativo.

No início da década de 1970, os funcionários das fábricas perceberam que com plantas maiores envolvendo grandes estoques de material perigoso a prática de aprender por erros já não era aceitável. Métodos foram desenvolvidos para identificar perigos e para quantificar as consequências das falhas. Eles evoluíram em grande parte para auxiliar no processo de tomada de decisão ao desenvolver ou modificar uma planta fabril. Pressões externas para identificar e quantificar o risco vieram mais tarde. Em meados da década de 1970, já havia a preocupação com a falta de controles formais para regular as atividades que poderiam levar a incidentes de grande impacto na saúde e segurança do público em geral (SMITH e SIMPSON, 2010).

As técnicas para quantificar o valor da frequência de falhas são as mesmas que as aplicadas anteriormente para a disponibilidade da planta, onde o custo da falha do equipamento era a principal preocupação. A tendência, nos últimos anos, tem sido a aplicação mais rigorosa dessas técnicas, juntamente com a verificação de terceiros, no campo da avaliação de perigos. Eles incluem análise de árvore de falhas (*fault tree analysis*), modo de falha e análise de efeito (*failure mode and effect analysis*), análise de falha de causa comum e, assim por diante (SMITH e SIMPSON, 2010).

A proliferação de software durante a década de 1980, em particular em sistemas de controle e segurança em tempo real, focou a atenção na necessidade de abordar falhas sistemáticas, uma vez que não podem ser quantificadas. Em outras palavras, enquanto as taxas de falha de *hardware* eram vistas como uma medida de confiabilidade previsível, os erros de *software* eram entendidos como não previsíveis. A partir deste momento, houve ampla aceitação de que era necessário considerar defesas qualitativas contra falhas sistemáticas. Isso deveria ser feito

como uma atividade adicional e separada do que já era comumente realizado: o cálculo da probabilidade de falhas de *hardware* (SMITH e SIMPSON, 2010).

Uma questão que surge, frequentemente, nas análises de sistemas é sobre o que deve ser classificado como equipamento relacionado à segurança. O termo "relacionado à segurança" (*safety-related*), segundo a IEC 61508, aplica-se a qualquer sistema com arquitetura descentralizada ou centralizada (com componentes programáveis) em que uma falha, isolada ou em combinação com outras falhas e erros, possa levar à morte, danos materiais e / ou ambientais. Os termos "relacionados à segurança" e "crítico para a segurança" (*safety-critical*) são frequentemente utilizados. A expressão "crítico para segurança" tende a ser usada onde somente uma única falha de um equipamento em questão, leva a uma fatalidade ou aumenta o risco para as pessoas expostas. O termo "relacionado à segurança" tem um contexto mais amplo, na medida em que inclui equipamentos para os quais uma única falha não é necessariamente crítica, somente quando esta se combina com a falha de algum outro item, levando a consequências perigosas.

Um equipamento ou software não pode ser excluído desta categoria - “relacionado à segurança” - apenas por identificar que existem meios alternativos de proteção. Isto seria pré-julgar o problema. Uma avaliação formal da integridade de segurança ainda seria necessária para determinar se o grau geral de proteção do equipamento ou software sob estudo é adequado (SMITH e SIMPSON, 2010).

2.1.1 Objetivos Qualitativos e Quantitativos de Segurança

Segundo Smith e Simpson (2010), observam-se as seguintes definições:

- Objetivo qualitativo: Aquele que busca minimizar a ocorrência de falhas sistemáticas (por exemplo, erros de software), aplicando uma variedade de defesas e disciplinas de projeto adequadas à gravidade do objetivo de risco tolerável.
- Objetivo quantitativo: Aquele que se ocupa em prever a frequência de falhas de hardware, comparando-a com algum objetivo de risco tolerável. Se o objetivo não for satisfeito, o projeto deve ser adaptado (por exemplo, incluindo redundâncias) até o atingimento da meta.

É importante entender porque é necessária essa dupla abordagem. Antes da década de 1980, as falhas de sistema geralmente poderiam ser identificadas como falhas de componentes específicos (por exemplo, falha de um relé, capacitor ou de um motor). No entanto, desde então, o crescimento da complexidade (incluindo o software) levou a falhas de sistema que possuem uma natureza mais sutil, cuja causa de um evento catastrófico, por exemplo, pode não ser atribuída à uma falha em componentes isolados (SMITH e SIMPSON, 2010).

Outras definições segundo Smith e Simpson (2010):

- Falhas aleatórias de hardware: São aquelas ligadas às falhas de componentes específicos e às quais atribui-se taxas de falha. O conceito de repetitividade permite modelar os sistemas propostos por meio da associação estatística de taxas de falhas de componentes similares em conjunto para prever o desempenho do projeto em questão.
- Falhas sistemáticas: Aquelas que não são atribuídas às falhas ou erros específicos e, portanto, são exclusivas de um determinado sistema e seu ambiente. Incluem problemas de tolerância de projeto e desempenho relacionado ao tempo de funcionamento, falhas relacionadas à modificações inadequadamente avaliadas e, claro, software. As taxas de falha não podem ser atribuídas a esses incidentes, uma vez que não permitem prever o desempenho de projetos futuros.

O conceito de níveis de integridade de segurança, conhecidos como SIL (*Safety Integrity Level*), é usado na maioria dos documentos de orientação na área de segurança nos ramos industriais, ferroviário, automotivo, nuclear e maquinário. O conceito é dividir o "espectro" da integridade em quatro níveis discretos e, depois estabelecer requisitos para cada nível. Quanto maior o SIL, então mais rigorosos se tornam os requisitos. Na norma IEC 61508 (e na maioria dos outros documentos), os quatro níveis são definidos como no Quadro 2.1.

Quadro 2.1 - *Safety Integrity Level – IEC 61508*

SIL	Alta taxa de demanda (Falhas/hora)	Baixa taxa de demanda (Probabilidade de falha quando há demanda)
4	$\geq 10^{-9}$ to $< 10^{-8}$	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-8}$ to $< 10^{-7}$	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-7}$ to $< 10^{-6}$	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-6}$ to $< 10^{-5}$	$\geq 10^{-2}$ to $< 10^{-1}$

Fonte: norma IEC 61508

Segundo Smith e Simpson (2010), as faixas dos níveis de integridade (SIL) para alta demanda e para baixa demanda são parâmetros diferentes. O primeiro é dimensional e o segundo é adimensional. Em função desta diferença, expressa-se o critério de alta demanda em falhas por hora. Se fosse expressa em falhas por ano os limites das faixas seriam os mesmos. A razão de haver duas colunas (alta e baixa demanda) é que existem duas maneiras pelas quais o objetivo de integridade pode ser descrito. A diferença pode ser melhor entendida por meio de exemplos.

Considere a falha do motor de um automóvel. O interesse está na taxa de falha porque a condição perigosa pode ser a consequência imediata da falha do item. Por outro lado, considere o *air bag* de um automóvel. Este é um sistema de proteção de baixa demanda no sentido de que as demandas são infrequentes (anos ou dezenas de anos podem passar sem que seja necessária a sua utilização). A taxa de falha por si só é de pouca utilidade para descrever sua integridade, uma vez que o perigo não incorre imediatamente após à falha e, portanto, deve-se levar em consideração o intervalo de teste. Colocado de outra forma, uma vez que a demanda é pouco frequente, as falhas podem estar dormentes, isto é, presentes durante o intervalo entre testes (SMITH e SIMPSON, 2010).

Uma pergunta, às vezes feita, é se o objetivo quantitativo for cumprido pela probabilidade de falha de *hardware*, então, qual alocação deve haver para as falhas sistemáticas (*software*)? O objetivo deve ser aplicado de forma igual às falhas de hardware aleatórias e às falhas sistemáticas. Em outras palavras, a meta numérica não está dividida entre os dois, mas aplicada às falhas de *hardware*. Existem requisitos como, por exemplo, o nível de rigor das análises de segurança, para cada faixa do critério SIL que devem ser aplicados às falhas sistemáticas (SMITH e SIMPSON, 2010).

2.2 REGULAMENTAÇÃO DA INDÚSTRIA AERONÁUTICA

Para a indústria aeronáutica, um dos documentos que define os objetivos de segurança é a AC (*Advisory Circular*) 25.1309-1. Descreve os meios aceitáveis para demonstrar conformidade com os requisitos de aeronavegabilidade do Regulamento Federal de Aviação §25.1309 da FAA (*Federal Aviation Administration*). A primeira versão da AC 25.1309 data de 1982 e sua tarefa principal é fornecer definições padrão de termos (incluindo classificações de perigo e probabilidade) para uso consistente em toda a estrutura de trabalho para a realização da segurança funcional de um avião. Enquanto os regulamentos (FAR – *Federal Aviation Regulation*) e os padrões (ARP – *Aerospace Recommended Practices*) usam termos como condição de falha e extremamente improvável, a AC 25.1309-1 define seus significados específicos.

O termo “erro” na AC reconhece o papel do erro humano (no desenvolvimento, fabricação, operação ou manutenção) como fonte de falhas do sistema, especialmente em sistemas aviônicos complexos e integrados. O termo “condições de falha” coloca foco nos efeitos de uma falha independente e separada das causas (AC/AMJ 25.1309, 2002).

A AC/AMJ 25.1309 (2002) contém as classificações das condições de falha por severidade (ou gravidade) do efeito. São elas (em inglês): “*Catastrophic*”, “*Hazardous*”, “*Major*”, “*Minor*” e “*No Safety Effect*”. Uma condição “*Catastrophic*” é a que resultaria em mortes múltiplas, geralmente com a perda do avião.

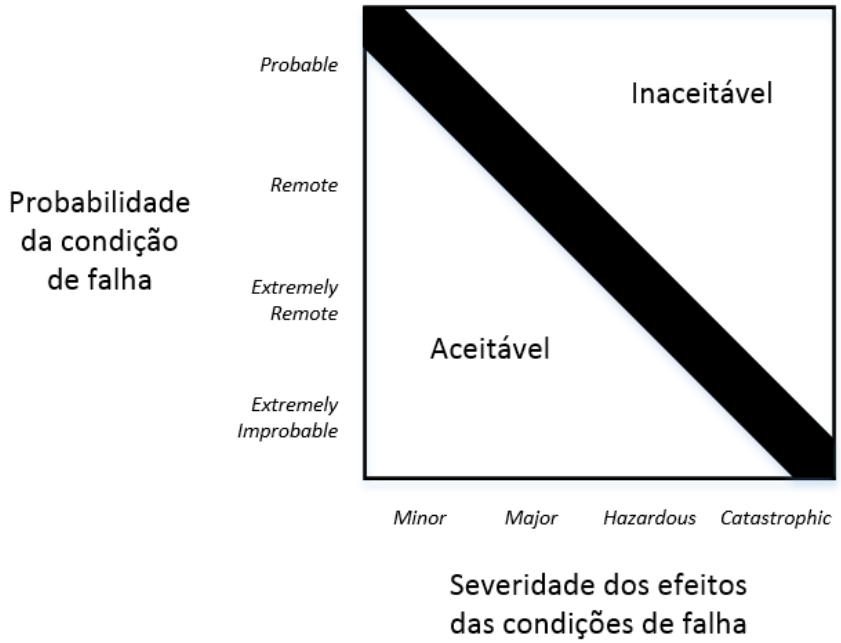
Para cada nível de severidade, são especificadas as faixas de probabilidade. Uma condição de falha “extremamente improvável”, por exemplo, significa: “tão improvável de acontecer que não é esperado que ocorra durante toda a vida operacional de uma frota do mesmo tipo de avião”. A definição quantitativa do termo é: condições de falha extremamente improváveis são aquelas que possuem uma probabilidade média por hora de voo da ordem de $1x10^{-9}$ ou menor. As outras faixas de probabilidade são definidas como segue: “extremamente remota”, “remota” e “provável”. Condições de falha extremamente remotas são aquelas que possuem uma probabilidade média por hora de voo da ordem de $1x10^{-7}$ ou menor, mas maiores que a ordem de $1x10^{-9}$. Condições de falha remotas são aquelas que possuem uma probabilidade média por hora de voo da ordem de $1x10^{-5}$ ou menor, mas maiores que a ordem de $1x10^{-7}$. E, por último, condições de falha prováveis são

aquelas que possuem uma probabilidade média por hora de voo maior que a ordem de grandeza de $1x10^{-5}$ (AC/AMJ 25.1309, 2002).

2.2.1 Objetivos de Segurança Segundo o Requisito §25.1309

Os objetivos visam garantir um nível de segurança aceitável para o equipamento e sistemas instalados no avião. Uma relação inversa, lógica e aceitável deve existir entre a probabilidade média por hora de voo e a gravidade dos efeitos da condição de falha, como mostrado na Figura 2.1:

Figura 2.1 - Relação entre Severidade e Probabilidade – AC/AMJ 25.1309



Fonte: AC/AMJ No: 25.1309 - *Draft ARSENAL revised*. 2002.

O Quadro 2.2 mostra os objetivos de segurança associados às condições de falha:

Quadro 2.2 - Objetivos de segurança Segundo a AC/AMJ No: 25.1309

Classificação das condições de falha	**Sem efeito para segurança**	***Minor***	***Major***	***Hazardous***	***Catastrophic***
Efeitos na aeronave	Nenhum efeito na capacidade operacional ou na segurança	Pequena redução na capacidade funcional ou nas margens de segurança	Redução significativa na capacidade funcional ou nas margens de segurança	Grande redução na capacidade funcional ou nas margens de segurança	Normalmente com perda total da aeronave
Efeitos no ocupantes, excluindo tripulação	Inconveniente	Desconforto físico	Sofrimento físico, possivelmente incluindo lesões	Lesão séria ou fatal a um pequeno número de passageiros ou tripulação da cabine	Múltiplas fatalidades
Efeitos na tripulação	Nenhum efeito para a tripulação	Pequeno aumento da carga de trabalho	Desconforto físico ou significativo aumento da carga de trabalho	Sofrimento físico ou carga de trabalho excessiva que prejudica a habilidade de executar tarefas	Fatalidades ou incapacitação
Probabilidade qualitativa permitida	Não há requisito de probabilidade	Provável	Remota	Extremamente Remota	Extremamente Improvável
Probabilidade quantitativa permitida: probabilidade média por de voo na ordem de:	Não há requisito de probabilidade	$< 10^{-3}$	$< 10^{-5}$	$< 10^{-7}$	$< 10^{-9}$

Fonte: AC/AMJ No: 25.1309 - *Draft ARSENAL revised*. 2002.

Além do Quadro 2.2, os objetivos de segurança para condições de falha catastróficas devem ser satisfeitos demonstrando que:

1. Nenhuma falha simples (ou falha única) resulta em uma condição de falha catastrófica;
2. Cada condição de falha catastrófica deve ser extremamente improvável.

2.3 ANÁLISE FUNCIONAL

Segundo a ARP 4761 (1996), a primeira análise funcional que se aplica a um novo sistema é a chamada Avaliação de Perigos Funcionais (*Functional Hazard Assessment* - FHA). Ela permite identificar e avaliar os perigos potenciais relacionados às funções de um sistema, independente dos detalhes da arquitetura. Pode, também, ser aplicada quando há mudanças relevantes em um sistema. Esta análise é utilizada no processo de desenvolvimento de um sistema para estabelecer os objetivos de segurança para as suas funções, visando a implementação de um projeto seguro.

Os passos principais do método FHA são:

1. Elaborar a lista de funções do sistema;
2. Determinar as condições de falha para cada função do sistema (as condições de falha são definidas pela perda ou mau funcionamento da função);
3. Analisar os efeitos de cada condição de falha;
4. Classificar a condição de falha baseado nos efeitos contidos nos critérios da norma (ex. AC 25.1309-1).

No Quadro 2.3, tem-se um exemplo de sistema, função e condição de falha (passos 1 e 2 do método FHA):

Quadro 2.3 - Exemplo de sistema, função e condição de falha

Sistema	Freios das rodas
Função	Desacelerar as rodas no solo
Condição de falha #1	Perda total e não anunciada da capacidade de desacelerar as rodas no solo
Condição de falha #2	Aplicação inadvertida de todos os freios de roda

Fonte: SAE ARP 4761

O próximo passo (3) do método FHA é analisar os efeitos de cada condição de falha, como pode ser visto no Quadro 2.4:

Quadro 2.4 - Exemplo de definição de efeitos das condições de falha

Condição de falha	Fase de voo	Efeitos da condição de falha na tripulação, passageiros e aeronave
Perda total e não anunciada da capacidade de desacelerar as rodas no solo	Pouso e decolagem abortada	A tripulação detecta a falha quando o freio é operado. Comanda os *spoilers* e utiliza os reversores na máxima potência. Esta situação pode resultar em saída de pista.
Aplicação inadvertida de todos os freios de roda	Decolagem, após velocidade de decisão	A tripulação não conseguirá decolar ou realizar um cancelamento da decolagem de forma segura, resultando em saída de pista com alta velocidade.

Fonte: SAE ARP 4761

No último passo (4) do método FHA, utiliza-se o Quadro 2.4 como base para avaliar os efeitos e classificar a severidade da condição de falha.

Quadro 2.5 - Classificação da severidade para cada condição de falha

Condição de falha	Efeitos da condição de falha na tripulação, passageiros e aeronave	Classificação da severidade
Perda total e não anunciada da capacidade de desacelerar as rodas no solo	A tripulação detecta a falha quando o freio é operado. Comanda os *spoilers* e utiliza os reversores na máxima potência. Esta situação pode resultar em saída de pista.	*Hazardous*
Aplicação inadvertida de todos os freios de roda	A tripulação não conseguirá decolar ou realizar um cancelamento da decolagem de forma segura, resultando em saída de pista com alta velocidade.	*Catastrophic*

Fonte: SAE ARP 4761

O Quadro 2.5 encerra os passos da análise funcional. Com as classificações de severidade estabelecidas é possível selecionar quais condições de falha terão análises detalhadas por meio de métodos como árvore de falhas.

2.4 ANÁLISE DE ÁRVORE DE FALHAS

No processo de desenvolvimento, é necessário comprovar que o sistema atende os objetivos de segurança (Quadro 2.2). No passo seguinte à avaliação de perigos funcionais do sistema, utiliza-se a análise de árvore de falha com o objetivo de identificar falhas únicas e combinações de falhas que podem levar à ocorrência da condição de falha. São elaboradas, em um projeto aeronáutico, árvores de falha para todas as condições de falha classificadas como *Hazardous* e *Catastrophic* e para algumas condições de falha classificadas com *Major* e *Minor*.

Segundo a ARP 4761, a análise de árvore de falha de sistemas é um método dedutivo, com orientação à falha. Seu foco é direcionado para uma condição específica que não se deseja que ocorra. Além disso, provê um método para a determinação das causas necessárias e suficientes que resultam no evento topo. Colocado de uma forma distinta, a análise de árvore de falha é um procedimento de avaliação *top-down* no qual um modelo qualitativo de um evento indesejado é construído e, então avaliado. O método também pode ser aplicado quantitativamente

para gerar informações úteis sobre a probabilidade de ocorrência do evento topo e da importância de todas as causas e eventos modelados na árvore de falha.

Uma árvore de falha é composta de entidades chamadas de portas (*gates*) que servem para permitir ou inibir a passagem de uma lógica em direção ao topo da árvore. As portas mostram os relacionamentos de eventos necessários para a ocorrência de um evento em um nível superior. Os eventos superiores são a saída das portas e os eventos inferiores são as entradas. Os diferentes símbolos das portas revelam o tipo de relacionamento que há entre as entradas e que será requerido para que o evento de saída ocorra (SAE ARP 4761, 1996).

É importante salientar que uma árvore de falha não é um modelo de todos os possíveis eventos de falha ou de todas as causas de uma falha do sistema. Ela é direcionada para representar o evento topo que corresponderá a um modo de falha específico do sistema e, portanto, incluirá apenas as falhas que contribuem para este evento topo. Ademais, estas não são todas as possibilidades de falha. São somente aquelas que foram avaliadas como sendo realistas pelo técnico que a elaborou a análise (SAE ARP 4761, 1996).

Todas as árvores de falha são compostas por três tipos de símbolos: portas, eventos básicos e transferência. Um retângulo contém a descrição da saída de um símbolo lógico ou de um evento (SAE ARP 4761, 1996).

Símbolos de portas são utilizados para agrupar os diversos ramos de uma árvore de falha. Os dois símbolos principais são as portas E e portas OU. Portas E são utilizadas quando o evento do nível superior pode apenas ocorrer quando todos as condições do nível inferior forem verdadeiras. Já as Portas OU são usadas quando o evento indesejado pode ocorrer se um ou mais eventos do nível inferior for verdadeiro (SAE ARP 4761, 1996).

Os eventos primários mais comuns são: o evento básico, evento condicional e evento não desenvolvido. Um círculo na base do retângulo representa um evento básico. Este é definido como um evento interno ao sistema sob análise e que não requer desenvolvimentos adicionais. Em outras palavras, o evento básico é capaz de causar uma falha e, para elementos físicos apenas, pode receber um valor de taxa de falha na forma de alocação ou como informação proveniente de um FMEA ou outra fonte (SAE ARP 4761, 1996).

O termo evento básico pode ser referente à falha de um componente. Como este trabalho tratará sobre um método de identificação de componentes críticos, deste ponto em diante, quando o termo evento básico aparecer, deve ser entendido como componente.

Neste trabalho, serão analisadas somente as árvores de falha que modelam condições de falha classificadas como *Catastrophic*.

2.5 AVALIAÇÃO DA SEGURANÇA DURANTE A OPERAÇÃO

A ARP 5150 oferece um processo sistemático para medir e monitorar a segurança. Para aprimorar os níveis de segurança durante o completo ciclo de vida do produto, não é suficiente apenas a avaliação da segurança de um produto aeronáutico na fase de projeto. A operação em curso de uma aeronave deve ser avaliada.

O processo de monitoramento contínuo da segurança pode ser aplicado tanto nas operações de uma linha aérea quanto na avaliação dos sistemas realizada pelo fabricante, a partir de informações de campo.

2.5.1 Segurança Contínua Segundo a ARP5150

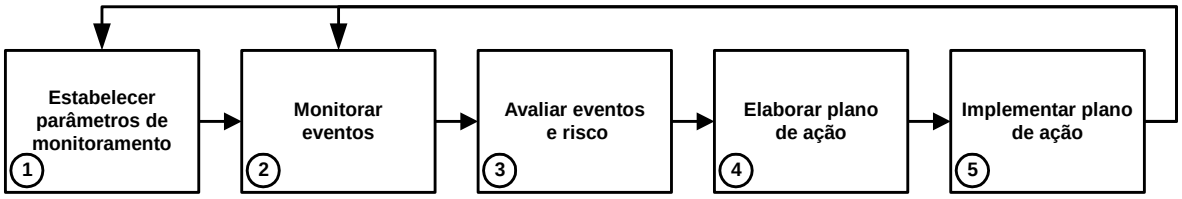
A gestão contínua da segurança é uma atividade dedicada a garantir que o risco seja identificado e devidamente eliminado ou controlado. Para tal, este processo deve ter uma abordagem lógica e sistemática. A segurança não é autossustentável. Quando um avião é entregue e está em condições perfeitas, ele tem um nível inicial de segurança. À medida que os aviões são operados, o nível de segurança é mantido através de um processo contínuo de monitoramento da experiência em serviço, identificando questões e oportunidades relacionadas à segurança e, em seguida, abordando essas questões ou oportunidades através de mudanças apropriadas no produto ou nos procedimentos.

O processo de avaliação contínua da segurança inclui três objetivos:

1. Manter a aeronavegabilidade da aeronave: Os eventos em serviço são avaliados com base nos efeitos no nível de segurança previsto no processo de certificação.
2. Manter a segurança do avião: Os eventos em serviço são avaliados em relação aos objetivos de segurança.
3. Melhorar a segurança do avião: Os eventos em serviço são avaliados para identificar oportunidades para diminuir seu número ou para superar os objetivos de segurança. Neste ponto, é preciso relembrar o conceito de que a manutenção e operação com seus respectivos procedimentos apenas mantém os níveis de segurança existentes. Para se aprimorar os níveis de segurança é preciso que sejam implementadas modificações nos sistemas e / ou procedimentos.

Um processo genérico e de alto nível segundo a norma ARP 5150 é mostrado na Figura 2.2:

Figura 2.2 - Processo genérico e de alto nível para avaliação contínua da segurança de acordo com a ARP 5150



Fonte: SAE ARP 5150

1. Estabelecimento de parâmetros para monitoramento

Começa com a determinação da estrutura, objetivos e metas de segurança específica da empresa, seja uma linha aérea ou fabricante (sempre respeitando os objetivos de segurança de certificação). Este processo também estabelece os parâmetros de monitoramento e seus valores.

2. Monitoramento dos eventos de campo

É o processo contínuo de busca de eventos específicos. Este monitoramento é baseado nos parâmetros estabelecidos na etapa anterior.

3. Avaliação dos eventos reportados e do respectivo risco

Parte do processo iniciado quando um evento é detectado. Inclui a avaliação do evento suficiente para determinar sua relevância e se é realmente necessário investigação mais profunda e detalhada. Inclui, também, uma determinação preliminar de risco para uso na priorização da avaliação inicial e no desenvolvimento do plano de ação. Com base na gravidade do evento e na avaliação inicial de risco, uma avaliação de risco mais detalhada e completa pode ser realizada.

4. Elaboração do plano de ação

Parte do processo que estabelece a correção ou melhoria, como mudança de projeto, mudança de operações, manutenção e / ou procedimentos de treinamento para o evento identificado. O plano de ação pode não ser necessário se o evento for considerado suficientemente benigno.

5. Disposição do plano de ação

É a avaliação e / ou implementação do plano de ação. Determinação da implementação ou não da ação, priorização e cronograma das atividades. Uma vez concluída a ação ou quando se determina não implementar a mesma, o processo retorna ao estado normal de monitoramento. Em alguns casos, a revisão ou atualização dos parâmetros de monitoramento pode ocorrer como resultado do evento ou da ação implementada.

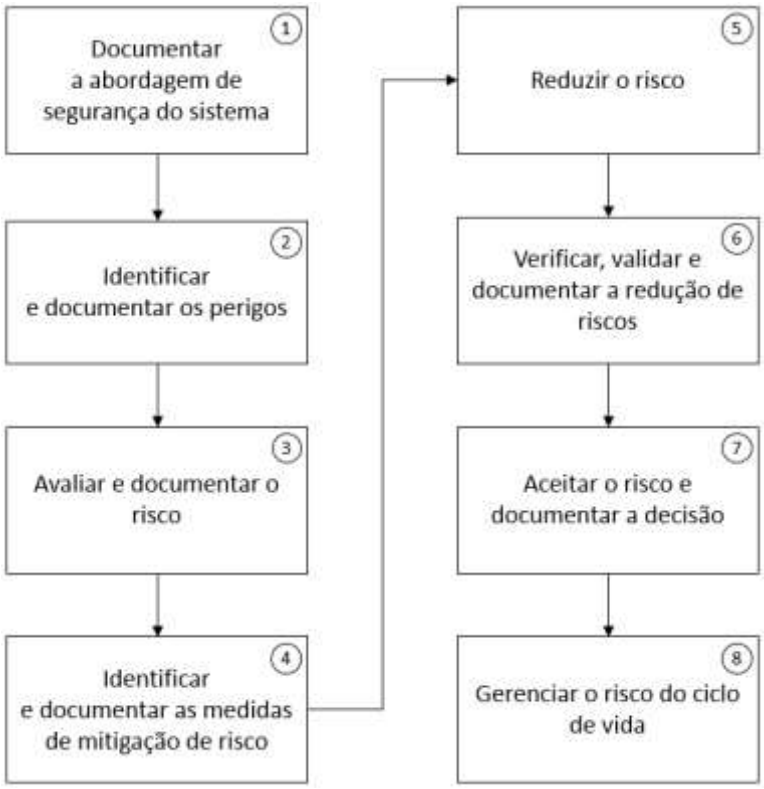
O método proposto neste trabalho se concentra nos passos 1, 2 e 3 do processo da ARP 5150, mais fortemente no passo 1, ou seja, estabelecer parâmetros de monitoramento. Outra característica relevante do método é que este visa a coleta sistemática e repetitiva dos dados de vida dos componentes identificados como críticos e a avaliação dos critérios de risco.

2.6 ANÁLISE DE RISCO SEGUNDO A NORMA MIL-STD-882E

A MIL-STD-882E fornece um método padrão e genérico para a identificação, classificação e mitigação de riscos. Pode ser aplicada para o tratamento de perigos relacionados a sistemas / produtos / equipamentos / infraestrutura (incluindo *hardware* e *software*) durante todo o projeto, desenvolvimento, teste, produção, uso e descarte.

O processo de segurança do sistema consiste em oito elementos, conforme mostra a Figura 2.3.

Figura 2.3 - Processo padrão e genérico para identificação, classificação e mitigação de riscos segundo MIL-STD-882E



Fonte: MIL-STD-882E

1. Documentar a abordagem de segurança do sistema

Este passo consiste em registrar como serão elaboradas as análises de segurança para sistemas e para a operação do produto.

2. Identificar e documentar perigos

O segundo passo diz respeito à identificação e registro dos perigos por meio das análises executadas conforme o primeiro item estabelece.

3. Avaliar e documentar o risco

Nesta parte do processo, os perigos identificados no item anterior são avaliados utilizando métodos como a avaliação de perigos funcionais e análise de árvore de falha. Deve-se utilizar critérios de severidade e probabilidade previamente estabelecidos. Uma matriz de risco deve, também, ser elaborada com os patamares de risco. Os Quadros 2.6, 2.7 e 2.8 mostram os níveis de severidade, probabilidade e de risco para a MIL-STD-882E.

Quadro 2.6 - Níveis de severidade de acordo com a norma MIL-STD-882E

Descrição	**Categoria de severidade**
Catastrophic	1
Critical	2
Marginal	3
Negligible	4

Fonte: MIL-STD-882E

Quadro 2.7 - Níveis de probabilidade de acordo com a norma MIL-STD-88E

Descrição	**Nível de probabilidade**
Frequent	A
Probable	B
Occasional	C
Remote	D
Improbable	E
Eliminated	F

Fonte: MIL-STD-882E

Quadro 2.8 - Níveis de risco para cada combinação de severidade e probabilidade de acordo com a norma MIL-STD-882E

Severidade / **Probabilidade**	***Catastrophic*** **(1)**	***Critical*** **(2)**	***Marginal*** **(3)**	***Negligible*** **(4)**
Frequent **(A)**	Alto	Alto	Sério	Médio
Probable ***(B)***	Alto	Alto	Sério	Médio
Occasional ***(C)***	Alto	Sério	Médio	Baixo
Remote ***(D)***	Sério	Médio	Médio	Baixo
Improbable ***(E)***	Médio	Médio	Médio	Baixo
Eliminated **(F)**	Risco eliminado			

Fonte: MIL-STD-882E

4. Identificar e documentar medidas de mitigação de risco

Potenciais mitigações para os perigos identificados devem ser discutidas. A meta é sempre buscar a eliminação do risco. Quando não for possível eliminar, o risco deve ser reduzido para o menor patamar aceitável, respeitando o custo, prazo e o desempenho do sistema. Estas ações de mitigação potenciais devem ser registradas.

