



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

sid.inpe.br/mtc-m21c/2018/06.11.18.44-TDI

UMA ESTRATÉGIA PARA TRATAMENTO DE FALHAS SISTÊMICAS (FDIR) EM ACDHS DE SATÉLITES DE PEQUENO E MÉDIO PORTE

Fernando Antonio Pessotta

Tese de Doutorado do Curso de Pós-Graduação em Engenharia e Tecnologia Espaciais/Engenharia e Gerenciamento de Sistemas Espaciais, orientada pelo Dr. Marcelo Lopes de Oliveira e Souza, aprovada em 24 de maio de 2018.

URL do documento original:

<http://urlib.net/8JMKD3MGP3W34R/3R9KC5P>

INPE
São José dos Campos
2018

PUBLICADO POR:

Instituto Nacional de Pesquisas Espaciais - INPE

Gabinete do Diretor (GBDIR)

Serviço de Informação e Documentação (SESID)

CEP 12.227-010

São José dos Campos - SP - Brasil

Tel.:(012) 3208-6923/7348

E-mail: pubtc@inpe.br

COMISSÃO DO CONSELHO DE EDITORAÇÃO E PRESERVAÇÃO DA PRODUÇÃO INTELECTUAL DO INPE (DE/DIR-544):

Presidente:

Dr. Marley Cavalcante de Lima Moscati - Centro de Previsão de Tempo e Estudos Climáticos (CGCPT)

Membros:

Dra. Carina Barros Mello - Coordenação de Laboratórios Associados (COCTE)

Dr. Alisson Dal Lago - Coordenação-Geral de Ciências Espaciais e Atmosféricas (CGCEA)

Dr. Evandro Albiach Branco - Centro de Ciência do Sistema Terrestre (COCST)

Dr. Evandro Marconi Rocco - Coordenação-Geral de Engenharia e Tecnologia Espacial (CGETE)

Dr. Hermann Johann Heinrich Kux - Coordenação-Geral de Observação da Terra (CGOBT)

Dra. Ieda Del Arco Sanches - Conselho de Pós-Graduação - (CPG)

Silvia Castro Marcelino - Serviço de Informação e Documentação (SESID)

BIBLIOTECA DIGITAL:

Dr. Gerald Jean Francis Banon

Clayton Martins Pereira - Serviço de Informação e Documentação (SESID)

REVISÃO E NORMALIZAÇÃO DOCUMENTÁRIA:

Simone Angélica Del Ducca Barbedo - Serviço de Informação e Documentação (SESID)

André Luis Dias Fernandes - Serviço de Informação e Documentação (SESID)

EDITORAÇÃO ELETRÔNICA:

Marcelo de Castro Pazos - Serviço de Informação e Documentação (SESID)

Murilo Luiz Silva Gino - Serviço de Informação e Documentação (SESID)



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

sid.inpe.br/mtc-m21c/2018/06.11.18.44-TDI

UMA ESTRATÉGIA PARA TRATAMENTO DE FALHAS SISTÊMICAS (FDIR) EM ACDHS DE SATÉLITES DE PEQUENO E MÉDIO PORTE

Fernando Antonio Pessotta

Tese de Doutorado do Curso de Pós-Graduação em Engenharia e Tecnologia Espaciais/Engenharia e Gerenciamento de Sistemas Espaciais, orientada pelo Dr. Marcelo Lopes de Oliveira e Souza, aprovada em 24 de maio de 2018.

URL do documento original:

<http://urlib.net/8JMKD3MGP3W34R/3R9KC5P>

INPE
São José dos Campos
2018

Dados Internacionais de Catalogação na Publicação (CIP)

Pessotta, Fernando Antonio.

P439e Uma estratégia para tratamento de falhas sistêmicas (FDIR) em ACDHs de satélites de pequeno e médio porte / Fernando Antonio Pessotta. – São José dos Campos : INPE, 2018.
xxviii + 261 p. ; (sid.inpe.br/mtc-m21c/2018/06.11.18.44-TDI)

Tese (Doutorado em Engenharia e Tecnologia Espaciais/Engenharia e Gerenciamento de Sistemas Espaciais) – Instituto Nacional de Pesquisas Espaciais, São José dos Campos, 2018.

Orientador : Dr. Marcelo Lopes de Oliveira e Souza.

1. Tratamento de falhas. 2. FDIR. 3. Diagnose. 4. Modos de falência. 5. ACDH. I.Título.

CDU 629.7.015:629.78



Esta obra foi licenciada sob uma Licença [Creative Commons Atribuição-NãoComercial 3.0 Não Adaptada](https://creativecommons.org/licenses/by-nc/3.0/).

This work is licensed under a [Creative Commons Attribution-NonCommercial 3.0 Unported License](https://creativecommons.org/licenses/by-nc/3.0/).

Aluno (a): **Fernando Antonio Pessóta**

Título: "UMA ESTRATÉGIA PARA TRATAMENTO DE FALHAS SISTÊMICAS (FDIR) EM ACDHs DE SATÉLITES DE PEQUENO E MÉDIO PORTE"

Aprovado (a) pela Banca Examinadora em cumprimento ao requisito exigido para obtenção do Título de **Doutor(a)** em

Engenharia e Tecnologia Espaciais/Eng. Gerenc. de Sistemas Espaciais

Dr. Walter Abrahão dos Santos



Presidente / INPE / São José dos Campos - SP

() Participação por Vídeo - Conferência

Dr. Marcelo Lopes de Oliveira e Souza



Orientador(a) / INPE / SJCampos - SP

() Participação por Vídeo - Conferência

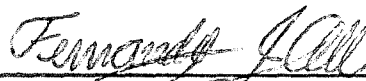
Dr. Geilson Loureiro



Membro da Banca / INPE / São José dos Campos - SP

() Participação por Vídeo - Conferência

Dr. Fernando José de Oliveira Moreira



Convidado(a) / EMBRAER / SJCampos - SP

() Participação por Vídeo - Conferência

Dr. Henrique Mohallem Paiva



Convidado(a) / UNIFESP / São José dos Campos - SP

() Participação por Vídeo - Conferência

Este trabalho foi aprovado por:

() maioria simples

unanimidade

AGRADECIMENTOS

Agradeço ao Instituto Nacional de Pesquisas Espaciais na pessoa do Dr. Mário Luiz Selingardi, chefe da Divisão de Eletrônica Aeroespacial, pela oportunidade, condições e recursos para o desenvolvimento deste trabalho.

Agradeço ao meu orientador, professor Dr. Marcelo Lopes de Oliveira e Souza pela orientação deste trabalho; pelos fundamentos sobre os quais muito do trabalho foi construído; pela dedicação e pelo entusiasmo demonstrados ao longo de todo o desenvolvimento.

Agradeço aos meus colegas do Grupo Supervisão de Bordo da Divisão de Eletrônica Aeroespacial:

Dr. Ronaldo Árias e Me. José Damião Duarte Alonso pelo apoio na análise do tratamento de falhas nos programas brasileiros e no modelamento funcional das funções de um ACDH;

Dr. Fabrício de Novaes Kucinskis pelas revisões e sugestões de melhorias deste documento;

Mestre e doutorando Fabio Batagin Armelin pela implementação dos simuladores utilizados neste trabalho;

Agradeço a Dra. Ana Paula de Sá Santos Rabello do Grupo de Engenharia da Dependabilidade do Serviço da Engenharia da Qualidade pelo apoio na utilização da FMEA.

RESUMO

O objetivo deste trabalho é propor uma estratégia para o tratamento de falhas sistêmicas (FDIR – Detecção, Isolamento/Identificação e Recuperação de Falhas) baseada na análise da arquitetura funcional do satélite, o que permite adiantar o projeto do FDIR para o início da Fase B do Ciclo de Vida de satélites de pequeno e médio porte, quando ainda é possível que as considerações de FDIR tenham um impacto mais efetivo no projeto dos subsistemas e do satélite como um todo. Para tanto, a arquitetura funcional é decomposta e os modos de falência mais significativos das funções, assim como suas causas e efeitos são identificados por meio de uma FMEA (Análise dos Modos de Falência e seus Efeitos) funcional. O comportamento cinemático do sistema é descrito por meio de grafo temporizado e os efeitos monitoráveis são identificados. Uma lógica inversa para a isolamento e/ou identificação dos modos de falência ativos é então definida com base: a) na compatibilidade dos mapas de Karnaugh de causa e efeito; b) na assinatura dos modos de falência no domínio espacial (generalizável para os domínios temporal e informacional). A estratégia é aplicada em um ACDH (Subsistema de Controle de Atitude e Tratamento de Dados) típico, que tem como referência o ACDH em desenvolvimento para a PMM (Plataforma Multimissão) e o satélite Amazônia. A arquitetura funcional do subsistema, definida com base nos documentos disponíveis, é decomposta em doze funções e cada uma dessas funções é decomposta em dois níveis funcionais. A estratégia é aplicada à função ‘Fornecer tempo de bordo’ do ACDH considerando os modos de falência ‘Não fornece tempo de bordo’ e ‘Fornecer tempo de bordo fora de especificação’. Lógicas inversas para detecção e diagnose com base na assinatura espacial dos modos de falência são propostas e repetidamente simuladas em diferentes condições para avaliação de seu desempenho. Em conclusão, o trabalho propõe uma abordagem funcional que pode ser aplicada nas fases iniciais de desenvolvimento, antecipando o tratamento de falhas sistêmicas da missão e permitindo a adoção de soluções que podem melhorar o desempenho do FDIR, o que pode, de acordo com a literatura, aumentar a autonomia e facilitar o tratamento de falhas em sistemas complexos/altamente integrados. O trabalho reinsere o tratamento de falhas em satélites como área de pesquisa no âmbito do Grupo de Supervisão de Bordo (SUBORD) da Divisão de Eletrônica Aeroespacial (DEA) do INPE.

Palavras-chave: Tratamento de falhas. FDIR. Diagnose. Modos de falência. ACDH.

A STRATEGY FOR TREATMENT OF SYSTEMIC FAULTS (FDIR) IN ACDHs OF SMALL AND MEDIUM SIZE SATELLITES

ABSTRACT

This work proposes a strategy for the treatment of systemic failures (FDIR – Fault Detection Isolation/Identification and Recovery) based on satellite functional architecture analysis, which allows to bring forward the FDIR project to the beginning of small and medium satellites Phase B Life Cycle, when it is still possible that FDIR considerations have a more effective impact on subsystem and satellite design. For this, the functional architecture is decomposed and the most significant functions failure modes, as well as their causes and effects, are identified through a functional FMEA (Failure Mode and Effects Analysis). The kinematic behavior of the system is described by means of a timed graph and the monitorable effects are identified. An inverse logic for the isolation and / or identification of active failure modes is then defined based on: a) the compatibility of cause and effect Karnaugh maps; b) the signature of the failure modes in the spatial domain (generalizable for the temporal and informational domain). The strategy is applied on a typical ACDH (Attitude Control and Data Handling Subsystem) subsystem, based on the ACDH under development for the PMM (Multimission Platform) and the Amazon satellite. The subsystem functional architecture, defined based on available documents, is decomposed in twelve functions and each of these functions is decomposed in two functional levels. The strategy is applied to the 'Provide on-board time' function considering the failure modes 'Do not provide on-board time' and 'Provide on-board time outside specification'. Inverse logics based on failure modes spatial signatures are proposed and repeatedly simulated in different conditions for performance evaluation. In conclusion, the work proposes a functional approach that can be applied on initial development phases, anticipating the mission systemic failures treatment and allowing the adoption of solutions that improve FDIR performance, which may, according to the literature, increase autonomy and facilitate failures management in complex/highly integrated systems. The work reinserts satellite failures treatment as a research area within the Onboard Supervision Group (SUBORD) of INPE Aerospace Electronic Division (DEA).

