UNIVERSIDADE FEDERAL DE SANTA CATARINA
DEPARTAMENTO DE ENGENHARIA MECÂNICA

Heitor Azuma Kagueiama

MÉTODO DE CARACTERIZAÇÃO E ANÁLISE DE CENÁRIOS DE FALHAS OCULTAS

Florianópolis

2018

Heitor Azuma Kagueiama

MÉTODO DE CARACTERIZAÇÃO E ANÁLISE DE CENÁRIOS DE FALHAS OCULTAS

Tese submetida ao Programa de Pós-Graduação em Engenharia Mecânica para a obtenção do Grau de Doutor em Engenharia Mecânica.
Orientador: Prof. Acires Dias, Dr. Eng.

Florianópolis

2018

Ficha de identificação da obra elaborada pelo autor, através do
Programa de Geração Automática da Biblioteca Universitária da UFSC.

Kagueiama, Heitor Azuma
Método de caracterização e análise de cenários de falhas ocultas / Heitor Azuma Kagueiama ; orientador, Acires Dias, 2018.
175 p.

Tese (doutorado) - Universidade Federal de Santa Catarina, Centro Tecnológico, Programa de Pós Graduação em Engenharia Mecânica, Florianópolis, 2018.

Inclui referências

1. Engenharia mecânica. 2. Análise de risco. 3. Análise de falhas. 4. Falhas ocultas. I. Dias, Acires. II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Engenharia Mecânica. III. Título.

Heitor Azuma Kagueiama

MÉTODO DE CARACTERIZAÇÃO E ANÁLISE DE CENÁRIOS DE FALHAS OCULTAS

Esta Tese foi julgada aprovada para a obtenção do Título de "Doutor em Engenharia Mecânica", e aprovada em sua forma final pelo Programa de Pós-Graduação em Engenharia Mecânica.

Florianópolis, 27 de agosto 2018.

Prof. Jonny Carlos da Silva, Dr. Eng.
Coordenador do Curso

Prof. Acires Dias, Dr. Eng.
Orientador

Banca Examinadora:

Prof. Acires Dias, Dr. Eng.
Presidente

Prof. Márcio José das Chagas Moura, Dr. Eng.
Relator

Banca Examinadora (continuação):

Prof. Victor Juliano De Negri, Dr. Eng.

Prof. André Ogliari, Dr. Eng.

À minha família e amigos, com carinho.

AGRADECIMENTOS

Ao professor Acires Dias, muito obrigado pela orientação e apoio não só no desenvolvimento deste trabalho mas ao longo dos anos de convivência. Sempre servindo de inspiração ao longo da minha vida acadêmica.

Ao grande amigo Eduardo Yuji Sakurada pelas discussões que deram origem a este trabalho, pela revisão e todo o apoio.

Ao Marcelo Cavalcante dos Santos por toda a ajuda e empenho no desenvolvimento dos modelos computacionais desta tese.

Aos colegas do Núcleo de desenvolvimento Integrado de Produtos (NeDIP) pela boa companhia, pelas discussões, pelos cafés da tarde e pelas batalhas digestivas.

Aos parceiros do quiosque pela experiêencia na construção civil e pelas ótimas cervejas.

Aos parceiros de escalada que proporcionaram momentos vitais para a sanidade mental ao longo desse processo.

À Luiza pela paciência, companheirismo e apoio durantes esses vários anos de doutorado.

À família, em especial aos meus pais, Alberto e Harumi, pelo apoio incondicional.

Ao Conselho Nacional de Pesquisa e Desenvolvimento Científico (CNPq) pelo auxílio financeiro na forma de bolsa de doutorado.

And so castles made of sand slips into the sea.
Eventually

Jimi Hendrix

RESUMO

Áreas de engenharia como aeroespacial, nuclear, petroquímica e comunicação envolvem sistemas complexos portadores de grande quantidade de energia. Nessas áreas é premissa de projeto a análise e identificação dos diferentes cenários operacionais e de falhas visando garantir a confiabilidade, aumentar a segurança e reduzir os riscos de acidentes. Considerando estes sistemas, o foco deste trabalho está nos cenários que envolvem as falhas ocultas. Normalmente atribuídas a falhas em sensores e componentes redundantes, as falhas ocultas não são percebidas imediatamente após sua ocorrência, pois não alteram o comportamento do sistema. Um componente redundante em falha, ou um atuador normalmente desligado são alguns exemplos de componentes sujeitos a falhas ocultas. Nesses casos, a falha só é percebida quando há a demanda pelo funcionamento do componente, podendo expor o sistema a cenários críticos dependendo do momento em que os componentes são demandados. O objetivo geral do trabalho é desenvolver um método que permita identificar falhas ocultas, os cenários de combinação de eventos que as caracterizam, avaliar a probabilidade de ocorrência desses cenários e seus impactos sobre a operação de sistemas. Para avaliar a solução proposta foi realizada a análise do sistema de combustível de aviões de caça, especificamente do tanque coletor, sob diferentes condições de voo: normal, invertido em manobra e invertido sustentado. O tanque coletor é composto por válvulas cuja função é reter combustível suficiente para executar manobras sob gravidade negativa, sendo a falha na alimentação de combustível durante a execução dessas manobras potencialmente catastrófica. Utilizando o método de Monte Carlo são obtidas amostras aleatórias de padrões de voo e ocorrência de falha que permitem verificar os cenários que resultam em falhas catastróficas do sistema ao longo do seu ciclo de vida pela falta de combustível no tanque coletor. Enquanto resultados, apresentam-se diferentes cenários de voo nos quais a aeronave está exposta a falhas ocultas, para descrever alternativas de projeto com vista a caracterizar e reduzir os riscos decorrentes destas falhas. É possível, por exemplo, evidenciar o comportamento do sistema sob diferentes condições de voo e verificar a influência que o uso de componentes diferentes no projeto do tanque tem sobre o volume de combustível disponível para a execução de manobras dentro de uma missão. Torna-se evidente a importância de combinar a ocorrência de falha com a operação do sistema para avaliar a exposição aos riscos

Palavras-chave: Falhas ocultas, confiabilidade, análise de risco, projeto de sistemas

ABSTRACT

Airspace, nuclear, chemical and communications engineering involve complex systems that carry great amount of energy. It is a design goal to analyse these systems and identify different operation and failure scenarios to garantee the reliability, increase safety and reduce risks. Given the complexity of such systems, this thesis focus on the scenarios that involve hidden failures. Usually these failures are attibuted to sensors and redundant components and are not detected because they don't have an emediate effect over the system behavior. A redundant component that fails, or an electric actuator that is normally off are two examples of components that are subjects to hidden failures. In these cases the failure is only detected once the components are demanded to become active, which might expose the system to critical scenarios depending on the moment that these transitions are demanded. The main goal of this thesis is the development of a method that allows the identification of hidden failure, the combination of events that characterize them, evaluate the occurrence probability and the impact over the system operation. To evaluate the proposed solution, combat aircraft fuel systems are analysed, specifically the colector tank, under different flight conditions: inverted, inverted during maneuvers, and sustained inverted. The collector tank has a set of flapper check valves that retain enough fuel to execute negative g maneuvers, and failues in the engine feed during these maneuvers are potencially catastrophic. Monte Carlo method is used for sampling flight profiles and failure times allowing the analysis of the scenarios that result in accidents throughout the system life cycle. As a result, different flight scenarios are described when the aircraft is exposed to risk scenarios, in order to identify design alternatives to reduce the risk exposure. As an example, it is possible to simulate the system behavior using different components and check how the fuel volume behaves during the maneuvers. Is becomes clear that it is necessary to combine failure occurence and the system operation to evaluate the risk exposure when it comes to hidden failures, instead of just using traditional reliability approaches that relates hidden failures only to redundant systems.

Keywords: Hidden failures, system safety, reliability, risk analysis, system design

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

Um sistema é a combinação de subsistemas e componentes, cujas funções são relacionadas para o cumprimento de um propósito específico. Um avião é composto pela fuselagem, asas, motores, trem de pouco, sistemas de controle, sistema elétrico entre outros com o propósito de gerar empuxo, forças de sustentação e voar. Um carro também é um sistemas composto por subsistemas e componentes (motor, chassi, suspensão, transmissão etc.)

O desempenho dessas funções pode ser verificado monitorando variáveis de controle como força, velocidade, volume etc., que variam ao longo da operação do sistema e determinam como este se comporta e desempenha suas funções. Se os motores não geram o empuxo (força) suficiente, o avião não é capaz de gerar as forças de sustentação e voar.

Falha é um evento que interfere no desempenho da função do item, podendo torná-lo parcial ou totalmente inoperante. Falha no sistema hidráulico das asas de um avião impedem que os atuadores alterem as superfícies de controle e ajustem as forças de sustentação necessárias para a realização do voo. As falhas podem ser analisadas em relação ao sistema como um todo, ou em relação aos subsistemas e componentes.

As falhas analisadas em nível de subsistemas e componentes podem ser então relacionadas para representar como elas afetam o sistema. Por exemplo, considerando-se um carro, pode-se verificar que ele simplesmente não liga. Nesse caso, não há distinção entre os subsistemas que não funcionam e que causam a falha.

Porém, a análise pode ser feita considerando os subsistemas e componentes. Nesse caso, se não há partida, percebe-se que a falha pode estar no sistema elétrico. Se há partida mas não há combustão, pode ser falha no sistema de combustível ou no motor. Nesse caso, as falhas tem causas e efeitos distintos para os subsistemas, mas o efeito sobre o sistema global (carro) é o mesmo: o carro não liga.

A função de um item - que pode ser um sistema, subsistemas ou componentes-, é definida na fase de projeto conceitual a partir dos requisitos do produto e de projeto, sistematizados e priorizados no projeto informacional. O projeto conceitual é a fase do processo de projeto onde são desenvolvidas as concepções alternativas para o produto (BACK et al., 2008), que melhor cumprirão a função do produto. A importância do estudo da falha ocorre pelo fato desta interferir na função do produto.

Ao longo do processo de projeto de sistemas, principalmente para os portadores de grande quantidade de energia ou fundamentais num processo técnico, os atributos de confiabilidade e risco devem ser obrigatoriamente

cumpridos, dada a severidade envolvida na perda da função devido a ocorrência de falhas.

A confiabilidade é um atributo que prioriza estudos e ações para garantir a função ao longo do ciclo de vida. Já os atributos relacionados à gestão dos riscos visa levantar, organizar e analisar as potencialidades dos perigos existentes nos princípios de solução requeridos para o desempenho da função e os riscos que podem advir, caso ocorra alguma falha de algum item.

Tanto a confiabilidade quanto os riscos são atributos inerentes ao tipo de produto projetado e dos conceitos de projeto selecionados.

Se um sistema necessita de um sistema motriz, por exemplo, como é o caso de um carro e de um avião, se a opção de projeto for utilizar motor elétrico ou a combustão, os princípios construtivos e de funcionamento dos dois princípios de solução são bastante distintos. Um motor a combustão está sujeito a forças mais severas sobre seus componentes (pela explosão que ocorre na câmara de combustão), mas o motor elétrico possui uma quantidade grande de componentes e os componentes são construtivamente mais suscetíveis às demandas do ambiente. Dessa forma a confiabilidade dos dois sistemas é claramente distinta.

Se considerarmos os perigos, essa diferença é ainda maior, já que pelas forças envolvidas no motor a combustão e pelo uso de combustível inflamável, os perigos podem se combinar e apresentar riscos de explosão, com consequências para a vida de pessoas.

O tipo de sistema que se está projetando define os requisitos de projeto, incluindo requisitos relacionados a confiabilidade e ao risco. Novamente comparando um avião e um carro, os requisitos de confiabilidade e os riscos envolvidos com o avião são consideravelmente mais exigentes que os de um carro. A queda de uma avião comercial tem consequência muito maior que a batida de um carro, tanto pela quantidade de passageiros afetados quanto para o ambiente ao redor.

Com base nos requisitos do produto definem-se conceitos que obedecem as exigências relativas à confiabilidade e ao risco. Um princípio de projeto comum para aumentar a confiabilidade e consequentemente reduzir os riscos de um evento indesejado, como a queda de um avião, é a utilização de redundâncias.

Quando se quer aumentar a confiabilidade e mitigar os riscos, utiliza-se o princípio de redundâncias. Esse princípio pode ser visto no projeto de aviões e seleção dos sensores de altitude. É exigência de projeto que os vários sensores redundantes sejam de fabricantes e lotes distintos, visando evitar que todos os sensores falhem ao mesmo tempo. O uso de redundâncias têm o objetivo de manter a função do produto mesmo que a falha de um dos itens venha a ocorrer. Essas redundâncias podem ser ativas, quando todos

os componentes operam ao mesmo tempo (como o exemplo dos sensores de altitude) ou passivas, quando um dos componentes fica em *stand by* e entra em operação quando o componente principal falha.

Quando a falha ocorre no item que está atuando na função, sua ocorrência pode ter efeito imediato sobre o funcionamento do sistema que permite sua detecção e, nesses casos, a falha é chamada de falha evidente. Por vezes, as falhas ocorrem nos itens que estão na condição de redundância passiva (*stand by*), podendo tornar sua ocorrência não detectável, e nesses casos as falhas são chamadas de falhas ocultas.

Assim, dependendo da facilidade de detecção, as falhas são classificadas como evidentes ou ocultas. Vale ressaltar que o conceito de falhas oculta não está restrito à falha de componentes redundantes, mas aos efeitos que as falhas tem sobre o funcionamento do sistema, que podem torná-las detectáveis ou não.

Este é um contexto de ocorrência de falhas que envolve alguma complexidade e é de extrema importância para os casos de sistemas técnicos que contém grande quantidade de energia, como por exemplo: usinas nucleares, sistemas aviônicos, aero-espacial, petróleo e petroquímica, ou mesmo sistema de grande importância para o mundo contemporâneo como os sistemas de abastecimento de água, retiradas de efluentes, geração, transmissão e distribuição de energia elétrica, sistemas de comunicação e telefonia, sistemas hospitalares etc.

Diante deste contexto, esta pesquisa tem o objetivo de desenvolver um método para modelagem e simulação de falhas ocultas. Com isso, busca-se contribuir em nível do projeto conceitual para auxiliar na melhoria da confiabilidade e segurança de sistemas técnicos que estão sendo concebidos, para fazer atualizações tecnológicas, ou ainda para estudar comportamentos de sistemas já em operação, para um determinado ciclo de vida.

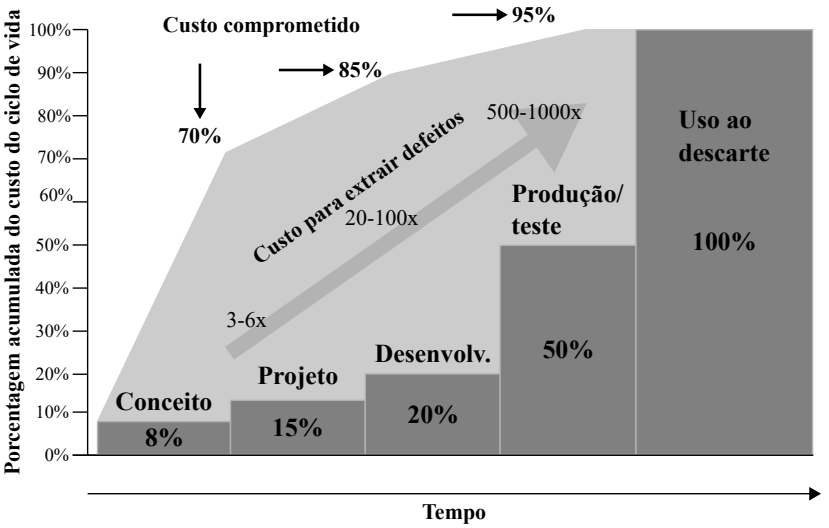
Estabelecer um método de análise que possa ser aplicado já na fase de projeto conceitual permite que os projetistas possam testar diferentes conceitos e verificar a exposição ao risco que cada princípios de solução proporciona. A identificação dos cenários de combinação de eventos que levam a incidentes e acidentes nas fases iniciais de projeto envolve alto grau de abstração, sendo muitas vezes impossível identificar em detalhe esses cenários. Como será visto ao longo deste trabalho, é possível utilizar modelos de falha que permitem cruzar eventos de falha e eventos de operação para gerar amostras aleatórias dos possíveis cenários de falha.

Segundo Pahl e Beitz (1977), aproximadamente 80% dos custos e possíveis problemas em um produto são comprometidos durante a fase de projeto e, por sua vez, aspectos como custo, qualidade e confiabilidade são inseridos no produto essencialmente na fase de projeto conceitual, por meio

da seleção de princípios de solução que satisfazem os requisitos do produto. Por essa razão, visando atender os requisitos de confiabilidade e gerenciar os riscos de novas concepções de produto, sem a necessidade de reprojeto, é necessário analisar a ocorrência de falhas o mais cedo possível durante o projeto.

Haskins et al. (2006) traz na Figura 1.1 a representação do comprometimento dos custos ao longo do ciclo de vida de um produto. As porcentagens ao longo do tempo representam o custo acumulado, concordando com a afirmação de Pahl e Beitz (1977) em que 8% dos custos do produto são comprometidos durante a concepção. A curva indica que quanto mais cedo se identificam melhorias de projeto, menor os custos para extrair eventuais defeitos, sendo que menor custo do produto é comprometido. Pode-se concluir pela figura que decisões tomadas durante o projeto sem os benefícios de contar com informações e análises pode trazer custos inaceitáveis para o produto.

Figura 1.1 – Custo comprometido durante o projeto



Fonte: Adaptado de Haskins et al. (2006)

Na análise de confiabilidade faz-se a caracterização das falhas para cada uma das funções do item que está sendo projetado e, quando possível, a quantificação das probabilidades de ocorrência. Essa quantificação é feita a partir do registro das ocorrências observadas em campo, durante o uso de um sistema e seus componentes, ou por meio de testes. Com esses dados de falha,

obtém-se distribuições de probabilidade que representam o comportamento das falhas e permitem estimar as ocorrências futuras, seja para um sistema em projeto ou durante o uso.

Essas estimativas de ocorrências futuras são úteis para identificar pontos críticos passíveis de melhoria de projeto (ou reprojeto), definir programas de manutenção ou verificar as probabilidade de eventos deflagradores de situações de perigo.

Se existe probabilidade de ocorrência, então há que avaliar também a consequência que a perda da função do sistema técnico pode proporcionar. É neste contexto que entra o estudo dos riscos, no qual se procede a análise da severidade da ocorrência de uma ou de várias falhas, ou seja, quais as consequências de tais falhas para a organização, o meio ambiente e para as pessoas. Esta atividade é chamada de análise de risco, na qual se desenvolvem cenários de eventos e o estudo das consequências relacionadas à ocorrência de um incidente.

Calil (2009) define risco como a probabilidade "P" de ocorrência de um estado futuro "x", dada a ocorrência de um estado inicial - que pode ser expressa pela probabilidade condicional *P(Estado futuro "x" | Estado inicial)* -, sendo necessário para sua completa caracterização o delineamento dos dois estados, além dos cenários que possibilitem esta transição (que compõem o perfil do risco).

A definição de Kumamoto e Henley (1996) caracteriza o risco a partir de cinco parâmetros: uma probabilidade de um cenário, o resultado de sua ocorrência (consequência), a significância ou utilidade (julgamento de valor), o cenário causal e a população afetada. Dessa forma, o conceito de risco pode ser representado conforme a Equação 1.1.

$$Risco \equiv (L_i, O_i, U_i, CS_i, PO_i) \mid i = 1, ..., n \tag{1.1}$$

sendo:

L = Probabilidade (likelihood)

O = Resultado (outcome)

U = Significância (utility)

CS = Cenário causal (causal scenario)

PO = População afetada pelo resultado (population affected by outcome)

i = Número de cenários possíveis

Os autores afirmam ainda que as pessoas têm uma atitude ambivalente em relação a resultados catastróficos de um incidente, pois uma pequena perturbação distribuída ao longo do tempo é ignorada, enquanto a soma de estímulos ocorridos no mesmo instante e localmente resultam em uma resposta

imediata.

Isso significa que a ocorrência de dez acidentes que resultam em uma morte cada tem menos impacto sobre a reação das pessoas, em comparação com dez mortes ocorridas em um único acidente. Essa atitude é chamada de aversão ao risco e, como resultado, sistemas como usinas nucleares, aeronaves, navios, petroquímica, entre outros são tratados com muito mais rigor para avaliar as consequências de possíveis falhas.

Acidentes industriais, no setor agrícola, hospitalares, veículos automotivos e motocicletas causam dezenas de milhares de mortes ao ano, representando alto risco para a população. Porém menos atenção é dada a esses acidentes devido ao fato que os acidente e as possíveis mortes resultantes ocorrem de forma incremental e dispersa.

Por outro lado, acidentes aéreos em aviões comerciais, apesar de menos frequentes e somar um número muito menor de mortes ao ano em comparação aos envolvendo veículos automotivos e motocicletas, causam grande comoção devido ao número de vítimas resultantes em um única ocorrência.

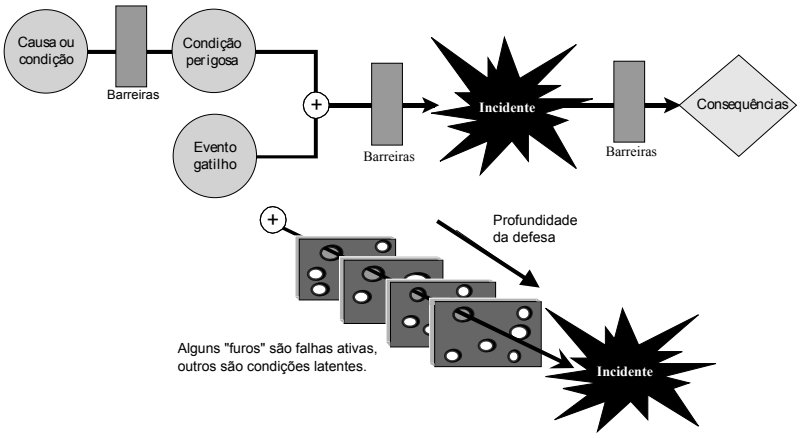
Como resultado dessa atitude ambivalente o esforço em aumentar a confiabilidade e reduzir a exposição ao risco em sistemas como aeronaves e usinas nucleares, por exemplo, é muito maior quando comparados a sistemas mais comum como carros e motos. A confiabilidade pode ser melhorada aumentando a robustez de componentes ou utilizando redundâncias, por exemplo, e o risco por meio da utilização de barreiras para evitar a ocorrência dos eventos deflagradores dos acidentes ou para conter as consequências.

A Figura 1.2 traz a representação do desencadeamento de um incidente e sua trajetória através de barreiras (MOSLEH; DIAS, 2004; MOSLEH et al., 2004). Todo item é portador de uma causa ou uma condição para a falha. Esta causa ou condição é o perigo que está embutido no próprio princípio de solução de um ou mais itens requeridos para uma ou mais funções.

As barreiras são utilizadas para mitigar a causa ou condição em relação ao cenário de incidente, ou seja, conter o perigo, independente da função que irá executar. Conforme pode ser observado na Figura 1.2, quando uma barreira é ultrapassada, há uma condição perigosa que é a primeira configuração de risco. A condição perigosa, se combinada com um evento gatilho, deflagra o cenário de incidente, ou seja, um incidente pode ocorrer. Um incidente pode ser, por exemplo, a perda da função do sistema (neste caso contribui para diminuir a confiabilidade apenas), danos ao meio ambiente, injúrias, mortes etc. e, nestes casos, se a possibilidade existe a análise de risco deve ser deflagrada.

Considerando-se, por exemplo, uma aeronave comercial em voo, em uma situação mais extrema, o incidente pode ser a queda da aeronave. A condição perigosa está no fato de a aeronave estar em voo a uma grande

Figura 1.2 – Modelo de desencadeamento de incidente



Fonte: Adaptado de Mosleh et al. (2004)

distância do solo e o evento gatilho pode ser a perda da função de um subsistema que compromete o voo, como os motores e as superfícies de controles (aileron, flaps, etc.). Por essa razão, em sistemas cuja operação envolve alto risco, é importante estudar de que forma se dá a perda da função do sistema. Variáveis como mostrados na Equação 1.1 podem e, nestes casos, devem ser consideradas.

Como já comentado, as falhas ocultas são caracterizadas por um ou mais eventos que compõem um cenário de falhas, e não são percebidas até que outro evento ocorra, tal como a falha de outro item ou mudanças operacionais do sistema. Entende-se mudança operacional como o ativar e desativar de subsistemas e componentes ao longo da operação.

Estas falhas são significativas nos sistemas técnicos portadores de grande quantidade de energia: geração e transmissão de energia; petroquímico; petróleo; aeronáutico entre outros, uma vez que podem comprometer o tempo de resposta de operadores e mantenedores e resultar em um incidente, com consequência para a integridade do sistema, para o ambiente ou para segurança humana.

O estudo de falhas ocultas na fase de projeto conceitual é motivado pela possibilidade de eliminar as causas dessas falhas ou, pelo menos, mitigar os efeitos no início do processo de projeto, para os casos em que redundâncias são requeridas.

Para tanto, propõe-se desenvolver um método de análise que permita simular a ocorrência de falhas ocultas e obter as probabilidades *a priori* nesta fase do processo de projeto. Tal método considera os vários cenários de ocorrência das falhas ocultas, utilizando-se de técnicas de análise funcional, técnicas de análise de falhas (diagramas causa e efeito, análise dos modos de falha e seus efeitos, análise por árvore de eventos ou análise por árvore de falhas), técnicas de modelagem comportamental do sistema (máquinas de estado finito, redes de Petri, autômatos, etc.) e, por fim a combinação dos modelos obtidos para a simulação de ocorrência dos vários eventos que compõem os cenários de falha, a partir de métodos estocásticos. Realizando simulações de diferentes casos, pretende-se avaliar se o modelo obtido permite comparar a influência dos diferentes princípios de solução definidos no projeto conceitual sobre a probabilidade de falha do sistema de forma mais prática, auxiliando os projetistas na tomada de decisão.

O método foi desenvolvido para ser aplicado na análise de diferentes sistemas, evidenciando as adaptações a serem feitas para ajustar o modelo dadas as características particulares de cada sistema, principalmente quanto à relação entre as falhas e as características de operação do sistema.

1.1 OBJETIVOS

O objetivo geral do trabalho é desenvolver um método que permita identificar falhas ocultas, avaliar a probabilidade de ocorrência e seus impactos sobre a operação de sistemas técnicos, na fase de projeto conceitual. Em síntese, modelar cenários de ocorrência de falhas ocultas para um ciclo de vida do sistema técnico avaliado.

Além do objetivo geral, o trabalho tem os seguintes objetivos específicos:

- Caracterizar falhas ocultas em sistemas técnicos. Tais falhas são caracterizadas a partir de transições de estados dos sistemas técnicos, seja por demandas operacionais ou pela ocorrência de outras falhas (evidentes), principalmente relacionadas a redundâncias.
- Identificar e caracterizar os cenários de ocorrência de falhas ocultas com risco potencial para os sistemas técnicos. Tais cenários são caracterizados por uma sequência de eventos que levam à falha catastrófica do sistema.
- Desenvolver modelo para o auxiliar o diagnóstico da ocorrência de falhas ocultas. A partir de modelos comportamentais dos sistemas e da relação

entre as falhas funcionais de subsistemas e componentes, pretende-se obter um modelo que permita a simulação para que a probabilidade de ocorrência das falhas ocultas possa ser determinada.

- Facilitar a análise da confiabilidade em projetos novos e em uso. A partir de uma taxa de falha desejada ou requerida para os itens pretende-se identificar e quantificar a probabilidade de ocorrência de potenciais falhas ocultas ao longo do ciclo de vida do sistema, visando a identificação de soluções de projeto que levem ao melhor controle sobre sua ocorrência.

- Facilitar a análise das informações para estimar a confiabilidade. Em projetos novos, a quantificação da confiabilidade é difícil pela pouca disponibilidade de informações, portanto pretende-se que o resultado do projeto de tese permita uma melhor avaliação da confiabilidade.

- Contribuir com a metodologia de projeto PRODIP no que se refere aos atributos de confiabilidade e risco. Percebe-se que no projeto de sistemas complexos torna-se necessário desenvolver novas perspectivas de análise dos princípios de solução, principalmente no tocante as inclusões de demandas de risco e confiabilidade. Tanto para desenvolvimento de novos produtos quanto para melhorias nos já existentes

1.2 JUSTIFICATIVA

Entende-se que ao identificar e avaliar a probabilidade de ocorrência de falhas ocultas a partir da fase de projeto conceitual pode-se organizar e avaliar o impacto no produto sobre a segurança e risco. Com isso pode-se também recomendar e instruir os projetistas em relação à aplicação de técnicas e ferramentas a serem utilizadas nas outras fases e etapas do projeto com vistas a garantia dos atributos de confiabilidade e segurança, conforme requerido no planejamento do produto.

No estudo de falhas ocultas é possível perceber que a exposição dos sistemas a cenários de risco pode ser frequente mesmo em situações que o sistema cumpre a missão requerida. É comum a ocorrência de falhas ocultas que não tem o efeito negativo de resultar no acidente apenas porque a operação não demandou a utilização do sistema ou componente falhado. Em sistemas críticos essa exposição não é aceitável.

1.3 MOTIVAÇÃO

A partir do contato com pesquisas dentro do Núcleo de Desenvolvimento Integrado de Produtos/UFSC (NeDIP/UFSC) e de outros grupos de pesquisa, como Laboratório de Sistemas Hidráulicos e Pneumáticos/UFSC (LASHIP/UFSC) e Division of Machine Design/Linköping University percebeu-se a necessidade de investigar mais a temática de confiabilidade e risco e sua correlação com as fases de desenvolvimento de produto.

A percepção que se tem é que estes atributos devem fazer parte do processo do projeto desde as primeiras fases do ciclo de vida do produto, mais especificamente nas fases de projeto informacional e conceitual.

A grande limitação existente para as análises de confiabilidade e risco é a falta de informação disponível, principalmente referente à ocorrência das falhas e obtenção das distribuições de probabilidade. Essa limitação é ainda maior quando se trata da fase de projeto dos sistemas.

De alguma maneira, as pesquisas desenvolvidas pelo grupo de pesquisa do NeDIP já vêm investigando esta temática, principalmente nos trabalho de Alonço (2004), Sakurada (2013), Kagueiama (2012) e Almeida (1999); e com estes trabalhos foi possível perceber que abordar a confiabilidade e segurança na fase de projeto conceitual, e melhorar a análise de falhas ocultas merecem um estudo mais aprofundado.

Desde 2014, motivado por programas de cooperação entre Brasil e Suécia, houve grande interação com grupos de pesquisa diversos com discussões relacionadas a sistemas aeronáuticos.

A participação no *Workshop Design and Product Development for Innovation: Connecting People, Disciplines, and Ideas* na Universidade Federal do ABC em 2015 possibilitou o contato com o professor Johan Ölvander, coordenador da Division of Machine Design/Linköpink University e a elaboração do projeto de pesquisa "Segurança e confiabilidade de sistemas na fase de projeto conceitual", submetido e aprovado na chamada CISB/CNPq.

O projeto possibilitou visitas dos pesquisadores da Suécia ao NeDIP/UFSC e de pesquisadores brasileiros à Linköping University e ao grupo que trabalha em segurança de sistemas dentro da empresa Saab. Duas pesquisas de doutorado, Johansson (2013) e Safavi (2013), chamaram atenção por tratarem diretamente com a otimização de projeto na fase de projeto conceitual.

A primeira trata diretamente sobre segurança de sistemas na fase de projeto conceitual, com a aplicação sobre sistemas aeronáuticos. A segunda, um pouco mais abrangente, trata da otimização multidisciplinar na fase de projeto conceitual. Entretanto foi possível perceber que aspectos relacionados a confiabilidade, segurança e risco não foram incorporados aos modelos desenvolvidos por Safavi (2013).

As visitas a Saab, também indicaram que o modelo de análise que utilizam é baseado na análise por árvore de falhas (FTA - *fault tree analysis*). Ao apresentar o objetivo desta pesquisa e algumas ideias de como cumprir este objetivo, identificou-se que esta abordagem representaria uma inovação na análise de alguns problemas de projeto, contextualizados nos produtos da empresa, neste tema de pesquisa.

Engenheiros da empresa relataram a necessidade de estudar em mais detalhes a ocorrência de falhas ocultas no sistema de combustível do avião Gripen, especificamente no tanque coletor. Este tanque utiliza válvulas redundantes e é comum apresentarem mais válvulas falhadas que o número aceitável definido em projeto.

Além disso, o princípio por trás da definição de falhas ocultas e do método proposto, que relaciona as falhas com as transições operacionais para obter amostras de cenários de risco, tem grande potencial para ser aplicado na análise de diversos sistemas ou problemas de áreas diversas. É possível fazer analogia, por exemplo, a problemas de evacuação de espaços com aglomeração de pessoas, simulando as falhas nas saídas de emergência e a capacidade de respostas das pessoas à situação de perigo.

Assim, a motivação está embasada em ampla literatura e também na perspectiva pessoal de envolver-se com a temática de metodologia de projeto de produto, principalmente tratando sobre os atributos de confiabilidade, segurança e risco.

O interesse por esta área surgiu desde a fase de estudante de graduação pela participação de projetos como MitiSF6 (que resultou na participação no livro "Metodologia para análise de risco: mitigação de perda de SF6 em disjuntores"), o desenvolvimento da pesquisa de mestrado e participação em outros projetos como "Brasil PCH: Diagnóstico sobre procedimentos O&M de pequenas centrais hidrelétricas".

1.4 ESTRUTURA DO TRABALHO

Este trabalho está estruturado em seis capítulos, cujos títulos e respectivos conteúdos são:

- **Capítulo 1 - Introdução**: apresenta os objetivos e algumas definições gerais da pesquisa, contextualizando o trabalho.

- **Capítulo 2 - Sistemas de combustível em aviões**: apresenta conceitos relacionados ao problema de aplicação desta tese, que consiste no tanque coletor de sistemas de combustível de aeronaves de combate cujo

diferencial está na capacidade de realizar voo sob gravidade negativa (invertido).

- **Capítulo 3 - Projeto de sistemas e a análise de risco**: neste capítulo são apresentados conceitos de projeto, visando analisar como a análise de falhas ocultas pode ser desenvolvida no projeto de sistemas.

- **Capítulo 4 - Falhas ocultas e os cenários de risco**: este capítulo apresenta conceitos de confiabilidade e risco, as definições de falhas ocultas, como as falhas ocultas são analisadas e como estas estão relacionadas às análises de confiabilidade, segurança e risco.

- **Capítulo 5 - Proposta para a análise de falhas ocultas**: apresenta a proposta desenvolvida para a análise de falhas ocultas e obtenção dos cenários de risco relacionados a sua ocorrência, a partir do relacionamento entre a ocorrência de falha e as características operacionais do sistema.

- **Capítulo 6 - Aplicação no tanque coletor de avião**: este capítulo apresenta a aplicação do modelo resultante do desenvolvimento da tese e os resultados da análise no tanque coletor de aeronaves de combate.

- **Capítulo 7 - Conclusões**: são apresentadas as conclusões resultantes da pesquisa e algumas considerações sobre possíveis desdobramentos da pesquisa em trabalhos futuros.

2 SISTEMAS DE COMBUSTÍVEL EM AVIÕES

Este capítulo apresenta características do sistema de propulsão de aeronaves, com foco no sistema de combustível, porque este garante a energia necessária para que um avião desenvolva as ações requeridas (decolar, cruzeiro, fazer manobras, aterrizar) dentro de uma missão. A prioridade será dada a aviões utilizados em operações de defesa, por que os sistemas de combustível destes aviões têm características bastante particulares em relação aos aviões comerciais. Há um conjunto de sistemas que devem operar em cada uma das condições de voo e nesta condição é requerida quantidade de combustível que lhe permite voar no tempo de missão recomendada.

A análise de sistemas técnicos sob a perspectiva da engenharia de sistemas permite alcançar um melhor equilíbrio entre os diferentes requisitos estabelecidos para o sistema. Sob essa perspectiva, um sistema é visto como o conjunto de subsistemas, elementos, componentes ou partes, formando um algo complexo e unitário com um propósito específico (HASKINS et al., 2006; SADRAEY, 2012; HIRSHORN et al., 2017). Os conceitos relacionados a engenharia de sistemas serão apresentados em mais detalhe no Capítulo 3.

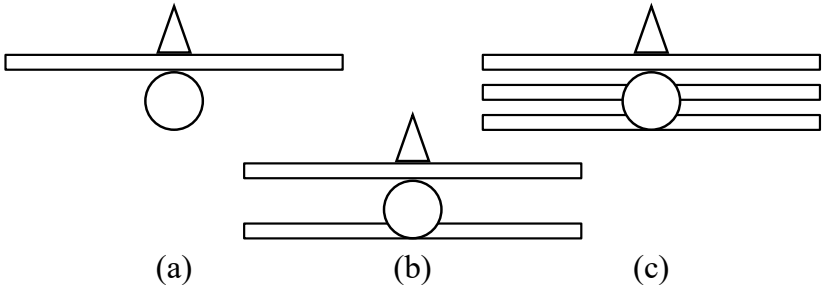
Vale ressaltar que a denominação de sistema e subsistema é relativo, sendo dependente do grau de detalhamento estabelecido para a análise.

Um automóvel, por exemplo, é um sistema complexo composto por uma série de subsistemas tais como: motor, chassi, suspensão, pneus, etc. Cada um desses subsistemas, por sua vez, pode ainda ser desdobrado em mais elementares chegando, por exemplo a partes e componentes. Por outro lado, se o foco da análise for o motor, por exemplo, este pode ser denominado de sistema e seus desdobramentos (pistões, bloco, velas, virabrequim etc) chamados de subsistemas.

Da mesma forma, aviões também podem ser tratados como sistemas complexos compostos por uma série de subsistemas e componentes (SADRAEY, 2012; RAYMER, 2012).

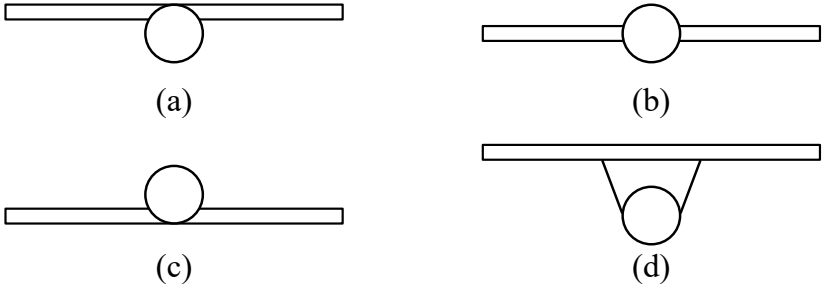
1. **Asa**. A principal função da asa é gerar as forças aerodinâmicas de sustentação para manter a aeronave no ar. Como consequência das asas, surgem dois fenômenos indesejados: momento positivo (*pitching moment*) em relação ao centro de gravidade da aeronave que deve ser compensado; e o arrasto aerodinâmico. As asas são também essenciais para o fornecimento da estabilidade lateral, contribuindo para a segurança de voo. As asas podem variar, por exemplo, quanto ao número (uma, duas ou três, na Figura 2.1) ou quanto a posição vertical (entre as quatros posições distintas da Figura 2.2).

Figura 2.1 – Variação das asas quanto ao número



Fonte: Sadraey (2012)

Figura 2.2 – Variação das asas quanto a posição

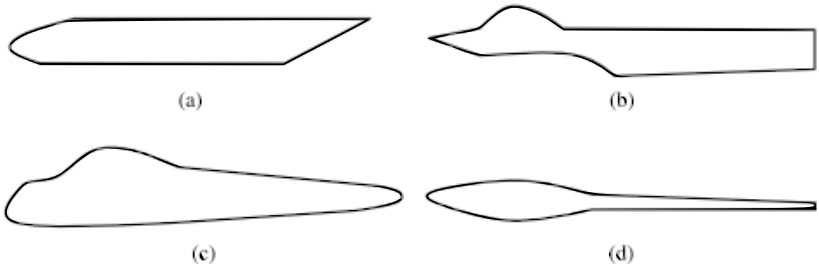


Fonte: Sadraey (2012)

2. **Fuselagem**. A principal função da fuselagem é acomodar a carga útil na aeronave, a qual inclui passageiros, carga, bagagem, armamento (em aeronaves militares), etc. A fuselagem é também onde são acomodados o piloto e demais membros da tripulação; e na maioria das vezes os tanques de combustíveis e motores. Além disso, o momento resultante entre a fuselagem e as caudas horizontal e vertical fazem com que a fuselagem desempenhe um papel importante na estabilidade longitudinal, direcional e no controle da aeronave. A fuselagem é composta por diferentes seções projetadas separadamente de acordo com requisitos relacionados a tripulação, carga útil, subsistemas internos etc, podendo assumir diferentes configurações, como exemplificado na Figura 2.3.