5. Reduzir risco

Dentre as possíveis soluções discutidas no passo prévio, seleciona-se aquelas que tem a capacidade de maior redução de risco, respeitando, novamente, o custo, prazo e viabilidade da modificação.

6. Verificar, validar e documentar a redução de riscos

As soluções implementadas para redução de risco devem ser validadas e verificadas por meio de análises, testes, demonstrações ou inspeção. O registro dessas ações complementa o passo 5.

7. Aceitar o risco e documentar a decisão

A norma MIL-STD-882E estipula que antes de colocar em operação um sistema, este deve ter seus riscos aceitos pelos níveis hierárquicos apropriados. Após uma campanha de redução de riscos, alguns riscos residuais persistem. Todos os riscos devem ser aceitos e documentados.

8. Gerenciar o risco do ciclo de vida

Após o sistema entrar em operação, todo o processo deve ser mantido e executado para os novos riscos que possam surgir. Modificações de sistema devem ser submetidas às análises deste processo e seus riscos identificados, mitigados, aceitos e documentados.

2.7 MÉTODO SISTEMÁTICO DE IDENTIFICAÇÃO DE COMPONENTES E GRUPOS DE CORTE CRÍTICOS EM ÁRVORES DE FALHAS

O método de identificação de componentes e grupos de corte críticos em árvores de falha tem os seus passos baseados no processo genérico e de alto nível exposto pela ARP 5150. Recapitulando os passos da ARP 5150, tem-se:

1. Estabelecimento de parâmetros para monitoramento;
2. Monitoramento dos eventos de campo;
3. Avaliação dos eventos reportados e do respectivo risco;
4. Elaboração do plano de ação;
5. Disposição do plano de ação.

São utilizados os três primeiros passos para elaborar o método, que é estruturado da seguinte forma:

1. Estabelecimento de parâmetros para monitoramento.

a. Seleção das árvores de falha que modelam condições de falha catastróficas.
b. Seleção dos componentes mais relevantes.

i. Determinação dos grupos de corte da árvore de falha com o *software* CAFTA.
ii. Aplicação das medidas de importância à árvore de falha com o *software* CAFTA.
iii. Seleção dos componentes mais relevantes utilizando o conceito de Pareto.

c. Seleção dos grupos de corte mais significativos com base na lista de componentes relevantes selecionados no passo 1.b.iii.
    i. São selecionados os grupos de corte formados pela combinação dos componentes selecionados.
d. Definição dos critérios de probabilidade para monitoramento dos grupos de corte.
    i. Os critérios de probabilidade utilizam os objetivos de probabilidade (objetivos de segurança estabelecidos para o sistema em estudo).

2. Monitoramento dos eventos de campo.

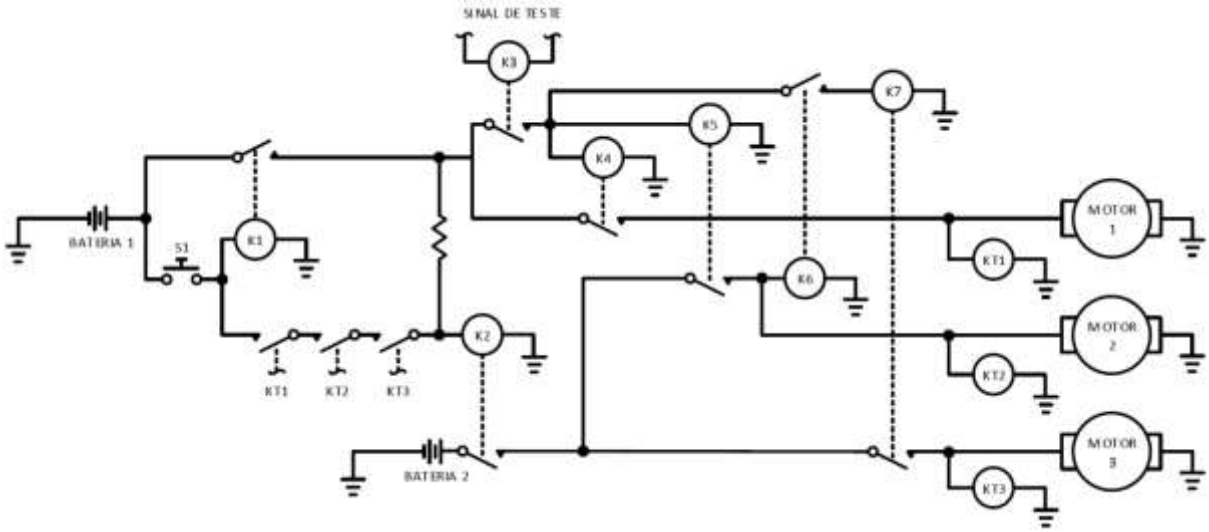
a. Levantamento dos dados de falha dos componentes relevantes selecionados no passo 1.b.iii.

3. Avaliação dos eventos reportados e do respectivo risco

a. Avaliação das probabilidades dos grupos de corte e comparação com critérios de probabilidade do passo 1.d.

Nos parágrafos a seguir, é apresentada a aplicação do método para um exemplo de árvore de falha extraída da norma NUREG-0492 *Fault Tree Handbook*. O sistema estudado é uma caixa de distribuição de potência. Os componentes que fazem parte do sistema são: botão de pressão (S1), relés (K1, K2, K3, K4, K5, K6 e K7), relés temporizados (KT1, KT2 e KT3), baterias (bateria 1 e bateria 2) e motores (M1, M2 e M3).

Figura 2.2.74 - Exemplo de caixa de distribuição de potência da NUREG-0492



Fonte: NUREG 0492

Os contatos dos relés temporizados são do tipo normalmente fechados. A partir do momento que o botão S1 é pressionado, energia da bateria 1 é aplicada às bobinas dos relés K1 e, em seguida, K2. Então, K1 e K2 fecham e permanecem nesta condição (*latched*). Em seguida, um sinal de teste de 60 segundos é imposto pelo relé K3, que tem como propósito checar a operação dos motores 1, 2 e 3. Uma vez fechado o K3, a energia da bateria 1 é aplicada às bobinas dos relés K4 e K5. O fechamento do relé K4 energiza e inicia a partida do motor 1. O fechamento do relé K5 permite que a bateria 2 forneça energia ao relé K6 e, também, ao motor 2. Finalmente, o fechamento do relé K6 permite que a bateria 1 forneça energiza para o relé K7, que por sua vez, fornece energia para a partida do motor 3.

Depois de um intervalo de 60 segundos, o relé K3 está programado para abrir, interrompendo a operação dos três motores. Se o relé K3 permanecer fechado após os 60 segundos, significando que falhou na posição fechada, todos os relés temporizados (KT1, KT2 e KT3) se abrem, retirando a energia do relé K1 e, consequentemente, encerrando a operação do sistema. Suponha-se que o relé K3 abra no tempo especificado, porém o relé K4 permanece fechado. Neste caso, o relé temporizador KT1 abrirá, tirando a energia do relé K1, encerrando, assim, a operação do sistema. KT2 e KT3 tem a mesma função do KT1, abrindo o relé K1 caso os relés K5 e K7 falhem fechados, respectivamente.

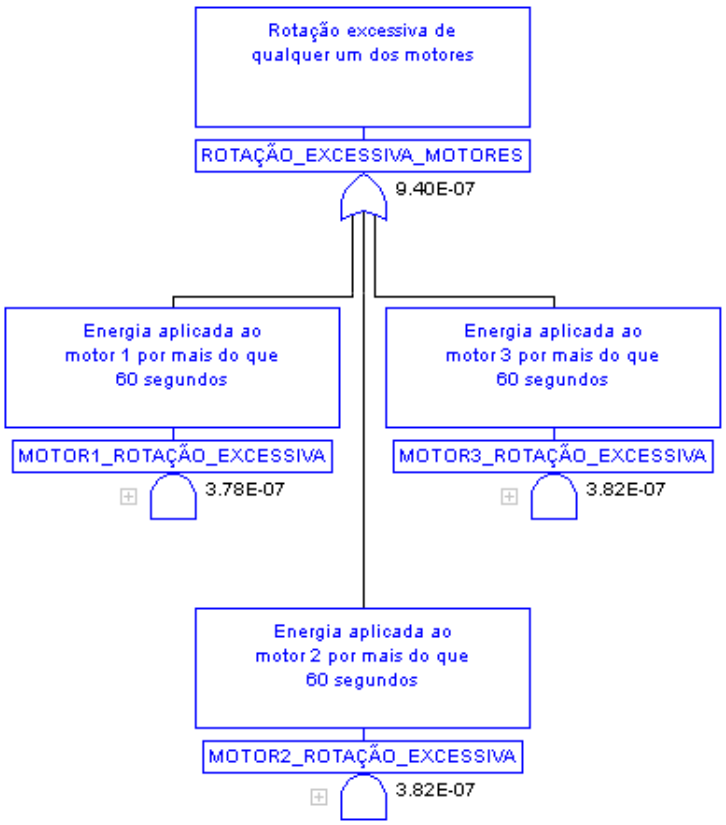
Este procedimento de teste dos motores acontece uma vez por dia. Dado que o sistema só opera quando é testado, o tempo de exposição fica estabelecido

como sendo t = 24 horas. Alguns componentes possuem falha latente, isto é, só é possível saber que falharam quando combinados com outras falhas. Este é o caso dos componentes K3, K4, K5, K6, K7, KT1, KT2 e KT3. Há uma verificação específica para determinar se há falha para estes componentes, cuja execução se dá a cada 2 semanas. Portanto, o tempo de exposição para estes componentes fica determinado como sendo t = 15 dias.

A função deste sistema é prevenir que os motores entrem em situação de rotação excessiva (*overrun*) depois da aplicação do sinal de teste. A partir da arquitetura do sistema e da descrição da sua operação a análise de árvore de falha é elaborada.

Segundo o método descrito no início desta sessão do trabalho, o passo 1.a., que diz respeito à seleção da árvore de falha, está concluído. A árvore de falha pode ser vista na Figura 2.5.

Figura 2.5 - Árvore de falha do exemplo de caixa de distribuição de potência da NUREG-0492



O próximo passo, 1.b.i., se refere à determinação dos grupos de corte.

Quadro 2.9 - Grupos de corte do exemplo de aplicação do método de identificação de componentes e grupos de corte críticos

#	Probabilidade do grupo de corte	Probabilidade do evento	Taxa de falha	Tempo de exposição	Evento básico	Descrição
1	1,81E-07	2,52E-04	7,00E-07	15 dias	K4_FALHA_FECHADO	Contato do relé K4 falha para abrir
		7,20E-04	3,00E-05	24 horas	S1_FALHADO_FECHADO	S1 falha para abrir
2	1,81E-07	2,52E-04	7,00E-07	15 dias	K5_FALHA_FECHADO	Contato do relé K5 falha para abrir
		7,20E-04	3,00E-05	24 horas	S1_FALHADO_FECHADO	S1 falha para abrir
3	1,81E-07	2,52E-04	7,00E-07	15 dias	K7_FALHA_FECHADO	Contato do relé K7 falha para abrir
		7,20E-04	3,00E-05	24 horas	S1_FALHADO_FECHADO	S1 falha para abrir
4	9,07E-08	2,52E-04	7,00E-07	15 dias	K4_FALHA_FECHADO	Contato do relé K4 falha para abrir
		3,60E-04	1,00E-06	15 dias	KT1_FALHA_FECHADO	KT1 falha para abrir quando contato K4 fechado por mais de 60s
5	9,07E-08	2,52E-04	7,00E-07	15 dias	K5_FALHA_FECHADO	Contato do relé K5 falha para abrir
		3,60E-04	1,00E-06	15 dias	KT2_FALHA_FECHADO	KT2 falha para abrir quando contato K5 fechado por mais de 60s
6	9,07E-08	2,52E-04	7,00E-07	15 dias	K7_FALHA_FECHADO	Contato do relé K7 falha para abrir
		3,60E-04	1,00E-06	15 dias	KT3_FALHA_FECHADO	KT3 falha para abrir quando contato K7 fechado por mais de 60s
7	8,64E-08	7,20E-04	3,00E-05	24 horas	S1_FALHADO_FECHADO	S1 falha para abrir
		1,20E-04	5,00E-06	24 horas	SINAL_TESTE_K3_CONTINUA	O sinal de teste continua habilitado no relé K3 por mais de 60 segundos
8	1,21E-08	1,68E-05	7,00E-07	24 horas	K3_FALHA_FECHADO	Contato do relé K3 falha para abrir
		7,20E-04	3,00E-05	24 horas	S1_FALHADO_FECHADO	S1 falha para abrir
9	4,23E-09	1,68E-05	7,00E-07	24 horas	K1_FALHA_FECHADO	Contato do relé K1 falha para abrir
		2,52E-04	7,00E-07	15 dias	K4_FALHA_FECHADO	Contato do relé K4 falha para abrir
10	4,23E-09	1,68E-05	7,00E-07	24 horas	K1_FALHA_FECHADO	Contato do relé K1 falha para abrir
		2,52E-04	7,00E-07	15 dias	K5_FALHA_FECHADO	Contato do relé K5 falha para abrir
11	4,23E-09	1,68E-05	7,00E-07	24 horas	K1_FALHA_FECHADO	Contato do relé K1 falha para abrir
		2,52E-04	7,00E-07	15 dias	K7_FALHA_FECHADO	Contato do relé K7 falha para abrir
12	4,23E-09	1,68E-05	7,00E-07	24 horas	K2_FALHA_FECHADO	Contato do relé K2 falha para abrir
		2,52E-04	7,00E-07	15 dias	K5_FALHA_FECHADO	Contato do relé K5 falha para abrir
13	4,23E-09	1,68E-05	7,00E-07	24 horas	K2_FALHA_FECHADO	Contato do relé K2 falha para abrir
		2,52E-04	7,00E-07	15 dias	K7_FALHA_FECHADO	Contato do relé K7 falha para abrir
14	2,02E-09	1,68E-05	7,00E-07	24 horas	K1_FALHA_FECHADO	Contato do relé K1 falha para abrir
		1,20E-04	5,00E-06	24 horas	SINAL_TESTE_K3_CONTINUA	O sinal de teste continua habilitado no relé K3 por mais de 60 segundos
15	6,05E-10	2,52E-04	7,00E-07	15 dias	K4_FALHA_FECHADO	Contato do relé K4 falha para abrir
		2,40E-06	1,00E-07	24 horas	S1_FECHA_INADVERTIDAMENTE	S1 fecha inadvertidamente
16	6,05E-10	2,52E-04	7,00E-07	15 dias	K5_FALHA_FECHADO	Contato do relé K5 falha para abrir

#	Probabilidade do grupo de corte	Probabilidade do evento	Taxa de falha	Tempo de exposição	Evento básico	Descrição
		2,40E-06	1,00E-07	24 horas	S1_FECHA_INADVERTIDAMENTE	S1 fecha inadvertidamente
17	6,05E-10	2,52E-04	7,00E-07	15 dias	K7_FALHA_FECHADO	Contato do relé K7 falha para abrir
		2,40E-06	1,00E-07	24 horas	S1_FECHA_INADVERTIDAMENTE	S1 fecha inadvertidamente
18	2,88E-10	2,40E-06	1,00E-07	24 horas	S1_FECHA_INADVERTIDAMENTE	S1 fecha inadvertidamente
		1,20E-04	5,00E-06	24 horas	SINAL_TESTE_K3_CONTINUA	O sinal de teste continua habilitado no relé K3 por mais de 60 segundos
19	2,82E-10	1,68E-05	7,00E-07	24 horas	K1_FALHA_FECHADO	Contato do relé K1 falha para abrir
		1,68E-05	7,00E-07	24 horas	K3_FALHA_FECHADO	Contato do relé K3 falha para abrir
20	4,03E-11	1,68E-05	7,00E-07	24 horas	K3_FALHA_FECHADO	Contato do relé K3 falha para abrir
		2,40E-06	1,00E-07	24 horas	S1_FECHA_INADVERTIDAMENTE	S1 fecha inadvertidamente
21	5,60E-15	3,60E-04	1,00E-06	15 dias	KT1_FALHA_FECHADO	KT1 falha para abrir quando contato K4 fechado por mais de 60s
		3,60E-04	1,00E-06	15 dias	KT2_FALHA_FECHADO	KT2 falha para abrir quando contato K5 fechado por mais de 60s
		3,60E-04	1,00E-06	15 dias	KT3_FALHA_FECHADO	KT3 falha para abrir quando contato K7 fechado por mais de 60s
		1,20E-04	5,00E-06	24 horas	SINAL_TESTE_K3_CONTINUA	O sinal de teste continua habilitado no relé K3 por mais de 60 segundos
22	7,83E-16	1,68E-05	7,00E-07	24 horas	K3_FALHA_FECHADO	Contato do relé K3 falha para abrir
		3,60E-04	1,00E-06	15 dias	KT1_FALHA_FECHADO	KT1 falha para abrir quando contato K4 fechado por mais de 60s
		3,60E-04	1,00E-06	15 dias	KT2_FALHA_FECHADO	KT2 falha para abrir quando contato K5 fechado por mais de 60s
		3,60E-04	1,00E-06	15 dias	KT3_FALHA_FECHADO	KT3 falha para abrir quando contato K7 fechado por mais de 60s

Em seguida, aplicam-se as medidas de importância aos grupos de corte (passo 1.b.ii.) para determinar quais os componentes mais relevantes, isto é, aqueles que contribuem para um maior risco do evento topo acontecer. A medida de importância utilizada será a Fussel-Vesely (FV).

Quadro 2.10 - Ranque dos componentes do exemplo de aplicação do método para a medida de importância Fussel-Vesely

Evento básico	Probabilidade do evento	Fussel-Vesely	% de contribuição	Descrição
S1_FALHADO_FECHADO	7,20E-04	6,83E-01	34,16%	S1 falha para abrir
K5_FALHA_FECHADO	2,52E-04	2,99E-01	14,96%	Contato do relé K5 falha para abrir
K7_FALHA_FECHADO	2,52E-04	2,99E-01	14,96%	Contato do relé K7 falha para abrir
K4_FALHA_FECHADO	2,52E-04	2,94E-01	14,71%	Contato do relé K4 falha para abrir
KT1_FALHA_FECHADO	3,60E-04	9,65E-02	4,83%	O sinal de teste continua habilitado no relé K3 por mais de 60 segundos
KT2_FALHA_FECHADO	3,60E-04	9,65E-02	4,83%	KT1 falha para abrir quando contato K4 fechado por mais de 60s
KT3_FALHA_FECHADO	3,60E-04	9,65E-02	4,83%	KT2 falha para abrir quando contato K5 fechado por mais de 60s
SINAL_TESTE_K3_CONTINUA	1,20E-04	9,43E-02	4,72%	KT3 falha para abrir quando contato K7 fechado por mais de 60s
K1_FALHA_FECHADO	1,68E-05	1,60E-02	0,80%	Contato do relé K1 falha para abrir
K3_FALHA_FECHADO	1,68E-05	1,32E-02	0,66%	Contato do relé K3 falha para abrir
K2_FALHA_FECHADO	1,68E-05	9,00E-03	0,45%	Contato do relé K2 falha para abrir
S1_FECHA_INADVERTIDAMENTE	2,40E-06	2,28E-03	0,11%	S1 fecha inadvertidamente

O conceito de Pareto pode ser observado no Quadro 2.10. Os quatro primeiros eventos (30%) correspondem a 78,79% do percentual de contribuição para a ocorrência evento topo. Com isso, tem-se a base para executar o passo 1.b.iii. Seleciona-se, portanto, os seguintes eventos para serem monitorados:

Quadro 2.11 - Eventos mais relevantes do exemplo de aplicação do método

#	**Componente**	**Modo de falha**
1	Botão de pressão S1	S1 falha fechado
2	Relé K5	K5 falha fechado
3	Relé K7	K7 falha fechado
4	Relé K4	K4 falha fechado

O Quadro 2.11 mostra que somente um modo de falha dos componentes é relevante, falhar fechado. O especialista responsável pela definição dos componentes críticos a serem monitorados pode decidir por monitorar o modo de falha específico (informação que é muito difícil de se obter) ou pode optar por

monitorar falhas funcionais, sem especificar os modos de falha. Dessa forma, o desempenho destes componentes críticos será acompanhado de perto, garantindo que as taxas de falha estarão dentro dos limites de segurança.

A próxima etapa está relacionada com os grupos de corte. Determina-se quais os mais significativos definindo aqueles que são compostos pela combinação dos componentes críticos. No Quadro 2.12 estão os grupos de corte compostos pela combinação dos componentes mais críticos.

Quadro 2.12 - Grupos de corte mais relevantes do exemplo de aplicação do método formados pelos componentes do Quadro 11

#	Probabilidade do grupo de corte	Probabilidade do evento	Taxa de falha	Tempo de exposição	Evento básico	Descrição
1	1,81E-07	2,52E-04	7,00E-07	15 dias	K4_FALHA_FECHADO	Contato do relé K4 falha para abrir
		7,20E-04	3,00E-05	24 horas	S1_FALHADO_FECHADO	S1 falha para abrir
2	1,81E-07	2,52E-04	7,00E-07	15 dias	K5_FALHA_FECHADO	Contato do relé K5 falha para abrir
		7,20E-04	3,00E-05	24 horas	S1_FALHADO_FECHADO	S1 falha para abrir
3	1,81E-07	2,52E-04	7,00E-07	15 dias	K7_FALHA_FECHADO	Contato do relé K7 falha para abrir
		7,20E-04	3,00E-05	24 horas	S1_FALHADO_FECHADO	S1 falha para abrir

Neste ponto do processo, tem-se determinados os componentes e os grupos de corte mais críticos. O esforço para monitorar somente estes componentes será muito menor em relação ao monitoramento de todos os componentes que participam deste sistema, otimizando, desta maneira, os recursos da área da empresa responsável pelo trabalho de monitoramento e análise dos dados de falha.

A etapa seguinte diz respeito ao critério que determinará quando deve ser realizada uma análise de risco. Para isso, é necessário conhecer os objetivos de segurança para este sistema: os níveis de severidade e de probabilidade, bem como a matriz de risco. No Quadro 2.13 é exposta a definição destes critérios.

Quadro 2.13 - Critério de níveis de risco a partir da combinação dos níveis de severidade e probabilidade para o exemplo de aplicação do método

Probabilidade do limite inferior	***Catastrophic** **	***Critical** **	***Marginal** **	***Negligible** **
$1x10^{-2}$	Alto	Alto	Sério	Médio
$1x10^{-3}$	Alto	Alto	Sério	Médio
$1x10^{-4}$	Alto	Sério	Médio	Baixo
$1x10^{-5}$	Sério	Médio	Baixo	Baixo
$1x10^{-6}$	Médio	Baixo	Baixo	Baixo
	Baixo	Baixo	Baixo	Baixo

* Níveis de severidade da norma MIL-STD-882E

O sistema deve atender os seguintes patamares de probabilidade, como mostra o Quadro 2.14:

Quadro 2.14 - Objetivos de probabilidade para cada nível de severidade para o exemplo de aplicação do método

Severidade	**Probabilidade**
Catastrophic *	< $1x10^{-6}$
Critical *	< $1x10^{-5}$
Marginal *	< $1x10^{-4}$
Negligible *	< $1x10^{-3}$

* Níveis de severidade da norma MIL-STD-882E

Dessa forma, para uma árvore de falha proveniente de uma condição de falha classificada como *Catastrophic*, esta deve ser menor que a probabilidade

de 1x10^{-6}. A probabilidade do evento topo para este exemplo é 9,40x10^{-7}, portanto o sistema atende os critérios de segurança.

A partir das informações acima, é possível determinar os critérios de probabilidade para os grupos de corte críticos, como mostra o Quadro 2.15.

Quadro 2.15 - Critérios de probabilidade dos grupos de corte para o exemplo de aplicação do método

Grupo de corte	Probabilidade Evento Básico 1	Probabilidade Evento Básico 2	Critério de probabilidade
1	Relé K4	Botão de pressão S1	Probabilidade de falha do relé K4 x Probabilidade de falha do Botão de pressão S1 < 1x10^{-6}
2	Relé K5	Botão de pressão S1	Probabilidade de falha do relé K5 x Probabilidade de falha do Botão de pressão S1 < 1x10^{-6}
3	Relé K7	Botão de pressão S1	Probabilidade de falha do relé K7 x Probabilidade de falha do Botão de pressão S1 < 1x10^{-6}

Tomando como exemplo o grupo de corte 1, extrai-se o seguinte significado: o produto da probabilidade de falha do relé 4 combinada com a probabilidade de falha do botão de pressão S1 deve ser menor que a probabilidade de 1x10^{-6}. Se o acompanhamento das falhas destes componentes mostrar que a combinação das probabilidades de falha está maior que o valor de 1x10^{-6}, então este é o indicativo que deve ser realizada uma análise de risco. A Equação 1 define o critério:

$$(1-e^{-(\lambda_{Relé\,K4}.t_{Exposição\,do\,relé})}).(1-e^{-(\lambda_{Botão\,S1}.t_{Exposição\,do\,botão})}) < 1.10^{-6} \qquad \text{Equação 1}$$

O próximo passo do processo é realizar o monitoramento dos eventos de campo dos componentes críticos. Como exemplo, determina-se que o levantamento das falhas mostrou que a taxa de falha do relé é $\lambda = 5.10^{-6}$ e a taxa de falha do botão é $\lambda = 6.10^{-5}$, então a probabilidade do grupo de corte será $\left(1 - e^{-\left(5.10^{-6}.360\right)}\right).(1 - e^{-\left(6.10^{-5}.24\right)}) = 2{,}59.10^{-6}$ que é maior que 1x10^{-6}. Tem-se evidência de que uma análise de risco deve ser elaborada, pois o critério de segurança não está mais sendo atendido. No Quadro 2.16 é possível constatar qual a categoria de risco que a condição atual das taxas de falha dos componentes está determinando, ou seja, risco Médio.

Quadro 2.16 - Resultado do nível de risco para o exemplo de aplicação do método

Probabilidade do limite inferior	***Catastrophic* ***	***Critical* ***	***Marginal* ***	***Negligible* ***
$1x10^{-2}$	Alto	Alto	Sério	Médio
$1x10^{-3}$	Alto	Alto	Sério	Médio
$1x10^{-4}$	Alto	Sério	Médio	Baixo
$1x10^{-5}$	Sério	Médio	Baixo	Baixo
$1x10^{-6}$	$2,59x10^{-6}$	Baixo	Baixo	Baixo
	Baixo	Baixo	Baixo	Baixo

* Níveis de severidade da norma MIL-STD-882E

A partir deste momento, outras atividades são necessárias como, por exemplo, a elaboração de um plano de ação e a sua implementação. Como este trabalho está focado nas partes 1, 2 e 3 do processo da ARP5150, o exemplo termina neste ponto.

2.8 SÍNTESE E CONCLUSÃO DO CAPÍTULO

No capítulo 2 foi apresentada explanação e importância dos objetivos de segurança e a presença do risco inerente a qualquer no projeto de sistemas. Em seguida, detalhou-se, para a regulamentação aeronáutica, a particularidade dos níveis de severidade e probabilidade, efeitos das condições de falha relacionados à aeronave, tripulantes e passageiros para cada nível de severidade. Também foram detalhados os objetivos e critérios de segurança como a comprovação de ausência de falha simples para condições catastróficas e a comprovação de que toda

condição de falha catastrófica deve cumprir com probabilidade extremamente improvável (menor que $1x10^{-9}$). Abordou-se a análise funcional de sistemas e a análise de árvore de falhas. Foram apresentados os processos de avaliação da segurança durante a operação contido na ARP 5150 e de análise de risco segundo a MIL-STD-882E. Por último, explicou-se o método proposto nesta monografia que visa identificar os componentes e grupos de corte críticos em árvores de falha.

Este trabalho apresenta um método que visa identificar itens para monitoramento contínuo de segurança de sistemas. Alguns dos pilares para sustentar este processo de monitoramento são: 1) estabelecimento de parâmetros, 2) monitoramento das taxas de falha dos componentes críticos a partir dos eventos de campo e 3) avaliação dos eventos e dos respectivos riscos. Estes três pilares são baseados no processo de avaliação contínua de segurança da ARP 5150. A análise de risco é baseada na MIL-STD-882E. Os objetivos de segurança são a base para formar os critérios de probabilidade ou parâmetros de monitoramento. O método de identificação dos componentes e grupos de corte críticos engloba os três pilares do processo de monitoramento.

O próximo capítulo abordará o referencial teórico necessário para executar os cálculos e análises presentes no método proposto nesta monografia. Cada uma das etapas do método engloba uma série de conceitos e estes serão detalhados e explicados de forma a prover a base para sua execução.

3 REFERENCIAL TEÓRICO

Este capítulo apresentará os conceitos teóricos que embasam o método proposto. Dentre os conceitos expostos estão: análise de dados de vida (*life data analysis* - LDA), as métricas *mean time between failure* (MTBF) e *mean time between unscheduled removals* (MTBUR), a comparação entre *mean time to failure* (MTTF), MTBF e MTBUR e as medidas de importância.

3.1 ANÁLISE DE DADOS DE VIDA

Segundo O'Connor e Kleyner (2012), o método *Life Data Analysis* (LDA) ou análise de dados de vida consiste, basicamente, em coletar dados de falha de componentes. Mais especificamente, tempos até falha e suspensões (tempos de operação dos itens que não falharam) e determinar uma distribuição matemática que melhor se adeque aos dados levantados. De posse da distribuição, derivam-se, então, os parâmetros que fornecem informação de vida do componente como, por exemplo, a confiabilidade, vida média (*mean time to failure* – MTTF), taxa de falhas, entre outros.

Este método é aplicável somente quando os dados são do tipo IID (*independently and identically distributed*), isto é, o componente ou sistema é não reparável, de acordo com O'Connor e Kleyner (2012). Quando o sistema é reparável, este possui falhas que dependem umas das outras. Colocando de outra maneira, as falhas sofrem influência de outras falhas. Esta condição expressa uma relação estocástica entre elas e deve ser representada por modelos matemáticos específicos que melhor representam esta condição, o que constitui um método de análise diferente da LDA (O'CONNOR e KLEYNER, 2012).

O'Connor e Kleyner (2012) destacam as maneiras de se construir uma distribuição: a construção da distribuição de dados de falha pode ser feita utilizando-se o método de plotagem de probabilidades (*probability plotting*) ou por meio de *software* especializado (ex: Weibull++ da Reliasoft). Como este segundo método é o mais comum devido à sua maior precisão, será apresentado somente o seu detalhamento.

A escolha do melhor modelo matemático, segundo O'Connor e Kleyner (2012), deve ser feita levando-se em consideração os seguintes aspectos:

- Melhor aderência dos dados ao modelo matemático;
- Experiência prévia de outras análises;
- Julgamento de engenharia.

É de fundamental importância lembrar que a análise de dados de vida é feita para componentes que operam em ambientes sujeitos aos estresses já conhecidos pelas disciplinas tradicionais de engenharia e que suas falhas são derivadas de processos físicos como fadiga, corrosão, desgaste. Portanto estes conhecimentos devem ser levados em consideração na escolha do modelo matemático adequado. Deve-se atentar para características como maturidade do sistema e onde este se encontra na curva da banheira, quais são os tipos de falha (modos de falha e qual a física da falha) e ao tamanho da amostra em relação à população do componente para saber qual é a representatividade dos dados (O'CONNOR e KLEYNER, 2012).