Key-Words: Failure handling. FDIR. Diagnosis. Failure modes. ACDH.

LISTA DE FIGURAS

	<u>Pág.</u>
Figura 1.1 – Estrutura do ACS com o supervisor para tratamento de falhas e as interfaces de telecomando e telemetria do satélite Ørsted.	2
Figura 1.2 – Exemplo de organização hierárquica de um FDIR.	3
Figura 1.3 – Arquitetura hierárquica dos processos aplicativos do satélite TerraSAR X.	4
Figura 2.1 – Classificação das naves espaciais pelo JHU/APL de acordo com sua massa (sem combustível).	14
Figura 2.2 – Classificação das naves espaciais pelo SSTP de acordo com sua massa (sem propelente).	15
Figura 2.3 – Operação tradicional de uma nave espacial com FCPs e MTLs; e a operação usando OBCPs.	22
Figura 2.4 – Exemplo de Arquitetura Federada.	23
Figura 2.5 – Exemplo de Arquitetura IMA.	23
Figura 2.6 – Arquitetura tradicional do sistema com o subsistema OBDH e o subsistema AOCS.	25
Figura 2.7 – Arquitetura inovada do sistema com o subsistema ACDH.	25
Figura 2.8 – Propagação do erro em sistemas computacionais.	30
Figura 2.9 – Encadeamento de falhas, erros e falências em sistemas computacionais.	31
Figura 2.10 – Encadeamento de eventos falha/falência no acidente do ônibus espacial Columbia.	33
Figura 2.11 – Representação gráfica da integração de FMEAs de diferentes níveis hierárquicos.	36
Figura 2.12 – Sumário das definições de FDI, FDD e FDIR.	40
Figura 2.13 – Desenvolvimento de um FDIR ao longo das fases do ciclo de vida.	41
Figura 2.14 – Processo de gerenciamento de falhas como parte do processo de engenharia de sistemas.	43
Figura 2.15 – Decomposição hierárquica funcional de um FDIR.	47

Figura 2.16 – Exemplo de hierarquia de FDIR para um satélite hipotético.	49
Figura 2.17 – Arquitetura com capacidade decisória.	51
Figura 2.18 – Diagrama de blocos da arquitetura Livingstone.	53
Figura 2.19 – Exemplo de um TFPG.	56
Figura 2.20 – Fluxo de trabalho para definição do repertório de falhas da missão WISE.	62
Figura 2.21 – Alocação de responsabilidades para proteção contra falhas na Cassini.	65
Figura 2.22 – Diagrama de blocos da arquitetura do AACS FP.	67
Figura 2.23 – Diagrama de blocos do subsistema ACDH e suas principais interfaces com subsistemas da Plataforma e Carga Útil.	73
Figura 3.1 – Relação entre falha e falência.	79
Figura 3.2 – Relação entre falha, falência e efeito.	79
Figura 3.3 – Processo de engenharia de sistemas.	84
Figura 3.4 – Integração FMEA e TFPG em uma Arquitetura Hierárquica.	88
Figura 3.5 – Causas dos modos de falência localizadas em regiões que podem ser tratadas de forma independente.	91
Figura 3.6 – Causas dos modos de falência intermitente e dos modos de falência permanente localizadas na mesma região.	91
Figura 3.7 – Exemplo de propagação de modos de falência pela estrutura do sistema.	92
Figura 3.8 – Exemplo de propagação de modos de falência por uma rede combinatória.	94
Figura 3.9 – Representação funcional da propagação dos modos de falência.	95
Figura 3.10 – Representação da identificação do modo de falência ativo a partir de sua assinatura.	96
Figura 3.11 – Analogia entre função bijetora e propagação dos modos de falência.	97
Figura 3.12 – Analogia entre função sobrejetora e propagação dos modos de falência caracterizando a ambiguidade de assinaturas.	98
Figura 3.13 – Desambiguação de assinaturas transformando a função sobrejetora em bijetora.	98

Figura 3.14 – (a) Efeito monitorado EM causado pela propagação mutuamente exclusiva de MF_1 e MF_2 . (b) Mapa de Karnaugh para o efeito E	100
Figura 3.15 – (a) Adição do efeito monitorado E_2M_2 independente de MF_1 . (b) Mapa de Karnaugh para os efeitos E_1 e E_2	100
Figura 3.16 – (a) Mapa de compatibilidade da função OU Exclusivo desambiguada. (b) Mapa de Karnaugh de MF_1 . (c) Mapa de Karnaugh de MF_2	101
Figura 3.17 – (a) Efeito monitorado EM causado pela propagação inclusiva de MF_1 e MF_2 ; (b) Mapa de Karnaugh para o efeito E	102
Figura 3.18 – (a) Adição do efeito monitorado E_1M_1 independente de MF_2 , e de E_2M_2 independente de MF_1 ; (b) Mapa de Karnaugh para os efeitos E_1 , E_2 e E_3	103
Figura 3.19 – (a) Mapa de compatibilidade da função OU inclusivo desambiguada. (b) Mapa de Karnaugh de MF_1 . (c) Mapa de Karnaugh de MF_2	104
Figura 3.20 – (a) Efeito monitorado EM causado pela propagação conjuntiva de MF_1 e MF_2 ; (b) Mapa de Karnaugh para o efeito E	104
Figura 3.21 – (a) Adição do efeito monitorado E_1M_1 independente de MF_2 e de E_2M_2 independente de MF_1 ; (b) Mapa de Karnaugh para os efeitos E_1 , E_2 e E_3	105
Figura 3.22 – (a) Mapa de compatibilidade da função E desambiguada. (b) Mapa de Karnaugh de MF_1 . (c) Mapa de Karnaugh de MF_2	106
Figura 3.23 – Analogia entre função injetora e a propagação dos modos de falência.	107
Figura 3.24 – Analogia entre função bijetora e o monitoramento de efeitos quando os monitores não apresentam falências.	108
Figura 3.25 – Analogia entre função bijetora e o monitoramento de efeitos: (a) quando a falência do monitor causa ambiguidade na assinatura; ou (b) quando a falência do monitor causa assinatura que não faz parte da imagem da função direta.	109

Figura 3.26 – Fluxograma básico de lógica acionada por evento para isolamento e/ou identificação por diferença de assinaturas.....	111
Figura 3.27 – Fluxograma básico de lógica acionada temporalmente para isolamento e/ou identificação por diferença de assinaturas.	112
Figura 3.28 – Fluxograma básico de lógica que combina acionamento por evento e acionamento temporal para isolamento e/ou identificação por diferença de assinaturas após a propagação dos modos de falência.	113
Figura 3.29 – Fluxograma básico para isolamento e/ou identificação com critério de biunivocidade.....	114
Figura 3.30 – Fluxograma básico para isolamento e/ou identificação com critério de biunivocidade e verificação de precedência.	115
Figura 3.31 – Fluxograma básico para isolamento e/ou identificação combinando os domínios espacial e temporal.	116
Figura 4.1 – Nível 1 e nível 2 da arquitetura funcional hierárquica do subsistema ACDH.....	124
Figura 4.2 - Decomposição funcional da função ‘Fornecer Tempo de Bordo’.	127
Figura 4.3 – Classificação de comandos de acordo com sua origem, forma de distribuição e tempo de atuação.	131
Figura 4.4 – Decomposição funcional da função ‘Fornecer Comando Direto’.	133
Figura 4.5 – Decomposição funcional da função Fornecer Comando Roteado Imediato.	136
Figura 4.6 – Decomposição das funções do subsistema ACDH.	139
Figura 4.7 – Arquitetura funcional hierárquica do subsistema ACDH.....	140
Figura 4.8 – Diagrama de propagação para função ‘Fornecer Tempo de Bordo’ no nível 1.	162
Figura 4.9 – Diagrama de propagação da função ‘Fornecer Tempo de Bordo’ no nível 2.	165
Figura 4.10 – Diagrama de propagação para função ‘Fornecer Tempo de Bordo’ no nível 3.....	167
Figura 4.11 – Diagrama de propagação da função ‘Fornecer Tempo de Bordo’ reduzida.....	171

Figura 4.12 – Diagrama de propagação da função ‘Fornecer Tempo de Bordo’ reduzida com os pseudos modos falência.....	173
Figura 4.13 – Mapa de Karnaugh da assinatura espacial dos modos e pseudo modo de falência da função ‘Fornecer Tempo de Bordo’ reduzida.....	174
Figura 4.14 – Mapa de compatibilidade da função ‘Fornecer Tempo de Bordo’ reduzida.....	175
Figura 4.15 – Mapa de Karnaugh para (a) <i>MF1</i> , (b) <i>MF2</i> , (c) <i>MF3</i> , (d) <i>MF4</i> e (e) <i>MF1’</i>	176
Figura 4.16 – Diagrama de propagação de um caso da literatura.....	178
Figura 4.17 – Decomposição do diagrama de propagação do caso da literatura: a) subdiagrama da propagação de <i>MF1</i> ; b) subdiagrama da propagação de <i>MF2</i> ; c) subdiagrama da propagação de <i>MF3</i> ; subdiagrama da propagação de <i>MF4</i>	179
Figura 4.18 – Diagrama de propagação do caso da literatura reduzido.	181
Figura 4.19 – Mapa de Karnaugh da assinatura espacial do caso da literatura reduzido.....	182
Figura 4.20 – Diagrama de propagação do caso da literatura reduzido desambiguado.	182
Figura 4.21 – Mapa de Karnaugh da assinatura espacial do caso da literatura reduzido desambiguado.	183
Figura 4.22 – Mapa de compatibilidade do caso da literatura reduzido desambiguado.	184
Figura 4.23 – Mapas de Karnaugh para: (a) <i>MF1</i> ; (b) <i>MF2</i> ; (c) <i>MF3</i> ; (d) <i>MF4</i>	185
Figura 4.24 – Modelamento da falência de monitores como falso positivo e falso negativo.	186
Figura 5.1 – Janela principal do GTKWave com formas de onda da simulação da função ‘Fornecer Tempo de Bordo’.....	189
Figura 5.2 – Janela do Notepad++ com trecho inicial do código VHDL da simulação da função ‘Fornecer Tempo de Bordo’.....	190

Figura 5.3 – Sumário dos resultados corretos da diagnose da função ‘Fornecer Tempo de Bordo’ quando nenhum dos monitores apresenta falência.....	199
Figura 5.4 – Sumário dos resultados corretos da diagnose da função ‘Fornecer Tempo de Bordo’ quando um dos monitores apresenta falência.	200
Figura 5.5 – Sumário dos resultados corretos da diagnose da função ‘Fornecer Tempo de Bordo’ quando dois dos monitores apresentam falência.	201
Figura 5.6 – Sumário dos resultados corretos da diagnose do caso da literatura quando nenhum dos monitores apresenta falência.....	204
Figura 5.7 – Sumário dos resultados corretos da diagnose do caso da literatura quando um dos monitores apresenta falência.	205
Figura 5.8 – Sumário dos resultados corretos da diagnose do caso da literatura quando dois dos monitores apresentam falência.	207
Figura A.1 – Decomposição funcional da função Fornecer Comando Roteado Temporizado.	228
Figura A.2 – Decomposição funcional da função ‘Fornecer Comando Imediato’.	230
Figura A.3 – Decomposição funcional da função ‘Fornecer Comandos Temporizados’.....	232
Figura A.4 – Classificação de telemetrias de acordo com a origem e o tempo de transmissão.....	233
Figura A.5 – Decomposição funcional da função ‘Fornecer Telemetria Tempo Real’.....	235
Figura A.6 – Decomposição funcional da função ‘Fornecer Telemetria Armazenada’.....	237
Figura A.7 – Decomposição funcional da função Estimar Atitude.....	238
Figura A.8 – Decomposição funcional da função ‘Propagar Órbita’.	240
Figura A.9 – Decomposição funcional da função ‘Comandar Atuadores’.....	243
Figura A.10 – Decomposição funcional da função ‘Gerenciar Modos e Transições’.....	245