3. **Cauda horizontal**. A cauda horizontal tem a função principal de imprimir a força aerodinâmica para a trimagem longitudinal (ajuste para manter a direção e altitude) da aeronave. É um elemento essencial para assegurar a estabilidade longitudinal da aeronave e a consequente se-

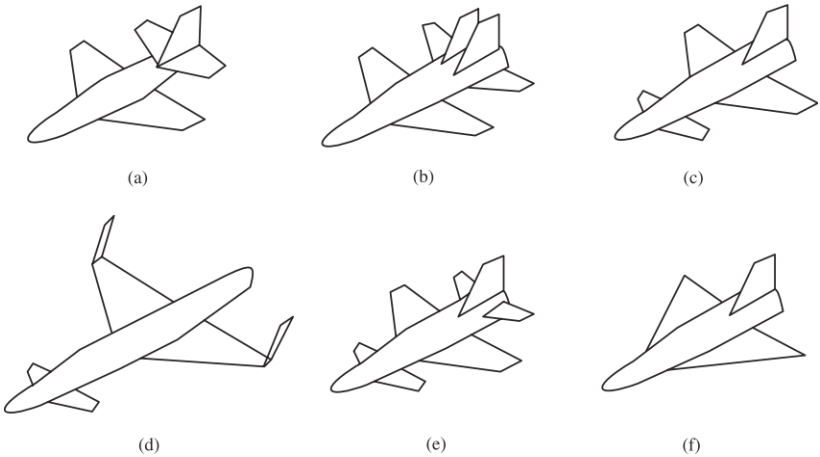
Figura 2.3 – Diferentes configurações de fuselagem



Fonte: Sadraey (2012)

gurança de voo. Alguns exemplos de configuração de cauda horizontal podem ser vistos na Figura 2.4.

Figura 2.4 – Diferentes configurações de cauda horizontal



Fonte: Sadraey (2012)

4. **Cauda vertical**. A principal função da cauda vertical é gerar as forças aerodinâmica para a trimagem direcional da aeronave. De maneira equivalente a cauda horizontal, a vertical é um elemento fundamental para a estabilidade direcional e consequente segurança de voo da aeronave. O controle direcional e a manobrabilidade da aeronave são determinados pela cauda vertical, tendo em vista que na maioria das aeronaves o leme é uma parte móvel da cauda vertical.

5. **Trem de pouso**. O trem de pouso tem a função principal de viabilizar as operações de poucos e decolagens. É o último subsistema a ser projetado, já que aspectos como a distribuição de carga da aeronave (centro de gravidade) devem ser conhecidos para que o subsistema possa ser projetado. As rodas são elementos fundamentais para a aceleração e desaceleração da aeronave de forma segura. O desempenho das rodas influencia, por exemplo, na quantidade de empuxo necessário para vencer o atrito dos pneus com o solo e a decolagem de forma mais eficiente.

6. **Sistema de propulsão**. O elemento principal do sistema de propulsão é o motor, ou motores. Sua função principal é gerar potência e empuxo para mover a aeronave, a partir da queima do combustível. O combustível, por sua vez, é um elemento essencial do sistema de propulsão e representa parte significativa do peso da aeronave. Sem este sistema a aeronave não é capaz de decolar de forma independente, mas ainda é capaz de planar e pousar.

Todos os subsistemas apresentados são fundamentais para o funcionamento da aeronave. No presente trabalho, o foco será dado ao subsistema de propulsão, mais especificamente o subsistema de combustível da aeronave.

2.1 SUBSISTEMA DE COMBUSTÍVEL

Evidentemente, uma aeronave é mais pesada que o ar. Logo, é necessária a aplicação de alguma força para que a aeronave possa sair do solo e adquirir altitude suficiente para ao menos planar.

Uma asa delta precisa ser lançada do alto de uma montanha para que possa utilizar correntes ascendentes de ar para planar. Um planador precisa ser rebocado por outra aeronave para que possa atingir determinadas altitudes e utilizar as mesmas correntes ascendentes de ar para planar, graças às suas características aerodinâmicas.

Da mesma forma, um avião é capaz de planar com certas limitações, mas para decolar e atingir grandes altitudes é necessário um sistema de propulsão para gerar empuxo suficiente para que possa levantar voo.

O princípio do sistema de propulsão de aeronaves segue a terceira lei de Newton (SADRAEY, 2012). A queima de combustível gera uma força contrária que desloca o ar para trás (ação) e como consequência a aeronave se move para a frente (reação).

O Quadro 2.1 apresenta um resumo das funções do sistema de propulsão, segundo Sadraey (2012).

Quadro 2.1 Funções do subsistema de propulsão

Categoria da função	Função
Função primária	Gerar força de propulsão
Função secundária	Gerar potência/energia para os demais subsistemas da aeronave, como o hidráulico e elétrico.
Função contribuinte (consequência da existência do sistema)	Estabilização e desestabilização. Reduz o conforto para tripulantes e passageiros devido ao ruído. Reduz o conforto para tripulantes e passageiros devido a transferência de calor para a cabine. Contribuição para a segurança no caso de um motor inoperante. Custo operacional pelo consumo de combustível. Impacto estrutural pela vibração do motor.

Fonte: Sadraey (2012)

Para sustentar o voo e assegurar a execução de manobras, é essencial o bom funcionamento do motor. Por se tratar de um elemento fundamental da aeronave, é comum a utilização de mais de um motor, principalmente em aeronaves maiores cuja capacidade de planar é limitada.

Sadraey (2012) salienta que apesar de os motores modernos terem confiabilidade elevada, a possibilidade da ocorrência de falhas jamais deve ser ignorada. Estatísticas demonstram que sempre ocorrem situações pouco favoráveis com potencial de levar a falha de motores e que essas situações vão continuar existindo.

Um exemplo recente é o acidente envolvendo o voo US Airways 1549, em que o piloto foi obrigado a pousar um Airbus A320 no rio Hudson, em Nova York. A causa do acidente foi a perda dos dois motores da aeronave devido à colisão com pássaros (HERSMAN et al., 2010). Este tipo de incidente é relativamente comum, porém a perda total dos dois motores foi algo que trouxe surpresa durante a investigação do acidente.

Por essa razão, existem normas bem definidas quanto ao número de motores a ser utilizado no projeto, dependendo do tipo de aeronave e tipo de missão requerida. É evidente que para motores iguais, a probabilidade de falha de dois em três ou três em quatro é extremamente mais baixa. Como o número de motores tem forte influência sobre custo e peso das aeronaves fez-se grande investimento na confiabilidade dos mesmos. Apesar disso, sempre é recomendado que seja empregado ao menos dois motores em aeronaves de grande porte, seja para transporte de carga ou de passageiros.

Para aeronaves militares de combate é possível encontrar projetos com um motor ou com dois motores. Nessas aeronaves, outros fatores além da segurança do piloto exercem grande influência nas decisões de projeto, tal

como a redução do peso, aumento da manobrabilidade e superioridade em combate da aeronave. Aviões como o *Boeing F/A-18E/F Super Hornet* e o *Lockheed Martin F-22 Raptor* possuem dois motores, enquanto o *Lockheed Martin F-35 Lightning II* e o *Saab JAS 39 Gripen* possuem um motor.

Apesar do número de motores assegurar maior confiabilidade para os aviões, essas medidas de nada valem se ocorrer falha no subsistema que alimenta o combustível dos motores.

2.1.1 Características gerais do subsistema de combustível

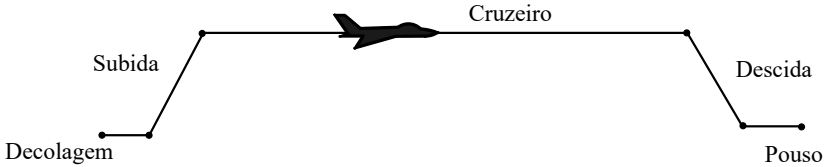
Grandes volumes de combustível devem ser armazenados, para que as aeronaves possam cumprir seus requisitos operacionais de voo (LANGTON et al., 2009). A quantidade total de combustível necessária para a aeronave completar uma missão depende das características do voo pretendido, das suas características aerodinâmicas (vento contrário aumenta o consumo, por exemplo) e do seu consumo específico. É comum, por exemplo, quando voamos em aeronaves comerciais vivenciar casos em que o piloto informa a chegada antecipada, ou casos em que há atraso devido as condições de vento encontradas ao longo voo.

Analogamente a um carro, o consumo de combustível depende das características de condução do motorista e das exigências do tráfego na pista. Acelerar demais em condições de tráfego intenso, em que é necessário frear frequentemente, significa desperdiçar a energia gerada pelo motor ao frear, sobrecarregando os freios e desperdiçando combustível. Por outro lado, ao viajar em estradas em boas condições com pouca necessidade de troca de marchas, diminui o consumo. Logo, a quantidade de combustível necessária está diretamente relacionada às condições de operação.

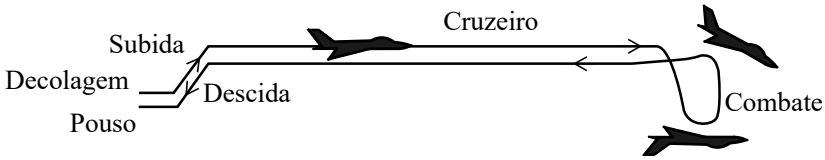
A Figura 2.5 apresenta alguns exemplos típicos de missões para três aeronaves. O exemplo (a) consiste em uma aeronave de carga ou passageiros que transporta algo de um lugar a outro. Neste caso, a operação consiste apenas na decolagem, no voo em velocidade de cruzeiro e no pouso. Já o exemplo (b) mostra a operação de uma aeronave de combate, que em algum momento ao longo do voo entra em combate (executando manobras severas que exigem um consumo maior de combustível) e depois retorna para o ponto de origem ou pousa em um segundo local. Por fim, o exemplo (c) trata de uma aeronave de reconhecimento que, ao atingir o ponto de interesse, apenas circula sem aumento significativo no consumo *loiter* e depois retorna ao ponto de origem.

Segundo Gavel (2007) a complexidade de sistemas de combustível varia desde sistemas pequenos, em aeronaves caseiras cujos sistemas são simples,

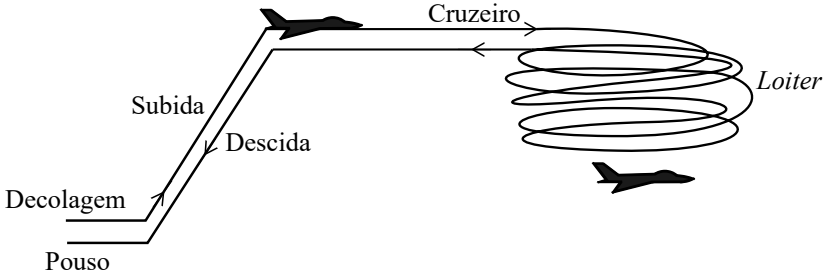
Figura 2.5 – Perfis de voo de diferentes tipos de missão de aeronaves



(a) Aeronave de carga ou passageiro



(b) Aeronave de combate



(c) Aeronave de reconhecimento

Fonte: Sadraey (2012)

até sistemas altamente complexos de aviões de caça modernos, os quais são críticos por afetarem o centro de gravidade, são muito caros e repletos de redundâncias.

Um sistema de combustível é composto pelos seguintes subsistemas principais:

- Subsistema de alimentação do motor.
- Subsistema de transferência de combustível.
- Subsistema de pressurização e ventilação.
- Subsistema de reabastecimento em terra e no ar.

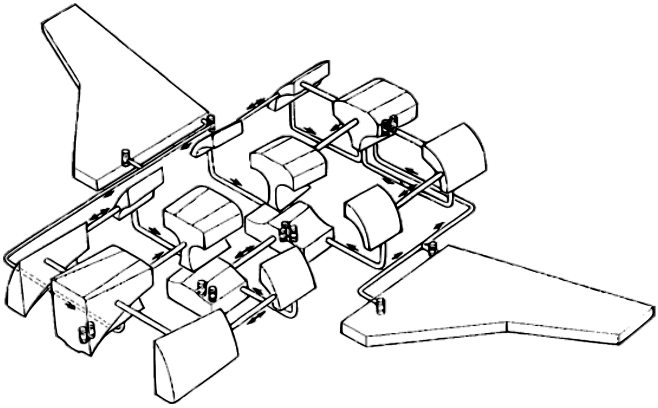
O aumento da complexidade traz desafios. Pela quantidade de combustível armazenado na aeronave, por exemplo, há a necessidade de que ao

abastecimento ocorra rapidamente. Com isso, houve o desenvolvimento de tanques de combustível pressurizados (LANGTON et al., 2009). A complexidade aumenta ainda mais quando se trata de aeronaves militares, pela limitação de espaço, exposição a disparos de armamentos e pela complexidade das manobras executadas

2.1.2 Subsistema de combustível em aeronaves militares

Assim como em aviões comerciais, nos militares o combustível é armazenado nas asas. Porém esses aviões possuem asas pequenas e finas. Dessa forma, os sistemas de combustível da maioria das aeronaves de combate consistem de diversos tanques espalhados nas asas e na fuselagem, como exemplificado na Figura 2.6. Além das limitações de espaço, essa característica visa solucionar problemas de agitação do combustível, centro de gravidade, ou segurança. O sistema pode ser pressurizado para evitar a cavitação das bombas, ebulição espontânea do combustível em grandes altitudes, ou para auxiliar na transferência de combustível (GAVEL, 2007)

Figura 2.6 – Arranjo de tanques de combustível em aeronaves militares



Fonte: Langton et al. (2009)

A função essencial do sistema de combustível é assegurar o fornecimento de combustível, sob quaisquer condições de altitude, velocidade, força da gravidade, ou outras variáveis que afetam a aeronave (MIHALYI, 2007). Por essa razão a pressurização do sistema é importante, e a forma mais comum de garantir essa pressurização é utilizando um tanque coletor. O tanque coletor, detalhado a seguir e representado na Figura 2.7, recebe o combustível do

sistema de tanques distribuído na aeronave e é constituído de bombas que fazem a alimentação da turbina, em cada uma das condições de voo exigida da aeronave, para a missão considerada.

Em geral, motores e sistemas de energia auxiliar de aeronaves militares são semelhantes aos de aeronaves comerciais (LANGTON et al., 2009). As principais diferenças são:

- Aeronaves de combates de alto desempenhos e aeronaves de ataque de longo alcance tipicamente requerem grandes vazões de alimentação de combustível para os motores, para que seja possível executar voos supersônicos e manobras severas em alta velocidade.

- Pela quantidade de equipamentos de aviônica e eletrônicos a bordo, normalmente o combustível é utilizado no resfriamento de tais equipamentos. Consequentemente, os tanques de combustível de aeronaves de combate apresentam temperaturas mais elevadas que os comerciais. As bombas devem ser capazes de operar sob condições de temperatura elevada.

- As condições operacionais de combate requerem que a alimentação de combustível dos motores seja mantida mesmo sob condições extremas de gravidade negativa.

A alimentação deve ser feita na condição normal de voo, na condição invertida de voo (gravidade negativa) e nas transições entre estas. Existem várias formas para garantir a alimentação de combustível sob essas condições de voo (normal, invertido e transições), que serão tratadas em mais detalhes ao longo do capítulo:

- Utilizar bombas com duas entradas de combustível (acima e abaixo) no tanque de armazenamento.

- Utilizar válvulas com peso na entrada das bombas.

- Utilizar uma mangueira com pesos, funcionando como uma espécie de pêndulo que muda a direção da entrada de acordo com a direção da gravidade e forças de aceleração.

- Utilizar um reservatório onde se encontram as bombas, que aprisiona combustível suficiente para a execução de manobras sob gravidade negativa.

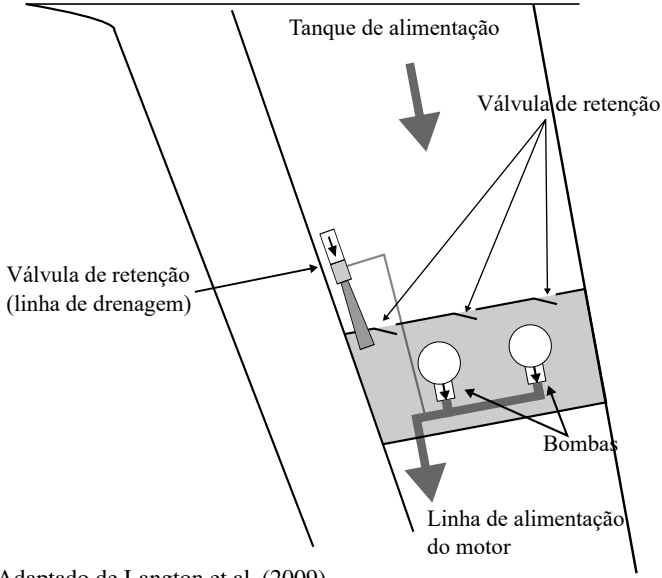
Este último princípio de solução consiste de um tanque coletor, que contém um conjunto de válvulas de retenção que permitem a entrada de

combustível quando em condições de gravidade normal, mas que não permitem a vazão de combustível sob gravidade negativa (voando invertido). O tanque coletor é uma solução normalmente utilizada nas aeronaves de defesa. Em face disso será dedicado uma atenção especial ao mesmo porque este modelo será utilizado para as análises a serem desenvolvidas no contexto desta tese.

2.2 TANQUE COLETOR

O arranjo geral de um sistema de combustível, além dos tanques de armazenamento, é composto por uma ou mais bombas de alimentação do(s) motor(es) e de um tanque coletor. Este tanque coletor é alimentado pelos tanques de armazenamento existentes nas asas e fuselagem por gravidade, que por sua vez, alimentam os motores por meio de bombas de combustível. A Figura 2.7 traz uma representação esquemática do tanque coletor.

Figura 2.7 – Representação do tanque coletor



Fonte: Adaptado de Langton et al. (2009)

O combustível armazenado na aeronave alimenta o tanque coletor por gravidade, na condição normal de voo. As válvulas de retenção tem a função de reter combustível na câmara onde se encontra a bomba, impedindo o retorno por gravidade em caso de voo invertido. A linha de drenagem atua para sugar o combustível retido em cantos remotos do tanque. Do tanque coletor, o

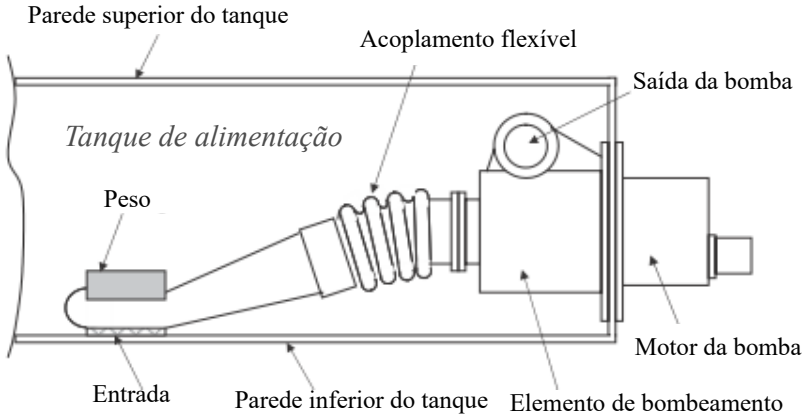
combustível é bombeado para o motor, em qualquer que seja a condição de voo. Logo, exige condições de projeto com especificidades para cada tipo de aeronave, levando em consideração as missões em que são empregadas.

Uma característica importante dos tanques coletores é que estes também contribuem para que a aeronave possa voar sob condições de gravidade negativa (de cabeça para baixo). Essa característica é essencial para aviões de combate tendo em vista as manobras que são exigidas deste tipo de aeronave.

Durante uma operação normal, uma aeronave comercial fica a maior parte do tempo sob condições de gravidade normal. Como diferentes situações podem ocorrer durante voo, existem recomendações de normas que demandam que as aeronaves sejam capazes de manter um voo seguro sob condições de gravidade negativa por até oito segundos (LANGTON et al., 2009).

No caso de aviões de acrobacia, a solução encontrada é a utilização de uma mangueira na entrada da bomba (Figura 2.8), capaz de se mover para cima e para baixo, de forma que sempre esteja com a ponta submersa em combustível, independente se durante um voo normal ou invertido. Essa solução funciona para este tipo de aeronave porque há apenas um tanque de alimentação que é onde se encontra a bomba de combustível.

Figura 2.8 – Solução para voo invertido em aviões de acrobacia



Fonte: Langton et al. (2009)

No caso dos aviões militares este princípio de solução não funciona, devido ao fato que os tanques de armazenamento estão espalhados nas asas e fuselagem, separados das bombas de alimentação dos motores.

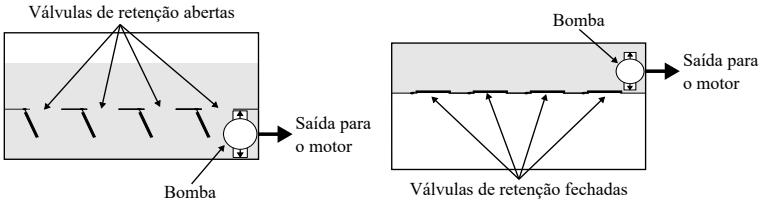
Durante o voo sob gravidade negativa, o combustível que desceu até o tanque coletor por gravidade tende a retornar aos tanques onde estava armazenado, presentes nas asas e fuselagem. Com isso as bombas podem ficar sem

combustível para bombear, o que neste caso poderia apagar o(s) motor(es).

A questão que surge nesse caso é: como fazer para manter combustível sendo bombeado para o(s) motor(es). Assim, uma das funções do tanque coletor é manter uma quantidade de combustível aprisionado em um lugar de tal forma que as bombas de combustível sejam supridas e possam manter a alimentação dos motores, mesmo na condição de voo invertido. No caso de aviões de combate de médio porte, a norma para a capacidade de manter o voo invertido é de dez segundos. Após esse período o tanque coletor deve encher novamente.

Os tanques coletores possuem duas sessões conectadas por válvulas de retenção. A Figura 2.9 traz uma representação esquemática do funcionamento dos tanques coletores, referentes a situações de gravidade negativa. Em condições normais de voo (Figura 2.9a), o combustível dos tanques de armazenamento desce por gravidade até o tanque coletor, completando o nível e alimentando a bomba de combustível.

Figura 2.9 – Representação esquemática do funcionamento dos tanques coletores



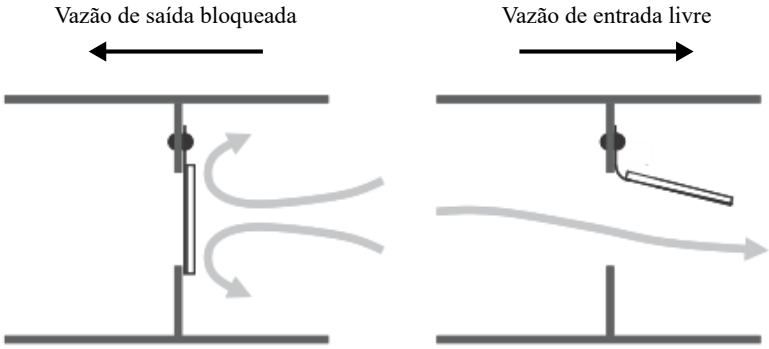
(a) Voo normal (b) Voo invertido

Quando a aeronave voa invertida, a gravidade negativa força o retorno do combustível para os tanques de armazenamento (Figura 2.9b). Porém as válvulas de retenção (Figura 2.10) fecham a passagem no sentido de retorno do combustível, mantendo o combustível presente na região da bomba, na porção inferior do tanque, mantendo a alimentação das bombas.

As bombas de combustível, por sua vez, tem duas entradas de combustível tanto por baixo quanto por cima, adaptando-se para os casos de voo normal e invertido. A Figura 2.11 traz dois exemplos de solução para as bombas. No primeiro exemplo (a), o assento da bomba possui um peso, que ajusta a posição da entrada da bomba de acordo com a orientação da aeronave. O segundo exemplo, conta com entrada tanto na parte superior quanto na parte inferior da bomba.

Os tanques coletores dos aviões de caça *Saab JAS 39 Gripen* utilizam o princípio da utilização de válvulas de retenção e bombas de combustível com duas entradas (Figura 2.11b). Tendo em vista a confidencialidade envolvida

Figura 2.10 – Funcionamento da retenção das válvulas



Fonte: Langton et al. (2009)

com este tipo de sistema, serão utilizados alguns dados aproximados para o estudo da ocorrência de falhas nestes tanques. O princípio de funcionamento do tanque é real, assim como o número de válvulas utilizadas. Entretanto, as taxas de falha das válvulas, os consumos de combustível, e as vazões são informações restritas, tratando-se de aproximações baseadas em dados reais.

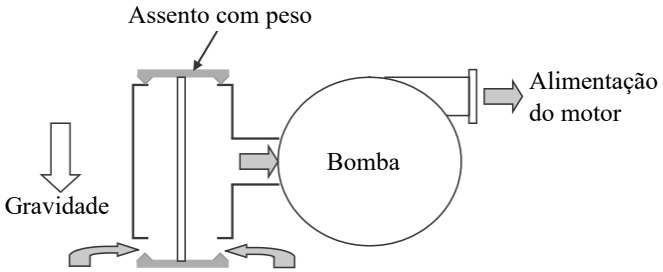
A análise dos cenários envolvendo a ocorrência de falhas ocultas em tanques coletores é o problema a ser estudado nesta tese. As características construtivas e de operação do sistema tornam este problema bastante aderente aos objetivos desta tese.

A conexão entre as duas sessões do tanque coletor é, normalmente, feita por um conjunto de válvulas que atuam de forma redundante no desempenho das respectivas funções. Com isso, assegura-se vazão suficiente para dentro do tanque coletor durante os voos em condição normal, além de contribuir para aumentar a confiabilidade do sistema.

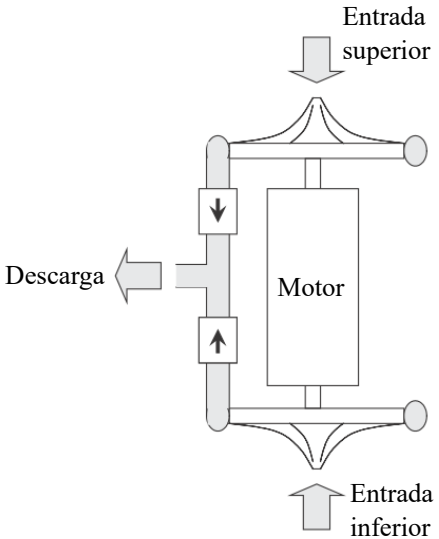
Todas as válvulas de um conjunto utilizado tem o mesmo diâmetro e vazão, sendo que as opções de diâmetro e vazão são variadas, dependendo de decisões de projeto. Em conjunto devem garantir a vazão necessária para que o suprimento de combustível dos motores seja assegurado.

A utilização de múltiplas válvulas visa aumentar a confiabilidade do tanque, na perspectiva de garantir a segurança de voo. Em outras palavras, para a falha do sistema de combustível, em torno das válvulas de retenção, seria necessário a ocorrência de falhas em diversas válvulas simultaneamente, até que a condição de suprimento de combustível ficasse comprometida. Nas condições normais de voo, além da saída de combustível pelo bombeamento para os motores, há a entrada de combustível por gravidade, desde que alguma válvula esteja funcionando corretamente e na condição aberta. Dependendo

Figura 2.11 – Tipo de solução de bombas de combustível para voos invertidos



(a) Voo normal



(b) Voo invertido

Fonte: Adaptado de Langton et al. (2009)

das vazões das válvulas, garante-se que a entrada de combustível no tanque coletor seja maior que a saída para os motores, mantendo um certo volume de combustível no mesmo.

Porém, no caso de voo invertido, não há combustível entrando no tanque coletor, apenas a saída do combustível que está sendo consumido pelos motores. Nesta condição, as válvulas de retenção desempenham a função de reter, e não permitir o retorno do combustível para os tanques da aeronave. Assim, fica contido no tanque coletor a quantidade dimensionada para a

execução das manobras invertidas.

As válvulas podem falhar abertas ou fechadas. Na ocorrência de falha aberta nas válvulas de retenção faz com que haja a perda de combustível não só para os motores, mas também para os tanques de armazenamento, que retorna devido à gravidade. Na ocorrência de falha fechada, diminui a entrada de combustível para o tanque coletor. Nesta condição, dependendo do ciclo de missão invertida, poderá não dar tempo de realimentar toda quantidade de combustível requerida para a missão subsequente de voo invertido.

Os tanques coletores são sistemas fechados, projetados para serem não manuteníveis. Ou seja, não passam por manutenção para a substituição preventiva das válvulas de retenção ao longo do ciclo de vida, que é em torno de duas mil horas de voo. Com isso, evita-se problemas como a contaminação do combustível e a inserção de falhas durantes a execução de procedimentos de manutenção. Além disso, não dispõem de sistemas de predição de falhas, como sensores. Dessa forma, o princípio de funcionamento e operação dos tanques coletores não permite a detecção da ocorrência de falhas nas válvulas até que o tanque seja aberto ao atingir o fim do ciclo de vida.

Nesses casos, as falhas ocorridas nas válvulas de retenção são chamadas de falhas ocultas, pois não são percebidas imediatamente após sua ocorrência, já que não há sistemas de predição de falhas e por não afetar diretamente o comportamento do sistema (KAGUEIAMA et al., 2016a). Este tipo de falha será descrito em detalhe no Capítulo 4.

O critério de falha dos tanques é, ao final ciclo de vida, que n válvulas estejam boas entre as N válvulas instaladas. Ou seja, que a quantidade de válvulas estabelecidas para a redundância do sistema seja satisfeita.

O problema de análise surgiu ao verificar-se que é comum encontrar um número maior de válvulas falhadas que a quantidade estabelecida no projeto ao abrir os tanques. Nesses casos, é possível inferir que não ocorreu a quedas das aeronaves pela combinação favorável entre as ocorrências das falhas das válvulas e os tipos de voo executados durante as missões. Ou seja, embora houvessem falhas ocultas, a combinação das operações de voo não levaram a falha por falta de combustível. Contudo, é possível simular as condições de operação e verificar se pode ocorrer combinações que levem a falha da aeronave, e por conseguinte, o incidente.

Esta análise inicial permitiu perceber que em muitos casos as aeronaves operam com grande exposição ao risco, pois a combinação de falhas com perfis de missão mais severas podem levar a acidentes. Por essa razão, nos capítulos seguintes serão apresentados conceitos sobre projeto, falhas ocultas, confiabilidade e os cenários de risco (KAGUEIAMA et al., 2016a, 2016b).

2.3 CONSIDERAÇÕES FINAIS

Neste capítulo foram apresentados alguns conceitos sobre o problema de aplicação da tese. A análise de confiabilidade dos tanques coletores é feito pela abordagem tradicional, que considera a combinação das válvulas de retenção como componentes redundantes, sem que a ordem de ocorrência das falhas seja significativa.

Como especificação de projeto foi definido que um número mínimos de válvulas esteja funcionando normalmente ao final do ciclo de vida do tanque, quando este é desmontado e avaliado.

Sob o atributo da mantenabilidade (definido no projeto) caracteriza-se o tanque como um item não manutenível. No caso desta aplicação, a troca dos componentes (válvulas) ocorre após um determinado número de voos, quando o tanque atinge o fim do ciclo de vida. Somente após a troca é que se avalia as condições do tanque e se tem a percepção do estado das válvulas (se ainda cumprem suas funções ou não).

Avaliar estes cenários de falhas para diferentes condições operacionais, ou mesmo para a extensão de vida do tanque é uma possibilidade que interessa tanto do ponto de vista econômico, quanto de segurança. Para tanto há que se definir um modelo que possibilite a combinação entre falhas e condições operacionais, por meio de simulações computacionais a partir das informações de estados funcionais.

Em nível do ciclo de vida do produto, assume-se desenvolver uma solução que possibilite simular os cenários de falhas ainda no nível do projeto conceitual, a partir dos requisitos de projeto: tipo de missão, manobras operacionais, tempo de cada manobra, quantidade de combustível no tanque, etc.

A solução proposta nesta tese oferece recursos para testar diferentes configurações de válvulas nos tanques coletores (alterando-se as vazões e número de válvulas) a partir do projeto conceitual e identificar cenários de risco para as aeronaves, combinando falhas e perfis de missão.

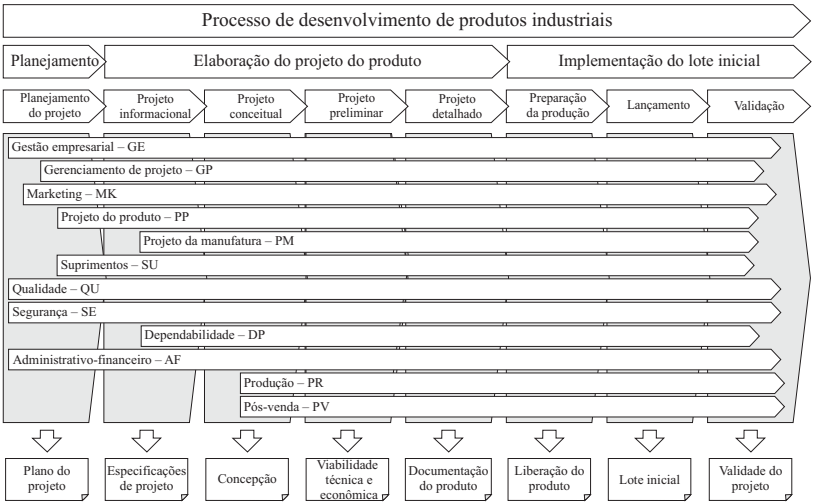
No próximo capítulo apresenta-se uma breve revisão de metodologia de projeto e análise de risco, para compreender por que optou-se por tratar esta análise dentro da fase do ciclo de vida do projeto conceitual.

3 PROJETO DE SISTEMAS E A ANÁLISE DE RISCO

O uso de metodologias de projeto é importante para assegurar a integração dos atributos do produto definidos pelos usuários, com o objetivo de obter produtos robustos, com menor probabilidade de falha, funcionalidade adequada, custo compatível, ergonomia, segurança, entre outros. Uma série de metodologias podem ser encontradas na literatura, desenvolvidas dentro de empresas e no meio acadêmico, como as encontradas nos trabalho de Asimov (1962), Pahl e Beitz (1977), Blanchard e Fabrycky (1981), Back (1983), Ullman (1992), Back et al. (2008).

A metodologia utilizada como referência, chamada PRODIP, foi desenvolvida com base nas pesquisas do Núcleo de Desenvolvimento Integrado de Produtos (NeDIP) da Universidade Federal de Santa Catarina (BACK et al., 2008), e é composta por três macro-fases (Figura 3.1): planejamento, elaboração do projeto do produto e implementação do lote inicial. A elaboração do projeto do produto é constituída por quatro fases de projeto: informacional, conceitual, preliminar e detalhado.

Figura 3.1 – Metodologia de referência PRODIP



Fonte: Back et al. (2008)

Em cada uma das fases tem-se saídas que servem de referência para tomadas de decisão, a partir de uma avaliação da equipe de projeto. Dependendo da importância, estas decisões são tomadas por grupos específicos que

estudam os atributos que são prioritários para o produto em desenvolvimento.

A metodologia, na sua forma integral, contempla muitos atributos que devem ser considerados ao longo do processo de projeto. Normalmente, os referenciais de confiabilidade e segurança são definidos na macrofase de planejamento de projeto, para cumprir requisitos de normas, leis, especificações próprias dos produtos, principalmente quando incorporam grande quantidade de energia.

A macrofase de elaboração do projeto do produto (Figura 3.1) adiciona mais valor ao produto e, como a confiabilidade e segurança (em muitos casos determinações legais) são características inerentes às soluções de projeto definidas durante esta fase do ciclo de vida, tais atributos devem ser considerados desde as etapas iniciais de projeto.

3.1 CONFIABILIDADE, SEGURANÇA E RISCO NO PROJETO

É possível classificar os projetos em quatro tipos (BACK et al., 2008):

- Projeto de inovação, que consiste em um produto com alto grau de originalidade, que satisfaz necessidades não atendidas por produtos existentes e que por essa razão, não dispõe de muitas fontes de informação para o levantamento das especificações;

- projeto de evolução, por sua vez, pode contar com a experiência acumulada na organização, pois trata-se de um reprojeto de um produto existente;

- projeto de variação consiste em introduzir algumas mudanças em um produto existente e, assim como o caso anterior, conta com a experiência acumulada;

- projeto reverso, por fim, consiste em utilizar a engenharia reversa para produzir um produto de outro fabricante já existente no mercado, contando com as características deste para levantar as especificações.

Independente do tipo de projeto, considerar os atributos de confiabilidade, segurança e risco na fase do projeto conceitual é sempre muito importante. Como já visto na Figura 1.1, na fase conceitual impacta-se em até 70% o custo do produto, e estes atributos normalmente são insignificativos para os custos de projeto.

De um lado, o projeto conceitual tem grande impacto sobre o cumprimento dos requisitos de projeto, mas por outro, a seleção, comparação e

otimização dos princípios de solução é muito complexa devido a indisponibilidade de informações (SAFAVI et al., 2012; SAFAVI, 2013).

Porém, como até a fase de projeto conceitual os custos envolvidos no projeto são consideravelmente baixos quando comparados com os custos das fases preliminar e detalhada, é bastante sensato tentar exaurir todos os conceitos relacionados com as funções do produto durante esta fase. Considerando-se os quatro tipos de projeto, a disponibilidade de informações que permitem a otimização pode variar. Em sua pesquisa, Safavi (2013) busca desenvolver a Otimização Multidisciplinar de Projeto (MDO - *multidisciplinary design optimization*), que consiste na utilização de diferentes modelos de otimização de diversas áreas de conhecimento aplicadas ainda na fase de projeto conceitual de sistemas, os quais são integrados utilizando meta modelos.

Tradicionalmente, a previsão da confiabilidade é mais viável na fase de projeto detalhado, utilizando dados de testes em protótipos e dados de campo para estimar a confiabilidade (ORMON et al., 2001). Entretanto, os autores chamam atenção que cerca de 66% dos custos do ciclo de vida de um produto são determinados ao fim do projeto conceitual. Como a confiabilidade é um fator de grande impacto sobre o custo, há grandes vantagens em se melhorar a confiabilidade no projeto conceitual.

A dificuldade em abordar a confiabilidade no projeto conceitual está na limitação das informações disponíveis. Taxas de falha, por exemplo, normalmente são desconhecidas para componentes recém desenvolvidos. Johansson (2013) chamou atenção para esses desafios envolvidos na análise de confiabilidade nas etapas iniciais de projeto. Segundo a autora, os dados estatísticos normalmente disponíveis são de sistemas já existentes, e não do sistema que está sendo projetado. Além disso, os dados podem ser comprometidos, pois os sistemas existentes podem ter passado por mudanças de projeto ao longo do ciclo de vida. Tal problema se torna ainda maior quando se trata de sistemas complexos fabricados em pequena escala (como ônibus espacial, usinas nucleares, protótipos de aeronaves não tripuladas, etc). Johansson (2013) buscou avaliar a utilização de técnicas clássicas de análise de falha como FTA (*fault tree analysis*), FMEA (*failure modes and effects analysis*), RBD (*reliability block diagram*) entre outras nas fases iniciais de projeto.

No projeto conceitual, diferentes princípios de solução são combinados para cumprir as subfunções do sistema técnico e, consequentemente, a função global. A avaliação da confiabilidade, segurança e risco de um sistema técnico pode ser iniciada por métodos teóricos e estatísticos, primeiramente pela determinação da confiabilidade de cada componente e então de forma mais ampla pela determinação da confiabilidade de cada subsistema, até que a confiabilidade de todo o sistema seja estabelecida (KUMAMOTO; HENLEY, 1996). Porém, este tipo de avaliação da confiabilidade não leva em consideração os

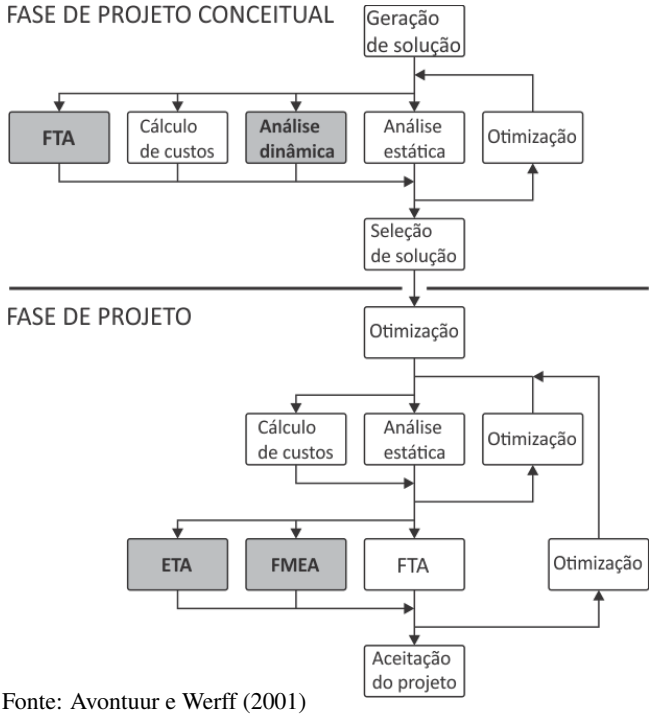
efeitos reais da interação entre o sistema, o ambiente e pessoas. Para tanto, os sistemas devem ser testados simulando-se as condições de uso.

Avontuur e Werff (2001) apresentam um método automatizado para a análise de confiabilidade aplicado a um trem de acionamento utilizado em sistemas maiores como pontes móveis e barreiras de contenção de rios. O método permite introduzir a análise de confiabilidade como um instrumento para projetistas durante o projeto conceitual, mas para isso os autores propuseram algumas alterações tanto no processo de projeto quanto na fase de projeto conceitual, conforme a Figura 3.2. As caixas claras representam o processo tradicional e as caixas destacadas representam etapas adicionadas visando a análise e otimização da confiabilidade. O método de análise da confiabilidade tem como base equações para análise por elementos finitos, cujo uso tradicionalmente se dá na análise de confiabilidade estrutural, porém nesta aplicação as equações são utilizadas para descrever as funções do trem de acionamento (conduzir carga e executar movimento) e para encontrar os mínimos *cut sets* em árvores de falha (FT - *fault trees*).