Em relação à maturidade dos componentes analisados, segundo O'Connor e Kleyner (2012), se o modelo Weibull for selecionado, pode-se determinar o comportamento da taxa de falha a partir do parâmetro β ou parâmetro de forma. Para $\beta<1$, a taxa de falha será decrescente, o que indica falhas relacionadas a defeitos de fabricação ou produto com baixa maturidade. Entretanto, se os dados forem provenientes de um componente maduro, com uma grande quantidade de horas de operação acumuladas, então se deve reanalisar o caso e experimentar outras distribuições. É necessário, também, neste caso, investigar se houve alguma modificação no processo fabril: analisar se há algum problema de qualidade ou verificar a variação na montagem dos componentes. Para $\beta\approx1$, o comportamento da taxa de falha será constante. Componentes eletrônicos costumam apresentar taxa de falha constante Entretanto, se não for um componente eletrônico, pode-se suspeitar da existência de múltiplos modos de falha no conjunto de dados ou, até mesmo, questionar a procedência dos dados de tempo até falha se for, por exemplo, um componente mecânico, que por natureza sofre desgaste (taxa de falha crescente). A taxa de falha constante também pode ser a indicação de falha causada por eventos externos, como uso e/ou manutenção inadequados. Para $\beta>1$,

as falhas se caracterizam por envelhecimento ou desgaste. O comportamento da taxa de falha será crescente; quanto maior a idade maior a quantidade de falhas. Em todos estes casos, deve-se sempre levar em consideração as peculiaridades de cada distribuição e se estas estão de acordo com a característica das falhas e onde elas se encaixam na curva da banheira. A distribuição exponencial sempre apresentará taxa de falha constante. Por outro lado, a normal (gaussiana) tem a característica de taxa de falha crescente e a lognormal molda um pico inicial com posterior comportamento decrescente da taxa de falha (O'CONNOR e KLEYNER, 2012).

3.1.1 Funções de Distribuição Contínua

Amostrando-se valores de uma variável aleatória contínua é possível construir o histograma desta população. Fazendo-se sucessivas medições, com cada vez mais amostras e reduzindo-se os intervalos do gráfico, o histograma tenderá a formar a curva que descreve a função densidade de probabilidade (*probability density function* – PDF) ou simplesmente a distribuição dos valores. A área abaixo da PDF é igual à unidade, uma vez que descreve o total de probabilidades dos valores possíveis da variável aleatória contínua "x" (O'CONNOR e KLEYNER, 2012).

$$\int_{-\infty}^{\infty} f(x)\,dx = 1 \qquad \text{Equação 2}$$

A probabilidade de um valor dentro de um intervalo determinado pelos valores "x_1" e "x_2" será a área delimitada por este intervalo, segundo O'Connor e Kleyner (2012).

$$P(x_1 < x < x_2) = \int_{x_1}^{x_2} f(x)\,dx \qquad \text{Equação 3}$$

O'Connor e Kleyner (2012) definem a função distribuição acumulada (*cumulative distribution function* - CDF), F(x), como aquela que provê a probabilidade de um valor ficar entre -∞ e x, e é definida a seguir:

$$F(x) = \int_{-\infty}^{x} f(x)\,dx \qquad \text{Equação 4}$$

F(x) ou F(t) é denominada "função de não confiabilidade" quando se trata de falha. Pode ser interpretada como sendo a probabilidade de falha acumulada antes de um valor de "x" ou de um valor de tempo t, comumente utilizado para falha de componentes.

A função confiabilidade, R(x) ou R(t), se traduz na probabilidade acumulada de um item não falhar antes de um valor "x" ou de um valor de tempo t. Segundo Dhillon (1999), a função confiabilidade é expressa como:

$$R(t) = 1 - F(t) = \int_{t}^{\infty} f(t)\,dt \qquad \text{Equação 5}$$

A função *hazard rate* pode ser definida, de acordo com Dhillon (1999), como:

$$\lambda(t) = \frac{f(t)}{R(t)} \qquad \text{Equação 6}$$

O valor de *mean time to failure* (MTTF) pode ser obtido por meio da Equação 7, segundo a norma MIL-STD-338B:

$$MTTF = \int_0^{\infty} t.f(t)\,dt \qquad \text{Equação 7}$$

3.1.2 Distribuição Exponencial

A distribuição exponencial é definida como a mais importante distribuição no área da confiabilidade, segundo a norma MIL-STD-338B. Ainda, segundo esta norma, são listadas as seguintes vantagens da distribuição exponencial:

- Contém somente um parâmetro de fácil estimação (λ).
- É matematicamente simples.
- Possui aplicabilidade bastante ampla.
- Possui característica aditiva, isto é, a soma de um número de variáveis independentes distribuídas exponencialmente é distribuída exponencialmente.
- Itens descritos por esta equação possuem taxa de falha constante.

A MIL-STD-338B define a função densidade de probabilidade (PDF) e a função confiabilidade, R(t), da distribuição exponencial como seguem:

$$f(t) = \lambda.e^{-\lambda t} \qquad \text{Equação 8}$$

$$R(t) = e^{-\lambda t} \qquad \text{Equação 9}$$

Com as Equações 5 e 9, tem-se, de acordo com Dhillon (1999):

$$F(t) = 1 - e^{-\lambda t} \qquad \text{Equação 10}$$

Por meio das equações 6, 8 e 9, mostra-se a característica de taxa de falha constante da equação 11, segundo a norma MIL-STD-338B:

$$h(t) = \frac{f(t)}{R(t)} = \frac{\lambda . e^{-\lambda t}}{e^{-\lambda t}} = \lambda$$ Equação 11

A relação entre taxa de falha (λ) e MTBF (*mean time between failure*) é uma característica muito importante da distribuição exponencial e pode ser vista abaixo, de acordo com a MIL-STD-338B:

$$MTBF = \frac{1}{\lambda}$$ Equação 12

3.1.3 Distribuição Weibull

A fórmula da função densidade de probabilidade da distribuição de Weibull com dois parâmetros é mostrada a seguir, de acordo com a MIL-STD-338B:

$$f(t) = \frac{\beta}{\eta}\left(\frac{t}{\eta}\right)^{\beta-1} e^{-\left(\frac{t}{\eta}\right)^{\beta}}$$ Equação 13

Onde:

t: variável aleatória contínua

β: parâmetro de forma ou inclinação

η: parâmetro de escala ou também chamado de vida característica (representa a chance de que 63,2% dos componentes falhem)

As funções confiabilidade, R(t), e hazard rate da distribuição Weibull, de acordo com a norma MIL-STD-338B, podem ser vistas abaixo:

$$R(t) = e^{-\left(\frac{t}{\eta}\right)^{\beta}}$$ Equação 14

$$\lambda(t) = \frac{\beta}{\eta}\left(\frac{t}{\eta}\right)^{\beta-1}$$ Equação 15

A distribuição Weibull é muito versátil e se molda a vários tipos de conjunto de dados, graças a seu parâmetro β. A norma MIL-STD-338B traz um resumo das distribuições que a Weibull é capaz de modelar dependendo do valor do parâmetro β.

Quadro 3.1 - Distribuições modeladas pela distribuição Weibull de acordo com o valor do parâmetro β

Valor de β	**Distribuição modelada**
β < 1	Gama
β = 1	Exponencial
β = 2	Lognormal
β = 3,5	Normal

Fonte: MIL-STD-338B

Outra característica da distribuição Weibull é que ela é capaz de representar conjuntos de dados com os três comportamentos de taxa de falha da curva da banheira: decrescente, constante e crescente. O'Connor e Kleyner (2012) abordam estas características, conforme Quadro 3.2:

Quadro 3.2 - Características da taxa de falha e do comportamento do tipo de falha para cada faixa de valor do parâmetro β da distribuição Weibull

Valor de β	Taxa de falha	Comportamento
β < 1	Decrescente	Está geralmente associado à falhas do tipo mortalidade infantil. Frequentemente, corresponde à falhas originadas na fabricação ou registradas logo após a produção.
β = 1	Constante	Está geralmente associado à vida útil. Frequentemente corresponde à seção intermediária da vida útil do produto e pode ser resultado de falhas aleatórias ou de combinação de mais de um modo de falha.
β > 1	Crescente	Está geralmente associado ao processo de desgaste, correspondendo à vida útil final do produto. Se registrado no início do ciclo de vida do produto, pode ser um sinal de um sério problema de projeto ou um problema de análise de dados.

Fonte: O'Connor e Kleyner (2012)

Devido à versatilidade da distribuição Weibull, em função do parâmetro β, ela é largamente utilizada para modelar conjuntos de dados de falha de componentes e, por isso se destaca no campo da confiabilidade, assim como a distribuição exponencial.

3.2 *MÉTODO MEAN TIME BETWEEN FAILURE*

Esta métrica é aplicada para itens reparáveis, isto é, itens que são substituídos após falha, enviados para reparo e que retornam para operação. Quando se utiliza MTBF como métrica, assume-se que a taxa de falha do item é constante, como enfatiza a norma MIL-STD-338B.

A equação do MTBF pode ser descrita, de acordo com a norma MIL-STD-338B, como:

$$\mathrm{MTBF} = \frac{\mathrm{T(t)}}{\mathrm{r}} \qquad \text{Equação 16}$$

Onde:

T(t) = tempo total de operação de um componente
r = número de falhas deste componente

A equação do MTBF para a situação onde um número de itens reparáveis é testado por um período de tempo com a substituição imediata dos itens falhados, segundo Benbow e Broome (2009), é dada por:

$$MTBF = \frac{n.m}{r} \qquad \text{Equação 17}$$

Onde:

n = número de itens
m = número de horas de teste
r = número de falhas do item

Este cálculo é muito utilizado pela facilidade de obtenção das informações de horas de voo da frota e do total de falhas do componente em estudo. No entanto, esta métrica não revela a idade do item e, sim a média de tempo entre remoções decorrentes de falha. O valor calculado pode se aproximar da média obtida por meio do método de análise de dados de vida, contudo para muitos casos pode haver discrepâncias significativas, principalmente quando o item tem comportamento de taxa de falha crescente ou decrescente. Outro fator que pode entregar um valor distorcido é a capacidade de confirmação das falhas pelas oficinas e laboratórios. Muitas vezes, o item retorna para o fabricante e o resultado das análises não confirma a falha (*no fault found* – NFF). O fato de a falha entrar ou não para o cálculo é diretamente proporcional à qualidade do resultado. Portanto, deve-se utilizar esta métrica com cautela.

3.3 *MÉTODO MEAN TIME BETWEEN UNSCHEDULED REMOVALS*

A métrica MTBUR é calculada dividindo-se o total de horas voadas acumuladas pelas unidades de um determinado componente em um período específico pelo número de remoções não programadas que ocorreram dentro do mesmo período (ATA Spec 2000 chapter 13).

$$\text{MTBUR} = \frac{\text{horas de voo totais da frota x número de unidades instaladas na aeronave}}{\text{número de remoções não programadas durante o mesmo período}} \quad \text{Equação 18}$$

O valor de MTBUR será sempre igual ou menor do que a métrica MTBF. Isto porque para o cálculo de MTBUR são utilizadas todas as remoções não programadas de um componente, com ou sem falha. Geralmente, remoções sem falha são provenientes de atividades de manutenção como pesquisas de pane (*troubleshooting*), onde não se sabe a causa da parada do sistema. Componentes são substituídos até que o sistema volte a funcionar corretamente. Dentre as remoções efetuadas, não se sabe qual componente estava falhado, até que a oficina de reparo do fabricante confirme a falha. No caso de não encontrar falha, o fabricante do componente registra no relatório da análise realizada que não foi possível reproduzir a falha.

3.4 COMPARAÇÃO ENTRE MTTF, MTBF E MTBUR

O MTBF gera um valor de vida média a partir de horas da frota divididas pelas falhas, conforme mostrou a Equação 16. O MTBUR também gera um valor médio, porém a partir de horas da frota divididas pelas remoções, conforme Equação 18. Tanto um como outro, assumem, portanto que o valor da taxa de falha é constante. De forma distinta, o método LDA, conforme descrito na seção 0, utiliza os tempos até falha e suspensões e molda uma distribuição matemática, a que melhor se adequar aos dados do componente. Desta distribuição então, por meio da Equação 7, calcula-se o MTTF. Neste caso, a taxa de falha pode ser decrescente, constante ou crescente. Será decorrência do comportamento da falha e da distribuição escolhida. Este processo se define conforme o tipo de componente (ex: mecânico, eletrônico, etc.) e em qual situação se encontra em relação à fase de vida

(infância – falhas prematuras, vida útil – falhas aleatórias ou envelhecimento – falhas por desgaste).

Para cada método, como explicado no parágrafo anterior, utilizam-se informações distintas. O Quadro 3.3 mostra um resumo do que é necessário para cada método:

Quadro 3.3 - Resumo das informações necessárias para utilização dos métodos LDA, MTBF e MTBUR

Informação	**LDA**	**MTBF**	**MTBUR**
Tempos até falha *	Necessita	Não necessita	Não necessita
Suspensões *	Necessita	Não necessita	Não necessita
Horas de voo da frota	Não necessita	Necessita	Necessita
Número de remoções	Não necessita	Não necessita	Necessita
Número total de falhas	Não necessita	Necessita	Não necessita
Confirmação da falha	Necessita	Necessita	Não necessita
Item não reparável **	Necessita	Não necessita	Não necessita

* estes dados devem ser coletados para cada componente

** ou primeira falha de item reparável

A seguir, é apresentado um exemplo de aplicação das três maneiras de se calcular um valor médio para um componente eletromecânico. O Quadro 3.4 traz informações de uma frota de aeronaves e respectivos dados de vida de um de seus componentes.

Quadro 3.4 - Dados de falha de componente eletromecânico

Aeronave #	Entrega da Aeronave	Média de horas de voo por mês	Horas de voo acumuladas	Posição do componente	Falha	Tempo até falha	Suspensão
1	1-fev-12	7,5	13.583	1.1		0	13.583
			13.583	1.2		0	13.583
2	1-abr-12	8	14.008	2.1	x	11.224	2.784
			14.008	2.2		0	14.008
3	1-mai-13	7,5	10.170	3.1		0	10.170
			10.170	3.2		0	10.170
4	1-set-13	8	9.864	4.1	x	8.630	1.234
			9.864	4.2		0	9.864
5	1-fev-14	7,2	7.776	5.1		0	7.776
			7.776	5.2	x	5.369	2.407
6	1-jun-14	7,2	6.912	6.1	x	5.098	1.814
			6.912	6.2		0	6.912
7	20-ago-14	7	6.160	7.1		0	6.160
			6.160	7.2		0	6.160
8	9-dez-14	7,1	5.460	8.1	x	3.942	1.518
			5.460	8.2		0	5.460
9	1-mar-15	6,9	4.740	9.1		0	4.740
			4.740	9.2	x	3.600	1.140
10	1-jul-15	6,7	3.786	10.1	x	3.782	4
			3.786	10.2		0	3.786
11	1-ago-15	6,8	3.631	11.1		0	3.631
			3.631	11.2		0	3.631
12	1-dez-15	7	2.884	12.1		0	2.884
			2.884	12.2		0	2.884
13	1-fev-16	6,5	2.275	13.1		0	2.275
			2.275	13.2		0	2.275
14	1-mar-16	6,7	2.151	14.1		0	2.151
			2.151	14.2		0	2.151
15	1-mai-16	6,5	1.690	15.1		0	1.690
			1.690	15.2		0	1.690
16	10-mai-16	6,4	1.606	16.1		0	1.606
			1.606	16.2		0	1.606
17	1-ago-16	6	1.008	17.1		0	1.008
			1.008	17.2		0	1.008

Aeronave #	Entrega da Aeronave	Média de horas de voo por mês	Horas de voo acumuladas	Posição do componente	Falha	Tempo até falha	Suspensão
18	1-set-16	5,9	808	18.1		0	808
			808	18.2		0	808
19	1-nov-16	5,9	448	19.1		0	448
			448	19.2		0	448
20	1-jan-17	5,8	87	20.1		0	87
			87	20.2		0	87

Utilizando-se a Equação 16, calcula-se o valor da métrica MTBF:

$$\mathrm{MTBF} = \frac{198.094}{7} = 28.299$$

Para calcular o valor da métrica MTBUR é necessário conhecer o número de remoções do componente em questão que aconteceram na vida da frota. Como este exemplo é fictício, elaborou-se o Quadro 3.5 para simular cenários diferentes:

Quadro 3.5 – Número de remoções e respectivo valor de MTBUR

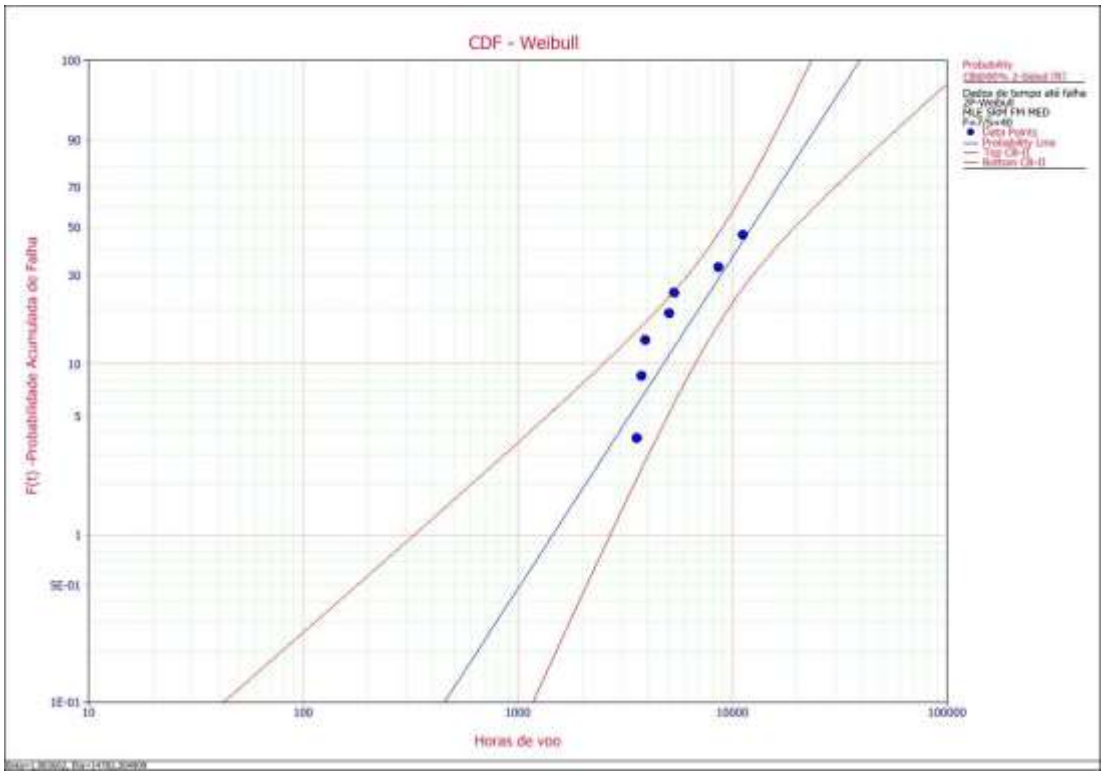
Remoções	MTBUR
10	19.809,44
15	13.206,29
20	9.904,72
25	7.923,78
30	6.603,15
35	5.659,84
40	4.952,36

Para o caso onde a quantidade de remoções é aproximadamente 2,85 vezes maior que o número de falhas (20 remoções), o cálculo da métrica MTBUR, utilizando-se a Equação 18, é o seguinte:

$$\mathrm{MTBUR} = \frac{198.094}{20} = 9.947$$

Para o método LDA, utilizou-se o *software* Weibull ++ 9. Com os valores do Quadro 3.4, calculou-se a distribuição Weibull com dois parâmetros pelo método *Maximum Likelihood Estimator* (MLE). O valor resultante para o parâmetro β (beta) foi 1,9836 e o valor resultante para o parâmetro η (eta) foi de 14782,30.

Gráfico 3.1 - Probabilidade acumulada de falha do exemplo de comparação entre MTTF, MTBF e MTBUR



O cálculo da distribuição Weibull para este exemplo é possível, pois os dados são referentes às primeiras falhas do componente em questão, conforme descrito na seção 0. Este é um item reparável, ou seja, quando há a falha, este é enviado para oficina, reparado e reenviado para o campo, retornando à operação. Pode-se utilizar o método LDA para as primeiras falhas somente, pois uma vez que a primeira falha ocorreu, no reparo são substituídas apenas algumas partes do item. Quando retorna à operação, possui partes com vidas diferentes. Dizemos que o item retornou *as bad as old*. Para este contexto, utilizam-se outros métodos de cálculo.

Para itens não reparáveis ou primeira falha de itens reparáveis, a vida média recebe o nome de *mean time to failure* (MTTF). O componente eletromecânico do exemplo apresentou o valor de MTTF, gerado a partir do método LDA, de 13.102,53.

Pode-se perceber diferença sensível entre os três valores: MTTF, MBTF e MTBUR. A métrica que mais precisamente estima a vida do componente é a MTTF, pois deriva-se da distribuição que modela os dados de vida.

A partir da Equação 12, obtêm-se a taxa de falha a partir do valor de MTBF:

$$\lambda = \frac{1}{28.299} = 3{,}53\text{x}10^{-5}$$

O valor de taxa de falha gerado pelo método LDA (via *software*) é $1{,}19\text{x}10^{-4}$.

O valor de MTBUR calculado para 20 remoções é menor que o valor de MTBF, portanto se utilizado para calcular a "taxa de falha" (o valor MTBUR contém remoções sem falha, portanto ele não implica diretamente em uma taxa de falha. No entanto, poderia ser utilizado de forma a obter um valor mais conservador), esta seria maior que a gerada a partir do MTBF.

3.5 MEDIDAS DE IMPORTÂNCIA

Segundo o *Fault Tree Handbook* da NASA, as medidas de importância são de suma relevância para se avaliar os resultados de uma análise de árvore de falha. Estas estabelecem a significância para todos os eventos da árvore com relação à sua contribuição para a probabilidade do evento topo. Tanto os eventos intermediários quanto os eventos básicos podem ser priorizados de acordo com sua importância. As medidas de importância também podem ser calculadas de forma a mostrar a variação de sensibilidade da probabilidade do evento topo, tanto um aumento quanto uma redução, para cada evento na árvore de falha. Pode-se calcular ambas as medidas de importância, a absoluta e a relativa.

O que se mostra útil, geralmente, sobre as medidas de importância é que relativamente poucos eventos contribuem para a probabilidade do evento topo, de acordo com o *Fault Tree Handbook* da NASA. Em várias análises de árvore de falha realizadas, menos de 20% dos eventos básicos se mostraram importantes contribuidores, respondendo por mais de 90% da probabilidade do evento topo. Ademais, a importância dos eventos na árvore de falha, geralmente, se agrupam em ordens de magnitude diferentes. Nestes casos, as importâncias são tão

dramaticamente diferentes que não dependem da precisão dos dados de vida dos componentes.

Além de prover a significância dos contribuidores, as medidas de importância podem ser usadas para alocar recursos. O *Fault Tree Handbook* da NASA exemplifica que estes recursos podem ser testes e ações de manutenção, inspeção, atualização e controle de qualidade. Com a ranque de importâncias, os recursos podem ser ajustados de forma a minimizar os gastos totais enquanto a probabilidade do evento topo é mantida, provendo, desta maneira, uma condição ganha-ganha. Outra forma de utilizar a informação proveniente das medidas de importância é destinar os recursos para os itens que podem minimizar a probabilidade do evento topo. Isso auxilia os tomadores de decisão a atingir grandes reduções de custo, por meio de uma avaliação objetiva, utilizando métodos sistemáticos para complementar as informações subjetivas.

As otimizações citadas acima foram realizadas em várias indústrias para reduzir os recursos em até 40% enquanto, ao mesmo tempo, mantém ou diminuem a probabilidade do evento topo. Uma das vantagens desta abordagem de alocação ótima é que importâncias de risco relativas podem ser utilizadas, as quais mostram menos incertezas que as absolutas. As incertezas destas medidas também podem ser equacionadas (*Fault Tree Handbook* – NASA – 2002).

As medidas importâncias também podem ser utilizadas para definir tempos de parada e de reparo permitidos e focar em atividades de diagnóstico voltadas a identificar as causas do evento topo e atividades de projeto e requisitos destinadas ao desenvolvimento de projetos mais robustos (*Fault Tree Handbook* – NASA – 2002).

Quatro tipos básicos de medidas de importância podem ser calculados para os diferentes tipos de aplicações descritas acima. São eles: Fussell-Vesely (F-V), *Risk Reduction Importance* ou *Risk Reduction Worth* (RRW), *Risk Increase Importance* ou *Risk Achievement Worth* (RAW) e Birnbaum's *Importance Measure* (Bi ou BM).

3.5.1 Fussell-Vesely (F-V)

O método Fussell-Vesely (FV) mede o percentual de contribuição global dos grupos de corte que contém um evento básico de interesse em relação ao risco total (*Idaho National Laboratory*). Esta medida de importância é, algumas vezes, chamada de “maiores contribuidores de importância”. Ambas as medidas, relativa e absoluta, de Fussel-Vesely são possíveis de serem determinadas para cada evento modelado na árvore de falha, não apenas para os eventos básicos, mas para os eventos intermediários (*Fault Tree Handbook* – NASA – 2002). A Equação 19 representa o método Fussel-Vesely, de acordo com o *Idaho National Laboratory*.

$$FV_{x_i} = \frac{\mathrm{F(i)}}{\mathrm{F(x)}} \qquad \text{Equação 19}$$

Onde:

F(i) é o risco apenas daqueles conjuntos de corte que contêm o evento x_i.
F(x) é o risco total de todos os conjuntos de corte.

Calcula-se o valor de FV de um evento básico (x_i) encontrando o valor dos conjuntos de corte que contêm o evento básico de interesse (x_i) e dividindo-se pelo valor de todos os conjuntos de corte que representam o risco total. O resultado do cálculo da medida de importância FV variará entre 0 e 1 (0% e 100%) (*Idaho National Laboratory*).

3.5.2 *Risk Reduction Importance* (RRI) ou *Risk Reduction Worth* (RRW)

Significa o valor de redução na probabilidade do evento topo para a condição onde se assume que um dado evento não ocorrerá. Em outras palavras, mede a quantidade que o risco total diminuirá se a probabilidade de falha de um evento básico fosse zero (“0”), ou seja, nunca falhar (*Idaho National Laboratory*). Esta medida está relacionada à medida anterior, Fussel-Vesely, e revela a máxima redução da probabilidade do evento topo ao se melhorar a confiabilidade de um item específico da árvore. Ambos os valores, absoluto e relativo, desta medida podem ser

determinados para cada evento contido no modelo (*Fault Tree Handbook* – NASA – 2002). A Equação 20 revela o cálculo do valor de RRW (*Idaho National Laboratory*). A Equação 21 revela o cálculo do valor de RRI (*Idaho National Laboratory*).

$$RRR_{x_i} = RRW_{x_i} = \frac{\mathrm{F(x)}}{\mathrm{F(0)}} \qquad \text{Equação 20}$$

$$RRI_{x_i} = \mathrm{F(x)} - \mathrm{F(0)} \qquad \text{Equação 21}$$

Onde:

F(x) é o risco total de todos os conjuntos de corte e todos os eventos básicos estão em sua probabilidade de falha nominal.

F(0) é o risco total com a probabilidade x_i do evento básico definida como zero “0”.

Calcula-se o valor de RRR de um evento básico (x_i) como a razão (*Risk Reduction Ratio*) ou diferença (*Risk Reduction Importance)* entre o valor de todos os conjuntos de corte representando o risco total e o valor do risco total com a probabilidade de falha para o evento básico de interesse (x_i) definido como zero “0”. O resultado do *Risk Reduction Ratio* varia entre “0” e “∞”. Esta medida de importância entrega a mesma classificação que a medida Fussell-Vesely (*Idaho National Laboratory*).

3.5.3 *Risk Increase Importance* (RII) ou *Risk Achievement Worth* (RAW)

Significa o valor de aumento na probabilidade do evento topo para a condição onde se assume que um dado evento ocorrerá. Em outras palavras, mede a quantidade que o risco total aumentaria se a probabilidade de falha de um evento básico fosse um (“1”) (por exemplo, se o componente estivesse fora de serviço ou falhado) (*Idaho National Laboratory*). Esta medida revela onde atividades de prevenção devem ser feitas para assegurar que um evento não ocorra. Uma vez que

as falhas com os maiores valores de RAW tem os maiores impactos no sistema, estas são as falhas que devem ser prevenidas. Esta informação alimenta, também, os planos de contingência (*Fault Tree Handbook* – NASA – 2002).

$$RRR_{x_i} = RRW_{x_i} = \frac{\mathrm{F(x)}}{\mathrm{F(0)}} \qquad \text{Equação 22}$$

$$RII_{x_i} = \mathrm{F(x)} - \mathrm{F(0)} \qquad \text{Equação 23}$$

Onde:

F(x) é o risco total de todos os conjuntos de corte e todos os eventos básicos que estão em sua probabilidade de falha nominal.

F(1) é o risco total com a probabilidade x_i do evento básico definida como um “1”.

Calcula-se o valor de RIR de um evento básico (x_i) como a razão (*Risk Increase Ratio*) ou diferença (*Risk Increase Importance)* entre o valor do risco total com a probabilidade de falha para o evento básico de interesse (x_i) definido como um “1” e o risco total. A medida em forma de razão é conhecida como *Risk Achievement Worth* (RAW) e seu resultado é sempre maior que um (“1”) (*Idaho National Laboratory*).

3.5.4 Birnbaum’s *Importance Measure* (Bi ou BM)

Significa a taxa de aumento na probabilidade do evento topo como resultado da mudança da probabilidade de um determinado evento (*Idaho National Laboratory*). Em outras palavras, mede a taxa de mudança no risco total como resultado de mudanças na probabilidade de um evento básico (*Fault Tree Handbook* – NASA – 2002).

$$B_{i_x} = \frac{\partial \mathrm{F(x)}}{\partial \mathrm{x}} \qquad \text{Equação 24}$$

Onde:

F(x) é o risco total de todos os conjuntos de corte e todos os eventos básicos que estão em sua probabilidade de falha nominal.

∂/∂x é a primeira derivada da expressão de risco em relação ao evento básico de interesse (x_i).

Quando a expressão de risco tem uma forma linear:

$$B_{i_{xi}} = F(1) - F(0) \qquad \text{Equação 25}$$

Onde:

F(1) é o risco total com a probabilidade x_i do evento básico definida como um “1”.

F(0) é o risco total com a probabilidade x_i do evento básico definida como zero “0”.

BM é equivalente a uma análise de sensibilidade e pode ser obtido calculando-se a probabilidade do evento topo após configurar o valor do evento em estudo para “1” e, depois subtraindo a probabilidade do evento topo pela probabilidade calculada com o evento em estudo configurado com o valor “0”. Em função da maneira como o BM é formulado, não leva em consideração a probabilidade do evento (*Fault Tree Handbook* – NASA – 2002).