LISTA DE TABELAS

	<u>Pág.</u>
Tabela 2.1 – Classificação de satélites proposta por Martin N Sweeting em 1991.	13
Tabela 2.2 – Classificação de satélites de acordo com a massa.	16
Tabela 2.3 – Comparação de satélites de observação ótica da Terra de pequeno, médio e grande porte.	17
Tabela 2.4 – Níveis de autonomia para a execução da missão.	27
Tabela 2.5 – Níveis de autonomia para o gerenciamento de dados.	27
Tabela 2.6 – Níveis de autonomia para o gerenciamento de falhas a bordo. ..	28
Tabela 2.7 – Detecção e recuperação de falhas nos níveis hierárquicos do FDIR.....	50
Tabela 2.8 – Detecção de Falências e Recuperação do Subsistema OBDH dos Satélites CBERS	71
Tabela 2.9 – Sumário do tratamento de falhas da Plataforma nas missões CBERS.....	72
Tabela 2.10 – Sumário do tratamento de falhas da Plataforma no satélite Amazonia 1.....	74
Tabela 2.11 – Sumário das arquiteturas e métodos analisados nesta revisão. 75	
Tabela 3.1 – Macroprocessos que Implementam os Subsistemas OBDH e AOCS.....	81
Tabela 3.2 - Modelos de tratamento de dados de falhas	86
Tabela 3.3 – Avaliação da Originalidade da Proposta.....	119
Tabela 4.1 – Análise Funcional Hierárquica dos Efeitos dos Modos de Falências da Função ‘Fornecer Tempo de Bordo’.	143
Tabela 4.2 – Análise Funcional Hierárquica dos Efeitos dos Modos de Falências da Função ‘Fornecer Comando Direto’.	147
Tabela 4.3 – Análise Funcional Hierárquica dos Efeitos dos Modos de Falências da Função ‘Fornecer Comando Roteado Imediato’. .	149

Tabela 4.4 – Falhas Identificadas na FMEA Funcional do ACDH para as Funções ‘Fornecer tempo de bordo’, ‘Fornecer comando direto’, ‘Fornecer comando roteado imediato’.....	155
Tabela 4.5 – Assinatura no domínio dos modos de falência da função ‘Fornecer Tempo de Bordo’.....	170
Tabela 4.6 – Assinaturas e Isolação/identificação dos modos de falência da função ‘Fornecer Tempo de Bordo’ reduzida.	172
Tabela 4.7 – Agrupamento dos dos modos de falência da função ‘Fornecer Tempo de Bordo’ reduzida em pseudos modos de falência.....	173
Tabela 4.8 – Assinaturas no domínio espacial dos modos de falência do caso da literatura.	180
Tabela 5.1 – Resultados das simulações da lógica proposta para a diagnose por diferença de assinaturas e detecção por eventos.	192
Tabela 5.2 – Resultados das simulações da lógica proposta para a diagnose por biunivocidade e detecção por eventos.	193
Tabela 5.3 – Resultados das simulações da lógica proposta para a diagnose por biunivocidade e verificação de precedência e detecção por eventos.....	193
Tabela 5.4 – Resultados das simulações da lógica proposta para a diagnose por diferença de assinaturas aplicada após a propagação das falências e detecção por eventos.	194
Tabela 5.5 – Resultados das simulações da lógica proposta para a diagnose por diferença de assinaturas e detecção por amostragem periódica.....	195
Tabela 5.6 – Resultados das simulações da lógica proposta para a diagnose por biunivocidade e detecção por amostragem periódica.	195
Tabela 5.7 – Resultados das simulações da lógica proposta para a diagnose por biunivocidade e verificação de precedência e detecção por amostragem periódica.....	196
Tabela 5.8 – Resultados das simulações da lógica proposta para a diagnose por diferença de assinaturas aplicada após a propagação das falências e detecção por amostragem periódica.	196

Tabela 5.9 – Sumário dos resultados corretos da diagnose da função ‘Fornecer Tempo de Bordo’.....	197
Tabela 5.10 – Sumário dos tempos médios necessários para a diagnose correta da função ‘Fornecer Tempo de Bordo’ pelas lógicas propostas.....	198
Tabela 5.11 – Sumário dos resultados corretos da diagnose do caso da literatura.....	202
Tabela 5.12 – Sumário dos tempos médios necessários para a diagnose correta do caso da literatura pelas lógicas propostas.....	203
Tabela B.1 – Análise Funcional Hierárquica dos Efeitos dos Modos de Falências da Função ‘Fornecer Comando Roteado Temporizado’	247
Tabela B.2 – Análise Funcional Hierárquica dos Efeitos dos Modos de Falências da Função ‘Fornecer Comandos Imediatos’	248
Tabela B.3 – Análise Funcional Hierárquica dos Efeitos dos Modos de Falências da Função ‘Fornecer Comandos Temporizados’	249
Tabela B.4 – Análise Funcional Hierárquica dos Efeitos dos Modos de Falências da Função ‘Fornecer Telemetria de Tempo Real’	250
Tabela B.5 – Análise Funcional Hierárquica dos Efeitos dos Modos de Falências da Função ‘Fornecer Telemetria Armazenada’	251
Tabela B.6 – Análise Funcional Hierárquica dos Efeitos dos Modos de Falências da Função ‘Estimar Atitude’	252
Tabela B.7 – Análise Funcional Hierárquica dos Efeitos dos Modos de Falências da Função ‘Propagar Órbita’	253
Tabela B.8 – Análise Funcional Hierárquica dos Efeitos dos Modos de Falências da Função ‘Comandar Atuadores’	257
Tabela B.9 – Análise Funcional Hierárquica dos Efeitos dos Modos de Falências da Função ‘Gerenciar Modos e Transições’.....	258
Tabela C.1 – Análise Funcional/Física dos Efeitos dos Modos de Falências da Função ‘Prover Processamento’	259

LISTA DE ABREVIATURAS E SIGLAS

ACDH	<i>Attitude Control and Data Handling Subsystem</i> – Subsistema de Controle de Atitude e Tratamento de Dados
ADM-Aeolus	<i>Atmospheric Dynamics Mission Aeolus Satellite</i>
AOCS	<i>Attitude and Orbit Control Subsystem</i> – Subsistema de Controle de Atitude e Órbita
CAST	<i>Chinese Academy of Space Technology</i>
CBERS	<i>China-Brazil Earth Resources Satellite</i>
CMD	Comando
CMDtemp	Comando Temporizado
ECSS	<i>European Cooperation for Space Standardization</i>
EMI	Electromagnetic Interference
EQUARS	<i>Equatorial Atmosphere Research Satellite</i>
ESA	<i>European Space Agency</i>
FCP	<i>Flight Control Procedures</i>
FDD	<i>Fault Detection and Diagnosis</i> – Detecção e Diagnose de Falha
FDI	<i>Fault Detection and Isolation</i> – Detecção e Isolação de Falhas
FDIR	<i>Fault Detection Isolation/Identification and Recovery</i> – Detecção, Isolação/Identificação e Recuperação de Falhas
FM	<i>Fault Management</i> (NASA-HDBK-1002) – Gerenciamento de Falhas
FMEA	<i>Failure Mode and Effects Analysis</i> (NASA-HDBK-1002) – Análise dos Modos de Falência e seus Efeitos
FMECA	<i>Failure Modes, Effects and Criticality Analysis</i> (ECSS-E-ST 70-11) – Análise dos Modos de Falência, seus Efeitos e Criticidade
FP	<i>Fault Protection</i> – Proteção contra Falhas
FTA	<i>Fault Tree Analysis</i> (NASA-HDBK-1002) – Análise da Árvore de Falha
GOCE	Gravity field and steady-state Ocean Circulation Explorer Satellite
GTEO	<i>Global Terrestrial Ecosystem Observatory</i>
IEEE	Instituto dos Engenheiros Eletricistas e Eletrônicos
IFAC	<i>International Federation of Automatic Control</i>
IFIP	<i>International Federation for Information Processing</i>
INPE	Instituto Nacional de Pesquisas Espaciais

JPL	<i>Jet Propulsion Laboratory</i>
MECB	Missão Espacial Completa Brasileira
MIRAX	Monitor e Imageador de Raios X
MTL	<i>Mission Time Line</i>
NASA	<i>National Aeronautics and Space Administration</i> – Administração Nacional da Aeronáutica e Espaço
OAOC	<i>Orbiting Astronomical Observatory C Satellite</i>
OBCP	<i>On-Board Control Procedure</i>
OBDH	<i>On-Board Data Handling Subsystem</i>
PMM	Plataforma Multimissão – Multimission Platform
PSS	<i>Power Supply Subsystem</i>
PUS	<i>Packet Utilization Standard</i>
RM	Gerenciamento de Redundâncias – <i>Redundancy Management</i>
RT	Referência de Tempo
SACI	Satélite de Aplicações Científicas
SCD	Satélite de Coleta de Dados
SEU	<i>Single Event Upset</i>
S/S	Subsistema
TB	Tempo de Bordo
TC	Telecomando
TFPG	<i>Timed Failure Propagation Graph</i>
TM	Telemetria
TMarmz	Telemetria Armazenada
WG	Working Group

SUMÁRIO

	<u>Pág.</u>
1 INTRODUÇÃO	1
1.1 Contexto	1
1.2 Motivações e Justificativas	5
1.2.1 Tratamento Tardio de Falhas Sistêmicas.....	5
1.2.1.1 Problema.....	5
1.2.1.2 Motivação – Antecipação do Tratamento de Falhas Sistêmicas	6
1.2.2 Baixa Autonomia Operacional.....	6
1.2.2.1 Problema.....	6
1.2.2.2 Motivação – Aumento da Autonomia.....	7
1.2.3 Dificuldade em Tratar Falhas de Sistemas Complexos e/ou Integrados.....	8
1.2.3.1 Problema.....	8
1.2.3.2 Motivação – Tratamento de Falhas de Sistemas Complexos e/ou Altamente Integrados	8
1.2.4 Impactos Negativos na Área Espacial.....	9
1.2.4.1 Problema.....	9
1.2.4.2 Motivação – Prevenção de Impactos Negativos nas Missões.....	9
1.3 Objetivo	10
1.4 Originalidade, Generalidade e Utilidade	10
1.5 Organização do Trabalho	11
2 CONCEITOS BÁSICOS E REVISÃO BIBLIOGRÁFICA	13
2.1 Classes de Satélites	13
2.2 Ciclo de Vida de uma Missão Espacial.....	17
2.3 Operação de Missões Espaciais	18
2.4 Subsistema ACDH.....	22
2.5 Autonomia	25
2.6 Falha, Erro e Falência (“Fault, Error and Failure”).....	28
2.7 FMEA/FMECA	34
2.7.1 FMEA Funcional.....	37
2.7.2 Modos de Falência de uma Função.....	37