Segundo Limbourg e Kochs (2008), durante o projeto, a avaliação da probabilística da confiabilidade não é o único objetivo final, sendo necessário a obtenção de valores que possam ser comparados e que permitam encontrar uma solução de projeto otimizada. No modelo de otimização da confiabilidade nas fases iniciais de projeto proposto pelos autores, um aspecto importante é a definição de um espaço de projeto, que permite estabelecer um conjunto promissor de alternativas de projeto que merecem ser avaliadas em detalhe. Porém o grande problema é a definição de um espaço de projeto factível e adequado às necessidades de quem toma as decisões de projeto (método de otimização). No trabalho, os autores propõem a abordagem pelo problema de alocação de redundâncias (RPA - *redundancy allocation problem*) para a definição do espaço de projeto e a utilização da modelagem de atributos, muito utilizada na engenharia de software para a avaliação das concepções de projeto visando identificar a concepção otimizada.

Porciúncula (2009) desenvolveu uma metodologia que resulta na geração dos modelos de confiabilidade e o cálculo da estimativa de confiabilidade de sistemas automáticos durante o processo de projeto, com o intuito de incorporar a estes sistemas maior competitividade em mercados que requerem precisão na atuação de dispositivos, garantia de funcionamento e facilidade de manutenção. A metodologia proposta permite capturar informações dos modelos estruturais, funcionais e comportamentais, ainda nas fases iniciais do processo de projeto de sistemas automáticos. Além disso, considera a interação das diferentes áreas tecnológicas dos sistemas automáticos assim como as diferentes configurações operacionais definidas no sistema durante sua vida útil.

Figura 3.2 – Proposta de processo de projeto e projeto conceitual ideais segundo Avontuur e van der Werff



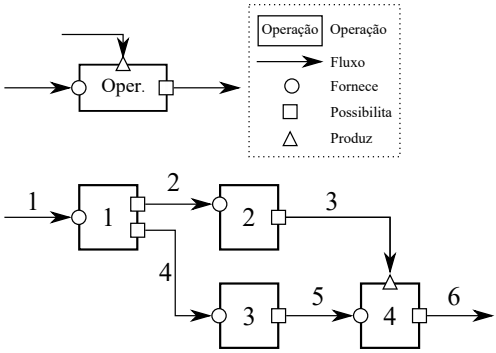
Fonte: Avontuur e Werff (2001)

Ormon et al. (2001), por sua vez, propuseram um modelo de predição da confiabilidade baseado em simulação no projeto conceitual. Como normalmente modelos de simulação para avaliação da confiabilidade aplicados nessa fase de projeto são específicos para determinados sistemas, os autores desenvolveram um modelo genérico que pode ser utilizado sem o conhecimento exato das taxas de falhas dos componentes do sistema. O modelo proposto estima a confiabilidade da missão do sistema, o tempo médio até a falha e o custo médio da missão. As estimativas são baseadas no número de subsistemas em série e nos componentes ativos ou em *stand by* de cada subsistema; nas taxas de falha conhecidas; distribuição triangular para parâmetros de componentes com taxas de falha desconhecidas; tempo de missão; e custos de componentes e missão.

Segundo Bai et al. (2008), técnicas de análise de falhas clássicas como FMEA (*failure mode and effects analysis*), AFD (*anticipatory failure determination*) e FTA (*fault tree analysis*) são utilizados na indústria para determinar

falhas potenciais na fase de projeto conceitual. Porém os autores afirmam que apesar do grande valor demonstrado ao longo dos anos, tais técnicas não fornecem informações sobre quais falhas são predominantes e devem ser tratadas com mais atenção, além de não auxiliar na escolha de diferentes conceitos em termos da confiabilidade. Com o objetivo de solucionar tais limitações, os autores sugerem o uso do método *Go-Flow*, que também é bastante utilizado na análise de confiabilidade. No método *Go-Flow*, operadores representam componentes ou relacionamentos lógicos no sistema, sinais representam conexões entre componentes (Figura 3.3) e então uma tabela com os relacionamentos e probabilidades é gerada. Porém, a técnica não é completamente adequada para a fase de projeto conceitual, mas os autores propõem a identificação de informações sobre falhas funcionais com base na síntese funcional do produto.

Figura 3.3 – Exemplo de elementos da técnica *Go-Flow*



Fonte: adaptado de Bai et al. (2008)

Apesar da dificuldade de se avaliar a confiabilidade e segurança no projeto conceitual, vale ressaltar que na maioria das vezes os conceitos selecionados para cumprir as funções do sistema são componentes ou subsistemas já utilizados em outros projetos, mas combinados de forma específica dentro do contexto do projeto em desenvolvimento. Dessa forma, verifica-se a possibilidade de, a partir da modelagem de como os componentes e subsistemas interagem (pelo fluxo de energia, por exemplo), utilizar dados de falha de outros sistemas como uma aproximação inicial para obter as probabilidades de falha *a priori* e auxiliar na tomada de decisão de projeto.

Zio (2013) afirma que ao projetar um sistema ou tentar melhorar um sistema existente, o engenheiro tenta antecipar padrões de operação do sistema para diferentes princípios de solução. Inevitavelmente a previsão do desempenho é feita a partir de modelos da realidade, que por definição nunca são aderentes à realidade em todos os detalhes. Os modelos são baseados nas

informações disponíveis sobre as interações entre os componentes dos sistema, nas interações do sistema com o ambiente e nos dados relacionados com as propriedades dos componentes do sistema. Segundo o autor, esses aspectos determinam como os componentes transitam entre seus possíveis estados e, desta forma, como o sistema se comporta. Por fim, a partir destes modelos, pode-se responder algumas questões sobre o futuro do sistema, como as falhas, manutenção, peças de reposição, equipe de manutenção, etc.

3.2 ABORDAGEM DE SISTEMA E A ANÁLISE DE FALHAS

Segundo Haskins et al. (2006), o processo de engenharia de sistemas tem uma natureza iterativa que dá suporte ao aprendizado e à melhoria contínua. No decorrer do processo, os engenheiros de sistemas desvendam os requisitos reais e propriedades que emergem do sistema. A complexidade pode levar a comportamentos inesperados e imprevistos do sistema, sendo um dos objetivos minimizar consequências indesejáveis. Esse objetivo é alcançado pela inclusão e contribuição de especialistas de áreas relevantes, trabalhando de forma coordenada.

Segundo Smith e Simpson (2004) para sistemas eletrônicos, uma parte significativa das falhas ocorridas não são resultantes das falhas diretas de subsistemas e componentes, mas de interações mais complexas dentro da operação do sistemas. Essa complexidade tem relação com fatores humanos, interferências do ambiente, variações na relação entre componentes e tolerâncias de projeto.

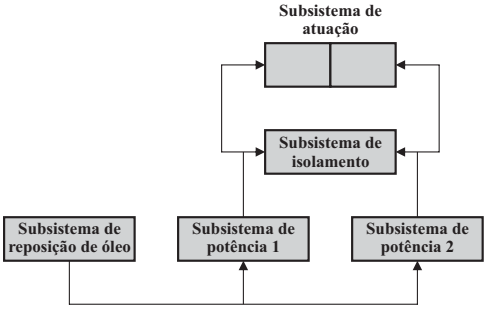
A engenharia de sistema fortalece a cultura de analisar os sistemas de forma mais ampla, visando identificar em mais detalhe as interações de subsistemas e componentes. Dependendo do tipo de sistema a ser projetado, as funções podem ser cumpridas pela combinação de subsistemas e componentes já existentes, mas combinados de forma específica para o sistema sendo projetado. Dessa forma, os dados relativos a falhas dos componentes isolados podem ser reaproveitado e a falha do sistema pode ser analisada ao estabelecer as relações entre os subsistemas e componentes.

Considerando-se o sistema hidráulico de movimentação do leme de um navio representado na Figura 3.4, por exemplo, é possível perceber que uma vez que os requisitos do sistema e as funções estejam definidos, os subsistemas representados podem ser projetados utilizando-se diferentes combinações de componentes (BIASOTTO, 2008; KAGUEIAMA, 2012).

Estes componentes, por sua vez, são os mesmos que podem ter sido usados em uma série de outros sistemas hidráulicos já projetados em algum momento, e os dados de falhas destes componentes podem estar disponíveis.

No caso específico de sistemas hidráulicos, existem diferentes bancos de dados de falhas disponíveis contendo as taxas de falhas para diversos componentes existentes, como o *Offshore Reliability Data* (SINTEF, 2002).

Figura 3.4 – Representação esquemática do sistema hidráulico do leme de um navio



Fonte: Biasotto (2008)

No caso do sistema hidráulico representado esquematicamente na Figura 3.4, os requisitos principais do sistema são o curso do leme (70 graus) e o tempo que o sistema leva para mover o leme de 35 graus de um bordo a 35 graus do bordo oposto (BIASOTTO, 2008). A existência do subsistema de potência 2 e do subsistema de isolamento é baseada em decisão de projeto visando melhorar a confiabilidade e segurança do sistema, tendo em vista que em caso de falha do subsistema de potência 1, o subsistema de potência 2 entra em operação. Além disso, existe a possibilidade de utilizar o subsistema de isolamento para desativar um dos pares de atuadores. Os componentes selecionados para compor os subsistemas representados dependem de decisões de projeto a partir das funções identificadas.

A partir deste exemplo é possível perceber que sistemas complexos fabricados em pequena escala, conforme citado por Johansson (2013), normalmente são compostos por subsistemas e componentes existentes e já utilizados no mercado. Porém, para que os dados de falha possam ser utilizados na fase de projeto de novos sistemas, não basta utilizar diretamente estes dados, pois a combinação dos subsistemas e componentes se dá de maneira específica para o sistema que está sendo projetado.

Assim, torna-se importante inserir modelos que detalhem como os subsistemas e componentes interagem especificamente no sistema projetado para que, desta forma, seja possível obter modelos que forneçam dados de confiabilidade mais próximos do real e então avaliar diferentes concepções de projeto visando otimizar a confiabilidade do sistema. Alguns trabalhos tratam

de alguma forma essas questões, como por exemplo o trabalho de Porciúncula (2009). Na fase conceitual de projeto de novos sistemas, montados a partir da recomposição de itens já existentes e de outras aplicações é possível utilizar especificações do projeto informacional e prover análise já considerando interfaces e outras estruturas funcionais. Nestes casos, simular a funcionamento no contexto de confiabilidade dinâmica (SAKURADA, 2013) e incluir análise de cenários advinda de falhas ocultas, torna-se importantes para orientar decisões de projeto.

3.3 CONSIDERAÇÕES FINAIS

No presente capítulo foi realizada uma breve revisão sobre o processo de projeto de produtos, tendo como modelo de referência o PRODIP; e de como a confiabilidade, a segurança e consequentemente a análise de risco são tratadas na fase de projeto conceitual.

No PRODIP, o final do projeto conceitual visa a concepção do produto. Para sistemas complexos, o principal nem sempre é a concepção do produto, mas a garantia que o sistema se comporta conforme o esperado, sem gerar consequências negativas para o homem e ambiente, dado que as consequências de uma falha podem ser bastante severas.

Levando-se em consideração o impacto que a fase de projeto conceitual tem sobre o cumprimento dos requisitos definidos para o produto em relação aos baixos custos envolvidos nas alterações de projeto durante esta fase, fica evidente a importância de se avaliar concepções e buscar soluções otimizadas nesta fase de projeto. Porém, a grande dificuldade está na falta de dados quantitativos que permitam avaliar as concepções de forma mais concreta.

Durante a revisão bibliográfica foi possível perceber um consenso sobre o fato que tradicionalmente a confiabilidade só é avaliada a partir da fase de projeto preliminar e detalhado, uma vez que, devido a falta de informação durante o projeto conceitual, apenas nestas fases podem começar a ser feitos testes para o levantamento dos dados de falha.

Além disso, foi possível perceber que as propostas de incorporar a análise de confiabilidade durante a fase de projeto conceitual tem o objetivo principal de automatizar a análise e buscar alternativas para se obter dados a priori que permitam uma avaliação preliminar. Entretanto, não encontrou-se trabalhos que consideram a existência de falhas ocultas ou então da consideração dos diferentes cenários causais resultantes da combinação de falhas de subsistemas e componentes nesta fase do processo de projeto.

Foi evidenciado também a importância de se definir as interações entre componentes do sistema para obter resultados mais próximos da realidade,

tendo em vista os problemas envolvidos com a disponibilidade de dados. A visão de engenharia de sistemas permite compreender um sistema complexo como uma combinação específica de componentes muitas vezes já existentes e conhecidos; e que modelando as interações entre estes componentes, tanto pela operação normal como sob a ocorrência de falhas, é possível avaliar melhor as falhas.

No Capítulo 4 será apresentada uma breve revisão sobre os conceitos que definem as falhas ocultas e que servirão como orientação para desenvolver a solução para o problema de pesquisa, no contexto de falhas ocultas. Será mostrado a importância das falhas ocultas para a definir os cenários de risco, que na maioria das vezes são difíceis de ser identificados durante o projeto.

4 FALHAS OCULTAS E OS CENÁRIOS DE RISCO

Conforme descrito no Capítulo 3, sistemas podem ser definidos como a interação de componentes associados para o cumprimento de uma função (CASSANDRAS; LAFORTUNE, 2008). O estado de um sistema, por sua vez, descreve comportamento do sistema em um dado instante de tempo.

A transição de estados de um sistema se dá pela ocorrência de um evento, o qual pode ser uma ação tomada sobre o sistema, uma ocorrência natural ditada pela natureza ou até a combinação de diferentes fatores.

Se considerarmos um carro, por exemplo, os estados operacionais podem ser definidos como "ligado", "desligado", "acelerando" e "freando". A transição entre os estados ocorre de acordo com a operação do sistema, no caso deste exemplo, o ato de dirigir o carro. Assim, ao girar a chave na ignição (evento A) o carro transita do estado "desligado" para o estado "ligado", e ao pisar no acelerador (evento B) o carro passa do estado "ligado" para o estado "acelerando".

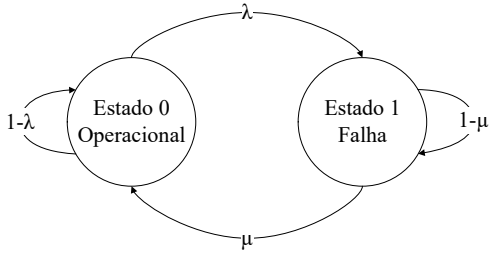
Além das demandas naturais da operação do sistema, os estados podem ainda ser definidos de acordo com falhas. Um sistema pode estar em um estado "com falha" ou "sem falha", por exemplo. Um sistema que opera normalmente encontra-se no estado "sem falha" até a ocorrência de um evento (falha) que o leva ao estado "com falha". Essa transição pode ou não resultar em um comportamento indesejado para o sistema, dependendo do tipo de falha. Caso a falha não influencie o funcionamento do sistema dentro do estado que se encontra, estas são chamadas de falhas ocultas. Estas falhas estão fortemente relacionadas aos estados operacionais do sistema, pois estes estados definem os efeitos da falha e sua detecção.

Diversos autores tratam falhas como sistemas markovianos (BILLINTON; ALLAN, 1992; KUMAMOTO; HENLEY, 1996; ZIO, 2013). Veras (2016), por exemplo, representa uma falha por meio de um modelo markoviano constituído de dois estados: um estado bom, ou operacional; e outro em falha (Figura 4.1). Para um sistema reparável, há uma probabilidade de falhar, representada por uma taxa de falha "λ"; e a probabilidade de o sistema sofrer manutenção, representado por uma taxa de recolocação "μ". No caso de sistemas não reparáveis (não manuteníveis) não há a taxa de recolocação.

Essa representação de falhas como sistemas markovianos também pode levar em consideração a degradação dos sistemas. Para isso, Veras (2016) utiliza uma abordagem multiestados, considerando níveis de degradação (estados intermediários) entre o estado operacional e de falha (Figura 4.2).

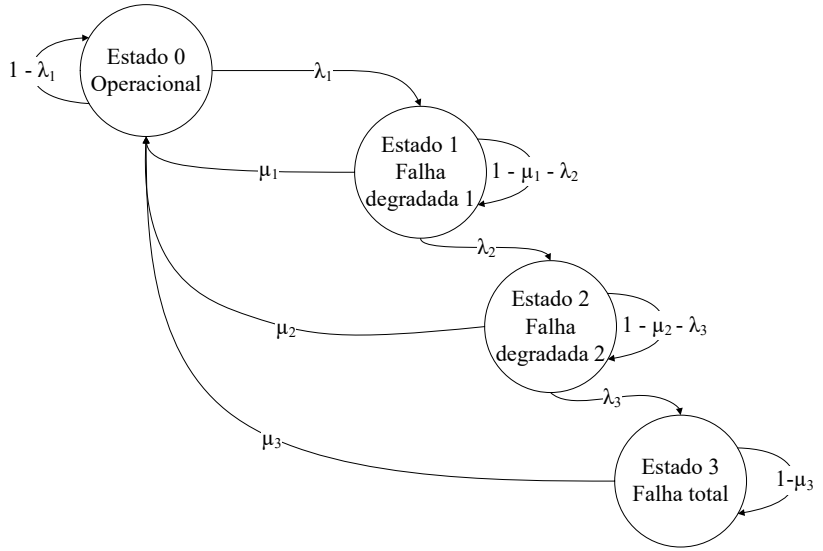
Para Isermann (2005) uma falha é um desvio não permitido de ao menos uma propriedade característica (atributo) do sistema do que é a condição

Figura 4.1 – Representação de falhas como modelo markoviano



Fonte: Veras (2016)

Figura 4.2 – Abordagem multiestados para a degradação de sistemas



Fonte: Veras (2016)

aceitável, usual e padrão.

A sequência de eventos que levam a um comportamento específico do sistema define um cenário. Neste trabalho, há o interesse em estudar os cenários que envolvem a ocorrência de falhas (mais especificamente falhas ocultas) e as transições naturais do sistema de acordo com sua operação. A ocorrência de falhas não leva o sistema obrigatoriamente a incidentes catastróficos, principalmente quando tratam-se de falhas ocultas. Isso ocorre pelo

fato de a consequência imediata das falhas ser dependente da condição sob a qual o sistema opera no instante em que a falha ocorre. Por essa razão, há o interesse em modelar a relação entre as falhas ocultas e a operação do sistema, ampliando desta forma o entendimento sobre os cenários de falha.

A confiabilidade, mantenabilidade e o risco estão relacionados com a operação do sistema, de acordo com os requisitos que serviram de referência para o desenvolvimento do projeto, e a possibilidade de ocorrência de falhas. Nenhum sistema é capaz de operar infinitamente dentro das condições definidas em projeto.

Seja pelo desgaste natural causado pela interação entre partes ou pela falha de algum componente devido a forças excessivas não previstas em projeto, eventualmente um sistema atinge o fim do ciclo de vida, quando deixa de cumprir suas funções corretamente.

O ponto em comum entre a confiabilidade, a mantenabilidade, e o risco está justamente nas falhas. A maneira como se aborda a análise de falhas e os objetivos que permeiam seu desenvolvimento, definem em que área ela está inserida e qual a finalidade.

Para a confiabilidade, o interesse está em saber qual a probabilidade da ocorrência de falhas ao longo do ciclo de vida, de acordo com as condições de operação. Já para a mantenabilidade, o interesse está em estabelecer medidas para evitar, retardar ou recuperar o item quando ocorrem as falhas. Sob o ponto de vista da segurança e do risco, o interesse está em saber quais falhas podem causar danos às pessoas ou ao meio ambiente. No caso da esfera estourar dentro do bolso, por exemplo.

A seguir estes conceitos serão abordados em mais detalhe, visando evidenciar a importância de mitigar as falhas em sistemas técnicos, especialmente em relação à definição de falhas ocultas. Este tipo de falha pode levar ao acúmulo de eventos indesejados e causar a exposição do sistema aos riscos.

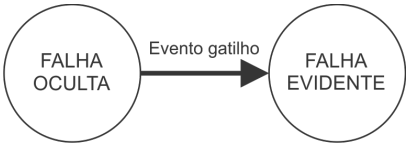
4.1 CONCEITOS DE FALHAS OCULTAS

A ocorrência de falhas ocultas é uma questão particular que deve ser trabalhada de forma diferenciada, pois pode comprometer tanto a identificação dos cenários de falha (por não ser facilmente observável) como a efetividade das barreiras estabelecidas quando estas envolvem procedimentos de operação e manutenção. Nowlan e Heap (1978) definem que uma falha é oculta quando sua ocorrência não é evidente.

A falha de um sistema é resultado das falhas de componentes, que por sua vez podem evidentes ou ocultas. Uma falha oculta necessita de um evento gatilho para que possa ser percebida, como ilustrado na Figura 4.3 e Figura 1.2

(Capítulo 1). De acordo com a Figura 4.3, quando uma falha é oculta, ela resulta em uma condição latente (sem efeito imediato sobre o sistema) e não é percebida até que ocorra um evento gatilho que evidencia a ocorrência da falha e que torna essa condição latente perceptível a um observador. Este evento pode ser a ocorrência de outra falha ou a mudança de estado de um ou mais componentes do sistema devido a uma demanda operacional.

Figura 4.3 – Transição de falha oculta para evidente



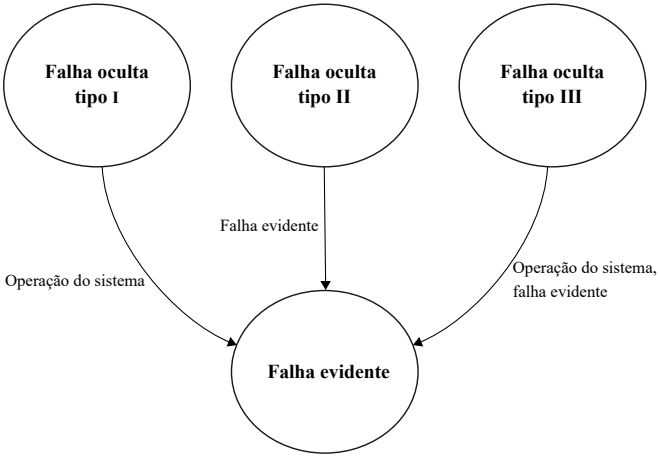
Tais falhas podem ser facilmente entendidas quando se observa componentes em *stand-by* ou em sensores. No caso de componentes em *stand-by*, quando uma falha ocorre não há alteração imediata no comportamento do sistema e a falha não é percebida até que por algum motivo (diante da falha do componente principal ou componente ativo) seja necessário que o componente reserva (*stand by*) entre em operação. No caso de falhas em sensores, falhas que causam erros de leitura só são percebidas quando for realizada alguma aferição. Assim, a condição de falha oculta não é percebida até que um evento requeira a utilização daquele item que está em falha ou que resulte em um comportamento que evidencie a existência de uma falha. Neste instante, deflagra-se uma condição crítica do sistema que, nos casos limites, pode gerar incidentes com consequências significativas.

A forte relação das falhas ocultas com as condições de operação dificulta a identificação deste tipo de falha. Por esta razão é necessário estabelecer uma definição mais clara de falhas ocultas. Na Figura 4.4 estão presentes os cenários gerais de um sistema com possibilidade de evidenciar as falhas ocultas, identificando-se três tipos de falhas ocultas, caracterizadas por serem evidenciadas a partir da ocorrência de diferentes eventos ou combinações de eventos gatilho.

A "Falha oculta tipo I" representa as falhas evidenciadas pelas transições de estado devido a operação normal do sistema: um componente está em operação, deve parar, volta a operar; requer participação de outro item, de sensores ou atuadores. Neste caso, não percebe-se a ocorrência de uma falha oculta, até que a mudança de estado se faça necessária. A "Falha oculta tipo II" representa os casos em que as falhas ocultas são evidenciadas pela ocorrência de uma falha evidente em um outro item do sistema. Estes casos podem ser verificados facilmente nas falhas de componentes em *stand by*, pois a falha

oculta deste tipo de componente é evidenciada quando a operação exige que este opere no lugar do componente principal (no caso de um procedimento de manutenção do componente principal, por exemplo), ou quando ocorre uma falha evidente no componente principal e o componente redundante (*stand by*) tem que entrar em operação. Em casos mais críticos, como os representados pela "Falha oculta tipo III", é necessário que tanto uma falha evidente quanto a transição do sistema pela operação ocorram para que a falha oculta seja evidenciada. Essa situação pode ser observada quando existe um controlador que define qual componente deve entrar em operação caso ocorra a falha de um outro componente.

Figura 4.4 – Cenários que evidenciam falhas ocultas



No contexto da manutenção centrada em confiabilidade (MCC), Nunes (2001) afirma que este modelo de gestão da manutenção atribui grande prioridade à avaliação e prevenção das falhas ocultas, pois apesar de não ter impacto direto sobre a produção (já que não trazem consequências imediatas ao sistema) as falhas ocultas expõem as instalações à possibilidade de ocorrência de múltiplas falhas. Como exemplo, o autor cita falhas em dispositivos de proteção como sensores, dispositivos de supervisão, botoeiras de comando, relés de proteção, sistemas anti-incêndio, equipamentos instalados em *stand by*, cujas falhas podem trazer consequências catastróficas para a instalação, com reflexos significativos para a imagem institucional.

Ainda segundo Nunes (2001), uma tendência natural ao se avaliar os riscos associados, as consequências das falhas ocultas e reduzir a probabilidade de sua ocorrência comprometer a instalação é a adoção de equipamentos redundantes, mais confiáveis e modernos. Porém, a adição de mais compo-

nentes com a finalidade de cumprir funções extras de prevenção da ocorrência de falhas ocultas pode não surtir os efeitos desejados, pois tais componentes extras tendem a também estar sujeitos a falhas ocultas.

Albinali e Meliopoulos (2017) relaciona as falhas ocultas a relés de proteção conhecidos como dispositivos eletrônicos inteligentes (IED - *intelligent electronic device*), usados na proteção de sistemas de distribuição de energia. Os autores definem as falhas ocultas como defeitos permanentes nos relés que causam o isolamento inapropriado de algum elemento do sistema, como consequência direta de outro evento. Nesses casos as falhas ocultas resultam em informações incorretas fornecidas aos IEDs que resultam na operação incorreta. Para solucionar os problemas com falhas ocultas, os autores propõem um esquema centralizado de proteção que permite o monitoramento e detecção das falhas ocultas, por meio da comparação entre medições coletadas do sistema e os modelos desenvolvidos.

Vale ressaltar que como a ocorrência da falha oculta só é percebida algum tempo depois que ela ocorreu, os dados de falha registrados durante a operação são incorretos (a falha pode ter ocorrido a muito tempo ou a pouco tempo), resultando em modelos imprecisos para a previsão de sua ocorrência. Desta forma, é necessário obter modelos que contemplem os diversos cenários que combinam transições operacionais dos sistema e as falhas para determinar quando uma falha oculta efetivamente ocorre.

Segundo Lienhardt et al. (2008), as falhas ocultas afetam principalmente sistemas redundantes e de proteção, tal como válvulas de segurança (ou alívio) e sensores. Porém, é possível identificar casos em que as falhas ocultas estão presentes em outros tipos de sistemas, quando a operação requer alterações constantes em seus estados de operação e que devido a ocorrência de falhas o sistema não responde corretamente. Podemos citar como exemplo, uma válvula que falhou aberta e que se deseja fechar sob determinadas condições de operação, como apresentado por Sakurada (2013).

Analisando-se o histórico de acidentes notórios ocorridos ao longo do tempo é possível perceber a grande influência das falhas ocultas, como nos casos da usina de Three Mile Island e do ônibus espacial Challenger (KUMAMOTO; HENLEY, 1996), por exemplo. Na usina de Three Mile Island, uma válvula de segurança que falhou aberta e a indicação no painel de controle que a válvula estava fechada resultaram no acidente. Já no caso do ônibus espacial, falhas nos anéis de borracha da vedação dos tanques de combustível levaram à explosão e morte de todos os tripulantes.

Maurino et al. (1995) afirmam que as falhas ocultas só são descobertas quando ocorrem falhas nas defesas ou barreiras do sistema, mas não é preciso esperar que um acidente ocorra para que ações sejam tomadas, pois lições aprendidas permitem identificar deficiências nas barreiras antes que acidentes

de grandes proporções ocorram. Portanto, é possível perceber a importância de se estudar melhor as falhas ocultas e estabelecer uma forma de melhorar a análise e gerenciamento de sua ocorrência.

Tradicionalmente as falhas ocultas são gerenciadas por meio da determinação de inspeções periódicas para verificar se a falha oculta está presente (LIU et al., 2017). Muitos trabalhos foram desenvolvidos com o objetivo de se estabelecer uma periodicidade ótima para procedimentos de manutenção preventiva. Na manutenção centrada em confiabilidade existe a tarefa de busca de falhas (*failure-finding tasks*), cujo objetivo é detectar a ocorrência, porém estas tarefas devem ser executadas de forma a exercer a mínima interferência sobre a operação do sistema, evitando-se a inclusão de outras falhas no equipamento. Assim, a maior parte dos esforços visam à otimização da peridiocidade das inspeções.

Liu et al. (2017) trazem outro trabalho com foco na determinação dos intervalos de inspeção para detecção de falhas ocultas. Segundo os autores, as falhas ocultas não levam a quebra do sistema, mas a existência de falhas ocultas pode resultar na perda de desempenho durante a operação do sistema. O trabalho traz o desenvolvimento de uma política de manutenção para sistemas complexos sujeitos a falhas ocultas, com o objetivo de estabelecer intervalos de inspeção para cada componente de tal forma que os custos a longo prazo possam ser minimizados.

Segundo Taghipour e Banjevic (2011), os diversos modelos desenvolvidos para estabelecer a peridiocidade de inspeção na manutenção preventiva podem ser classificados de acordo com quão próximo de sua condição inicial o sistema retorna após a execução de procedimento de manutenção. Alguns modelos assumem que após a manutenção o sistema se encontra tão bom quanto novo; e outros consideram procedimentos de manutenção imperfeitos, tornando as taxas de falha mais altas que os valores iniciais. Dessa forma, os autores propõem um modelos para a otimização da peridiocidade de inspeção para identificar a ocorrência de falhas ocultas, assumindo:

- falhas ocultas não interrompem necessariamente a operação do sistema mas podem causar redução no desempenho do sistema;
- as falhas só podem ser corrigidas em inspeções periódicas do sistema;
- uma penalidade (em termos de custo) é aplicada de acordo com o tempo transcorrido entre a ocorrência da falha e sua detecção na próxima inspeção;
- um componente em falha pode ser minimamente reparado ou trocado com probabilidade dependente da idade;

- inspeções são perfeitas e o tempo de reparo pode ser desprezado;
- as falhas de cada componente são processos de Poisson não homogêneos.

Em outro artigo, Taghipour e Banjevic (2012) incorporam as falhas evidentes (chamadas de falhas duras) a dois modelos que estabelecem a peridiocidade de inspeção junto com as falhas ocultas (chamadas de falhas moles), aplicado em equipamentos médicos. Os autores chamam a atenção para a importância de se incorporar ambos os tipos de falhas em modelos de otimização em sistemas complexos. Em ambos os casos os componentes são minimamente reparados ou substituídos quando uma falha é identificada, sendo que as falhas ocultas são verificadas em inspeções periódicas ou em inspeções de oportunidade, e as falhas evidentes são identificadas imediatamente após a ocorrência. No primeiro modelo, considera-se que para ambas as falhas os componentes podem ser minimamente reparados ou substituídos, de acordo com suas condições ou estados. O segundo modelo considera inspeções periódicas de componentes sujeitos a falhas evidentes e a possibilidade de substituição preventiva baseada na condição constatada durante a inspeção. Ambos os modelos são solucionados matematicamente pela derivação de equações recursivas (nas quais um termo é definido por um termo de ordem anterior) e um algoritmo de otimização é utilizado para calcular os valores requeridos.

Lienhardt et al. (2008), por sua vez, definem a tarefa de busca de falhas como um processo markoviano e, a partir desta suposição, derivam as taxas de falha e a peridiocidade otimizada para as inspeções. Para desenvolver o modelo, as seguintes suposições foram assumidas:

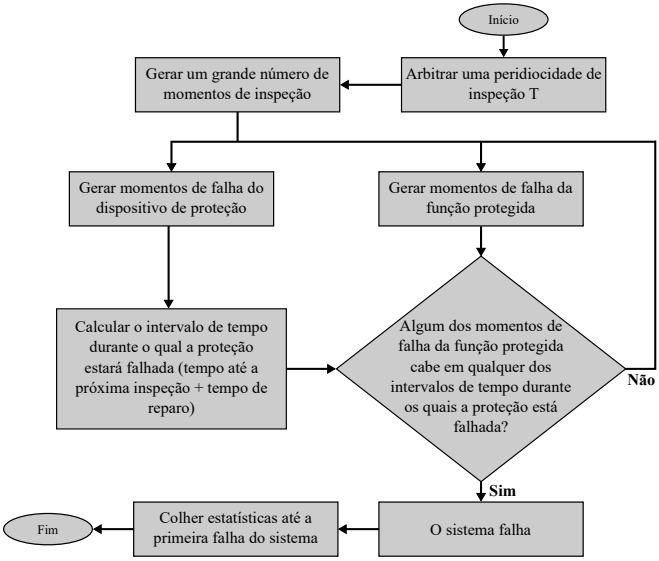
- demandas operacionais são processos de Poisson não-homogêneos;
- a taxa de falha de um sistema com falha oculta é função do tempo;
- se durante a inspeção o sistema com falha oculta está em operação, nada é feito;
- em caso de manutenção corretiva, o reparo é mínimo.

Hokstad e Frøvig (1996) abordaram em sua pesquisa as falhas chamadas de degradação e críticas. As falhas críticas são aquelas que resultam no comprometimento da operação do sistema. As falhas de degradação, por sua vez, são aquelas que não comprometem completamente a operação do sistema mas sinalizam a ocorrência potencial de uma falhas crítica, caso não seja executado algum reparo, agindo como sensores para a ocorrência das

falhas críticas. Os autores sugerem a revisão das taxas de falha, considerando a dependência entre os dois tipos de falha por meio da modelagem de mecanismos de falha. Esta modelagem utiliza processos markovianos em que os estados correspondem a graus de degradação dos componentes do sistema. O trabalho é aplicado em sistemas em *stand by*, os quais estão sujeitos a falhas ocultas, chamadas pelos autores de *fail-to-operate*.

A Figura 4.5 apresenta o modelo desenvolvido por Assis (2012) para estabelecer a peridiocidade de inspeção de falhas ocultas. No trabalho, o autor relaciona as falhas ocultas com componentes cuja função é de proteção, tal como sensores e válvulas de segurança. Com isso, define-se o conceito de função protegida (função do sistema) e função protetora (função dos componentes de proteção). Dessa forma, o trabalho consiste em otimizar a inspeção dos componentes de proteção, cujas falhas são modeladas de acordo com uma distribuição de Weibull de tri-paramétrica, admitindo-se modos de degradação representados pelo parâmetro de forma. Para isso, o autor considera duas situações possíveis:

Figura 4.5 – Cenários que evidenciam falhas ocultas



Fonte: Assis (2012)

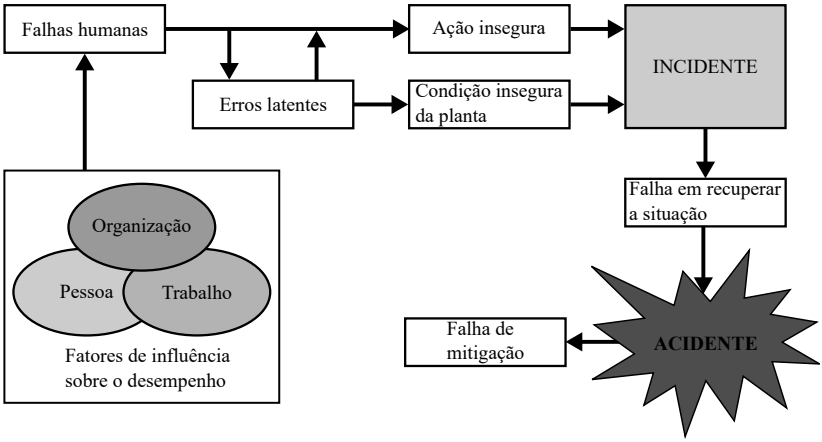
- O componente de proteção se encontra operacional e atua, dando início a uma ação, e o sistema é recuperado em um curto intervalo de tempo e com custo reduzido.

- O componente de proteção se encontra em falha e, caso ocorra a falha da função protegida (principal do sistema) as consequências são mais graves, resultando em um tempo de recuperação e custo maiores.

Vale ressaltar que, segundo Moubray (1997), é possível constatar que em determinados sistemas técnicos em torno de 40% das falhas são classificadas como falhas ocultas e que em torno de 80% destas dependem de tarefas de detecção de falhas. Porém, é evidente que para sistemas críticos como aeronaves, usinas nucleares, entre outros, essa abordagem tradicional das falhas ocultas não é viável, pois qualquer tipo de falha nesses sistemas pode ter consequências catastróficas.

Reino Unido (2017) define as falhas ocultas em relação a fatores humanos. Segundo o documento, acidentes são causados por falhas ativas ou ocultas (latentes) que podem levar a erros humanos. O modelo de acidentes relacionados a falhas humanas está apresentado na Figura 4.6.

Figura 4.6 – Modelo de acidente relacionado a falha humana



Fonte: Reino Unido (2017)

As falhas ocultas são definidas como atos ou condições ocultas (latentes) que levam aos erros humanos ou violações de procedimentos. As falhas ativas são definidas como atos ou condições que conduzem às condições de incidentes. Estas falhas estão relacionadas a pessoas mais ativas sobre a operação sendo executada, são imediatas e podem ser evitadas por alterações no projeto, no treinamento ou na operação do sistema. As condições ocultas (latentes) levam às falhas ocultas e são influenciadas por pressões gerenciais e sociais que escondem comportamentos inadequados para a operação do

sistema. Por mais treinamento que as pessoas possuam, estas sempre estão sujeitas a erros.

É possível perceber a partir da bibliografia existente que as falhas ocultas são normalmente tratadas por meio de inspeções periódicas. Os diferentes modelos existentes buscam incorporar diferentes aspectos relevantes sobre a ocorrência das falhas ocultas, tal como a influência de falhas evidentes ou o conceito de degradação de componentes, porém não consideram a influência dos estados operacionais sobre a definição das falhas ocultas.

Além disso, é possível perceber que os modelos necessitam de algum dado de falha observado sobre os componentes. Entretanto, sabe-se que dados reais sobre os sistemas são escassos, principalmente quando se trata da fase de projeto do ciclo de vida. Por essa razão, o presente trabalho propõe uma forma de integrar modelos de falha comumente utilizados com modelos comportamentais de tal forma que seja possível utilizar dados sobre componentes utilizados em outros sistemas existentes para se estimar as probabilidades de ocorrência de falhas ocultas em sistemas durante o projeto.

4.2 PROBLEMA DE REFERÊNCIA

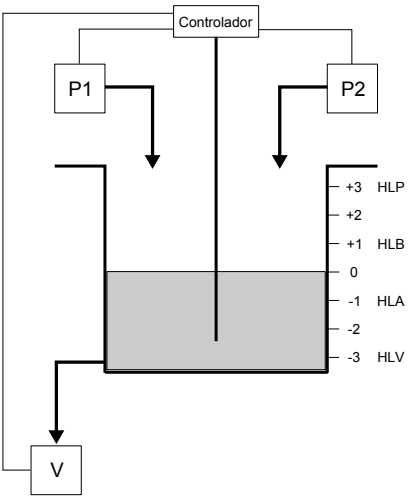
Para facilitar o entendimento dos conceitos que envolvem a definição de falhas ocultas e suas consequências, será utilizado o problema de referência baseado no sistema de arrefecimento de usinas nucleares. Este problema foi utilizado para avaliar e comparar diferentes metodologias empregadas na análise de confiabilidade dinâmica (MARSEGUERRA; ZIO, 1996; MARSEGUERRA et al., 1998; CODETTA-RAITERI; BOBBIO, 2006; SAKURADA, 2013). A confiabilidade dinâmica é uma análise de confiabilidade aplicada em sistemas dinâmicos, onde ocorrem mudanças ao longo do tempo na configuração do sistema, nas variáveis de estado do sistema ou em alguma característica de seus componentes (SAKURADA, 2013). Em função das mudanças observadas, ações são tomadas a fim de impedir a falha total do sistema técnico.

O sistema está representado na Figura 4.7 e sua função é manter o nível de água estável. Como pode ser visto, ele é composto por um reservatório, duas bombas P1 e P2 (P2 em *stand by*), uma válvula V e um controlador.

As bombas e a válvula tem a mesma vazão, podendo resultar em uma variação de nível no reservatório igual a 0,6m/h. A falha de um componente (bombas ou válvula) é oculta quando não causa variação do nível do reservatório, sendo que os três componentes tem a mesma vazão. Se P1 falhar aberta, por exemplo, o nível não será alterado até que V falhe fechada ou que P2 falhe aberta. As funções e estados operacionais na condição normal de operação (sem variação no nível do reservatório) dos componentes do sistema estão

apresentados no Quadro 4.1. O Quadro 4.2 apresenta o comportamento da variação de nível de acordo com os estados dos componentes.