3.6 SÍNTESE E CONCLUSÃO DO CAPÍTULO

No capítulo 3 foi apresentado o referencial teórico para a aplicação do método de identificação de componentes e grupos de corte críticos em árvores de falha. Os seguintes tópicos foram abordados:

- Análise de dados de vida
    - Funções de distribuição contínua
    - Distribuição Exponencial
    - Distribuição Weibull

- Método *mean time between failure*
- Método *mean time between unscheduled removals*
- Comparação entre MTTF, MTBF e MTBUR
- Medidas de importância

A análise de árvore de falha utilizada nos projetos da aviação toma como base a distribuição exponencial. Por meio do valor de MTBF dos componentes determina-se a taxa de falha e, assim chega-se ao valor de probabilidade dos eventos básicos por meio da Equação 10. As medidas de importância, por sua vez, são utilizadas para a elaboração do ranque dos eventos básicos que mais contribuem para o evento topo da árvore de falha. Com este ranque é possível selecionar os itens mais relevantes por meio do conceito de Pareto, que mostra a relação de poucos eventos contribuindo para uma parte significativa da probabilidade do evento topo.

Após a determinação da lista de eventos que devem ser monitorados, os conceitos de análise de dados de vida, MTBF e MTBUR provêm a base teórica para o cálculo da taxa de falha dos componentes durante a vida em operação. A distribuição Weibull e Exponencial são as mais utilizadas. A primeira serve de base para a análise de dados de vida e a segunda para o cálculo do MTBF e MTBUR.

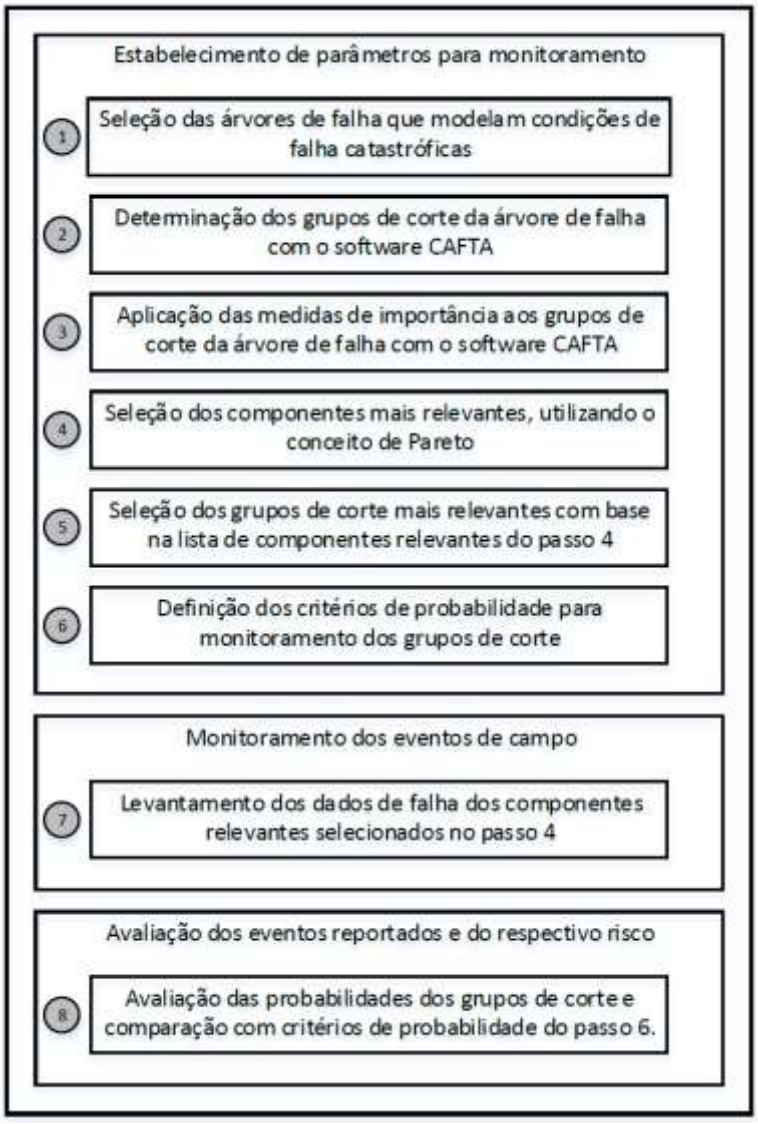
O próximo capítulo engloba todos os cálculos e análises para se aplicar o método proposto nesta monografia. Utilizará como base o referencial teórico abordado no capítulo 3. Ao todo, foram selecionadas seis árvores de falha de seis sistemas diferentes. O método será apresentado em detalhes para a árvore de falha do sistema 1. Para as demais árvores de falha, serão mostrados o ranque de contribuição dos componentes para o evento topo calculado pela medida de importância Fussel-Vesely, os componentes selecionados e a porcentagem de itens monitorados em relação ao total de itens existentes na árvore de falha em estudo. Ao final, haverá um resumo do total de itens de todas as árvores de falha e o número final de itens monitorados, a fim de enfatizar o potencial de otimização que é possível atingir com o método para a implantação de um processo de monitoramento contínuo de segurança.

4 DESENVOLVIMENTO

4.1 APLICAÇÃO DO MÉTODO

Este capítulo da monografia trará em detalhes a execução do método de identificação de componentes e grupos de corte críticos em árvores de falha descrito no capítulo 2, seção 2.7. Fará, também, a aplicação do referencial teórico do capítulo 3. A Figura mostra os passos do método.

Figura 4.1 - Etapas do método de identificação de componentes e grupos de corte críticos em árvores de falha

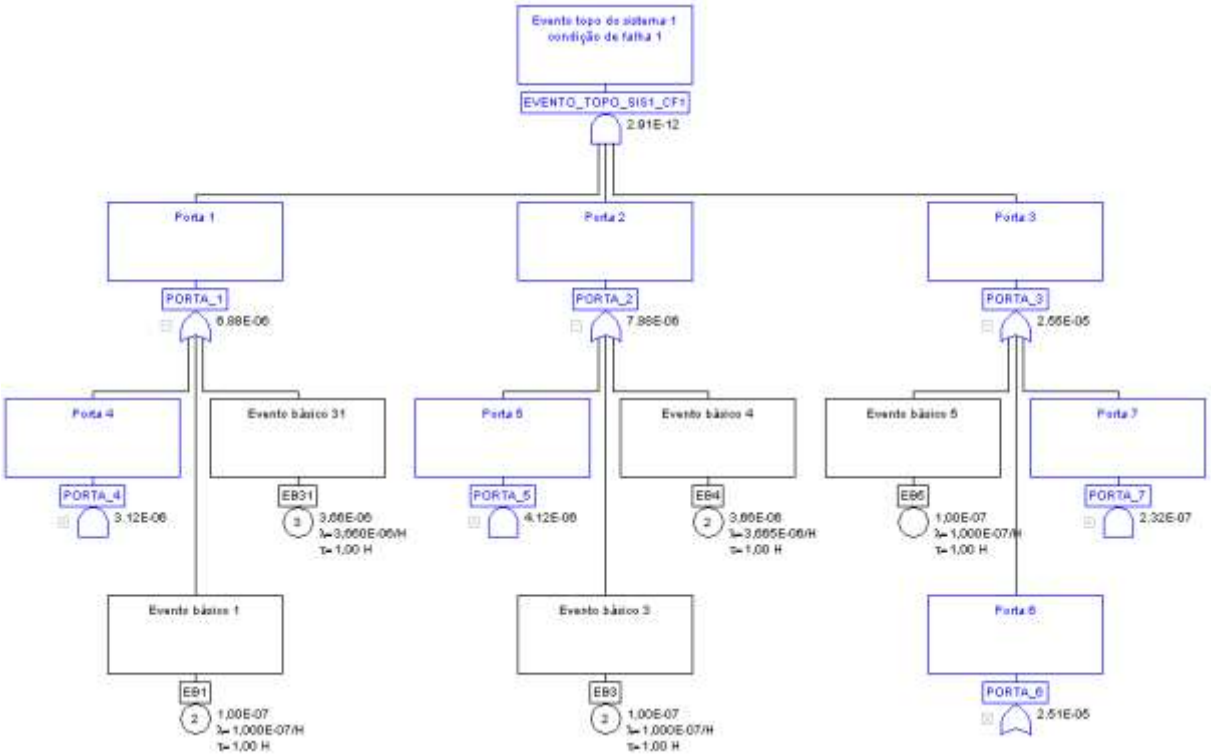


O primeiro passo do método é o estabelecimento de parâmetros para monitoramento. Para estabelecer os parâmetros, algumas etapas devem ser cumpridas. O início do processo se resume à seleção das árvores de falha que modelam as condições de falha classificadas com severidade catastrófica. Para executar o método, foram selecionadas 6 árvores de falha de 6 sistemas diferentes.

A próxima etapa para se estabelecer os parâmetros de monitoramento é a seleção dos componentes mais relevantes. Esta etapa divide-se em três passos. O primeiro é a determinação dos grupos de corte da árvore de falha por meio do *software* CAFTA. O segundo passo é a aplicação das medidas de importância aos grupos de corte das árvores de falha, também por meio do *software* CAFTA. O terceiro passo é a seleção dos componentes mais relevantes, utilizando o conceito de Pareto. Como o número de árvores de falha é grande, o processo é demonstrado com apenas uma árvore de falha. Para as demais árvores de falha serão apresentados somente os resultados.

A árvore de falha a partir da qual o método será detalhado por ser vista, resumidamente, na Figura 4.2.

Figura 4.2 - Árvore de falha do sistema 1



A partir da árvore de falha, determinam-se os grupos de corte por meio do *software* CAFTA. No Quadro 4.1 é mostrado o resultado dos grupos de corte (foram gerados 5197 grupos de corte. Mostra somente as primeiras 10 combinações):

Quadro 4.1 - Grupos de corte da árvore de falha do sistema 1

#	Probabilidade do grupo de corte	Probabilidade do evento	Taxa de falha	Tempo de exposição	Evento básico	Descrição
1	2,12E-13	1,66E-04	1,66E-04	1 hora de voo	EB33	Evento básico 33
		7,68E-06	7,68E-06	1 hora de voo	EB63	Evento básico 63
		1,66E-04	1,66E-04	1 hora de voo	EB7	Evento básico 7
2	1,28E-13	1,66E-04	1,66E-04	1 hora de voo	EB33	Evento básico 33
		7,68E-06	7,68E-06	1 hora de voo	EB63	Evento básico 63
		1,00E-04	1,00E-04	1 hora de voo	EVENTO_EXTERNO_1	Evento externo 1
3	1,28E-13	7,68E-06	7,68E-06	1 hora de voo	EB63	Evento básico 63
		1,66E-04	1,66E-04	1 hora de voo	EB7	Evento básico 7
		1,00E-04	1,00E-04	1 hora de voo	EVENTO_EXTERNO_2	Evento externo 2
4	9,92E-14	1,66E-04	1,66E-04	1 hora de voo	EB33	Evento básico 33
		3,60E-06	3,60E-06	1 hora de voo	EB49	Evento básico 49
		1,66E-04	1,66E-04	1 hora de voo	EB7	Evento básico 7
5	8,41E-14	1,66E-04	1,66E-04	1 hora de voo	EB33	Evento básico 33
		7,00E-02	2,00E-06	35.000 horas de voo	EB51	Evento básico 51
		4,36E-05	4,36E-05	1 hora de voo	EB55	Evento básico 55
		1,66E-04	1,66E-04	1 hora de voo	EB7	Evento básico 7
6	8,41E-14	1,66E-04	1,66E-04	1 hora de voo	EB33	Evento básico 33
		7,00E-02	2,00E-06	35.000 horas de voo	EB51	Evento básico 51
		4,36E-05	4,36E-05	1 hora de voo	EB56	Evento básico 56
		1,66E-04	1,66E-04	1 hora de voo	EB7	Evento básico 7
7	7,68E-14	7,68E-06	7,68E-06	1 hora de voo	EB63	Evento básico 63
		1,00E-04	1,00E-04	1 hora de voo	EVENTO_EXTERNO_1	Evento externo 1
		1,00E-04	1,00E-04	1 hora de voo	EVENTO_EXTERNO_2	Evento externo 2
8	5,98E-14	1,66E-04	1,66E-04	1 hora de voo	EB33	Evento básico 33
		3,60E-06	3,60E-06	1 hora de voo	EB49	Evento básico 49
		1,00E-04	1,00E-04	1 hora de voo	EVENTO_EXTERNO_1	Evento externo 1
9	5,98E-14	3,60E-06	3,60E-06	1 hora de voo	EB49	Evento básico 49
		1,66E-04	1,66E-04	1 hora de voo	EB7	Evento básico 7
		1,00E-04	1,00E-04	1 hora de voo	EVENTO_EXTERNO_2	Evento externo 2
10	5,07E-14	7,00E-02	2,00E-06	35.000 horas de voo	EB51	Evento básico 51
		4,36E-05	4,36E-05	1 hora de voo	EB55	Evento básico 55
		1,66E-04	1,66E-04	1 hora de voo	EB7	Evento básico 7
		1,00E-04	1,00E-04	1 hora de voo	EVENTO_EXTERNO_2	Evento externo 2

Em seguida, aplica-se o cálculo das medidas de importância aos grupos de corte. A medida de importância revelará o ranking dos eventos, organizados do que

contribui com um maior risco para o evento topo até o que contribui para um menor risco para o evento topo. O Quadro 4.2 mostra o resultado do ranque.

Quadro 4.2 - Ranque de contribuição dos eventos básicos para o evento topo da árvore de falha do sistema 1

Evento básico	Probabilidade do evento	Fussel-Vesely	% de contribuição	Descrição
EB7	1,66E-04	4,91E-01	14,38%	Evento básico 7
EB33	1,66E-04	4,90E-01	14,35%	Evento básico 33
EB63	7,68E-06	2,97E-01	8,70%	Evento básico 63
EVENTO_EXTERNO_1	1,00E-04	2,96E-01	8,67%	Evento externo 1
EVENTO_EXTERNO_2	1,00E-04	2,95E-01	8,64%	Evento externo 2
EB51	7,00E-02	2,43E-01	7,12%	Evento básico 51
EB55	4,36E-05	2,06E-01	6,03%	Evento básico 55
EB56	4,36E-05	2,06E-01	6,03%	Evento básico 56
EB52	4,10E-02	1,41E-01	4,13%	Evento básico 52
EB49	3,60E-06	1,39E-01	4,07%	Evento básico 49
EB58	1,73E-06	6,65E-02	1,95%	Evento básico 58
EB19	2,19E-05	6,41E-02	1,88%	Evento básico 19
EB45	2,19E-05	6,41E-02	1,88%	Evento básico 45
EB12	1,41E-05	4,13E-02	1,21%	Evento básico 12
EB38	1,41E-05	4,12E-02	1,21%	Evento básico 38
EB53	1,19E-02	4,06E-02	1,19%	Evento básico 53
EB14	1,26E-05	3,66E-02	1,07%	Evento básico 14
EB40	1,26E-05	3,66E-02	1,07%	Evento básico 40
EB59	9,00E-07	3,43E-02	1,00%	Evento básico 59
EB8	6,14E-06	1,77E-02	0,52%	Evento básico 8
EB34	6,14E-06	1,77E-02	0,52%	Evento básico 34
EB54	2,91E-06	1,30E-02	0,38%	Evento básico 54
EB13	4,54E-06	1,28E-02	0,37%	Evento básico 13
EB39	4,54E-06	1,28E-02	0,37%	Evento básico 39
EB60	3,40E-07	1,27E-02	0,37%	Evento básico 60
EB32	4,00E-06	1,10E-02	0,32%	Evento básico 32
EB31	3,66E-06	1,03E-02	0,30%	Evento básico 31
EB4	3,66E-06	1,03E-02	0,30%	Evento básico 4
EB69	4,76E-04	8,56E-03	0,25%	Evento básico 69
EB6	3,00E-06	8,44E-03	0,25%	Evento básico 6

Evento básico	Probabilidade do evento	Fussel-Vesely	% de contribuição	Descrição
EB64	4,76E-04	8,44E-03	0,25%	Evento básico 64
EB61	1,30E-07	4,69E-03	0,14%	Evento básico 61
EB16	1,56E-06	4,17E-03	0,12%	Evento básico 16
EB43	1,56E-06	4,17E-03	0,12%	Evento básico 43
EB18	1,51E-06	3,98E-03	0,12%	Evento básico 18
EB42	1,51E-06	3,98E-03	0,12%	Evento básico 42
EB5	1,00E-07	3,57E-03	0,10%	Evento básico 5
EB17	1,29E-06	3,38E-03	0,10%	Evento básico 17
EB44	1,29E-06	3,38E-03	0,10%	Evento básico 44
EB15	1,06E-06	2,66E-03	0,08%	Evento básico 15
EB41	1,06E-06	2,66E-03	0,08%	Evento básico 41
EB62	6,00E-08	2,03E-03	0,06%	Evento básico 62
EB11	2,20E-07	5,25E-04	0,02%	Evento básico 11
EB36	2,20E-07	5,25E-04	0,02%	Evento básico 36
EB10	2,00E-07	4,50E-04	0,01%	Evento básico 10
EB35	2,00E-07	4,50E-04	0,01%	Evento básico 35
EB1	1,00E-07	1,13E-04	0,00%	Evento básico 1
EB3	1,00E-07	1,13E-04	0,00%	Evento básico 3
EB65	7,68E-06	1,13E-04	0,00%	Evento básico 65
EB50	1,00E-08	0,00E+00	0,00%	Evento básico 50
EB66	1,30E-07	0,00E+00	0,00%	Evento básico 66
EB67	2,00E-07	0,00E+00	0,00%	Evento básico 67
EB68	3,40E-07	0,00E+00	0,00%	Evento básico 68
EB70	1,00E-07	0,00E+00	0,00%	Evento básico 70

Os dez primeiros eventos correspondem a 82,12% do percentual de contribuição do risco para a ocorrência evento topo. A árvore de falha do sistema 1 contém 69 eventos, portanto a porcentagem de eventos monitorados será de 14,49%.

Os seguintes eventos devem ser monitorados, conforme mostra o Quadro 4.3:

Quadro 4.3 - Componentes que mais contribuem para o evento topo da árvore de falha do sistema 1

#	**Evento básico**
1	Evento básico 7
2	Evento básico 33
3	Evento básico 63
4	Evento externo 1
5	Evento externo 2
6	Evento básico 51
7	Evento básico 55
8	Evento básico 56
9	Evento básico 52
10	Evento básico 49

A próxima etapa está relacionada com os grupos de corte. Determinam-se quais os mais significativos, definindo aqueles que são compostos pela combinação dos componentes críticos. No Quadro 4.4 estão os grupos de corte compostos pela combinação dos componentes mais críticos.

Quadro 4.4 - Grupos de corte formados pelos eventos básicos que mais contribuem para o evento topo da árvore de falha do sistema 1

#	Probabilidade do grupo de corte	Probabilidade do evento	Taxa de falha	Tempo de exposição	Evento básico	Descrição
1	2,12E-13	1,66E-04	1,66E-04	1 hora de voo	EB33	Evento básico 33
		7,68E-06	7,68E-06	1 hora de voo	EB63	Evento básico 63
		1,66E-04	1,66E-04	1 hora de voo	EB7	Evento básico 7
2	1,28E-13	1,66E-04	1,66E-04	1 hora de voo	EB33	Evento básico 33
		7,68E-06	7,68E-06	1 hora de voo	EB63	Evento básico 63
		1,00E-04	1,00E-04	1 hora de voo	EVENTO_EXTERNO_1	Evento externo 1
3	1,28E-13	7,68E-06	7,68E-06	1 hora de voo	EB63	Evento básico 63
		1,66E-04	1,66E-04	1 hora de voo	EB7	Evento básico 7
		1,00E-04	1,00E-04	1 hora de voo	EVENTO_EXTERNO_2	Evento externo 2
4	9,92E-14	1,66E-04	1,66E-04	1 hora de voo	EB33	Evento básico 33
		3,60E-06	3,60E-06	1 hora de voo	EB49	Evento básico 49
		1,66E-04	1,66E-04	1 hora de voo	EB7	Evento básico 7
5	8,41E-14	1,66E-04	1,66E-04	1 hora de voo	EB33	Evento básico 33
		7,00E-02	2,00E-06	35.000 horas de voo	EB51	Evento básico 51
		4,36E-05	4,36E-05	1 hora de voo	EB55	Evento básico 55
		1,66E-04	1,66E-04	1 hora de voo	EB7	Evento básico 7
6	8,41E-14	1,66E-04	1,66E-04	1 hora de voo	EB33	Evento básico 33

#	Probabilidade do grupo de corte	Probabilidade do evento	Taxa de falha	Tempo de exposição	Evento básico	Descrição
		7,00E-02	2,00E-06	35.000 horas de voo	EB51	Evento básico 51
		4,36E-05	4,36E-05	1 hora de voo	EB56	Evento básico 56
		1,66E-04	1,66E-04	1 hora de voo	EB7	Evento básico 7
7	7,68E-14	7,68E-06	7,68E-06	1 hora de voo	EB63	Evento básico 63
		1,00E-04	1,00E-04	1 hora de voo	EVENTO_EXTERNO_1	Evento externo 1
		1,00E-04	1,00E-04	1 hora de voo	EVENTO_EXTERNO_2	Evento externo 2
8	5,98E-14	1,66E-04	1,66E-04	1 hora de voo	EB33	Evento básico 33
		3,60E-06	3,60E-06	1 hora de voo	EB49	Evento básico 49
		1,00E-04	1,00E-04	1 hora de voo	EVENTO_EXTERNO_1	Evento externo 1
9	5,98E-14	3,60E-06	3,60E-06	1 hora de voo	EB49	Evento básico 49
		1,66E-04	1,66E-04	1 hora de voo	EB7	Evento básico 7
		1,00E-04	1,00E-04	1 hora de voo	EVENTO_EXTERNO_2	Evento externo 2
10	5,07E-14	7,00E-02	2,00E-06	35.000 horas de voo	EB51	Evento básico 51
		4,36E-05	4,36E-05	1 hora de voo	EB55	Evento básico 55
		1,66E-04	1,66E-04	1 hora de voo	EB7	Evento básico 7
		1,00E-04	1,00E-04	1 hora de voo	EVENTO_EXTERNO_2	Evento externo 2
11	5,07E-14	7,00E-02	2,00E-06	35.000 horas de voo	EB51	Evento básico 51
		4,36E-05	4,36E-05	1 hora de voo	EB56	Evento básico 56
		1,66E-04	1,66E-04	1 hora de voo	EB7	Evento básico 7
		1,00E-04	1,00E-04	1 hora de voo	EVENTO_EXTERNO_2	Evento externo 2
12	5,07E-14	1,66E-04	1,66E-04	1 hora de voo	EB33	Evento básico 33
		7,00E-02	2,00E-06	35.000 horas de voo	EB51	Evento básico 51
		4,36E-05	4,36E-05	1 hora de voo	EB55	Evento básico 55
		1,00E-04	1,00E-04	1 hora de voo	EVENTO_EXTERNO_1	Evento externo 1
13	5,07E-14	1,66E-04	1,66E-04	1 hora de voo	EB33	Evento básico 33
		7,00E-02	2,00E-06	35.000 horas de voo	EB51	Evento básico 51
		4,36E-05	4,36E-05	1 hora de voo	EB56	Evento básico 56
		1,00E-04	1,00E-04	1 hora de voo	EVENTO_EXTERNO_1	Evento externo 1
14	4,92E-14	1,66E-04	1,66E-04	1 hora de voo	EB33	Evento básico 33
		4,10E-02	1,17E-06	35.000 horas de voo	EB52	Evento básico 52
		4,36E-05	4,36E-05	1 hora de voo	EB55	Evento básico 55
		1,66E-04	1,66E-04	1 hora de voo	EB7	Evento básico 7
15	4,92E-14	1,66E-04	1,66E-04	1 hora de voo	EB33	Evento básico 33
		4,10E-02	1,17E-06	35.000 horas de voo	EB52	Evento básico 52
		4,36E-05	4,36E-05	1 hora de voo	EB56	Evento básico 56
		1,66E-04	1,66E-04	1 hora de voo	EB7	Evento básico 7

A etapa seguinte diz respeito ao critério que determinará quando deve ser realizada uma análise de risco. No Quadro 4.5 é exposta a definição destes critérios:

Quadro 4.5 - Critério de risco para a aplicação do método de identificação de componentes e grupos de corte críticos

Probabilidade do limite inferior	***Catastrophic* ***	***Critical* ***	***Marginal* ***	***Negligible* ***
$1x10^{-4}$	Alto	Alto	Sério	Médio
$1x10^{-5}$	Alto	Alto	Sério	Médio
$1x10^{-6}$	Alto	Sério	Médio	Baixo
$1x10^{-7}$	Sério	Médio	Baixo	Baixo
$1x10^{-8}$	Médio	Baixo	Baixo	Baixo
	Baixo	Baixo	Baixo	Baixo

* Níveis de severidade da norma MIL-STD-882E

Segundo o Quadro 4.5, o sistema deve atender os seguintes patamares de probabilidade:

Quadro 4.6 - Objetivos de probabilidade para cada nível de severidade

Severidade	**Probabilidade**
*Catastrophic**	$< 1x10^{-8}$
*Critical**	$< 1x10^{-7}$
*Marginal**	$< 1x10^{-6}$
*Negligible**	$< 1x10^{-5}$

* Níveis de severidade da norma MIL-STD-882E

Dessa forma, para uma árvore de falha proveniente de uma condição de falha classificada como *Catastrophic*, esta deve ser menor que a probabilidade de $1x10^{-8}$. A probabilidade do evento topo para este exemplo é $2{,}91x10^{-12}$, portanto o sistema atende os critérios de segurança.

A partir das informações provenientes dos resultados apresentados até este ponto, é possível determinar os critérios de probabilidade para os grupos de corte críticos, conforme Quadro 4.7.

Quadro 4.7 - Critérios de probabilidade dos grupos de corte formados pelos eventos que mais contribuem para o evento topo

Grupo de corte	Probabilidade do primeiro Evento Básico	Probabilidade do segundo Evento Básico	Probabilidade do terceiro Evento Básico	Probabilidade do quarto Evento Básico	Critério de probabilidade
1	Evento básico 33	Evento básico 63	Evento básico 7	-	Prob. EB 33 x Prob. EB 63 x Prob. EB 7 < $1x10^{-8}$
2	Evento básico 33	Evento básico 63	Evento externo 1	-	Prob. EB 33 x Prob. EB 63 x Prob. Evento Externo 1 < $1x10^{-8}$
3	Evento básico 63	Evento básico 7	Evento externo 2	-	Prob. EB 63 x Prob. EB 7 x Prob. Evento externo 2 < $1x10^{-8}$
4	Evento básico 33	Evento básico 49	Evento básico 7	-	Prob. EB 33 x Prob. EB 49 x Prob. EB 7 < $1x10^{-8}$
5	Evento básico 33	Evento básico 51	Evento básico 55	Evento básico 7	Prob. EB 33 x Prob. EB 51 x Prob. EB 55 x Prob. EB 7 < $1x10^{-8}$
6	Evento básico 33	Evento básico 51	Evento básico 56	Evento básico 7	Prob. EB 33 x Prob. EB 51 x Prob. EB 56 x Prob. EB 7 < $1x10^{-8}$
7	Evento básico 63	Evento externo 1	Evento externo 2	-	Prob. EB 63 x Prob. Evento Externo 1 x Prob. Evento Externo 2 < $1x10^{-8}$
8	Evento básico 33	Evento básico 49	Evento externo 1	-	Prob. EB 33 x Prob. EB 49 x Prob. Evento Externo 1 < $1x10^{-8}$
9	Evento básico 49	Evento básico 7	Evento externo 2	-	Prob. EB 49 x Prob. EB 7 x Prob. Evento Externo 2 < $1x10^{-8}$
10	Evento básico 33	Evento básico 51	Evento básico 55	Evento externo 1	Prob. EB 33 x Prob. EB 51 x Prob. EB 55 x Prob. Evento externo 1 < $1x10^{-8}$
11	Evento básico 33	Evento básico 51	Evento básico 56	Evento externo 1	Prob. EB 33 x Prob. EB 51 x Prob. EB 56 x Prob. Evento Externo 1 < $1x10^{-8}$
12	Evento básico 51	Evento básico 55	Evento básico 7	Evento externo 2	Prob. EB 51 x Prob. EB 55 x Prob. EB 7 x Prob. Evento Externo 2 < $1x10^{-8}$
13	Evento básico 51	Evento básico 56	Evento básico 7	Evento externo 2	Prob. EB 51 x Prob. EB 56 x Prob. EB 7 x Prob. Evento Externo 2 < $1x10^{-8}$
14	Evento básico 33	Evento básico 52	Evento básico 55	Evento básico 7	Prob. EB 33 x Prob. EB 52 x Prob. EB 55 x Prob. EB 7 < $1x10^{-8}$
15	Evento básico 33	Evento básico 52	Evento básico 56	Evento básico 7	Prob. EB 33 x Prob. EB 52 x Prob. EB 56 x Prob. EB 7 < $1x10^{-8}$

Tomando como exemplo o grupo de corte 1, extrai-se o seguinte significado: o produto da probabilidade de falha do evento básico ou componente 33 vezes a probabilidade de falha do evento básico ou componente 63 vezes a probabilidade de falha do evento básico ou componente 7 deve ser menor que a probabilidade de $1x10^{-8}$. Se o acompanhamento das falhas destes componentes mostrar que a combinação das probabilidades de falha está maior que o valor de $1x10^{-8}$, então este é o indicativo que deve ser realizada uma análise de risco.

Utilizando-se a Equação 10, obtêm-se a fórmula do critério de monitoramento do grupo de corte 1:

$$(1-e^{-(\lambda_{EB33}.t_{ExposiçãoEB33})}).(1-e^{-(\lambda_{EB63}.t_{ExposiçãoEB63})}).(1-e^{-(\lambda_{EB7}.t_{ExposiçãoEB7})}) < 1.10^{-8} \quad \text{Equação 26}$$

O próximo passo do processo é realizar o monitoramento dos eventos de campo dos componentes críticos. Para exemplificar este passo, será utilizado o primeiro grupo de corte que é composto pela combinação das probabilidades de falha dos eventos básicos ou componentes 33, 63 e 7. Os componentes 33 e 7 são do mesmo tipo, isto é, existem dois componentes fisicamente iguais na aeronave. O monitoramento destes 3 itens é feito em uma frota de 196 aeronaves com, aproximadamente, 44.000 horas de voo acumuladas.

Para os componentes 33 e 7, são apresentados registros reais de falhas da operação do modelo de aeronave em estudo. As falhas confirmadas - “F” - (estas são as primeiras falhas na vida deste tipo de componente, por isso é possível utilizar o método análise de dados de vida - LDA) e as suspensões - “S” - são apresentadas no Quadro 4.8.