2.8	FDIR (Fault Detection, Isolation and Recovery)	38
2.8.1	Introdução	38
2.8.2	Detecção, Isolação, Identificação e Recuperação	39
2.8.3	Processo de Desenvolvimento do Tratamento de Falhas (FDIR)	40
2.8.4	Recursos e Mecanismos de um FDIR.....	44
2.8.4.1	Redundância	44
2.8.4.2	Modo Seguro de Operação	45
2.8.5	Estratégias de FDIR.....	45
2.8.6	Arquiteturas de FDIR	46
2.8.6.1	Arquiteturas Hierárquicas	46
2.8.6.2	Arquitetura com Capacidade Decisória	50
2.8.7	Métodos de Detecção, Isolação, Identificação e Recuperação.....	51
2.8.7.1	Métodos Baseados em Modelos	52
2.8.7.2	Métodos que Utilizam Redes Bayesianas	53
2.8.7.3	Métodos que Utilizam Lógica <i>Fuzzy</i>	54
2.8.7.4	Métodos Baseados em Automação Cognitiva	54
2.8.7.5	Métodos Baseados em TFPG (Timed Failure Propagation Graph)	55
2.8.7.6	Trabalhos Desenvolvidos no INPE	58
2.8.8	Algumas Estratégias de FDIR Utilizadas em Missões Espaciais	58
2.8.8.1	Satélite Ørsted.....	58
2.8.8.2	Satélite WISE	60
2.8.8.3	Missão Cassini-Huygens	63
2.8.8.4	Formação de Satélites TerraSAR-X e TanDEM-X	68
2.8.8.5	Formação Autônoma de Satélites	69
2.8.8.6	Satélites CBERS 3&4.....	69
2.8.8.7	PMM e o Satélite Amazonia 1	72
2.8.9	Sumário das Arquiteturas e Métodos de FDIR Revistos	74
3	PROPOSTA DE ESTRATÉGIA PARA O TRATAMENTO DE FALHAS	79
3.1	Conceitos de Falha, Erro e Falência usados neste Trabalho	79
3.2	Implicações do Tratamento de Falhas Sistêmicas na Fase C da Missão, como atualmente adotado no INPE	80

3.3	Abordagens para a Definição da Estratégia	83
3.3.1	Descrição Funcional da Arquitetura do Subsistema.....	83
3.3.2	Descrição do Comportamento do Sistema por meio de Modelos de Falhas	85
3.3.3	Tratamento de Falências Funcionais	88
3.3.3.1	Modo de Falência ‘Não Realizar a Função’	88
3.3.3.2	Modo de Falência ‘Realizar a Função Fora de Especificação’	89
3.3.3.3	Modo de Falência ‘Realizar a Função Intermitentemente’	89
3.3.4	Abordagem por Teoria e Análise para a Diagnose de Falências no Domínio Espacial	91
3.3.4.1	Hipóteses para a Diagnose de Falências no Domínio Espacial	93
3.3.4.2	Propagação e Diagnose no Domínio Espacial Modeladas como Funções Direta e Inversa	95
3.3.5	Abordagem por Modelagem e Simulação para a Diagnose de Falências no Domínio Espacial	109
3.3.5.1	Lógica para Isolação e/ou Identificação por Diferença de Assinaturas.....	110
3.3.5.2	Lógica para Isolação e/ou Identificação por Biunivocidade.....	113
3.3.5.3	Lógica para Isolação e/ou Identificação por Biunivocidade e Verificação de Precedência.....	114
3.3.5.4	Isolação e/ou Identificação nos Domínios Espacial / Temporal.....	115
3.4	Sumário da Estratégia para o Tratamento de Falhas Sistêmicas	116
3.5	Avaliação da Originalidade da Proposta.....	118
4	APLICAÇÃO DA ESTRATÉGIA A UM ACDH BASEADO NA PMM DO INPE, E A UM CASO DA LITERATURA	123
4.1	Aplicação da Estratégia a um ACDH baseado na PMM do INPE.....	123
4.1.1	Arquitetura Funcional do ACDH	123
4.1.1.1	Funções do ACDH	123
4.1.1.2	Função ‘Fornecer Tempo de Bordo’	125
4.1.1.3	Função ‘Fornecer Comandos’	130
4.1.1.4	Comandos Gerados em Solo	131
4.1.1.5	Consolidação da Arquitetura Funcional do ACDH.....	138

4.1.2	FMEA Funcional Hierárquica do ACDH	141
4.1.3	Repertório de Falhas do ACDH	154
4.1.4	Tratamento da Função ‘Fornecer Tempo de Bordo’	155
4.1.4.1	Comportamento Cinemático do ACDH na Presença de Falências da Função ‘Fornecer Tempo de Bordo’	156
4.1.4.2	Detecção e Diagnose	168
4.1.5	Aplicação da Abordagem por Modelagem e Simulação.....	170
4.1.6	Aplicação da Abordagem por Teoria e Análise	171
4.2	Aplicação da Estratégia a um Caso da Literatura.....	177
4.2.1	Abordagem por Modelagem e Simulação	177
4.2.2	Abordagem por Teoria e Análise	180
5	VALIDAÇÃO DA ESTRATÉGIA PARA O TRATAMENTO DE FALHAS	187
5.1	Ambiente de Modelagem e Simulação	187
5.1.1	Simulador GHDL	187
5.1.2	Visualizador GTKWave	188
5.1.3	Notepad++	189
5.1.4	GNU Make	190
5.2	Principais Características do Simulador das Lógicas de Detecção e Diagnose	190
5.3	Resultados das Simulações	191
5.3.1	Resultados da Simulação da Função ‘Fornecer Tempo de Bordo’	192
5.3.2	Resultados das Simulações de um Caso da Literatura.....	194
5.4	Análise dos Resultados das Simulações	197
5.4.1	Análise dos Resultados Obtidos para a Função ‘Fornecer Tempo de Bordo’	197
5.4.1.1	Nenhuma Falência de Monitor	198
5.4.1.2	Uma Falência de Monitor	200
5.4.1.3	Duas Falências de Monitor.....	201
5.4.2	Análise dos Resultados Obtidos para o Caso da Literatura.....	202
5.4.2.1	Nenhuma Falência de Monitor	203
5.4.2.2	Uma Falência de Monitor	204
5.4.2.3	Duas Falências de Monitor.....	206

6	CONCLUSÕES	209
6.1	Contribuições.....	209
6.2	Sugestões para Trabalhos Futuros	210
	REFERÊNCIAS BIBLIOGRÁFICAS	213
	APÊNDICE A – DECOMPOSIÇÃO FUNCIONAL DAS FUNÇÕES DO ACDH	
	(CONTINUAÇÃO).....	227
A.1	Comandos Gerados em Solo (Continuação)	227
A.1.1	Função ‘Fornecer Comandos Roteados Temporizados’	227
A.2	Comandos Gerados em Bordo	228
A.2.1	Função ‘Fornecer Comandos Imediatos’	228
A.2.2	Função ‘Fornecer Comandos Temporizados’	230
A.3	Função ‘Fornecer Telemetrias’	232
A.3.1	Classificação das Telemetrias e Caracterização dos seus Modos de Falência.....	232
A.3.2	Função ‘Fornecer Telemetrias de Tempo Real’	233
A.3.3	Função ‘Fornecer Telemetrias Armazenadas’	235
A.4	Função ‘Estimar Atitude’	237
A.5	Função ‘Propagar Órbita’	239
A.6	Função ‘Comandar Atuadores’	242
A.7	Função ‘Gerenciar Modos e Transições’.....	243
	APÊNDICE B – FMEA FUNCIONAL HIERÁRQUICA DO ACDH	
	(CONTINUAÇÃO).....	247
	APÊNDICE C – FMEA FUNCIONAL/FÍSICA DA FUNÇÃO ‘PROVER	
	PROCESSAMENTO’	259

1 INTRODUÇÃO

1.1 Contexto

No início da exploração do espaço por meio de veículos espaciais, a responsabilidade pelas tarefas operacionais da missão era concentrada no Segmento Solo. A utilização de computadores embarcados, iniciada em 1964 com a missão Gemini IV e introduzida em missões não tripuladas em 1972, com o satélite *Orbiting Astronomical Observatory C* (OAO-C) (TOMAYKO, 1988), permitiu ao Segmento Solo transferir tarefas operacionais para o Segmento Espacial, onde passaram a ser executadas de forma autônoma. O satélite Landsat 2, por exemplo, lançado em 1975, já realizava a bordo o tratamento de telecomandos temporizados e verificava se as telemetrias estavam dentro de seus limites (TOMAYKO, 1988).

Desde então, mais e mais tarefas têm sido progressivamente transferidas para o Segmento Espacial, e a necessidade de operações autônomas avançadas em espaçonaves vem aumentando significativamente. Esta necessidade não se restringe às missões interplanetárias, onde a autonomia é um requisito essencial, mas está também presente em missões em órbita do planeta, como as de observação da Terra, em vista do interesse crescente na redução dos custos operacionais dessas missões (GESSNER et al., 2004).

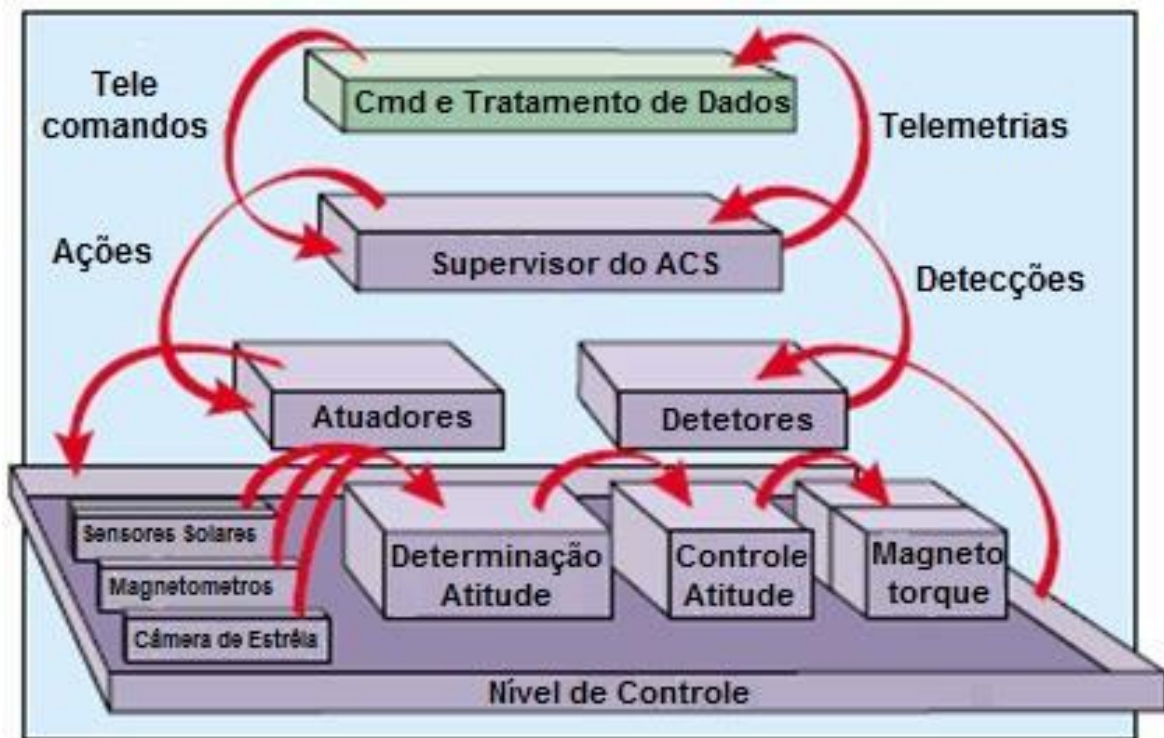
Nesse contexto, o gerenciamento de falhas a bordo é essencial para uma espaçonave (GESSNER et al., 2004; OLIVE, 2010) e sua implementação deve ser compatível com o nível de autonomia adotado para a missão.

O gerenciamento de falhas a bordo é baseado no paradigma Detecção, Isolamento/Identificação e Recuperação de Falhas (*Fault Detection, Isolation/Identification and Recovery - FDIR*), o qual provê para o segmento espacial a capacidade de sobreviver a situações críticas de forma autônoma, sem a intervenção do segmento solo.

As estratégias (arquiteturas + métodos) de FDIR variam fortemente com os tipos e cenários das missões e os benefícios esperados com relação aos requisitos de custo, desempenho e disponibilidade.

