MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES
INSTITUTO NACIONAL DE PESQUISAS ESPACIAIS

sid.inpe.br/mtc-m21b/2018/02.08.18.35-PUD

DEPENDABILIDADE EM SISTEMAS ESPACIAIS E ANÁLISE DE FALHAS REAIS EM SATÉLITES

Roberta de Cássia Ferreira Porto

Monografia de Qualificação de Doutorado do Curso de Pós-Graduação em Engenharia e Tecnologias Espaciais/Engenharia e Gerenciamento de Sistemas Espaciais, orientada pelo Dr. Marcelo Lopes de Oliveira e Souza.

URL do documento original:
<http://urlib.net/8JMKD3MGP3W34P/3QGKDJP>

INPE
São José dos Campos
2018

PUBLICADO POR:

Instituto Nacional de Pesquisas Espaciais - INPE
Gabinete do Diretor (GBDIR)
Serviço de Informação e Documentação (SESID)
Caixa Postal 515 - CEP 12.245-970
São José dos Campos - SP - Brasil
Tel.:(012) 3208-6923/6921
E-mail: pubtc@inpe.br

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES
INSTITUTO NACIONAL DE PESQUISAS ESPACIAIS

sid.inpe.br/mtc-m21b/2018/02.08.18.35-PUD

DEPENDABILIDADE EM SISTEMAS ESPACIAIS E ANÁLISE DE FALHAS REAIS EM SATÉLITES

Roberta de Cássia Ferreira Porto

Monografia de Qualificação de Doutorado do Curso de Pós-Graduação em Engenharia e Tecnologias Espaciais/Engenharia e Gerenciamento de Sistemas Espaciais, orientada pelo Dr. Marcelo Lopes de Oliveira e Souza.

URL do documento original:
<http://urlib.net/8JMKD3MGP3W34P/3QGKDJP>

INPE
São José dos Campos
2018

RESUMO

Esta monografia objetiva apresentar conceitos da Dependabilidade em sistemas e relacioná-los com algumas disciplinas do curso de Engenharia e Tecnologias Espaciais, área de concentração Engenharia e Gerenciamento de Sistemas Espaciais. A monografia apresenta um levantamento de falhas reais do subsistema de suprimento de energia de dois satélites em forma de estudo de caso. Estes estudos de casos são apresentados como um exemplo da aplicação dos conceitos adquiridos no decorrer do curso e descrevem as possíveis causas das falhas relatadas, suas consequências, ações utilizadas para evitar de forma *a priori* e ações para tolerar/corrigir falhas *a posteriori* e/ou restabelecer o sistema. São listados alguns trabalhos atuais correlatos ao tema, que tratam de análise, tratamento ou predição de falhas existentes na literatura. Esta monografia destaca a importância e relevância à temática de falhas para garantir a dependabilidade em sistemas. Mostra que muitos trabalhos vêm sendo estudados, mas ainda há muito por fazer, o que leva a uma grande motivação para desenvolver a tese de doutorado nesta vertente. A conclusão que se obtém com a realização deste trabalho é que conceber com sucesso um sistema dependável é uma questão desafiadora, assunto de investigação em andamento na literatura.

Palavras-chave: Dependabilidade em Sistemas. Confiabilidade. Falhas. Subsistema de suprimento de energia.

LISTA DE FIGURAS

Pág.

LISTA DE TABELAS

Pág.

LISTA DE SIGLAS E ABREVIATURAS

AOCS	Attitude and Orbit Control Subsystem (Subsistema de controle de atitude e Órbita)
BAT	Battery (Bateria)
BCC	Battery charge Controller (Controle de Carga da Bateria)
BDR	Battery Discharge Regulator (Regulador de Carga e Descarga da Bateria)
DOD	Depth of Discharge (Profundidade de Descarga)
EOC	End of Charge (Fim de carga)
ETA	Event Tree Analysis (Análise da Árvore de Eventos)
FDI	Failure Detection and Isolation (Detecção e Isolamento de Falhas)
FDIR	Failure Detection, Isolation and recovery (Detecção, Isolamento e Recuperação de Falhas)
FMEA	Failure Modes and Effects Analysis (Análise dos Modos de Falhas e Efeitos)
FMECA	Failure Modes, Effects and Criticality Analysis (Análise dos Modos de Falhas, Efeitos e Criticidade)
FTA	Faul Tree Analysis (Análise de Árvore de Falhas)
INPE	Instituto Nacional de Pesquisas Espaciais
MTBF	Mean Time Between Failures (Tempo médio entre falhas)
MTTF	Mean Time To Failure (Tempo Médio Para a Falha)
MTTR	Mean Time To Repair (Tempo Médio Para Reparo)
PCU	Power Conditioning Unit (Unidade de Condicionamento de Potência)
PDU	Power Distribution Unit (Unidade Distribuidora de Potência)
PPS	Power Supply Subsystem (Subsistema de Suprimento de energia)
RAM	Reliability, Availability e Maintainability (Confiabilidade, disponibilidade e Manutenabilidade)
RBD	Reliability Block Diagram (Diagrama de Blocos de Confiabilidade)

S1	Satélite 1
S2	Satélite 2
SAG	Solar Array Generator (Gerador Solar/Painel Solar)
SAG1	Painel Solar 1
SAG2	Painel Solar 2
V/T	Curvas de tensão final de carga (voltage), compensadas em temperatura (temperature)

SUMÁRIO

Pág.

1 INTRODUÇÃO

Com a crescente evolução da tecnologia, evidenciou-se a grande necessidade de se prever falhas nos componentes utilizados em produtos pois, cada vez mais, as organizações realizam operações em ambientes de alto risco. Um exemplo disso são os sistemas de satélites, aviões, automóveis e controles de tráfego aéreo que estão se tornando cada vez mais complexos e/ou altamente integrados, integrando várias tecnologias e operando em ambientes extremamente exigentes.

Com tal evolução, a indústria aeroespacial tornou-se um dos principais usuários e beneficiários da Engenharia de Sistemas, estimulando e desenvolvendo produtos e ferramentas cada vez mais poderosos. Uma das mais relevantes é a Dependabilidade, que inclui a análise de Confiabilidade, Disponibilidade e Manutenabilidade, entre outros tópicos de suma importância.

Nesta monografia são apresentados os conceitos básicos da Dependabilidade de sistemas espaciais, assim como uma análise de falhas reais ocorridas em satélites, ambas com base em disciplinas cursadas na pós-graduação do Instituto Nacional de Pesquisas Espaciais, detalhadas na Tabela 1.1.

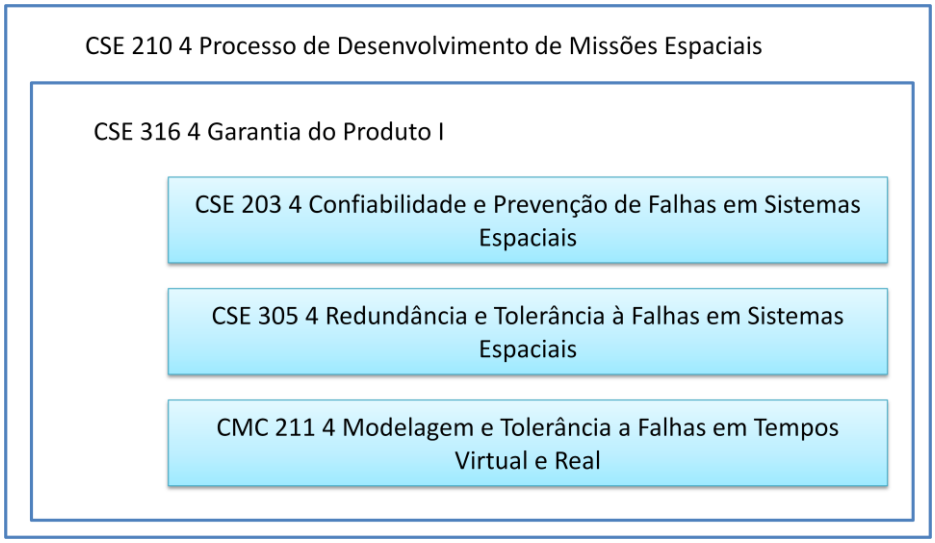
Tabela 1.1 – Disciplinas do Curso de Pós Graduação do INPE selecionadas como base de conhecimento para esta monografia.

CSE-203-4	Confiabilidade e Prevenção de Falhas em Sistemas Espaciais
CSE-305-4	Redundância e Tolerância a Falhas em Sistemas Espaciais
CSE-316-4	Garantia do Produto de Sistemas Espaciais I
CMC-211-4	Modelagem e Tolerância a Falhas em Tempos Virtual e Real
CSE-210-4	Processo de Desenvolvimento de Missões Espaciais

As disciplinas selecionadas são altamente relacionadas entre si, como pode ser visualizado na Figura 1.1. A disciplina Processo de Desenvolvimento de Missões Espaciais (CSE-210-4) é abrangente, aborda os modelos e fases de desenvolvimento; revisões, organizações e atividades de projeto; atividades de engenharia de sistema; assim como

conceitos de garantia do produto e cálculos de Confiabilidade adotados nos projetos. A disciplina Garantia do Produto (CSE-316-4), por sua vez, trata de aspectos de prevenção e tolerância de falhas, tópicos que são aprofundados nas outras três disciplinas selecionadas.

Figura 1.1 – Relação entre as disciplinas selecionadas.



1.1. Objetivo

O objetivo deste documento é desenvolver uma monografia e submetê-la ao Exame de Qualificação de Doutorado do Curso de Pós-Graduação em Engenharia e Tecnologias Espaciais (ETE) área de concentração em Engenharia e Gerenciamento de Sistemas Espaciais (CSE).

Segundo o regimento ETE/CSE, o Exame de Qualificação de Tese consta de uma exposição oral de uma monografia escrita com foco em conceitos básicos consistentes com o assunto da futura tese e deve avaliar a amplitude e a profundidade dos conhecimentos e a capacidade crítica do aluno.

1.2. Organização do trabalho

O capítulo 2 desta monografia de Qualificação de Doutorado é destinado à apresentação dos conceitos básicos referentes à Dependabilidade em Sistemas, suas métricas, assim como abordagens e técnicas objetivas, que são utilizadas para alcançar a dependabilidade dos sistemas aeroespaciais e automotivos. Neste capítulo os conceitos apresentados

são relacionados com algumas disciplinas cursadas no Curso de Pós-Graduação em ETE do INPE, disciplinas detalhadas na Tabela 1.1.

O capítulo 3 está em concordância com todas as disciplinas listadas na Tabela 1.1. Este capítulo aborda um estudo de casos relatando falhas reais no subsistema de suprimento de energia de satélites. Este estudo de caso é apresentado como um exemplo da aplicação dos conceitos adquiridos no decorrer do curso e procura levantar/avaliar:

- As causas das falhas;
- As consequências das falhas;
- Ações utilizadas para evitar/tolerar de forma *a priori*;
- Ações para corrigir e restabelecer o sistema.

O estado da arte é apresentado no capítulo 4, neste capítulo são listados alguns dos trabalhos pesquisados que tratam de assuntos correlatos ao tema apresentado nesta monografia: Dependabilidade em sistemas Espaciais e análise de falhas. Este capítulo objetiva destacar a importância do assunto e o quão tem sido investigado e estudado na literatura.

E por último são apresentadas as conclusões deste documento.

2 CONCEITOS BÁSICOS E REVISÃO BIBLIOGRÁFICA

Neste capítulo os conceitos básicos são apresentados e complementados por definições adicionais. Caracteres em negrito são usados quando um termo é definido, enquanto que caracteres em itálico é um convite para chamar a atenção do leitor. A correspondência das definições com cada uma das disciplinas mencionadas nesta monografia é destacada no decorrer deste capítulo.

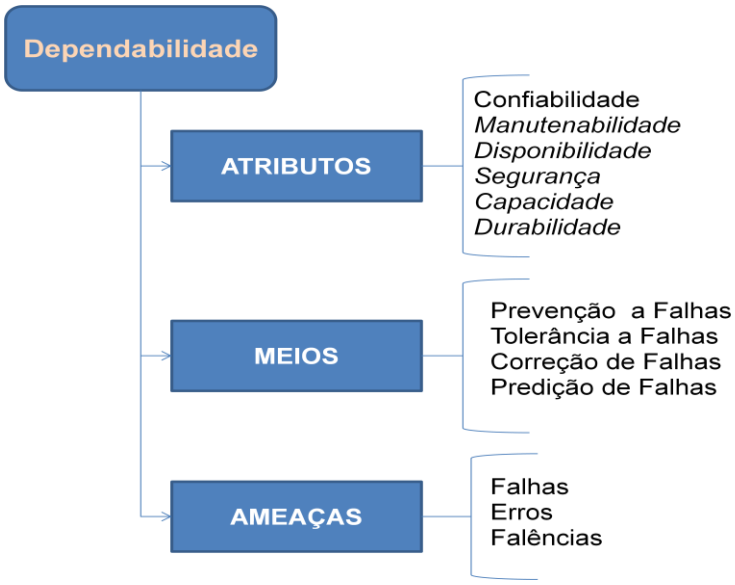
2.1. Dependabilidade

Nas disciplinas CSE-203-4 (Confiabilidade e Prevenção de Falhas em Sistemas Espaciais), CSE-305-4 (Redundância e Tolerância a Falhas em Sistemas Espaciais), CMC-211-4 (Modelagem e Tolerância a Falhas em Tempos Virtual e Real) e CSE-316-4 (Garantia do Produto de Sistemas Espaciais I) foram abordados os conceitos de Dependabilidade.

Dependabilidade é um termo muito utilizado na década de 80 e 90 em sistema de computadores, em softwares. No entanto, é relativamente novo em Engenharia de Sistemas e, nos últimos anos vem ganhando destaque na Engenharia e Garantia de Sistemas.

Avizienis, et al. (2004), e outros autores, discutem em suas publicações os conceitos fundamentais de Dependabilidade aplicados a sistemas de computação. Neste documento é salientado os conceitos que se aplicam a sistemas espaciais, como por exemplo, a divisão que os autores fazem de Dependabilidade em três partes: os atributos de dependabilidade; as ameaças (obstáculos para alcançar a Dependabilidade) e os meios para alcançá-la, ilustrados na Figura 2.1.

Figura 2.1 – Árvore de Dependabilidade.



Fonte: Adaptado de Avizienis, et al. (2004)

Dependabilidade é uma métrica vetorial composta por outras métricas escalares que são extremamente importantes para a tomada de decisões. (SOUZA e PORTO 2016) Pode ser interpretada como uma métrica do quanto se pode depender tecnicamente, economicamente, socialmente, etc., da condição de funcionamento de um componente em um ou mais instantes durante a missão, isto é, indica a qualidade do serviço prestado por um sistema e a confiança no serviço prestado.

As métricas escalares de Dependabilidade geralmente são: Confiabilidade *(Reliability),* Manutenabilidade *(Maintainability),* Disponibilidade *(Availability),* Segurança a Acidentes *(Safety),* Segurança a Intrusões *(Security), Capacidade (Capability),* Durabilidade *(Durability)*, etc. (VILLEUMER, 1992) Estes atributos estão intensamente relacionados de tal forma que, se um atributo não cumprir os requisitos a Dependabilidade está seriamente ameaçado.

De acordo com Lafraia (2001), a dependabilidade pode ser expressa como a probabilidade de um componente iniciar ou ocupar um dos seus modos de operação durante uma missão específica ou desempenhar as funções associadas aos modos de operação solicitados.

Rabello (2016) apresenta a Dependabilidade sob a ótica das Disciplinas CSE-316-4 (Garantia do Produto de Sistemas Espaciais I) e CSE-210-4 (Processo de Desenvolvimento de Missões Espaciais), "***Dependabilidade*** *é um aspecto essencial em qualquer projeto da área espacial contribuindo para a qualidade global do produto final".* Abordando não somente o conceito de Dependabilidade, mas também sobre o programa de dependabilidade para missões espaciais que orienta para a definição e escolhas de itens e materiais, direciona a análise de riscos e os pontos fracos do projeto.

No seu sentido mais amplo, dependabilidade poderá ser definida como a ciência de dependência sob condições incertas: compreende o conhecimento dessas incertezas, a respectiva avaliação, a sua previsão, medição e seu controle. Dependabilidade pode ser definida também como a capacidade de uma entidade desempenhar uma ou várias funções necessárias sob condições e tempo prescritos ambos com incertezas.

2.2. Os Atributos de Dependabilidade

Os atributos de Dependabilidade foram estudados com detalhes nas disciplinas CSE-203-4 (confiabilidade e Prevenção de Falhas em Sistemas Espaciais) e CSE-308-4 (Redundância e Tolerância a Falhas em Sistemas Espaciais); e foram abordados de forma menos detalhada nas disciplinas CMC-211-4 (Modelagem e Tolerância a Falhas em Tempos Virtual e Real) e CSE-316-1 (Garantia do Produto I)

Como mencionado anteriormente Dependabilidade é composta por várias métricas, geralmente na literatura são destacadas as Métricas Confiabilidade (*Reliability), Disponibilidade (Availability), Manutenabilidade (Maintainability), Segurança contra acidente (Safety) e Segurança contra intrusões (Security).*

- **Disponibilidade** é a capacidade de um item estar em estado disponível para executar uma função necessária,
- **Confiabilidade** é a capacidade de um item executar a função necessária sob condições e tempo prescritos.