Quadro 4.8 - Dados de falha e suspensão dos eventos básicos 7 e 33 do sistema 1

#	Horas de voo	Aeronave	#	Horas de voo	Aeronave	#	Horas de voo	Aeronave	#	Horas de voo	Aeronave	#	Horas de voo	Aeronave
S	123	1	S	266	41	S	6	83	S	69	124	S	104	166
S	123	1	S	266	41	S	6	83	S	21	125	S	48	167
S	384	2	S	32	42	S	190	84	S	21	125	S	48	167
S	384	2	S	32	42	S	190	84	S	171	126	S	45	168
S	47	3	S	345	43	S	37	85	S	171	126	S	45	168
S	47	3	S	345	43	S	37	85	S	184	127	S	30	169
S	527	4	S	697	44	S	218	86	S	184	127	S	30	169
S	527	4	S	697	44	S	218	86	S	122	128	S	25	170
S	288	5	S	151	45	S	73	87	S	122	128	S	25	170
S	288	5	S	151	45	S	73	87	S	42	129	S	20	171
S	585	6	S	292	46	S	57	88	S	42	129	S	20	171
S	585	6	S	292	46	S	57	88	S	231	130	S	116	172
S	403	7	S	101	47	S	53	89	S	231	130	S	116	172
S	403	7	S	101	47	S	53	89	S	235	131	S	30	173
S	523	8	S	352	48	S	278	90	S	235	131	S	30	173
F	463	8	S	352	48	S	278	90	S	350	132	S	112	174

#	Horas de voo	Aeronave	#	Horas de voo	Aeronave	#	Horas de voo	Aeronave	#	Horas de voo	Aeronave	#	Horas de voo	Aeronave
S	60	8	S	363	49	S	50	91	S	350	132	S	112	174
S	310	9	S	363	49	S	50	91	S	90	133	S	35	175
S	310	9	S	892	50	S	97	92	S	90	133	S	35	175
S	351	10	S	892	50	S	97	92	S	192	134	S	30	176
S	351	10	S	280	51	S	190	93	S	192	134	S	30	176
S	536	11	S	280	51	S	190	93	S	35	135	S	60	177
F	533	11	S	182	52	S	154	94	S	35	135	S	60	177
S	1105	12	S	182	52	S	154	94	S	71	136	S	60	178
F	992	12	S	148	53	S	271	95	S	71	136	S	60	178
S	113	12	S	148	53	S	271	95	S	224	137	S	45	179
S	444	13	S	422	54	S	159	96	S	224	137	S	45	179
S	444	13	S	422	54	S	159	96	S	340	138	S	25	180
S	381	14	S	213	55	S	320	97	S	340	138	S	25	180
S	381	14	S	213	55	S	320	97	S	79	139	S	63	181
S	575	15	S	230	56	S	224	98	S	79	139	S	63	181
S	575	15	S	230	56	S	224	98	S	354	140	S	97	182
F	822	16	S	770	57	S	191	99	S	354	140	S	97	182
S	822	16	S	770	57	S	191	99	S	189	141	S	10	183
S	463	17	S	465	58	S	254	100	S	189	141	S	10	183
S	463	17	S	465	58	S	254	100	S	91	142	S	45	184
S	433	18	S	599	59	S	132	101	S	91	142	S	45	184
S	433	18	S	599	59	S	132	101	S	274	143	S	68	185
F	978	19	S	394	60	S	814	102	S	274	143	S	68	185
S	978	19	S	394	60	S	814	102	S	181	144	S	50	186
S	519	20	S	379	61	S	128	103	S	181	144	S	50	186
F	476	20	S	379	61	S	128	103	S	15	145	S	60	187
S	43	20	S	330	62	S	88	104	S	15	145	S	60	187
S	262	21	S	330	62	S	88	104	S	215	146	S	30	188
S	262	21	S	223	63	F	499	105	S	215	146	S	30	188
S	536	22	S	223	63	S	216	105	S	89	147	S	109	189
S	536	22	S	48	64	F	714	105	S	89	147	S	109	189
S	230	23	S	48	64	S	233	106	S	30	148	S	43	190
S	230	23	S	462	65	S	233	106	S	30	148	S	43	190
S	479	24	S	462	65	S	348	107	S	49	149	S	22	191
S	479	24	S	356	66	S	348	107	S	49	149	S	22	191
S	115	25	S	356	66	S	332	108	S	66	150	S	22	192
S	115	25	S	436	67	S	332	108	S	66	150	S	22	192
S	259	26	S	436	67	S	154	109	S	151	151	S	33	193
S	259	26	S	461	68	S	154	109	S	151	151	S	33	193
S	118	27	S	461	68	S	10	110	S	10	152	S	25	194
S	118	27	S	172	69	S	10	110	S	10	152	S	25	194
S	240	28	S	172	69	S	112	111	S	108	153	S	10	195

#	Horas de voo	Aeronave	#	Horas de voo	Aeronave	#	Horas de voo	Aeronave	#	Horas de voo	Aeronave	#	Horas de voo	Aeronave
S	240	28	S	148	70	S	112	111	S	108	153	S	10	195
S	232	29	S	148	70	S	99	112	S	63	154	S	5	196
S	232	29	S	855	71	S	99	112	S	63	154	S	5	196
S	206	30	S	855	71	S	183	113	S	24	155			
S	206	30	S	170	72	S	183	113	S	24	155			
S	114	31	S	170	72	S	362	114	S	183	156			
S	114	31	S	177	73	S	362	114	S	183	156			
S	314	32	S	177	73	S	212	115	S	125	157			
S	314	32	S	137	74	S	212	115	S	125	157			
S	241	33	S	137	74	S	110	116	S	98	158			
S	241	33	S	272	75	S	110	116	S	98	158			
S	247	34	S	272	75	S	238	117	S	30	159			
S	247	34	S	188	76	S	238	117	S	30	159			
S	165	35	S	188	76	S	30	118	S	139	160			
S	165	35	S	330	77	S	30	118	S	139	160			
S	236	36	S	330	77	S	135	119	S	15	161			
S	236	36	S	208	78	S	135	119	S	15	161			
S	79	37	S	208	78	S	136	120	S	18	162			
S	79	37	S	102	79	S	136	120	S	18	162			
S	912	38	S	102	79	S	22	121	S	42	163			
F	493	38	S	320	80	S	22	121	S	42	163			
F	418	38	S	320	80	S	131	122	S	25	164			
S	795	39	S	128	81	S	131	122	S	25	164			
S	795	39	S	128	81	S	336	123	S	103	165			
S	701	40	S	267	82	F	115	123	S	103	165			
S	701	40	S	267	82	S	69	124	S	104	166			

Serão calculados os valores de taxa de falha dos componentes 33 e 7, tanto pelo método do MTBF quando pelo método de LDA. Primeiramente, para o MTBF, a partir da Equação 16, tem-se:

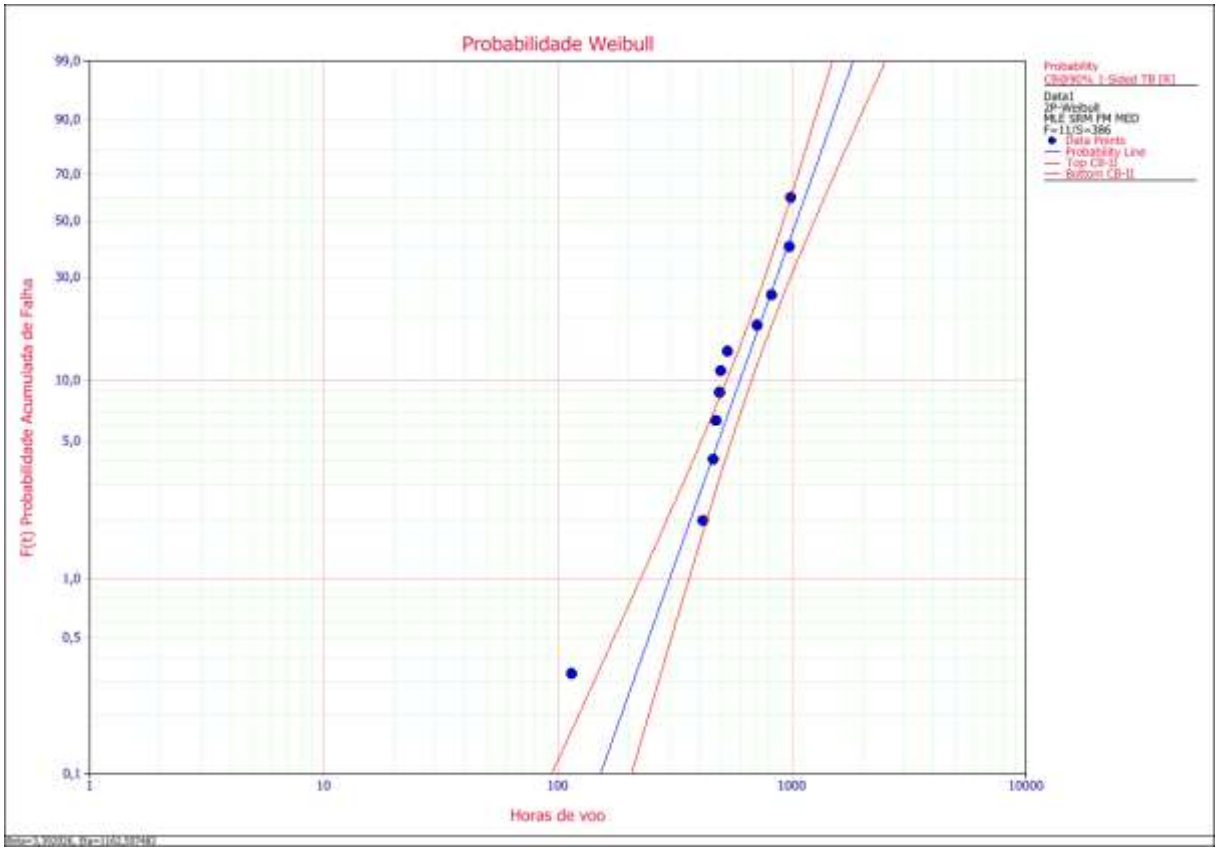
$$\mathrm{MTBF}=\frac{44.000\times 2}{11}=8.000$$

A taxa de falha calculada para o MTBF, a partir da Equação 12, resulta no seguinte:

$$\lambda=\frac{1}{8.000}=1{,}25\mathrm{x}10^{-4}$$

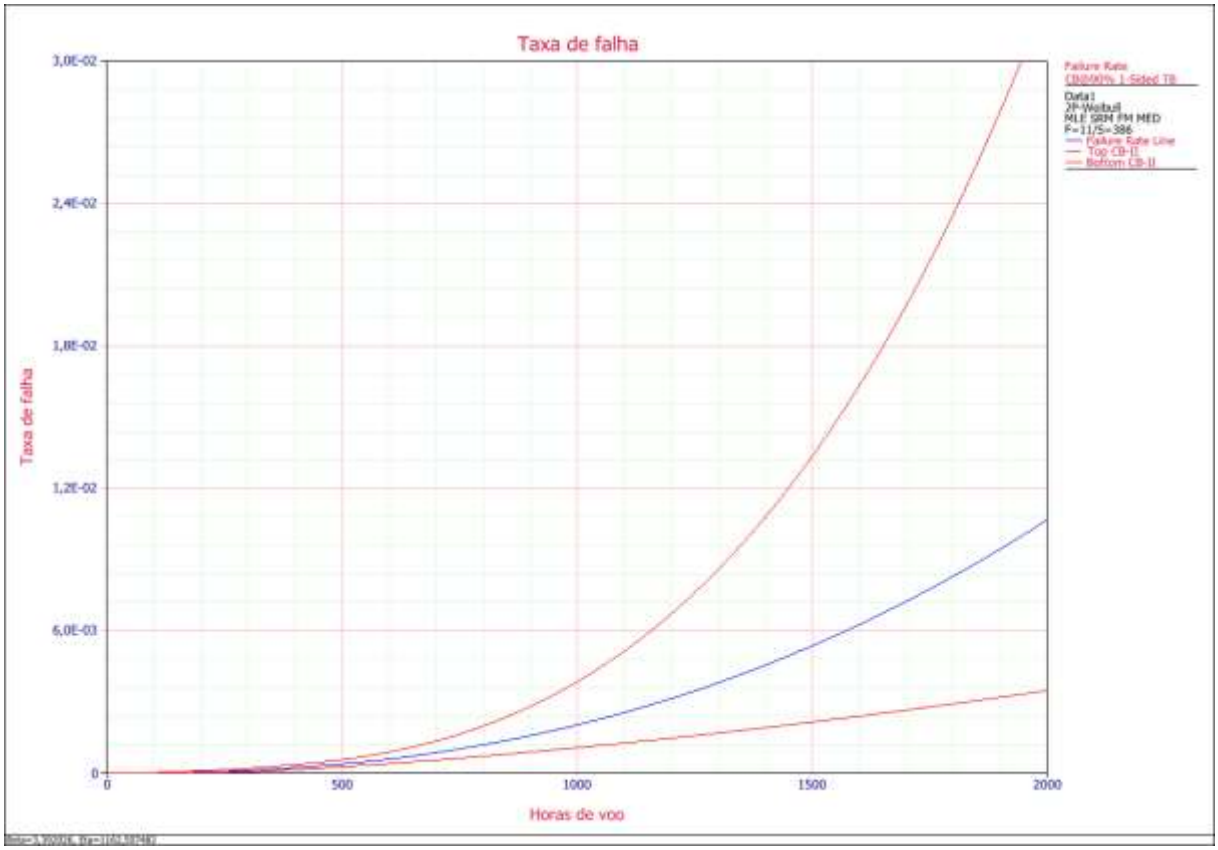
A seguir, a taxa de falha foi calculada utilizando-se o *software* Weibull ++ 9 pelo método de LDA. Com os valores do Quadro 4.8, calculou-se a distribuição Weibull com dois parâmetros pelo método *Maximum Likelihood Estimator* (MLE). O valor resultante para o parâmetro β (beta) foi 3,3920 e o valor resultante para o parâmetro η (eta) foi de 1162,5074.

Gráfico 4.1 - Probabilidade de falha acumulada Weibull para os componentes 7 e 33 do sistema 1



O Gráfico 4.1 mostra a probabilidade acumulada de falha para a distribuição Weibull com dois parâmetros. Os pontos azuis representam as falhas e a linha azul representa o valor mediano de probabilidade de falha acumulada. Por exemplo, para 1.000 horas de voo o valor mediano de probabilidade de falha acumulada é de aproximadamente 40%. As linhas vermelhas representam os limites de confiança de 90%.

Gráfico 4.2 - Taxa de falha para os componentes 7 e 33 do sistema 1



O valor do parâmetro β (beta) é maior que o valor 1, portanto a taxa de falha tem comportamento de desgaste. No Gráfico 4.2 é possível constatar a curva de taxa de falha crescente com o tempo que denota a condição de desgaste. No Quadro 4.9 são expostos os valores de taxa de falha para cada valor de hora de voo.

Quadro 4.9 - Valor de taxa de falha em função das horas de voo para os componentes 7 e 33

Horas de voo	Taxa de falha
100	8,25E-06
200	4,33E-05
300	1,14E-04
400	2,27E-04
500	3,88E-04
600	6,00E-04
700	8,67E-04
800	1,19E-03
900	1,58E-03
1000	2,04E-03
1100	2,56E-03
1200	3,15E-03
1300	3,81E-03
1400	4,55E-03
1500	5,37E-03
1600	6,26E-03
1700	7,24E-03
1800	8,30E-03
1900	9,45E-03
2000	1,07E-02

Para o evento básico ou componente 63, a quantidade de falhas é fictícia e foi determinada a fim de construir o exemplo para este trabalho. No Quadro 4.10, são expostos os números de remoções e falhas do componente do evento básico 63.

Quadro 4.10 - Número de remoções e falhas confirmadas do componente do evento básico 63

Componente do evento básico 63	
Número de remoções	13
Número de falhas confirmadas	3

A partir da Equação 16, obtêm-se o valor da métrica MTBF:

$$\mathrm{MTBF}=\frac{44.000}{3}=14.667$$

A taxa de falha calculada a partir da Equação 12 para o MTBF resulta no seguinte valor:

$$\lambda=\frac{1}{14.667}=6{,}82\mathrm{x}10^{-5}$$

A partir da Equação 18, obtêm-se o valor da métrica MTBUR:

$$\mathrm{MTBUR}=\frac{44.000}{10}=4.400$$

A taxa de falha calculada a partir da Equação 12 para o MTBUR resulta no seguinte valor:

$$\lambda=\frac{1}{4.400}=2{,}24\mathrm{x}10^{-4}$$

Neste ponto, tem-se as taxas de falha calculadas pelos métodos de MTBF, MTBUR e LDA para todos os itens. A partir da Equação 26, que é o critério de probabilidade para executar o monitoramento do grupo de corte 1, e utilizando-se o valor de taxa de falha dos componentes dos eventos básicos 7, 33 e 63 provenientes do MTBF, tem-se o seguinte resultado:

$$(1-e^{-(1{,}25.10^{-4}.1)}).(1-e^{-(6{,}82.10^{-5}.1)}).(1-e^{-(1{,}25.10^{-4}.1)})=1{,}07.10^{-12}$$

Este valor atende ao critério de $1\mathrm{x}10^{-8}$. Recalculou-se, então, o critério de probabilidade para executar o monitoramento do grupo de corte 1, porém, desta vez,

utilizando-se o valor de taxa de falha dos componentes dos eventos básicos 33 e 7 a partir do método LDA e o valor de taxa de falha para o MTBF e MTBUR do componente do evento básico 63. Como os valores de taxa de falha dos componentes 7 e 33 variam com a hora de voo devido ao fato do comportamento da taxa de falha ser crescente com o tempo (característica de desgaste), elaborou-se o Quadro 4.11:

Quadro 4.11 - Comparação do resultado de probabilidade do grupo de corte 1

Horas de voo	Comp. 33 e 7 λ (MTBF)	Comp. 33 e 7 λ (LDA)	Comp. 63 λ (MTBF)	Comp. 63 λ (MTBUR)	Probabilidade do grupo de corte 1 (Comp. 33 e 7 - MTBF Comp. 63 - MTBF)	Probabilidade do grupo de corte 1 (Comp. 33 e 7 - LDA Comp. 63 - MTBF)	Probabilidade do grupo de corte 1 (Comp. 33 e 7 - LDA Comp. 63 - MTBUR)
100	1,25E-04	8,25E-06	6,82E-05	2,24E-04	1,07E-12	4,64E-15	1,52E-14
200	1,25E-04	4,33E-05	6,82E-05	2,24E-04	1,07E-12	1,28E-13	4,20E-13
300	1,25E-04	1,14E-04	6,82E-05	2,24E-04	1,07E-12	8,86E-13	2,91E-12
400	1,25E-04	2,27E-04	6,82E-05	2,24E-04	1,07E-12	3,51E-12	1,15E-11
500	1,25E-04	3,88E-04	6,82E-05	2,24E-04	1,07E-12	1,03E-11	3,37E-11
600	1,25E-04	6,00E-04	6,82E-05	2,24E-04	1,07E-12	2,45E-11	8,06E-11
700	1,25E-04	8,67E-04	6,82E-05	2,24E-04	1,07E-12	5,12E-11	1,68E-10
800	1,25E-04	1,19E-03	6,82E-05	2,24E-04	1,07E-12	9,65E-11	3,17E-10
900	1,25E-04	1,58E-03	6,82E-05	2,24E-04	1,07E-12	1,70E-10	5,58E-10
1000	1,25E-04	2,04E-03	6,82E-05	2,24E-04	1,07E-12	2,83E-10	9,30E-10
1100	1,25E-04	2,56E-03	6,82E-05	2,24E-04	1,07E-12	4,46E-10	1,46E-09
1200	1,25E-04	3,15E-03	6,82E-05	2,24E-04	1,07E-12	6,75E-10	2,22E-09
1300	1,25E-04	3,81E-03	6,82E-05	2,24E-04	1,07E-12	9,86E-10	3,24E-09
1400	1,25E-04	4,55E-03	6,82E-05	2,24E-04	1,07E-12	1,41E-09	4,62E-09
1500	1,25E-04	5,37E-03	6,82E-05	2,24E-04	1,07E-12	1,96E-09	6,42E-09
1600	1,25E-04	6,26E-03	6,82E-05	2,24E-04	1,07E-12	2,66E-09	8,72E-09
1700	1,25E-04	7,24E-03	6,82E-05	2,24E-04	1,07E-12	3,55E-09	1,17E-08
1800	1,25E-04	8,30E-03	6,82E-05	2,24E-04	1,07E-12	4,66E-09	1,53E-08
1900	1,25E-04	9,45E-03	6,82E-05	2,24E-04	1,07E-12	6,03E-09	1,98E-08
2000	1,25E-04	1,07E-02	6,82E-05	2,24E-04	1,07E-12	7,72E-09	2,54E-08

Nota-se que, para o cálculo utilizando-se o valor de taxa de falha proveniente do método LDA para os componentes 7 e 33 e o valor de taxa de falha proveniente do método de MTBF para o componente 63, o resultado de probabilidade para executar o monitoramento do grupo de corte 1 atende ao critério de $1x10^{-8}$. No entanto, os resultados de probabilidade utilizando-se o valor de taxa de falha proveniente do método de MTBUR para o componente 63 não atendem o critério de $1x10^{-8}$ a partir de 1.700 horas de voo e, portanto uma análise de risco

deve ser realizada. Importante salientar que esta é uma abordagem conservadora, uma vez que se toma o valor de MTBUR e se calcula a taxa de falha como se todas as remoções fossem falhas confirmadas. Mesmo esta hipótese não sendo confirmada até este momento, conservadoramente, utiliza-se esta abordagem a fim de investigar mais a fundo a situação e tomar as ações adequadas, primando assim pela segurança do produto. Abaixo, está o resultado da probabilidade do grupo de corte 1, utilizando-se o valor de taxa de falha proveniente do método LDA para os componentes 7 e 33 e o valor de taxa de falha proveniente do método de MTBUR para o componente 63:

$$(1-e^{-(7{,}24.10^{-3}.1)}).(1-e^{-(2{,}24.10^{-4}.1)}).(1-e^{-(7{,}24.10^{-3}.1)}) = 1{,}17.10^{-8}$$

Utilizando-se os critérios de risco, determina-se a classificação de risco. No Quadro 4.12 é possível constatar qual a categoria de risco definida a partir das taxas de falha dos componentes, ou seja, risco Médio.

Quadro 4.12 - Classificação de risco para o sistema 1

Probabilidade do limite inferior	***Catastrophic** **	***Critical** **	***Marginal** **	***Negligible** **
$1x10^{-4}$	Alto	Alto	Sério	Médio
$1x10^{-5}$	Alto	Alto	Sério	Médio
$1x10^{-6}$	Alto	Sério	Médio	Baixo
$1x10^{-7}$	Sério	Médio	Baixo	Baixo
$1x10^{-8}$	$1{,}17x10^{-8}$	Baixo	Baixo	Baixo
	Baixo	Baixo	Baixo	Baixo

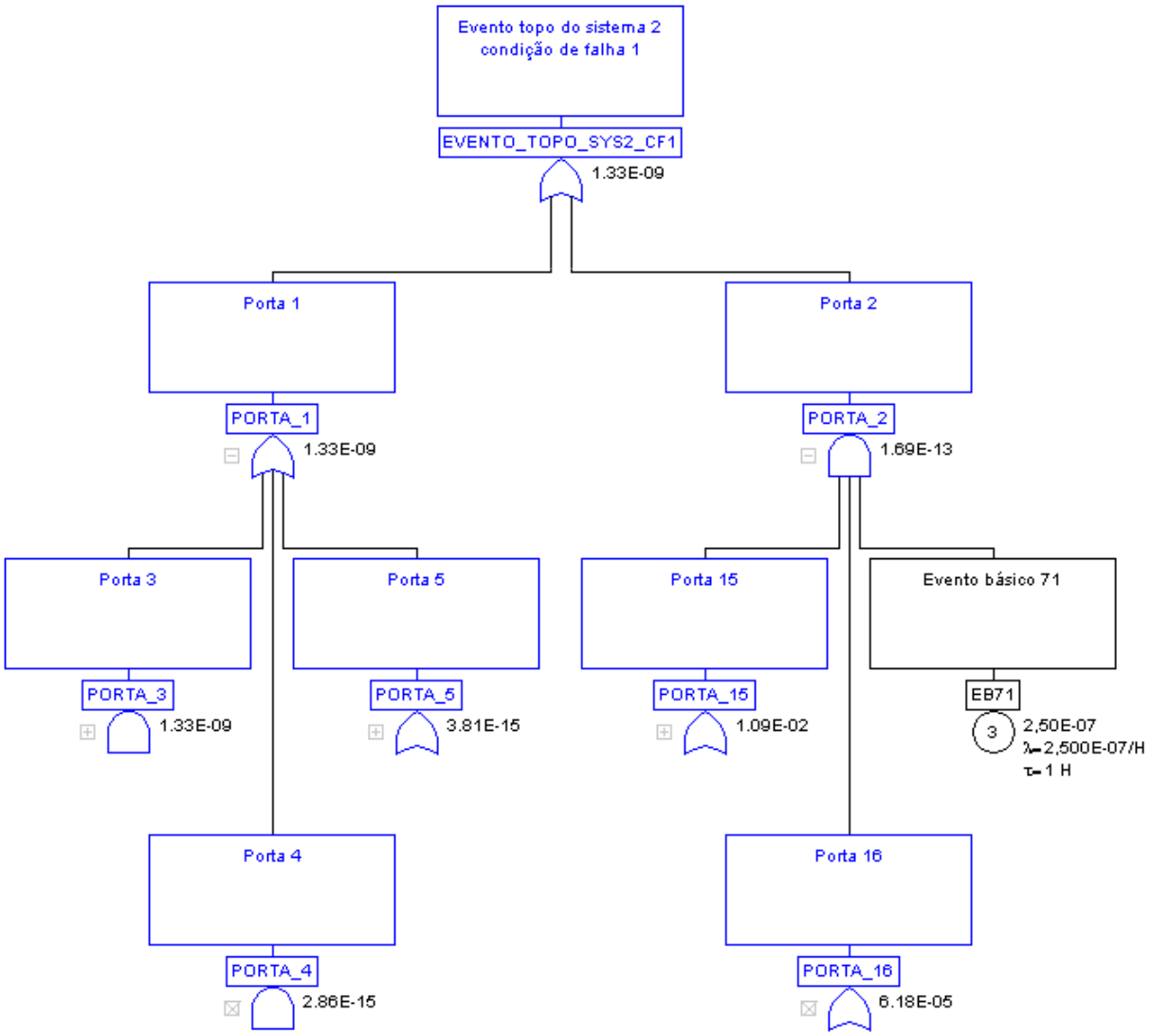
* Níveis de severidade da norma MIL-STD-882E

A partir deste ponto, outras atividades são necessárias como, por exemplo, a elaboração de um plano de ação e a sua implementação. Estas atividades não serão detalhadas, pois este trabalho está focado nos passos 1, 2 e 3 do processo da ARP5150.

Para as árvores de falha dos sistemas 2 a 6 serão mostrados os resultados das medidas de importância, os eventos selecionados e a porcentagem de itens monitorados em relação ao total de itens existentes na árvore de falha em estudo.

Na Figura 4.3 encontra-se resumida a árvore de falha do sistema 2.

Figura 4.3 - Árvore de falha do sistema 2



A partir da árvore de falha, determinam-se os grupos de corte e aplica-se o cálculo das medidas de importância aos grupos de corte.

Quadro 4.13 - Ranque de contribuição dos eventos básicos para o evento topo da árvore de falha do sistema 2

Evento básico	Probabilidade do evento	Fussel-Vesely	% de contribuição	Descrição
EB71	2,50E-07	1,00E+00	49,99%	Evento básico 71
EB72	5,31E-03	1,00E+00	49,99%	Evento básico 72
EB97	4,53E-05	9,37E-05	0,00%	Evento básico 97
EB89	4,82E-03	5,60E-05	0,00%	Evento básico 89
EB93	4,57E-03	5,32E-05	0,00%	Evento básico 93
EB99	1,32E-05	2,73E-05	0,00%	Evento básico 99
EB92	1,57E-03	1,83E-05	0,00%	Evento básico 92
EB96	3,03E-06	6,27E-06	0,00%	Evento básico 96
EB83	2,20E-07	2,51E-06	0,00%	Evento básico 83
EB84	5,35E-05	2,51E-06	0,00%	Evento básico 84
EB85	2,83E-04	2,51E-06	0,00%	Evento básico 85
EB75	2,83E-04	6,69E-07	0,00%	Evento básico 75
EB76	1,32E-05	6,69E-07	0,00%	Evento básico 76
EB77	1,32E-05	6,69E-07	0,00%	Evento básico 77
EB78	2,83E-04	6,69E-07	0,00%	Evento básico 78
EB98	2,66E-07	5,85E-07	0,00%	Evento básico 98
EB86	3,13E-08	3,34E-07	0,00%	Evento básico 86
EB87	5,35E-05	3,34E-07	0,00%	Evento básico 87
EB88	2,83E-04	3,34E-07	0,00%	Evento básico 88
EB79	2,83E-04	2,51E-07	0,00%	Evento básico 79
EB80	5,35E-06	2,51E-07	0,00%	Evento básico 80
EB81	2,83E-04	2,51E-07	0,00%	Evento básico 81
EB82	5,35E-06	2,51E-07	0,00%	Evento básico 82
EB73	1,32E-05	1,67E-07	0,00%	Evento básico 73
EB74	7,00E-05	1,67E-07	0,00%	Evento básico 74
EB91	5,35E-06	8,36E-08	0,00%	Evento básico 91
EB94	5,35E-06	8,36E-08	0,00%	Evento básico 94
EB95	5,35E-06	8,36E-08	0,00%	Evento básico 95
EB90	1,45E-07	0,00E+00	0,00%	Evento básico 90

Os 2 primeiros eventos correspondem a 99,98% do percentual de contribuição do risco para a ocorrência evento topo. A árvore de falha do sistema 2 contém 29 componentes, portanto a porcentagem de componentes monitorados será de 6,90%.