As estratégias de FDIR, ou seja, as arquiteturas mais os métodos de detecção, isolamento e recuperação, mais antigas são usualmente baseadas numa arquitetura hierárquica, composta por até três camadas, onde o tratamento de falhas é concentrado no nível mais alto. Em Bøgh e Blanke (1997), por exemplo, é apresentado o subsistema *Attitude Control System* (ACS) tolerante a falhas do 1º satélite dinamarquês – o Ørsted. Bøgh e Blanke (1997) apresentam a arquitetura do FDIR e descrevem suas funções e operação, assim como as conexões internas ao ACS e as conexões com o subsistema *Command and Data Handler* (C&DH). A Figura 1.1 mostra a estrutura do ACS com o supervisor para tratamento de falhas e as interfaces de telecomando e telemetria.

Figura 1.1 – Estrutura do ACS com o supervisor para tratamento de falhas e as interfaces de telecomando e telemetria do satélite Ørsted.



Fonte: Adaptado de Bøgh e Blanke (1997).

As estratégias de FDIR mais recentes são usualmente baseadas numa arquitetura hierárquica multicamada e distribuída, onde cada nível realiza sua própria detecção, isolamento/identificação e recuperação de falhas de acordo com métodos específicos. Se não for possível a recuperação da falha no nível em que a mesma ocorreu, a responsabilidade passa para o nível imediatamente acima e, assim, sucessivamente (SCHWAB et al., 2012). A Figura 1.2 apresenta um exemplo de organização das camadas hierárquicas de um FDIR.

Figura 1.2 – Exemplo de organização hierárquica de um FDIR.

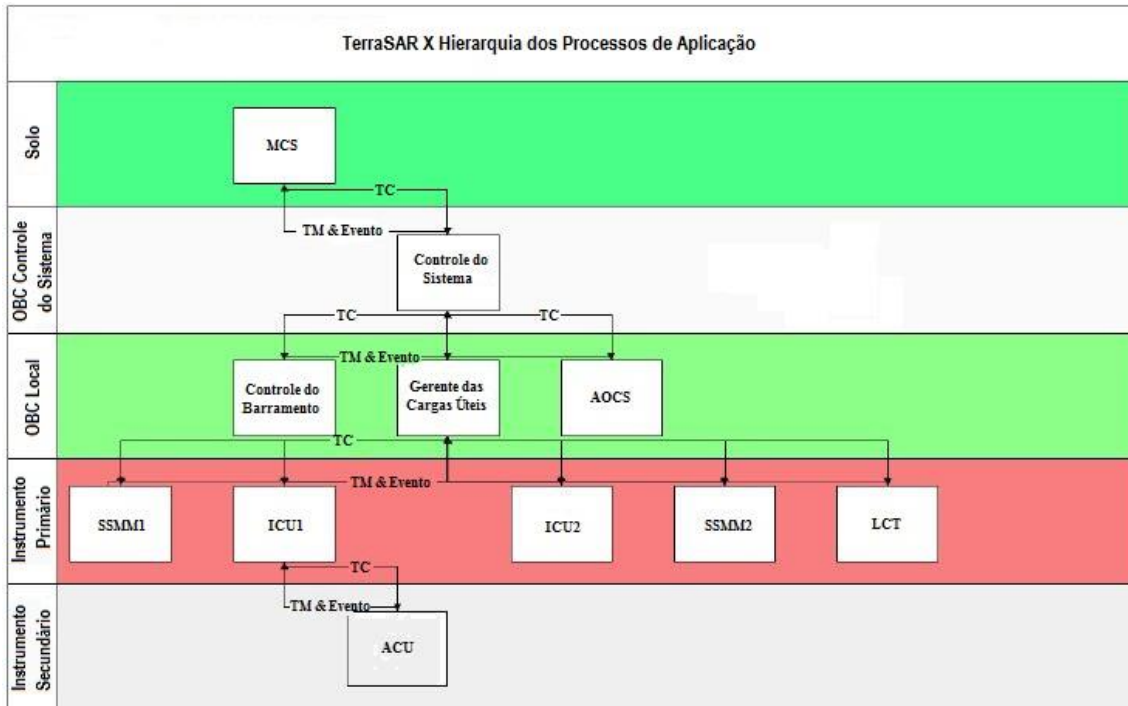


Fonte: Adaptado de Eickhoff (2012) e Pasquet et al. (2015).

Em Schwab et al. (2012), por exemplo, é apresentado o FDIR da formação composta pelos satélites de observação por radar TerraSAR-X e TanDEM-X. O trabalho apresenta o FDIR global da formação, o qual é composto pelo Segmento Solo e pelo Segmento Bordo. Com foco nos satélites, Schwab et al. (2012) descrevem a arquitetura e a operação de seus FDIRs. A arquitetura do FDIR é baseada numa concepção multicamada, hierárquica e distribuída na qual cada camada realiza sua própria detecção, isolamento e recuperação. A Figura 1.3 mostra a arquitetura multicamada, hierárquica e distribuída dos

processos aplicativos que incluem as aplicações específicas de FDIR. Estes e outros casos são tratados com mais detalhes na Seção 2.6.

Figura 1.3 – Arquitetura hierárquica dos processos aplicativos do satélite TerraSAR X.



Fonte: Adaptado de Schwab et al. (2012).

De acordo com Wander e Fostner (2012), embora as estratégias de FDIR atualmente utilizadas no domínio espacial pareçam adequadas tanto para missões de observação da Terra, onde a intervenção humana no caso de falhas inesperadas pode ser realizada várias vezes ao longo do dia, como para satélites de comunicação, onde a abordagem “falha com segurança” (*fail safe*) tem sido adotada com sucesso, as estratégias convencionais de FDIR usadas no espaço apresentam deficiências significativas como a frequente falta de isolamento de falhas, observabilidade parcial do estado real do sistema e falta de conhecimento a bordo da capacidade operacional geral do sistema. Além dessas deficiências, a escolha conservadora de valores de limiares para verificação de limites de parâmetros acaba por provocar a colocação da nave no modo seguro desnecessariamente, acarretando um excessivo tempo fora de operação das missões.

1.2 Motivações e Justificativas

Com experiência que vai de microssatélites a satélites de grande porte, o desenvolvimento de satélites no Brasil pelo INPE teve início com o programa Missão Espacial Completa Brasileira - MECB, que produziu os satélites de pequeno porte da série Satélite de Coleta de Dados - SCD (SCD-1, SCD-2 e SCD-2A). A seguir, em cooperação com a China, o programa China Brazil Earth Resources Satellite – CBERS produziu até o momento cinco satélites de grande porte, CBERS-1, CBERS-2, CBERS-2B, CBERS-3 e CBERS-4, e um sexto, o satélite CBERS-4A encontra-se em desenvolvimento.

Em paralelo com o satélite CBERS-1, foi desenvolvido o projeto Satélite de Aplicações Científicas – SACI que resultou nos microssatélites SACI-1 e SACI-2. A partir do ano 2000, o Brasil iniciou o desenvolvimento da Plataforma Multimissão – PMM com o objetivo de ser utilizada em satélites de médio porte para aplicações científicas e de observação da Terra. O satélite de observação da Terra Amazonia-1, primeiro a utilizar a plataforma PMM, encontra-se atualmente em fase de desenvolvimento.

Com a experiência acumulada ao longo dessas missões é possível identificar pelo menos quatro problemas que são motivações para o desenvolvimento desta tese.

1.2.1 Tratamento Tardio de Falhas Sistêmicas

1.2.1.1 Problema

O tratamento das falhas sistêmicas nas missões brasileiras tem, como regra geral, seu início na fase C da missão (definição detalhada do projeto). O conceito de ciclo de vida de uma missão espacial e suas fases é tratado com mais detalhes na seção 2.2 deste trabalho. O tratamento de falhas na fase C impõe restrições no estabelecimento de estratégias para a missão. As estratégias propostas nesta fase para o tratamento de falhas sistêmicas têm como principal recurso o uso de réplicas dos equipamentos. A adição generalizada de redundâncias pode, em função de seu custo, não ser a melhor

estratégia ou mesmo não ser uma solução viável para satélites de pequeno e médio porte.

1.2.1.2 Motivação – Antecipação do Tratamento de Falhas Sistêmicas

O gerenciamento de falhas deve seguir as fases do ciclo de vida da missão e os processos de engenharia de sistemas, acoplado ao desenvolvimento do sistema nominal (NASA, 2012; GESSNER et al., 2004).

Agências como a NASA (*National Aeronautics and Space Administration*) e a ESA (*European Space Agency*) recomendam iniciar o processo de gerenciamento de falhas das missões espaciais já na primeira fase do ciclo de vida da missão, ou seja, na Fase 0 (análise da missão e definição de requisitos), de acordo com o ECSS (*European Cooperation for Space Standardization*), (ECSS, 2009b) ou na Pré-Fase A (estudos conceituais), de acordo com NASA (2012).

No entanto, de acordo com Alana et al. (2012), a definição e o projeto de um FDIR são frequentemente realizados nas últimas etapas de um projeto devido aos seus fortes vínculos com outras partes do sistema, prejudicando dessa forma uma eventual maturidade do FDIR.

A definição tardia do FDIR é um problema que ocorre também nas missões brasileiras onde as estratégias sistêmicas de tratamento de falhas são definidas na fase C do ciclo de vida da missão (seção 3.2). A primeira motivação deste trabalho é antecipar o tratamento de falhas sistêmicas do ACDH para a fase B (definição preliminar do projeto).

1.2.2 Baixa Autonomia Operacional

1.2.2.1 Problema

Os satélites da série CBERS (seção 2.8.8.6), os maiores e mais complexos satélites com participação brasileira, têm capacidade para: a) executar operações pré-planejadas pelo Segmento Solo; b) armazenar dados essenciais da missão; e, c) colocar o satélite numa configuração segura após uma falência

do sistema. De acordo com a norma ECSS-E-ST-70-11C (2008) os níveis de autonomia das missões CBERS podem ser classificados como E2 (capacidade de execução a bordo de operações definidas pelo Segmento Solo) para a execução da missão, D1 (capacidade de armazenagem a bordo de dados essenciais da missão após uma falência ou uma indisponibilidade do Segmento Solo) para o gerenciamento de dados da missão, e F1 (capacidade de estabelecer configuração segura após falência do Segmento Espacial) para o gerenciamento de falhas a bordo. A classificação dos níveis de autonomia de uma missão espacial é tratada com mais detalhes na seção 2.5 deste trabalho.

O satélite Amazônia-1 (seção 2.8.8.7) tem características semelhantes aos satélites da série CBERS para a execução da missão, gerenciamento de dados e gerenciamento de falhas e pode, portanto, ser classificado da mesma forma quanto aos níveis de autonomia.

1.2.2.2 Motivação – Aumento da Autonomia

Como mencionado na Seção 1.1, a crescente tendência de aumento da autonomia dos satélites científicos e de observação da Terra tem, como consequência, a necessidade de aplicação de conceitos mais complexos de FDIR. Exemplos de aumento da autonomia na execução das operações nominais da missão e no gerenciamento de dados da missão, o satélite GOCE (*Gravity field and steady-state Ocean Circulation Explorer*), lançado em 2009 pela ESA tinha como requisito um período de autonomia de 72 horas e o satélite ADM-Aeolus (*Atmospheric Dynamics Mission Aeolus*), com previsão de lançamento para 2017 pela ESA, tinha como requisito a redução do envolvimento do centro de operação a um dia a cada sete dias (GESSNER et al., 2004).