- **Manutenabilidade** é a capacidade de um item ser mantido ou restaurado para um estado em que pode executar sua função sob condições e tempo prescritos.
- **Segurança a Acidentes:** é geralmente medida pela probabilidade de uma entidade 'E', sob dadas condições, não causar eventos catastróficos ou críticos acidentalmente, estado onde a medida do risco de ferir pessoas ou causar danos é menor ou limitado a um risco aceitável. (VILLEMEUR, 1992).
- **Segurança contra intrusões:** é a capacidade de o sistema operar sem falhas catastróficas intencionalmente, ou ainda, é a probabilidade de que o sistema não incorrerá em falhas catastróficas em um intervalo de tempo prédeterminado.

ECSS (2016) declara que o termo **dependabilidade** é reconhecido pelo acrônimo RAM (*Reliability, Availability and Maintainability*) e apresenta uma definição focada na garantia do produto, "*dependabilidade deve ser entendido como a capacidade de fornecer as funcionalidades necessárias a um nível de desempenho suficiente para atingir os objetivos da missão*".

Em concordância com a ECSS (2016) esta monografia destaca a Dependabilidade como RAM e apresenta definições complementares para os atributos Confiabilidade, Disponibilidade e Manutenabilidade.

2.2.1. Disponibilidade

Esta métrica pode ser classificada em Disponibilidade Média (Mean Availability) e Disponibilidade Pontual (Point Availability). Disponibilidade Média é interpretada como a disponibilidade operacional, durante o período de vida útil. É a proporção do tempo de atividade do sistema (tempo total em que o sistema está disponível) dividido pelo tempo total de simulação (tempo total). (RELIAWIKI, 2017).

$$\bar{A} = \frac{Uptime}{Total\ time}$$

Disponibilidade pontual é a capacidade de um item estar em estado disponível para executar uma função necessária, definida como a probabilidade de um sistema ser capaz de exercer a sua função requerida em um determinado instante de tempo.

O atributo Disponibilidade tem grande consequência em muitas missões, pois o sistema deve exercer a função requerida no instante exato de solicitação, como por exemplo, uma aeronave que é carregada e programada para partir ou um míssil balístico no qual pode ser ordenado a lançar em qualquer momento ou, ainda, um *no-break* hospitalar em qualquer situação de interrupção ou variação da energia elétrica. *A disponibilidade depende claramente da Confiabilidade e da Manutenabilidade de cada sistema*.

2.2.2. Manutenabilidade

De acordo com os autores Souza e Porto (2016) e Lafraia (2001), **Manutenabilidade** é a *probabilidade* de que um dispositivo ou sistema será *mantido* ou *restaurado* à condição operacional em um determinado período de tempo com *procedimentos* e *recursos previstos*.

Quando aplicado a um componente de um sistema, **Manutenabilidade** é uma propriedade não somente de concepção, mas também da instalação no sistema. É expressa como a probabilidade refletindo a *incerteza* no *tempo exigido* para as operações de manutenção. É importante não confundir Manutenabilidade com Manutenção do item, ressaltando que **Manutenção** é “o conjunto de ações, procedimentos e recursos previstos destinados a recolocar um item à condição operacional”. A manutenabilidade incorpora a manutenção para sistemas reparáveis.

A manutenabilidade deve incorporar, durante as fases de concepção e desenvolvimento, aspectos como: métodos, informações e pessoal requerido para o diagnóstico em cada fase; procedimentos (plano de voo, troca de componentes, alterações no circuito impresso, soldas, etc), ferramentas, etc.

2.2.3. Confiabilidade

O atributo **Confiabilidade** de acordo com Lewis (1996), Souza e Carvalho (2005) é determinado por meio da grandeza *probabilidade* do sistema funcionar sem ocorrência de falha, durante um período de tempo e sob determinadas condições de operação, quantificando o sucesso da missão.

Segundo Souza e Porto (2016), a Confiabilidade tem a intenção de:

- ✓ Capturar os requisitos de Confiabilidade de todos os stakeholders de um produto, processo, etc;
- ✓ Desdobra-los em especificações para todas as fases do desenvolvimento;
- ✓ Fornecer meios de análise para a verificação das fases e para a validação e certificação do produto, processo, etc.

A métrica Confiabilidade está ligada as falhas durante **a vida útil do produto** e, não ao longo do ciclo de vida, ou seja exclui os períodos de mortalidade infantil e envelhecimento, esses períodos serão abordados adiante. A Confiabilidade do sistema depende de vários fatores como a qualidade, a idade dos componentes e a complexidade do sistema analisado. Ela fornece informações probabilísticas sobre o comportamento do sistema no futuro, baseando em informações probabilísticas sobre o comportamento do sistema no passado, ao longo do tempo e dos componentes. Para a determinação da Confiabilidade é relevante considerar o tempo de utilização do sistema, as características do ambiente, assim como as condições de utilização e o desempenho. (LAFRAIA, 2001; SOUZA E CARVALHO, 2005).

2.3. Qualidade e outros conceitos importantes para a Dependabilidade de sistemas

É impossível tratar a dependabilidade de um sistema ou mesmo a Confiabilidade sem relacionar a qualidade, pois os termos estão altamente relacionados. Dependabilidade e Confiabilidade já foram

definidas e relacionadas. Neste tópico trataremos de definições de qualidade e termos afins que são discutidos em todas as disciplinas mencionadas, no entanto, entre elas se destacam as disciplinas CSE-316-4 (Garantia do Produto de Sistemas Espaciais I) e CSE-210-4 (Processo de Desenvolvimento de Missões Espaciais).

Muitas definições referentes à qualidade são encontradas, mesmo assim este termo é subjetivo e confundido em meio a tantas interpretações. Neste documento a definição utilizada ao termo **qualidade** é: o grau de atendimento aos requisitos. Desta forma, é necessário definir requisito. **Requisito** é a tradução técnica quanto às necessidades referentes ao produto, declaração do comportamento desejado, desempenho e outras características do sistema a ser desenvolvido; ou seja, são as condições que devem ser atendidas.

Não é incomum confundir Qualidade com Conformidade. **Conformidade** é grau de atendimento às especificações. **Especificação** é a descrição dos requisitos técnicos com características do produto para o projeto de sistemas. O documento de Requisitos descreve os problemas, as necessidades requeridas, já o documento de Especificações descreve as soluções técnicas para o produto. O equívoco gerado entre Qualidade e Conformidade se deve a algumas definições, como a declarada por InMetro (1993-2012):

> Qualidade, no contexto do Inmetro, compreende *o grau de atendimento (ou conformidade) de um produto*, processo, serviço ou ainda um profissional a requisitos mínimos estabelecidos em normas ou regulamentos técnicos, ao menor custo possível para a sociedade.

A definição acima está correta e reflete a situação ideal, onde a especificação cobre cada requisito (Requistos = Especificações), entretanto nem sempre isso acontece.

Fazendo uma comparação entre qualidade e confiabilidade, podemos dizer que Qualidade é uma variável que reflete o início imediato da vida útil, isso porque é possível verificar a qualidade do produto imediatamente após a produção (Qualidade é o grau de atendimento aos requisitos).

Confiabilidade, por sua vez, reflete ao período de vida útil, o funcionamento cotidiano sem falhas durante um período de tempo determinado (desempenho sem falhas).

Um programa de dependabilidade deve trazer orientações e definições para garantir a Qualidade e Confiabilidade do sistema (seleção de itens e materiais, análise de riscos, pontos fracos, etc.).

2.4. Ameaças à Dependabilidade de Sistemas: Falhas

Este tópico é destinado à terminologia relacionada a Falhas, a denominação destes termos é estudada nas disciplinas CMC-211-4 (Modelagem e Tolerância a Falhas em Tempos Virtual e Real) e CSE-316-4 (Garantia do Produto de Sistemas Espaciais I). É particularmente difícil uma definição que abranja em si o entendimento comum sobre estes termos, de maneira universal. Por isto, a seguir são dadas as definições escolhidas que serão tomadas como terminologia ao longo do trabalho de doutorado a ser desenvolvido.

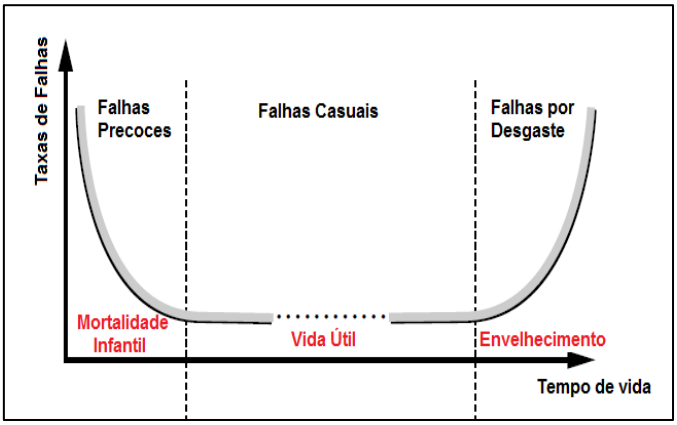
A definição de **falha** em Confiabilidade seria o insucesso parcial no funcionamento do produto. Isermann (2006) complementa com outra definição mais abrangente e clara para **falha *(fault),*** como: “um desvio não permitido de ao menos uma propriedade ou característica do sistema de sua condição padrão, usual, aceitável”.

Lafraia (2001) apresenta a definição de **taxa de falhas** (representada por λ) em Confiabilidade seria “*a frequência relativa com que as falhas ocorrem, num certo intervalo de tempo, medida pela percentagem de falhas para cada hora de operação ou número de operações do sistema ou componente*”. Isso indica a necessidade de entender e definir os tipos de falhas a fim de trabalhar o sistema estudado para que não venha a falhar em operação.

A taxa de falhas dos produtos ao longo do tempo de um componente ou sistema é modelada de uma maneira geral pela **Curva da Banheira** (“*Bathtub Curve*”). Esta curva associa as Fases do Ciclo de Vida do componente (I- Mortalidade Infantil, II- Vida Útil e III- Desgaste ou

Envelhecimento) aos possíveis valores da taxa de falhas, como mostra a Figura 2.2.

Figura 2.2 – Curva de Falhas conhecida como Curva da Banheira.



Existem muitos termos referentes a falhas e de grande importância para a análise de sistemas. Abaixo são destacados:

Erro (Error) pode ser interpretado como a discrepância observada entre uma variável medida e uma faixa aceitável para o valor esperado desta variável. Um erro é tipicamente um sintoma para a existência de uma falha em algum artefato. (GLINZ, 2014)

Sintoma da Falha é qualquer alteração da percepção normal do sistema. Manifestação e/ ou sinalizador observável da falha.

Assinatura (Signature) da falha é o rastro da falha feito a partir de um conjunto de sintomas, pelo qual é possível identificar qual falha ocorreu. Por exemplo, no espectro de frequência que pode ser usado para a identificação da falha. (TEIXEIRA, 2007)

Causa da falha - causa presumivelmente associada a um determinado modo de falha. (ECSS-Q-ST-30-02C, 2009)

Modo de Falha – É a maneira ou forma como o item falha. A anormalidade de desempenho do item, o leva a ser classificado como falho. (SGOBBA, 2016)

Criticidade da Falha - Uma medida combinada da severidade de um modo de falha e sua probabilidade de ocorrência. (ECSS-Q-ST-30-02C, 2009)

Efeito da falha - Consequência de um modo de falha de certo item na operação, função ou Status do item. (ECSS-Q-ST-30-02C, 2009)

Propagação da falha - Evento físico ou lógico causado por falha interna do produto que pode levar a falhas. Ou seja, os modos de falha que podem propagar para as interfaces (ex. da nave para a carga útil) (ECSS-Q-ST-30-02C, 2009; SGOBBA, 2016)

Efeito Final - Consequência de um modo de falha, endereçado a um item, no funcionamento, função ou estado do produto sob investigação e suas interfaces. (ECSS-Q-ST-30-02C, 2009)

Falência (Failure) é definida como a interrupção permanente da habilidade do sistema de realizar uma determinada função sob condições de operação específicas. E pode ser classificada em:

- **Falência Insignificante ou menor (Insignificant/Minor Failure):** Qualquer falha que poderia causar degradação menor nas funções de desempenho do sistema ou da missão, sem qualquer dano considerável a vida ou membro do sistema.
- **Falência significante ou Maior (Significant/Major Failure):** Qualquer falha que poderia causar degradação maior nas funções de desempenho do sistema ou missão, com qualquer dano considerável a vida ou membro do sistema.
- **Falência Crítica (Critical Failure):** Qualquer falha que poderia causar a perda da missão, que poderia causar lesões incapacitantes, mas não fatais ou doenças ocupacionais temporárias; dano crítico a propriedades públicas ou privadas; dano crítico ao sistema de voo e interface ou as instalações terrestres e/ou dano crítico ao meio ambiente.

  Falência Catastrófica (Catastrophic Failure): Qualquer falha que poderia causar potencialmente a perda de vidas, lesões incapacitantes

ou doenças ocupacionais permanentes, perda do sistema de voo e interface, perda de instalações do lançamento, perda do sistema e/ou efeitos ambientais altamente prejudiciais. (LEITE, 2007, VILLEMEUR,1992, ECSS-Q-ST-30-02C, 2009 e ECSS-Q-ST-30C, 2009)

Cada instituição adapta a classificação das categorias de severidade para atender necessidades específicas de cada programa. Estas classificações de severidade são apresentadas, para cada Programa do INPE, nos documentos de Requisitos da Garantia do Produto. A tabela 2.1

Tabela 2.1 – .Categorias de severidades

Categoria de Severidade	**Efeito no Subsistema**
Catastrófico	Perda do tempo de vida do Subsistema maior que 50%
Crítico	Perda do tempo de vida do Subsistema entre 25% e 50%
Significante ou Maior	Perda de qualquer equipamento redundante
Insignificante	Outros

Repertório de Falhas é o conjunto das falhas que devem ser estudadas e tratadas. É a especificação básica para o desenvolvimento de um Sistema de Detecção e Diagnóstico de Falhas.

Itens Críticos são ameaças potenciais para o desempenho, qualidade, dependabilidade e segurança de um sistema, podendo atingir unidades, (subsistema, equipamento, componente, material, processo e função). Um item (componente, subsistema ou sistema) é considerado item crítico quando seu modo de falha for identificado como:

- *Single point failure* **+** severidade identificada como catastrófica, crítica ou maior.
  "*Single point failure"* (termo geralmente traduzido por "Ponto de Falha Simples" ou "Ponto único de falha" ou ainda "Ponto critico de falha") juntamente com pelo menos uma classificação de severidade do efeito da falha identificada como catastrófica, crítica

ou maior. (ECSST-30-02C, 2009) No entanto, caso o item tenha uma altíssima confiabilidade ou probabilidade de ocorrência muito baixa este pode não ser considerado crítico.

- Outra maneira de identificar um item como crítico é quando um dos seus modos de falha possui consequências de falha classificadas como catastróficas.

2.4.1. Tipos de falhas

Dos vários tipos de falhas, nesta monografia são destacados os tipos:

- **Falhas Simples** - Define-se por falha simples aquela que atinge somente um parâmetro ou componente por vez.
- **Falha de Ponto único ou Ponto de Falha Simples *(Single point failures***): É a falha de um item pode resultar na falha irrecuperável do sistema e não é compensada através de redundância ou procedimento operacional alternativo. (MIL-STD-1629, 1983)
- **Falhas Compostas -** Falhas múltiplas ou compostas são aquela que atingem vários parâmetros ou componentes simultaneamente, podendo se propagar e afetar mais de um parâmetro do sistema.
- **Falhas de modo Comum -** Duas ou mais falhas do mesmo modo, devidas a uma única causa; (*Modo de falha*: é a descrição da maneira pelo qual um item falha em cumprir com a sua missão.)
- **Falhas Abruptas -** Falha repentina de um componente.
- **Falha Incipiente -** Falha que ocorre lentamente em um componente.
- **Falha latente -** Falha oculta, a falha que não é imediatamente detectável.
- **Falha intermitente** – É a perda de algumas funções ou alguma característica em um produto por um período de tempo limitado; este, subsequente, recupera a sua função. (QI, GANESAN, PECHT, 2008)

2.5. Meios de melhorar a Dependabilidade de sistemas

Para melhorar a Dependabilidade de sistemas é necessário o estudo e controle dos possíveis erros (*errors*), falhas (*faults*), defeitos (*defects*) e falências (*failures*). Existem quatro abordagens que trabalham o sistema com uso de métodos, propriedades e ferramentas para realizar a prevenção, tolerância, remoção e até o tratamento da falha no sistema antes que esta ocorra. Essas abordagens são:

- **Prevenção a falhas** (*Fault avoidance*) – Abordagem que tenta Impedir a ocorrência ou introdução de falhas. Envolve a seleção de métodos de projeto e de tecnologias adequadas para os seus componentes. Esta abordagem é amplamente estudada na disciplina CSE-203-4 (Confiabilidade e Prevenção de Falhas em Sistemas Espaciais), e é abordada parcialmente nas disciplinas CSE-316-4 (Garantia do Produto de Sistemas Espaciais I) e CSE-210.-4 (Processo de Desenvolvimento de Missões Espaciais).
- **Tolerância a falhas** (*Fault tolerance*) – Abordagem que fornece o serviço esperado mesmo na presença de falhas. Tolera a ocorrência da falha. Esta abordagem é amplamente estudada na disciplina CSE-305-4 (Redundância e Tolerância a Falhas em Sistemas Espaciais) e é abordada parcialmente nas disciplinas CSE-316-4 (Garantia do Produto de Sistemas Espaciais I) e CSE-210.-4 (Processo de Desenvolvimento de Missões Espaciais).
- **Correção de falhas** (*Fault correction*) – Abordagem que expressa a capacidade do sistema eliminar ou contornar as falhas, voltar ao estado correto de operação. Esta abordagem é estudada na disciplina CMC-211-4 (Modelagem e Tolerância a Falhas em Tempos Virtual e Real).
- **Predição de falhas** (*Fault prediction*) – Abordagem que procura a determinação do tipo, tamanho, localização da falha antes mesmo que ela ocorra e não permite que incida. Esta abordagem é estudada na disciplina CMC-211-4 (Modelagem e Tolerância a Falhas em Tempos Virtual e Real).