Figura 4.7 – Exemplo para falha oculta



Fonte: Sakurada (2013)

Quadro 4.1 Funções do subsistema de propulsão

Componente	Função	Estado normal
Bomba P1	Fornecer fluido	Ligado
Bomba P2	Fornecer fluido	Desligado
Válvula V	Drenar fuido	Ligado
Reservatório	Armazenar fluido	-
Controlador	Ler nível do fluido e controlar o nível do reservatório	-

Fonte: Sakurada (2013)

Neste exemplo clássico, o controlador é um elemento considerado perfeito (não sujeito a falhas) e, caso seja detectada a variação do nível do reservatório (mais ou menos 1), este componente comanda o desligamento das bombas e o fechamento da válvula. A falha do sistema ocorre quando o nível atinge mais 3 ou menos 3. Assim, é possível perceber que quando um componente falha de forma que não seja possível alterar seu estado (P1 falha aberta, por exemplo), o comando do controlador se torna um evento que evidencia a falha oculta, o que torna importante a inclusão das transições de

Quadro 4.2 Taxa de variação de nível de pelo estado dos componentes

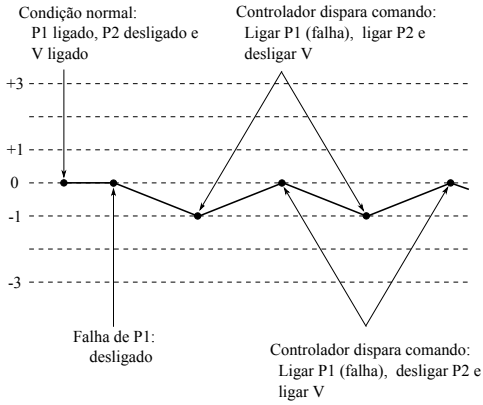
Configuração	P1	P2	V	Vazão
1	Ligado	Desligado	Desligado	0,6 m/h
2	Ligado	Ligado	Desligado	1,2 m/h
3	Ligado	Desligado	Ligado	0,0 m/h
4	Ligado	Ligado	Ligado	0,6 m/h
5	Desligado	Desligado	Desligado	0,0 m/h
6	Desligado	Ligado	Desligado	0,6 m/h
7	Desligado	Desligado	Ligado	-0,6 m/h
8	Desligado	Ligado	Ligado	0,0 m/h

Fonte: Sakurada (2013)

estados nos modelos probabilísticos de falhas ocultas.

A Figura 4.8 apresenta um exemplo de cenário de falha evidente obtido nas simulações resultantes do trabalho de Sakurada (2013), no qual foi desenvolvido um método de análise de confiabilidade dinâmica utilizando o Método de Monte Carlo para a obtenção de tempos de falha aleatórios a partir das taxas de falha dos componentes. Uma falha evidente pode ser, por exemplo, uma falha que causa o desligamento da bomba P1, causando o aumento do nível do reservatório; ou então o desligamento da válvula, causando a diminuição do nível do reservatório.

Figura 4.8 – Cenário de falha evidente

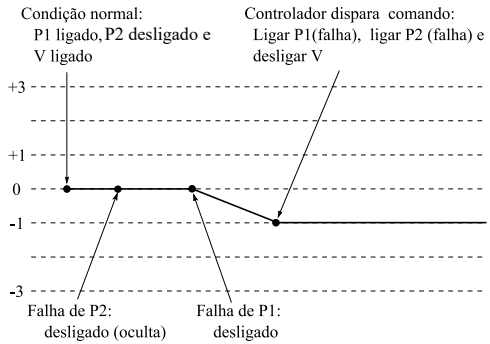


Fonte: Sakurada (2013)

A Figura 4.9 apresenta um cenário de falha oculta, no qual houve a falha fechada da bomba P2 mas tal falha só foi percebida após a falha da

bomba P1, que fez o controlador comandar o ligamento das bombas e o fechamento da válvula, porém a bomba P2 não respondeu. A partir da análise dos resultados do trabalho foi possível perceber que na maioria dos casos em que foi observada a falha do sistema (transbordamento ou esvaziamento do reservatório), a causa foi a ocorrência de falha oculta de algum componente. Além disso, o trabalho chamou a atenção para a importância de se desenvolver pesquisa específica sobre falhas ocultas, pois percebe-se que se o controlador comandar os componentes periodicamente e não apenas como resposta a variações do nível do reservatório (causado por falhas) o número de ocorrência de falhas ocultas cresceria consideravelmente.

Figura 4.9 – Cenário de falha oculta



Fonte: Sakurada (2013)

Considerando-se o ciclo de vida do sistema técnico, o estudo das falhas ocultas tem grande influência tanto na fase de projeto quanto na fase de uso. Durante a fase de projeto as conclusões obtidas a partir da caracterização da ocorrência das falhas ocultas na análise de confiabilidade podem influenciar diretamente o reprojeto ou a seleção de novos princípios de solução de um produto, tais como a opção por adicionar componentes redundantes, adicionar componentes para monitorar as causas de uma falha ou então, por exemplo, optar por componentes mais complexos ou mais simples desde que menos suscetíveis a ocorrência de falhas ocultas. Já na fase de uso, o resultado da análise influencia diretamente os procedimentos de manutenção adotados, pois auxilia o mantenedor na tomada de decisões como: priorizar a manutenção de componentes, elaboração de procedimentos para identificar as falhas ocultas dos componentes e estabelecimento de barreiras para impedir a propagação de falhas(SAKURADA, 2013).

4.3 MODELOS COMPORTAMENTAIS

Os modelos comportamentais são necessários para que as transições de estado dos componentes do sistema sejam incorporadas na análise das falhas ocultas, pois as transições são eventos que podem tornar uma falha oculta em evidente. Assim, o comportamento dinâmico do sistema faz parte das características que definem as falhas ocultas.

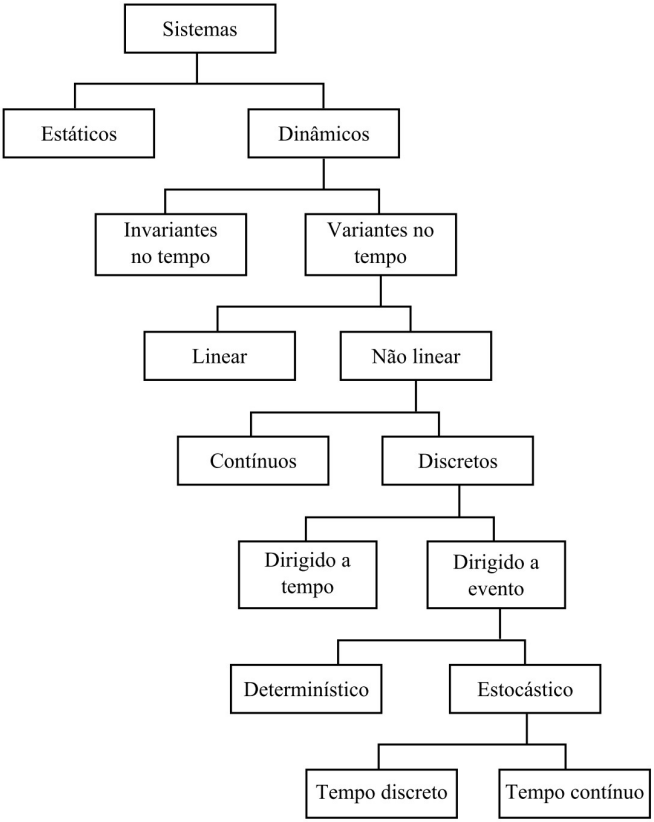
Retornando ao problema de referência (Figura 4.7), considerando-se agora que o controlador não é mais um elemento passivo, que só comanda a mudança de estado das bombas e da válvula quando verifica que houve mudança o nível do reservatório. É possível perceber que se o controlador comandar periodicamente que a bomba P2 entre em operação no lugar de P1, torando-se um elemento ativo, a identificação das falhas ocultas será alterada. A partir deste exemplo simples é possível perceber que para se analisar a ocorrência das falhas ocultas não basta considerar apenas modelos tradicionais baseados em causa e efeitos dos modos de falha, mas deve-se incorporar a interação entre as falhas o comportamento normal do sistema.

Sistemas dinâmicos podem ser classificados em sistemas contínuos no tempo e sistemas a eventos discretos (CASSANDRAS; LAFORTUNE, 2008). A Figura 4.10 traz uma representação esquemática da classificação de sistemas. Sistemas contínuos são aqueles normalmente representados por modelos de equações diferenciais que capturam o comportamento físico do sistema; enquanto sistemas a eventos discretos são representados por modelos que descrevem de forma lógica a transição entre os diferentes estados discretos dada a ocorrência de diferentes eventos. De forma simplificada, o estado de um sistema em um dado instante de tempo define como será seu comportamento naquele instante de uma forma que pode ser medida.

Cury (2001), define sistema a evento discreto como um sistema dinâmico que evolui de acordo com a ocorrência abrupta de eventos físicos, em intervalos de tempo em geral irregulares e desconhecidos. Além disso, o sistema permanece em um determinado estado até que o evento de transição ocorra, como apresentado na Figura 4.11. Como na análise de falhas e confiabilidade o interesse está apenas na ocorrência de um dado evento (como a transição de um estado sem falha para com falha, por exemplo), tratar os aspectos dinâmicos do sistema de forma discreta se mostra bastante adequada.

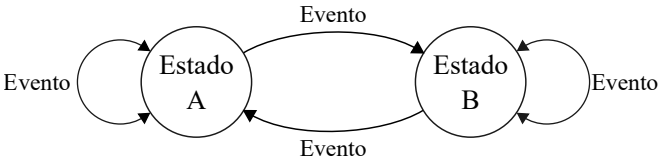
Um exemplo típico de sistema a evento discreto pode ser observado em um cruzamento entre ruas, cujo fluxo de carros é controlado por um semáforo (CASSANDRAS; LAFORTUNE, 2008; CURY, 2001), como o apresentado na Figura 4.12. No exemplo, os veículos deslocam-se em quatro direções distintas: de 1 para 2, de 1 para 3, de 2 para 3 e de 3 para 2. Os eventos que afetam o sistema são a chegada de veículos (para cada direção), a partida

Figura 4.10 – Classificação de sistemas



Fonte: Cassandras e Lafortune (2008)

Figura 4.11 – Representação de um sistema a evento discreto

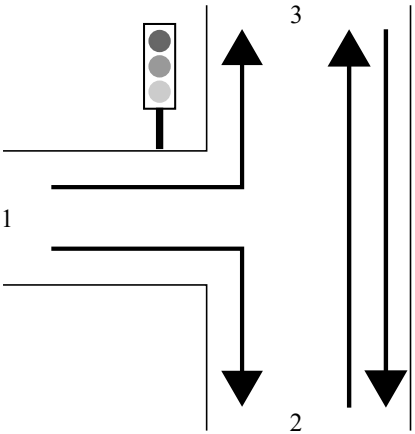


Fonte: Cassandras e Lafortune (2008)

de veículos (para cada direção), o sinal tornar-se verde e o sinal tornar-se vermelho. No projeto de sistemas discretos como este, diferentes técnicas são utilizadas para modelar o comportamento (entre as mais comuns estão

autômatos e redes de Petri) para assegurar que a combinação indesejada de eventos não ocorra, tal como o sinal ficar verde simultaneamente para dois carros que podem colidir.

Figura 4.12 – Exemplo de sistema a evento discreto



Fonte: Cassandras e Lafortune (2008)

Para modelar sistemas discretos é importante avaliar se o comportamento é determinístico ou aleatório (estocástico). No primeiro caso, dada uma variável de entrada para um tempo t, o estado do sistema neste tempo *t* pode ser calculado. Já para sistemas estocásticos, o estado dos sistema é aleatório, podendo-se obter apenas uma distribuição que define a probabilidade do sistema encontrar-se em um dado estado.

As transições de estado causadas pelas falhas podem ser modeladas utilizando métodos de análise de falhas, porém as transições de estados causadas pela operação normal do sistema (ligar ou desligar um componente) devem ser modeladas utilizando técnicas específicas para então serem incorporadas aos modelos das falhas.

Apesar das falhas e as mudanças operacionais de estado ocorrerem continuamente no tempo, o interesse maior é nos estados dos componentes (com falha ou não, ligado ou não). Por essa razão é interessante modelar as transições de estados como sistema a eventos discretos. Entre os vários métodos que podem ser usados no métodos proposto, estão:

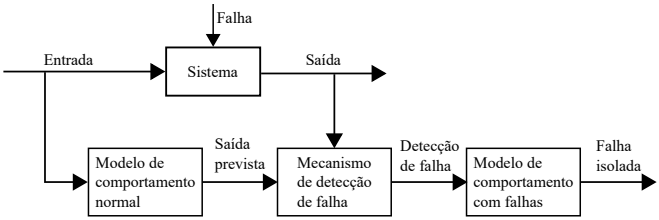
- Rede de petri (CASSANDRAS; LAFORTUNE, 2008);
- Cadeias de Markov (BARBU; LIMNIOS, 2008; CASSANDRAS; LAFORTUNE, 2008);

- Máquina de estados finitos (ANDERSON, 2006; CASSANDRAS; LAFORTUNE, 2008).

Os modelos comportamentais podem ser usados para representar não só os eventos relacionados a operação dos sistemas discretos como representar outros eventos que podem ocorrer, tal como as falhas. No trabalho de Zaytoon e Lafortune (2013), cujo foco são métodos de diagnóstico em sistemas a eventos discretos, as falhas são tratadas como causas de desvios não desejados, de um sistema ou seus componentes, em relação ao seu comportamento normal ou esperado.

A Figura 4.13 apresenta uma configuração clássica para o diagnóstico de falhas utilizada por Zaytoon e Lafortune (2013). Porém, os autores buscam apenas a detecção de falhas por alterações no comportamento do sistema e a detecção de qual componente é responsável por tal alteração, sem a intenção de obter um modelo que permita prever quando uma falha ocorre, além de não incorporar conceitos de análise de falha, visando a identificação de modos de falha e suas causas. Por outro lado, é possível perceber que a utilização de modelos comportamentais comuns à análise de sistemas a eventos discretos é bastante aderente a análise de falhas, uma vez que sejam combinados com modelos de causa-efeito tradicionalmente usados na análise de confiabilidade, como árvores de falhas, por exemplo.

Figura 4.13 – Configuração clássica para diagnóstico de falhas



Fonte: Zaytoon e Lafortune (2013)

Simeu-Abazi et al. (2010) citam três divisões para técnicas de diagnóstico de falhas em sistemas dinâmicos:

- Métodos de detecção e isolamento de falhas: requerem modelos analíticos de processos físicos, permitindo a comparação entre medições e os modelos de predição.
- Sistemas especialistas: utiliza o conhecimento de especialistas e uma máquina de inferência para o diagnóstico.
- Sistemas a eventos discretos: descreve o sistema em estados e descrevem sua evolução pelas transições de estado.

O método desenvolvido por Simeu-Abazi et al. (2010) utiliza autômatos para modelar o comportamento do sistema como a eventos discretos. A abordagem dos autores é a de diagnóstico baseado em modelo, na qual as entradas e saídas do sistema sob supervisão são monitoradas para detectar as falhas e isolar a fonte da falha. Porém, o modelo desenvolvido não considera reparos ou a ocorrência com atraso das falhas.

Pode-se ainda encontrar alguns trabalhos que utilizam redes de Petri para analisar a confiabilidade de sistemas. Kleyner e Volovoi (2010) utilizaram redes de Petri estocásticas para calcular a disponibilidade de sistemas crítico de segurança sob demanda, aplicado especificamente em controladores eletrônicos de airbags automotivos. Sadou e Demmou (2009), por sua vez, utilizam redes de Petri para derivar cenários que podem levar o sistema a uma situação crítica, aplicando o modelo desenvolvido na análise de sistemas embarcados, sob o argumento que árvores de falha não são suficientes para a análise de sistemas dinâmicos, pois para estes sistemas o tempo e outros eventos devem ser considerados.

Por fim, Kmenta e Ishii (1998) propuseram o uso de modelos comportamentais para simular o comportamento dinâmico da operação de sistemas e auxiliar a identificação de modos de falha associados a interação entre os sistemas de controle e sistemas físicos, nas etapas iniciais de projeto. Segundo os autores, listar em detalhes os modos de falha de um sistema é uma etapa crucial do desenvolvimento da análise de confiabilidade. Para isso, o trabalho desenvolvido utiliza modelos comportamentais para relacionar o comportamento desejado com componentes, ambiente operacional, sistemas relacionados e lógica de controle; além de simulação qualitativa do comportamento para fornecer uma estrutura de identificação de modos de falha e seus efeitos.

4.4 CONSIDERAÇÕES SOBRE CONFIABILIDE E RISCO NO CONTEXTO DAS FALHAS OCULTAS

A confiabilidade, mantenabilidade e o risco de sistemas são disciplinas relacionadas ao estudo de falhas, buscando prever sua ocorrência, identificar formas de evitá-las e mitigar as consequências de sua ocorrência. Essas disciplinas são abordadas separadamente, apesar de terem forte relação e definirem como o sistema se comporta e interage com pessoas e meio ambiente.

De fato, Kristiansen (2013) afirma que as análises de confiabilidade, mantenabilidade, disponibilidade e risco são desenvolvidas em sistemas com o objetivo de mantê-los disponíveis (por exemplo, pela redução da probabilidade de falha) e de minimizar os efeitos das falhas.

4.4.1 Confiabilidade

A qualidade dos resultados obtidos na análise de confiabilidade é dependente da capacidade do analista em caracterizar as falhas nos sistemas técnicos, tanto pelos eventos que levam à sua ocorrência quanto a sua quantificação por meio de probabilidades.

Segundo Dias (1996), a confiabilidade é a capacidade de um item desempenhar uma função requerida sob condições especificadas, durante um dado intervalo de tempo.

Billinton e Allan (1992), definem a confiabilidade como "a probabilidade de um sistema desempenhar seu propósito adequadamente por um período desejado, dentro das condições de operação encontradas". Essa definição separa a confiabilidade em quatro partes:

- Probabilidade: é a chance de que um sistema cumpra suas funções até um dado tempo. No caso do tanque coletor de um avião, a probabilidade define a chance de ter um número mínimo de válvulas operando até o final do ciclo de vida do tanque.
- Desempenho adequado: estabelece os critérios que definem o cumprimento das funções dos sistemas. Para o tanque coletor é a capacidade de manter um volume mínimo de combustível para subrir as demandas do motor.
- Tempo: é o instante que se deseja saber se o sistemas estará operando. No caso do tanque coletor, o interesse está em saber se as falhas ocorrem antes do final do ciclo de vida do tanque.
- Condições de operação: define quão severas são as demandas sobre o sistemas. Quanto mais severas as condições, maior a chance de um sistema falhar em um dado instante de tempo. Quanto mais severas forem as manobras do avião (quantidade maior de voos invertidos, por exemplo) maior será a chance de não haver combustível suficiente no tanque coletor para a execução de manobras invertidas.

A forma clássica de se avaliar a confiabilidade de sistemas utiliza diagramas de blocos de confiabilidade (RBD - *Reliability block diadrams*), que estabelece os arranjos entre componentes. Rebello et al. (2018) consideram a técnica mais universal utilizada na análise de confiabilidade.

Sakurada (2013) ressaltou que é possível verificar que esta abordagem clássica da confiabilidade não é suficiente para representar os cenários de falha e modelar os sistemas. Rebello et al. (2018) afirmam que esses métodos

tradicionais são inadequados para a modelagem dos sistema complexos e compostos por múltiplos subsistemas e componentes, encontrados nos setores de engenharia atuais.

Geralmente os incidentes resultantes das falhas em sistemas ocorrem pela combinação de vários eventos. A abordagem clássica não considera a ordem de ocorrência dos eventos, além da intervenção humana, por meio de procedimentos de manutenção ou mudanças na operação do sistema (emergência, por exemplo). Por essa razão, existem trabalhos sobre confiabilidade dinâmica, na qual os aspectos dinâmicos do sistema (ligar e desligar, manutenção etc.) são incorporados aos modelos.

Sakurada (2013), por exemplo, desenvolveu uma metodologia para a análise de confiabilidade dinâmica baseada no uso do método de Monte Carlos para a obtenção de amostras de tempos de falha para a confiabilidade, de acordo com aspectos dinâmicos como a comutação de componentes e a possibilidade de recuperar o sistema por meio de ações de manutenção.

O método de Monte Carlo (BILLINTON; ALLAN, 1992; ZIO, 2013) é um método de simulação numérica que tem como base a utilização de variáveis aleatórias. Dispondo de uma série de simulações pode-se obter uma distribuição de probabilidades que representa satisfatoriamente o comportamento do sistema.

Wang et al. (2018), por exemplo, utiliza o método de Monte Carlo para obter amostras de cenários de ataques cibernéticos em sistemas de usinas nucleares. Com isso, os autores buscaram testar a vulnerabilidade do sistema para diferentes magnitudes de ataques e sob diferentes comportamentos (quanto às capacidades adaptativas e de resposta dos atacantes). Essas variações são obtidas a partir de amostras aleatórias utilizando o método.

Em outro trabalho, Gascard e Simeu-Abazi (2018) utilizam o método de Monte Carlo na análise quantitativa de árvores de falhas dinâmicas, a partir da obtenção de amostras para os tempos de falhas, que então propagam desde as causas raiz até o evento de topo. Segundo os autores a utilização do método de Monte Carlo permite a utilização de qualquer distribuição de probabilidade para os tempos de falha. Além disso, o método permite obter as probabilidades tanto para o evento de topo como para os eventos intermediários.

Voltando ao contexto de confiabilidade dinâmica, Amin et al. (2018) desenvolveu uma técnica de análise de disponibilidade dinâmica, baseado em redes bayesianas dinâmicas. A técnica tem o propósito de representar a relação complexa entre causas de falhas e identificar as causas que tornam um sistema potencialmente vulnerável, reduzindo os tempos de parada. O trabalho tem aplicação em um sistema de alarme de incêndio e na análise de cenários de perigos em um sistema de geração de vapor.

Por fim, Rebello et al. (2018) apresentam uma metodologia para a

análise de confiabilidade funcional de sistemas que permite relacionar os estados de degradação dos componentes com os estados funcionais do sistema utilizando redes bayesianas dinâmicas. O monitoramento em tempo real de indicadores das funções e das condições dos componentes atualizam a rede.

4.4.2 Risco

A análise e gerenciamento de risco consiste em avaliar as consequências da ocorrência de diferentes eventos combinados dentro da operação de um sistema complexo que resultam em mudanças de estado, visando identificar seus impactos para a o homem, o meio ambiente, a organização etc. Calil (2009) define riscos em relação a dois aspectos: segurança e continuidade. Neste trabalho o interesse está nos riscos relacionados a segurança.

A segurança está relacionada com as consequências que a perda da função pode ter sobre o homem, o meio ambiente ou sobre o próprio sistema técnico (DIAS et al., 2011). Guimarães (2003) define segurança como a "capacidade 'de uma entidade evitar a ocorrência, dentro de condições pré-estabelecidas, de eventos críticos para o seu funcionamento ou catastróficos para seus operadores e meio ambiente.

Desta forma, a análise de risco busca estabelecer medidas para evitar a ocorrência de cenários com consequências severas por meio da identificação e definição de barreiras. A confiabilidade faz parte da análise de risco por estabelecer a probabilidade de um sistema falhar (estado indesejado) e permitir avaliar as consequências das falhas.

O risco pode ser definido a partir de cinco parâmetros: a probabilidade de um cenário, o resultado de sua ocorrência, a significância ou utilidade, o cenário causal e a população afetada. Estas definição está representada na equação 1.1.

Segundo Kumamoto e Henley (1996), pessoas diferentes podem definir diferentes resultados para a ocorrência de um evento, pois é impossível prever tais resultados com exatidão. Segundo os autores, é por esta razão que muitos criticam a premissa básica da análise probabilística do risco (PRA - *probabilistic risk assessment*), pois não se sabe ao certo a viabilidade de enumerar todos os resultados possíveis para novas tecnologias e novas situações. Árvores de falha, por exemplo, são comumente usadas para enumerar falhas e cenários, entretanto diferentes PRAs podem gerar diferentes árvores de falha para o mesmo sistema.

Os autores citam como exemplo a análise da ruptura de um vaso de pressão devido a pressão excessiva. A ruptura por defeito do tanque sob pressão nominal, implosão devido a pressão baixa e sabotagem são ignoradas.

Diferentes técnicas podem ser empregadas na análise de sistemas complexos e, dependendo das hipóteses assumidas e dos modelos utilizados para representar o comportamento dos sistemas, a análise pode resultar em diferentes cenários de falha.

Por essa razão, pode-se verificar a importância do uso de simulação para que os diversos eventos possíveis possam ser combinados e os cenários de falhas possam ser corretamente identificados para dar continuidade a análise de risco. Para isso, diferentes modelos devem ser usados para que a simulação englobe o máximo de informações relevantes para a caracterização dos cenários de falha, tornando o modelo resultante mais próximo do comportamento real do sistema.

Jia et al. (2016) abordam as falhas ocultas na avaliação de riscos de eventos em cascata. Os autores citam algumas ferramentas existentes para a análise de falhas em cascata, chamando atenção para o fato que esse tipo de falha está normalmente relacionados a falhas em sistemas de proteção.

Neste contexto, a caracterização das falhas ocultas exerce um papel importante pois a ocorrência não é percebida de forma imediata. Com isso, este tipo de falha é difícil de prever, dado que sua ocorrência não tem impacto imediato para a operação do sistema. Assim, em dadas condições, pode haver o acúmulo de eventos indesejados do sistema e consequente comprometimento das barreiras estabelecidas para evitar a ocorrência dos cenários com potencial de risco e ou então para conter as consequências.

Desta forma, além da caracterização detalhada dos cenários de falha que caracterizam as falhas ocultas, para que seja possível desenvolver modelos de confiabilidade para a obtenção das probabilidades de ocorrência, deve-se levar consideração as características operacionais do sistema, por meio de modelos específicos.

4.5 CONSIDERAÇÕES FINAIS

Neste capítulo foram apresentados alguns aspectos importantes para o detalhamento das falhas ocultas. Conforme apresentado, este tipo de falha tem a característica principal de não exercer influência sobre o comportamento do sistema imediatamente após sua ocorrência.

Para que as falhas ocultas sejam percebidas é necessário que outro evento ocorra, seja este evento um comando para ligar um componente ou uma falha em outro componente, por exemplo. Por esta razão, estas falhas demonstram-se críticas por ter consequências sobre a operação do sistemas apenas a partir da combinação de eventos, podendo comprometer os procedimento estabelecidos para operação e manutenção do sistema; ou então causar

um comportamento não previsto que resulta em maior tempo para retornar o sistema ao seu estado normal de operação.

A partir das referências estudadas, é possível perceber que tradicionalmente as falhas ocultas são tratadas no contexto da manutenção centrada em confiabilidade (MCC), por meio da otimização da peridiocidade de inspeção. Porém, também é possível perceber que esta abordagem tem o foco em subsistema e componentes de proteção (sensores, válvulas de segurança etc.) ou redundantes. Além disso, os métodos existentes não diferenciam os modos de falhas dos componentes e subsistemas analisados, que dependendo do tipo e dos estados dos componentes podem ou não ser ocultos.

Para exemplificar os conceitos apresentados sobre as falhas ocultas foi utilizado um problema clássico utilizado na análise da confiabilidade dinâmica. Este exemplo é um problema bastante simples que permite o fácil entendimento dos conceitos apresentados. Além disso, este exemplo será utilizado ao longo do desenvolvimento deste trabalho, dada sua simplicidade e a possibilidade de inserir mais funções de forma controlada que aumentam sua complexidade, tal como a possibilidade do controlador atuar periodicamente, alterando os estados das bombas.

Por fim foram apresentados alguns conceitos relativos ao detalhamento do comportamento operacional do sistema. Entende-se que dependendo das características operacionais do sistema, a falha de um componente pode ou não ser oculto, dependendo da combinação de estados operacionais dos componentes. Os sistemas serão tratados como a eventos discretos dirigidos a eventos (falha ou demanda operacional). As referências demonstram que métodos utilizados para representar este tipo de sistema é bastante aderente à análise de falhas, sendo usados em alguns casos na análise de confiabilidade. No Capítulo 5 será apresentada a proposta de tese e uma proposta dos passos a serem seguidos para o desenvolvimento do modelo proposto.

5 PROPOSTA PARA A ANÁLISE DE FALHAS OCULTAS

O presente trabalho apresenta uma proposta de solução para a análise de sistemas sujeitos a falhas ocultas, permitindo identificar cenários de combinação de eventos que expõem sistemas complexos ao risco de acidentes.

A caracterização dos cenários de risco depende da identificação dos eventos que podem deflagrar condições de perigo e a identificação das situações em que esses eventos ocorrem. Quando os sistemas estão sujeitos a falhas ocultas, a identificação desses cenários é dificultada, pois muitas vezes o analista nunca presenciou determinadas situações ao longo do ciclo de vida do sistema.

No projeto de sistemas essa dificuldade em identificar cenários é ainda maior, pois depende de muita abstração e da capacidade de prever combinações diversas de eventos.

Além de identificar os cenários, é necessário quantificar as probabilidades de ocorrência. Muitos dos eventos que deflagram condições de risco são falhas ou consequências de sua ocorrência. Para quantificar as probabilidade de ocorrências de falhas, utiliza-se métodos de análise de confiabilidade.

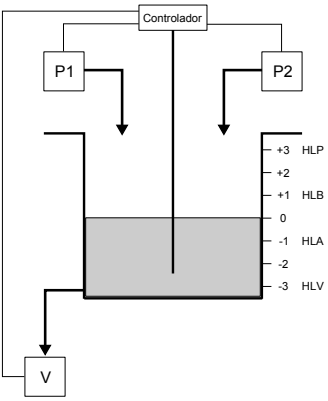
A abordagem tradicional da confiabilidade consiste em estabelecer os arranjos em série e paralelo dos subsistemas e componentes, obtendo-se os diagramas de blocos para o cálculo da confiabilidade do sistema, desconsiderando suas características dinâmicas. Esta abordagem não leva em consideração as condições de operação quando a falha ocorre, que pode ou não levar a falha completa do sistema.

Para exemplificar as etapas do método apresentado neste capítulo, será utilizado o problema de referência (Figura 5.1) dos trabalhos de Sakurada (2013), Marseguerra e Zio (1996), Marseguerra et al. (1998), Codetta-Raiteri e Bobbio (2006), apresentado previamente no Capítulo 4.

Neste exemplo, a confiabilidade é analisada dinamicamente, ou seja, considerando as transições do sistema, como a comutação de componentes e a capacidade de recuperar a operação do sistema em caso de falhas. Este problema contém poucos componentes e o funcionamento é simples, mas possui características dinâmicas bastante claras, tornando um bom exemplo para explicar os conceitos que envolvem o método proposto. Além disso, apesar de ser baseado em um caso real, consiste em um sistema teórico, criado para ser didático e para permitir a comparação de resultados de diferentes métodos de análise de confiabilidade dinâmica.

Além deste exemplo clássico, outros exemplos serão utilizados para explicar os conceitos, baseados em sistemas e problemas de análise encontrados no cotidiano, facilitando o entendimento do leitor. Entre estes exemplos

Figura 5.1 – Exemplo para falha oculta



Fonte: Sakurada (2013)

estão automóveis e o problema de evacuação de ambientes com aglomeração de pessoas.

É possível perceber que principalmente para sistemas complexos produzidos em pequena escala (as vezes em montagens específicas), em muitos casos o sistema a ser projetado é desenvolvido a partir de uma customização de um sistema existente.

Usinas de geração de energia ou alguns sistemas embarcados em navios e aeronaves, por exemplo, são adaptados para serem utilizados em um contexto de operação um pouco diferente, mas o princípio construtivo e os componentes envolvidos são os mesmos.

Metodologias de projeto são desenvolvidas para serem aplicadas no projeto de sistemas inovadores e a inovação dificulta ainda mais a análise aprofundada da falha no contexto dos cenários descritos na Figura 4.4. No caso de produtos inovadores, a dificuldade se dá pela escassez de informações relativas às falhas. Além de conhecer quais os modos de falhas, é necessário a coletas de dados de falha para que possa ser realizada uma análise quantitativa das falhas, visando prever suas ocorrências.

Quando possível pode-se coletar dados de falhas, além da coleta de dados de campo, utilizando técnicas como ensaios acelerados; ou como no presente trabalho, utilizando métodos matemáticos como o de Monte Carlo para obter amostras grandes de dados a partir de poucos dados iniciais.

Por essa razão, entende-se ser importante propor um método que possa ser utilizado inclusive na fase de projeto conceitual. O método pode ser utilizado tanto para sistema existentes, sendo utilizado com certo grau de certeza sobre os dados de falha, quanto para atualizações de um sistema

existente, quando se leva em consideração modelos que permitam estabelecer as diferenças entre o sistema a ser projetado e o existente.

As referências, conforme apresentado no Capítulo 4, indicaram que as falhas ocultas são abordadas com foco na otimização dos tempos de inspeção. Entretanto, há um consenso quanto a dificuldade em analisar as falhas ocultas devido a indisponibilidade de informações. Além disso, é possível perceber que os diferentes modos de falha dos componentes sujeitos a falhas ocultas não são tratados de forma distinta, apesar de ser facilmente constatável que diferentes modos de falhas podem ter diferentes efeitos sobre o sistemas, podendo ser ou não ocultos. Por essa razão, é evidente a importância de relacionar os estados operacionais dos sistemas com a ocorrência dos modos de falha para caracterizar as falhas ocultas.

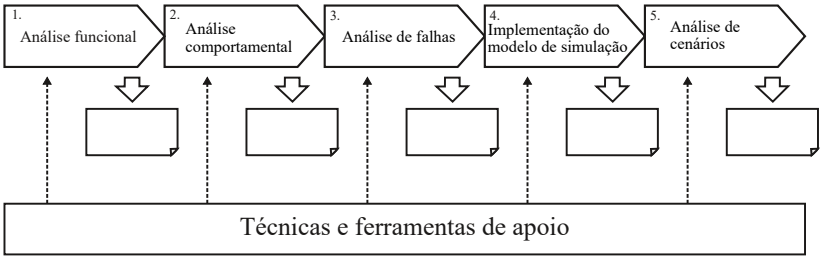
Para melhor tratar o problema, estruturou-se um método para integrar ações, técnicas e ferramentas para tratar a falha oculta, a partir da fase de projeto conceitual. Nesta fase de projeto da metodologia de referência PRODIP, os princípios de solução para o cumprimento das funções do sistema começam a ser definidos, permitindo dar início a análise das falhas ocultas potenciais. Pode-se, por exemplo, comparar os princípios de solução quanto aos cenários de ocorrência de falhas ocultas e consequente exposição do sistema ao risco.

O método de análise desenvolvido consiste nas seguintes etapas (Figura 5.2):

- **Análise funcional**: consiste em identificar as funções e componentes do sistema visando estabelecer variáveis de controle que definem as falhas do sistema.
- **Análise comportamental**: consiste em identificar as transições operacionais do sistema, visando identificar quando os componentes são demandados ao longo do tempo e de que forma essas transições afetam a variável de controle.
- **Análise de falhas**: consiste em identificar como os componentes falham e quais as consequências dessas falhas sobre a variável de controle.
- **Implementação do modelo de simulação**: consiste em desenvolver os modelos de simulação, permitindo combinar os elementos que compõem os cenários de risco.
- **Análise de cenários**: consiste em testar diferentes casos, tanto alterando componentes quanto características de operação do sistema, visando identificar a exposição do sistema as condições de perigo.

As etapas de aplicação do método são descritas por atividades a serem desenvolvidas, visando complementar as informações de saída. Para isso, as

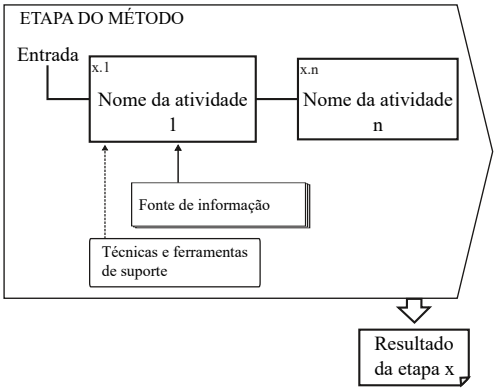
Figura 5.2 – Método proposto para caracterização e análise de cenários de falhas ocultas



etapas contam com entradas relacionadas ao objeto de estudo. Para o problema de referência, por exemplo, a entrada seria o reservatório e o conjunto de informações disponíveis sobre ele, como informações de projeto, descrição do componentes, dados de falha, informações sobre a operação, etc.

A Figura 5.3 exemplifica os elementos dos diagramas utilizados para a descrição das etapas do métodos proposto.

Figura 5.3 – Descrição dos diagramas de representação das etapas do método proposto



As atividades a serem desenvolvidas em cada etapa são numeradas de forma sequencial, como exemplificado na Figura 5.3. Vale ressaltar que a representação sequencial não significa que a saída de uma atividade é entrada da atividades seguinte. A representação significa que ao longo das atividades, as informações e modelos de saída da etapa são complementadas.

Cada atividade requer informações de variadas fontes, como documentação sobre o sistema técnico, diagramas, informações de especialistas etc. Nos diagramas, as fontes de informações estão ligadas as atividades por linhas

contínuas.

Além de informações, a execução das atividades necessitam de técnicas de suporte para auxiliar na organização das informações e desenvolvimento dos modelos de saída das etapas do modelo. Essas técnicas e ferramentas estão representadas abaixo das atividades e conectadas por linhas tracejadas.

Na descrição das etapas do método proposto são apresentadas as técnicas e as fontes de informação recomendadas. Vale ressaltar que por se tratar de um método geral, aplicável para a análise dos mais diversos tipos de sistemas, essas recomendações nem sempre são aplicáveis, como pode ser constatado na análise apresentada no Capítulo 6. Em alguns casos, já existem informações disponíveis sobre o sistema que tornam desnecessário aplicar uma técnica específica em uma dada etapa do método.

A utilização do método no contexto de desenvolvimento de produto se dá pela adaptação dos resultados das etapas do método proposto para os diferentes princípios de solução a partir da fase de projeto conceitual. Considerando o problema de referência, por exemplo, as funções dos componentes são as mesmas, mas pode-se optar por diferentes modelos de bombas e válvulas, resultando em modos de falha e taxas de falhas diferentes. Desta forma, o comportamento das variáveis de controle mudam, bem como o detalhamento das falhas.

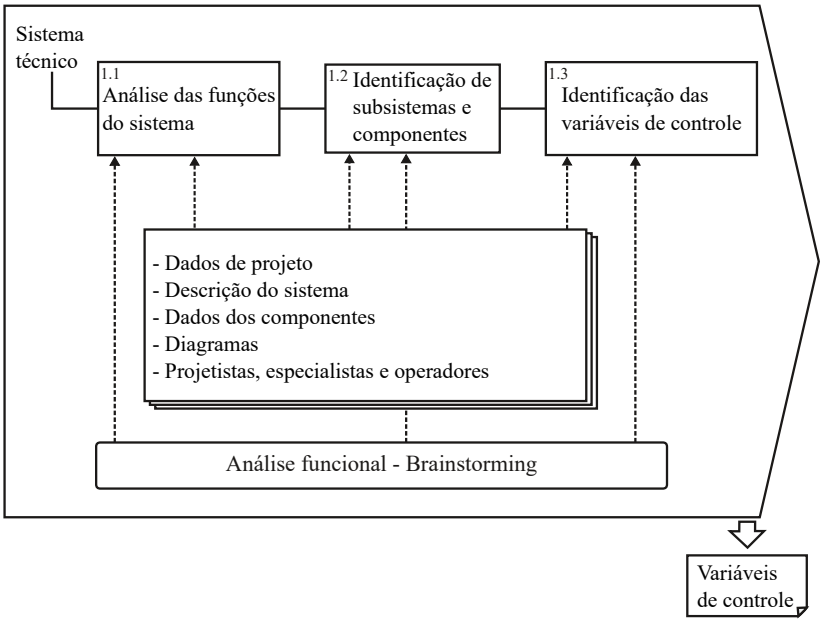
Além disso, o método pode ser utilizado ao longo do processo de projeto por permitir a alteração de alguns parâmetros de projeto como taxas de falhas, vazões, número de componentes, a partir dos modelos já desenvolvidos. Com isso, pode-se avaliar os cenários de falhas ocultas e identificar possíveis alterações de projeto mais otimizadas.

5.1 ANÁLISE FUNCIONAL

A primeira etapa para a análise consiste na caracterização das funções dos sistemas. Conforme pode ser observado na Figura 5.4, esta etapa consiste em analisar as funções, identificar os componentes e subsistemas (princípios de solução) responsáveis pelo cumprimento das funções e a identificação das variáveis de controle que definem se o sistema cumpre ou não as funções requeridas.

O desdobramento do sistema pelas funções auxilia a comunicação entre os envolvidos na análise e orientam a sua priorização de acordo com as funções essenciais do sistema.