No âmbito brasileiro, Kucinskis (2012) aponta um crescente nível de complexidade em missões já previstas e em diferentes fases de desenvolvimento como os satélites MIRAX (Monitor e Imageador de Raios X) e EQUARS (*Equatorial Atmosphere Research Satellite*), e propõe que a operação das mesmas seja baseada em objetivos. De acordo com Kucinskis

(2012) “a operação baseada em objetivos apresenta-se como uma evolução do paradigma de operação vigente, com potencial para suprir as demandas operacionais de futuras missões. Mais do que isso, o conceito de operações baseadas em objetivos abre caminho para operações total ou parcialmente autônomas do segmento espacial”.

De acordo com Gessner et al. (2004); Olive (2010); Vander et al. (2012), o gerenciamento de falhas é essencial para o aumento dos níveis de autonomia e sua implementação deve ser compatível com os níveis adotados para a missão.

Em vista do exposto, a introdução de estratégias de FDIR que podem aumentar a autonomia de missões envolvendo satélites de pequeno e médio porte, compatíveis com os satélites utilizados nas missões brasileiras, é um segundo motivador deste trabalho.

1.2.3 Dificuldade em Tratar Falhas de Sistemas Complexos e/ou Integrados

1.2.3.1 Problema

Sistemas complexos e/ou altamente integrados caracterizam-se pelo número de diferentes funções que são capazes de realizar, pelas interações entre as funções e pelas interações entre as funções e o ambiente em que estão inseridas. Esse cenário favorece o aumento da quantidade de modos potenciais de falência e dificulta a detecção das falências, a isolação das falhas e recuperação do sistema.

1.2.3.2 Motivação – Tratamento de Falhas de Sistemas Complexos e/ou Altamente Integrados

O crescimento da complexidade e/ou integração dos sistemas impõe novos desafios para o tratamento de suas falhas. Na área espacial, Wander e Förstner (2013) mencionam que o crescente aumento nos requisitos de disponibilidade e de desempenho das missões espaciais tem elevado a

complexidade do sistema e feito com que o sucesso da missão dependa de resposta adequada às anomalias decorrentes de mudanças inesperadas no ambiente e às falhas nos seus componentes e subsistemas. Morgan (2005) observa ainda que à medida que uma espaçonave torna-se mais complexa, a diagnose da falha e a recuperação do sistema torna-se uma tarefa mais difícil e demorada para ser realizada.

Assim, a terceira motivação deste trabalho está em tratar falhas de um ACDH, subsistema mais integrado e mais complexo que os utilizados nas missões anteriores do Programa Espacial Brasileiro.

1.2.4 Impactos Negativos na Área Espacial

1.2.4.1 Problema

Com custos que podem chegar a centenas de milhões de reais, a perda de missões espaciais em decorrência de falhas pode resultar na redução ou até mesmo corte de investimentos na área.

A falta desses recursos prejudica todas as organizações envolvidas no desenvolvimento e operação de missões, sejam elas governamentais ou privadas, reduzindo e desmotivando equipes formadas ao longo de anos de trabalho e força os usuários de produtos espaciais, sejam eles científicos ou comerciais, a buscar alternativas de fornecimento.

1.2.4.2 Motivação – Prevenção de Impactos Negativos nas Missões

O Programa Espacial Brasileiro conviveu com a perda de quatro missões: SCD-2A, SACI-1, SACI-2 e CBERS-3. Destes, a perda do SCD-2A, SACI-2 e CBERS-3 são decorrentes de falhas no lançador enquanto que a perda do SACI-1 deve-se a falha do próprio satélite.

A perda de uma missão em decorrência de falhas tem repercussão negativa na sociedade e reflexos, com maior ou menor intensidade, no Programa Espacial e em seus gestores, no INPE e em seus engenheiros, técnicos, et alli.

A perda do satélite SACI-1 em 1999, por exemplo, teve forte repercussão negativa, eclipsando o sucesso do satélite CBERS-1 (os dois satélites foram colocados em órbita pelo mesmo veículo lançador). Na época o assunto foi amplamente explorado pela mídia e até por programas humorísticos. A matéria “O vexame do SACI”, publicada no dia 27/10/1999, na Edição 1.621 da revista VEJA (<http://veja.abril.com.br/>) é um exemplo de como o assunto foi tratado.

Assim, a quarta motivação deste trabalho está em propor estratégias que aumentem a cobertura das falhas de um ACDH e, dessa forma, reduzir os riscos de perda de uma missão.

1.3 Objetivo

O objetivo da tese é propor uma estratégia para o tratamento de falhas sistêmicas (FDIR) em ACDHs de satélites de pequeno e médio porte. Essa estratégia é baseada na análise da arquitetura funcional - em detrimento da física - do satélite, o que permite adiantar o projeto do FDIR para o início da Fase B do ciclo de vida, quando ainda é possível que as considerações de FDIR tenham um impacto mais efetivo no projeto dos subsistemas e do satélite como um todo.

Por conter uma abordagem funcional, a estratégia ora apresentada tem o potencial de mitigar a complexidade associada à abordagem da arquitetura física, quando aplicada a subsistemas complexos e/ou altamente integrados. De forma a demonstrar tal potencial, optou-se por aplicar a estratégia a um estudo de caso voltado a ACDHs de satélites de pequeno e médio porte, embora ela seja aplicável a qualquer outro subsistema.

1.4 Originalidade, Generalidade e Utilidade

Com relação ao trabalho:

- A avaliação da originalidade é realizada por meio de tabelas que, em um primeiro momento sumariza os resultados obtidos e, em um segundo momento, apresenta o resultado do levantamento bibliográfico e

compara com a proposta do trabalho. As tabelas atualizadas são apresentadas na seção 2.8.9 (Tabela 2.11 – Sumário das arquiteturas e métodos analisados nesta revisão) e na seção 3.5 (Tabela 3.3 – Avaliação da originalidade da proposta).

- A generalidade está no fato de a estratégia poder ser estendida a outros subsistemas e às cargas úteis e, ainda ser aplicada a outras classes de satélites;
- A utilidade está na possibilidade de a estratégia poder ser aplicada em missões que se enquadram no escopo do Programa Nacional de Atividades Espaciais – PNAE.

1.5 Organização do Trabalho

No Capítulo 1, Introdução, apresentam-se a contextualização do trabalho assim como suas motivações, justificativas e objetivos.

No Capítulo 2, Conceitos Básicos e Revisão Bibliográfica, são apresentados os resultados da revisão bibliográfica e os conceitos básicos relativos a uma missão espacial, tais como classes de satélite, ciclo de vida e operação de uma missão, e os relativos ao tratamento de falhas (FDIR), tais como os conceitos de falha, erro e falência e os de detecção, isolamento, identificação e recuperação. O Capítulo inclui ainda uma revisão de trabalhos relativos às arquiteturas e métodos de FDIR e às estratégias adotadas em algumas aplicações.

No Capítulo 3, Proposta de Estratégia para o Tratamento de Falhas, é desenvolvida a estratégia proposta no trabalho e apresentada uma avaliação da originalidade.

No Capítulo 4, Aplicação da Estratégia ao Subsistema ACDH, a estratégia desenvolvida no trabalho é aplicada a um subsistema ACDH baseado no ACDH da PMM e do satélite Amazônia e a um caso da literatura.

No Capítulo 5, Validação da Estratégia para o Tratamento de Falhas, apresentam-se os resultados da simulação de lógicas de diagnose propostas aplicadas à função 'Fornecer Tempo de Bordo' do ACDH da PMM e a um caso da literatura.

No Capítulo 6, Conclusões, são apresentadas as contribuições do trabalho e sugestões para trabalhos futuros.

2 CONCEITOS BÁSICOS E REVISÃO BIBLIOGRÁFICA

2.1 Classes de Satélites

De acordo com Kramer e Cracknell (2008), há várias formas de se classificar os satélites como, por exemplo, por função, por tipo de órbita, custo, dimensões, massa e etc. A classificação pela massa torna-se, no entanto, muito útil devido a sua relação direta com os custos de lançamento, os quais representam uma parcela significativa do custo total das missões (em torno de US\$20.000/kg para satélites pequenos, de acordo com Rogers et al. (2014)). Segundo os autores, a primeira classificação conhecida de satélites de acordo com a massa (apresentada na Tabela 2.1) foi proposta em 1991 por Martin N Sweeting do grupo *Surrey Satellite Technology Ltd* (SSTL).

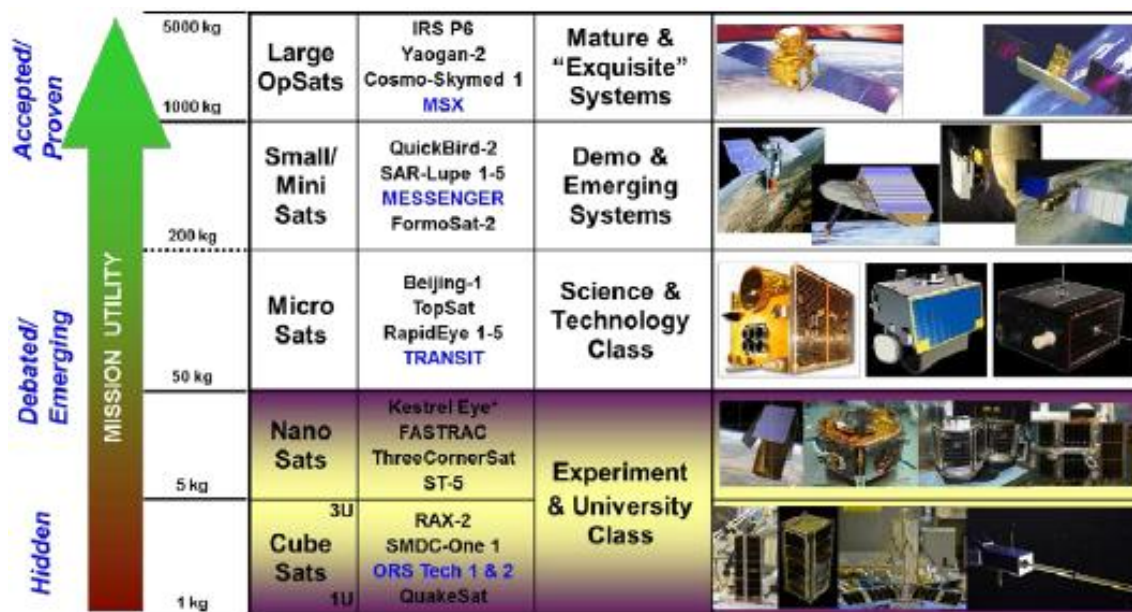
Tabela 2.1 – Classificação de satélites proposta por Martin N Sweeting em 1991.

Classificação	Massa (kg)
Satélites Grandes	> 1.000
Satélites Pequenos	500-1.000
Minissatélites	100-500
Microssatélites	10-100
Nanossatélites	< 10

Posteriormente, a classificação originalmente proposta por Sweeting foi revisada com a introdução de mais duas classes de satélites (Picossatélites, com massa entre 100 g e 1 kg e Femtossatélites, com massa entre 1 g e 100 g) e a alteração da classe Minissatélites, que passou a incluir satélites de 100 kg a 1000 kg. Com a alteração na classe Minissatélite, o termo “satélite pequeno” passou a ser utilizado para cobrir todos os satélites com massa inferior a 1000 kg. (KRAMER; CRACKNELL, 2008). Embora, de acordo com os autores, essas modificações tenham sido adotadas por diversas organizações e autores, não há consenso na literatura com relação à questão.

O *The Johns Hopkins University Applied Physics Laboratory* (JHU/APL), por exemplo, agrupa as naves espaciais de acordo com a Figura 2.3 (ROGERS et al, 2014). O JHU/APL classifica os satélites entre 200 kg e 1000 kg como satélites pequenos ou minissatélites.

Figura 2.1 – Classificação das naves espaciais pelo JHU/APL de acordo com sua massa (sem combustível).