2.5.1. Propriedades e métricas/métodos para a melhoria da Dependabilidade

São muitas as propriedades e métricas utilizadas em sistemas que ajudam na produção de sistemas dependáveis. As propriedades e métricas enfatizadas nesta monografia são: Redundância, Cobertura, MTBF, MTTF, MTTR, FDI e FDIR. Propriedades e métricas estas relatadas e/ou utilizadas/estudadas nas disciplinas destacadas nesta monografia.

Redundância (*Redundancy*) é a propriedade de um dispositivo ou sistema ter mais do que um meio de executar sua função, sendo essa uma das técnicas utilizadas para aumentar a Confiabilidade, ou seja, tornar o sistema tolerante a falhas. Esta propriedade permite tolerar uma falha de um ou mais componentes, sem comprometer o funcionamento do sistema. A redundância do sistema não implica necessariamente haver componentes extras dentro do sistema (***Redundância Física***), mas implica que o mesmo fornece mais de uma forma de derivar e processar a informação desejada (***Redundância Informacional***).

Um sistema que não tem redundância é chamado de ***simplex***. Quando se analisa essa configuração mais simples, que é o modo sem redundância *(Simplex*), a análise se limita em avaliar o funcionamento de cada componente, pois, se o sistema opera sem falhas, todos os componentes funcionam. Pode-se mensurar individualmente o grau de falha de cada componente e o impacto de cada componente no funcionamento do sistema.

Componentes redundantes podem ser operados em duas maneiras diferentes no sistema: A redundância ativa (*Active redundancy*) e a Redundância em Espera (*standby redundancy*).

- **Redundância ativa** se refere a uma configuração do sistema em que todos os componentes estão em funcionamento durante todo o período de operação. Neste caso, os conjuntos de componentes redundantes podem ser utilizados para verificar a consistência no

seu funcionamento. Neste caso não há necessidade de chavear para o elemento redundante ou desconectar a unidade que falhou. A ECSS-Q-ST-30-02C (2009) resume-o como "*Estado em que todos os meios para realizar uma função requerida se destinam a funcionar simultaneamente.*"

- A **redundância em espera** é a que os componentes redundantes ficam inoperantes até ser necessário e somente após a necessidade (devido à falha) são colocados em serviço a partir de chaveamento.

Cobertura (*Coverage*) é a propriedade de um sistema que define sua capacidade de tolerar falhas de um subconjunto específico de componentes.

Sistemas redundantes podem ser concebidos para fornecer uma cobertura para falhas de alguns dos seus componentes, mas não todas elas. Um sistema pode também ser concebido para cobrir a primeira falha de um componente de certo tipo, mas não o segundo. A cobertura fornecida por um sistema é uma descrição específica do seu nível de redundância. (SOUZA & CARVALHO, 2005; RELIASOFT COPORATION, 2010).

Tempo médio até a falha - *MTTF (Mean Time To Failure*) Este pode ser interpretado como o tempo esperado para a falha de sistemas não reparáveis.

É, naturalmente, possível e provável que o tempo médio para a primeira falha de um componente (MTTF) seja diferente do tempo médio para a outra falha, após uma falha e reparação. Isto depende "se o componente reparado ficou tão bom quanto um novo", ou seja, se as suas características ao longo da vida após o reparo são essencialmente as mesmas que para um componente novo do mesmo tipo. Na prática, raramente se tem informações suficientes para distinguir MTBF de MTTF. (SOUZA & CARVALHO, 2005).

Tempo médio entre Falhas - *MTBF (Mean Time Between Failures*) É um indicador comum de Confiabilidade de componentes e sistemas, é definido no contexto em que o equipamento de missão que falhou é reparado (sistemas com possibilidade de manutenção) e devolvido para serviço. Nesse contexto, MTBF é o tempo esperado que o componente irá executar corretamente sua função até a próxima falha.

Souza e Porto (2016) afirmam que este conceito se aplica em situações que não admitem reparos (contexto espacial), caso em que seria mais significativo chamar de "*tempo médio de operação esperado"*.

$$MTBF = \frac{1}{\lambda}\,, \quad \lambda = taxa\ de\ falha$$

Tempo médio para Reparo - MTTR (*Mean Time To Repair*) Este é o tempo esperado para o dispositivo ou sistema retornar ao serviço após um chamado de manutenção. Não utilizado no contexto espaciais.

Detecção e Isolação de Falhas - FDI (*Failure Detection and Isolation*) Esta é a função de detectar a ocorrência de falhas de componentes em sistemas operacionais e isolar ou identificar o componente que falhou. FDIR implica um processo de tomada de decisão, é implementado em algumas formas de sistemas tolerantes a falhas, mas não são todos.

Detecção, Isolação e Recuperação de Falhas- FDIR (*Failure Detection, Isolation and recovery*) Esta é a propriedade FDI adicionada a função de reparar o componente que falhou.

Em geral muitos métodos/ferramentas são utilizados para trabalhar as abordagens de Prevenção a falhas, Tolerância a falhas, Correção de falhas e Predição de falhas. Assim como muitos métodos, ferramentas e abordagens são usados para analisar o impacto das falhas na Confiabilidade do sistema. Dos muitos métodos se destacam:

- Análise da Árvore de Falhas (FTA – "*Fault Tree Analysis*");
- Análise dos Modos de Falhas e Efeitos (FMEA – "*Failure Modes and Effects Analysis*");

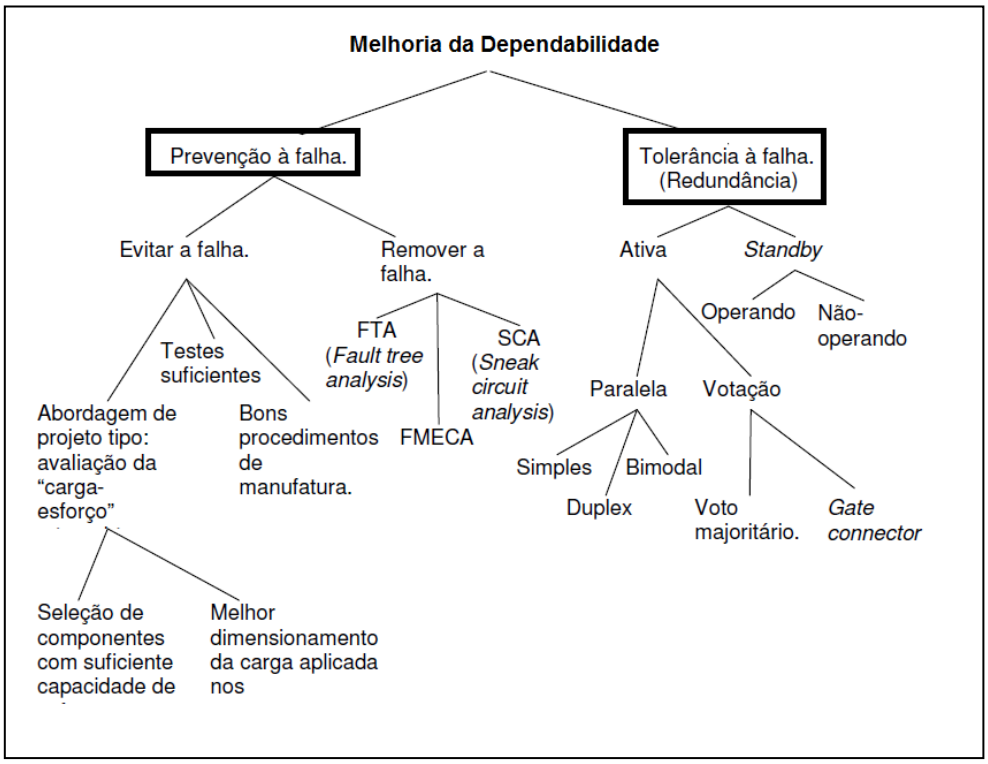
- Análise dos Modos de Falhas, Efeitos e Criticidade (FMECA – "*Failure Modes, Effects and Criticality Analysis*");
- Análise da Árvore de Eventos (ETA – "*Event Tree Analysis*");
- Diagrama de Blocos de Confiabilidade (RBD – "*Reliability Block Diagram*");
- Análise de Markov ("Markov Analysis").

Usualmente esses métodos são complementares, alguns são utilizados em conjunto para definir quais falhas merecem mais atenção. Estes métodos/ferramentas são extremamente úteis e veêm sendo utilizados há muitas décadas, no entanto estes focam na preservação operacional do sistema em modo normal de operação. Em uma análise *a priori*, essas ferramentas são muito utilizadas na primeira abordagem de Confiabilidade (Prevenção à Falhas).

A abordagem (Prevenção de Falhas) foca em evitar a falha e/ou eliminar as falhas ou as fontes propícias a falhar com bons procedimentos de manufatura, métodos de projeto, testes para detectar possíveis falhas precoces e removê-las, etc. A Prevenção de falhas está relacionada com a verificação do projeto, onde se utilizam os vários métodos já citados nesta monografia. Mesmo realizando esta abordagem a fim de evitar falhas, ainda podem ocorrer falhas inesperadas; então, para um projeto mais robusto a abordagem de Tolerância a Falhas é aplicada ao sistema. Esta tem por objetivo que o sistema tenha mais de um meio de realizar certas funções, para que mesmo com alguma parte falhada, o sistema possa cumprir com sucesso sua missão. (Ver Figura 2.3)

Na Figura 2.3 são apresentadas as características de duas abordagens de Confiabilidade: Prevenção de falha e Tolerância a Falhas, sendo estas amplamente utilizadas para melhoria da Confiabilidade em desenvolvimento de projetos.

Figura 2.3 – Relação das duas primeiras abordagens de Confiabilidade no processo de melhoria da Dependabilidade



Fonte: Adaptado de Asenek, V.; Sweeting, M.; Ward (2017)

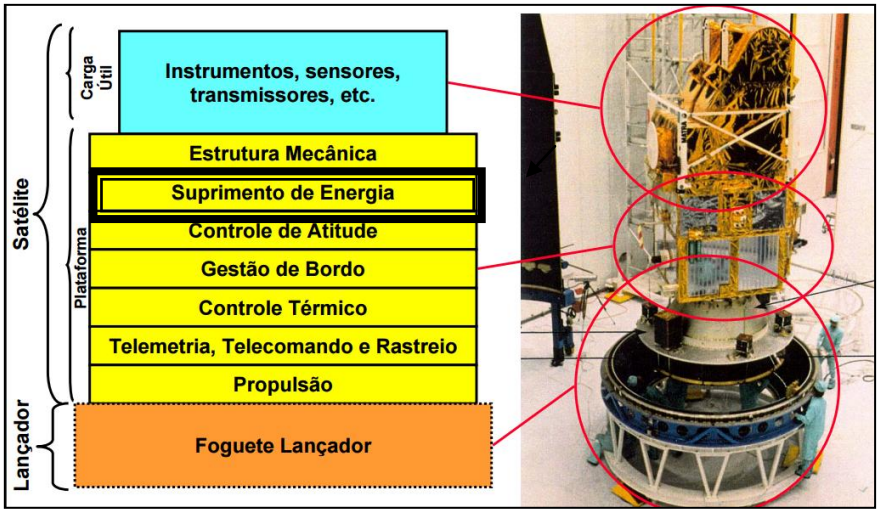
3 ESTUDO DE CASO

3.1. Descrição e característica do subsistema analisado

Os assuntos relacionados à descrição e características do subsistema estão relacionados com todas as disciplinas mencionadas na Tabela 1.1.

O satélite, denominado um componente pertencente ao segmento espacial, é uma das partes de uma missão espacial, é a parte colocada em órbita. O satélite é composto por outras duas grandes partes: Carga útil e Plataforma. A Carga útil é composta por equipamentos destinados a cumprir a missão. A Plataforma fornece à carga útil todos os serviços necessários ao seu funcionamento. Ela é composta por equipamentos necessários para o funcionamento do satélite que são divididos em subsistemas. Na Figura 3.1 um satélite é apresentado integrado ao último estágio de seu lançador, onde é possível identificar os vários subsistemas de um satélite convencional. (Souza, 2007; INPE, 2002)

Figura 3.1: As partes de um satélite.



Fonte: Adaptado de Souza (2004)

Nesta monografia o Subsistema de Suprimento de Energia (PSS – “Power Supply Subsystem”) é destacado, isto porque as abordagens empregadas e as falhas apresentadas neste documento foram atribuídas a este subsistema. Ele é considerado um dos mais importantes subsistemas da plataforma, pois ele deve ser dimensionado de forma a gerar, armazenar,

converter e distribuir energia necessária para os demais equipamentos durante toda a missão espacial.

Segundo Torres (2014) o subsistema de suprimento de energia é responsável por:

- Converter energia solar em energia elétrica utilizando células fotovoltaicas;
- Produzir e armazenar potência nas baterias para alimentar as cargas do satélite em períodos de eclipse;
- Fornecer potência para todos os equipamentos do satélite (com níveis de tensão e potência diferentes nas fases e modos de operação);
- Fornecer meios para o correto condicionamento do excesso de energia gerada, durante os períodos de iluminação solar;
- Fornecer telemetrias para monitorar as condições de operação dos equipamentos do subsistema;
- Fornecer meios para realizar o controle de carga e descargas das baterias.

O subsistema analisado foi desenvolvido com os seguintes equipamentos:

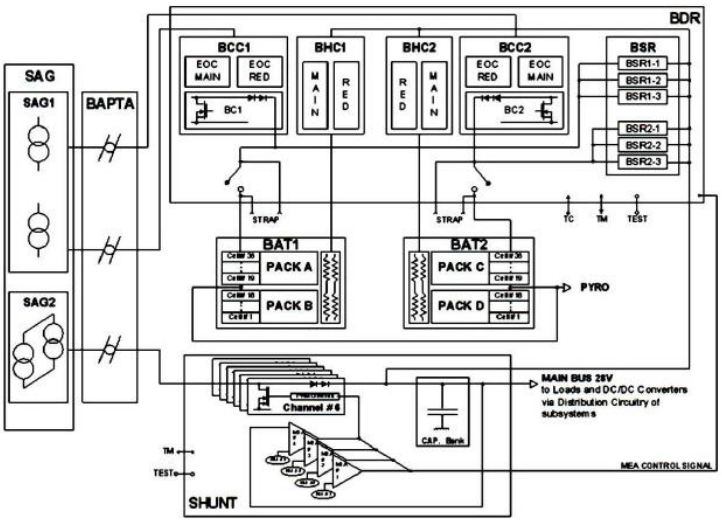
- **Gerador Solar (SAG - *Solar Array Generator*)** - Painel solar dividido em duas seções; SAG1 (conectado as baterias) e SAG2 (conectado ao SHUNT);
- **Baterias (BAT1 e BAT2)** - Armazenamento de energia - baterias do tipo Níquel- Cádmio. As Baterias “BAT1 e BAT2” não são redundantes, as duas são operantes, é uma opção do projeto;
- **Regulador de Descarga das Baterias (BDR - *Battery Discharge Regulator*) e Regulador Shunt (SHUNT)** - Unidades de Condicionamento de Potência (PCU), representando a eletrônica de potência utilizada no gerenciamento e regulação do sistema. A energia é disponibilizada para o satélite por meio de um barramento regulado, a partir do qual ocorre a distribuição pela Unidade Distribuidora de Potência (PDU) às diversas cargas úteis;

SHUNT: É responsável por controlar diretamente a potência disponibilizada pelo painel solar.