Figura 5.4 – Etapa de análise funcional do método proposto



5.1.1 Atividade 1.1 - Análise das funções

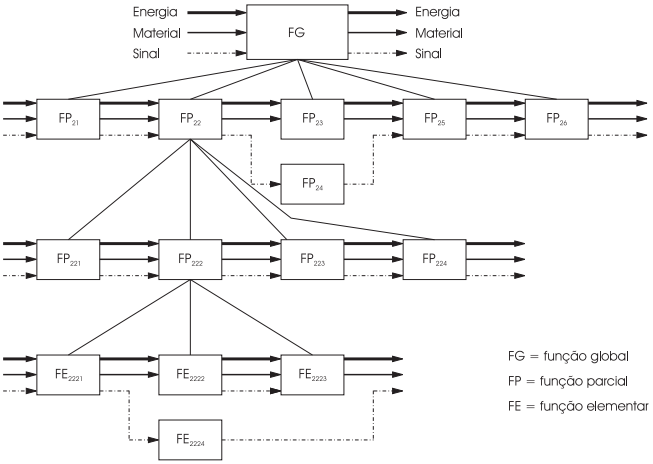
O relacionamento entre subsistemas e componentes pelas entradas e saídas de energia, material e sinal permite entender as consequências da falha de um dado subsistema (ou componente) sobre outro e sobre o sistema global. Com isso, pretende-se identificar falhas funcionais de subsistemas e componentes que possuem os mesmos efeitos sobre o sistema global.

A análise das funções é fundamental para o início do processo de análise de falha. A falha, em grande parte, é evidenciada por algum problema identificado no cumprimento das funções do sistema. Assim, uma vez bem definida a função, torna-se mais fácil caracterizar a falha.

A análise funcional de produto é uma técnica que permite identificar as funções e subfunções relativas ao sistema, subsistemas e componentes relacionando-as por meio do fluxo de energia, material e sinal, conforme apresentado na Figura 5.5.

Para o problema do reservatório, por exemplo, a utilização da análise funcional permite desdobrar as funções do sistema como apresentado na Figura 5.6. A função global do sistema é definida como “Manter o nível na

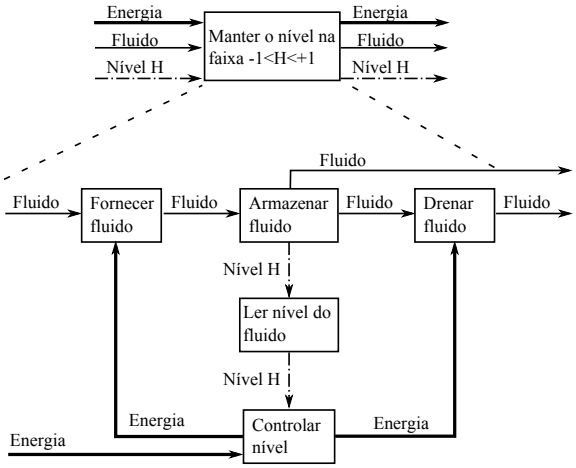
Figura 5.5 – Técnica de análise funcional de produtos



Fonte: Back et al. (2008)

faixa -1<H<+1". Essa função por sua vez é desdobrada em subfunções, como "Fornecer fluido", "Armazenar fluido", "Drenar fluido", etc.

Figura 5.6 – Análise funcional do problema de referência

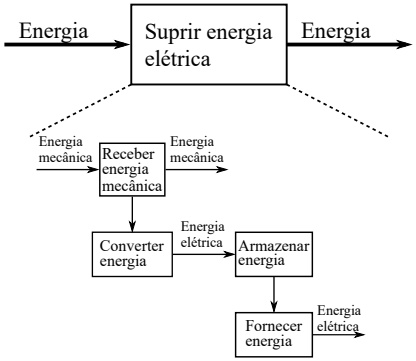


Fonte: Sakurada (2013)

Um outro exemplo simples para ilustrar a análise de funções é o sistema

elétrico de um carro. Pode-se definir a função global como “Suprir energia elétrica”. A função global pode ser desdobrada conforme a Figura 5.7, quando se considera apenas o suprimento de energia para os demais componentes do carro.

Figura 5.7 – Exemplo de funções de um sistema elétrico de um carro hipotético



5.1.2 Atividade 1.2 - Identificação de subsistemas e componentes

Uma vez identificadas as funções, os subsistemas e componentes responsáveis pelo cumprimento de cada subfunção podem ser identificados e, com isso, o relacionamento entre eles é evidenciado.

Esta atividade é bastante simples, porém dependendo da complexidade do sistema sendo analisado, a quantidade de componentes e o relacionamento com as funções pode ser trabalhosa.

A identificação dos subsistemas e componentes consiste em registrar as partes em que o sistema é estruturalmente desdobrado.

Um carro é composto por diversos subsistemas, como motriz, elétrico, transmissão, suspensão etc. Estes subsistemas, por sua vez, podem ser desdobrados em componentes.

Considerando-se novamente o sistema elétrico de um carro, as funções identificadas na análise das funções podem ser atribuídas a componentes específicos. A função do alternador é gerar energia elétrica, transformando a energia mecânica transmitida pelo motor em energia elétrica. Essa energia elétrica gerada carrega a bateria, que então alimenta os demais componentes do sistema.

As atividades 1.1 e 1.2 (Figura 5.4) podem ser executadas de diversas formas, dependendo do tipo de sistema que está sendo analisado e da disponibilidade de informações. O objetivo principal dessas atividades é levantar

algumas informações para auxiliar na determinação das variáveis de controle da atividade 1.3.

No caso de sistemas que estão sendo projetados, as funções e subfunções do sistema podem variar e a identificação dos subsistemas e componentes depende dos princípios de solução selecionados durante o projeto conceitual.

Se considerarmos, por exemplo, um sistema sendo projetado para a movimentação linear de uma carga. Dependendo das especificações de projeto, essa movimentação pode ser feita por atuadores elétricos, hidráulicos ou pneumáticos. Nesses casos, os fluxos de energia, material e sinal variam, assim como as variáveis de controle que estabelecem se a carga está sendo movimentada adequadamente, como velocidade e força aplicada.

Porém, independente do princípio de solução selecionada neste exemplo hipotético, estes princípios são amplamente utilizados para diversas aplicações, o que facilita a identificação das variáveis de controle. Com isso, as saídas das atividades 1.1 e 1.2 podem ser alcançadas de forma simplificada.

5.1.3 Atividade 1.3 - Identificação das variáveis de controle

As variáveis de controle definem como as funções do sistema estão sendo cumpridas. O monitoramento das variáveis de controle permite identificar quando o comportamento do sistema desvia do comportamento estabelecido em projeto. Como definido no Capítulo 4, as falhas resultam em comportamento fora do padrão aceitável.

No caso do problema de referência as funções do sistema estão identificadas na Figura 5.6. Com base na análise funcional é possível identificar que o cumprimento da função do sistema é definido pelo nível do reservatório. Dessa forma, este nível é a variável de controle de interesse para a modelagem das falhas ocultas.

As falhas ocultas, por sua vez, não resultam em variação imediata no desempenho do sistema. Ou seja, não causam variações perceptíveis sobre as variáveis que definem padrões de comportamento.

Para a identificação das variáveis de controle algumas questões devem ser respondidas:

- *Qual a função do sistema?*
- *Qual variável define o cumprimento da função do sistema?*
- *Quais as especificações de projeto para a variável de controle?*
- *Quais os componentes com influência sobre a variável de controle?*

- *Qual a relação entre os estados dos componentes e o comportamento da variável de controle?*

Voltando ao exemplo do sistema elétrico de um carro, a variável de controle que define o cumprimento das funções do sistema é a energia elétrica. O alternador gera a energia, a bateria armazena e os demais componentes consomem.

Considerando-se os estados dos componentes do sistema, é fácil entender a influência sobre a variável de controle. Uma vez que o carro está ligado, o alternador gera energia constantemente, contribuindo com o aumento da energia (variável de controle) disponível no sistema. Neste caso, a falha do componente resulta na falta de energia disponível no sistema, caso a energia armazenada na bateria acabe. No caso do alternador, os estados são "ligado" e "desligado", e as transições ocorrem pelo ligar e desligar do motor ou pela ocorrência de falhas. As falhas impedem que o componente seja acionado ou causam o desligamento do mesmo.

A bateria, por sua vez, é um elemento passivo. Este componente sempre está operando, pois ele carrega quando o alternador está operando e descarrega quando há algum componente do sistema elétrico demandando energia. Falhas na bateria significam que este componente é incapaz de reter a energia armazenada, descarregando mesmo quando não há componentes demandando energia.

Retornando ao problema de referência, com o nível do reservatório identificado como variável de controle, a partir da análise funcional da Figura 5.6, torna-se evidente a relação dos componentes e o nível do reservatório. A operação das bombas contribuem para o aumento do nível do reservatório e a válvula contribui com o esvaziamento do reservatório.

O controlador é um elemento passivo que apenas reage a variações do nível. Sua contribuição para o nível do reservatório não é direta, dependendo de como os componentes (bombas e válvula) reagem aos comandos do controlador de ligar e desligar.

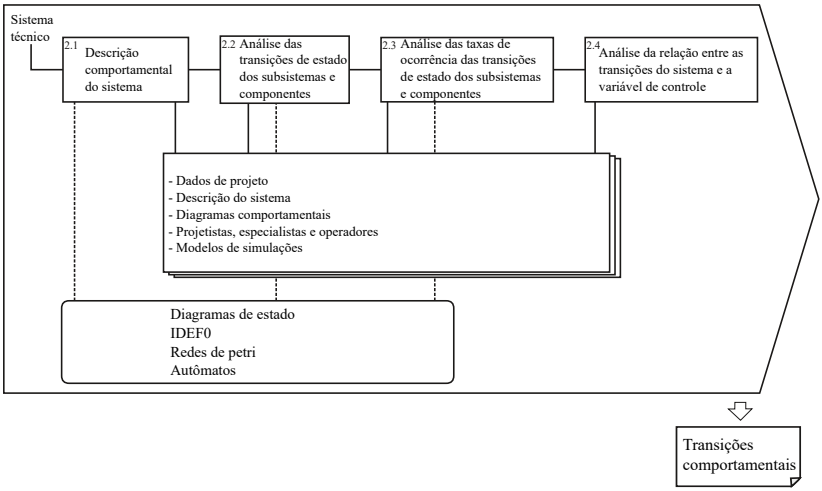
5.2 ANÁLISE COMPORTAMENTAL

As transições operacionais do sistema definem quando os componentes sofrem mudança de estado. O conhecimento sobre essas mudanças de estado, combinado com a existência ou não de falhas definirá se o sistema será capaz de cumprir com as demandas de transição da operação.

A etapa de análise comportamental da Figura 5.2 está detalhada na Figura 5.8 e visa o entendimento da operação do sistema, com o objetivo de modelar quais as transições de estado dos componentes que ocorrem apenas

pela operação normal do sistema, e não pela ocorrência de falhas.

Figura 5.8 – Etapa de análise comportamental do método proposto



Essa etapa é importante pois essas transições definem quando uma falha é potencialmente oculta. Para isso, é necessário:

- uma descrição comportamental do sistema (informal ou utilizando técnicas de representação);
- a análise das transições de estados dos componentes e subsistemas;
- a análise das taxas de transições de estados;
- e a análise da dependência entre as transições de estados e a variável de controle, com o objetivo de identificar como uma falha pode afetar o comportamento do componente e afetar a função global do sistema.

Vale ressaltar que quanto mais dinâmico for o sistema, com transições frequentes e em intervalos curtos de tempo, mais complexo é a análise de comportamento. Dependendo dos casos, é apropriado simplificar as considerações das transições de acordo com os objetivos da análise.

5.2.1 Atividade 2.1 - Descrição comportamental

A descrição comportamental pode ser feita por meio de textos ou utilizando técnicas de representação, como diagramas de estado, redes de Petri

e autômatos, por exemplo.

O tipo de técnica a ser utilizado depende das características do sistema. Se o sistema tiver um comportamento tal que seja essencial representar de forma contínua, será necessário formular equações que descrevem esse comportamento.

No caso do problema de referência (Figura 5.1) as transições são comandadas pelo controlador. Nesse caso, o controlador é um elemento passivo que apenas responde à variação de nível do reservatório, comandando a mudança de estado dos componentes (de ligado para desligado). A possibilidade de existência de falhas define se os componentes respondem ao comando do controlador e se o nível do reservatório será controlado.

A relação dos componentes com a variável de controle é simples. Quando as bombas estão ligadas há vazão para aumento do nível do reservatório e quando a válvula está aberta, há vazão para diminuição do nível. Como na condição normal de operação uma das bombas fica desligada, o nível se mantém constante.

5.2.2 Atividade 2.2 - Análise de transições

A análise das transições de estado dos componentes do sistema visa identificar sob que condições as transições ocorrem. As características de operação do sistema estabelecem quando e quais componentes sofrem transições de estado.

Ligar ou desligar um componente que tem influência sobre a variável de controle é importante para determinar se as funções estão sendo cumpridas.

No caso do sistema do problema de referência, em operação normal, os comandos do controlador sobre os componentes visa combinar os estados dos componentes de acordo com o Quadro 5.1. Quando o sistema encontra-se com o nível (H) em zero, o sistema está na condição normal de operação, com a bomba P1 ligada e a válvula V aberta. Com isso o nível permanece estável, e a bomba P2 permanece desligada.

Quadro 5.1 Comandos do controlador de acordo com o nível H

H	Bomba P1	Bomba P2	Válvula V
0	Ligado	Desligado	Ligado
-1	Ligado	Ligado	Desligado
+1	Desligado	Desligado	Ligado

Fonte: Sakurada (2013)

Quando o controlador detecta a redução do nível, a intenção é que ele

aumente o nível o mais rápido possível de volta a zero. Por isso, as duas bombas são ligadas e a válvula desligada. Uma vez que o nível atinge zero, as bombas e a válvula são comandadas a retornar aos estados originais. Nesse caso, a ocorrência ou não de falhas determina se o controlador é bem sucedido.

Já no caso do nível subir até +1, o controlador age de forma inversa, comandando o desligamento das bombas e a abertura da válvula. Da mesma forma, uma vez que o nível é retomado, os componentes são comandados a voltar para os estados originais.

Nesse caso especificamente, as transições de estado dos componentes podem ser representadas de forma discreta, pois no intervalo entre dois eventos (ligar e desligar de um componente, por exemplo) o comportamento da variável de controle é previsível e não precisa ser monitorado continuamente.

Se o sistema sob análise sofre um processo de desgaste que vai alterando continuamente o desempenho e cumprimento das funções, é necessário desenvolver modelos contínuos para que os resultados da simulação represente a realidade.

5.2.3 Atividade 2.3 - Análise das taxas de transições

As taxas de transições determinam quando os componentes do sistema são demandados. Essa informação é importante quando o comportamento do sistema for modelado, utilizando-se essas taxas para comandar as transições dos componentes do modelos durante a simulação.

O conhecimento sobre a frequência com que essas transições ocorrem também ajuda a determinar qual o nível de exigência sobre os componentes do sistema, já que dependendo da condição de operação, alguns componentes são demandados e outros não.

Se considerarmos sistemas com redundância ativa, por exemplo, todos os componentes redundantes atuam ao mesmo tempo. Já se a redundância for passiva, apenas o elemento ativo é demandado. Se, por outro lado, as características do sistema determinam que em dado intervalo de tempo seja feito a troca do componente passivo, a demanda é completamente diferente. Neste terceiro caso, por exemplo, torna-se mais fácil a detecção de falhas ocultas no elemento passivo.

As taxas de transição também ajudam a entender com que frequência o sistema opera sob condições mais severas.

Considerando-se a utilização de um carro. Dependendo das características do motorista ou da pista em que o carro circula, as demandas sobre o carro e o risco a que este está exposto podem variar. Com isso, a exigência estrutural sobre componentes como freio, pneus, além do consumo de combustível

podem variar.

No caso do problema de referência, as transições de estado ocorrem em função da variação do nível do reservatório. Ou seja, as transições ocorrem apenas em função da ocorrência de falhas em algum dos componentes que resulte na variação do nível. Dessa forma, a taxa de transição de estados é dependente da taxa de falhas.

5.2.4 Atividade 2.4 - Análise da relação entre transições e a variável de controle

Esta atividade da etapa de análise comportamental é a mais complexa dependendo do sistema em análise.

Se o sistema for composto por uma grande quantidade de componentes e subsistemas com relação complexa de interação entre eles, a identificação e representação dessas interações pode se tornar bastante difícil.

A Figura 5.9 apresenta um exemplo de representação do comportamento do sistema. Note-se que os estados operacionais identificados representam combinações de estados dos componente, que resultarão em comportamentos diferentes da variável de controle. Os eventos determinam quando as transições ocorrem, podendo ser por exemplo, o comando de um operador que liga ou desliga componentes, ou a ação de um controlador, por exemplo.

A representação das transições usando diagramas de estados, como a Figura 5.9 é recomendável por facilitar o entendimento para a implementação dos modelos de simulação. Em cada estado operacional, a variável de controle "X" (vazão, temperatura ou força, por exemplo) tem um comportamento específico.

Os estados operacionais são definidos pelas diferentes combinações dos estados dos componente do sistema. A Figura 5.10 traz um exemplo do desdobramento do "Estado operacional 1" da Figura 5.9 pelos estados operacionais dos componentes. Cada componente contribui com uma variação "Δx" na variável de controle "X", dependendo de seu estado operacional (ligado ou desligado, por exemplo). O somatório das contribuições de todos os componentes para a variação da variável de controle determina como essa variável "X" se comportará em um dado estado operacional do sistema.

No caso do problema do reservatório, a relação entre as transições e a variável de controle, é bastante simples. Por se tratar de um sistema com apenas três componentes e uma variável de controle, a modelagem é feita em função das vazões e dos estados dos componentes (Equação 5.1), ou seja, a variação do nível do reservatório é dependente de quais componentes estão contribuindo com a vazão de fluido e as vazões de cada componente.

Figura 5.9 – Exemplo de representação da transição de estados

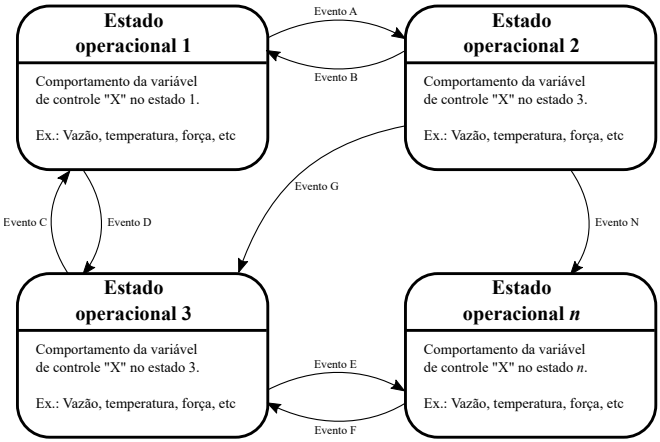
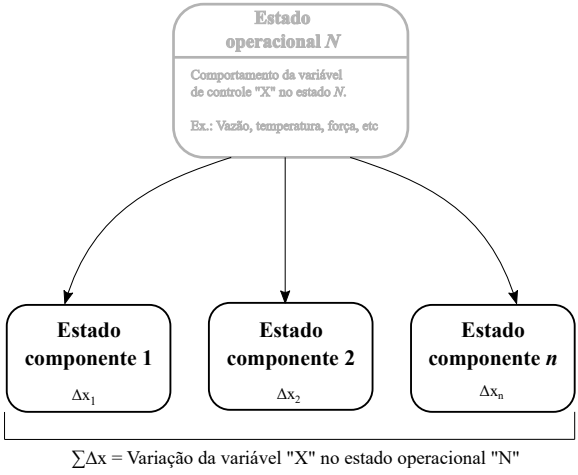


Figura 5.10 – Exemplo de representação de estados operacionais pelos estados dos componentes



$$\frac{\Delta H}{\Delta t} = E_{P_1} \cdot \dot{q}_{P_1} + E_{P_2} \cdot \dot{q}_V + E_V \cdot \dot{q}_V \tag{5.1}$$

sendo:
E_{P_1} = *Estado da bomba* P_1
$\dot{q}_{P_1}$ = *Vazão da válvula* P_1
E_{P_2} = *Estado da bomba* P_2

$\dot{q}_{P_2}$ = *Vazão da válvula* P_2
E_V = *Estado da válvula*
$\dot{q}_V$ = *Vazão da válvula V*

Os estados do sistema são definidos pelas combinações de estados do componentes apresentados no Quadro 5.1. Adotando-se valores 1 para o componente no estado "aberto" e 0 para estado "fechado", a equação de variação de nível representa claramente o comportamento do sistema em casa estado operacional, de acordo com as mudanças de estados dos componentes.

Vale ressaltar que nesta etapa busca-se analisar apenas a ocorrência dos eventos de transição operacional do sistema. Para o exemplo do reservatório, se considerarmos agora que o controlador é um elemento ativo que comanda com uma determinada frequência a mudança de estado das bombas (P1 desliga e P2 liga, por exemplo) as transições dos componentes passam a ocorrer por características da operação e não apenas como resposta às falhas. Esta etapa tem o objetivo de analisar essas transições de estado dos componentes para então ser modelada e combinada com o modelo de transição de estados causado por falhas de componentes, que será detalhada a seguir.

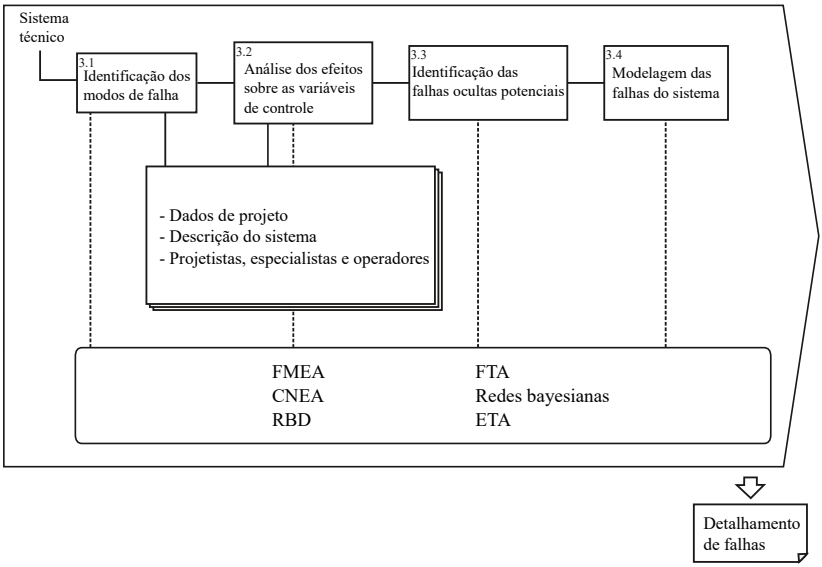
5.3 ANÁLISE DE FALHA

A etapa de análise de falhas (representada na Figura 5.11) tem o objetivo de identificar as cadeias causais das falhas permitindo, entre outras coisas, avaliar a consequência da falha de um dado componente ou subsistema sobre o comportamento dos demais, do sistema e da variável de controle.

Nesta etapa, o conhecimento sobre o sistema permite: identificar os modos de falha dos componentes e subsistemas; analisar as causas e efeitos; analisar quais causas estão relacionadas com variações na variável de controle; identificar quais falhas podem ser ocultas; identificar quais são os eventos que evidenciam as falhas ocultas (eventos-gatilho); e por fim identificar alguns cenários de falhas ocultas.

Para a execução das atividades desta etapa podem ser utilizadas técnicas para auxiliar a análise de falhas como FMEA (*failure modes and effect analysis*), CNEA (*causal network event analysis*), FTA (*fault tree analysis*), redes bayesianas, ETA (*event tree analysis*). O uso dessas técnicas permite formalizar o conhecimento acumulado para facilitar a implementação dos modelos de simulação do sistema.

Figura 5.11 – Etapa de análise de falhas do método proposto



5.3.1 Atividade 3.1 - Identificação dos modos de falha

Um modo de falha é definido como a maneira que o componente em estudo deixa de executar a sua função ou desobedece as especificações (SAKURADA, 2001). Analisando o sistema por uma abordagem funcional, o modo de falha consiste na não-função. Por exemplo, se a função de um dado sistema é exercer uma força, o modo de falha é a incapacidade de exercer tal força. Seguindo uma abordagem estrutural, o modo de falha está associado a aspectos físicos, tais como resistência mecânica, carregamento e dureza, que podem resultar em um modo de falha "rompimento".

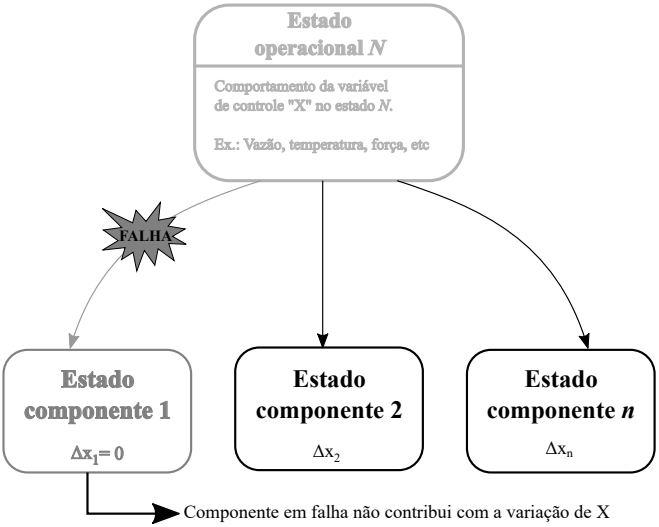
Os modos de falha podem ser definidos de forma determinística (falha ou não falha, por exemplo) ou considerando multiestados, quando há diferentes níveis de degradação. Esses níveis de degradação resultam em um dado componente operando parcialmente.

5.3.2 Atividade 3.2 - Análise dos efeitos sobre as variáveis de controle

Os efeitos dos modos de falha consistem em como os modos de falha podem ser percebidos, ou seja, quais as consequências da sua ocorrência para operação do sistema. Enquanto o modo de falha ocorre internamente

no sistema/componente, os efeitos são percebidos externamente (SAKURADA, 2001). A Figura 5.12 exemplifica a representação das consequências de uma falha dentro dos diagramas de estado.

Figura 5.12 – Exemplo de representação de estados operacionais pelos estados dos componentes



Neste caso, a falha do componente 1 anula sua influência sobre a variável de controle. Dessa forma, deve-se avaliar qual a consequência da falha para o cumprimento da função do sistema.

5.3.3 Atividade 3.3 - Identificação das falhas ocultas potenciais

É importante perceber que os efeitos dos modos de falha permitem definir se a falha é potencialmente oculta ou não. Os efeitos que um modo de falha pode ter sobre o sistema depende das condições de operação no instante que o modo de falha ocorreu.

Dependendo do sistema, é possível identificar *a priori* algumas falhas ocultas potenciais e os eventos gatilho que as evidenciam, ou que fazem com que as falhas ocultas passem a ter efeito sobre o sistema.

No caso de sistemas com redundância passiva, por exemplo, fica claro que o componente passivo é que está sujeito a falha oculta. A demanda que o elemento passivo entre em operação, seja pela operação normal ou falha do componente ativo, é o evento gatilho que converte a falha oculta em evidente.

Um outro exemplo com falha oculta potencial fácil de ser identificada

são sistemas com sensores. As ações de controle do sistema, sejam automáticos ou pela intervenção de operadores, se dá a partir das informações que os sensores fornecem. O problema é que as falhas não são identificáveis sem que haja uma espécie de contra prova. Um exemplo desse tipo de falha ocorreu no acidente de Three Mile Island (KUMAMOTO; HENLEY, 1996).

Considerando-se o problema de referência. Os modos de falha identificados para sistema são componente "falha ligado" e "falha desligado". Os efeitos que estes modos de falha tem sobre o sistema dependem diretamente do estado operacional do sistema. Em condição normal de operação, uma falha ligada da bomba P1 não altera imediatamente o nível do reservatório, ou seja, não há um efeito imediato perceptível sobre o sistema. Porém, se a mesma bomba falha desligada, não há fluido sendo bombeado para dentro do reservatório e este começa a drenar.

5.3.4 Atividade 3.4 - Modelagem das falhas do sistema

Uma vez que os modos de falha são identificados, é preciso fazer o levantamento das taxas de falhas. A questão do levantamento das taxas de falhas normalmente traz complicações devido a indisponibilidade de dados. É possível encontrar bancos de dados de falha de sistemas com aplicações específicas como SINTEF (2002), voltado para sistemas *offshore*, mas a utilização nem sempre é viável por terem sido obtidas a partir de condições de operação específicas.

A definição de confiabilidade estabelece claramente que a análise tem relação com as condições de operação. Esse problema é ainda maior na análise durante o projeto. Quando se considera o projeto como a combinação de componentes já existentes para uma finalidade específica, basear os valores de taxas de falhas em componentes utilizados em outros sistemas semelhantes é uma saída bastante viável. Mesmo sem representar completamente a realidade, essa saída permite testar diferentes concepções para o projeto e estimar qual a melhor solução.

No problema de referência, por exemplo, pode-se basear as taxas de falhas das bombas e da válvula em componentes semelhantes, utilizados em sistemas de bombeamento de água com outras aplicações. Além disso, pode-se variar as taxas de falha e verificar quais valores são mais apropriados para a operação do sistema. Entretanto, para esse caso, as taxas de falha são conhecidas (Tabela 5.1).

Para modelar as falhas do sistema, estas são consideradas determinísticas, "sem falha" e "com falha". As taxas de falha são conhecidas e então pode-se determinar o comportamento do sistema nas diferentes ocorrências

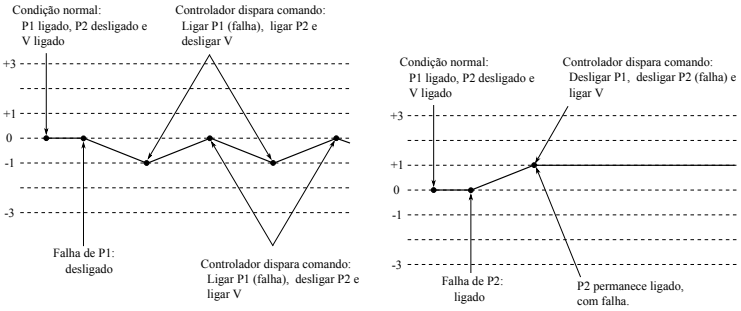
Tabela 5.1 Taxas de falhas do problema de referência

Componente	Taxa de falha (falhas/hora)
Bomba P1	0,004566
Bomba P2	0,005714
Válvula V	0,003125

Fonte: Sakurada (2013)

de falhas. Alguns exemplos de falhas e seus efeitos estão apresentados na Figura 5.13.

Figura 5.13 – Modos de falha do problema de referência e os efeitos sobre o sistema



(a) Falha em P1l (b) Falha em P2

5.4 IMPLEMENTAÇÃO DO MODELO DE SIMULAÇÃO

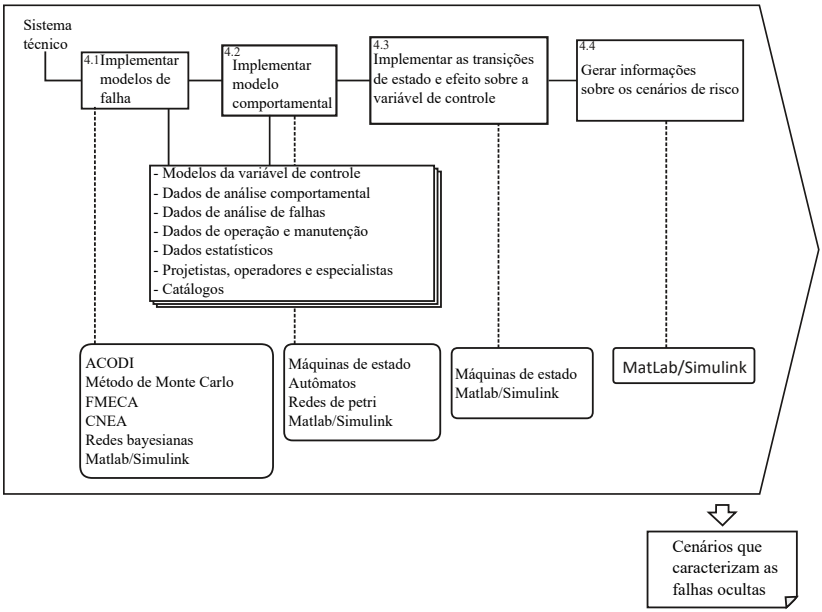
Com a execução das análises funcional, comportamental e de falha, as informações necessárias para a implementação dos modelos e simulação dos cenários estão definidas. As atividades de implementação do modelo de análise estão apresentadas na Figura 5.14.

5.4.1 Atividade 4.1 - Implementar modelos de falha

O método desenvolvido baseia-se na obtenção de amostras para os diversos eventos que definem estados de operação do sistema.

Entre estes eventos estão as ocorrências de falhas dos diversos subsiste-

Figura 5.14 – Etapa de implementação do modelos de análise do método proposto



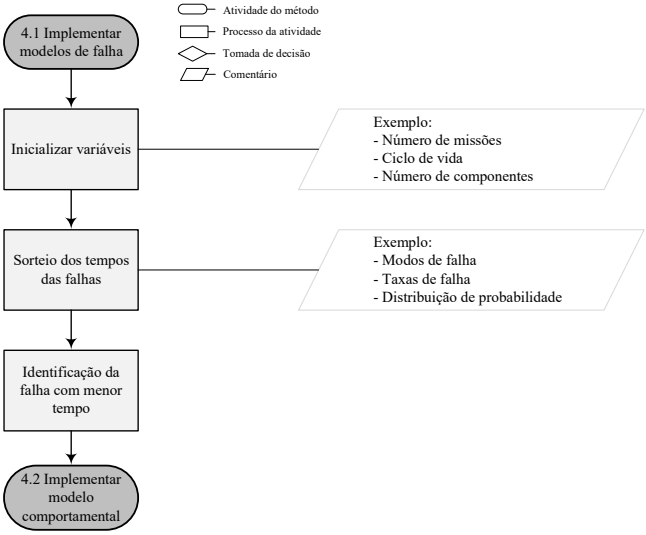
mas e componentes que compõem o sistema. A Figura 5.15 traz os processos envolvidos nesta atividade.

O primeiro passo para a implementação do método obviamente consiste em estabelecer os dados de entrada que definem as condições de operação do sistema. Entre essas informações, podem-se citar como exemplo:

- número de missões que o sistema executa, que define os ciclos de iterações do modelos;
- ciclo de vida do sistema, que define quais os tempos de falha são relevantes e quando as simulações podem parar;
- qual o número de componentes, que permite verificar por exemplo qual o comportamento do sistema alterando o número de elementos redundantes; e
- quais as especificações do sistema para a variável de controle, que determinam sucesso ou falha de uma missão.

A partir dos modos de falhas identificados na etapa anterior do método, as taxas de falha de cada modo de falha e a definição das distribuições de

Figura 5.15 – Atividade de implementação dos modelos de falhas



probabilidade mais aderentes à representação dos componentes, parte-se para a implementação do sorteio dos tempos de falha.

A distribuição exponencial é uma das distribuições mais utilizadas para modelar falhas em sistemas, sendo apropriada quando a falha ocorre de forma aleatória, ou seja, quando a ocorrência de um dado evento é independente dos eventos ocorridos no passado. Essa falta de memória da distribuição exponencial a torna apropriada para representar modelos marvokianos, em que o comportamento futuro está condicionado apenas ao estado presente, desconsiderando o tempo de permanência neste estado.

Entretanto, na modelagem de sistemas em que se considera níveis de degradação, as falhas, além de ser aleatórias, passam a depender das ocorrências dos diferentes níveis de degradação do sistema. Nesses casos, deve-se buscar uma distribuição mais apropriada para representar a ocorrência de tais eventos. No caso de eventos raros, uma distribuição apropriada seria a distribuição de Poisson.

O sorteio dos tempos de falha é o início da aplicação do método de Monte Carlo. A simulação de Monte Carlo é uma boa estratégia quando não há muita informação sobre as falhas e transições de estado na operação do sistema que permita relacionar as ocorrências de falhas de um componente com variações de comportamento do sistema. As probabilidades condicionais que relacionam esses eventos exemplificam o tipo de informação necessária para realizar a análise.

Considerando a variável aleatória tempo de falha $T \in [0, \infty]$ exponencial, dado que a função probabilidade acumulada de falhas $F_T(t)$ e a função densidade de probabilidade $f_T(t)$ são representadas por:

$$F_T(t) = 1 - e^{-\lambda t}; f_T(t) = \lambda e^{-\lambda t} \tag{5.2}$$

sendo λ a taxa de falha de um dado componente. A confiabilidade $R_T(t)$ é dada por:

$$R_T(t) = e^{-\lambda t} \tag{5.3}$$

Atribuindo-se um valor aleatório sorteado para a confiabilidade $R \sim [0,1]$, obtém-se uma amostra para o tempo de falha de um dado componente:

$$t = -\frac{1}{\lambda} log(1 - R) \tag{5.4}$$

Obtendo-se tempos de falha para todos os componentes e verificando suas consequências para a operação do sistema ao longo do ciclo e vida, obtém-se uma amostra de um sistema que cumpriu este ciclo. Repetindo este processo para até que seja obtido uma amostra grande de casos, pode-se avaliar com certo grau de certeza as probabilidades de ocorrência de acidentes.

Normalmente, os dados existentes são taxas de falhas isoladas de componentes e taxas de transição de estado operacional do sistema. A partir desses dados é viável aplicar o método de Monte Carlo e obter amostras de tempos de ocorrência dos vários eventos que descrevem o comportamento do sistema.

Um mesmo componente pode ter mais de um modo de falha. No caso do problema de referência, os componentes podem falhar ligado ou desligado. O sorteio dos tempos é realizado para ambos os modos de falhas. Aquele modo de falha cujo tempo sorteado foi menor será o modo de falha considerado para o componente nas simulações. A partir da combinação das falhas como comportamento, o modelo começa a tomar forma.

5.4.2 Atividade 4.2 - Implementar modelo comportamental

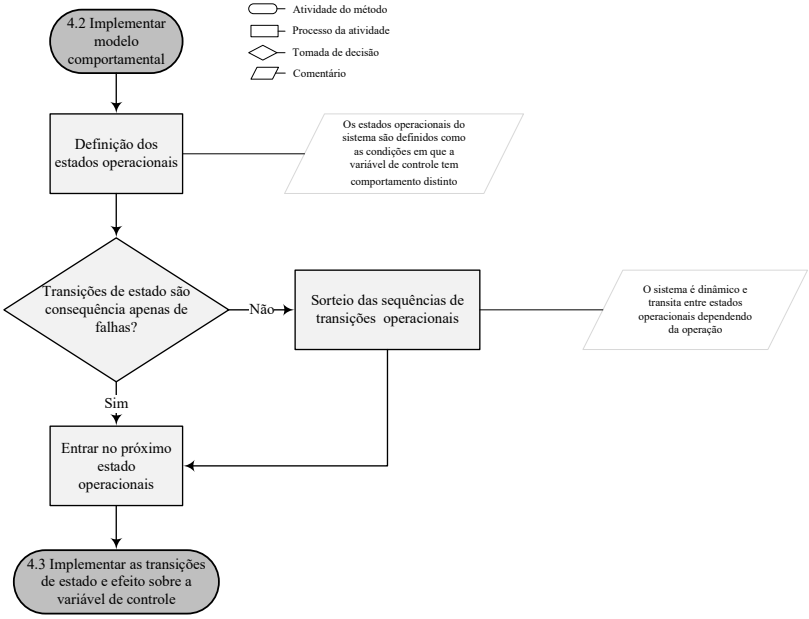
A atividade de implementar o modelo comportamental é a mais delicada do método proposto. Os modelos comportamentais dependem da abordagem dada aos sistemas. Conforme apresentado no Capítulo 4, os sistemas podem ser, por exemplo, discretos ou contínuos.

No caso das análise de falhas ocultas, não é necessário representar o comportamento continuamente. Basta conhecer os estados operacionais do

sistema, definidos pela combinação de estados dos componentes do sistema e saber por quanto tempo o sistema permanece em um estado operacional para então calcular qual o efeito sobre a variável de controle.

A Figura 5.16 apresenta em detalhes os passos para a implementação dos modelos comportamentais.

Figura 5.16 – Atividade de implementação dos modelos comportamentais



A identificação dos estados operacionais depende de como o analista interpreta o problema. É importante deixar claro que os estados operacionais são definidos de acordo com as diferentes condições que podem afetar a variável de controle e que de alguma forma tem relação com a ocorrência de falhas. Por exemplo, para determinar os estados operacionais é importante considerar os estados dos componentes e a capacidade dos componentes entrarem nesses estados pela existência ou não de falhas.

Essas condições podem ser por exemplo, um sistema que opera em condição normal (em que o consumo de um fluido é normal) e condição de emergência (quando o consumo é reduzido). A transição entre estes estados operacionais pode ser simulado para representar diferentes situações em que eles ocorrem, sendo ainda afetados por eventuais falhas.

Se considerarmos novamente o problema de referência da Figura 5.1,

os estados operacionais podem ser definidos como a combinação dos estados dos componentes. Nesse caso específico, as transições não ocorrem periodicamente como característica da operação. Os estados operacionais são característica da ocorrência de falhas e das demandas do controlador para impedir as falhas por transbordamento e esvaziamento. As transições de estados operacionais, por exemplo, P1 ligada, P2 desligada e V ligada para P1 ligada, P2 ligada e V desligada ocorre apenas como comando do controlador a partir de variações pra baixo da variável de controle "Nível H".

A capacidade do sistema entrar nos estados operacionais depende da existência ou não de falhas. Ou seja, pode-se comandar que o sistema entre em um dado estado operacional, baseado na combinação de estados dos componentes, mas a existência de falhas não permite que os componentes responsam ao comando. Nesses casos, identificam-se mais estados operacionais definidos pela existência ou não de falhas.