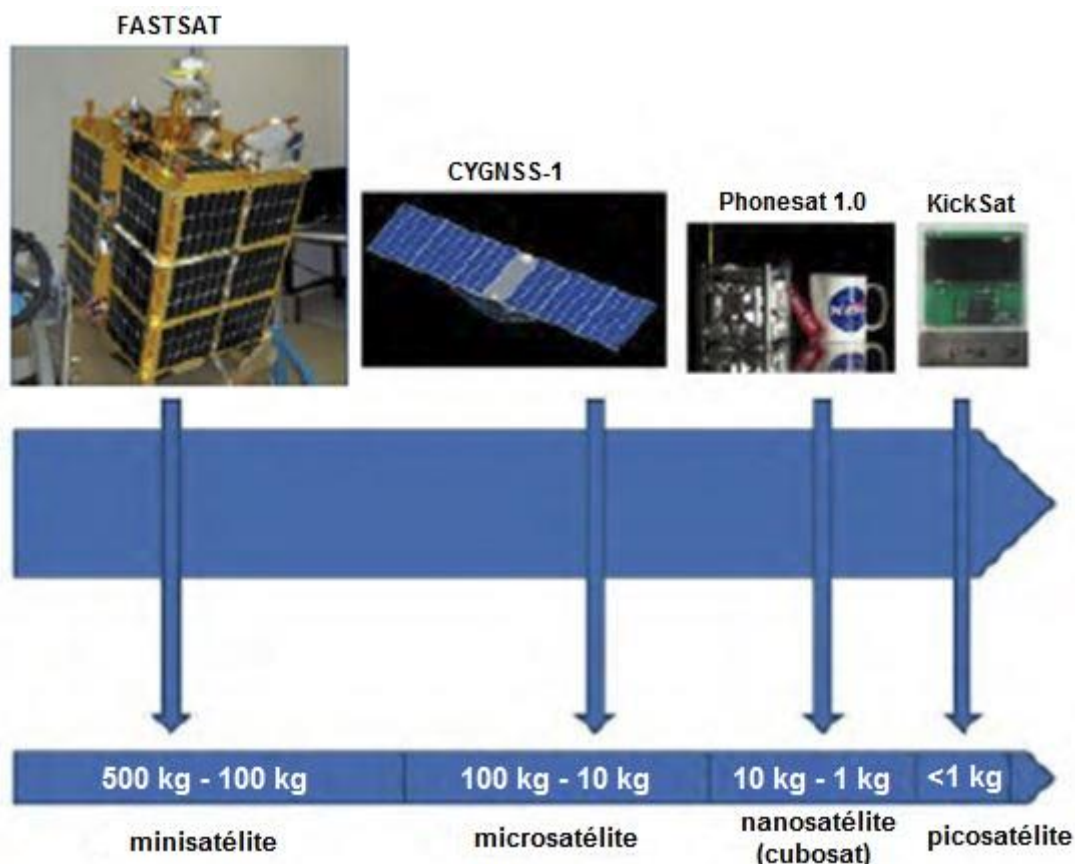
Fonte: Rogers et al. (2014).

Já o *NASA's Small Spacecraft Technology Program* (SSTP) da *National Aeronautics and Space Administration* (NASA) classifica as naves espaciais de acordo com a Figura 2.2. O SSTP considera como pequena toda nave espacial com massa menor que 180 kg (NASA, 2014).

Outras classificações podem ainda ser encontradas como, por exemplo, Capó-Lugo e Bainum (2011); Encyclopedia of Science (2015); Weeden (2010); Wikipedia (2015).

Neste trabalho é considerada a classificação apresentada na Tabela 2.2.

Figura 2.2 – Classificação das naves espaciais pelo SSTP de acordo com sua massa (sem propelente).



Fonte: Adaptado de NASA (2014).

De acordo com NASA (2014), “Naves espaciais pequenas tem-se tornado mais atraentes devido a custos de desenvolvimento mais baixos e a menores tempos de fornecimento. Existe uma relação natural de compromisso entre tamanho e funcionalidade de uma nave, mas o avanço nas tecnologias de miniaturização e integração tem diminuído o escopo desse balanço. A integração efetiva de componentes individuais pode aumentar substancialmente a funcionalidade e a densidade do sistema reduzindo sua massa e volume”.

Na mesma linha, Rogers et al. (2014) defendem a utilização de satélites pequenos e propõem o emprego de satélites com uma única carga útil, os quais denominam SensorSats. De acordo com os autores, satélites com uma só carga útil evitam a complexidade do projeto com múltiplas cargas úteis tais

como interferência entre os requisitos de calibração, tamanho, temperatura e potência.

Tabela 2.2 – Classificação de satélites de acordo com a massa.

Classificação	Massa (kg)
Satélites Grandes	> 1.000
Satélites Médios	500-1.000
Minisatélites / Satélites Pequenos	100-500
Microsatélites	10-100
Nanosatélites	1-10
Picosatélites	0.1-1
Femtosatélites	< 0,1

A Tabela 2.3 compara alguns exemplos de satélites de observação ótica da Terra de três classes distintas: grande porte (CBERS-4 e ResourceSat-1), médio porte (Amazonia-1 e FormoSat-2) e pequeno porte (TopSat) tendo como parâmetro: a) a complexidade do Subsistema de Controle de Atitude e Órbita – AOCS, caracterizada pelos tipos e quantidades de sensores e atuadores utilizados; b) a complexidade da carga útil, caracterizada pela quantidade e resolução das câmeras de imageamento.

Na elaboração da Tabela 2.3 são utilizados dados disponíveis publicamente das seguintes fontes: a) CBERS-4: NASA Spaceflight.com (2014, 2013); Em Órbita (2014); GlobalSecurity.org (2014); b) ResourceSat-1: eoPortal (2015a); c) Amazonia-1: INPE (2010); d) FormoSat-2: eoPortal (2015b); e) TopSat: BROOKS (2001); CAWLEY (2003).

Embora não seja um levantamento extensivo, a Tabela 2.3 mostra tendência a uma menor complexidade do subsistema AOCS e da Carga Útil com a redução da massa do satélite. Os tipos e as quantidades de sensores e atuadores utilizados pelo satélite Amazonia-1, compatíveis com satélites de grande porte, deve-se ao mesmo utilizar todos os instrumentos possíveis de serem utilizados

na PMM, uma vez que o mesmo representa a primeira implementação do conceito de Plataforma Multimissão no Brasil.

Tabela 2.3 – Comparação de satélites de observação ótica da Terra de pequeno, médio e grande porte.

Características	Satélites				
	CBERS-4	Resource Sat-1	Formo Sat-2	Amazonia-1	TopSat
Lançamento	2014	2003	2004	2019	2005
Massa	2080 kg	1360 kg	760 kg	680 kg	115 kg
Quantidade de Cargas Úteis	6	3	2	1	1
Câmera de Maior Resolução	5,0m	5,8 m	2 m	64 m	2,5m
Acurácia do Apontamento	0,1°	0,15°	0,12°	0,05°	Inform. não disponível
Estabilidade (<i>deriva</i>)	0,001°/s	0,0004°/s	Inform. não disponível	0,001°/s	Inform. não disponível
Determinação de Atitude	0,03°	Inform. não disponível	0,02°	0,005°	Inform. não disponível
GPS	Qtde. não disponível	Não utiliza	Não utiliza	2	Não utiliza
Sensor de Estrelas	Qtde. não disponível	Qtde. não disponível	2	2	Não utiliza
Giroscópio	Qtde. não disponível	Qtde. não disponível	Qtde. não disponível	4	3
IRU	Não utiliza	Não utiliza	Qtde. não disponível	Não utiliza	Não utiliza
Roda de Reação	Qtde. não disponível	4	4	4	4
Magnetotorque	Qtde. não disponível	2	Não utiliza	3	3
<i>Thruster</i>	Qtde. não disponível	8x1N, 4x11N	Qtde. não disponível	6	Não utiliza
Magnetômetro	Não utiliza	Não utiliza	Não utiliza	2	Não utiliza
Sensor Solar	Qtde. não disponível	Qtde. não disponível	Não utiliza	8	Qtde. não disponível
Sensor de Terra	Qtde. não disponível	Qtde. não disponível	Não utiliza	Não utiliza	Qtde. não disponível

2.2 Ciclo de Vida de uma Missão Espacial

O ciclo de vida de uma missão espacial é dividido em sete fases por agências como a NASA e a ESA as quais são caracterizadas por revisões e pontos de

decisão. Embora as fases recebam denominações diversas por parte das agências, a alocação de atividades por fases é relativamente semelhante. NASA (2016) classifica as fases do ciclo de vida da missão como descrito a seguir.

- Pré-Fase A: Estudos conceituais;
- Fase A: Conceito e desenvolvimento de tecnologia;
- Fase B: Projeto preliminar e conclusão da tecnologia;
- Fase C: Projeto final e fabricação;
- Fase D: Montagem do sistema, integração e teste e lançamento;
- Fase E: Operação e manutenção;
- Fase F: Encerramento.

Já a ESA (ECSS, 2009) classifica as fases como indicado a seguir.

- Fase 0: Análise da missão e identificação de necessidades;
- Fase A: Viabilidade;
- Fase B: Definição preliminar;
- Fase C: Definição detalhada;
- Fase D: Qualificação e produção;
- Fase E: Utilização;
- Fase F: Descarte.

2.3 Operação de Missões Espaciais

A norma ECSS-E-ST-70-11C (2008) define “operação” como as atividades realizadas pelos segmentos solo e espacial com a finalidade de garantir o

fornecimento dos produtos e serviços da missão, recuperar de contingências a bordo, executar a manutenção de rotina e gerenciar os recursos de bordo a fim de maximizar o fornecimento dos produtos e serviços e a vida útil da missão.

No que diz respeito às características de operação, as missões podem, basicamente, ser classificadas em três tipos: missões em órbita baixa, missões em órbita geoestacionária e missões interplanetárias.

De acordo com Eickhoff (2012), os objetivos da operação e os recursos necessários para sua execução diferem ligeiramente para os três tipos básicos de missões. Para uma missão em órbita baixa, os objetivos da operação são:

- Realizar a calibração da plataforma e cargas úteis;
- Realizar o controle e a monitoração da plataforma e cargas úteis;
- Enviar para o satélite dados operacionais e receber os produtos da missão;
- Realizar manobras de correção de órbita;
- Manter o desempenho das cargas úteis;
- Realizar as atividades de recuperação no caso de falhas;
- Remover o satélite de órbita.

Para este tipo de missão, o Segmento Solo conta com uma rede de estações terrenas.

Para uma missão em órbita geoestacionária, os objetivos da operação são:

- Realizar a calibração da plataforma e cargas úteis;
- Realizar o controle e monitoração da plataforma e cargas úteis;
- Realizar manobras de correção de órbita ou de posição;

- Manter o desempenho das cargas úteis;
- Realizar as atividades de recuperação no caso de falhas;
- Colocar o satélite da órbita para descarte no final de sua vida útil.

Para este tipo de missão, o Segmento Solo conta normalmente com uma única estação terrena, uma vez que o satélite está permanentemente visível.

Para uma missão interplanetária, os objetivos da operação são:

- Realizar a calibração da plataforma e cargas úteis;
- Realizar o controle e monitoração da plataforma e cargas úteis;
- Enviar para a sonda dados operacionais e receber os produtos da missão;
- Enviar para a sonda as atualizações do *software* de bordo (OBSW) para as diferentes fases da missão;
- Comandar e controlar as mudanças de trajetória e as manobras de visita rápida;
- Manter o desempenho das cargas úteis;
- Realizar as atividades de recuperação no caso de falhas;

Para este tipo de missão, o Segmento Solo conta com uma rede específica de estações terrenas para missões interplanetárias.