- **Conversores de corrente contínua (DC/DC *Converters*)** – Estes tem o objetivo de produzir tensões específicas para um conjunto de equipamentos. Fazem a alteração da tensão do barramento principal em valores de tensões específicas para distribuir sob demanda a algumas cargas do satélite que não são alimentadas pelo barramento principal (28 V). Garantem uma tensão de saída regulada. É unidade responsável pela distribuição de energia e proteção das cargas e do barramento.
  (TORRES, 2014; MAGALHÃES, 2012).

As principais funções do subsistema de suprimento de energia são o condicionamento da energia primária gerada pelos painéis solares (SAG1 e SAG2), durante os períodos de iluminação solar que armazena em uma fonte secundária (baterias – BAT1 e BAT2) para utilizar durante os períodos de eclipse e é distribuída aos equipamentos. O controle do estado de carga da bateria é realizado pelo circuito de fim-de-carga (*End-of-charge* - EOC), que limita a carga da bateria ligando e desligando a corrente que a carrega. O condicionamento da potência do barramento principal é realizado pelo equipamento SHUNT e pelo Regulador de Descarga da Bateria (*Battery Discharge Regulator* – BDR) que em conjunto controlam a potência fornecida pelos SAGs e pelas baterias, provendo o satélite e os conversores DC/DC com um barramento principal estabilizado. Depois de condicionada, o subsistema realiza a distribuição dessa energia para os diversos subsistemas do satélite através do barramento principal (28 V) e em diversos níveis de tensão e corrente solicitados pelas cargas, através dos conversores “DC/DC´s”. (TORRES, 2014, BARUEL, 2012; FREIRE, 2009 e AZEVEDO, 2011).

Figura 3.2: Subsistema de potência dos satélites CBERS



Fonte: Torres (2014)

Os satélites possuem muitos tipos diferentes de telemetrias. As telemetrias usadas para este trabalho indicam valores medidos por sensores e estados de equipamentos, ou seja, são as telemetrias analógicas do subsistema de suprimento de energia. Telemetrias analógicas são aquelas relativas a valores analógicos, como por exemplo, dados de corrente, temperatura, etc. Estas telemetrias estão associadas às baterias, ao painel solar, aos equipamentos SHUNT e BDR e são ilustradas na Tabela 3.1.

Tabela 3.1: Telemetrias do Subsistema de suprimento de energia.

Sigla da Telemetria	Descrição da Telemetria
TMD001	Tensão do Barramento Principal.
TMD002	Corrente do Barramento Principal.
TMD003	Tensão de saída do Main Error Amplifier
TMD013/017	Corrente de Entrada do BDR
TMD014/018	Tensão das Baterias
TMD015/019	Temperatura das baterias
TMD016/020	Tensão mínima de grupo de célula
TMD021	Corrente de saída do BRD
TMD022/023	Corrente dos painéis solares

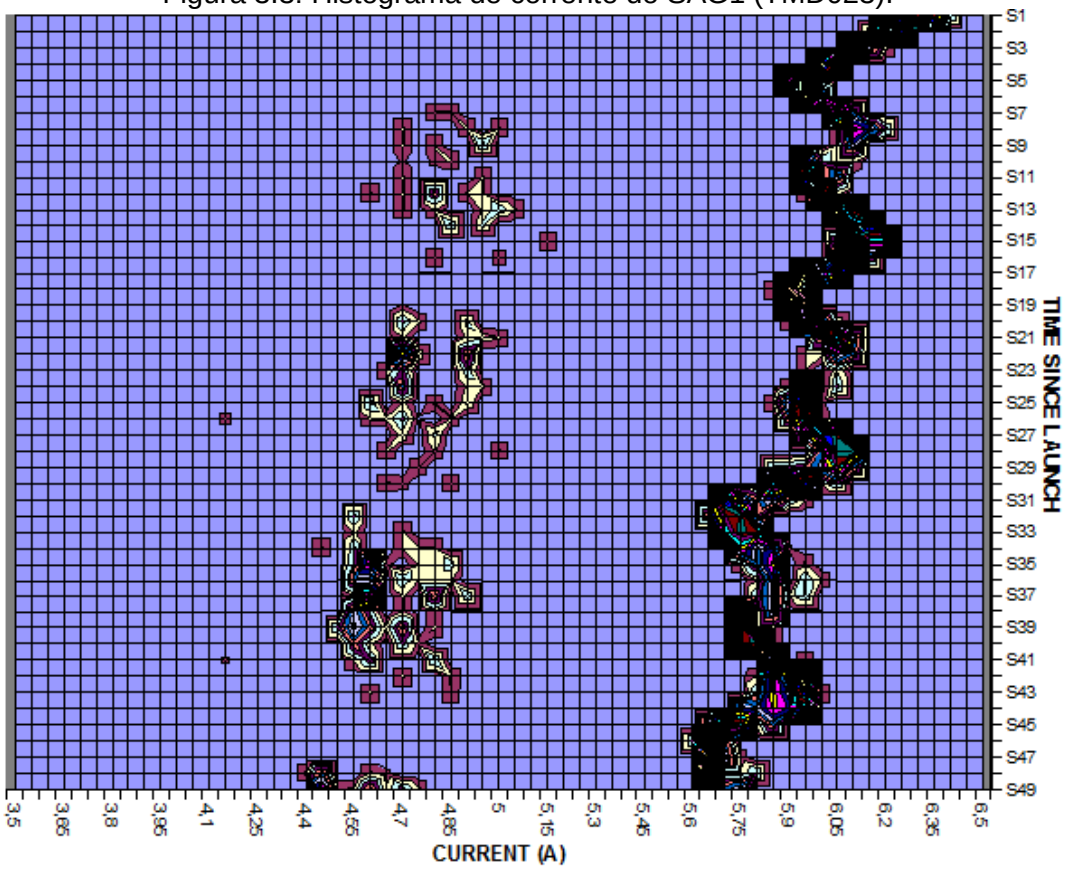
Fonte: INPE (2005).

3.2. Estudo de caso 1 - Falha na conexão em Painel Solar do Satélite S1

Uma anomalia na corrente elétrica foi detectada no painel solar (SAG1 B) poucos meses após o lançamento do S1 (1999), no entanto, ela ocorria de forma ocasional (intermitente) e foi investigada após 4 anos em órbita, quando foi possível obter dados suficientes para a análise. (INPE, 2003)

Foi observado que em alguns períodos do ano a telemetria (TMD023) do painel solar SAG1B apresentava valores de corrente elétrica abaixo do esperado para os períodos de iluminação solar, sugerindo problemas no suprimento de energia para a bateria 2. A Figura 3.3 apresenta um histograma tridimensional mostrando o número de vezes que um dado valor da telemetria TMD023 foi observado durante seu ciclo de vida do satélite S1. Na Figura 3.3, o eixo da ordenada representa os meses transcorridos desde o lançamento do satélite (Outubro, 1999), enquanto o eixo da abscissa representa os valores de corrente elétrica (Ampére). A frequência das medidas é observada através das cores: cores mais escuras representam uma maior ocorrência de um dado valor no tempo.

Figura 3.3: Histograma de corrente do SAG1 (TMD023).



Fonte: INPE (2003).

De acordo com Inpe (2003) da análise da Figura 3.3 foi possível fazer as seguintes observações:

- Nas regiões de valores normais (próximos a 6A) há uma diminuição gradual no valor da telemetria de corrente elétrica. Este efeito é considerado normal e advém da degradação do painel solar;
- Há valores não esperados para períodos iluminados;
- Existe uma diferença de aproximadamente de 1,2A nos valores de corrente elétrica entre as duas regiões (Valores não esperados e valores considerados normais para períodos iluminados);
- Com o tempo, a frequência de valores não esperados aumentou;
- Normalmente, de Janeiro a Março de cada ano, por um efeito sazonal, esses valores intermediários não esperados (medição de baixo valor) não ocorreram.

Os valores considerados normais para a telemetria TMD023 estão na faixa de 0 a 7.2A, sendo zero nos períodos de eclipse (não há iluminação solar) e próximos a 6A nos períodos de iluminação solar.

3.2.1. Discussão da Possível causa da anomalia na corrente elétrica

Um levantamento das possíveis causas hipotéticas da anomalia foi realizado. Entre as hipóteses levantadas a mais provável e considerada a causa real da anomalia foi a falha na conexão da cablagem do painel solar.

O SAG foi inspecionado durante a integração no edifício de lançamento e nesta inspeção foi observado que as linhas de retorno dos cabos do SAG são unidos na cablagem da asa. Esta junção foi realizada sem o uso de técnicas de alívio de tensão mecânica para proteger a soldagem. Observou-se também que a junta soldada é firmemente fixada ao arnês (*harness*) e submetida à tensão mecânica devido ao ciclo de temperatura. A junta soldada usa folha de prata de espessura de 0,05 mm para unir os cabos. Esta folha pode facilmente fadigar e rachar, o que deve ter ocorrido; com isso, provavelmente sucedeu um problema de mau contato intermitente causando a redução da corrente do SAG. (INPE, 2003).

Esta falha poderia ser tolerada com o uso de redundância na cablagem, pois segundo Inpe (2003), a documentação de cablagem da asa do SAG (*SAG Wing Cabling documentation*) mostra que existem 6 ligações entre grupos de três ou quatro linhas de retorno do SAG1 e SAG2 que são ligados a um único cabo, sem redundância. E complementa declarando que “a falta de redundância naquelas soldagens e cabos provoca o aparecimento de vários modos de falha de ponto único (*single-point-failure*)”.

A variação de corrente observada corresponde exatamente à variação de corrente esperada se ocorresse uma falha de ponto único numa junção soldada de 4 circuitos (*strings*). De fato, a corrente de string média calculada pela divisão da corrente total SAG1-B (~ 6A) pelo número de circuitos (22) é 0,27A. A variação da corrente observada, é de

aproximadamente 1,2 A, corresponde à corrente de 4 circuitos, como 0,27A * 4 = 1,09A. (INPE, 2003)

3.3. Estudo de caso 2 - Falhas em 2 baterias do satélite S2

O desempenho da bateria em uma missão espacial é, sem dúvidas um fator extremamente importante, podendo limitar a vida útil da missão ou até mesmo comprometer o desempenho da missão em caso de falhas.

Destacamos nesta monografia as falhas das duas baterias de um mesmo satélite, porém em momentos diferentes de sua vida útil. O satélite, mencionado aqui como S2 utiliza baterias do tipo Níquel Cádmio.

A partir de 1967 este tipo de bateria passou a ser extremamente utilizada. Este foi também o período em que surgiram muitas missões espaciais com essa tecnologia o que fez várias agências governamentais americanas financiarem vários estudos para entender os fenômenos em baterias e, com isso, desenvolver novas células que fossem capazes de cumprir com os padrões de qualidade espacial. Isto resultou em um manual de baterias Níquel Cádmio publicado pela NASA relatando lições aprendidas, intitulado "*Handboobk for Handling of Nickel-Cadmium Batteries: Lessons Learned*". (FORD,RAO & YI, 1994).

Atualmente as baterias de Níquel Cádmio não são amplamente utilizadas como na década de 60 e 70, mas ainda se encontram em uso em aplicações espaciais devido à sua robustez a grande número de ciclos de carga e descarga bem como sua boa capacidade em suportar longos períodos de armazenamento. (MAGALHÂES, 2010)

3.3.1. Estudo de caso 2A – falha na BAT2 do satélite S2

O satélite S2 funcionou excelentemente durante 18 meses até que ocorreu uma falha no subsistema de suprimento de energia.

Uma análise dos dados de telemetria das órbitas anteriores à falha mostrou equilíbrio em todos os aspectos, (tensão de carga, tensão de

descarga, profundidade de descarga, temperatura, etc), entre as duas baterias e não mostrava condições de alarme nas telemetrias.

A anomalia foi detectada na primeira passagem, e, na seguinte, foram emitidos os comandos necessários para recuperação da anomalia. Os comandos enviados atuaram corretamente, mas a anomalia persistiu e, para preservar a segurança do satélite, foram emitidos com sucesso comandos para cancelar todas as operações de carga útil. Imediatamente iniciou-se uma análise detalhada dos dados do subsistema de suprimento de energia enviados pelo satélite durante as últimas passagens. Observou-se que várias outras telemetrias eram anormais ou apresentavam valores alarmantes, a Tabela 3.2 apresenta a relação destas telemetrias.

Tabela 3.2: Telemetrias do PPS que apresentavam valores anormais ou alarmantes.

Sigla da Telemetria	Descrição da Telemetria
TMD001	Tensão do Barramento Principal.
TMD002	Corrente do Barramento Principal.
TMD003	Tensão de saída do Main Error Amplifier (MEAS)
TMD013/017	Corrente de Entrada do BDR
TMD014/018	Tensão das Baterias
TMD015/019	Temperatura das baterias
TMD016/020	Tensão mínima de grupo de célula
TMD022/023	Corrente dos painéis solares

3.3.1.1. Discussão sobre a possível causa da Falha

A causa mais provável é uma falha de ponto único (*single point failure*), uma falha em aberto na BAT2 que, apesar de constar na lista de itens críticos, esta não foi eliminada. Isto porque este modo de falha é considerado muito raro neste tipo de bateria (Níquel Cádmio) existindo pouquíssimas ocorrências reportadas. Assim, este modo de falha não foi considerado provável e ações de mitigação não foram tomadas para eliminá-lo durante a fase de projeto.

Em Inpe (2005) são apresentadas, além da baixa probabilidade de ocorrência, outras duas razões específicas utilizadas para a não eliminação deste modo de falha considerado crítico.

- O aumento significativo da massa do satélite se introduzisse redundância de baterias;
- O aumento significativo de custo e complexidade para o circuito eletrônico de desvio para a célula falhada.

Como já mencionado o satélite S2 falhou porque houve uma falha da BAT2 em circuito aberto. Esta falha provavelmente foi provocada pela ruptura das ligações elétricas seguida pelo secamento do eletrólito celular, este causado pela ruptura da caixa da célula. A causa da ruptura foi um curto-circuito interno entre placas celulares seguido de aumento da pressão interna ou uma ruptura de uma solda de célula defeituosa. Há maior probabilidade de o problema ser na solda, pois não há redundância nas soldas da caixa da célula. (Inpe, 2005). Acredita-se que a origem do problema foi o controle de qualidade inadequado.

Com a falha da BAT2, algumas das consequências ao satélite S2 em nível de subsistema, são:

- Perda da potência do SAG1B;
- Capacidade de pico de potência inferior durante eclipse e luz solar;
- Maior Profundidade de Descarga (DOD) em BAT1;
- Maior corrente de descarga em BAT1;
- Ciclo de temperatura mais alta em BAT1;
- Maior temperatura de BAT1;
- A degradação mais rápida de BAT1;
- Tempo de vida BAT1 reduzido.

Algumas recomendações podem reduzir ou eliminar o risco de tais ocorrências, ou os efeitos desta falha em futuras missões. Estas recomendações não são de simples execução; no entanto, devem ser consideradas para uma análise ou discussão mais detalhada. Uma das

medidas seria melhorar o controle de qualidade do fabricante do acumulador que tem a função de integrar os acumuladores formando a bateria (atividade de total responsabilidade do fabricante do acumulador). Outras seriam mudanças no projeto de Subsistema de Suprimento de energia de forma que permita a perda de uma de suas baterias sem grande comprometimento da capacidade e a utilização de circuitos do tipo *bypass* (desvio) ao redor de cada célula da bateria.

3.3.2. Estudo de caso 2B – falha na BAT1 do satélite S2

Com a falha da bateria (BAT2) em aberto, falha mencionada acima em 3.1.1, a bateria remanescente (BAT1) teve que prover sozinha toda a energia do satélite durante os eclipses seguintes. As consequências da falha na BAT2, mencionadas acima, provocaram possíveis problemas na BAT1.

As baterias do satélite são carregadas durante o período de iluminação solar para serem utilizadas durante os períodos de eclipse. O carregamento da bateria é realizado através do BCC e do circuito EOC. O circuito aplica pulsos de corrente para verificar o nível de descarga da bateria (DOD) e, quando necessário a bateria é carregada. Quando as baterias entram em estado de emergência os painéis são mais bem apontados para o Sol (a fim de garantir o suprimento de energia) e os equipamentos são desligados (para economizar energia). Desta maneira as baterias carregam mais rápido que o normal. (AZEVEDO, 2011).