Quando a transição de estados é definida pela operação normal do sistema, pode-se obter amostras aleatórias baseadas em taxas de transição para simular o comportamento do sistema em diferentes cenários.

Considerando novamente o problema de referência, mas dessa vez adicionando a hipótese do controlador inverter a bomba redundante periodicamente, ou seja, transitar periodicamente entre P1 ligada e P2 desligada, para P2 desligada e P1 ligada. Nesse caso, não há alteração no comportamento da variável de controle (nível do reservatório), mas é importante para modelar comportamento e falhas. Nesse caso, vale definir essas combinações de bombas como estados distintos.

Uma vez que os tempos dos estados operacionais são definidos, tem-se a sequencias das transições e pode-se avaliar como o sistema opera conforme a transição entre estes estados e a ocorrência das falhas.

5.4.3 Atividade 4.3 - Implementar as transições de estado e efeito sobre a variável de controle

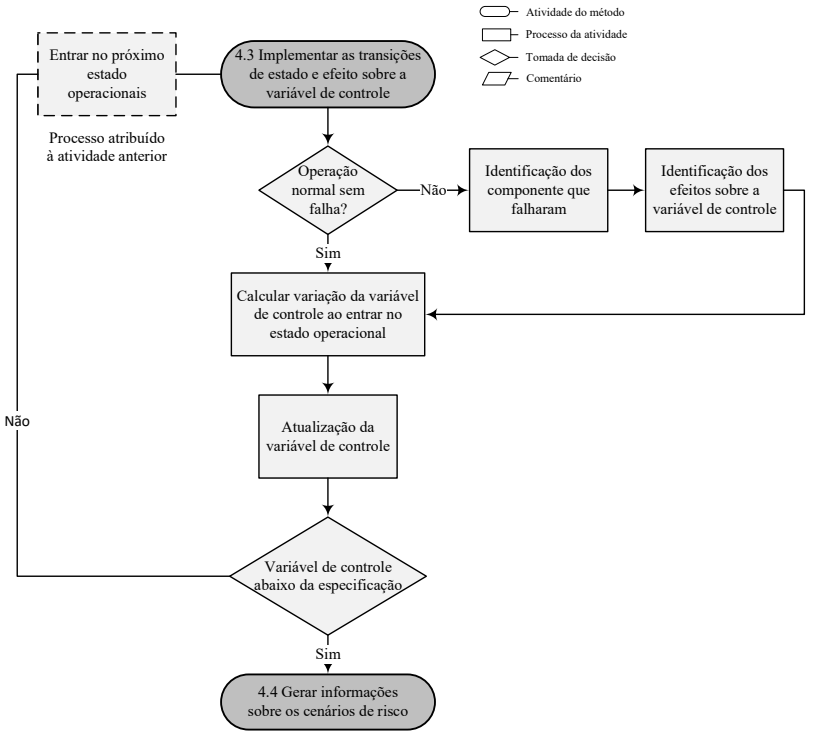
Ao analisar qualquer sistema, é fácil perceber alguma relação entre o comportamento esperado, definido pelos estados operacionais e a ocorrência de falhas. A norma MIL-STD-721C, traz claramente esta relação na sua definição de falha, como o evento, ou estado inoperante, no qual um item ou parte dele não apresenta, ou não poderia apresentar, o desempenho previamente especificado (USA/DOD, 1981).

Conforme a definição, as falhas impedem que o sistema se comporte conforme o esperado ao entrar em um dado estado operacional. Por essa razão, é essencial relacionar os estados operacionais modelados na atividade anterior

com a ocorrência de falhas.

A Figura 5.17 apresenta em detalhes os passos para a implementação da combinação de falhas e comportamento.

Figura 5.17 – Atividade de implementação das transições de estado e efeito sobre a variável de controle



A relação entre o comportamento do sistema e as falhas pode ser feita de diferentes formas, dependendo do tipo de sistema que se está analisando. Em alguns sistemas, por exemplo, a ocorrência de falhas não impede que o sistema entre em um dado estado operacional. Porém a falha afeta como a variável de controle se comporta, dada a entrada do sistema em um estado operacional.

Se considerarmos uma sala que deve ter a temperatura controlada por um conjunto de equipamentos de ar condicionado (redundantes). A falha de um dos equipamentos não impede o controle da temperatura, mas afeta a velocidade que o ambiente atinge a temperatura desejada. Uma vez que há a

demanda para baixar a temperatura os aparelhos sem falha serão ligados e a temperatura abaixará, mas com um gradiente menor.

Em outros sistemas a falha impede que o sistema entre no estado operacional desejado. No caso do problema de referência, por exemplo, a ocorrência de falhas em uma das bombas ou na válvula pode causar alteração na variável de controle (bomba P1 falha desligada, por exemplo) ou impedir que o sistema entre em um estado operacional. Se ocorre uma falha desligada em P2 (nesse caso uma falha oculta), esta falha impede que o sistema entre no estado P1 ligado, P2 ligado e V desligada, em caso do nível do reservatório baixar. O Quadro 5.2 apresenta os estados operacionais que relacionam os estados dos componentes do problema de referência.

Quadro 5.2 Estados operacionais do problema de referência

Estados	**P1**	**P2**	**V**
Estado 1	Ligado	Desligado	Desligado
Estado 2	Ligado	Ligado	Desligado
Estado 3	Ligado	Desligado	Ligado
Estado 4	Ligado	Ligado	Ligado
Estado 5	Desligado	Desligado	Desligado
Estado 6	Desligado	Ligado	Desligado
Estado 7	Desligado	Desligado	Ligado
Estado 8	Desligado	Ligado	Ligado

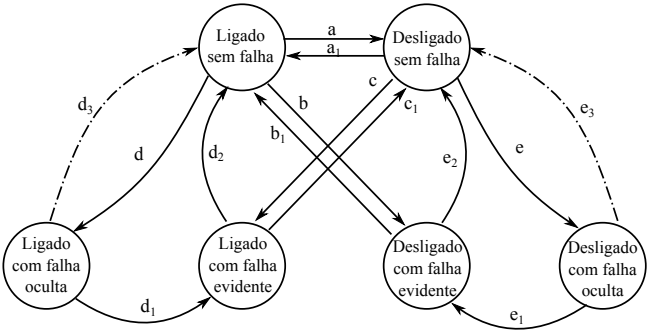
As transições ocorrem a partir do monitoramento da variável de controle “Nível H” e pela ocorrência de falhas. Nesse caso, o relacionamento do comportamento e das falhas é feito diretamente na definição do estados operacionais.

A Figura 5.18 representa as transições de estados dos componentes quando se considera as condições funcionais “com falha”, “sem falha”, “ligado”e “desligado”. Neste exemplo é possível diferenciar as transições de estados devido a ocorrência de falhas e devido a demandas operacionais do sistema (no caso do controlador detectar variação no nível H). Em condições normais de operação (sem falha), o componente pode estar nos estados “ligado sem falha” ou “desligado sem falha” e a transição ocorre pelos eventos gatilho de comando do controlador representados por “a” e “a_1”. Transições como “d” e “d_3” são causados por falha e manutenção, respectivamente.

Com os modelos que simulam as ocorrências das transições entre os estados operacionais do sistema, têm-se as relações entre as transições de estados dos componentes puramente pela operação normal e as ocorrências de falhas.

A partir dessa combinação, pode-se verificar como a variável de con-

Figura 5.18 – Transições de estado dos componentes do problema de referência



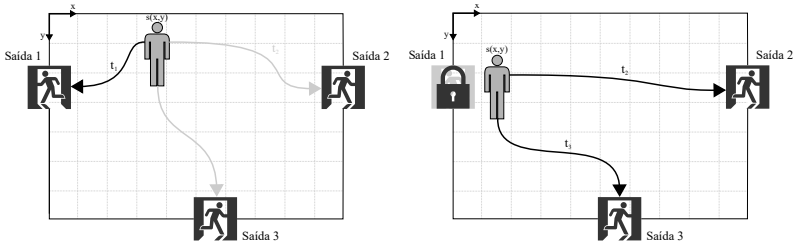
Fonte: Sakurada (2013)

trole se comporta quando o sistema entra em cada estado operacional. Conhecendo-se o tempo que o sistema permaneceu em cada estado, verifica-se qual a condição da variável de controle.

No problema de referência, por exemplo, verifica-se o tempo que o sistema permaneceu em um dado estado de operação que combina os estados de P1, P2 e V, para calcular qual o nível que o fluido atingiu (se transbordou ou se esvaziou). Entre outras coisas, este tempo define, por exemplo, quanto tempo a equipe de manutenção teria para recuperar um componente com falha e permitir que o sistema retorne ao seu estado normal de operação (P1 ligada, P2 desligada e V ligada).

O métodos apresentado pode ser utilizado em diferentes aplicações além do projeto de sistemas. Se considerarmos a análise de um espaço com aglomeração de pessoas, o método pode ser aplicado com a finalidade de verificar a eficiência das saídas de emergência, por exemplo (Figura 5.19).

Figura 5.19 – Exemplo de análise de saídas de emergência



(a) Representação do estado inicial (b) Representação do estado com falha

A Figura 5.19a representa a decisão de uma pessoa dentro do ambiente

sob condição de perigo (como o incêndio dentro do espaço) e as opções que podem ser tomadas para a evacuação. Pelo modelo de desencadeamento de incidente apresentado na Figura 1.2 do Capítulo 1, as saídas de emergências são portas corta fogo e atuam como barreiras de contingência do incidente.

O ambiente pode ser mapeado e a posição de uma pessoa *s(x,y)* pode ser sorteado aleatoriamente. As normas estabelecem a velocidade considerada para o dimensionamento das saídas e, com isso, pode-se definir quanto tempo a pessoa leva para chegar em cada uma das saídas a partir da posição inicial.

Sorteando-se aleatoriamente a escolha por uma das saídas, levando em consideração diferentes pesos de acordo com a posição da pessoa (tendência de sair pela porta mais próxima) e a probabilidade maior de sair pela saída 3 por ser também a entrada, pode-se obter o comportamento das pessoas para o caso da evacuação.

Os estados comportamentais são definidos pela escolha sorteada da pessoa sair pela saída 1, 2 ou 3. Cada estado significa uma velocidade (ou tempo) específico para a evacuação, dependente da posição inicial da pessoa. A combinação das falhas com o comportamento está na detecção da ocorrência de uma falha ao chegar em uma saída e constatar que a porta está com falha (no caso da Figura 5.19b, representada pelo cadeado). Nesse caso, o efeito sobre a variável de controle é o tempo maior pela necessidade de escolher uma saída alternativa à escolha inicial e o novo deslocamento necessário.

Pode-se então verificar a consequência de falhas nas barreiras de contingência dos cenários de risco, como representado na Figura 5.19b. Nesse caso, uma pessoa desloca-se normalmente para a saída 1, dado sua proximidade dessa saída. Entretanto, ao chegar na saída e tentar abri-la, percebe-se que a porta está fechada. Esse caso representa o exemplo de uma falha oculta e não há informação de que a porta está fechada até que alguém tente abri-la. Nesse caso, a capacidade de evacuação está comprometida, pois as pessoas que se deslocaram até a saída 1 e evidenciam a falha da porta, devem tomar uma nova decisão e se deslocar para as saídas 2 ou 3. Assim, a variável de controle "tempo de evacuação" apresenta um resultado pior.

Com o modelo do sistema em mãos, o analista pode então partir para a etapa de análise de cenários, alterando concepções construtivas do sistema (alterando componentes a partir dos requisitos dos clientes e de requisitos de projeto) ou características operacionais para identificar e verificar a ocorrência de diferentes cenários de risco envolvendo falhas ocultas.

5.5 ANÁLISE DE CENÁRIOS

Esta etapa do método consiste em testar variações sobre o sistema e verificar como este se comporta em relação à ocorrência de falhas e dos cenários de combinação de eventos que expõe o sistema ao risco.

Desta forma, pode-se testar diferentes concepções de projeto e ter uma estimativa do comportamento futuro do sistema sendo projetado.

No caso do problema de referência, pode-se verificar o comportamento alterando-se as vazões dos componentes. Como demonstrado na Equação 5.1, as vazões afetam a velocidade que o nível do reservatório varia. Aumentado as vazões, por exemplo, se os cenários de falha resultarem no aumento do nível, a velocidade será maior e a equipe de manutenção terá um tempo menor para retornar o sistema à condição inicial.

Se a válvula for substituída por duas válvulas com a metade da vazão da válvula original, por exemplo, a falha de uma dessas válvulas terá um efeito claramente diferente sobre o sistema, já que o nível do reservatório subirá de forma mais lenta.

Outra questão que pode ser facilmente testada é a alteração no comportamento do controlador, estabelecendo que este alterne periodicamente a bomba ativa e passiva. Com isso a detecção das falhas ocultas será maior, tendo em vista que ocorrerá a demanda da bomba passiva, por exemplo, que é o evento gatilho para esta detecção. Além disso, haverá um comportamento bastante distinto para o sistema, pois com as falhas, os componentes podem não responder corretamente à esse aumentos de frequência nas demandas de transição de estados.

Se considerarmos o exemplo da evacuação, pode-se verificar como o sistema se comporta em caso de alteração no número, tamanho e posição das portas. O número e tamanho de portas em um ambiente com aglomeração de pessoas é definido por norma. Simulando diferentes casos com a variação dessas características das saídas de emergência pode-se verificar a efetividade das normas.

Pode-se ainda, inserir um fator de atraso na tomada de decisão, também baseado em valores aleatórios para representar a redução da capacidade cognitiva das pessoas e consequência atraso na tomada de decisão que compromete a velocidade de evacuação. Isso permite aproximar ainda mais os modelos ao comportamento de um caso real.

Ao final da implementação, o método deve gerar informações que permitam analisar os cenários de risco. Entre essas informações estão gráfico que permitam comparar as transições de estados operacionais e as variações nas variáveis de controle. Outra informação pertinente são os tempos de falha e sequências de transições sorteadas aleatoriamente, permitindo replicar e

analisar em detalhes os casos em que houve falha na missão.

5.6 CONSIDERAÇÕES FINAIS

O presente capítulo apresentou os passos para a aplicação do método desenvolvido para a análise de cenários que envolvem falhas ocultas, desde a fase de projeto conceitual de sistemas.

As etapas iniciais do método consistem basicamente em levantar e organizar informações que servem de base para a implementação dos modelos de simulação.

A análise das funções, por exemplo, é uma etapa bastante comum em processos de projeto. A grande questão é que para a implementação é necessário conhecer em detalhes quais são e como se comportam as variáveis de controle.

Da mesma forma, modelos comportamentais e de falha são amplamente difundidos no projeto e análise de sistemas. O modelos comportamentais são usados, por exemplo, no projeto de sistemas de controle por meio de técnicas como redes de Petri, autômatos, entre outras.

Modelos de falhas também são bastante difundidos, porém normalmente não englobam as características dinâmicas do sistema. Técnicas como FMEA e FTA são bastante utilizadas na caracterização de falhas, mas a identificação das influências da operação sobre o comportamento do sistema após a ocorrência de falhas é complexa e depende bastante do grau de experiência do analista.

O método proposto utiliza o método de Monte Carlo para implementar os modelos de falha e comportamento. A ideia é gerar amostras dos diferentes eventos (falhas e transições operacionais) e verificar como o sistema se comporta. Com isso, obtém-se uma grande quantidade de cenários aleatórios, que muitas vezes não são enxergados a priori pelos analistas.

Por fim, esse métodos de análise permite ainda testar variações de projeto e estimar o comportamento futuro dos sistemas em projeto. Dessa forma, é uma ferramente bastante útil para auxiliar na análise de tomada de decisão durante o projeto.

No Capítulo 6 será apresentada a aplicação do método aqui detalhado na análise de falhas do tanque coletor de um avião de combate. Como descrito previamente, este sistema é composto por componentes redundante cujas falhas são ocultas. A partir da análise do sistema pode-se aferir quão exposto ao risco o avião pode se encontrar ao longo de suas missões.

6 APLICAÇÃO NO TANQUE COLETOR DE AVIÃO

O Capítulo 2 apresentou uma breve discussão sobre as características dos sistemas de combustível de aeronaves, visando o contexto de aplicação desta tese.

As aeronaves são sistemas complexos compostos por subsistemas e componentes que funcionam de forma combinada para o cumprimento da função global, que é voar de acordo com perfis de voo exigidos pela missão.

As características operacionais de aeronaves militares são bastante distintas das aeronaves comerciais. Entre as diferenças estão os tipos de manobras que a militar é capaz de executar. Apesar de normas exigirem que as aeronaves comerciais sejam capazes de voar sob gravidade negativa por curtos períodos de tempo, como requisito de segurança, elas não executam este tipo de manobra durante a operação normal.

As aeronaves de combate, por sua vez, executam este tipo de manobra frequentemente por se tratar de um recurso essencial para a superioridade em combate contra aeronaves inimigas. Para viabilizar este tipo de manobra, os aviões de combate contam com tanques coletores capazes de reter combustível na região onde este é bombeado para o motor.

O problema de tese surgiu como demanda de engenheiros da *Saab Aeronautics* no desenvolvimento do programa de colaboração entre o Brasil e Suécia a partir de 2014, desde a compra de aeronaves *Gripen NG* pela Força Aérea Brasileira. Este programa de cooperação entre os dois países viabilizou a realização de um período sanduíche e a interação com engenheiros da Saab.

Os aviões de caça Gripen contam com apenas um motor e por esta razão, há uma grande preocupação quanto ao funcionamento do sistema de combustível da aeronave. A falta de combustível durante voos invertidos, por menor que seja a duração, pode apagar o motor, sendo sua partida durante o voo inviável. Obviamente, por se tratar de um avião com apenas um motor, esta falha causa a sua queda.

O tanque coletor, em especial, segue o conceito apresentado no Capítulo 2 em que válvulas de retenção são utilizadas na divisão das duas câmaras do tanque, visando assegurar que combustível suficiente fique retido na região onde se encontra a bomba de combustível da aeronave. Obviamente, a falta de combustível resulta na parada do motor, mas além disso, pouco combustível no tanque pode resultar na sucção de vapor de combustível que pode resultar em cavitação nas bombas.

Uma questão de grande importância nos sistemas de combustível é a preocupação quanto a contaminação. A presença de água ou outros contaminantes pode trazer sérios riscos ao funcionamento do sistema de propulsão. Por

essa razão, os tanques não passam por manutenção ao longo do ciclo de vida, e este conta com um conjunto de válvulas redundantes visando asseguram o seu funcionamento até que seja trocado.

No início de cada missão, considera-se que a aeronave foi abastecida completamente. Ao longo da missão, o volume de combustível é dependente da vazão de combustível bombeado pela bomba do tanque coletor e consumido pelo motor.

O consumo de combustível do motor, por sua vez, é dependente do tipo de manobra executada pela aeronave. No caso de voo com *afterburner*, por exemplo, o consumo de combustível é máximo.

Afterburner ocorre quando há a necessidade de mais força do motor para executar alguma manobra específica. Para isso, mais combustível é injetado próximo da saída da turbina, havendo uma segunda queima de combustível que resulta em mais empuxo do motor. Por consequência dessa injeção extra de combustível, o consumo é maior.

O processo de aplicação da análise é bastante complexo devido a confidencialidade dos dados relativos a aeronave. Por se tratar de aeronave militar, os detalhes construtivos do sistema não podem ser compartilhados. Para compensar essa limitação de informação, durante as interações com os engenheiros da empresa, foram estabelecidos alguns dados aproximados sobre o sistema que, segundo os próprios engenheiros, possibilitam a análise e trazem uma aproximação bastante satisfatória sobre o sistema real.

6.1 DADOS DE ENTRADA PARA A ANÁLISE DO SISTEMA DO TANQUE COLETOR

Os dados utilizados como referência para a realização das simulações são os seguintes:

- Capacidade do tanque coletor: 1500 kg.
- Capacidade total de combustível da aeronave: 7300 kg.
- Densidade do combustível: 0,8 kg/l.
- Quantidade de válvulas: 5.
- Ciclo de vida do tanque: 2000 horas de voo.

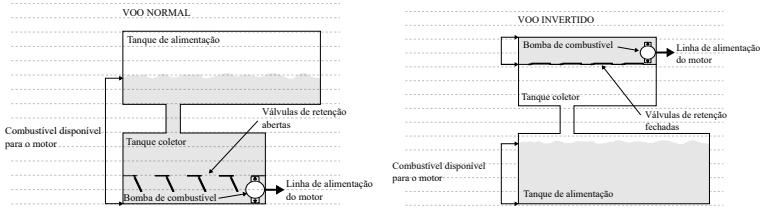
Além desses dados, algumas descrições foram passadas para auxiliar na modelagem do funcionamento do tanque, que serão descritas e utilizadas na execução das etapas e atividades do método desenvolvido.

6.2 ANÁLISE FUNCIONAL

6.2.1 Atividade 1.1 - Análise das funções

O tanque coletor (Figura 6.1) tem a função principal de assegurar que sempre exista um volume mínimo de combustível na seção onde se encontra a bomba de combustível. Dessa forma, sempre há combustível para alimentar o motor e evita-se a sucção de vapor de combustível (formado por variações de pressão resultante da variação de altitude) que pode causar cavitação na bomba. Além disso, estando submersa a bomba é resfriada pelo combustível, que circula pelos tanques presentes nas asas e fuselagem da aeronave.

Figura 6.1 – Representação do tanque coletor de aeronaves



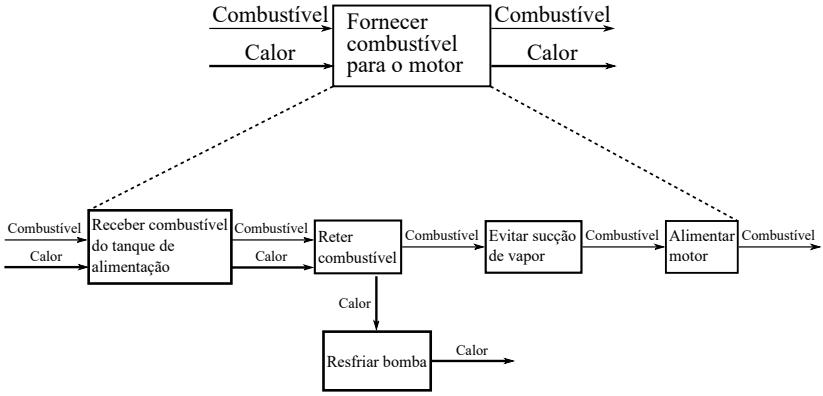
(a) Voo normal (b) Voo invertido

Assim, as funções do tanque coletor que podem ser identificadas são:

- Manter volume mínimo de combustível na seção da bomba.
- Reter combustível na região da bomba.
- Alimentar combustível do motor.
- Receber combustível dos tanques de alimentação.
- Resfriar a bomba.
- Evitar sucção de vapor de combustível.

A Figura 6.2 apresenta as funções utilizando a técnica de análise funcional. Como o objetivo deste trabalho é analisar falhas relativas a falta de combustível no tanque coletor, as funções relativas ao resfriamento da bomba e sucção de vapor de combustível não serão consideradas. Essa definição de escopo para o problema é aceitável pelo fato destas funções terem relação com

Figura 6.2 – Análise funcional do problema de referência



modos de falha diferentes do sistema de combustível, que não se referem a falhas ocultas nas válvulas de retenção.

Com as funções do sistema identificadas, parte-se para a identificação e caracterização dos componentes.

6.2.2 Atividade 1.2 - Identificação de subsistemas e componentes

Na Figura 6.1, além do tanque coletor, estão representados os tanques de alimentação de combustível, espalhados pelas asas e fuselagem, e que fornecem o combustível para o tanque coletor. Estes tanques estão fora do escopo de análise em relação a análise de falhas, mas estão representados devido a sua influência sobre as vazões de combustível nas válvulas e entre as seções internas do tanque coletor.

Toda a vazão de combustível entre os tanque de alimentação e o tanque coletor ocorre pela ação da gravidade.

O tanque coletor é dividido em duas seções conectadas pelas válvulas de retenção. Essas válvulas permitem que o combustível passe para a seção onde a bomba se encontra (região abaixo das válvulas de retenção da Figura 6.1a) mas não permitem que o combustível retorne durante voos invertidos.

Os componentes principais do tanque coletor são as válvulas. A ocorrência de falhas nesses componentes é que compromete a circulação de combustível entre as seções do tanque coletor e o cumprimento da função global do sistema.

O foco do trabalho está na operação do tanque coletor em relação à confiabilidade das válvulas. Desta forma, a bomba, a estrutura do tanque e os

tanques de alimentação serão considerados isentos de falhas.

Como opção de projeto, pode-se selecionar diferentes modelos de válvulas, alterando-se os diâmetros e consequentes vazões.

6.2.3 Atividade 1.3 - Identificação das variáveis de controle

A seção onde a bomba se encontra tem 1/3 do volume total do tanque coletor. A variável de controle que define se o sistema cumpre a função global é o volume de combustível.

Dessa forma, a simulação deve acompanhar as variações no volume do tanque após as execuções das manobras do avião.

O tanque coletor deve assegurar que sempre haja uma quantidade mínima de combustível no tanque coletor suficiente para executar uma manobra invertida de forma sustentada por até 10 segundos. Dessa forma, monitorando o volume na seção da bomba, é detectada a falha do sistema.

Como o combustível dos tanques de alimentação flui até o tanque coletor por gravidade, a coluna de combustível é um fator que influencia a vazão de combustível entre as seções A e B do tanque coletor.

Normalmente este comportamento é modelado por equações que determinam o comportamento contínuo do sistema. Porém, nesta tese, optou-se pela abordagem discreta em face das limitações de acesso a informações sobre o sistema. Contudo, em face da solução computacional adotada, infere-se que a solução seja adequada para o problema em tese.

Além disso, para determinar as equações necessárias para utilizar a abordagem contínua, é necessária a determinação de uma série de variáveis que, dadas as mesmas limitações de acesso as informações sobre o sistema, se torna inviável.

Desta forma, de acordo com a descrição do sistema dada pelos engenheiros consultados, para representar essa variação da vazão, dois casos são identificados: quando o tanque está cheio até chegar na metade do volume; e quando o tanque atinge a metade do volume até o fim.

A Tabela 6.1 apresenta as informações sobre as válvulas consideradas.

Tabela 6.1 Caracterização das válvulas de retenção

Modelo	**Diâmetro interno (pol)**	**Vazão mássica tanque cheio (kg/s)**	**Vazão mássica meio tanque (kg/s)**
3"	2,8"	7,2 kg/s	5,1kg/s
2"	2"	3,8kg/s	2,7kg/s

6.3 ANÁLISE COMPORTAMENTAL

A análise comportamental permite representar como o avião opera em situações reais de voo.

No caso do problema aqui analisado, o comportamento é dado pelas manobras executadas pela aeronave, sendo que as falhas apenas afetam como o sistema responde às transições de estado comportamental, em termos da variação da variável de controle "volume de combustível".

6.3.1 Atividade 2.1 - Descrição comportamental

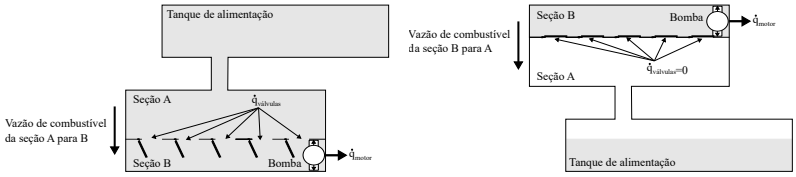
Para o desenvolvimento da análise, considera-se que para a decolagem em cada missão a aeronave está com o tanque cheio.

Uma missão é iniciada sempre pela decolagem e encerrada no pouso, quando há o sucesso da missão e a aeronave não cai. Durante a missão, a aeronave pode executar combinações diversas de manobras dependentes das características da missão.

Se a aeronave está apenas se deslocando entre duas bases, por exemplo, não há necessidade de executar manobras mais severas, como o voo invertido sustentado. Nesse caso, a aeronave apenas decola, voa em condição normal e pousa ao fim da missão.

Se considerarmos que a aeronave entra em combate ou está em missões de treinamento que simulam situações de combate, manobras invertidas fazem parte do repertório do piloto para conseguir evadir e atacar o inimigo. Essas manobras podem ter invertidas rápidas (*roll*) ou voos invertidos sustentados por alguns segundos. Essas manobras tem um consumo maior de combustível, além de demandar o bom funcionamento da retenção, já que consome combustível da seção B do tanque (Figura 6.3).

Figura 6.3 – Representação do tanque coletor de aeronaves



(a) Voo normal sem falha (b) Voo invertido sem falha

Na Figura 6.3 estão representadas as vazões de combustível entre as seções A e B, quando todas as válvulas estão operando na condição tão boas

quanto novas. Conforme pode ser observado, a vazão de A para B na condição normal é dependente da somatória das vazões das válvulas. Já no caso do voo invertido, a vazão de B para A é zero, dado que não há ocorrência de falhas nas válvulas.

Em condição normal de voo as válvulas de retenção permitem a entrada de combustível, vindo por gravidade dos tanques de alimentação, na seção onde está a bomba. Além de fornecer combustível para o motor, essa região do tanque coletor deve ficar submersa para resfriar a bomba de combustível e para evitar o bombeamento de vapor de combustível.

Os estados das válvulas (aberto ou fechado) influenciam como o volume de combustível irá variar nas seções do tanque coletor durante a execução de manobras.

As transições de estado das válvulas do tanque são dependentes das manobras que a aeronave executa. A Figura 6.3 ilustra os estados das válvulas de acordo com o tipo de manobra. Em voo normal (Figura 6.3a), a demanda é que as válvulas estejam abertas, permitindo que o combustível entre no tanque coletor e passe livremente para a seção da bomba, enchendo essa seção do tanque.

Quando a aeronave voa invertida (Figura 6.3b), a demanda é que as válvulas fechem. Com isso, o combustível da seção superior fica retido e alimenta o motor durante a execução da manobra.

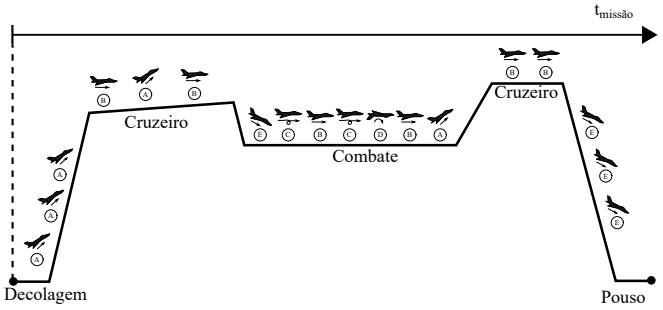
As características das missões quanto à combinação de manobras não é algo que siga um padrão bem definido. Por essa razão, a simulação de cenários reais é bastante complexa e praticamente impossível de ser executada. Normalmente o que se faz é definir algumas características de voo e a partir delas a verificação de como a aeronave se comporta.

Dessa forma, para analisar o comportamento do tanque coletor, a opção é obter diferentes combinações de manobras, fornecendo os mais variados perfis de missão e verificar em que casos a aeronave cai.

6.3.2 Atividade 2.2 - Análise de transições de estado dos componentes e subsistemas

Como descrito na seção anterior, sob o ponto de vista operacional, as transições dos estados dos componentes (válvulas abertas ou fechadas) dependem do tipo de manobra que a aeronave executa. As manobras, por sua vez são combinadas durante a execução de uma missão. A Figura 6.4 traz um exemplo de missão. Como pode ser observado, uma missão pode ser dividida em algumas fases: decolagem, voo em cruzeiro, combate e pouso. Em cada fase da missão, diferentes manobras podem ser executadas.

Figura 6.4 – Exemplo de missão, descrita em função das manobras



Cada missão tem uma duração específica, determinada pelo objetivo e pela autonomia de combustível. Com base no volume máximo de combustível que pode ser abastecido e no consumo em voo normal sem *afterburner*, a aeronave tem uma autonomia calculada em 35,8 minutos (sem reabastecimento em voo). Assim, a duração padrão das missões será considerada de 30 minutos.

O perfil da missão é variável e diferentes combinações de manobras podem ser executadas. Cada tipo de manobra tem um padrão de consumo diferentes.

A forma utilizada para representar as missões foi por uma abordagem discreta, identificando-se diferentes sequências de manobras com comportamento conhecido.

Por exemplo, pode-se gerar uma manobra que envolve um voo normal, seguido por uma manobra invertida sustentada, seguida por voo normal, e assim sucessivamente. Cada manobra dessas tem um consumo específico.

Dessa forma, as manobras definidas foram:

- Decolagem: marca o início da missão, quando o avião encontra-se com o tanque cheio.
- Voo normal: manobra mais comum, quando a aeronave se encontra na posição normal.
- Invertido: manobra sob gravidade negativa executada de forma sustentada.
- *Roll*: execução de manobra invertida instantânea durante o voo.
- Pouso: marca o final da missão quando o avião é bem sucedido.

É importante destacar que manobras de subida e descida ao longo do voo são consideradas como manobras normais. O consumo de combustível é semelhante ao voo normal e não há transição de estados das válvulas.

6.3.3 Atividade 2.3 - Análise das taxas de ocorrência das transições de estado

Considerando-se a característica altamente dinâmica do sistema em análise e os objetivos finais do trabalho, optou-se por representar o comportamento do sistema de forma discreta.

As transições de estado das válvulas ocorrem de acordo com as manobras executadas durante a operação do sistema. Quando as válvulas operam normalmente, elas ficam abertas em voo normal e fechadas em manobras invertidas.

Seguindo uma abordagem discreta para a representação das manobras durante uma missão, para cada estado operacional identificado (manobra) foram definidos tempos fixos para a duração. Dessa forma, pode-se sortear diferentes sequencias de manobras que caracterizam a missão e a somatória dos tempos das manobras correspondem a duração total da missão.

Atribuindo-se pesos para manobras, correspondentes a chance de a manobra ser sorteada, pode-se definir se uma missão é mais ou menos severa sobre o sistema (com mais ou menos manobras invertidas, por exemplo). Voos normais tem peso maior por ser a forma que o avião mais voa e o invertido tem peso menor por ser menos frequente. Aumentando o peso do voo invertido, aumenta-se a frequência com que estes são sorteados.

A Figura 6.5 exemplifica a formação dos padrões de voos e sorteio das manobras de acordo com a definição dos pesos. Na Figura 6.5a, por exemplo, a frequência de manobras invertidas é bem maior que na Figura 6.5b, dado que os pesos são respectivamente 10% e 2%.

Vale ressaltar que com esta abordagem, voos normais de longa duração são facilmente representados, pois com peso maior nas manobras normais, maior probabilidade de ocorrência de sorteios para que os voos normais aconteçam em sequência.

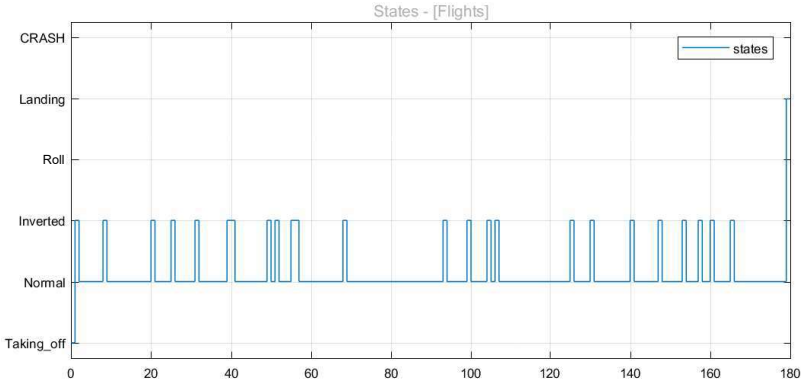
Por exemplo, pode-se fixar a duração de um voo normal em 10 segundos. Para modelar um perfil de voo em que essa manobra acontece durante um período maior, o sorteio resulta em uma sequência de manobras normais. Esse exemplo pode ser verificado na Figura 6.6.

A formação dos perfis de voo é feita pelo sorteio de sequências aleatórias de voos, visando obter amostras variadas de perfis, permitindo verificar uma grande variedade de casos que podem ocorrer na vida real.

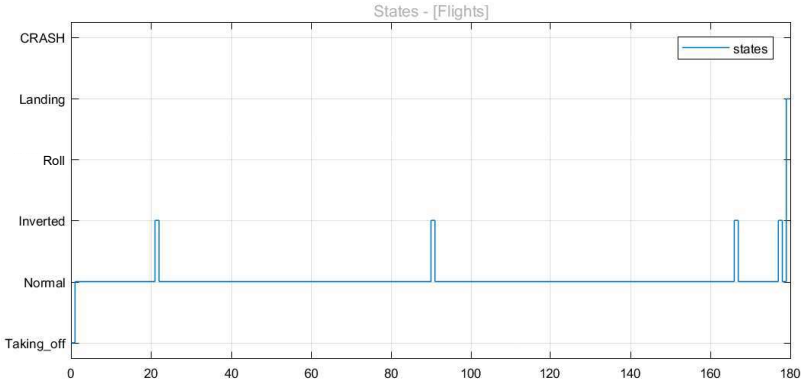
O ciclo de vida do tanque coletor é formado por um conjunto de missões que soma as 2000h estabelecidas em projeto. Este conceito está representado na Figura 6.7.

Para alterar a severidade dos perfis de voo, aumentam-se os pesos das manobras invertida e *roll*, já que estas manobras possuem um consumo de

Figura 6.5 – Influência dos pesos na formação dos perfis de voo



(a) Exemplo de sorteio de manobras invertidas com peso 10%



(b) Exemplo de sorteio de manobras invertidas com peso 2%

Figura 6.6 – Modelo de voo normal longo

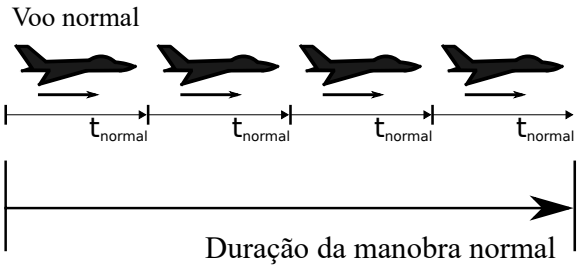
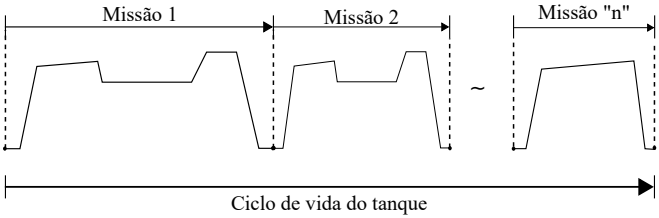


Figura 6.7 – Ciclo de vida do tanque coletor



combustível maior.

Por fim, vale ressaltar que esta representação discreta dos perfis de voo permite aproximar o modelo de uma representação contínua. Isso significa que reduzindo-se o tempo de duração definido para cada manobra, reduz-se o incremento de tempo em cada transição de estado. Além disso, pode-se utilizar distribuições de probabilidade para obter durações aleatórias para a durações das manobras. Porém, para que isso seja possível é necessário obter mais detalhes quanto aos pesos e possivelmente criar estados intermediários para que o modelos das missões tenha os detalhes desejados.

6.3.4 Atividade 2.4 - Análise da relação entre transições e a variável de controle

O consumo de combustível é dependente do tipo de manobra. Voos invertidos com *afterburner*, que é quando combustível extra é injetado na saída da turbina aumentando o empuxo gerado, são os com consumo mais elevado.

Além do combustível que é queimado apenas para a movimentação da aeronave, uma porção também é queimada para a geração de energia de outros sistemas da aeronave. Esses consumos são dados por:

- Consumo em voo normal pelo motor: 2,4 kg/s.
- Consumo em voo normal para outros sistemas: 0,35 kg/s.
- Consumo durante voo invertido com *afterburner* pelo motor: 6 kg/s.
- Consumo durante voo invertido com *afterburner* para outros sistemas: 0,35 kg/s

O comportamento da variável de controle “Volume de combustível” para o sistema de combustível todo é dependente apenas do consumo do motor. Se estabelecermos um volume de controle em volta do sistema de combustível

fica fácil perceber, já que o único combustível que entra é o que foi abastecido, em solo, e o consumido é o do motor durante o voo.

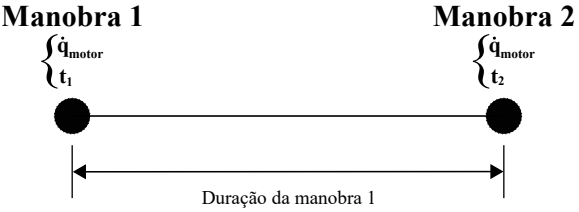
Se considerarmos o tanque coletor, por sua vez, este comportamento é um pouco mais complexo. Neste caso, considerando que todas as válvulas e demais componentes estão sem falha (Figura 6.3), o volume de combustível varia segundo:

- Combustível que flui dos tanques de alimentação para o tanque coletor, por gravidade, quando a aeronave executa voos normais;
- combustível que flui da seção A do tanque coletor (parte superior) para a seção B (inferior) quando a aeronave executa voos normais;
- combustível consumido da seção B (onde de encontra a bomba de combustível) do tanque coletor pelo motor, tanto para voo normal como invertido.

As seções do tanque coletor foram representadas na Figura 6.3. As variações dos volumes são dependentes das manobras executadas pela aeronave, sendo diferente em voo normal e voo invertido.