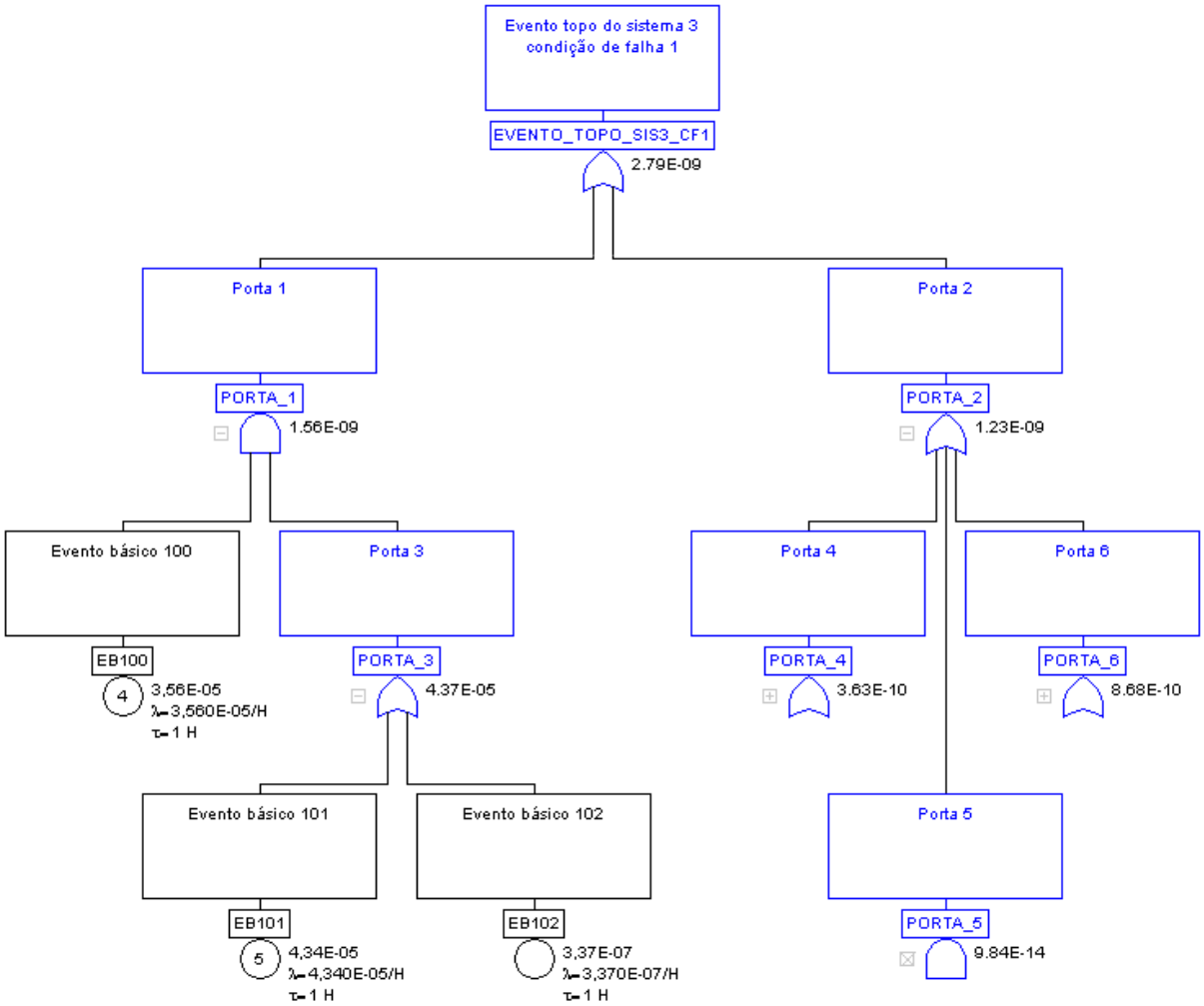
Os seguintes eventos devem ser monitorados:

Quadro 4.14 - Componentes que mais contribuem para o evento topo da árvore de falha do sistema 2

#	**Eventos básicos**
1	Evento básico 71
2	Evento básico 72

Na Figura 4.4 encontra-se resumida a árvore de falha do sistema 3.

Figura 4.4 - Árvore de falha do sistema 3



A partir da árvore de falha, determinam-se os grupos de corte e aplica-se o cálculo das medidas de importância aos grupos de corte.

Quadro 4.15 - Ranque de contribuição dos eventos básicos para o evento topo da árvore de falha do sistema 3

Evento básico	Probabilidade do evento	Fussel-Vesely	% de contribuição	Descrição
EB101	4,34E-05	8,66E-01	43,28%	Evento básico 101
EB100	3,56E-05	5,59E-01	27,93%	Evento básico 100
EB113	2,00E-05	3,11E-01	15,54%	Evento básico 113
EB103	1,59E-05	1,09E-01	5,45%	Evento básico 103
EB105	1,59E-05	1,09E-01	5,45%	Evento básico 105
EB104	3,14E-06	2,14E-02	1,07%	Evento básico 104
EB106	3,14E-06	2,14E-02	1,07%	Evento básico 106
EB102	3,37E-07	4,30E-03	0,21%	Evento básico 102

Os 3 primeiros eventos correspondem a 86,75% do percentual de contribuição do risco para a ocorrência evento topo. A árvore de falha do sistema 3 contém 15 componentes, portanto a porcentagem de componentes monitorados será de 20,0%.

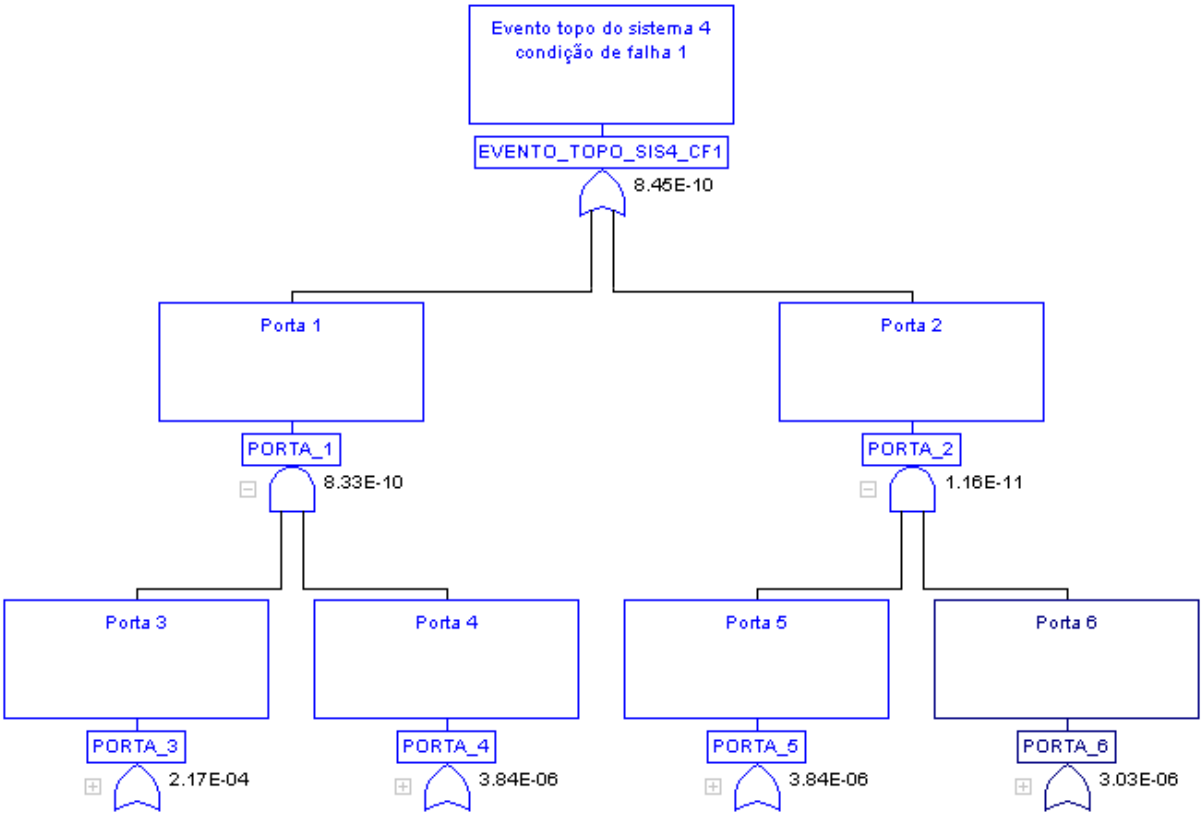
No Quadro 4.16 estão os eventos que devem ser monitorados:

Quadro 4.16 - Componentes que mais contribuem para o evento topo da árvore de falha do sistema 3

#	**Eventos básicos**
1	Evento básico 101
2	Evento básico 100
3	Evento básico 113

Na Figura 4.5 encontra-se resumida a árvore de falha do sistema 4.

Figura 4.5 - Árvore de falha do sistema 4



A partir da árvore de falha, determinam-se os grupos de corte e aplica-se o cálculo das medidas de importância aos grupos de corte.

Quadro 4.17 - Ranque de contribuição dos eventos básicos para o evento topo da árvore de falha do sistema 4

Evento básico	Probabilidade do evento	Fussel-Vesely	% de contribuição	Descrição
EB117	3,03E-06	7,91E-01	33,21%	Evento básico 117
EB118	3,53E-05	1,60E-01	6,72%	Evento básico 118
EB133	2,40E-05	1,09E-01	4,58%	Evento básico 133
EB134	2,40E-05	1,09E-01	4,58%	Evento básico 134
EB137	2,40E-05	1,09E-01	4,58%	Evento básico 137
EB138	2,40E-05	1,09E-01	4,58%	Evento básico 138
EB142	5,95E-03	9,07E-02	3,81%	Evento básico 142
EB143	5,94E-05	9,07E-02	3,81%	Evento básico 143
EB144	1,70E-06	8,19E-02	3,44%	Evento básico 144
EB145	1,88E-01	8,19E-02	3,44%	Evento básico 145
EB125	1,00E-04	7,00E-02	2,94%	Evento básico 125
EB126	1,00E-04	7,00E-02	2,94%	Evento básico 126
EB120	1,51E-05	6,87E-02	2,88%	Evento básico 120

Evento básico	Probabilidade do evento	Fussel-Vesely	% de contribuição	Descrição
EB123	1,35E-05	6,12E-02	2,57%	Evento básico 123
EB124	1,35E-05	6,12E-02	2,57%	Evento básico 124
EB127	1,20E-01	5,44E-02	2,28%	Evento básico 127
EB128	1,20E-01	5,44E-02	2,28%	Evento básico 128
EB122	1,00E-05	4,53E-02	1,90%	Evento básico 122
EB154	8,24E-06	3,20E-02	1,34%	Evento básico 154
EB158	8,70E-02	1,61E-02	0,68%	Evento básico 158
EB161	8,70E-02	1,61E-02	0,68%	Evento básico 161
EB164	8,70E-02	1,61E-02	0,68%	Evento básico 164
EB167	8,70E-02	1,61E-02	0,68%	Evento básico 167
EB129	3,44E-02	1,57E-02	0,66%	Evento básico 129
EB130	3,44E-02	1,57E-02	0,66%	Evento básico 130
EB116	2,08E-06	7,43E-03	0,31%	Evento básico 116
EB115	1,76E-06	6,29E-03	0,26%	Evento básico 115
EB121	1,00E-06	4,53E-03	0,19%	Evento básico 121
EB150	5,21E-03	4,16E-03	0,17%	Evento básico 150
EB151	2,04E-06	2,73E-03	0,11%	Evento básico 151
EB135	4,60E-07	2,09E-03	0,09%	Evento básico 135
EB136	4,60E-07	2,09E-03	0,09%	Evento básico 136
EB139	4,60E-07	2,09E-03	0,09%	Evento básico 139
EB140	4,60E-07	2,09E-03	0,09%	Evento básico 140
EB152	1,07E-06	1,46E-03	0,06%	Evento básico 152
EB119	2,66E-07	1,21E-03	0,05%	Evento básico 119
EB131	1,00E-06	1,56E-04	0,01%	Evento básico 131
EB132	1,00E-06	1,56E-04	0,01%	Evento básico 132
EB169	5,50E-03	1,49E-04	0,01%	Evento básico 169
EB153	4,71E-06	1,00E-04	0,00%	Evento básico 153
EB155	1,23E-06	2,62E-05	0,00%	Evento básico 155
EB141	8,26E-06	1,73E-05	0,00%	Evento básico 141
EB147	4,42E-06	3,67E-06	0,00%	Evento básico 147
EB156	1,09E-05	2,09E-06	0,00%	Evento básico 156
EB157	1,09E-05	2,09E-06	0,00%	Evento básico 157
EB159	1,09E-05	2,09E-06	0,00%	Evento básico 159
EB160	1,09E-05	2,09E-06	0,00%	Evento básico 160
EB162	1,09E-05	2,09E-06	0,00%	Evento básico 162
EB163	1,09E-05	2,09E-06	0,00%	Evento básico 163
EB165	1,09E-05	2,09E-06	0,00%	Evento básico 165
EB166	1,09E-05	2,09E-06	0,00%	Evento básico 166
EB146	1,49E-06	7,86E-07	0,00%	Evento básico 146
EB148	1,74E-06	7,86E-07	0,00%	Evento básico 148
EB149	1,00E-07	0,00E+00	0,00%	Evento básico 149
EB168	1,57E-06	0,00E+00	0,00%	Evento básico 168
EB172	2,25E-04	0,00E+00	0,00%	Evento básico 172
EB173	4,53E-05	0,00E+00	0,00%	Evento básico 173
EB174	6,21E-05	0,00E+00	0,00%	Evento básico 174

Os 13 primeiros eventos correspondem a 81,51% do percentual de contribuição do risco para a ocorrência evento topo. A árvore de falha do sistema 4 contém 60 componentes, portanto a porcentagem de componentes monitorados será de 21,67%.

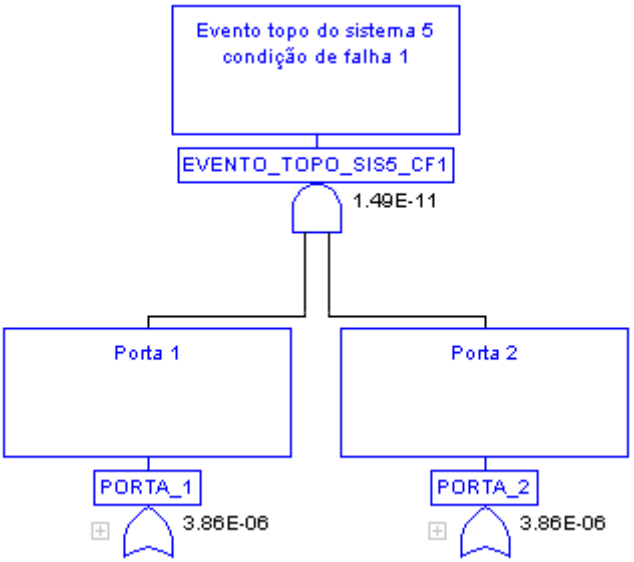
No Quadro 4.18 são mostrados os eventos que devem ser monitorados:

Quadro 4.18 - Componentes que mais contribuem para o evento topo da árvore de falha do sistema 4

#	**Eventos básicos**
1	Evento básico 117
2	Evento básico 118
3	Evento básico 133
4	Evento básico 134
5	Evento básico 137
6	Evento básico 138
7	Evento básico 142
8	Evento básico 143
9	Evento básico 144
10	Evento básico 145
11	Evento básico 125
12	Evento básico 126
13	Evento básico 120

Na Figura 4.6 encontra-se resumida a árvore de falha do sistema 5.

Figura 4.6 - Árvore de falha do sistema 5



A partir da árvore de falha, determinam-se os grupos de corte e aplica-se o cálculo das medidas de importância aos grupos de corte.

Quadro 4.19 - Ranque de contribuição dos eventos básicos para o evento topo da árvore de falha do sistema 5

Evento básico	Probabilidade do evento	Fussel-Vesely	% de contribuição	Descrição
EB179	2,23E-06	5,77E-01	28,85%	Evento básico 179
EB183	2,23E-06	5,77E-01	28,85%	Evento básico 183
EB178	1,00E-06	2,59E-01	12,95%	Evento básico 178
EB182	1,00E-06	2,59E-01	12,95%	Evento básico 182
EB181	5,02E-07	1,30E-01	6,50%	Evento básico 181
EB185	5,02E-07	1,30E-01	6,50%	Evento básico 185
EB180	1,31E-07	3,39E-02	1,70%	Evento básico 180
EB184	1,31E-07	3,39E-02	1,70%	Evento básico 184

Os 4 primeiros eventos correspondem a 83,60% do percentual de contribuição do risco para a ocorrência evento topo. A árvore de falha do sistema 5 contém 8 componentes, portanto a porcentagem de componentes monitorados será de 50,00%.

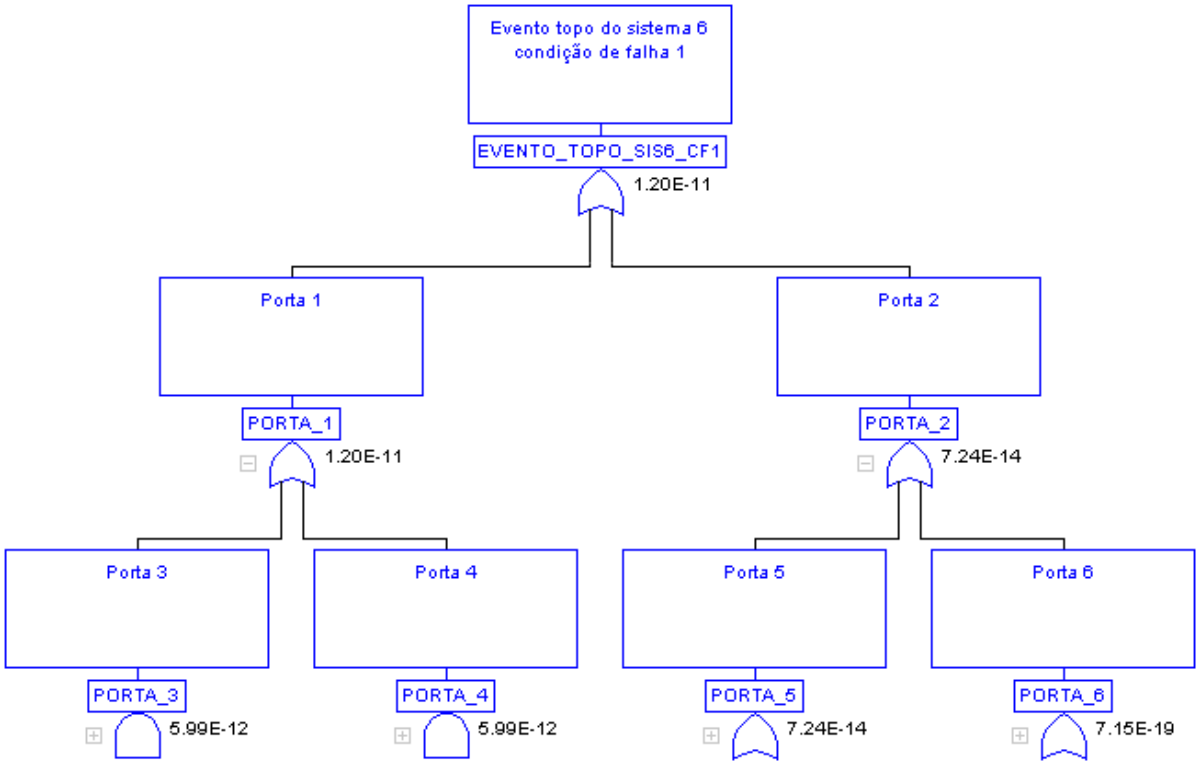
Os seguintes eventos devem ser monitorados:

Quadro 4.20 - Componentes que mais contribuem para o evento topo da árvore de falha do sistema 5

#	**Eventos básicos**
1	Evento básico 179
2	Evento básico 183
3	Evento básico 178
4	Evento básico 182

Na Figura 4.7 encontra-se resumida a árvore de falha do sistema 6.

Figura 4.7 - Árvore de falha do sistema 6



A partir da árvore de falha, determinam-se os grupos de corte e aplica-se o cálculo das medidas de importância aos grupos de corte.

Quadro 4.21 - Ranque de contribuição dos eventos básicos para o evento topo da árvore de falha do sistema 6

Evento básico	Probabilidade do evento	Fussel-Vesely	% de contribuição	Descrição
EB186	6,69E-07	4,91E-01	24,25%	Evento básico 186
EB191	6,69E-07	4,91E-01	24,25%	Evento básico 191
EB188	8,63E-06	4,85E-01	23,96%	Evento básico 188
EB193	8,63E-06	4,85E-01	23,96%	Evento básico 193
EB189	1,75E-07	9,81E-03	0,48%	Evento básico 189
EB194	1,75E-07	9,81E-03	0,48%	Evento básico 194
EB187	8,44E-09	6,19E-03	0,31%	Evento básico 187
EB192	8,44E-09	6,19E-03	0,31%	Evento básico 192
EB225	1,00E+00	6,01E-03	0,30%	Evento básico 225
EB236	1,00E+00	6,01E-03	0,30%	Evento básico 236
EB237	1,00E+00	6,01E-03	0,30%	Evento básico 237
EB239	1,38E-07	6,01E-03	0,30%	Evento básico 239
EB240	2,62E-07	3,00E-03	0,15%	Evento básico 240
EB241	1,00E+00	3,00E-03	0,15%	Evento básico 241
EB242	2,62E-07	3,00E-03	0,15%	Evento básico 242
EB243	1,00E+00	3,00E-03	0,15%	Evento básico 243
EB190	3,85E-08	2,17E-03	0,11%	Evento básico 190
EB195	3,85E-08	2,17E-03	0,11%	Evento básico 195
EB198	1,13E-07	0,00E+00	0,00%	Evento básico 198
EB199	1,66E-06	0,00E+00	0,00%	Evento básico 199
EB203	1,13E-07	0,00E+00	0,00%	Evento básico 203
EB204	1,66E-06	0,00E+00	0,00%	Evento básico 204
EB209	2,74E-13	0,00E+00	0,00%	Evento básico 209
EB221	3,22E-07	0,00E+00	0,00%	Evento básico 221
EB222	4,02E-07	0,00E+00	0,00%	Evento básico 222
EB238	1,38E-07	0,00E+00	0,00%	Evento básico 238
EB244	1,02E-06	0,00E+00	0,00%	Evento básico 244
EB245	2,79E-07	0,00E+00	0,00%	Evento básico 245
EB246	8,49E-08	0,00E+00	0,00%	Evento básico 246
EB247	1,00E+00	0,00E+00	0,00%	Evento básico 247
EB248	1,00E+00	0,00E+00	0,00%	Evento básico 248
EB253	1,02E-06	0,00E+00	0,00%	Evento básico 253
EB254	2,79E-07	0,00E+00	0,00%	Evento básico 254
EB255	8,49E-08	0,00E+00	0,00%	Evento básico 255

Os 4 primeiros eventos correspondem a 96,42% do percentual de contribuição do risco para a ocorrência evento topo. A árvore de falha do sistema 6 contém 77 componentes, portanto a porcentagem de componentes monitorados será de 5,19%.

No Quadro 4.22 são mostrados os eventos que devem ser monitorados:

Quadro 4.22 - Componentes que mais contribuem para o evento topo da árvore de falha do sistema 6

#	**Eventos básicos**
1	Evento básico 186
2	Evento básico 191
3	Evento básico 188
4	Evento básico 193

No Quadro 4.23 é mostrado o resumo da quantidade de eventos de cada árvore de falha, a quantidade de eventos que o método selecionou para serem monitorados para cada árvore de falha, a porcentagem de itens monitorados por árvore de falha, total de eventos de todas as árvores de falha, total de eventos selecionados e porcentagem geral de eventos selecionados pelo método para todas as seis árvores de falha.

Quadro 4.23 – Porcentagem de eventos selecionados a partir da aplicação do método

Árvore de falha	Total de eventos da árvore de falha	Eventos selecionados para monitoramento	% de eventos monitorados
Sistema 1	54	10	18,52%
Sistema 2	29	2	6,90%
Sistema 3	15	3	20,00%
Sistema 4	60	13	21,67%
Sistema 5	8	4	50,00%
Sistema 6	77	4	5,19%
Total	243	36	14,81%

A partir do Quadro 4.23 é possível constatar a otimização para os eventos que serão monitorados. Foram selecionados 14,81% do total de eventos de todas as árvores de falha. Com isso, nota-se o potencial benefício do método na priorização dos itens críticos de árvores de falha, que possibilita reduzir os recursos empregados para monitorar os dados de campo dos componentes e, também, focar nos itens mais relevantes para a segurança do sistema.

4.2 SÍNTESE E CONCLUSÃO DO CAPÍTULO

Neste capítulo foi apresentado, passo a passo, o método de identificação de componentes e grupos de corte críticos em árvores de falha. São três principais passos: 1) estabelecimento de parâmetros para monitoramento, 2) monitoramento dos eventos de campo e 3) avaliação dos eventos reportados e do respectivo risco. Ao todo, foram selecionadas 6 árvores de falha para aplicar o método. Para a primeira delas, executou-se o método em detalhes. A árvore completa pode ser vista no Apêndice A. Para as outras 5 árvores de falha foram apresentados os resultados do ranque de contribuição para o evento topo, os eventos selecionados e a porcentagem de eventos escolhidos em relação ao total de eventos de cada árvore de falha. Ao final, mostrou-se o resumo geral dos eventos selecionados para todas as árvores de falha.

O primeiro passo do método (estabelecimento de parâmetros para monitoramento) possui algumas etapas. Para se chegar ao critério de monitoramento, é preciso que os eventos básicos mais relevantes sejam selecionados, ou seja, aqueles que mais contribuem para a probabilidade do evento topo. Para tal, utiliza-se o método da medida de importância Fussel-Vesely. Após esta etapa, a escolha dos eventos é baseada no conceito de Pareto. Como descrito na seção 3.5, alguns poucos eventos respondem por uma parcela substancial do risco ou da probabilidade do evento topo nas análises de árvore de falha. O passo seguinte é identificar os grupos de corte formados por estes eventos mais relevantes. Por fim, elabora-se os critérios de probabilidade para monitorar os grupos de corte selecionados, utilizando os objetivos de segurança (níveis de probabilidade referentes a cada patamar de severidade).

Os próximos passos do método tratam do levantamento de eventos de campo para avaliar a taxa de falha dos componentes selecionados e a avaliação do critério de probabilidade dos grupos de corte a fim de determinar se é necessário executar uma análise de risco. O exemplo utilizado mostrou que por meio do método LDA é possível construir a curva de taxa de falha do componente. Alguns componentes apresentam taxa de falha crescente e, portanto podem necessitar de modificações de projeto devido à avaliação de segurança, caso o critério de probabilidade do grupo de corte em questão não seja atendido. É importante destacar a vantagem do método LDA em relação ao método MTBF. O primeiro

mostra com maior precisão o comportamento da falha do componente. O segundo apresenta maior facilidade de cálculo e demanda menos informações de campo, todavia provê um valor constante de taxa de falha, mesmo que o item esteja falhando por desgaste. Esta característica de taxa de falha constante pode levar a decisões equivocadas sobre como proceder a partir dos valores levantados pelo processo de monitoramento. Em outras palavras, pode levar à não execução de uma análise de risco e modificação do item ou sistema.

No próximo capítulo, serão abordados os pontos positivos e negativos do método. Serão abordadas, também, as dificuldades encontradas e soluções utilizadas na execução do método. Os objetivos iniciais do trabalho serão resgatados e discutidos para elaboração da conclusão do trabalho.

Será apresentada também, uma seção com sugestões de ideias para trabalhos futuros. Os pontos deste trabalho onde há potencial para aprofundamento e melhoria do método serão destacados.

5 CONCLUSÃO

Esta monografia contém a proposta de um método de identificação de componentes e grupos de corte críticos em árvores de falha. Este toma crédito das análises elaboradas durante a fase de projeto. Com isso, aproveita-se o esforço já empregado para o desenvolvimento do produto, economizando horas substanciais de engenharia na elaboração de novas árvores de falha. Outro benefício do método é a seleção dos itens que mais contribuem para a probabilidade do evento topo, a partir do ranque gerado pela medida de importância Fussel-Vesely e do conceito de Pareto. Com isso, o foco na segurança do sistema é estabelecido. O resultado da aplicação do método para as 6 árvores de falha escolhidas mostrou que apenas uma parcela de todos os eventos (14,81% do total de eventos de todas as árvores de falha) contribui para uma grande parte da probabilidade dos eventos topo, como pode ser observado no Quadro 4.23.

Para se estabelecer um programa de monitoramento contínuo de taxas de falha de componentes em operação há de se empregar recursos variados. Com a geração do ranque de contribuição dos itens para o evento topo e, em seguida, com a seleção de uma parcela dos eventos mais críticos de um sistema ou conjunto de sistemas, os recursos necessários são sensivelmente reduzidos, possibilitando instaurar um programa de monitoramento otimizado com foco em segurança.

Em uma árvore de falha, os eventos básicos constituem-se por modos de falhas de componentes que podem levar à perda parcial ou total da função do componente. O acompanhamento dos componentes em operação requer esforço considerável. Se todos os modos de falha de cada componente fossem monitorados, talvez esta atividade se tornasse inviável, devido à extensa quantidade de recursos necessários. Este cenário se traduziria em custos muito elevados. Dada esta situação, a maneira escolhida neste trabalho para equacionar esta restrição foi considerar a taxa de falha do componente englobando todos os possíveis modos de falha. A partir desta abordagem, há um conservadorismo nos valores encontrados. No entanto, levando-se em consideração o foco em segurança, os casos que revelarem um risco maior do que o critério estabelecido podem ser investigados à fundo. Se necessário, um esforço adicional pode ser empregado para entender mais detalhadamente o comportamento de falha do componente em foco. Por outro lado,

com o risco mantendo-se dentro dos limites estabelecidos, não seria necessário aumentar o esforço no detalhamento das falhas.

A partir do ranque de contribuição dos eventos básicos para a probabilidade do evento topo, escolhe-se os eventos mais relevantes a partir do conceito de Pareto. Os eventos selecionados formam os grupos de corte para a determinação dos parâmetros de monitoramento. Para algumas árvores de falha foi constatado durante a aplicação do método, que alguns grupos de corte não eram selecionados, pois um ou mais eventos que os constituem não foram previamente escolhidos a partir do ranque gerado pela medida de importância Fussel-Vesely. Para este tipo de situação, o conhecimento do especialista é fundamental, pois este entende à fundo as características do sistema e pode determinar se eventos adicionais devem ser selecionados além da margem estabelecida pelo conceito de Pareto, a fim de incluir grupos de corte aos parâmetros de monitoramento. A contribuição do especialista é de suma importância e traz robustez ao método.

Uma das partes fundamentais do método é a determinação dos objetivos de probabilidade para cada nível de severidade. Os patamares de probabilidade aceitáveis para as respectivas severidades serão a base para a determinação do critério para os níveis de risco. Estes objetivos devem estar estabelecidos no início do processo, bem como os níveis de risco que determinarão a eficácia do processo de análise de risco e, consequentemente, as ações subsequentes para realizar a gestão do risco. Existem várias normas como a IEC 61508 que trazem padrões e que podem e devem ser utilizados como referência na determinação dos objetivos de segurança da aplicação em questão.