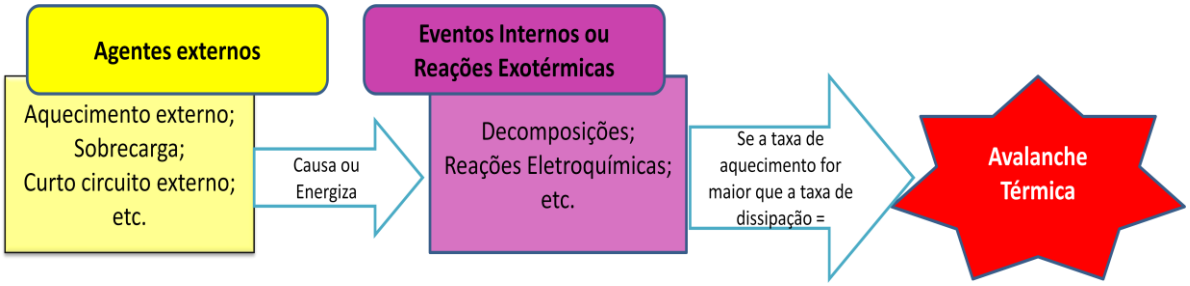
Devido à combinação da aplicação dos pulsos de verificação por um período mais longo que o normal e um problema com a duração dos pulsos, a bateria remanescente passou a receber uma carga maior que se transformava parcialmente em calor. Este excesso de calor não era totalmente dissipado através do sistema térmico, fazendo com que a cada ciclo de iluminação a bateria se aquecesse um pouco mais. (AZEVEDO, 2011).

Com o passar do tempo, a taxa de aquecimento na BAT1 tornou-se maior que a taxa de dissipação o que levou a bateria em dois períodos

diferentes da missão espacial a uma **avalanche térmica**, falha considerada catastrófica e que poderia perder o satélite S2.

Avalanche térmica pode ser caracterizada como um desbalanceamento energético. Segundo Deveau (2015), a avalanche térmica ocorre quando a bateria está sob carga, em um estado de recarga após um evento de descarga. Essencialmente, o calor interno gerado durante o carregamento excede a velocidade à qual o calor pode ser dissipado. (Ver Figura 3.4).

Figura 3.4: Avalanche térmica.



Fonte: Adaptado de Kim (2008).

Acredita-se que a falha na BAT1 foi decorrente de problemas no subsistema de controle de atitude e órbita (AOCS), ou seja, com a falha o satélite deixou de apontar para o lugar correto e os painéis solares, responsáveis pela produção da energia elétrica que o abastece, pararam de receber os raios de Sol da maneira ideal, afetando o subsistema de suprimento de energia. Este problema original no AOCS levou o satélite a um estado de emergência e neste estado a prioridade é garantir o suprimento de energia visando manter o satélite até que o problema fonte seja resolvido. No entanto, a falha da BAT2 colaborou fortemente para a ocorrência desta falha, pois as consequências da falha da BAT2 afetam diretamente a BAT1.

3.3.2.1. Detalhamento e discussão sobre as falhas de avalanche térmica

Segundo Magalhães (2012), a tensão final de descarga é um excelente indicativo da perda de capacidade da bateria. A Figura 3.5 mostra a queda de tensão final de descarga da BAT1 após a falha da BAT2. Isso indica que a sobrecarga na BAT1 fez com que esta produzisse uma

profundidade de descarga (DOD) maior. A profundidade de descarga maior evidencia o processo de degradação da bateria; com isso, a necessidade de aumentar as curvas V/T. Conforme as curvas V/T eram corrigidas, ocorria o aumento no valor médio da temperatura da bateria (BAT1) bem como no valor da flutuação (*ripple)* de temperatura, devida à maior corrente de descarga à que a bateria ficou submetida, como mostra a Figura 3.6.

A Figura 3.7 mostra a operação ao longo dos anos de 2003 a 2007 em termos de corrente do SAG. Nesta figura é possível observar pela queda gradativa da corrente, além das variações sazonais da corrente em função da órbita, o efeito de degradação e variações do ângulo do painel. Ao final de 2007, nas datas destacadas, a Figura 3.7 mostra o período em que o satélite S2 entra em estado de emergência, período em que aponta os painéis solares mais diretamente ao sol.

O perfil de operação de carga útil em termos de corrente é explicito na Figura 3.8. Ele mostra a redução considerável da corrente do barramento a partir da falha da bateria 2, evento considerado catastrófico, pois isto indica a diminuição das operações do satélite objetivando não comprometer ainda mais a bateria remanescente (BAT1). A Figura 3.8 evidencia também o período em que o satélite S2 entra em modo de emergência, onde a corrente sofre uma queda ainda maior.

O evento “modo de emergência” mencionado anteriormente nas figuras destacadas (Nov/2007) é o fato que antecede a primeira avalanche térmica. A primeira avalanche térmica sofrida pelo satélite S2 é descrita na Figura 3.9. Uma vez que a Figura 3.9 abrange várias curvas, sua escala dificulta a visualização de alguns detalhes; no entanto, pode-se observar um aumento da corrente do painel solar, no momento que o S2 entra em emergência e aponta o painel com menor ângulo ao sol. Neste período, a corrente do barramento (TMD 002 em amarelo) também aumenta, o que aumenta a transferência de calor entre bateria e ambiente. Com isso, a temperatura da bateria aumenta (TMD015 em verde), momento em que as equipes de solo diminuem a carga do

satélite, o que diminui a corrente do barramento. Este fato melhora a temperatura da bateria por um breve período, causando uma leve queda na temperatura. No entanto, ao diminuir a corrente do barramento a profundidade de descarga da bateria durante o eclipse também diminui. Isso faz com que o processo de carga injete mais Ampères-hora na bateria no próximo período solar. Com isso, a eficiência de carga da bateria tende a diminuir, transformando quase toda a potência elétrica de carga em calor. Com o aumento gradativo da temperatura, a eficiência de carga cai abruptamente fechando um ciclo vicioso. A análise de outros sensores disponibilizados por outros subsistemas mostrou que a temperatura da BAT1 continuou aumentando e atingiu temperaturas próximas a 60°C. (MAGALHÂES, 2012).

Segundo Inpe (2005), após a ocorrência da falha na BAT2, caso houvesse redução do pico de capacidade de potência e da margem de equilíbrio de energia, algumas recomendações deveriam ser realizadas para assegurar o uso máximo das capacidades de satélite. As ações seriam:

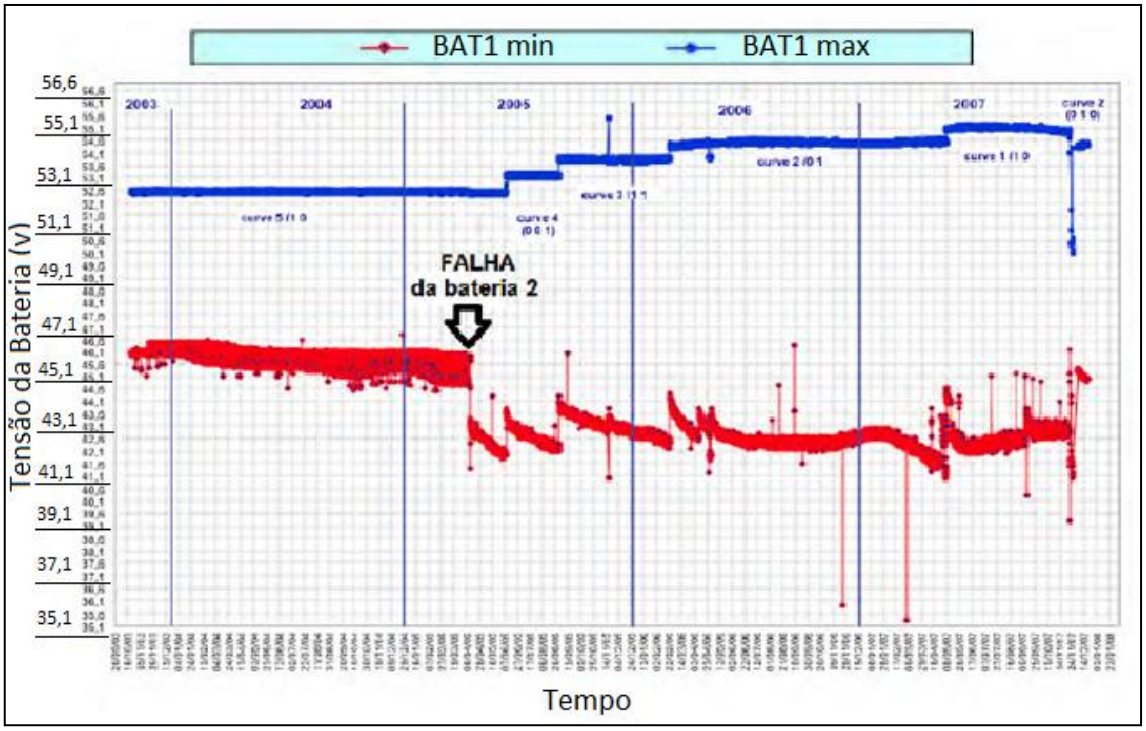
- Desligar os equipamentos desnecessários para reduzir o consumo de energia em espera, reduzindo a profundidade de descarga (DOD) da BAT1 e com isso maximizar o tempo de vida da bateria remanescente e melhorar o balanço energético.
- Alterar os modos de operação dos equipamentos de carga útil para reduzir o consumo de energia, a profundidade de descarga (DOD) da BAT1 e melhorar o balanço energético.
- Evitar o funcionamento da carga útil durante os períodos de eclipse, pois isso aumenta a profundidade de descarga (DOD) da BAT1 e potencializa o desequilíbrio de energia.
- Limitar o tempo de operação para melhorar o balanço energético.

Estas ações foram realizadas após a primeira avalanche térmica, o que o fez o sistema se estabilizar e voltar a operar. No entanto, por volta de dois anos mais tarde o problema se repetiu sob as mesmas condições. A

Figura 3.10 mostra a segunda avalanche após o satélite S2 entrar em modo de emergência.

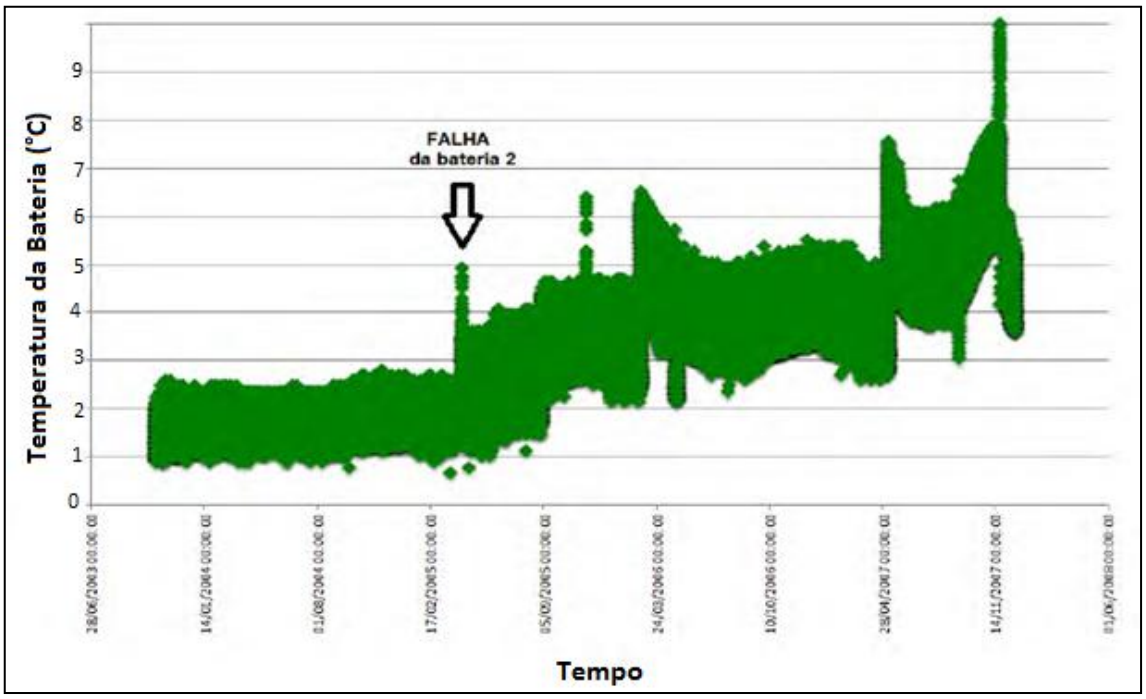
Outras possibilidades poderiam ser incluídas, como por exemplo, a incorporação nas versões seguintes do PSS de um controlador de carga da bateria. Desta forma, não se permitiria colocar corrente demais no carregamento da bateria, mesmo com disponibilidade de carga. Outra opção seria adotar outras topologias (Ver Freire, 2009) e, ou ainda, adotar um barramento não regulado, podendo neste caso, ter variações maiores de tensão e, portanto, a possibilidade de continuar funcionando no caso de falha por curto interno.

Figura 3.5: Comportamento da tensão da bateria 1 ao longo do tempo.



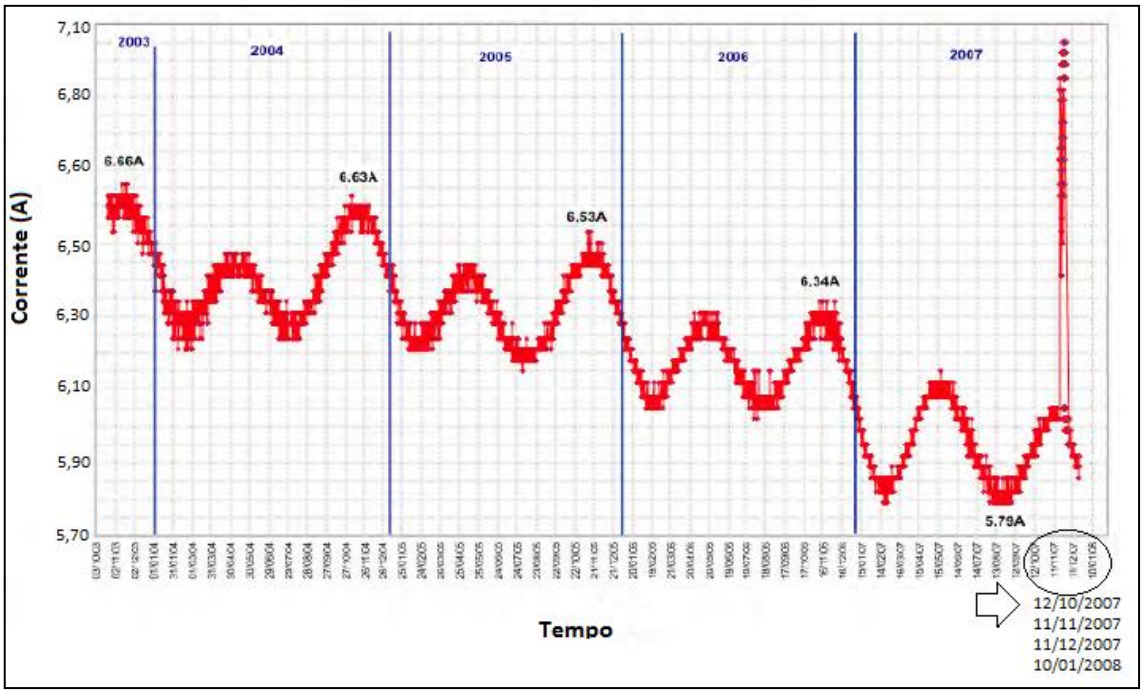
Fonte: Adaptado de Magalhães (2012).

Figura 3.6: Temperatura da bateria 1 entre os anos de 2003 e 2007.



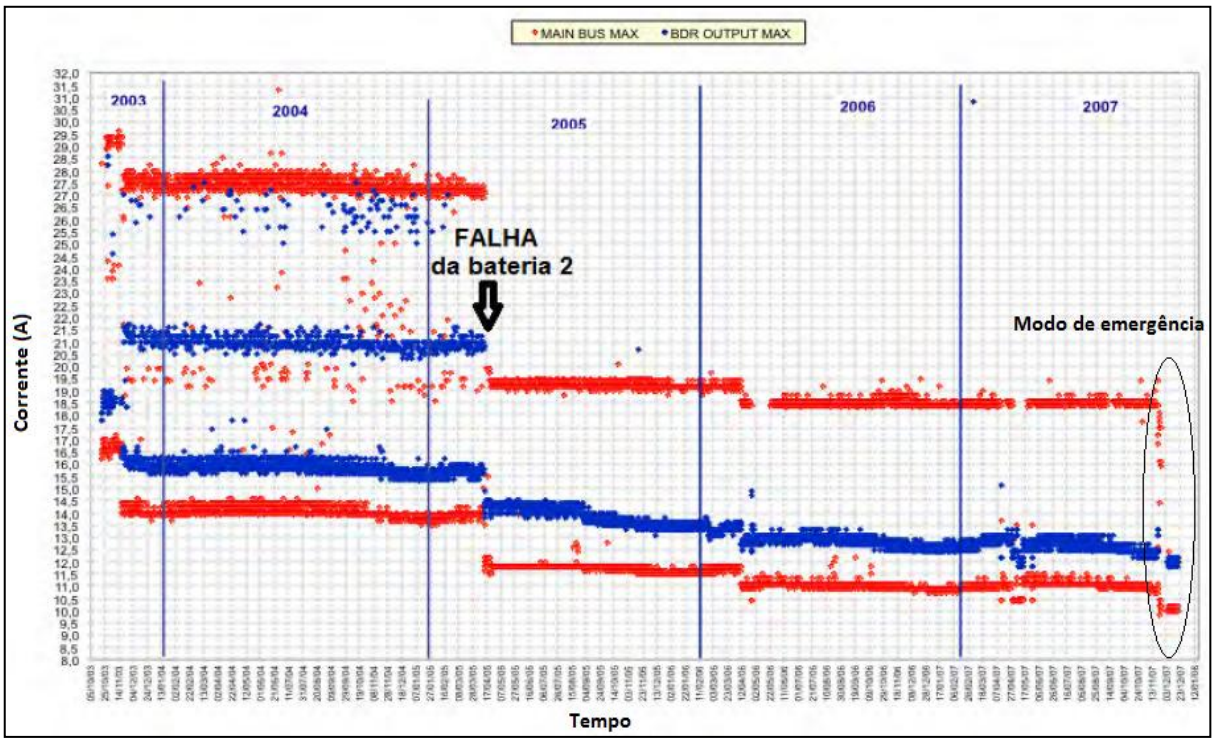
.Fonte: Magalhães (2012).