Essa variação de combustível pode ser calculada a partir do consumo de combustível em cada manobra e o tempo que o avião permaneceu nessa manobra. Considerando o exemplo da Figura 6.8. No instante t_1 a aeronave entra na manobra 1, cuja duração é fixa. Quando ocorre a transição para a manobra 2, o cálculo do volume é feito multiplicando-se a duração da manobra 1 pelo consumo do respectivo tipo de manobra ($\dot{q}$). Os tempos t_1 e t_2 marcam os instantes em que há as transições de estado (manobras) definidos a partir do sorteio aleatório.

Figura 6.8 – Cálculo dos volumes considerando os eventos discretos



6.3.4.1 Voo normal

O volume total de combustível da aeronave, considerando-se a divisão em seções representada na Figura 6.3, é dado por:

$$V_{Total} = f(\dot{q}_{motor}) \tag{6.1}$$

Considerando como volume de controle os tanques de combustível, sem reabastecimento no ar. Durante a missão a variação no volume total é função apenas do combustível consumido pelo motor.

O volume de combustível presente no tanque coletor em um dado instante, considerando-se as duas seções que o separam é dado por:

$$V_{Coletor}(t) = V_A(t) + V_B(t) \tag{6.2}$$

A variação do volume nas partes que compõem o tanque coletor (seção A e seção B na Figura 6.3) é dependente do tipo de manobra executada e dos estados das válvulas, que podem ou não apresentar falha, sendo estas falha aberta ou falha fechada. Considerando-se as válvulas funcionando normalmente, em voo normal temos:

$$\sum \dot{q}_{valvulas} > \dot{q}_{motor} \tag{6.3}$$

A vazão das válvulas, por sua vez, é dependente da quantidade de combustível presente no tanque coletor, conforme explicitado no Tabela 6.1. Dessa forma, para calcular o volume dependente das vazões das válvulas, é necessário primeiro verificar o volume de combustível presente no tanque, para então selecionar qual valor de vazão utilizar. Além disso, deve-se verificar qual o modelo de válvula utilizado.

Sem a ocorrência de falhas, no voo normal as válvulas estão todas abertas e a vazão da seção A para a seção B é máxima. Dessa forma, a seção B (onde está a bomba) nunca ficará sem combustível enquanto houver combustível nos tanques de alimentação.

Dado que ainda haja combustível no tanque de alimentação, o volume do tanque coletor, assim como das seções do tanque, é máximo conforme a Equação 6.4. Vale ressaltar que a seção A e o tanque de alimentação estão conectador livremente e que a transferência de combustível entre eles é instantânea.

$$V_A(t) = V_{A_{max}}; V_B(t) = V_{B_{max}} \tag{6.4}$$

Quando não há mais combustível nos tanques de alimentação, o volume da seção A começa a cair, sendo calculado em um dado instante t por:

$$V_A(t) = V_A(t-1) - \dot{q}_{motor} \cdot \Delta t \tag{6.5}$$

Enquanto ainda há combustível no na seção A do tanque coletor, a seção B ainda continua com o volume máximo.

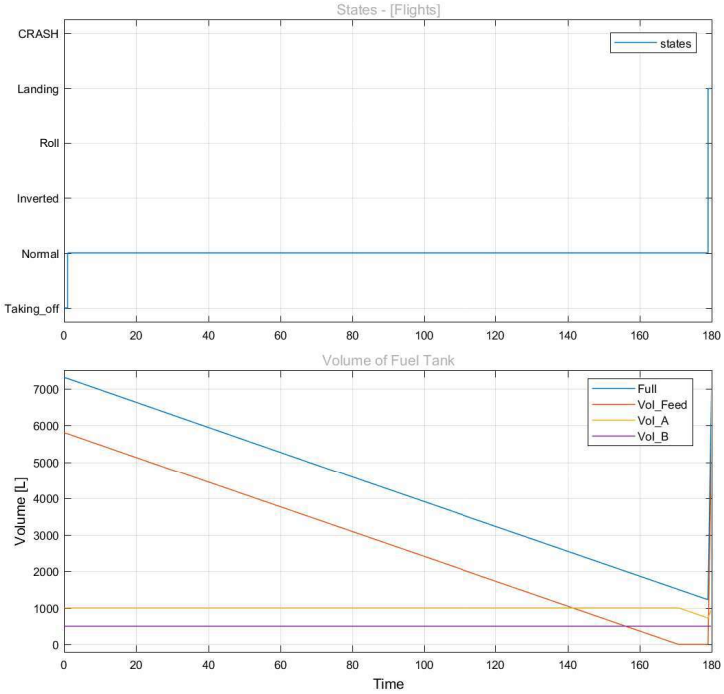
Por fim, quando não há mais combustível na seção A do tanque, o volume da seção B (onde se encontra a bomba) em um dado instante t, é calculado por:

$$V_B(t) = V_B(t-1) - \dot{q}_{motor} \cdot \Delta t \tag{6.6}$$

Estes comportamentos descritos dos volumes dos tanques em voo normal sem a ocorrência de falhas pode ser visualizado na Figura 6.9.

A Figura 6.9 consiste em dois gráficos, sendo o superior o que representa as manobras executadas em uma missão, e o gráfico inferior o que representa o comportamento dos volumes. A linha *"Full"* representa o comportamento do volume total de combustível da aeronave, a linha *"Vol_Feed"* o volume de combustível do conjunto de tanques de alimentação, a linha *"Vol_A"* o volume de combustível da seção A do tanque coletor e a linha *"Vol_B"* o volume de combustível da seção B.

Figura 6.9 – Comportamento dos volumes de combustível em voo normal sem falhas



6.3.4.2 Voo invertido

Quando as válvulas não apresentam falha e o avião se encontra em voo invertido, a retenção de combustível funciona e não há vazão de retorno para os tanques de armazenamento. Com isso, o volume de combustível na seção B (onde se encontra a bomba) no início da manobra invertida é máxima e o volume ao final da manobra é determinado pelo consumo do motor.

Dessa forma:

$$\sum \dot{q}_{valvulas} = 0 \tag{6.7}$$

Portanto:

$$V_B(t) = V_B(t-1) - \dot{q}_{motor} \cdot \Delta t \tag{6.8}$$

$$V_A(t) = V_A(t-1) \tag{6.9}$$

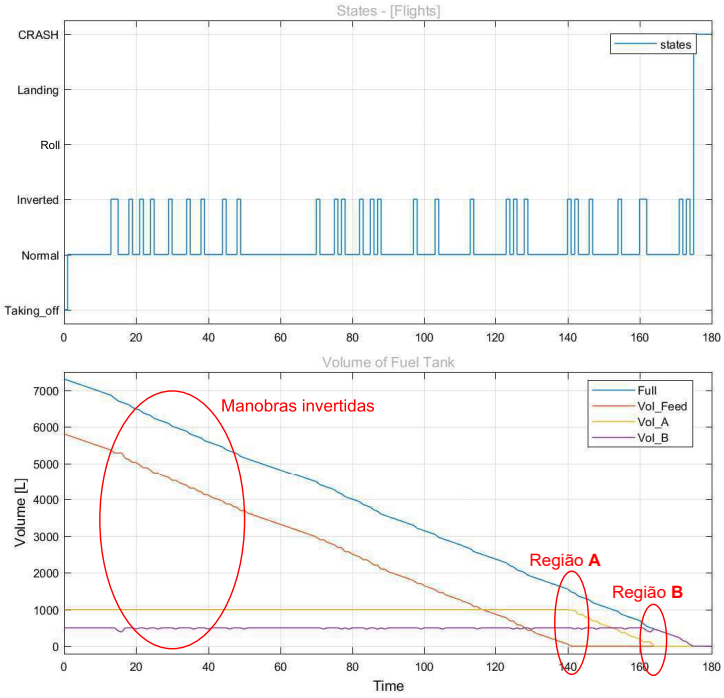
Como não há vazão da seção A para a seção B, o volume da seção A e dos tanques de alimentação somados permanece constante. Dado que a transferência de combustível entre o tanque de alimentação e a seção A do tanque coletor é instantânea, considera-se que o volume de combustível da seção A permanece constante. O comportamento dos volumes em voo invertido sem falhas pode ser observado na Figura 6.10.

A região A representa o instante em que acaba o volume de combustível dos tanques de alimentação (representado pela linha "Vol_Feed"). A partir desse instante o volume do tanque coletor começa a ser consumido. Em voo normal, isso significa que o volume "Vol_A" começa a baixar.

A região B indica o instante que acaba o combustível da seção A do tanque coletor. Com isso o volume da seção B ("Vol_B") começa a baixar.

A Figura 6.11 apresenta uma aproximação da região onde ocorre uma manobra invertida no caso do gráfico da Figura 6.10. Percebe-se que durante a manobra, o consumo de combustível é maior, causando alteração na variação da linha que representa o volume total de combustível da aeronave ("Full"). O volume "Vol_Feed" é calculado pela diferença entre o volume total da aeronave e o volume do tanque coletor. Por essa razão, observa-se a variação desse volume. A linha do volume da seção B apresenta variação dado que o combustível ficou retido para a execução da manobra invertida e durante a manobra o motor consome parte desse combustível.

Figura 6.10 – Comportamento dos volumes de combustível em voo invertido sem falhas



6.4 ANÁLISE DE FALHA

O cenário crítico para o sistema é a falta de combustível durante a execução de manobras invertidas. A aeronave conta com medidores de combustível análogo ao de carro. Esses medidores indicam quanto combustível ainda há na aeronave, mas não indicam em qual parte do sistema esse combustível se encontra.

Por essa razão, é impossível o piloto saber que o sistema está funcionando normalmente e que há combustível suficiente para executar manobras invertidas. Assim, todas as falhas ocorridas nas válvulas, independente do modo de falhas, são ocultas (Figura 6.12).

Figura 6.11 – Relação entre os volumes nas manobras invertidas

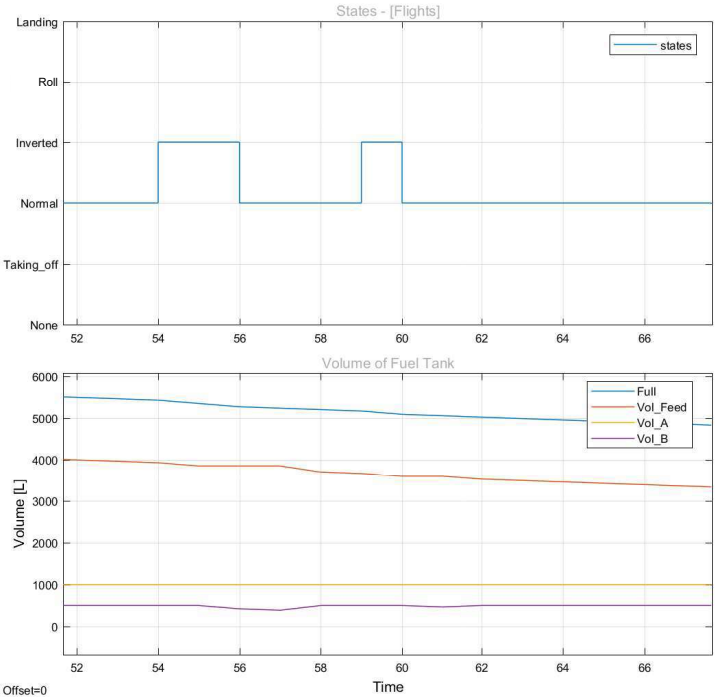
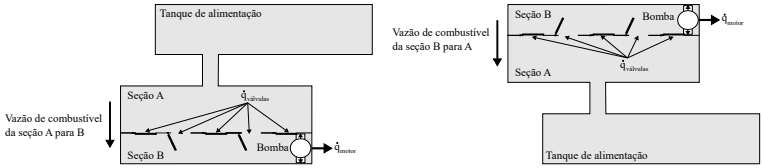


Figura 6.12 – Representação dos volumes dos tanques e das vazões com ocorrência de falhas



(a) Voo normal (b) Voo invertido

6.4.1 Atividade 3.1 - Identificação dos modos de falha

Na análise desenvolvida as falhas dos componentes são tratadas como processos markovianos com apenas dois estados, um sem falha (operacional) e um estado com falha.

Dessa forma, os modos de falha identificados para válvulas são:

- Válvula travada aberta: uma combinação de válvulas abertas não retém combustível na seção da bomba.

- Válvula travada fechada: uma combinação de válvulas fechadas reduz a entrada de combustível na seção da bomba quando o avião voa normal.

Como forma de detalhar ainda mais as falhas das válvulas, poderiam ser definidos modos de falhas que representam níveis de degradação. Dessa forma, as falhas resultariam nas válvulas parcialmente abertas em diferentes níveis. Porém, neste trabalho só foi possível definir os modos de falha acima citado, dado que não há dados disponíveis quanto as taxas de ocorrência de eventuais modos de falha intermediários.

Para fins de análise futura, visando oferecer ainda mais informação aos projetistas, seria interessante buscar as informações necessárias para integrar níveis de degradação dos componentes à analise do sistema.

6.4.2 Atividade 3.2 - Análise dos efeitos sobre as variáveis de controle

As falhas fechadas nas válvulas resultam em menor vazão de combustível da seção A (superior) para a seção B (onde se encontra a bomba). Com isso, ao executar uma manobra invertida, é necessário a execução de uma manobra normal por mais tempo para que o volume na seção da bomba (Figura 6.12) seja restaurado ao nível máximo. Dessa forma, assegura-se que ao voar invertido novamente, a autonomia da aeronave seja máxima

As falhas abertas, por sua vez, são as falhas mais críticas para o sistema. Quando estas falhas ocorrem, o volume de combustível da seção da bomba (B) diminui muito mais rápido que o normal durante os voos invertidos.

Com isso, a aeronave tem um tempo muito menor para concluir a manobra invertida antes que todo o combustível retido no tanque seja consumido. Considerando-se que durante a manobra invertida o consumo de combustível é mais alta que no voo normal, torna-se evidente que as falhas abertas são mais preocupantes que as falhas fechadas.

As possíveis causas para esses modos de falha são a contaminação do combustível por partículas estranhas ou pela formação de borra de combustível.

6.4.3 Atividade 3.3 - Identificação das falhas ocultas potenciais

Para esse sistema em particular, todas as falhas ocorridas nos componentes são ocultas, independente dos modos de falha.

Como o sistema não conta com sensores, exceto pelo sensor de nível

que mede a quantidade total de combustível e determina a autonomia de voo da aeronave, não é possível a detecção da ocorrência de falhas pelo piloto durante os voos.

Além da ausência de sensores, os modos de falha só influenciam o sistema dependendo das manobras que são executadas. Porém, os efeitos dos modos de falha também não são detectáveis pelo piloto. Válvulas abertas, por exemplo, não interferem no voo normal e durante a manobra invertida elas apenas ajudam a drenar a seção B do tanque coletor, mas enquanto a aeronave consegue voar normalmente, não são detectáveis.

Por fim, as falhas ocorridas nas válvulas não podem ser detectadas por meio de inspeção periódica, dado que por decisão de projeto, os tanques são selados e as válvulas não podem ser verificadas.

6.4.4 Atividade 3.4 - Modelagem das falhas do sistema

Entre as informações disponíveis sobre o sistema estão os modelos das válvulas e as taxas de falhas. Em função do sigilo das informações referentes ao sistema real, as taxas de falha são aproximadas e baseadas nas informações reais. Essas taxas de falhas estão apresentadas na Tabela 6.2. Segundo os engenheiros consultados, esses dados representam uma aproximação satisfatória para testar o método de análise proposto.

Tabela 6.2 Taxas de falhas dos modelos de válvulas

Modelo	**Taxa de falha aberta (falhas/hora)**	**Taxa de falha fechada (falhas/hora)**
3"	$4,1 \cdot 10^{-4}$	$2 \cdot 10^{-6}$
2"	$4,6 \cdot 10^{-4}$	$2,4 \cdot 10^{-6}$

As taxas de falhas são usadas no sorteio dos tempos de falha dos componentes. A comparação entre os tempos de falhas e os tempos das manobras executadas na simulação do comportamento da aeronave permite avaliar os efeitos dos modos de falha sobre o volume de combustível no tanque coletor.

Conforme citado anteriormente, ocorrência dos modos de falha identificados tem diferentes efeitos sobre o sistema, dependendo da manobra que está sendo executada. Os efeitos dos modos de falha para os tipos de manobras serão detalhados a seguir.

6.4.5 Voo normal

Durante o voo normal, as únicas falhas com consequências sobre o volume de combustível no tanque coletor são as falhas fechadas. Essas falhas reduzem a vazão de combustível para a seção da bomba (seção B da Figura 6.12).

Para que a vazão da seção A para a seção B seja menor que o consumo do motor é necessária a ocorrência de múltiplas válvulas com falha fechada ao mesmo tempo, cujo número depende das vazões de cada válvula.

Assim, quando o número de válvulas sem falha é suficiente para assegurar a vazão entre as seções maior que o consumo do motor:

$$\sum \dot{q}_{valvulas} > \dot{q}_{motor} \tag{6.10}$$

Nesse caso, a seção B (onde está a bomba) ainda terá combustível enquanto houver combustível nos tanques de alimentação. Dado que ainda haja combustível disponível nos tanques coletores, os volumes das partes do tanque coletor são dadas por:

$$V_A(t) = V_{A_{max}}; V_B(t) = V_{B_{max}} \tag{6.11}$$

Porém, quando a quantidade de válvulas falhadas fechadas resultam em uma vazão para a seção B menor que o consumo do motor:

$$\sum \dot{q}_{valvulas} < \dot{q}_{motor} \tag{6.12}$$

Quando ainda há combustível nos tanques de alimentação, os volumes das partes do tanque coletor são dados por:

$$V_A(t) = V_{A_{max}} \tag{6.13}$$

$$V_B(t) = V_B(t-1) - (\dot{q}_{motor} - \dot{q}_{valvulas}) \cdot \Delta t \tag{6.14}$$

6.4.6 Voo invertido

Falhas fechadas não afetam o volume de combustível no voo invertido. Porém quando há falhas abertas, o volume reduz mais rápido que o consumo do motor, pois combustível também é drenado para a seção A e consequentemente para os tanques de alimentação.

Assim, no voo invertido, quando:

$$\sum \dot{q}_{valvulas} \neq 0 \tag{6.15}$$

O volume da seção A depende do volume dos tanques de alimentação, pois durante o voo invertido o combustível da seção A tende a retornar ao tanque de alimentação. Como durante o voo invertido é indiferente se o combustível está na seção A ou nos tanques de alimentação (já que eles estão conectados e a transferência de combustível entre eles é instantânea), será considerada a soma dos dois volumes. Assim, os volumes das seções do tanque coletor são calculadas por:

$$V_A(t) + V_{alim}(t) = (V_A(t-1) + V_{alim}(t-1)) + \dot{q}_{valvulas} \cdot \Delta t \tag{6.16}$$

$$V_B(t) = V_B(t-1) - (\dot{q}_{motor} + \dot{q}_{valvulas}) \cdot \Delta t \tag{6.17}$$

A Figura 6.13 apresenta a comparação do comportamento dos volumes de combustível com e sem falhas durante voo invertido. É possível perceber que com a ocorrência de falhas (Figura 6.13b) há vazão de combustível de volta para os tanques de alimentação durante as manobras invertidas. O consumo mais acentuado na linha de volume "Vol_A" indica que além consumo do motor, há redução de volume da seção B do tanque pela retorno de combustível para os tanques de alimentação.

6.5 IMPLEMENTAÇÃO DO MODELO DE SIMULAÇÃO

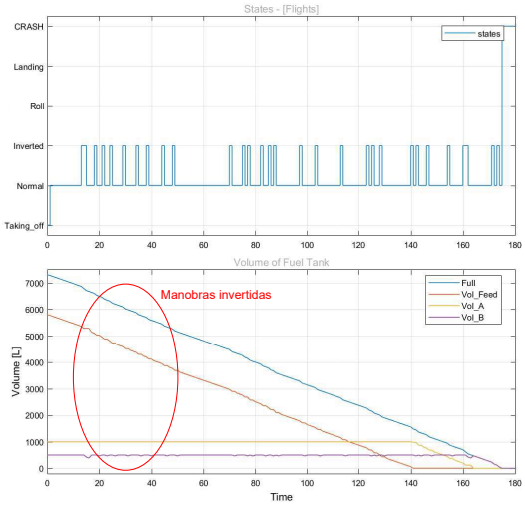
A implementação do modelo de simulação foi feita utilizando o *software* Matlab/Simulink utilizando principalmente os recursos de máquinas de estado (*Stateflow*). A vantagem de se utilizar tal recurso está no uso de blocos para representar os diferentes elementos envolvidos na modelagem de sistemas, permitindo o uso de funções específicas e facilitando a atualização do modelo.

6.5.1 Atividade 4.1 - Implementar modelos de falha

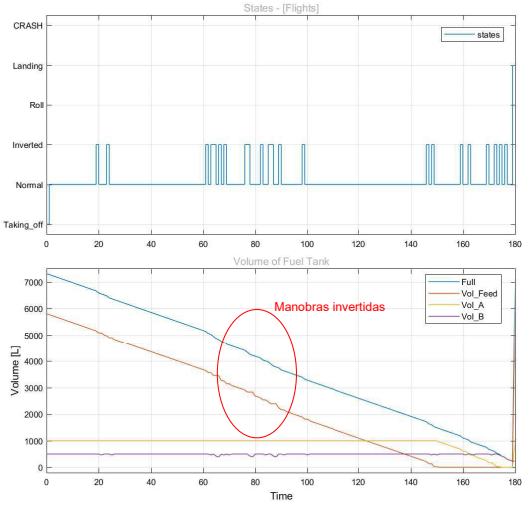
As variáveis de entrada dos modelos são:

- Volumes do tanque coletor: utilizado no modelo para calcular as transferências de combustível entre as seções do tanque coletor de acordo com as manobras e monitorar o volume de combustível na seção B do

Figura 6.13 – Comparação dos volumes em voo invertido sem e com falha de válvulas



(a) Sem falha



(b) Com falhas

tanque.

- Volume do tanque de alimentação: complemento para o volume do tan-

que coletor para determinar o volume total de combustível da aeronave.

- Volume mínimo: determina o critério de falhas, sendo que a aeronave não pode executar uma manobra quando atinge este volume.

- Número de válvulas: define quantos componentes influenciam a transferência de combustível entre as seções dos tanques e que estão sujeitos a falhas.

- Número de missões: determina o ciclo de vida do sistema (cada missão tem 30 minutos de voo). O ciclo de vida definido para o tanque coletor é de 2000h de voo, mas para fim de testes é interessante definir o número de missões como dado de entrada das simulações para permitir testes de diferentes ciclos de vida.

- Tempo de missão: define a duração de cada missão e quantas manobras de duração definidas devem ser sorteadas.

- Pesos das manobras: determina a frequência com que cada manobra é sorteada aleatoriamente.

- Taxas de falhas: determinam os tempos que serão sorteados e os modos de falha de cada componente. Utilizar as taxas de falha como dado de entrada permite testar o sistema utilizando componentes com confiabilidade maior ou menor.

De acordo com os passos da atividade 4.1 ilustrados na Figura 5.15, com as variáveis inicializadas, parte-se para o sorteio dos tempos de falha. Os sorteios foram feitos pela função específica do Matlab, utilizando as taxas de falha como parâmetro médio da função.

Em cada rodada de simulação que representa o ciclo de vida do tanque um novo sorteio dos tempos de falha é executada.

Por fim, com os tempos de falha sorteados, faz-se a comparação entre os tempos para falhas abertas e falhas fechadas. Assim, o menor tempo de falha define qual modo de falha irá efetivamente ocorrer em cada válvula.

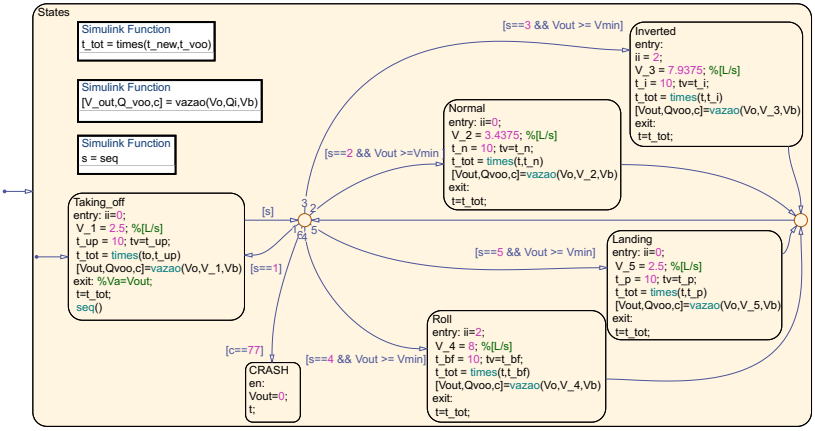
6.5.2 Atividade 4.2 - Implementar modelo comportamental

Como citado anteriormente, os estados operacionais para o tanque coletor são definidos pelas manobras executadas pela aeronave.

Os pesos de cada manobra são utilizado para sortear a sequência de manobras que a aeronave irá executar durante a missão simulada.

O conhecimento *a priori* das sequências de manobras permite estabelecer uma máquina de estados, definindo-se as manobras como os estados operacionais do sistema. Dessa forma, em cada passo de simulação o sistema entra em um dado estado (manobra), verifica o que está acontecendo com a variável de controle, atualiza os valores necessários e entra no próximo estado. A Figura 6.14 apresenta a máquina de estados resultante, desenvolvida utilizando a biblioteca específica do Simulink.

Figura 6.14 – Modelo de comportamento por máquina de estados



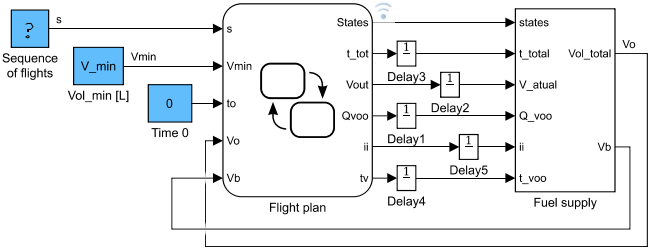
No caso da aeronave, a transição entre os estados operacionais (representada pelas setas) ocorre apenas pela operação de acordo com as manobras necessárias durante o voo. Por essa razão, as transições na máquina de estado ocorrem de acordo com a sequência sorteada no início da simulação. Todo voo começa pela decolagen (“Taking off”) e então as manobras sorteadas no início da simulação começam a ser executadas (“Normal”, “Inverted” e “Roll”).

Quando a verificação dos volumes detecta que o volume existente não é suficiente para a execução da manobra seguinte da sequência, a aeronave cai (“Crash”). Os volumes são calculados cada vez que o sistema entra em cada estado, com base nas variáveis como consumo (“V_2” no estado normal, por exemplo), tempo de duração da manobra (“t_n” no estado normal, por exemplo), volumes anteriores, etc.

6.5.3 Atividade 4.3 - Implementar as transições de estado e efeito sobre a variável de controle

O modelo geral pode ser divido em duas partes principais (Figura 6.15): máquina de estados, que simula a execução de um dado perfil de voo aleatório; e a verificação do volume de combustível da aeronave, que é dependente das manobras, dos estados das válvulas e determina se ocorrerá a falta de combustível na manobra, podendo levar a queda da aeronave.

Figura 6.15 – Modelo geral que relaciona as manobras de voo e o combustível



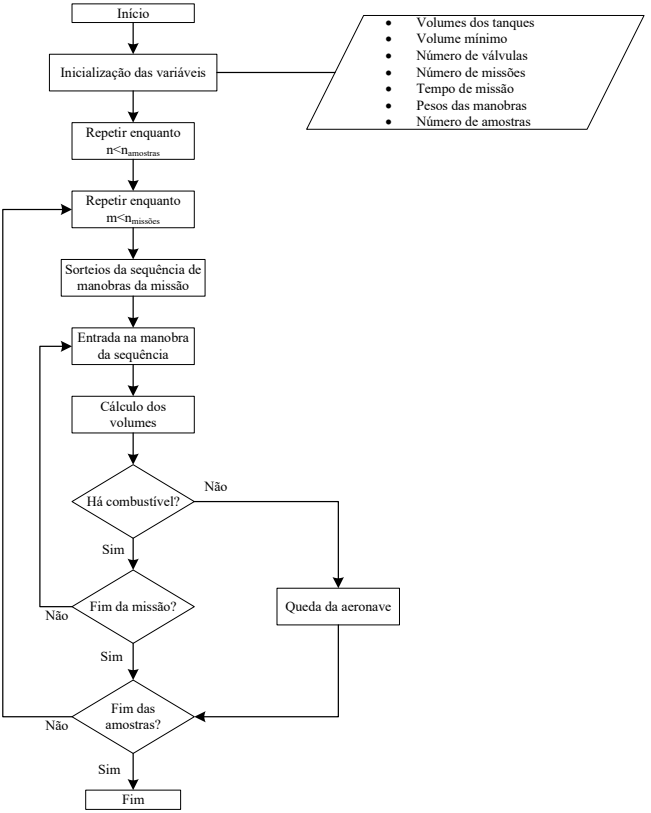
A Figura 6.16 apresenta o fluxograma para auxiliar no entendimento do modelo implementado. Enquanto o número de amostras definido na entrada do modelo não é atingido, as missões aleatórias são geradas pelo sorteio de sequências de manobras. A máquina de estados faz a simulação da entrada nas manobras e cada vez que o sistema entra em uma dada manobra são verificados os volumes de combustível.

Para verificar o comportamento do volume de combustível no tanque, o modelo de simulação:

- Verifica se há falha em algum componente;
- identifica o estado operacional (manobra) da aeronave;
- identifica qual o modo de falhas ocorrido; e
- atualiza os estados dos componentes.

A verificação se há falha ou não é feita pela comparação entre os tempos de falha sorteados para as válvulas e o tempo total transcorrido na simulação do ciclo de vida do tanque. Como citado anteriormente, cada manobra tem duração fixa e o tempo transcorrido é calculado pela multiplicação das manobras executadas e os respectivos tempos de duração.

Figura 6.16 – Fluxograma do modelo de simulação implementado



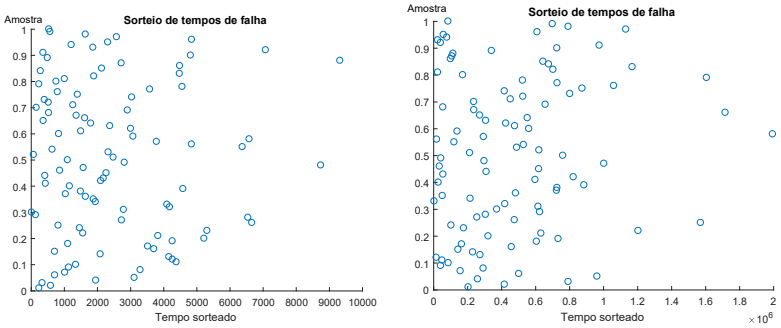
A comparação se o tempo de falha sorteado é menor que o tempo transcorrido define se há ou não falha nas válvulas do tanque coletor.

Na atividade 4.1 é feita a comparação entre os tempos sorteados para falha aberta e falha fechada. O menor tempo sorteado para cada válvula define o modo de falha que será considerado ao longo do ciclo de vida do tanque.

Pelos valores das taxas de falha, é possível perceber que a chance de ocorrência de falhas abertas é consideravelmente maior que as falhas fechadas. Para o caso de amostras com cem sorteios representados parcialmente na Figura 6.17, por exemplo, é possível perceber que, apesar de ser raro, pode acontecer de a falha fechada ser sorteada com tempo menor e definir o modo de falha de uma válvula. O ponto mais a esquerda da Figura 6.17b, por exemplo representa um tempo sorteado em torno de 1400 horas (claramente dentro do

tempo de ciclo de vida do tanque).

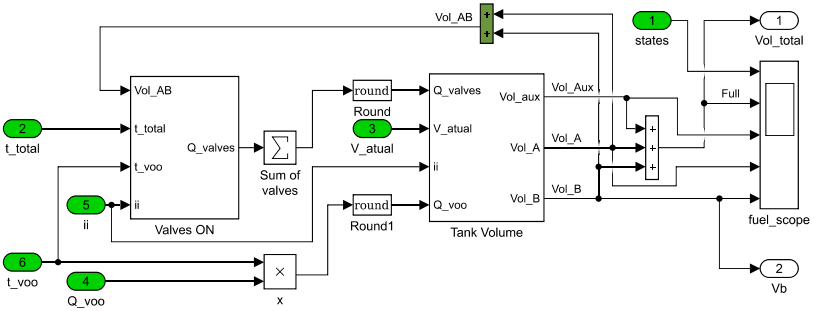
Figura 6.17 – Comparação entre os tempos sorteados para falhas abertas e falhas fechadas



(a) Dispersão dos tempos de falha aberta (b) Dispersão dos tempos de falha fechada

Conhecendo os estados das válvulas e estabelecendo sua relação com o estado operacional da aeronave, os volumes das seções do tanque coletor são calculados, seguindo os princípios das equações da Seção 6.4.4 deste capítulo. O modelo resultante utilizando os blocos do Simulink está apresentado na Figura 6.18

Figura 6.18 – Modelo para cálculo das vazões e volumes dos tanques



O fluxograma da Figura 6.19 apresenta a lógica por traz da modelo implementado na Figura 6.18. Quando a aeronave entra em uma manobra, é verificado se ocorreu uma falha durante a manobra anterior. Caso tenha ocorrido, dependendo do modo de falha (aberto ou fechado) o modelo atualiza o "sinal" da válvula falhada indicando o sentido que a válvula permite a vazão.

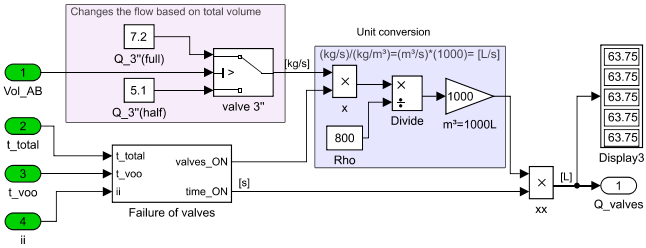
Então, o modelo calcula o combustível consumido e que fluiu entre as seções do tanque, atualizando os valores de volume.

Figura 6.19 – Fluxograma do cálculo dos volumes

Para a modelagem das vazões das válvulas, dois aspectos importantes foram considerados: a possibilidade de variar os modelos das válvulas, alterando as vazões e as taxas de falhas; e a variação da vazão dependente do volume total de combustível disponível na aeronave.

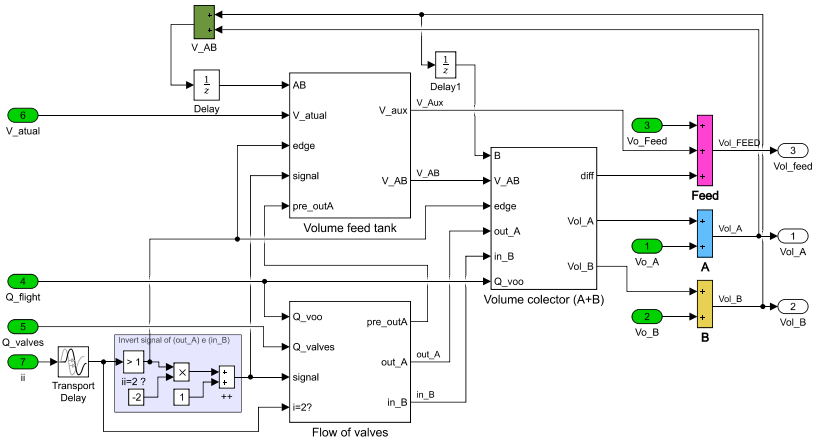
Ao entrar em um dado estado operacional, o modelo verifica qual o volume total de combustível no estado anterior e, para calcular as vazões de combustível entre as seções do tanque, faz o chaveamento para a vazão adequada a ser utilizada. O modelo resultante está apresentado na Figura 6.20. Na caixa "*Failure of valves*" é feita a comparação entre os instantes das falhas com o tempo atual, a comparação dos tempos de falha com o tempo total de voo e a verificação das manobras invertidas. Com isso, as vazões das válvulas são atualizadas quanto ao valor e sentido (de A para B ou de B para A, dependendo da manobra).

Figura 6.20 – Modelo para a seleção das vazões com base no volume de combustível



O modelo calcula ainda o volume que foi consumido na ultima manobra e verifica quanto combustível sobrou nas seções do tanque coletor (Figura 6.21). Quando a aeronave executa uma manobra invertida, se houver falhas abertas, parte do combustível da seção B retorna para a seção A. Essas variações de volume são computadas a partir da mudança no sentido da vazão das válvulas (caixa "*Flow of valves*"), dependente da ocorrência de falhas e das manobras. As variações dos volumes de combustível, na medida que vão sendo calculados, podem ser representados na forma gráfica (como a Figura 6.13) ao longo da simulação, facilitando a interpretação dos cenários por parte dos projetistas e analistas.

Figura 6.21 – Modelo de cálculo dos volumes consumido e restante do tanque coletor



Por fim, com os valores atualizados dos volumes de combustível das seções do tanque coletor e do tanque de alimentação, pode-se verificar se haverá combustível suficiente para executar a próxima manobra prevista dentro da sequência sorteada no início da definição da missão. Quando houver combustível suficiente o sistema entra no próximo estado de voo, caso contrário a aeronave cai.

6.6 ANÁLISE DE CENÁRIOS

Os resultados das simulações trazem dois tipos básicos de informação:

- Como o sistema se comporta ao longo do ciclo de vida, a partir de um grande número de simulações.

- Como o sistema se comporta nas missões.

As simulações de ciclo de vida são importantes para avaliar como as decisões de projeto afetam a vida do tanque coletor. Com isso, pode-se variar, por exemplo, o número de válvulas ou as taxas de falha e verificar o impacto sobre o sistema.

Além disso, pode-se verificar se é prudente reduzir o tempo definido para substituição do tanque ou se possível estender a vida.

Já as simulações das missões permitem avaliar qual a relação entre as falhas ocorridas e o tipo de manobra que o piloto pode executar.

Pode-se verificar ainda a influência do número de válvulas, taxas de falhas, modos de falha, tempos de falha entre outros aspectos sobre a probabilidade de ocorrência de quedas da aeronave.

A forma como o modelo foi gerado, permite alterar a frequência com que as manobras mais severas ocorrem, trocar as taxas de falhas das válvulas, alterar o número de válvulas, alterar as vazões das válvulas, além de outras variáveis da operação da aeronave.

6.7 RESULTADOS

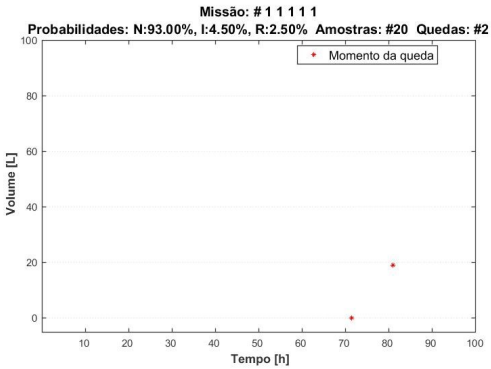
Os resultados aqui apresentados foram obtidos a partir de simulações para o ciclo de vida e para missões isoladas.

6.7.1 Simulações do ciclo de vida

A Figura 6.22 traz um exemplo de simulação de voo para falhas abertas de válvulas, com a ocorrência de quedas da aeronave representado pelos pontos. Neste exemplo, os pesos das manobras utilizados foram:

- Normal: 93%
- Invertido: 4,5%
- Roll: 2,5

Figura 6.22 – Simulação de voo em um perfil de missão com falhas abertas

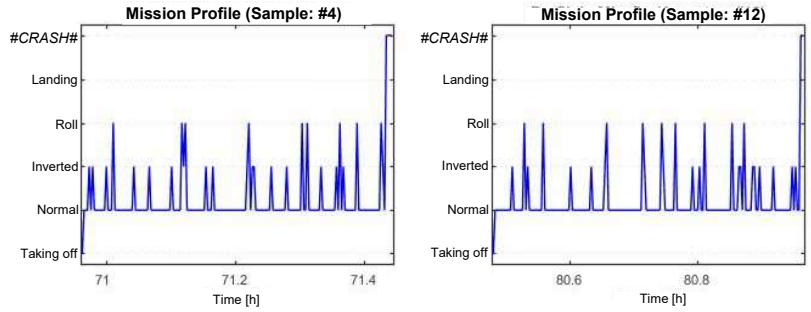


No gráfico da Figura 6.22 é possível identificar o tempo do ciclo de vida em que a queda ocorreu (no eixo "x") e qual era o volume total de combustível disponível na aeronave no instante da queda. Isso permite avaliar se a queda ocorreu devido à manobra executada com pouco combustível retido no tanque coletor, ou seja, devido às falhas ocultas das válvulas. Neste exemplo, é possível perceber que em um dos casos a queda ocorre pela manobra, já que ainda havia em torno de 20l de combustível; enquanto o segundo caso a queda ocorre pelo consumo total do combustível.

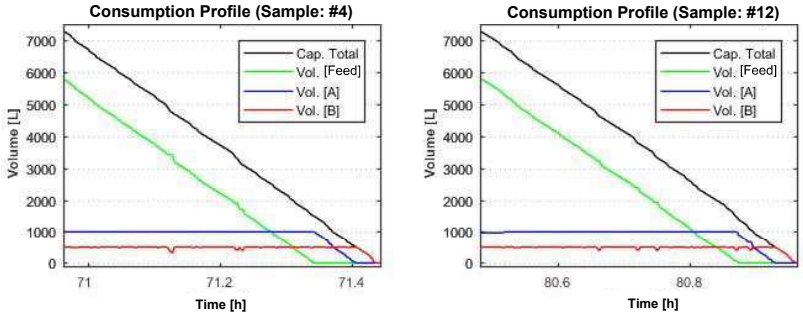
Para o mesmo caso da Figura 6.22, os perfis de voo das missões que resultaram na queda e o comportamento dos volumes de combustível podem ser analisados graficamente, conforme apresentado na Figura 6.23.