O monitoramento da vida dos componentes durante a operação é outra parte fundamental do método. A coleta e tratamento dos dados de campo pode ser uma tarefa repleta de obstáculos e consumidora de grande esforço e recursos. Talvez esta seja a etapa que apresenta as maiores dificuldades. Como apresentado, utilizou-se três maneiras de calcular a taxa de falha dos componentes: MTBF, MTBUR e análise de dados de vida (*life data analysis*). Na aplicação do método para a árvore de falha do sistema 1, os resultados mostraram que utilizando a taxa de falha proveniente do MTBF para os três componentes do grupo de corte 1, o critério de probabilidade se mantinha dentro do limite aceitável (risco baixo). Todavia, quando se analisou as falhas e suspensões dos componentes 7 e 33, a análise da taxa de falha pelo método LDA revelou um comportamento de desgaste, isto é, taxa

de falha crescente com o tempo. O Quadro 4.11 revelou que combinando a taxa de falha dos componentes 7 e 33 calculada a partir de LDA e a taxa de falha do componente 63 proveniente do MTBF, o critério de probabilidade ainda permaneceu dentro do limite aceitável. Somente na combinação da taxa de falha do componente 63 proveniente do MTBUR (abordagem conservadora) com a taxa de falha dos componentes 7 e 33 extraídas do LDA é que se constatou que, a partir de 1.700 horas de voo, o risco se tornou médio. Algumas considerações podem ser originadas do exemplo descrito: a primeira delas é que a taxa de falha proveniente do MTBF não revela a vida do componente e, sim a média de tempo entre falhas. Além disso, assume-se que a distribuição é exponencial, pois a taxa de falha é constante. Estas características podem levar a entendimentos distorcidos e conclusões equivocadas, escondendo um risco maior do que o calculado. Já o método LDA traz outras limitações, apesar das vantagens de conseguir mostrar a vida real do componente e o comportamento da taxa de falha a partir dos dados coletados. Para o LDA é necessário obter os dados de falha e suspensões, tarefa que requer esforço considerável. Além disso, só pode ser aplicado para componentes não reparáveis ou para as primeiras falhas de componentes reparáveis. Do contrário, diferentes métodos devem ser aplicados para se determinar a taxa de falha do componente em estudo. A partir do exposto, é necessário ponderar sobre os métodos disponíveis e adequar as atividades de coleta e tratamento de dados, visando a elaboração e aplicação de um processo de monitoramento de segurança. Se possível, aplicar o LDA pela sua precisão e clareza no entendimento do comportamento da taxa de falha. Em segundo lugar, o MTBF e MTBUR, lembrando que o MTBUR trará valores mais conservadores. Mesmo assim, sua utilização pode revelar a necessidade de investigações mais detalhadas das falhas de um determinado componente, tendo em vista que o MTBF necessita da confirmação da falha, o que, por vezes, pode demorar para ser obtida. Além disso, o MTBUR está ligado à quantidade de remoções, consequentemente, podendo revelar outros problemas de operação ou manutenção dos sistemas.

O método exposto neste trabalho oferece a condição de ser executado periodicamente. Uma vez que os objetivos de probabilidade para os respectivos níveis de severidade e os níveis de risco estejam definidos, pode-se estabelecer intervalos repetitivos de coleta de dados e análise dos critérios de probabilidade dos

grupos de corte. Com isso, configura-se um processo sistemático de monitoramento da segurança do sistema em questão, análise e gestão do risco.

A partir do detalhamento do método no capítulo 4 e das argumentações expostas acima, conclui-se que o método de identificação de componentes e grupos de corte críticos em árvores de falha provê as condições para entender quais são os itens do sistema que mais impactam na probabilidade do evento topo da árvore de falha e, assim possibilita a determinação do foco otimizado nos componentes e grupos de corte que são mais relevantes para o monitoramento da segurança. Além disso, estabelece os objetivos de probabilidade referentes a cada nível de severidade, criando uniformidade no entendimento dos patamares de risco e gerando as bases para a implantação do processo de gestão de risco. Gera-se, também, a necessidade de organizar, adequar e implementar uma coleta e tratamento de dados que ofereça as informações necessárias para acompanhar a vida dos componentes, os respectivos valores de taxa de falha e seu comportamento, o que se mostra de fundamental importância na determinação adequada do nível de risco. Por fim, propicia, a partir da determinação do risco, a base para a tomada de decisão sobre possíveis medidas para mitigar e eliminar os riscos que ultrapassam os limites aceitáveis, garantindo, de forma sistemática, os níveis adequados de segurança para a operação do(s) sistema(s).

5.1 SUGESTÕES PARA TRABALHOS FUTUROS

Como explicado na conclusão, uma das partes fundamentais do método é o monitoramento dos dados de vida dos componentes durante a operação. As informações de falhas e suspensões são essenciais para qualquer análise quantitativa, desde a análise de dados de vida, até a análise de árvore de falhas e a gestão de risco. A partir desta constatação, pode-se identificar alguns pontos de melhoria e possíveis novos temas para futuras monografias como, por exemplo, acompanhar o processo de coleta de dados de um sistema, adquirindo registros como data de fabricação, data de instalação do item, data de remoção com confirmação da falha, data de saída da oficina para reparo, data de reinstalação no sistema, característica de operação (ciclos ou horas, operação esporádica ou constante), item reparável ou não reparável. De posse destas informações seria

possível determinar o tempo até falha e suspensões. Se o item for não reparável, utilizar análise de dados de vida e se for reparável, utilizar análise de crescimento de confiabilidade. O trabalho não ficaria restrito à coleta apenas. A ideia é que o estudo revele maneiras de entender os processos da empresa na qual o sistema está em operação e propor maneiras de adquirir dados automaticamente. Por exemplo, extrair a data de fabricação da plataforma de dados da empresa onde esta informação já é utilizada. Entender onde e como a data de instalação e remoção, data de reparo, data de reinstalação do componente no sistema são registradas e como podem ser migradas para um sistema de gestão de dados específico para confiabilidade. Existem sistemas prontos que já fazem a gestão de ativos. Todavia, o trabalho teria como foco aprender as particularidades da empresa em estudo e entender o fluxo das informações de forma a adaptar, organizar e estabelecer as mudanças e melhorias para se instaurar um processo de coleta e análise de dados sistemático, personalizado para o caso específico do estudo.

Uma ramificação da proposta exposta no primeiro parágrafo, seria o estudo do dia a dia dos técnicos que trabalham diretamente com os sistemas de uma determinada empresa. Quais são as dificuldades encontradas no registro das falhas? Que tipo de mudança de processo poderia resolver os obstáculos existentes e favorecer a coleta e registro preciso das informações? Além disso, um ponto largamente estudado no campo de jogos eletrônicos que pode estimular a atividade de aquisição de dados é o processo de recompensa. Que tipo de reconhecimento pode ser implementado para incentivar a participação de cada colaborador envolvido com a operação e manutenção de sistemas na construção de bancos de dados mais completos e precisos? Existe alguma maneira de criar algum tipo de pontuação para os técnicos que mais contribuírem? Esta pontuação poderia gerar bônus ou entregar prêmios para os colaboradores com maior número de pontos obtidos a cada semestre ou ano? A criação de algum tipo de aplicativo de *smartphone* poderia ser criado, a fim de auxiliar este processo? Enfim, o tema do trabalho seria o estudo e entendimento do processo de aquisição de dados com foco nas características humanas que podem favorecer a coleta das informações. Adicionalmente, como implementar ferramentas que estimulem os colaboradores, baseadas nos mecanismos de recompensa.

Uma segunda sugestão baseada na coleta de dados seria o estudo de como os componentes podem ser projetados pensando na transmissão automática dos

registros de instalação e remoção, reinstalação, parâmetros de operação, quantidade de atuações ou ciclos. Isso ajudaria a reduzir o esforço e recursos para a aquisição das informações de falha, tipo e quantidade de utilização do item e níveis de estresse. O trabalho pode abordar todas as ferramentas, ideias e novas tecnologias que tem o potencial de ser empregadas no projeto de componentes e sistemas “inteligentes” no que diz respeito ao registro automático de dados para substanciar as análises de confiabilidade.

Outra sugestão de tema para monografia é a avaliação de um sistema a partir das medidas de importância utilizadas neste trabalho. Quais são os pontos mais vulneráveis do sistema? Quais os componentes que contribuem para uma maior parcela do risco do evento topo da árvore de falha? Quais componentes podem ser substituídos a fim de se alcançar maiores patamares de segurança? Como os resultados gerados pelas medidas de importância podem auxiliar na criação do plano de manutenção? Que tipo de mudanças podem ser implementadas a fim de reduzir o custo da operação e manutenção sem que o nível de segurança do sistema seja impactado? O trabalho geraria recomendações de modificação de sistema, redução de custo e informações para criação de um plano de manutenção com foco em segurança. A base da análise seria a utilização das medidas de importância aplicadas às árvores de falha.

REFERÊNCIAS

BENBOW, Donald. BROOME, Hugh. **The Certified Reliability Engineer Handbook**. Wisconsin: American Society for Quality, 2009.

Dennehy, Penny. The Boeing Company. Presentation: Improved Performance through the use of Defined Metrics. Disponível em: http://www.spec2000.com/presentations/georget.pdf. Acesso em: 31 jul. 2018.

Department of Defense, USA. **Electronic Reliability Design Handbook** – MIL-HDBK-338 revision B. 1998.

Department of Defense, USA. **System Safety** – MIL-STC-882 revision E. 2012.

DHILLON, B. S. **Design Reliability**: Fundamentals and Applications. Ontario: CRC Press, 1999.

FAA – Federal Aviation Administration. **System Design and Analysis** - AC/AMJ No: 25.1309 - Draft ARSENAL revised. 2002. Disponível em: https://www.faa.gov/regulations_policies/rulemaking/committees/documents/media/TAEsdaT2-5241996.pdf. Acesso em: 1 ago. 2018.

NASA Office of Safety and Mission Assurance. **Fault Tree Handbook with Aerospace Applications**. Washington: NASA, 2002.

O'CONNOR, Patrick. KLEYNER, Andre. **Practical Reliability Engineering**. 5th ed. West Sussex: Wiley, 2012.

SAE International. **Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment –** ARP 4761. 1996.

SAE International. **Safety Assessment of Transport Airplanes in Commercial Service –** ARP 5150. 2003.

SMITH, David J. SIMPSON, Kenneth G. L. **Safety Critical Systems Handbook**: A Straight forward Guide to Functional Safety, IEC 61508 (2010 EDITION) and Related Standards. Amsterdam: Elsevier, 2010.

Idaho National Laboraty. Importance Measures. Disponível em: https://www.nrc.gov/docs/ML1216/ML12160A479.pdf. Acesso em: 1 ago. 2018.

APÊNDICE A – ÁRVORE DE FALHA DO EXEMPLO DA NUREG-0492

Este apêndice apresenta a árvore de falha do sistema de caixa de distribuição de potência da NUREG-0492 para a qual é mostrado exemplo de aplicação do método de identificação de componentes e grupos de corte críticos em árvores de falha.

Figura A.A.1 - Árvore de Falha do Exemplo da NUREG-0492 – Página 1

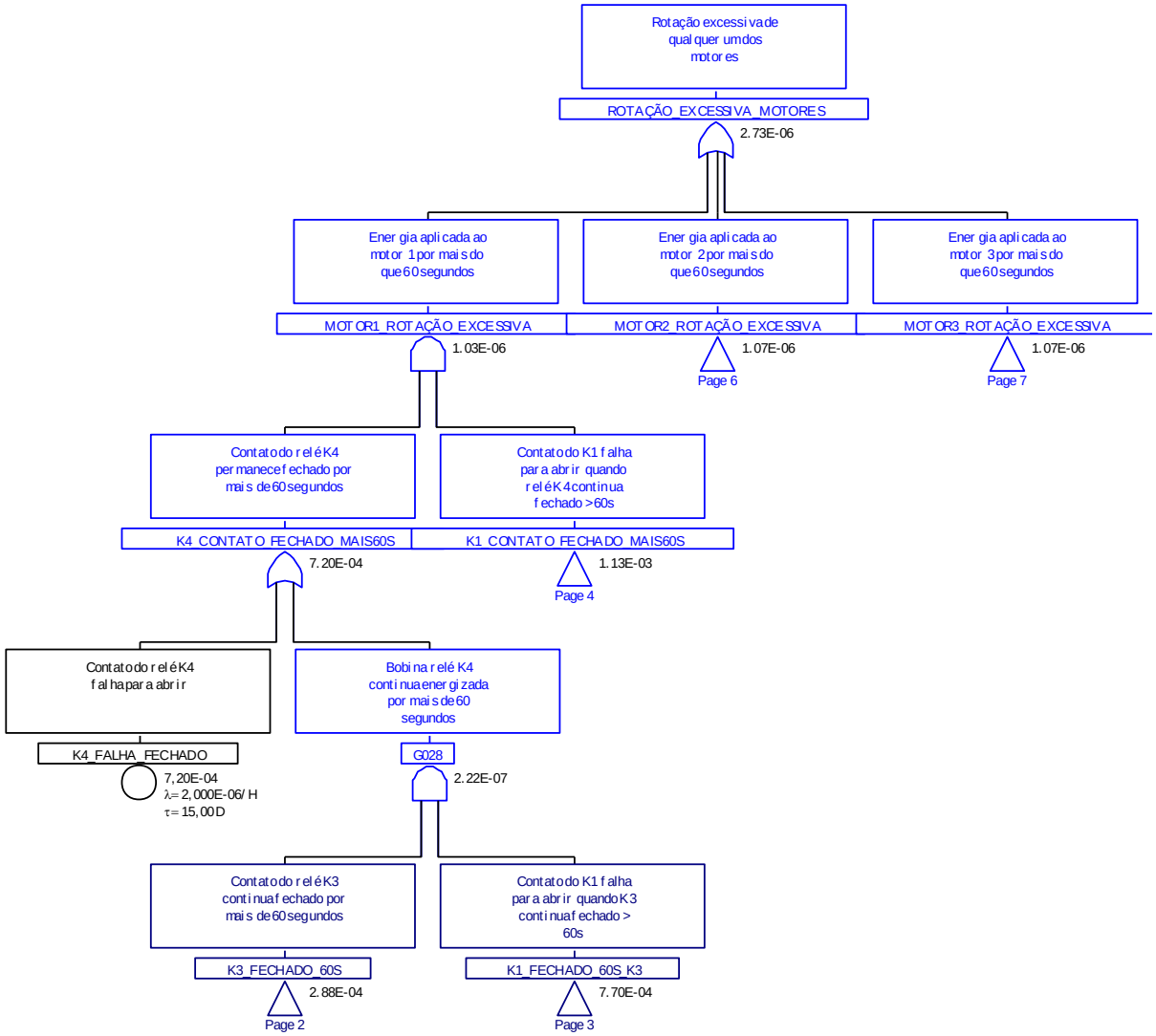


Figura A.A.2 - Árvore de Falha do Exemplo da NUREG-0492 – Página 2

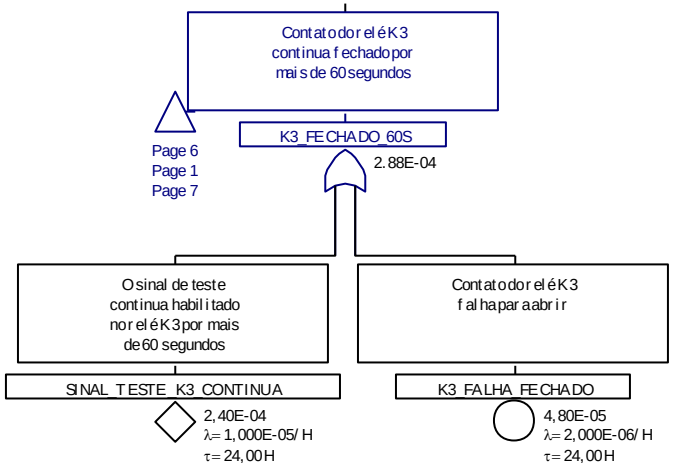


Figura A.A.3 - Árvore de Falha do Exemplo da NUREG-0492 – Página 3

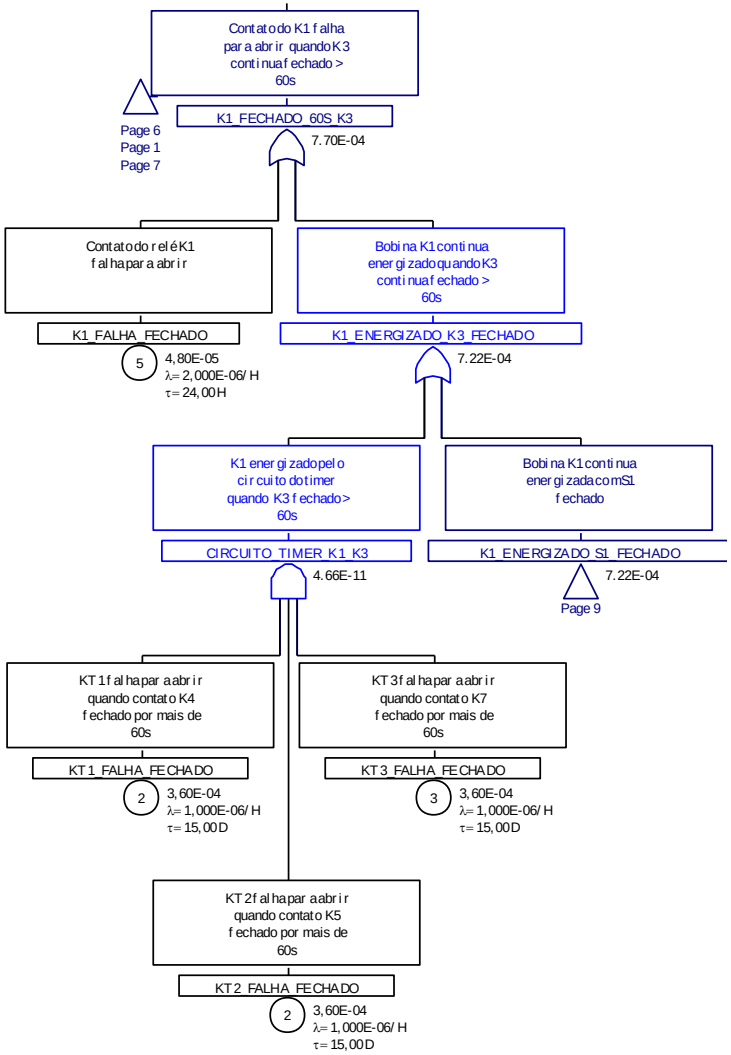


Figura A.A.4 - Árvore de Falha do Exemplo da NUREG-0492 – Página 4

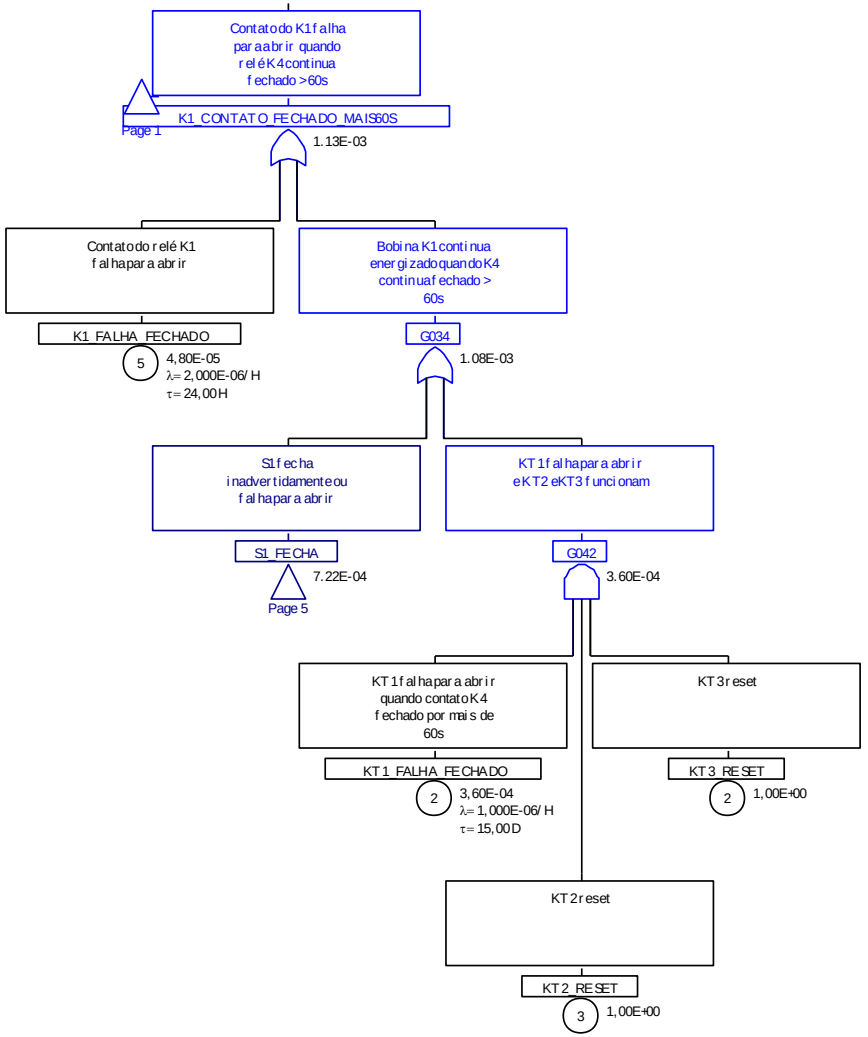


Figura A.A.5 - Árvore de Falha do Exemplo da NUREG-0492 – Página 5

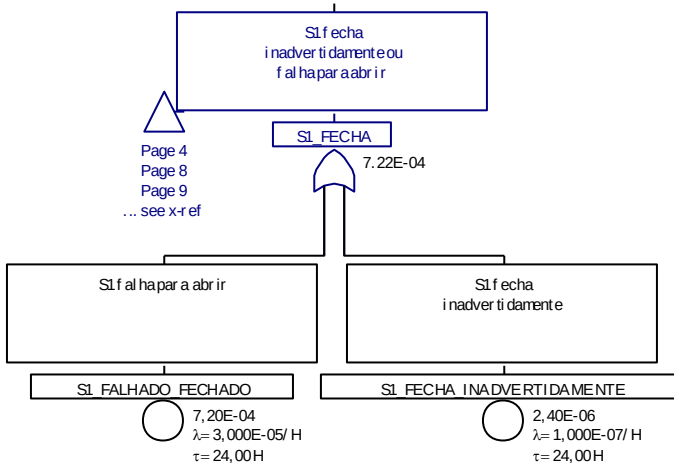


Figura A.A.6 - Árvore de Falha do Exemplo da NUREG-0492 – Página 6

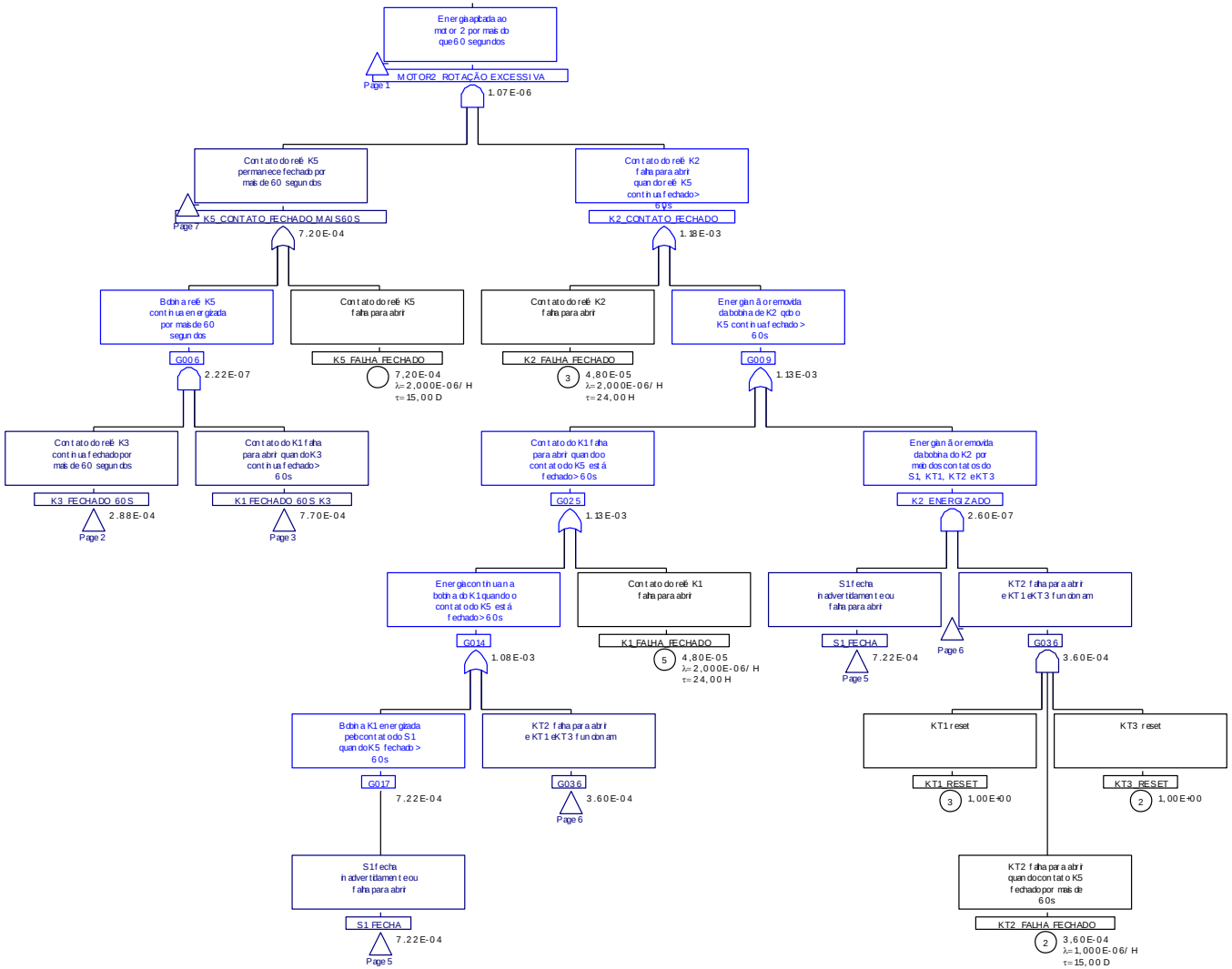


Figura A.A.7 - Árvore de Falha do Exemplo da NUREG-0492 – Página 7

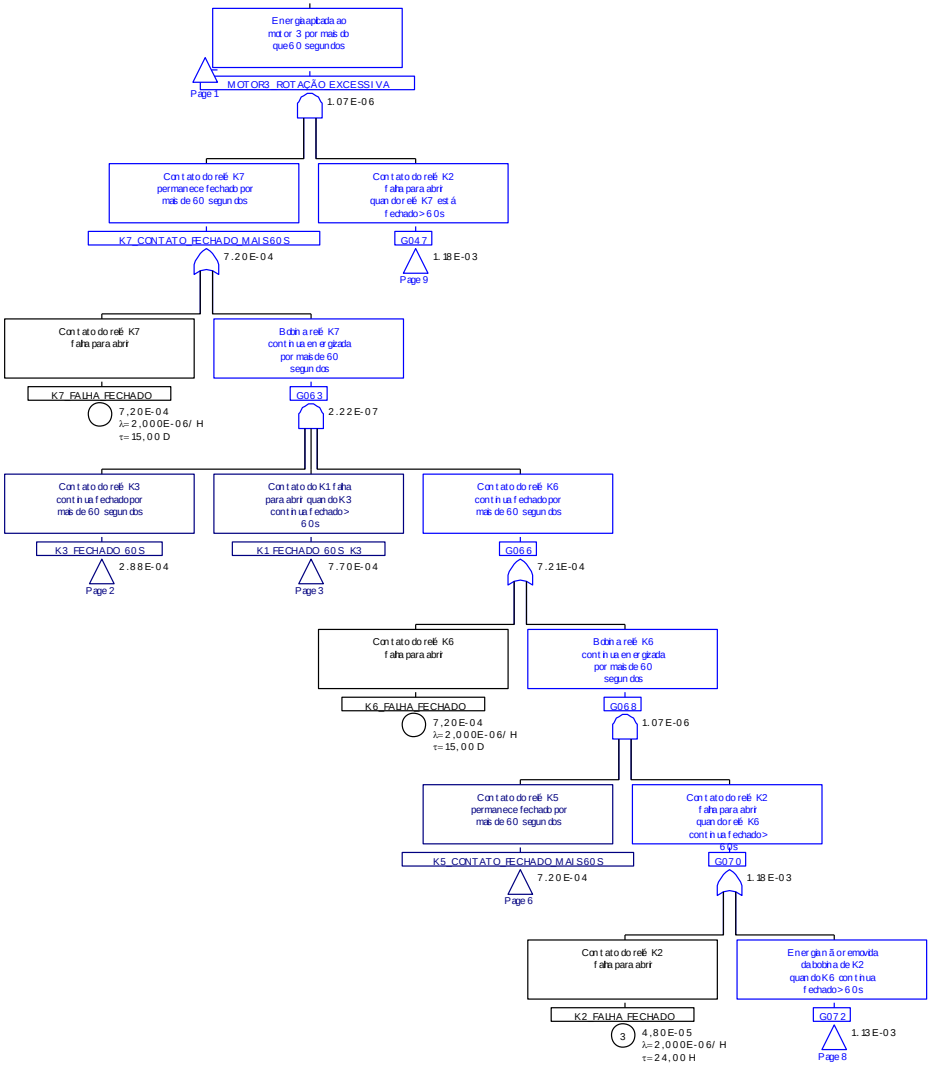


Figura A.A.8 - Árvore de Falha do Exemplo da NUREG-0492 – Página 8

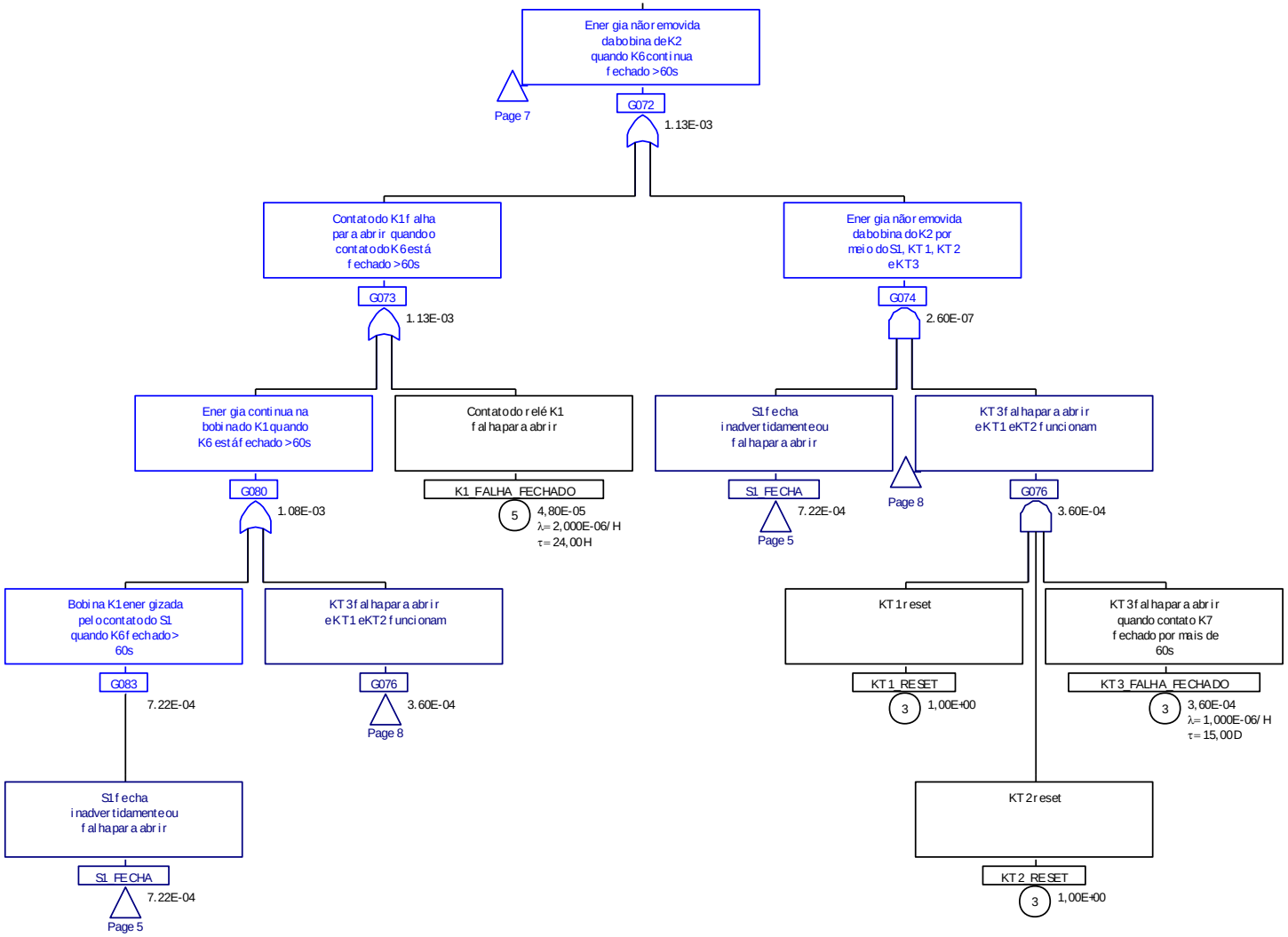
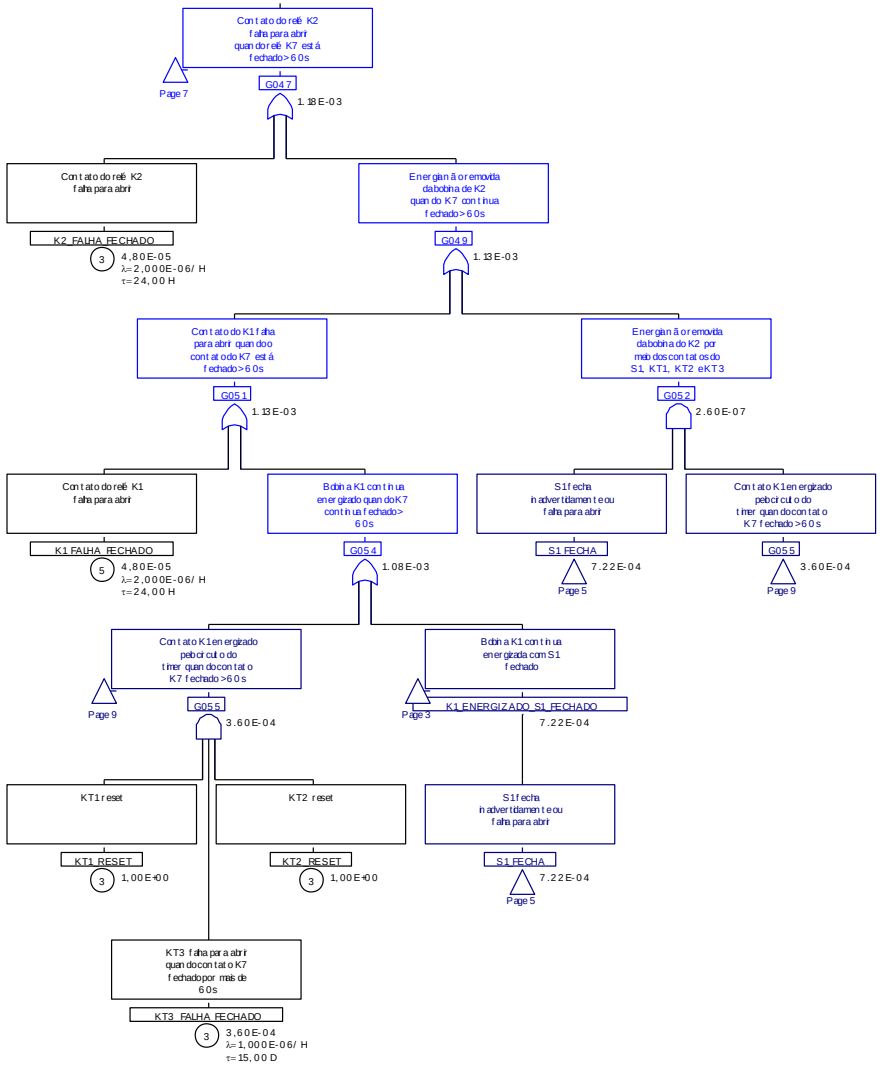