Figura 3.7: Corrente do SAG entre os anos de 2003 e 2007.



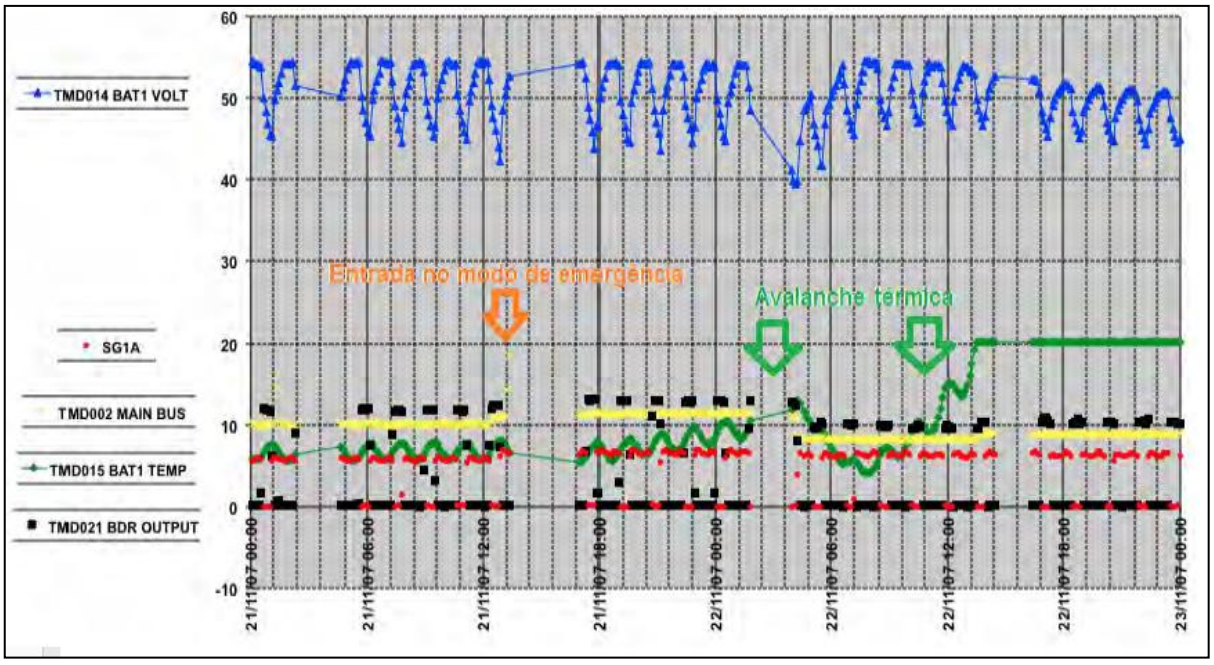
Fonte: Adaptado de Magalhães (2012).

Figura 3.8: Correntes de operação do barramento entre os anos de 2003 e 2007.



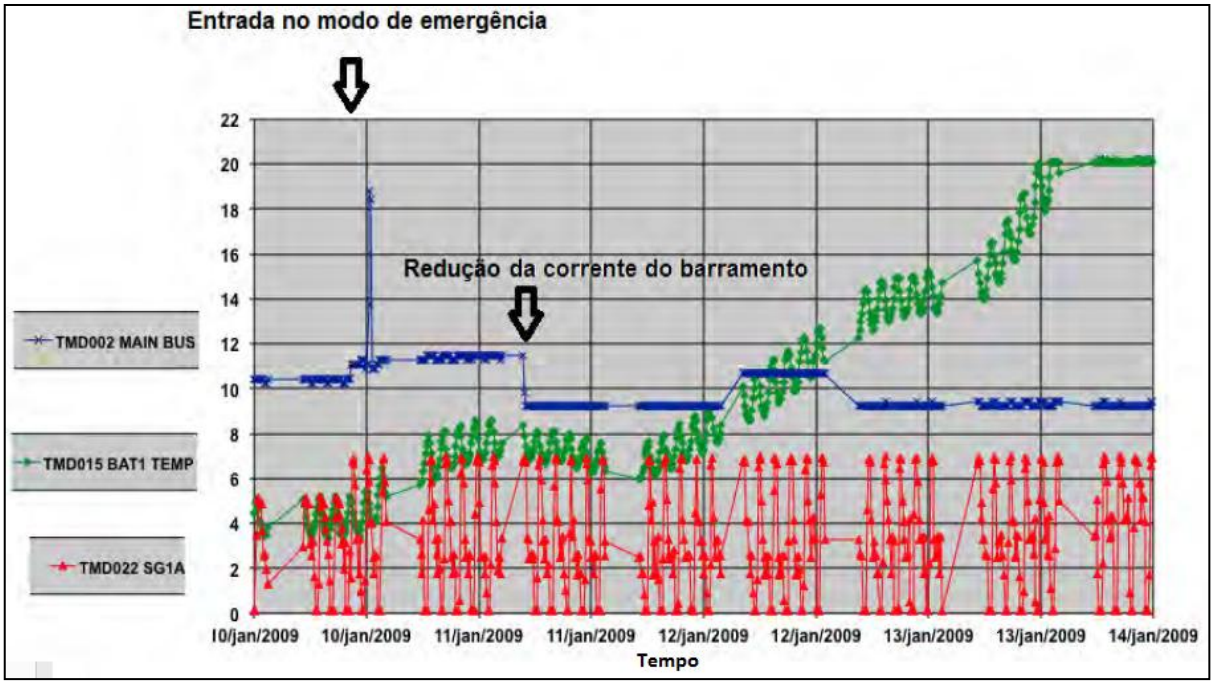
Fonte: Adaptado de Magalhães (2012).

Figura 3.9: Primeira avalanche na temperatura da bateria 1. Temperatura da bateria em ^{o}C (TMD015 BAT1 TEMP-curva verde), tensão da bateria em volts (TMD014 BAT1 VOLT-curva azul), corrente do painel solar em ampère (SAG1Acurva vermelha), Corrente do barramento em Ampère (TMD002 MAIN BUS-curva amarela) e corrente de saída do BDR em Ampère (TMD021 BDR OUTPUT-curva preta).



Fonte: Magalhães (2012).

Figura 3.10: Segunda avalanche na temperatura da bateria 1. Temperatura da bateria em oC (TMD015 BAT1 TEMP-curva verde), corrente do painel solar em Ampère (SAG1A-curva vermelha), Corrente do barramento em Ampère (TMD002 MAIN BUS-curva azul).



Fonte: Magalhães (2012).

3.3.3. Outros relatos de falhas em baterias

Gross (1984) fez uma revisão dos tipos de falhas em baterias de Níquel Cádmio em 31 espaçonaves e constatou que esse tipo de bateria raramente falha por completo. A maior parte dos problemas relatados foi a degradação da bateria evidenciada por problemas de tensão. Na maioria dos casos, o baixo desempenho das baterias foi compensado por redução de carga, o que também ocorreu nos relatos de falhas em baterias mencionados nesta monografia.

A Tabela 3.3 apresenta as falhas encontradas nas espaçonaves e o número de vezes que cada uma ocorreu. Baixa tensão de descarga foi a falha mais comum.

Tabela 3.3: As principais causas de falhas em baterias Níquel Cádmio.

Causa da falha	Número de ocorrências	Percentagem (%)
Baixa tensão de descarga	13	42
Alta tensão de descarga	5	16
Bateria ou célula em curto	5	16
Bateria, circuito ou célula em aberto	2	6
Problemas causados por outros elementos	3	10
Causas diversas ou desconhecidas	3	10

Fonte: Gross (1989).

Algumas das falhas relatadas por Gross (1989) são destacadas na Tabela 3.4. As duas primeiras falhas são falhas em aberto, chamando a atenção para a segunda falha cuja causa e consequência são muito similares ao estudo de caso 2A. As outras falhas destacadas na Tabela 3.4 são semelhantes ao estudo de caso 2B.

Na espaçonave OAO-1 da Tabela 3.4, a carga (possivelmente útil) em uma das baterias fez com que o DoD aumentasse resultando em redução da vida útil da bateria e acarretando no fenômeno de aquecimento.

Tabela 3.4: Algumas das falhas em baterias Níquel Cádmio.

Espaçonave	Falha ocorrida
Classified spacecraft	Um circuito aberto repentino ocorreu em uma das três baterias. Isso foi diagnosticado como provavelmente a abertura de um conector intercelular, causado por estresse mecânico durante a ciclagem.
171	Após 4,3 anos de operação sem problemas, uma das duas baterias ativas repentinamente falha em circuito aberto. Não foi possível determinar se o problema era com uma célula, uma junta de solda ou um conector. Em seguida, uma das duas baterias sobressalentes foi ligada para substituir a bateria que falhou e funcionou corretamente.
OAO-1	Esta espaçonave tinha uma carga sequencial entre três baterias. O sequenciador falhou, fazendo com que a carga ficasse em apenas uma das baterias. Com isso a bateria aqueceu muito, chegando a temperaturas de aproximadamente 70°C. Como resultado, o sistema necessitou ser desligado. Esta falha foi causada inteiramente pelo controle.
172, 173, 174	Depois de vários anos de funcionamento, as baterias apresentaram um aumento na tensão de carga e uma diminuição na tensão de descarga. A operação da espaçonave não foi afetada.

Fonte: Gross (1989).

3.4. Falhas relatadas x Abordagens

Como já mencionado, existem quatro abordagens utilizadas para melhorar a dependabilidade de sistemas. As abordagens são:

1. Prevenção a Falhas
2. Tolerância a Falhas
3. Correção de Falhas
4. Predição de Falhas

No estudo de caso 1 as duas primeiras abordagens de Confiabilidade foram empregadas e a discussão a respeito da falha nos mostra que estas duas abordagens poderiam ser mais bem empregadas para que a falha não voltasse a ocorrer. O uso de técnicas de alivio de tensão mecânica para proteger a solda é uma abordagem de Prevenção a falha e a redundância que poderia ser feita na cablagem é uma das medidas utilizadas na abordagem de Tolerância a Falhas. No entanto, ao analisar a recomendação de redundar a cablagem não é aplicável, devido ao peso da cablagem, a baixa probabilidade de ocorrência de falha de conexão (excluindo a questão de proteção mecância da solda) e a implementação de macanismos de comutação dos cabos. Neste caso, após a falha, a abordagem de correção de falhas não foi empregada, já que nenhuma ação foi realizada para a solução e reestabelecimento do sistema, isso porque o satélite já estava em fase final de vida útil. A análise foi *a posteriori*.

Percebemos a aplicação das duas primeiras abordagens no estudo de caso 2. Métodos, ferramentas e análises para a Prevenção e Tolerância a falhas foram empregadas. Ainda assim, no caso 2A o sistema falhou supostamente pela ausência de redundância e por falhas no controle de qualidade do fabricante do acumulador. A falha foi detectada e medidas foram tomadas para a correção da falha, mas sem sucesso. No caso 2B a falha foi de origem secundária e o sistema foi capaz de: detectar a falha, entrando em estado de emergência, e de contornar as falhas voltando ao estado correto de operação, em conformidade com a terceira abordagem

com sucesso. Com falha da bateria 2 (Caso 2A), a bateria 1 passou a ser a única operacional, passou a trabalhar e um regime acima do previsto (pois as baterias não eram redundantes) o que aparenta uma propagação da falha. A bateria 1 (Caso 2B) passou a ter um DOD muito maior que o previsto encurtando o número de ciclos que a bateria suporta. Caberia uma análise para avaliar qual a vida útil restante da bateria 1 nas novas condições de operação, com DOD maior e temperatura de operação também maior, o número de ciclos de carga e descarga certamente deve ser menor.

Os casos de falhas apresentados aqui não tratam ou exemplificam a quarta abordagem. Nenhuma das falhas foi preditas antes da ocorrência. Lembrando que esta abordagem objetiva determinar o tipo, tamanho e localização da falha antes da ocorrência visando impedir a ocorrência da falha. Por este motivo tem sido foco de investigações nos últimos anos e atualmente é um assunto em destaque.

4 ESTADO DA ARTE

Atualmente, o interesse em projetar sistemas dependáveis é o objetivo de um número crescente de organizações e empresas. A disponibilidade crescente de tecnologias complexas e altamente integradas tornou isso uma abordagem atraente e altamente investigada. Mencionar sistemas dependáveis implica em primeiro lugar, considerar sistemas com alta Confiabilidade, ou seja, estudo de técnicas e abordagens que garantam a funcionalidade do sistema. Isto aumenta o interesse pela terceira e quarta abordagens de Confiabilidade.

A Tabela 4.1 mostra algumas informações coletadas ou o estado da arte em duas abordagens de Confiabilidade: Correção de Falhas e Predição de Falhas. Estas informações foram organizadas por ano, autores e o lugar onde foram desenvolvidos os conceitos e métodos.

Tabela 4.1: Trabalhos coletados na literatura sobre estudo de falhas.

	ANO E LOCAL	AUTOR E INSTITUIÇÃO	CONCEITO
1	2005 Brasil	Baccarini, L. M. R. Universidade Federal de Minas Gerais - Tese de Doutorado	Este trabalho propõe desenvolver e implementar um sistema de detecção e diagnóstico de falhas elétricas (curto-circuito entre espiras do estator, quebra de barras e/ou anéis do rotor) e mecânicas (desalinhamento, desbalanceamento, folga mecânica) em motores de indução trifásicos. A metodologia adotada foi a obtenção de modelos matemáticos que permitam simular as falhas citadas, simulação computacional dos modelos, desenvolvimento de estratégias de detecção e diagnóstico de falhas e implementação em bancada experimental.
2	2005 China	Teaw, E., Hou, G., Gouzman, M., Tang, K.W., Kane, M., Kesluk, A., Farrell, J. A – Trabalho apresentado em evento	Os autores apresentam um projeto para o Wireless Health Monitoring System. Os autores consideram que a expectativa de vida média aumentou nos últimos anos bem como a média da expectativa de vida. A assistência médica para idosos, com 65 anos ou mais, está se tornando progressivamente mais importante. Eles discutem um projeto de um dispositivo que pode remotamente monitorar sinais vitais de usuários. O objetivo é projetar um sistema de sensores sem fio, o Health Tracker 2000, que pode monitorar os sinais vitais dos usuários e notificar parentes e pessoal médico de sua localização durante situações de risco de vida. O Health Tracker 2000 combina redes de sensores sem fio, tecnologia RFID (*Radio Frequency Identification*) e VSM (*Vital Sign Monitoring*) para monitorar os sinais vitais simultaneamente, mantendo o controle da localização dos usuários.
3	2007 Brasil	Leite, A. C.; INPE – Dissertação de Mestrado	Este trabalho estuda os modos de falhas em sensores e atuadores da PMM e propõem métodos para a sua detecção. O autor estudou estratégias de detecção de falhas: por observadores e por estimadores de estado. Neste trabalho são definidos alguns modos de falha (em conjunto com seus respectivos modelos matemáticos) como casos de estudo.