Nos gráficos da Figura 6.23a é possível perceber uma sequência maior de manobras invertidas próximo ao instante em que acaba o combustível dos tanques de alimentação, observável na Figura 6.23b. Dessa forma, as manobras mais severas ocorrem nos instantes mais críticos pelo baixo volume

Figura 6.23 – Exemplo de perfis de voo e volume em casos que ocorreu queda



(a) Perfis de voo



(b) Volumes

de combustível, resultando na queda. Nos perfis de missão em que não há uma frequência tão grande de voos, a chance de queda é significativamente menor, sendo verificável apenas com a realização de um grande número de simulações.

O ciclo de vida da aeronave é determinada pelo número de missões. Assim, um ciclo de vida de 2000h equivale a 4000 missões. Para obter amostras suficientes do método de Monte Carlo, é preciso realizar repetidas simulações para o ciclo de vida. O resultado obtido com 50 amostras de ciclos de vida de 2000h para os mesmo pesos das manobras está apresentado na Figura 6.24. Os pesos utilizados para os perfis de voo estão apresentados na Tabela 6.3 .

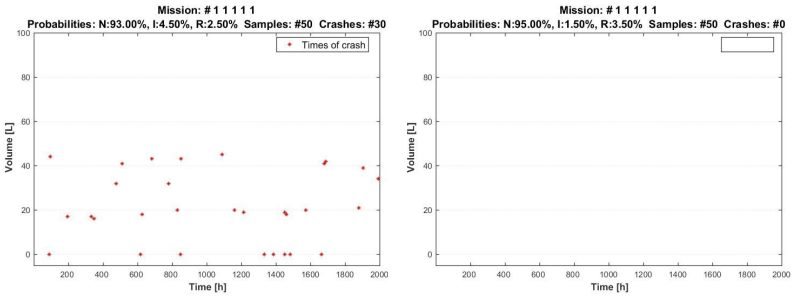
Pela Figura 6.24 é possível perceber a influência das manobras invertidas para a ocorrência de quedas das aeronaves. Para ambos os casos as características de ciclo de vida, números de válvulas e número de amostras são as mesmas. A diferença consiste basicamente nos pesos utilizados para o

sorteio das manobras. Na Figura 6.24a é possível perceber uma série de quedas devido tanto a manobras invertidas quanto pelo consumo total de combustível, enquanto na Figura 6.24b não há registro de quedas.

Tabela 6.3 Pesos das manobras utilizadas para simular o ciclo de vida de 2000h

	Perfil A	**Perfil B**
Normal	93%	95%
Invertido	1,5%	1,5%
Roll	3,5%	3,5%

Figura 6.24 – Resultado para ciclo de vida de 2000h



(a) Perfil com mais voos invertidos (b) Perfil com menos voos invertidos

Um outro exemplo de resultado, apresentado na Figura 6.25, traz uma simulação para o ciclo de vida de 2000h, mas com perfis de missão com probabilidade maior de voo invertido em relação ao "*roll*" que o simulado na Figura 6.24. Nesse caso, foram obtidas 100 amostras e houve a ocorrência de uma queda.

A Figura 6.26 apresenta resultados de simulação para 300 e 500 amostras (6.26a e 6.26b, respectivamente). A partir desses resultados percebe-se que os modelos de simulações são coerentes em relação à ocorrência de quedas. Levando-se em consideração o número de aviões construídos até o momento (em torno de 250 até 2018) e o fato de que não foram observadas quedas devido a falhas no tanque coletor, as quedas observadas nas simulações devem ser eventos raros, quando as manobras se aproximam de casos reais. No caso das 500 amostras, em particular, a queda foi observado na amostra 284, ou seja, todas as aeronaves construídas já deveriam ter os tanques trocados para que houvesse uma queda.

Realizando simulações como as apresentadas na Figura 6.27, utilizando os mesmos pesos para os sorteio dos perfis de voo, foi feita a comparação entre sistemas considerando diferentes tempos de ciclo de vida e números

Figura 6.25 – Simulação de voo em um perfil de missão com falhas abertas

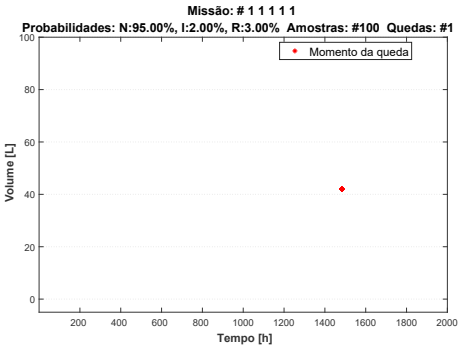
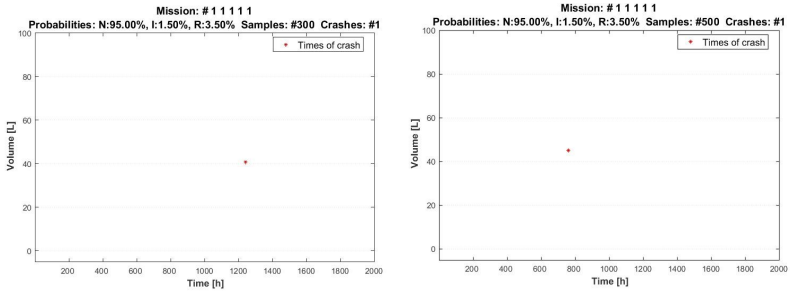


Figura 6.26 – Resultados de simulações para ciclo de vida de 2000h



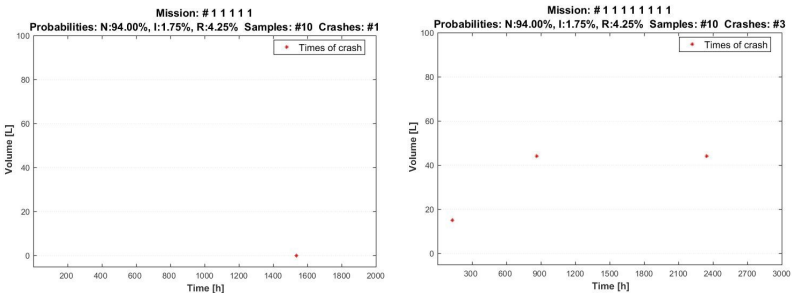
(a) 300 amostras (b) 500 amostras

de válvulas. Observou-se, por exemplo, que aumentando o ciclo de vida de 2000h para 3000h e aumentando as válvulas de 5 para 8, houve o aumento nas ocorrências de queda. Nos gráficos estão apresentados os pesos utilizados para os perfis de voo (94% normal, 1,75% invertido e 4,25% "*roll*") e a ocorrência de voos invertidos é baixa, semelhante ao ocorrido na Figura 6.24b.

Com base no volume de combustível no ponto onde houve a queda na Figura 6.27a, percebe-se que a queda ocorreu pelo consumo total do combustível. Na Figura 6.27b, entretanto, as quedas ocorreram durante as manobras invertidas, já que ainda havia combustível no sistema. Isso significa que mais válvulas resultam em mais falhas abertas e consequentemente, mais quedas em voos invertidos. O aumento do ciclo de vida aumenta também a chance de haver mais válvulas falhadas ao mesmo tempo. O modelo permite realizar outras variações do sistema, conforme a necessidade do projetista.

É importante ressaltar que normalmente as quedas devem ser situações

Figura 6.27 – Comparação de sistemas pela variação no número de válvulas



(a) Ciclo de vida de 2000h (b) Ciclo de vida de 3000h

raras. As simulações resultarão em casos isolados de quedas, que devem ser analisados em detalhes para verificar quais as circunstâncias e que a queda ocorreu. Para realizar essa análise, são realizadas simulações de missões separadamente, replicando as características que levaram às quedas, tais como ocorrências de falhas e sequências de manobras que compõem os perfis de missão.

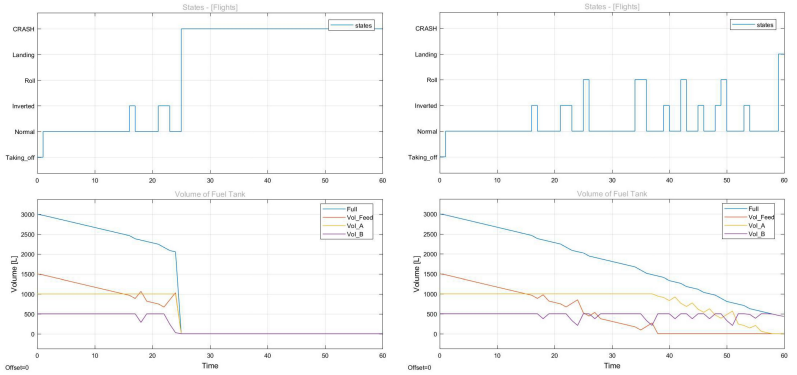
6.7.2 Simulações de missões

O resultados apresentados na Figura 6.28, são de casos distintos em que há duas falhas ocorridas antes do início de uma missão específica. No exemplo da Figura 6.28a, ambas as falhas são abertas. Nesse caso, é possível verificar que para o mesmo perfil de voo, a aeronave cai. Por fim, na Figura 6.28b, uma falha é aberta e a outra é fechada. Nesse caso, a aeronave não cai, mas é perceptível a variação do comportamento dos volumes de combustível quando comparado com o primeiro caso.

Os resultados das simulações apresentados na Figura 6.29 representam casos em que as falhas ocorrem durante o voo. Na Figura 6.28a, a falha é fechada e a aeronave consegue completar a missão. Porém, no no caso da Figura 6.28b, a aeronave cai, pois a falha ocorrida é aberta e o combustível na seção B do tanque coletor acaba antes do final da manobra invertida.

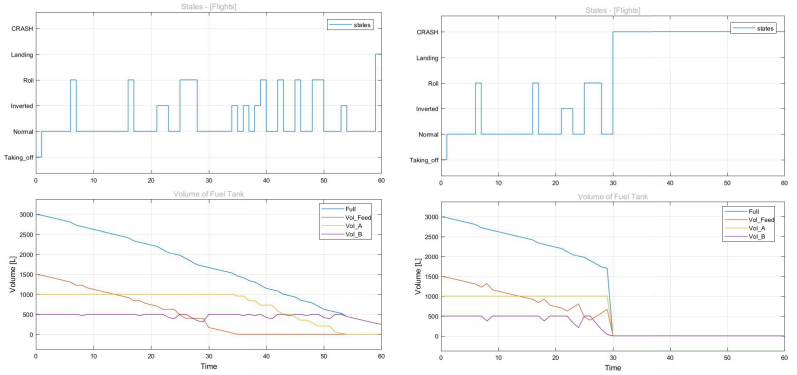
As simulações de missões permite verificar em detalhe como a aeronave se comporta em perfis de voo específicos. Na Figura 6.30 é apresentada uma simulação de missão com duração de 32 minutos e com três falhas abertas ocorridas. Observando os perfis de voo de cada missão é possível perceber que na quinta missão, em que ocorre a queda, há mais manobras de curta e longa duração. Dessa forma o consumo é maior e a aeronave cai.

Figura 6.28 – Resultados de missões com a ocorrência de falhas



(a) Duas válvulas abertas (b) Uma válvula falhada aberta e uma fechada

Figura 6.29 – Simulações de falhas ocorrendo durante os voos



(a) Válvula falha fechada (b) Válvula falha aberta

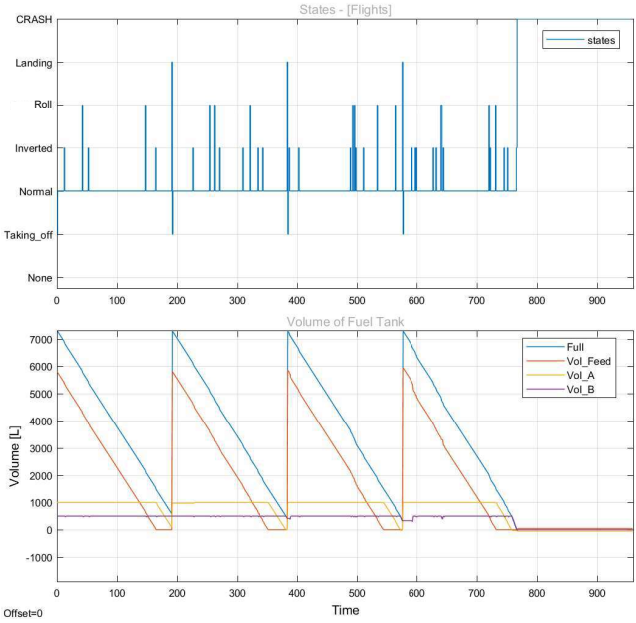
6.8 CONSIDERAÇÕES FINAIS

O presente capítulo apresentou a aplicação do método desenvolvido proposto na análise do tanque coletor.

As etapas iniciais consistiram na coleta e organização das informações referentes as características construtivas do sistema e às falhas dos componentes. As atividades desenvolvidas são comuns a outros métodos utilizados na analise de confiabilidade e risco.

Pelos aspectos gerais do sistema, o processo de análise funcional e de

Figura 6.30 – Exemplo de relação entre falhas e perfis de missão sobre a queda das aeronaves



análise de falhas é bastante simples.

Para o tanque coletor em especial, por se tratar de um sistema em que as válvulas mudam de estado (aberto e fechado) apenas como resposta execução de manobras, o relacionamento entre as falhas e a operação se mostrou bastante direta. A modelagem do comportamento do sistema, utilizando uma abordagem discreta a partir de pesos que definem a frequência das manobras se mostrou bastante satisfatória e clara de ser implementada.

A parte que exigiu maior esforço foi a modelagem da influência das manobras e falhas sobre a variável de controle "volume de combustível". AS vazões a ser consideradas são variáveis, em função do volume total de combustível da aeronave, dos modelos de válvulas utilizados, da ocorrência de falhas e das manobras executadas. A combinação de todas essas variáveis para determinar a contribuição de cada válvula para a variação dos volumes se mostrou bastante trabalhosa.

Os resultados gráficos resultantes das simulações são recursos bastante úteis para auxiliar na interpretação e eventuais tomadas de decisão sobre alterações do sistema. A forma que o método foi implementado permite testar

variações do sistema de forma prática e clara.

Por fim, a análise do sistema permitiu verificar pontos para eventuais melhorias do método de análise, além de permitir a identificação de outros sistemas análogos passíveis de serem usados para testar ainda mais a aplicabilidade do método.

7 CONCLUSÕES E RECOMENDAÇÕES PARA TRABALHOS FUTUROS

Nos capítulos iniciais deste documento, procurou-se evidenciar a necessidade de tratar as falhas ocultas de forma mais detalhada, integrando os aspectos operacionais dos sistemas ao contexto de ocorrência de falhas. Essa necessidade é ainda maior quando se considera as etapas de projeto de sistemas.

No Capítulo 2 foi apresentado o problema de aplicação da solução e que motivou o desenvolvimento desta pesquisa. Sistemas aeronáuticos representam muito bem as características altamente dinâmicas que tornam a análise de falhas ocultas ainda mais importante. Como foi explicitado no Capítulo 4 a ocorrência de uma falha é detectável ou não dependendo do momento da operação em que ela ocorre.

Outra questão muito importante das falhas ocultas, apresentado no Capítulo 3, é a dificuldade de prever possível cenários em que elas ocorrem. Como explicitado no capítulo, as decisões de projeto principalmente nas fases iniciais tem grande impacto sobre o produto final sem representar custos significativos para o ciclo de vida do produto. Por essa razão, torna-se importante analisar e tomar decisões sobre a confiabilidade e o risco de sistemas o mais cedo possível.

Entretanto, a falta de informações nas fases iniciais torna difícil prever esses cenários. Por essa razão, há grande interesse em contar com métodos de análise que forneçam mais e melhores informações para que os projetistas possam tomar as decisões necessárias.

O método desenvolvido para a análise de falhas ocultas a partir do projeto conceitual foi descrito no Capítulo 5. O método foi desenvolvido visando ser aplicável na análise de diferentes tipos de sistemas.

Para isso, foi adotada uma abordagem discreta que permite o monitoramento dos efeitos das diferentes transições de estado sobre uma variável de controle que define a falha total do sistema. A parte mais delicada do método é a análise comportamental do sistema e definição dos estados operacionais. Em alguns casos, estes estados são determinados apenas pela operação do sistema, em outros as transições ocorrem apenas em decorrência das falhas e por fim existem sistemas em que os estados operacionais são determinado pela combinação entre a ocorrência de falhas e a operação.

Para facilitar o entendimento de como abordar o sistema ao definir os estados operacionais, foram utilizados alguns exemplos de fácil entendimento. Entre estes exemplos está o problema de referência apresentado no Capítulo 4, utilizado para validar metodologias de análise de confiabilidade dinâmica.

O problema de evacuação de ambientes também foi utilizado para exemplificar o caso em que os estados operacionais são definidos pelos diferentes caminhos que podem ser tomados pelas pessoas. Este exemplo demonstra casos de sistemas em que a operação é bastante complexa e as transições de estado operacional do sistema são bastante variáveis.

A análise das falhas segue os mesmos métodos consolidados e utilizados amplamente tanto na academia quanto na indústria. O diferencial está no foco específico dado na identificação de potenciais falhas ocultas.

Como saídas da aplicação do método estão informações gráficas que permitem verificar como o sistema se comporta em diferentes cenários de ocorrência de eventos como falhas e transições operacionais, bem como alterando características de projeto, como o número de componentes ou o uso de componentes mais robustos.

Por fim, no Capítulo 6 foi apresentado o processo de aplicação do método desenvolvido na análise de falhas do tanque coletor de um avião de combate. Neste problema, todas as falhas dos componentes são ocultas, mas a análise se mostrou importante por permitir verificar que apesar de não ocorrer quedas na vida real, as aeronaves estão constantemente sujeitas a quedas dado o número de componentes falhados, mas as quedas não ocorrem devido as características de voo das aeronaves.

7.1 QUANTO AOS OBJETIVOS

O objetivo geral do trabalho foi desenvolver um método que permita analisar a ocorrência de falhas ocultas e seus impactos sobre os sistemas, na fase de projeto conceitual. Para estruturar o cumprimento do objetivo geral deste trabalho, foram definidos os seguintes objetivos específicos, detalhados no Capítulo 1:

- Caracterizar falhas ocultas em sistemas técnicos.
- Caracterizar os riscos decorrentes das falhas ocultas.
- Desenvolver modelo para o diagnóstico da ocorrência de falhas ocultas.
- Facilitar a análise da confiabilidade em projetos novos e em uso.
- Facilitar a análise das informações para estimar a confiabilidade.
- Contribuir com a metodologia de projeto PRODIP no que se refere aos atributos de confiabilidade e risco.

O método desenvolvido combina as falhas dos componentes de um sistema, seus efeitos sobre a variável de controle e as transições comportamentais. Pela definição de falhas ocultas, essa combinação permite verificar quando as falhas afetam ou não a operação do sistema, permitindo ou não sua detecção.

Além de permitir a identificação dos cenários de combinação de eventos que permeiam a ocorrência das falhas ocultas, o método permite ainda calcular a ocorrência de tais cenários.

O método foi estruturado para que os modelos desenvolvidos facilitem a análise das alterações de projeto sobre a ocorrência das falhas ocultas, por meio modelagem das funções e subfunções do sistema, integradas com a modelagem de ocorrência de falhas. Os efeitos das alterações de projeto foram testados na modelagem do tanque coletor, quanto ao número e modelos de válvulas, tempos de missão e ciclo de vida. Com isso, as possíveis concepções de projeto podem ser testadas e avaliadas nas fases iniciais de projeto.

Além disso, as limitações em relação às informação de falhas, típicas das fases iniciais de projeto, foram contornadas pelo uso do método de Monte Carlo, pela geração de cenários de combinações de eventos de falhas e operacionais. Em relação às premissas iniciais da tese, este resultado demonstrou potencial de uso do método desenvolvido, na análise de problemas diversos em que essas limitações estão presentes.

Por fim, o método contribui com metodologias de projeto por abordar de forma direta os requisitos de confiabilidade, risco e segurança nas fases inciais, principalmente a de projeto conceitual. A compreensão é que este método poderá ser utilizado tanto para projetos novos quanto nas ações de otimização de produtos, principalmente, os portadores de grande quantidade de energia, como é o caso do exemplo aplicado nesta tese.

7.2 RESULTADOS E CONTRIBUIÇÕES

O resultado principal do trabalho é o método que estrutura as etapas a serem seguidas e as atividades a serem desenvolvidas para que o objetivo final de analisar as falhas ocultas seja alcançado.

Ao longo do desenvolvimento do método, buscou-se definir as técnicas a serem utilizadas para auxiliar no desenvolvimento das atividades, bem como estabelecer de forma clara, por meio de exemplos, como os diferentes sistemas devem ser abordados.

Na análise de confiabilidade utilizando técnicas consagradas como FMEA e FTA, é comum nos depararmos com a variabilidade dos resultados das análises principalmente devido a variedade de interpretações que podem ser dadas para um mesmo sistema. A geração de cenários resultante do método

se integra claramente com o uso da FMEA e FTA, pois oferece uma visão ampliada das relações causa/efeito tanto das ocorrência dos modos de falha quanto das transições de oepração do sistema.

A estrutura do método em etapas e atividades estabelece como os estados operacionais do sistema devem ser definidos. Dessa forma, contribui com o melhor entendimento sobre a abordagem dada ao sistema e permite a utilização do método em diferentes tipos de aplicação, como as exemplificadas no Capítulo 5,.

A possibilidade de simular diferentes características dos componentes, além de contribuir com o projeto, contribui com o desenvolvimento de fornecedores. Isso porque pode-se testar diferentes taxas de falhas de componentes, por exemplo, e definir quais as metas de confiabilidade dos componentes a serem adquiridos de fornecedores.

Vale ressaltar que o método contribui para verificar se, como decisão de projeto, convém considerar a possibilidade de reduzir o tempo definido para a substituição do tanque, ou se ainda é possível estender sua vida útil; relacionar falhas ocorridas e o tipo de manobra que o piloto pode verificar; e ainda a partir do número de válvulas, taxa de falha e tempo entre as falhas, a probabilidade de ocorrência de possíveis eventos de falha da aeronave.

O método ainda pode ser utilizado para avaliar o impacto da manutenção sobre a ocorrência de falhas no sistema. Isso poderia ser feito, por exemplo, atribuindo eventuais falhas oriundas de procedimentos incorretos (com uma taxa de ocorrência atribuída), como a contaminação do combustível ou instalação invertida nas válvulas. Ao mesmo tempo que essas falhas de procedimento inserem falhas no sistemas, a manutenção permite a detecção das falhas ocultas.

Por fim, uma das grandes vantagens de utilizar o método é a velocidade alcançada para executar as simulações. Uma manobra da aeronave, representada como um evento discreto, tem uma duração longa definida como dado de entrada do modelo, porém na simulação a transição entre as manobras ocorre de forma instantânea uma vez que os cálculos e atualizações dos volumes são realizados. Dessa forma, poucos segundos de simulação representam horas da vida real do sistema. Essa velocidade permite obter grandes amostras em curtos espaços de tempo. Além disso, os modelos não requerem grande esforço computacional para ser simulados.

7.3 RECOMENDAÇÕES PARA TRABALHOS FUTUROS

- **Considerar níveis de degradação**. A aplicação da análise no tanque coletor considerou as falhas sujeitas a apenas dois modos de falha, aberto

ou fechado. Com isso o efeito sobre o sistema é direto, permitindo ou não a vazão de combustível. Por essa razão, é recomendável realizar a análise considerando diferentes níveis de degradação que resultam em vazões parciais de combustível. Dessa forma, o comportamento dos volumes é alterado e se aproxima mais de eventuais cenários reais. Além disso, essa características altera a capacidade de recuperação dos volumes na execução de manobras.

- **Desenvolver testes específico para informações de análise de falha oculta**. A dependência de dados para realizar análise de falha, principalmente falhas ocultas é a principal dificuldade encontrada. Por não serem detectadas, os dados de falhas ocultas não são registrados imediatamente após sua ocorrência. Uma saída é desenvolver procedimentos de teste que permitam levantar os dados de falha dos componentes passíveis de sofre falhas ocultas para alimentar os dados necessários para aplicação do método desenvolvido neste trabalho.

- **Aplicar o método na análise do problema de referência considerando controlador ativo**. O problema do reservatório é baseado em um sistema real de resfriamento de reator nuclear. Uma forma de melhorar a detecção das falhas ocultas nos componentes seria tornar o controlado um elemento ativo, que comanda a troca periódica da bomba que está ligada pela bomba em *stand by*. Com a simulação desse caso pode-se avaliar os benefícios de implementar essa alteração no projeto do sistema.

- **Aplicar o modelo na análise da evacuação de ambientes**. O projeto de ambientes com aglomeração de pessoas deve seguir normas bem estabelecidas quanto as saídas de emergência. Porém, um aspecto muito significativo em situações de emergência, como incêndio é a capacidade das pessoas tomarem decisão sob situações de perigo. A utilização do método para a análise desse tipo de situação permite avaliar se as normas satisfazem os requisitos de tempo de evacuação, levando em consideração o atraso das pessoas ao tomar as decisões.

- **Utilizar o método para modelo de diagnóstico de falhas de sistemas**. Como o método consiste em combinar transições de estados relacionados às falhas e à operação do sistema, obtendo-se grandes amostras aleatórias a partir de poucos dados, pode-se utilizá-lo para coletar as probabilidades condicionais que alimentam sistemas de diagnóstico de falha, baseado por exemplo em redes bayesianas. A grande dificuldade de se utilizar sistemas como esse está justamente na coleta das probabilidades de falha *a priori*, que normalmente é feita a partir da consulta de

especialistas. Porém em sistemas com grande complexidade a estimativa das probabilidade se torna inviável.

REFERÊNCIAS

ALBINALI, H. F.; MELIOPOULOS, A. Hidden failure detection via dynamic state estimation in substation protection systems. In: IEEE. *Saudi Arabia Smart Grid COnference(SASG)*. Saudi Arabia, 2017. p. 1–6. **Proceedings ...**

ALMEIDA, J. C. *Uma metododologia de projeto baseada na confiabilidade - aplicação á redes de distribuição de gás canalizada*. Dissertação (Mestrado em Engenharia Mecânica) — Universidade Federal de Santa Catarina (UFSC), Florianópolis, 1999.

ALONÇO, A. S. *Metodologia de projeto para a concepção de máquinas agrícolas seguras*. 221 p. Tese (Doutorado em Engenharia Mecânica) — Universidade Federal de Santa Catarina (UFSC), Florianópolis, 2004.

AMIN, M. T.; KHAN, F.; IMTIAZ, S. Dynamic availability assessment of safety critical systems using a dynamic bayesian network. *Reliability Engineering & System Safety*, Elsevier BV, v. 178, p. 108–117, 2018. <https://doi.org/10.1016/j.ress.2018.05.017>.

ANDERSON, J. A. *Automata theory with modern applications*. [S.l.]: Cambridge University Press, 2006.

ASIMOV, M. *Introduction to design*: fundamentals of engineering dsign. New Jersey: Prentice Hall, 1962.

ASSIS, R. Periodicidade óptima de inspecções na procura de falhas ocultas. In: *Encontro Nacional de Riscos, Segurança e Fiabilidade*. [S.l.: s.n.], 2012.

AVONTUUR, G. C.; WERFF, K. van der. An implementation of reliability analysis in the conceptual design phase of drive trains. *Reliability Engineering & System Safety*, Elsevier, v. 73, n. 2, p. 155–165, 2001.

BACK, N. *Metodologia de projeto de produtos industriais*. Rio de Janeiro: Guanabara Dois, 1983.

BACK, N.; OGLIARI, A.; DIAS, A.; SILVA, J. C. *Projeto integrado de produtos*: planejamento, concepção e modelagem. 1. ed. São Paulo: Editora Manole Ltda., 2008. 601 p.

BAI, Z.; LI, X.; TAN, R.; LIAN, B. A function failure analysis method for improving reliability of the product based on go-flow methodology. In: IEEE. *IEEE International Conference on Industrial Engineering and Engineering Management, 2008. IEEM 2008*. Singapore, 2008. p. 550–555.

BARBU, V. S.; LIMNIOS, N. *Semi-Markov Chains and Hidden Semi-Markov Models toward Applications*. 1. ed. New York: Springer-Verlag New York, 2008. 226 p.

BIASOTTO, E. *Sistema de governo do navio Itabuna*: Estudo de confiabilidade do sistema hidráulico de acionamento do leme. Florianópolis, 2008. Relatório final para Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq).

BILLINTON, R.; ALLAN, R. N. *Reliability Evaluation of Engineering Systems*: Concepts and techniques. New York: Plenun Press, 1992.

BLANCHARD, B. S.; FABRYCKY, W. J. *Systems engineering and analysis*. New Jersey: Prentice Hall, 1981.

CALIL, L. F. P. *Metodologia para análise de risco: foco na segurança e na continuidade*. Tese (Doutorado em Engenharia Mecânica) — Universidade Federal de Santa Catarina (UFSC), Florianópolis, 2009.

CASSANDRAS, C. G.; LAFORTUNE, S. *Introduction to Discrete Event Systems*. 2. ed. New York: Springer US, 2008. 772 p.

CODETTA-RAITERI, D.; BOBBIO, A. Stochastic petri nets supporting dynamic reliability evaluation. *International Journal of Materials & Structural Reliability*, v. 4, n. 1, p. 65–77, 2006.

CURY, J. E. R. Teoria de controle supervisório de sistemas a eventos discretos. *V Simpósio Brasileiro de Automação Inteligente (Minicurso)*, 2001.

DIAS, A. *Metodologia para análise da confiabilidade em freios pneumáticos automotivos*. Tese (Doutorado em Engenharia Mecânica) — Universidade Estadual de Campinas (UNICAMP), Campinas, 1996.

DIAS, A.; CALIL, L. F. P.; RIGONI, E.; SAKURADA, E. Y.; OGLIARI, A.; KAGUEIAMA, H. A. *Metodologia para análise de risco*: Mitigação de perda de SF_6 em disjuntores. 1. ed. Florianópolis, SC: Nova Letra Gráfica & Editora, 2011. 1304 p. ISBN: 978-85-98128-42-9.

GASCARD, E.; SIMEU-ABAZI, Z. Quantitative analysis of dynamic fault trees by means of monte carlo simulations: Event-driven simulation approach. *Reliability Engineering & System Safety*, Elsevier, 2018.

GAVEL, H. *On aircraft fuel systems : conceptual design and modeling*. Tese (Doutorado) — Linköping University, The Institute of Technology, Linköping, 2007.

GUIMARÃES, L. d. S. *Gerenciamento de Riscos e Segurança de Sistema*. 1. ed. São Paulo: iEditora, 2003.

HASKINS, C.; FORSBERG, K.; KRUEGER, M.; WALDEN, D.; HAMELIN, D. *Systems engineering handbook*: A guide for system life cycle processes and activities. 3. ed. San Diego, 2006.

HERSMAN, D. A.; HART, C. A.; SUMWALT, R. L. *Loss of Thrust in Both Engines After Encountering a Flock of Birds and Subsequent Ditching on the Hudson River*: Accident report ntsb/aar-10/03. Washington DC, 2010.

HIRSHORN, S. R.; VOSS, L. D.; BROMLEY, L. K. Nasa systems engineering handbook. 2017.

HOKSTAD, P.; FRØVIG, A. T. The modelling of degraded and critical failures for components with dormant failures. *Reliability Engineering & System Safety*, Elsevier, v. 51, n. 2, p. 189–199, 1996.

ISERMANN, R. *Fault-Diagnosis Systems*: An introduction from fault detection to fault tolerance. 1. ed. New York: Springer, 2005. 475 p. ISBN 3540241124.

JIA, Y.; XU, Z.; LAI, L. L.; WONG, K. P. Risk-based power system security analysis considering cascading outages. *IEEE Transactions on Industrial Informatics*, v. 12, n. 2, p. 872–882, April 2016. ISSN 1551-3203.

JOHANSSON, C. *On System Safety and Reliability in Early Design Phases : Cost Focused Optimization Applied on Aircraft Systems*. 62 p. Tese (Doutorado) — Linköping University, The Institute of Technology, 2013.

KAGUEIAMA, H. A. *Sistematização de técnicas de análise de falha e projeto para confiabilidade*. Dissertação (Mestrado em Engenharia Mecânica) — Universidade Federal de Santa Catarina (UFSC), Florianópolis, 2012.

KAGUEIAMA, H. A.; DIAS, A.; ÖLVANDER, J. Hidden failure characterization and the influence of system dynamic behavior. In: *International Conference On Probabilistic Safety Assessment and Management (PSAM), 13*. Seoul: IAPSAM, 2016. **Proceedings ...**

____. Hidden failure scenarios of an aircraft collector fuel tank. In: *Aerospace Tachnology 2016*. Solna: [s.n.], 2016. **Proceedings ...**

KLEYNER, A.; VOLOVOI, V. Application of petri nets to reliability prediction of occupant safety systems with partial detection and repair. *Reliability Engineering & System Safety*, Elsevier, v. 95, n. 6, p. 606–613, 2010.

KMENTA, S.; ISHII, K. Advanced fmea using meta behavior modeling for concurrent design of products and controls. In: *ASME design engineering technical conferences*. Atlanta: ASME, 1998. **Proceedings...**

KRISTIANSEN, S. *Maritime transportation: safety management and risk analysis*. [S.l.]: Routledge, 2013.

KUMAMOTO, H.; HENLEY, E. J. *Probabilistic risk assessment and management for engineers and scientist*. 2ª. ed. New York: IEEE Press Marketing, 1996. ISBN 0780310047.

LANGTON, R.; CLARK, C.; HEWITT, M.; RICHARDS, L. *Aircraft fuel systems*. New Jersey: John Wiley & Sons, 2009.

LIENHARDT, B.; HUGUES, E.; BES, C.; NOLL, D. Failure-finding frequency for a repairable system subject to hidden failures. *AIAA Journal of Aircraft*, v. 45, n. 5, p. 1804–1809, 2008.

LIMBOURG, P.; KOCHS, H.-D. Multi-objective optimization of generalized reliability design problems using feature model: A concept for early design stages. *Reliability Engineering & System Safety*, Elsevier, v. 93, n. 6, p. 815–828, 2008.

LIU, B.; YEH, R.-H.; XIE, M.; KUO, W. Maintenance scheduling for multicomponent systems with hidden failures. *IEEE Transactions on Reliability*, IEEE, v. 66, n. 4, p. 1280–1292, 2017.

MARSEGUERRA, M.; ZIO, E. Monte carlo approach to psa for dynamic process systems. *Reliability Engineering & System Safety*, Elsevier, v. 52, n. 3, p. 227–241, 1996.

MARSEGUERRA, M.; ZIO, E.; DEVOOGHT, J.; LABEAU, P.-E. A concept paper on dynamic reliability via monte carlo simulation. *Mathematics and Computers in simulation*, Elsevier, v. 47, n. 2-5, p. 371–382, 1998.

MAURINO, D.; REASON, J.; JOHNSTON, N.; LEE, R. *Beyond aviation human factors*. 1. ed. London: Routledge, 1995. ISBN 9781351955706.

MIHALYI, L. *Multi objective optimization and probabilistic design on aircraft fuel system*. Dissertação (Mestrado em Engenharia Espacial) — Lulea University of Technology, Lulea, 2007.

MOSLEH, A.; DIAS, A. *Towards an integrated methodology for identification, classification, and assessment of aviation systems hazards*. Washington, 2004. Final Report. Center for Technology Risk – Studies.

MOSLEH, A.; DIAS, A.; EGHBALI, G.; FAZEN, K. An integrated framework for identification, classification, and assessment of aviation systems hazards. In: *International Conference On Probabilistic Safety Assessment and Management (PSAM), 7*. Berlin: IAPSAM, 2004. **Proceedings ...**

MOUBRAY, J. *Reliability-centred Maintenance*. 2. ed. Norwalk: Industrial Press, Inc., 1997. ISBN 9780750633581.

NOWLAN, F.; HEAP, H. *Reliability-centered Maintenance*. Dolby Access Press, 1978. <https://books.google.com.br/books?id=ztQeAQAAIAAJ>.

NUNES, E. L. *Manutenção centrada em confiabilidade (MCC): análise da implantação em uma sistemática de manutenção preventiva consolidada*. Tese (Doutorado em Engenharia Mecânica) — Universidade Federal de Santa Catarina (UFSC), Florianópolis, 2001.

ORMON, S. W.; CASSADY, C. R.; GREENWOOD, A. G. A simulation-based reliability prediction model for conceptual design. In: IEEE. *Reliability and Maintainability Symposium*. Philadelphia, 2001. p. 433–436.

PAHL, G.; BEITZ, W. *Konstruktionslehre*. Berlin: Springer Verlag, 1977.

PORCIÚNCULA, G. S. *Metodologia para análise de confiabilidade no projeto de sistemas automáticos*. Tese (Doutorado em Engenharia Mecânica) — Universidade Federal de Santa Catarina (UFSC), Florianópolis, 2009.

RAYMER, D. *Aircraft Design: A Conceptual Approach*. 5. ed. Washington: American Institute of Aeronautics and Astronautics, Inc., 2012.

REBELLO, S.; YU, H.; MA, L. An integrated approach for system functional reliability assessment using dynamic bayesian network and hidden markov model. *Reliability Engineering & System Safety*, Elsevier BV, 2018. <https://doi.org/10.1016/j.ress.2018.07.002>.

REINO UNIDO. Health And Safety Executive (HSE). Department For Work And Pensions. *Core topic 2: HF in accident investigations*. Liverpool, 2017. <http://www.hse.gov.uk/humanfactors/topics/core2.pdf>. Acessado em 23 nov. 2017.

SADOU, N.; DEMMOU, H. Reliability analysis of discrete event dynamic systems with petri nets. *Reliability Engineering & System Safety*, Elsevier, v. 94, n. 11, p. 1848–1861, 2009.

SADRAEY, M. H. *Aircraft design: A systems engineering approach*. New Jersey: John Wiley & Sons, 2012. 808 p. ISBN 978-1-119-95340-1.

SAFAVI, E. *Collaborative Multidisciplinary Design Optimization : A Framework Applied on Aircraft Systems and Industrial Robots*. 56 p. Tese (Doutorado) — Linköping University, The Institute of Technology, 2013.

SAFAVI, E.; GOPINATH, V.; ÖLVANDER, J.; GAVEL, H. A collaborative tool for conceptual aircraft systems design. In: *AIAA Modeling and simulation technologies conference*. Minneapolis: AIAA, 2012. p. 4716.

SAKURADA, E. Y. *As técnicas de análise dos modos de falhas e seus efeitos e análise de Ã¡rvore de falhas no desenvolvimento e na avaliação do produto*. Dissertação (Mestrado em Engenharia Mecânica) — Universidade Federal de Santa Catarina (UFSC), Florianópolis, 2001.

SAKURADA, E. Y. *Metodologia para análise de confiabilidade dinâmica*. Tese (Doutorado em Engenharia Mecânica) — Universidade Federal de Santa Catarina (UFSC), Florianópolis, 2013.

SIMEU-ABAZI, Z.; MASCOLO, M. D.; KNOTEK, M. Fault diagnosis for discrete event systems: Modelling and verification. *Reliability Engineering & System Safety*, Elsevier, v. 95, n. 4, p. 369–378, 2010.

SINTEF INDUSTRIAL MANAGEMENT. *OREDA*: Offshore reliability data. 4th. ed. Trondheim, 2002.

SMITH, D. J.; SIMPSON, K. G. *Functional Safety: A straightforward guide to applying IEC 61508 and related standards*. New York: Routledge, 2004.

TAGHIPOUR, S.; BANJEVIC, D. Periodic inspection optimization models for a repairable system subject to hidden failures. *IEEE Transactions on Reliability*, IEEE, v. 60, n. 1, p. 275–285, 2011.

____. Optimal inspection of a complex system subject to periodic and opportunistic inspections and preventive replacements. *European Journal of Operational Research*, Elsevier, v. 220, n. 3, p. 649–660, 2012.

ULLMAN, D. G. *The mechanical design process*. New York: McGraw-Hill, 1992.

USA (United States of America). DOD (Department of Defense). *MIL-STD-721C*: Definitions of terms for reliability and maintainability. Washington, 1981.

VERAS, R. M. *Uma sistemática para análise de degradação de sistemas técnicos*. Dissertação (Mestrado em Engenharia Mecânica) — Universidade Federal de Santa Catarina (UFSC), Florianópolis, 2016.

WANG, W.; CAMMI, A.; MAIO, F. D.; LORENZI, S.; ZIO, E. A monte carlo-based exploration framework for identifying components vulnerable to cyber threats in nuclear power plants. *Reliability Engineering & System Safety*, Elsevier, v. 175, p. 24–37, 2018.

ZAYTOON, J.; LAFORTUNE, S. Overview of fault diagnosis methods for discrete event systems. *Annual Reviews in Control*, Elsevier, v. 37, n. 2, p. 308–320, 2013.

ZIO, E. *The Monte Carlo simulation method for system reliability and risk analysis*. 1. ed. London: Springer-Verlag, 2013. ISBN 9781447145882.