Figura A.A.9 - Árvore de Falha do Exemplo da NUREG-0492 – Página 9



APÊNDICE B – ÁRVORE DE FALHA DO SISTEMA 1

Este apêndice apresenta a árvore de falha do sistema 1 para a qual o método de identificação de componentes e grupos de corte críticos em árvores de falha foi apresentado em detalhes.

Figura A.B.1 - Árvore de Falha do Sistema 1 – Página 1

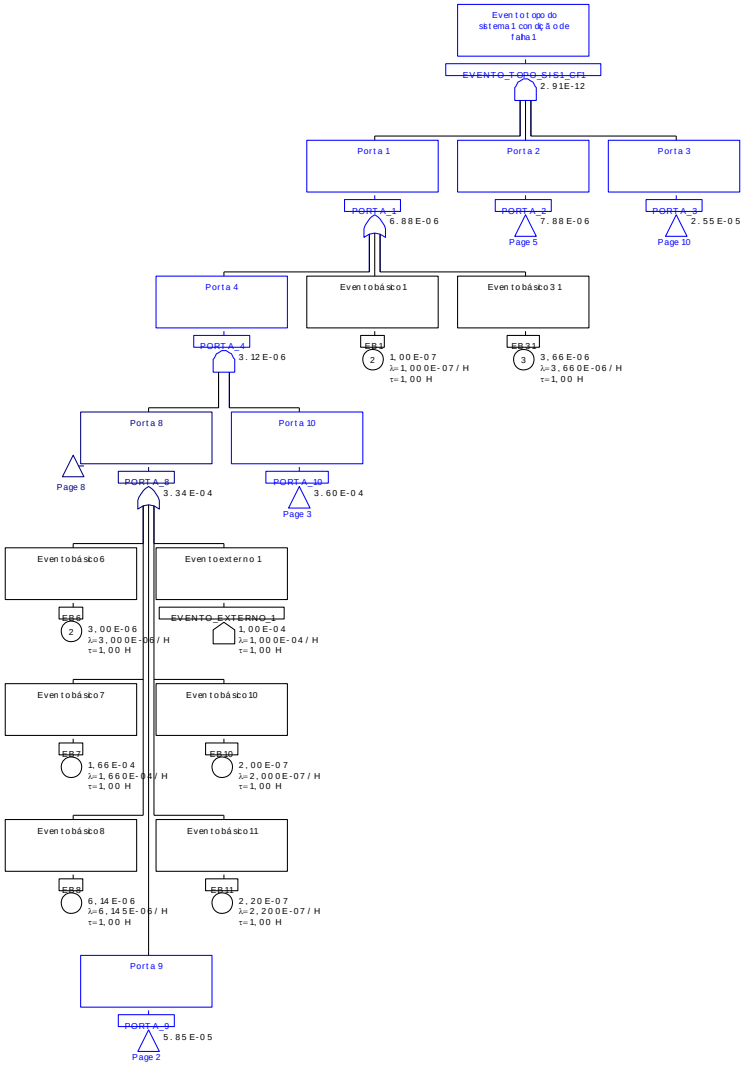


Figura A.B.2 - Árvore de Falha do Sistema 1 – Página 2

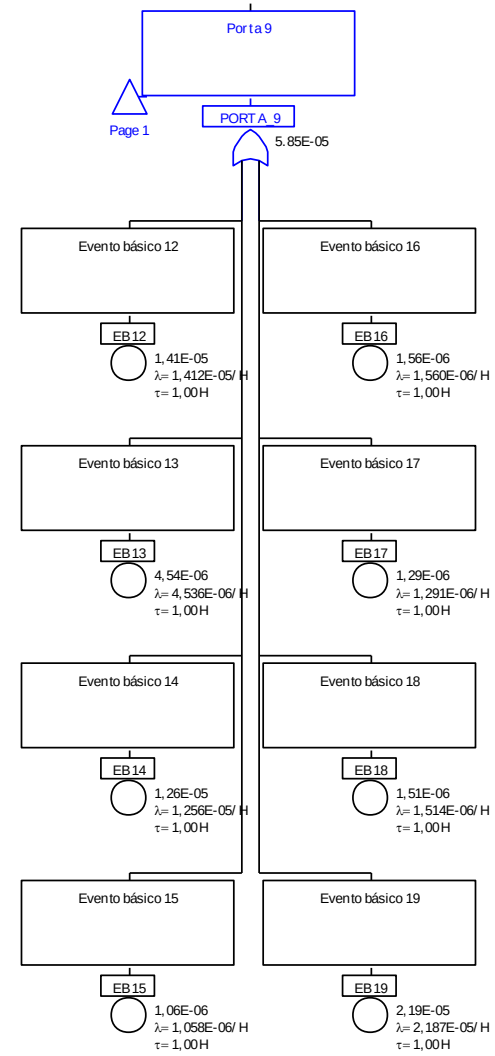


Figura A.B.3 - Árvore de Falha do Sistema 1 – Página 3

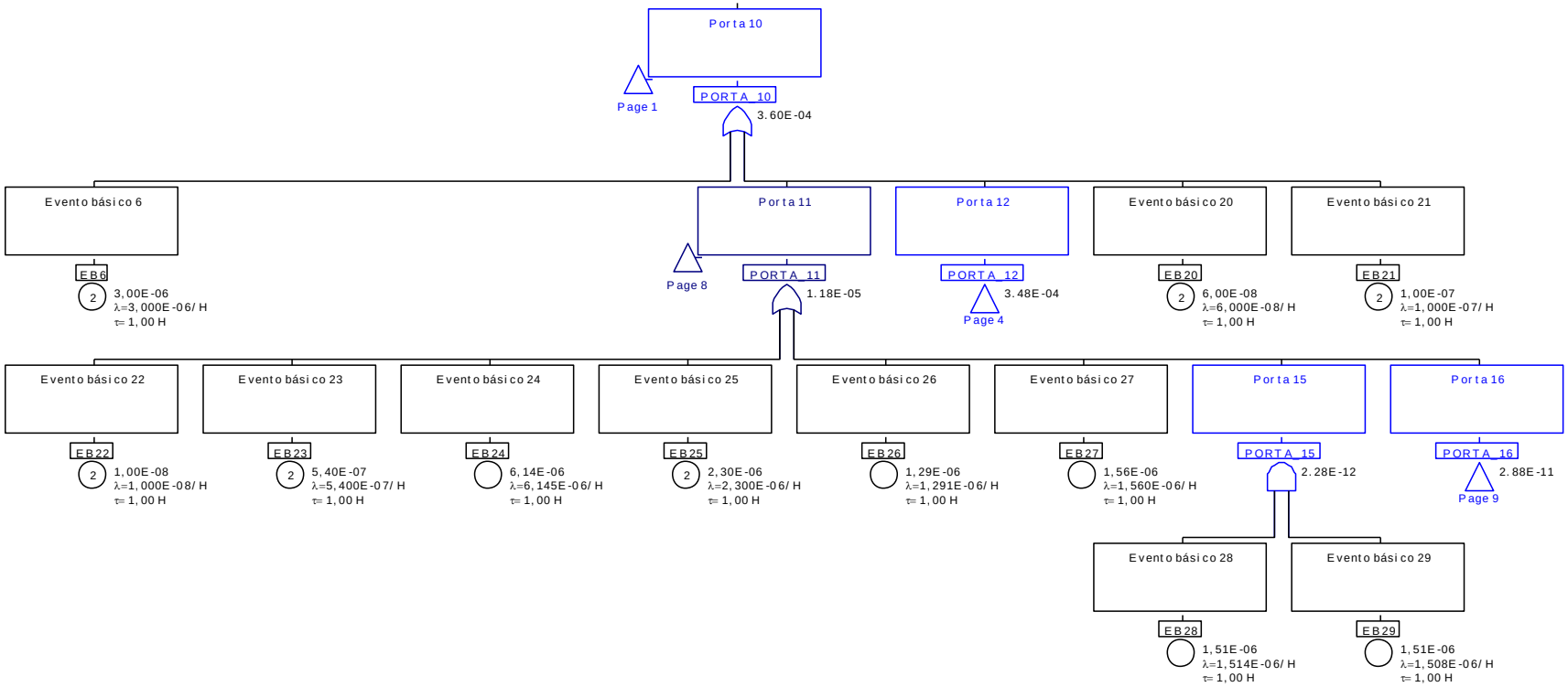


Figura A.B.4 - Árvore de Falha do Sistema 1 – Página 4

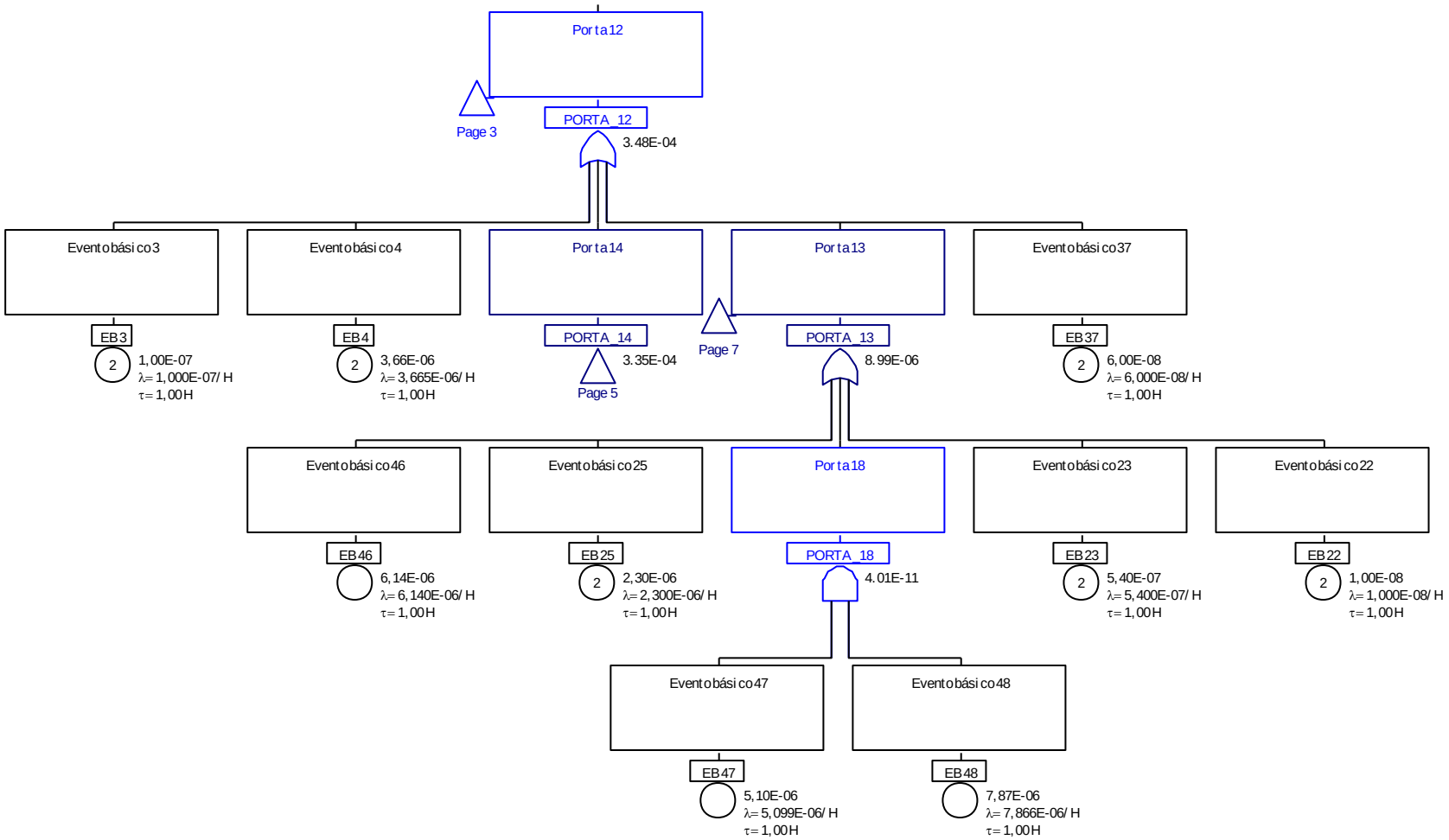


Figura A.B.5 - Árvore de Falha do Sistema 1 – Página 5

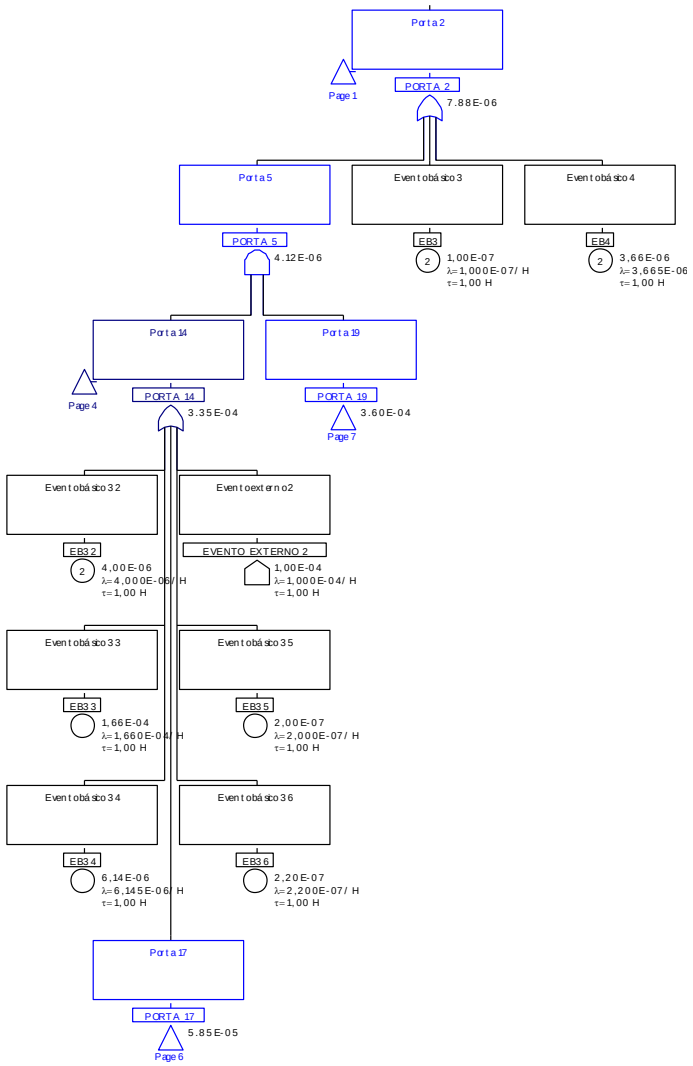


Figura A.B.6 - Árvore de Falha do Sistema 1 – Página 6

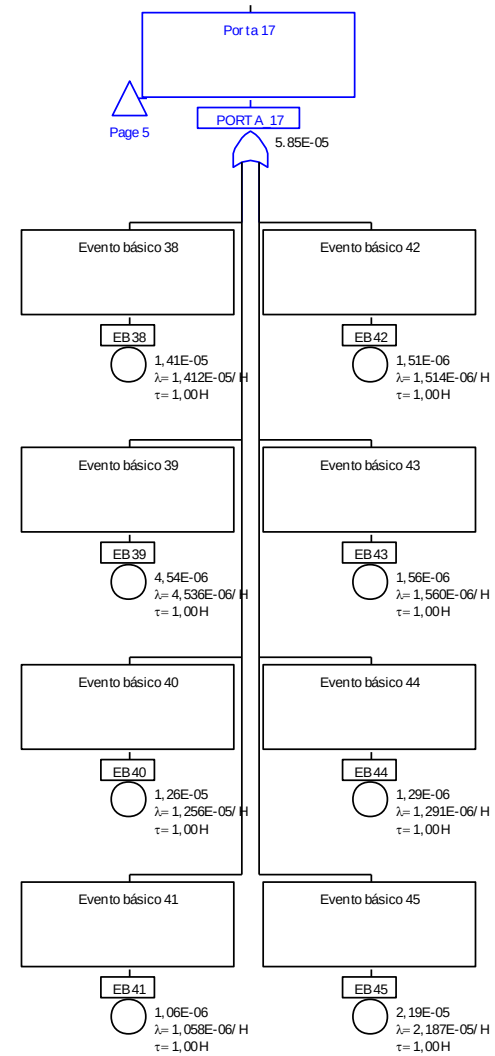


Figura A.B.7 - Árvore de Falha do Sistema 1 – Página 7

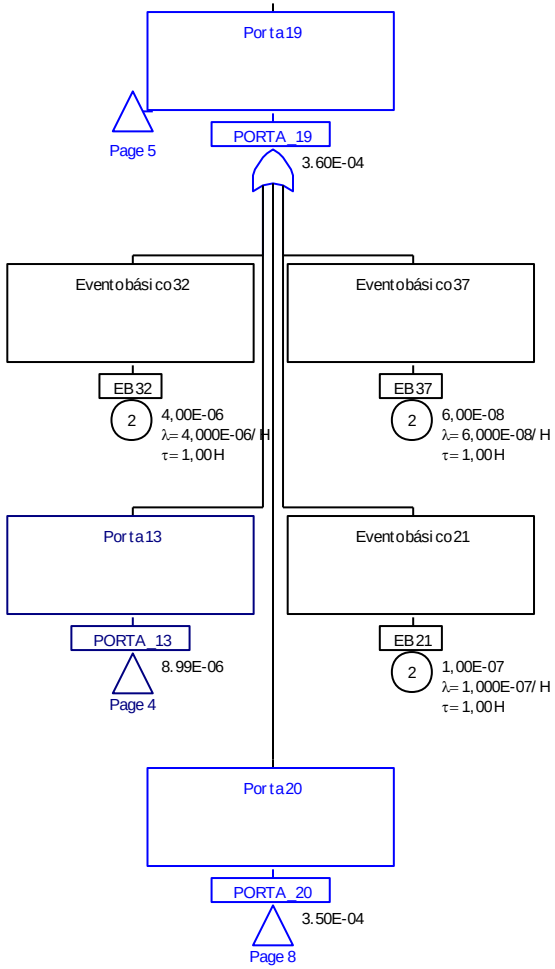


Figura A.B.8 - Árvore de Falha do Sistema 1 – Página 8

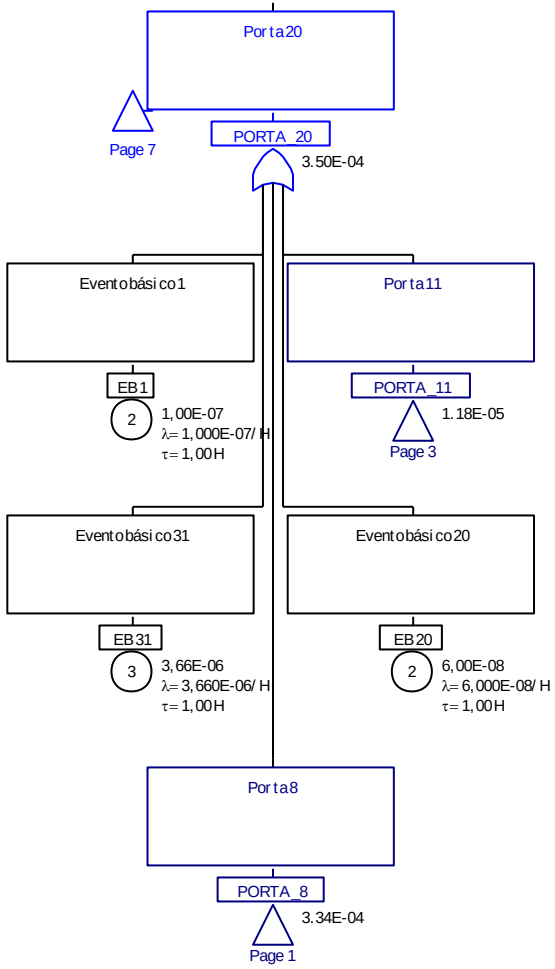


Figura A.B.9 - Árvore de Falha do Sistema 1 – Página 9

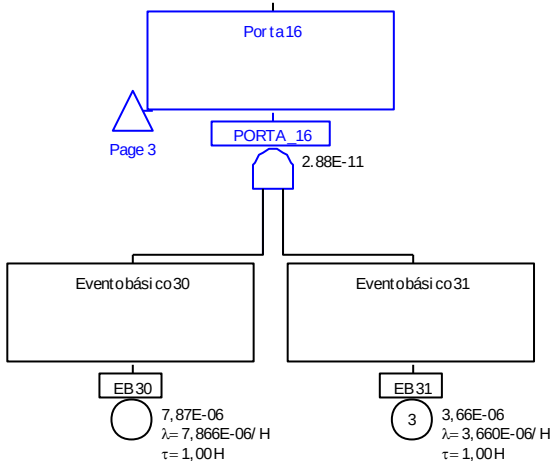


Figura A.B.10 - Árvore de Falha do Sistema 1 – Página 10

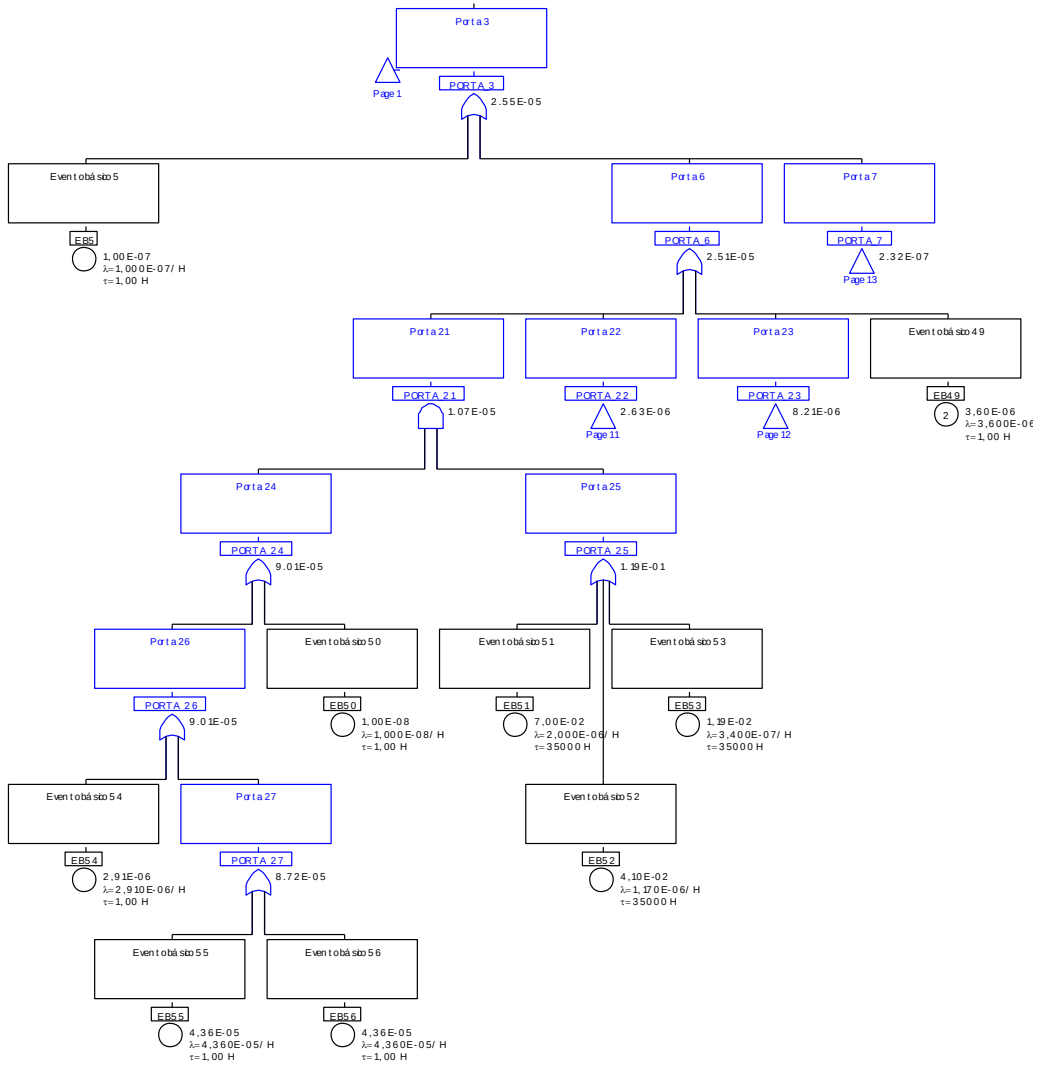


Figura A.B.11 - Árvore de Falha do Sistema 1 – Página 11

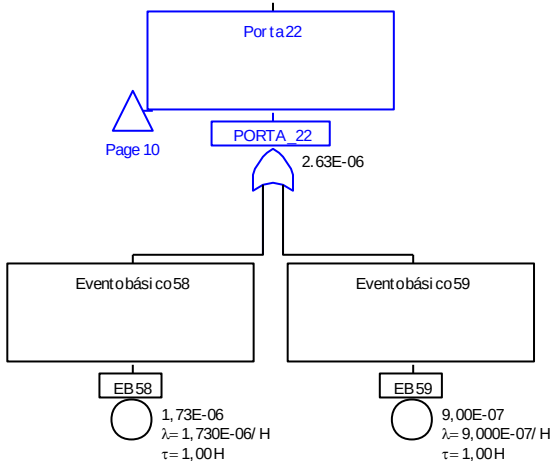


Figura A.B.12 - Árvore de Falha do Sistema 1 – Página 12

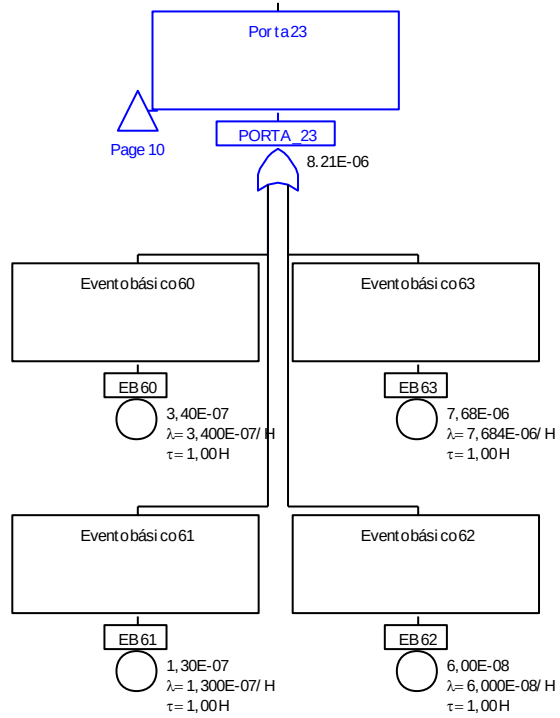


Figura A.B.13 - Árvore de Falha do Sistema 1 – Página 13