Continuação

4	2009 Estados Unidos	Gastineau, A., Johnson, T., Schultz, Departamento de Engenharia civil da Universidade de Minnesota – Artigo (A survey)	Os autores apresentam uma discussão sobre os sistemas de monitoramento de saúde e inspeções, fazem um levantamento dos métodos para tratar o envelhecimento da infra-estrutura. Centenas de pontes no estado de Minnesota estão obsoletas ou estruturalmente deficientes. Para estender com segurança a vida dessas pontes, uma inspeção rigorosa seria necessária. Essas inspeções são onerosas e demoradas. No entanto, o campo de monitoramento de saúde da ponte pode ser capaz de aliviar parte do custo. Este relatório define a terminologia relacionada ao monitoramento da saúde da ponte e fornece um glossário geral dos sistemas de monitoramento disponíveis. O relatório não detalha o sistema específico de cada uma das 38 empresas analisadas, mas oferece as características gerais, vantagens e desvantagens de um sistema. Uma visão geral de 25 sistemas baseados em diferentes técnicas é apresentada. (DIC), fadiga eletroquímica, impedância elétrica (para corrosão), medidores de tensão de resistência elétrica, indicadores de vida de fadiga, Sensores de fibra ótica, posicionamento global (GPS), radar de penetração do solo (GPR), eco de impacto, termografia infravermelha, resistência à polarização linear (para corrosão), potenciômetros de cordas (potenciômetro linear), transdutor linear variável diferencial (LVDT), Teor de cloretos, dispositivos de escorregamento, inclinação e declinação, sistemas de varredura C e ultra-sônicos e sistemas vibratórios de strain gauge.
5	2010 Estados Unidos	Wald, R., Khoshgoftaar, T., Beaujean, P. P. et al Universidade da Flórida – Trabalho apresentado em evento	Os autores consideram que "*Prognostics and health monitoring* (PHN) é um foco importante e crescente na concepção e manutenção de sistemas complexos. Está sendo aplicado a uma ampla gama de problemas, desde máquinas industriais até sistemas aviónicos e baterias. O trabalho apresenta uma revisão do trabalho existente no contexto de uma nova aplicação: reparação e manutenção de sistemas autônomos, um exemplo é uma frota de turbinas oceânicas. Várias abordagens de PHM são consideradas, incluindo técnicas modeladas e impulsionadas por dados, bem como estratégias híbridas .
6	2010 India	Mehala, N. Departamento Nacional de Engenharia Elétrica do Instituto de Tecnologia de Kurukshetra - Tese de doutorado	Discute sobre os muitos métodos de monitoramento de condições, incluindo monitoramento de vibração, monitoramento térmico, monitoramento químicos, monitoramento de emissão acústica, mas todos esses métodos de monitoramento requerem sensores caros ou ferramentas especializadas. As técnicas atuais da monitoração são aplicadas geralmente para detectar os vários tipos de falhas do motor de indução tais como a falha do rotor, falta em curto do enrolamento, falha dos rolamentos, falha da carga etc.
7	2011 Brasil	Neto, H.M.; INPE – Dissertação de Mestrado	Este trabalho estuda os requisitos e especificações para a tolerância a falha simples do sistema de controle de atitude da Plataforma MultiMissão. Apresenta conceitos relacionados à detecção de falhas, Dependabilidade e seus atributos.
8	2011 Reino Unido	Amor-Segan, M. , Jones, R. P. A Universidade de Warwick – Trabalho apresentado em evento	A complexidade aumenta o problema de diagnosticar falhas nos sistemas elétricos e eletrônicos de um veículo que, assim se torna cada vez mais difícil. Muitas falhas resultam de distúrbios ou interações de nível de sistema que são difíceis de interpretar e diagnosticar usando os diagnósticos a nível de componentes existentes que, tradicionalmente, se concentraram no diagnóstico do sistema mecânico. O autor discute a necessidade de uma nova abordagem a nível do sistema para a gestão de falhas nos sistemas eletrônicos em rede de um veículo e como isto pode ser possível, utilizando os dados das redes de dados de um veículo. Compara as diferentes abordagens da indústria de monitoramento de saúde a nível de sistema de ambientes complexos de computação distribuída e apresenta uma proposta para a aplicação de monitoramento de saúde para uma arquitetura elétrica e eletrônica automotiva.

Continuação

9	2011 Brasil	Azevedo, D. N. R.; Ambrósio, A. M.; Vieira, M Inpe – Relatório Técnico (Monografia)	Azevedo (2011) em seu relatório procura realizar uma análise em telemetria que aplica em partes a abordagem de predição de falhas. Azevedo (2011) apresenta um estudo prático que avaliou a hipótese de se utilizar algoritmos de agrupamento K-means e Expectation Maximization para detectar antecipadamente falhas utilizando as anomalias dos satélites que serviriam de apoio aos especialistas e operadores. O estudo foi eficiente em predizer anomalias onde mais de um atributo comportaram-se de forma anômala, e pelo menos uma delas saia dos limites especificados. Mas, não eficientes para pequenos e silenciosos desvios em apenas uma telemetria.
10	2012 Brasil	Sartori, I., Amaro, C. A, Júnior, M. B. S., Embiruçu, M. Universidade Federal da Bahia – Artigo de jornal	Neste trabalho é feita uma reflexão sobre a pesquisa em detecção, diagnóstico e correção de falhas, a partir de uma análise crítica das definições e terminologias utilizadas na literatura. São propostas as terminologias e definições que parecem mais apropriadas para a área, suas atividades básicas e seus objetos de estudo, a partir do confronto das visões de diversos autores. Também são apontados os principais sistemas industriais investigados nos últimos anos para a resolução de problemas de detecção, diagnóstico e correção de falhas, e são averiguadas quais são as técnicas mais aplicadas na resolução destes problemas.
11	2012 India	Kiran, M.J, Teja, S.R. K.L.University – Artigo de jornal	Os autores trabalharam para desenvolver um sistema para detectar a condição de um veículo monitorando os parâmetros internos que são usados na avaliação do estado de saúde atual do veículo. No projeto, um sistema embutido no veículo está sendo desenvolvido para gerar um relatório de saúde do veículo (*VHR - vehicle health report*) sempre que necessário pelo usuário. Ele também atua como um veículo amigável, monitorando as emissões do carro que, por sua vez ajudam na regulação (por tomar medidas adequadas para reduzir as emissões de acordo com as falhas indicadas no VHR) da poluição ambiental. Prevê os erros futuros de modo que se possa ter uma viagem ininterrupta e se possa evitar acidentes. Assim, alerta o motorista sobre erros futuros e o ajuda em uma movimentação segura. Os dados necessários para a geração do relatório de saúde consistem em valores de parâmetros (saídas de sensores embutidos) de diferentes sistemas dentro do veículo.
12	2014 India	Siddiqui1, K. M., Sahay , K, Giri, V.K. Departamento do Instituto de Engenharia e Tecnologia Universidade de Tecnologia de Gorakhpur – Artigo de jornal	Neste trabalho, o autor faz um levantamento abrangente de falhas de máquina de indução, métodos de diagnóstico e aspectos futuros no monitoramento de saúde do motor de indução. Ele apresenta vários métodos que são usados para diagnosticar falhas para o motor de indução de velocidade constante, como lógica fuzzy, redes neurais e algoritmo genético, etc. A partir do levantamento abrangente, descobriu-se que o método de Transformada Rápida de Fourier (FFT) usado para análise de estado estacionário e a Transformada Wavelet (WT) usada para análise transitória com os métodos de Processamento de Sinal Digital (DSP) dão resultados excelentes.
13	2014 Estados Unidos	Vogl, G.W., Weiss, B. A., Donmez, M. A. Instituto Nacional de Padrões e Tecnologias de Gaithersburg em Maryland – Trabalho apresentado em	As tecnologias de prognóstico e gestão da saúde Saúde (*Prognostics and Health Montoring*-PHM) reduzem o tempo e os custos para a manutenção de produtos ou processos através de atividades de diagnóstico e prognóstico eficiente e econômico. Essas atividades visam fornecer informações acionáveis para permitir uma tomada de decisão inteligente para melhorar o desempenho, segurança, Confiabilidade e manutenção. O Instituto Nacional de Padrões e Tecnologia (NIST) realizou um levantamento de normas relacionadas ao PHM aplicáveis aos sistemas de fabricação para determinar as necessidades abordadas por tais padrões, a extensão desses padrões e quaisquer pontos comuns, bem como lacunas potenciais entre os documentos. São resumidas as normas

Continuação

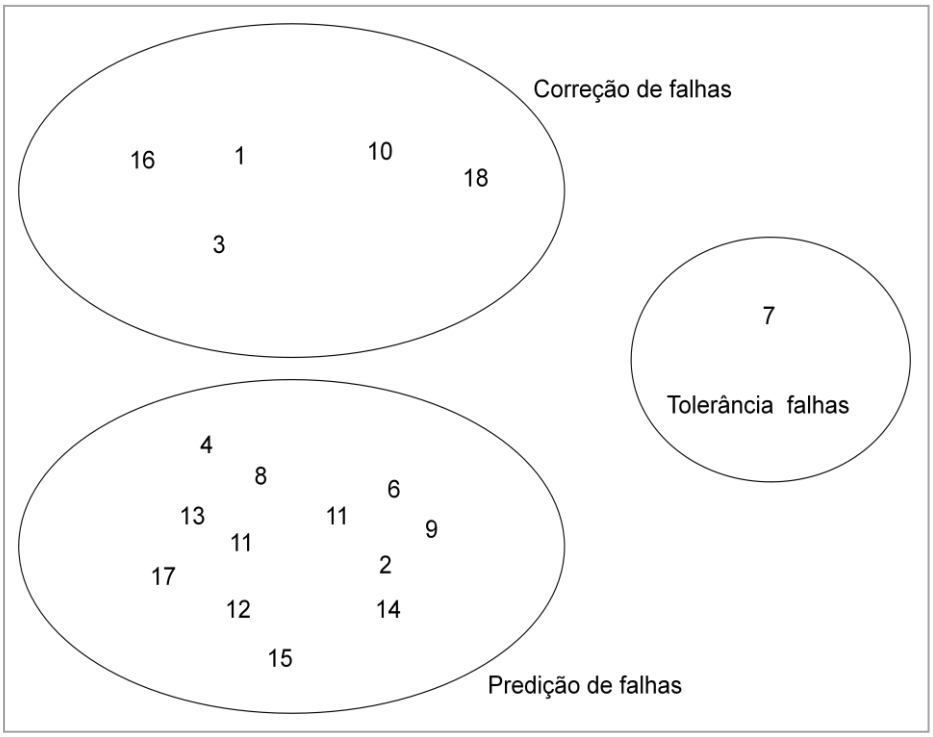
		evento	de várias organizações nacionais e internacionais, incluindo as da IEC (*International Electrotechnical Commission),* da ISO (*International Organization for Standardization*) e da SAE International. E são identificadas as áreas para futuros desenvolvimentos de normas relacionadas com o PHM. "
14	2015 Croácia	Miljković, D. – Artigo de jornal	O autor discute que os motores de indução são amplamente utilizados em unidades industriais porque são robustos, confiáveis e econômicos. A Análise de Assinatura de Corrente de Motor (MCSA) é uma técnica de monitoramento de condição usada para diagnosticar problemas em motores de indução. Está ganhando rapidamente a aceitação na indústria hoje. Os testes são realizados on-line sem interromper a produção com o motor funcionando sob carga em condições normais de operação. O MCSA pode ser usado como ferramenta de manutenção preditiva para detectar falhas comuns de motores em estágios iniciais e, como tal, prevenir falhas catastróficas caras, interrupções de produção e prolongar a vida útil do motor. Ele pode ser usado como uma ferramenta diagnóstica e poderosa adição à vibração e monitoramento térmico (verificando uma falha com mais de uma tecnologia). MCSA é um método de campo mais amplo de *Análise de Assinatura Elétrica* (ESA), útil para analisar não apenas motores de indução elétrica, mas também geradores, transformadores de potência, bem como outros equipamentos elétricos. A mais popular destas técnicas são: Análise de Assinatura Atual (CSA), Análise de Assinatura de Voltagem (VSA), *Extended Park Vector Approach* (EPVA) e Análise de Assinatura de Potência Instantânea (IPSA). O autor apresenta uma breve revisão introdutória do método, Técnicas de detecção de falhas e assinaturas atuais de várias falhas.
15	2015 India	Lambat, M. M., Wagaj, S. C. Departamento de Telecomunicações – Artigo de jornal	Projeto do sistema de monitoramento de saúde para os pesquisadores é um tema “quente”. Sistemas de monitoramento de saúde são usados em todos os campos, como hospitais, unidades de cuidados domiciliários, esportes. O trabalho discute os projetos de diferentes sistemas de monitoramento de saúde e suas especificações. Explica diferentes técnicas para projetar um sistema de monitoramento de saúde.
16	2016 Brasil	Siqueira, J.E. M.; INPE – Tese de doutorado	Esta tese estuda o problema de detecção e diagnóstico de falhas em sistemas de controle reconfiguráveis. Ele possui uma ampla revisão de literatura sobre métodos disponíveis para detecção e diagnóstico de falhas, que será bastante útil ao trabalho a ser desenvolvido. O autor aborda as falhas que acontecem fora do computador. A partir de um modelo LTI genérico, o autor propõe um repertório de falhas de sensores e de atuadores, as falhas são modeladas e caracterizadas, considerando para cada modo de falha, como as topologias das malhas de controle são afetadas, o impacto gerado (propagação temporal) nas malhas de controle, e os conteúdos espectrais específicos. Então é proposto um método que se baseia nas potências espectrais de um conjunto pré-determinado de resíduos (de sensores e de atuadores) e no uso de clusterização como meio de obtenção dos limiares de falhas.
17	2016 Alemanha	Deb, A., Vermeulen, B., Dijk, L. NXP Semiconductors, Business Unit Automotive – Trabalho apresentado em evento	Os componentes de semicondutores são obrigados a funcionar de forma confiável em aplicações críticas de segurança nos domínios automotivo e aeronáutico. As duras condições de operação e a migração para novas tecnologias aceleram o desgaste de semicondutores no campo. Assim, o envelhecimento representa um risco de Confiabilidade. Este problema é normalmente resolvido por alocação de uma margem de tempo bastante ampla para lidar com as piores condições, o que só pode ocorrer raramente na prática. O autor apresenta uma visão geral das técnicas proeminentes de monitoramento do desgaste. As técnicas de monitoramento de desgaste são desenvolvidas com várias aplicações. As três principais aplicações são: 1) Caracterização do processo, 2) Otimização da Confiabilidade de desempenho e 3) Monitoramento da saúde em tempo de execução. Muitas técnicas de monitoramento do desgaste foram investigadas. O autor

Continuação

			categoriza sistematicamente as técnicas proeminentes e avalia cada categoria para o aplicativo de monitoramento de saúde; Discute brevemente os principais mecanismos de desgaste. Apresenta As técnicas para monitoramento.
18	2017 Brasil	Pessota, F. A. Inpe – Tese de doutorado	A necessidade de operação autônoma de naves espaciais vem aumentando significativamente, e decorre do interesse crescente tanto na redução dos custos operacionais como na redução do tempo de reação e de tomada de decisões a bordo. Missões científicas e de observação da Terra já previstas e em diferentes fases de desenvolvimento no Brasil apontam na mesma direção. A definição de estratégias para tratamento de falhas nas missões brasileiras tem historicamente o seu início na fase C da missão, quando a arquitetura física do satélite já está estabelecida e os equipamentos já foram ou estão sendo adquiridos ou desenvolvidos. A definição tardia restringe o tratamento de falhas a bordo, o qual é limitado pelos recursos e mecanismos implantados a priori nos equipamentos pelos seus fornecedores e aos mecanismos e recursos passíveis de serem incluídos no software de bordo e, em consequência, restringe a possibilidade de operação autônoma da missão. Este trabalho propõe a antecipação da definição de estratégias para o tratamento de falhas sistêmicas (FDIR) em ACDHs de satélites de pequeno e médio porte para a fase da B da missão. As estratégias são propostas partindo dos requisitos funcionais de um ACDH típico, que tem como referência o ACDH em desenvolvimento para a PMM, considerando os modos mais significativos de falência das principais funções e a propagação das falhas na arquitetura funcional. A validação das estratégias é realizada por meio de modelagem e simulação utilizando o simulador TrueTime.

A figura 4.1 mostra quais as abordagens de confiabilidade são empregadas nos trabalhos apresentados na Tabela 4.1.

Figura 4.1: Relação entre as abordagens de confiabilidade e os trabalhos pesquisados até o momento.



5 CONCLUSÕES

Nesta monografia de Qualificação de Doutorado foram apresentados os conceitos básicos consistentes com o assunto da futura tese. Conceitos são referentes a Dependabilidade em Sistemas e suas métricas, dando ênfase à métrica Confiabilidade, relacionando os conceitos apresentados com algumas disciplinas cursados no curso de pós-graduação ETE do INPE.

Foram apresentados dois estudos de caso relatando falhas reais no subsistema de suprimento de energia de satélites, procurando analisar levantar/avaliar as causas das falhas, suas consequências, ações utilizadas para evitar/tolerar as falhas e ações para corrigir e restabelecer o sistema após a falha. Onde o autor demonstra sua profundidade de conhecimento e capacidade crítica do assunto.

Conceber um sistema dependável com sucesso é uma questão desafiadora que é um assunto de investigação em andamento na literatura. Diferentes abordagens têm sido adotadas para analisar e verificar a dependabilidade de um projeto de sistema. Este processo está longe de ser óbvio e muitas vezes são dificultadas devido às limitações das abordagens de análise de Confiabilidade e verificações clássicas com abordagens estáticas. Pretende-se com a futura tese de doutorado contribuir desenvolvendo uma maneira de predição de falhas em sistemas espaciais.

Esta monografia destaca a importância e relevância à temática de falhas para garantir a dependabilidade em sistemas. Mostra que muitos trabalhos vêm sendo estudados, mas ainda há muito por fazer.

REFERÊNCIAS BIBLIOGRÁFICAS

AMOR-SEGAN, M.; JONES, R. P. A framework for health monitoring of automotive electrical and electronic control systems. In: IEEE VEHICULAR NETWORKING CONFERENCE (VNC), 2011. 8p. **Proceedings…** Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6117140>. Acesso em: 16 abr.2016.

ASENEK, V.; SWEETING, M.; WARD, J.; **Reliability prediction and improvement of electronic systems on-board modern cost-effective microsatellites**. Disponível em < http://ysc.sm.bmstu.ru/microsat/e-library/ccdh/radiation/apres.htm>. Acesso em: 11 abr. 2017.

AVIZIENIS, A. et al. Basic concepts and taxonomy of dependable and secure computing. **IEEE Transactions on Dependable and Secure Computing**, v. 1, n. 1, p.1-23, Jan.-Mar. 2004.

_____. **Fundamental concepts of dependability**. Disponível em < http://pld.ttu.ee/IAF0530/16/avi1.pdf> Acesso em: 15 jan. 2017.

AZEVEDO, D. N. R.; AMBRÓSIO, A. M.; VIEIRA, M. **Estudo sobre técnicas de detecção automática de anomalias em satélites**. São José dos Campos: INPE, versão: 2011-10-16. Disponível em: <http://urlib.net/8JMKD3MGP7W/3AKGJDH>. Acesso em: 03 mar. 2017.

BACCARI, L. M. R. **Detecção e diagnóstico de falhas em motores de indução.** 207p.Tese (Doutorado em Engenharia e Elétrica) – Universidade Federal de Minas Gerais, Belo Horizonte, 2005.

BARUEL, M. F. **Estudo da variação da corrente fotogerada nos painéis solares dos satélites do INPE.** 2012. 124 p. (sid.inpe.br/mtc-m19/2012/01.31.13.30-TDI). Dissertação (Mestrado em Engenharia e Gerenciamento de Sistemas Espaciais) - Instituto Nacional de Pesquisas Espaciais, São José dos Campos, 2012. Disponível em: <http://urlib.net/8JMKD3MGP7W/3B9TDP2>. Acesso em: 20 fev. 2017.

DEB, A.; VERMEULEN, B.; DIJK, L. Overview of health monitoring techniques for reliability. In: WORKSHOP ON EARLY RELIABILITY MODELING FOR AGING AND VARIABILITY IN SILICON SYSTEMS, 2016, Germany. **Proceedings…** 2016. 4p.

DEVEAU, E. **Technical note**: understanding thermal runaway. 2015. 2p. Disponível em: <http://www.alber.com/Docs/TN-11001Thermal%20Runaway%20Detection%20Tech%20Note.pdf>. Acesso em: 15 mar. 2017.

EUROPEAN COOPERATION FOR SPACE STANDARDIZATION (ECSS) **ECSS-Q-ST-30C:** space product assurance – Dependability, Noordwijk, Holanda, 2009. 54p.

EUROPEAN COOPERATION FOR SPACE STANDARDIZATION (ECSS). **ECSS-Q-ST-30-02C:** space product assurance - failure modes, effects (and criticality) analysis (FMEA/FMECA), Noordwijk, Holanda, 2009. 74 p.

EUROPEAN COOPERATION FOR SPACE STANDARDIZATION (ECSS). **Standardization training program Q30 discipline:** dependability. The University of Arizona, Tucson, USA, 2016. Disponível em: <http://ecss.nl/wp-content/uploads/2016/09/ECSS-Training-L2-Q302016-06-28.pdf>. Acesso em: 14 dez. 2016.

FORD, F. E.; RAO, G. M.; YI, T. Y. **Handbook for handling and storage of Nickel-Cadmium batteries: lessons learned**. Nasa Reference Publication. Greenbelt : GSFC, 1994. 81p. Disponível em< https://ntrs.nasa.gov/search.jsp?R=19940022110>. Acesso em: 4 abr. 2017.

FREIRE, C. F. S. **Estudo de topologias de subsistemas de suprimento de energia de satélites e desenvolvimento de um procedimento de projeto da topologia híbrida**. 2009. 236 p. (INPE-15778-TDI/1521). Dissertação (Mestrado em Mecânica Espacial e Controle) - Instituto Nacional de Pesquisas Espaciais (INPE), São José dos Campos, 2009. Disponível em: <http://urlib.net/8JMKD3MGP8W/34RUHR2>. Acesso em: 20 fev. 2017.

GASTINEAU, A.; JOHNSON, T.; SCHULTZ, A. **Bridge health monitoring and inspections systems:** a survey of methods. Minnesota: Minnesota Department of Transportation Research Services Section Transportation Building, Sept.2009. 194p.

GLINZ, M. A. **Glossary of requirements engineering terminology**. Zurich: University of Zurich, 2014. 130p. Disponível em < http://www.future-network-cert.at/fileadmin/user_upload/pdf/FN_Cert_2016/ireb_cpre_glossary_16_en.pdf>. Acesso em: 03 fev. 2017.

GROSS, S. **Failure modes experienced on spacecraft NiCd batteries**. NASA Goddard Space Flight Center, 1984. p.197-207. (SEE N85-31371 20-33) Disponível em: < https://ntrs.nasa.gov/search.jsp?R=19850023073>. Acesso em: 10 mar. 2017.

INSTITUTO NACIONAL DE METROLOGIA, QUALIDADE E TECNOLOGIA (INMETRO). **Avaliação da conformidade**. 2012. Disponível em: < http://inmetro.gov.br/qualidade/>. Acesso em: 14 fev. 2017.

INSTITUTO NACIONAL DE PESQUISAS ESPACIAIS (INPE). O Projeto de uma missão espacial - como construir um satélite. In: SERRA JÚNIOR, Aguinaldo Martins; MILONE, André de Castro; SALLES, Carlos Eduardo Rolfsen; BASTOS NETTO, Demétrio; BARCELOS, Eduardo Dorneles; LOYOLLA, Eduardo Fábio de Carvalho; MACAU, Elbert Einstein Nehrer; MORAES, Elisabete Caria; CARVALHO, Himilcon de Castro; BRAGA, João; LEITE, João Brasil Carvalho; FERREIRA, Luiz Geraldo; SOUZA, Marcelo Lopes de Oliveira e; MOREIRA, Maurício Alves; SILVA, Meireluce Fernandes da; FERREIRA, Nelson Jesus; BOGOSSIAN, Otávio Luiz; MILANI, Paulo Giácomo; ROZENFELD, Pawel; CARMONA, Ricardo Luiz da Rocha; SERENO, Sandro Eduardo A.; ARAUJO, Sérgio Antônio Frazão; SAUSEN, Tania Maria; SCHULZ, Walkiria (Ed.). **Terceira escola do espaço**. São José dos Campos: INPE, 2002. p. 55, Capítulo 1. Disponível em CD-ROM. (INPE-8973-PUD/61). Disponível em: <http://urlib.net/6qtX3pFwXQZsFDuKxG/EG8Uq>. Acesso em: 20 jan. 2017.

INSTITUTO NACIONAL DE PESQUISAS ESPACIAIS - SERVIÇO DE GARANTIA DO PRODUTO. **Anomaly of TMD023 of Cbers FM1**. São José dos Campos: INPE, 2003. 13p.

INSTITUTO NACIONAL DE PESQUISAS ESPACIAIS - SERVIÇO DE GARANTIA DO PRODUTO. **Preliminary report on Cbers 2 anomaly of april 13th, 2005.** São José dos Campos: INPE, 2005. 53p.

ISERMANN, R. **Fault diagnosis systems:** an introduction from fault detection to fault tolerance. Heidelberg, Germany: Springer, 2006. ISBN (978-3-642-12767-0).

KIM, G.H.; PESARAN, A.; SMITH, K. Thermal abuse modeling of li-ion cells and propagation in modules. In: INTERNATIONAL SYMPOSIUM ON LARGE LITHIUM-ION BATTERY TECHNOLOGY AND APPLICATION, 4.; ADVANCED AUTOMOTIVE BATTERY CONFERENCE, 8. 2008, Tampa, Florida. **Proceedings...** Disponível em: <https://www.nrel.gov/transportation/assets/pdfs/43186.pdf>. Acesso em: 21 mar. 2017.

KIRAN, M.J.; TEJA, S.R. Vehicle health monitoring system. **International Journal of Engineering Research and Applications**, v.2, p.1162-1167, Sept.- Oct. 2012. ISBN (2248-9622).

LAFRAIA, J. R. B. **Manual de confiabilidade, mantenabilidade e disponibilidade.** Rio de Janeiro, Brasil: Qualitymark, 2001. 388p. ISBN (8573032944)

LAMBAT, M. M.; WAGAJ, S. C. Review: health monitoring system. **International Journal of Science and Research (IJSR)**, v.4, n.10,p.1-4, Oct., 2015.

LEITE, A. C. **Detecção e diagnóstico de falhas em sensores e atuadores da plataforma multi-missão**. 374p. Dissertação (Mestrado em Engenharia e Tecnologias Espaciais) - Instituto Nacional de Pesquisas Espaciais (INPE), São José dos Campos, 2007.

LEWIS, E. E. **Introduction to reliability engineering**. 2. ed. New York, NY: John Wiley and Sons, 1996. 435 p. ISBN (9780471018339).

MAGALHÃES, R. O. **Estudo de avalanche térmica em um sistema de carga e descarga de bateria em satélites artificiais.** 2012. 171 p. (sid.inpe.br/mtc-m19/2012/01.16.14.31-TDI). Tese (Doutorado em Mecânica Espacial e Controle) - Instituto Nacional de Pesquisas Espaciais, São José dos Campos, 2012. Disponível em: <http://urlib.net/8JMKD3MGP7W/3B7FP2H>. Acesso em: 20 jan. 2017.

MANELLI NETO, H. **Estudo de requisitos e especificações para a tolerância a falha simples do sistema de controle de atitude da plataforma multimissão**. 209p. Dissertação (Mestrado em Engenharia e Tecnologias Espaciais) - Instituto Nacional de Pesquisas Espaciais (INPE), São José dos Campos, 2011.

MEHALA, N. **Condition monitoring and fault diagnosis of induction motor using motor current signature analysis**. Thesis (Doctr in Electrical Engineering) - National Institute of Technology Kurukshetra, India, 2010.

MILITARY STANDARD (MIL STD). **MIL-STD-1629A:** NOTICE 1: procedures for performing a failure mode, effects and criticality analysis. Washington, 1983. 80p.

MILJKOVIĆ, D. Brief review of motor current signature analysis. **HDKBR INFO CrSNDT Journal**, v.5, n.1, p.14-23, June 2015. ISBN (1847-9340).

PORTO, R. C. F. **Análise e comparação dos manuais da família MIL-HDBK-217F e proposta de melhoria de processos de confiabilidade de equipamentos eletrônicos espaciais**. 2014. 437 p. (sid.inpe.br/plutao/2014/11.24.15.05-TDI). Dissertação (Mestrado em Engenharia e Gerenciamento de Sistemas Espaciais) - Instituto Nacional de Pesquisas Espaciais (INPE), São José dos Campos, 2014.

QI, H.; GANESAN, S.; PECHT, M. No-fault-found and intermittent failures in electronic products. **Microelectronics Reliability,** v.48, p.663-674, 2008. Disponível em <

http://www.prognostics.umd.edu/calcepapers/08_Qi_No_Fault_Found_Intermittent_Failure.pdf >. Acesso em: 05 abr. 2017.

RABELLO, A. P. S. S. **Um novo processo para melhorar a dependabilidade de sistemas espaciais entre as fases de planejamento e projeto detalhado incluindo extensões do Diagrama de Markov (DMEP) e da FMECA (FMEP) a projetos.** 2017. 344 p. IBI: <8JMKD3MGP3W34P/3MP6RNL>. (sid.inpe.br/mtc-m21b/2016/11.07.17.54-TDI). Tese (Doutorado em Engenharia e Gerenciamento de Sistemas Espaciais) - Instituto Nacional de Pesquisas Espaciais (INPE), São José dos Campos, 2016.

RELIASOFT CORPORATION. **Reliability hot wire the magazine for the reliability Professional**: conceitos de confiabilidade. 2010. Disponível em < http://www.reliasoft.com.br/hotwire/edicao58/conceito58.htm>. Acesso: 23 jan. 2016.

RELIAWIKI. **Systems analysis(RBDs and Fault Trees)** Chapter 7: Repairable systems analysis through Simulation. Disponível em: <http://www.reliawiki.org/index.php/Repairable_Systems_Analysis_Through_Simulation> Acesso: 12 jun. 2017.

SARTORI, I. et al. Detecção, diagnóstico e correção de falhas: uma proposição consistente de definições e terminologias. **Ciência & Engenharia (Science & Engineering Journal)**, v. 21, n. 2, p. 41-53, dez. 2012.

SGOBBA, T. **Treinamento em tópicos da garantia da qualidade em programas espaciais**. Notas de aula da Disciplina Garantia do Produto. Tradução por Inaldo Albuquerque; Alirio Brito, 2016.

SIDDIQUI1, K. M.; SAHAY , K.; GIRI, V.K. Health monitoring and fault diagnosis in induction motor: a review. **International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering**, v. 3, n.1, p.1-17, Jan. 2014. Disponível em:< https://www.ijareeie.com/upload/2014/january/12_Health.pdf>. Acesso em: 15 abr 2016.

SIQUEIRA, J.E. M., **Uma abordagem no domínio "frequência-estrutura" para detecção e diagnóstico de falhas em sistemas de controle reconfiguráveis**. 484p. Tese (Doutorado em Engenharia e Tecnologias Espaciais) - Instituto Nacional de Pesquisas Espaciais (INPE), São José dos Campos, 2016.

SOUZA, M. L. O.; CARVALHO, T. R. The fault avoidance and the fault tolerance approaches for increasing the reliability of aerospace and automotive systems. In: SAE BRASIL, São Paulo, 2005. **Anais...** p. 15. (INPE-13723-PRE/8916).

SOUZA, M. L. O.; PORTO, R. C. F. The fault correction and the fault prediction approaches for increasing the reliability of aerospace and automotive systems. In: SAE BRASIL, São Paulo, 2016. **Anais...** 2016.

SOUZA, P. N. Aspectos técnicos. In: SOUZA, P. N.; FONSECA, I. M. (Ed.). **AEB escola:** programa de formação continuada de professores. São José dos Campos: INPE, 2004. Parte 1, p. 18. (INPE-12213-PUD/165). Disponível em: <http://urlib.net/sid.inpe.br/marciana/2005/01.31.10.35>. Acesso em: 17 jan. 2017.

SOUZA, P. N. **Satélites e plataformas espaciais**. São José dos Campos: INPE, 2007. (INPE-12345-PUD/167 Edição 2007). Disponível em: < http://www.cdcc.usp.br/cda/oba/aeb/satelites_alta_resolucao_31jul07.pdf> Acesso em: 17 jan. 2017.

TEAW, E.; HOU, G.; GOUZMAN, M.; TANG, K.W.; KANE, M.; KESLUK, A.; FARRELL, J. A wireless health monitoring system. In: IEEE INTERNATIONAL CONFERENCE ON INFORMATION ACQUISITION, 2005, China. **Proceedings…** IEEE, 2005.

TORRES, L. C. G. **Análise do comportamento elétrico dos geradores solares da série de satélites CBERS e a confrontação dos resultados com os dados de projeto**. 2014. 201 p. (sid.inpe.br/mtc-m21b/2014/06.18.14.10-TDI). Dissertação (Mestrado em Engenharia e Gerenciamento de Sistemas Espaciais) - Instituto Nacional de Pesquisas Espaciais (INPE), São José dos Campos, 2014. Disponível em: <http://urlib.net/8JMKD3MGP5W34M/3GG84KS>. Acesso em: 21 fev. 2017.

VILLEMEUR, A. **Reliability, availability, maintainability and safety assessment**: methods and techniques. New York: Wiley, 1992. 398 p. ISBN (978-0-471-93048-8).

VOGL, G.W.; WEISS, B. A.; DONMEZ, M. A. Standards for Prognostics and Health Management (PHM) techniques within manufacturing operations. In: ANNUAL CONFERENCE OF THE PROGNOSTICS AND HEALTH MANAGEMENT SOCIETY, 2014. **Proceedings…** 2014. 13p.

WALD, R. et al. A review of prognostics and health monitoring techniques for autonomous ocean systems. In: INTERNATIONAL ISSAT ON RELIABILITY AND QUALITY IN DESIGN, 16., 5-7 August, 2010. **Proceedings…** 2010. 6p. ISBN (978-0-9763486-6-5).

TEIXEIRA, A. J. **Detecção identificação e reconfiguração de falhas múltiplas em sensores de sistemas lineares invariantes no tempo.**

2005. 312 p. IBI: <6qtX3pFwXQZGivnJSY/KaHQU>. (INPE-14487-TDI/1168). Tese (Doutorado em Mecânica Espacial e Controle) - Instituto Nacional de Pesquisas Espaciais, São José dos Campos, 2005. Disponível em: <http://urlib.net/6qtX3pFwXQZGivnJSY/KaHQU>. Acesso em: 12 abr. 2017