Nas missões de exploração da atmosfera ou da superfície de corpos celestes por meio de sondas e *rovers*, a comunicação destes com o Segmento Solo é realizada por meio de naves espaciais em órbita ou próximas ao corpo celeste alvo, que operam como repetidoras de sinal.

De acordo Wander e Förstner (2012), a operação de naves espaciais é tradicionalmente realizada por meio de Procedimentos de Controle de Vôo –

FCPs (*Flight Control Procedures*) e Sequências de Comandos – MTLs (*Mission Time Line*). Os FCPs são executados passo a passo pelo Segmento Solo e consistem do envio de Telecomandos para a espaçonave e a verificação das Telemetrias recebidas em solo. Os MTLs são sequências de Telecomandos temporizados enviados de solo e executados pelo *software* de bordo quando o tempo requerido é atingido.

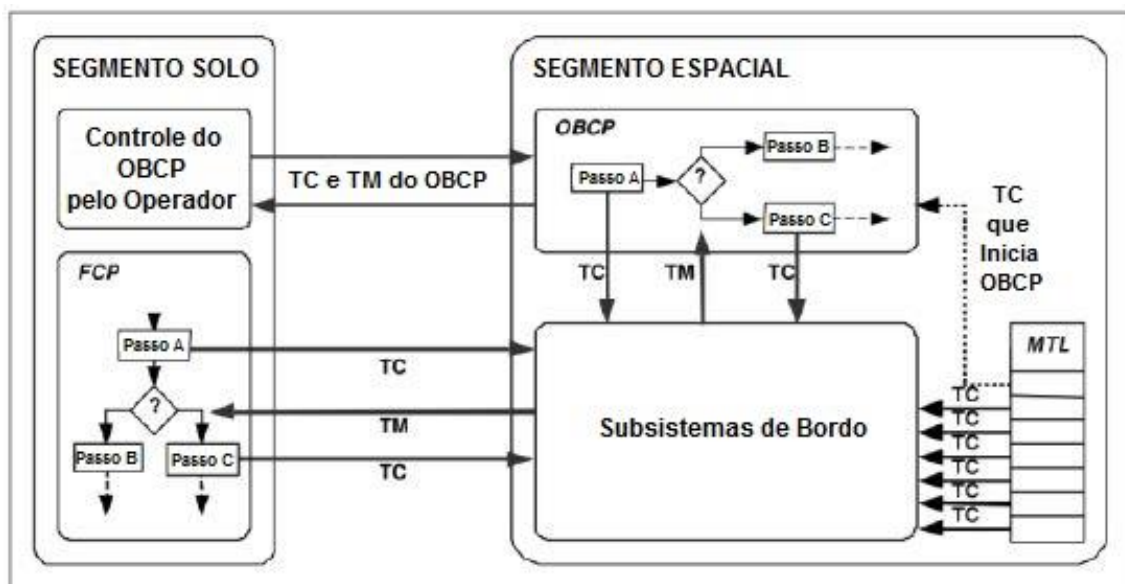
Também é possível realizar a operação por meio de Procedimentos de Controle a Bordo – OBCPs (*On-Board Control Procedures*). OBCPs são úteis tanto para o tratamento de operações nominais como para a automatização mais intensa das operações, de forma a permitir que o Segmento Solo prepare e envie para a espaçonave sequências complexas de operações. Os OBCPs são ativados por meio de Telecomandos ou por meio de eventos previamente definidos.

OBCPs são programas desenvolvidos para serem executados por uma máquina virtual OBCP os quais podem ser facilmente carregados, executados ou substituídos a bordo de uma espaçonave. Os procedimentos são roteiros de comandos que são montados a partir do serviço de comandos do PUS (*Packet Utilization Standard*) (WANDER; FÖRSTNER, 2012). A Figura 2.3 mostra a operação tradicional de uma nave espacial e a operação usando OBCPs.

Como indicado na Figura 2.3, os OBCPs são executados em um ambiente separado e seguro, o que permite a criação e carregamento de novos procedimentos em vôo ao mesmo tempo em que não requer modificação, carregamento e validação do *software* de bordo.

Os OBCPs são usados em missões da ESA para operação nominal e operação FDIR (WANDER; FÖRSTNER, 2012).

Figura 2.3 – Operação tradicional de uma nave espacial com FCPs e MTLs; e a operação usando OBCPs.



Fonte: Adaptado de Wander e Förstner (2012).

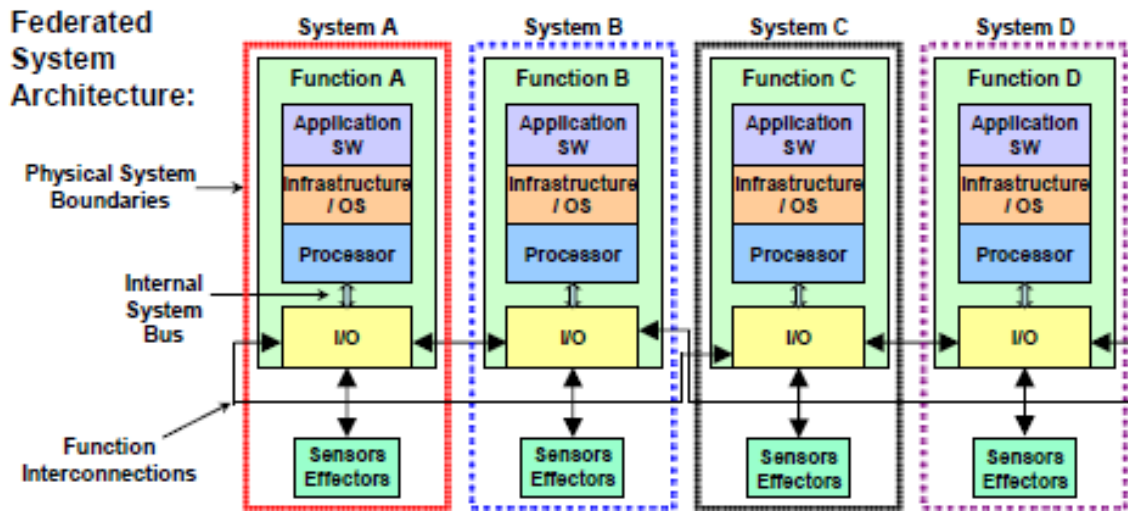
2.4 Subsistema ACDH

A disponibilização de microprocessadores com alta capacidade de processamento possibilitou a integração de funções em sistemas complexos impulsionada por fatores como a redução de massa, volume e energia.

Na indústria aeronáutica, essa tendência é observada após 1980 com a introdução do conceito de Avionica Modular Integrada (*Integrated Modular Avionics - IMA*).

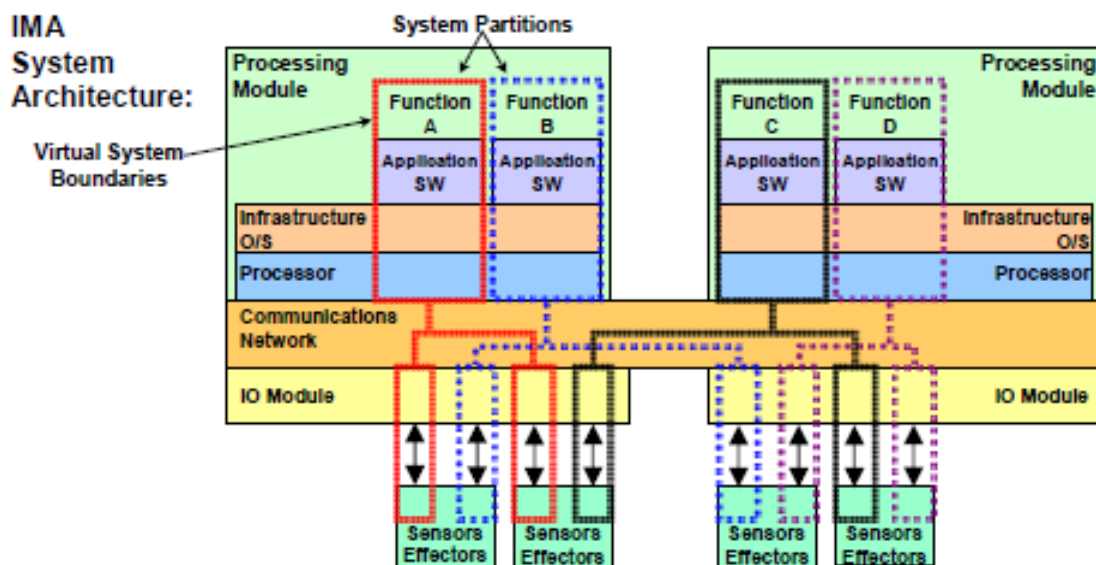
Esse novo conceito permitiu que arquiteturas federadas, as quais utilizam conjuntos independentes de recursos computacionais (processamento, comunicação e entrada/saída) para cada função (Figura 2.4) pudessem ser substituídas pelas arquiteturas IMA (Figura 2.5), nas quais os recursos computacionais (processamento, comunicação e interfaces de entrada/saída) são particionados para serem utilizados de forma compartilhada por múltiplas funções.

Figura 2.4 – Exemplo de Arquitetura Federada.



Fonte: Watkins (2006).

Figura 2.5 – Exemplo de Arquitetura IMA.



Fonte: Watkins (2006).

Na área espacial a tendência à integração funcional acontece a seguir, resultando na integração das funções de supervisão de bordo, tradicionalmente alocadas no subsistema OBDS (*On-Board Data Handling Subsystem*), com as funções de controle de atitude e órbita, tradicionalmente alocadas no subsistema AOCS (*Attitude and Orbit Control Subsystem*), em satélites de pequeno, médio e grande porte.

Em torno do ano 2000, a indústria espacial europeia disponibiliza equipamentos tais como: 1) Unidade de Gerenciamento da Espaçonave – produzido pela RUAG Space AB (www.ruag.com/space), antiga Saab Ericsson Space; 2) Sistema Integrado para o Gerenciamento de Espaçonave – produzido pela Thales Alenia Space (www.thalesaleniaspace.com), antiga Laben S.p.A; e 3) Equipamento Integrado de Controle e Dados – produzido pela Airbus Defence and Space (<http://www.airbus.com/defence.html>), antiga Astrium Space, com recursos para a integração das funções de supervisão de bordo e controle de atitude e órbita.

No início dos anos dois mil, o INPE adota a integração das funções de supervisão de bordo e controle de atitude e órbita na plataforma PMM. No INPE, as funções integradas são alocadas no subsistema Controle de Atitude e Tratamento de Dados (*Attitude Control and Data Handling* – ACDH).

Mantendo basicamente a mesma arquitetura do sistema computacional usado nos subsistemas OBDH e AOCS, a integração das funções proporciona redução significativa dos recursos computacionais, da massa, do volume e da potência necessários para a realização das funções de controle de atitude e órbita e supervisão de bordo.

Com fins ilustrativos, a Figura 2.6 mostra a arquitetura tradicional do sistema com os subsistemas OBDH e AOCS; e a Figura 2.7 mostra a arquitetura inovada com os subsistemas integrados no ACDH. Nessas figuras, é adotada a topologia em estrela para os subsistemas e o sistema. Nessas figuras, OBC (*On Board Computer*) representa o computador dos subsistemas, TC (*Telecommand Module*) representa o Módulo de Telecomando, TM (*Telemetry Module*) representa o Módulo de Telemetria, RM (*Reconfiguration Module*) representa o Módulo de Reconfiguração, e MM (*Mass Memory*) representa o módulo Memória de Massa. Nos subsistemas OBDH e ACDH, o tratamento de falhas no nível subsistema e sistema é realizado pelo OBC e RM. No subsistema ACDH, o OBC e RM somente tratam de falhas no nível subsistema.

Figura 2.6 – Arquitetura tradicional do sistema com o subsistema OBDH e o subsistema AOCS.

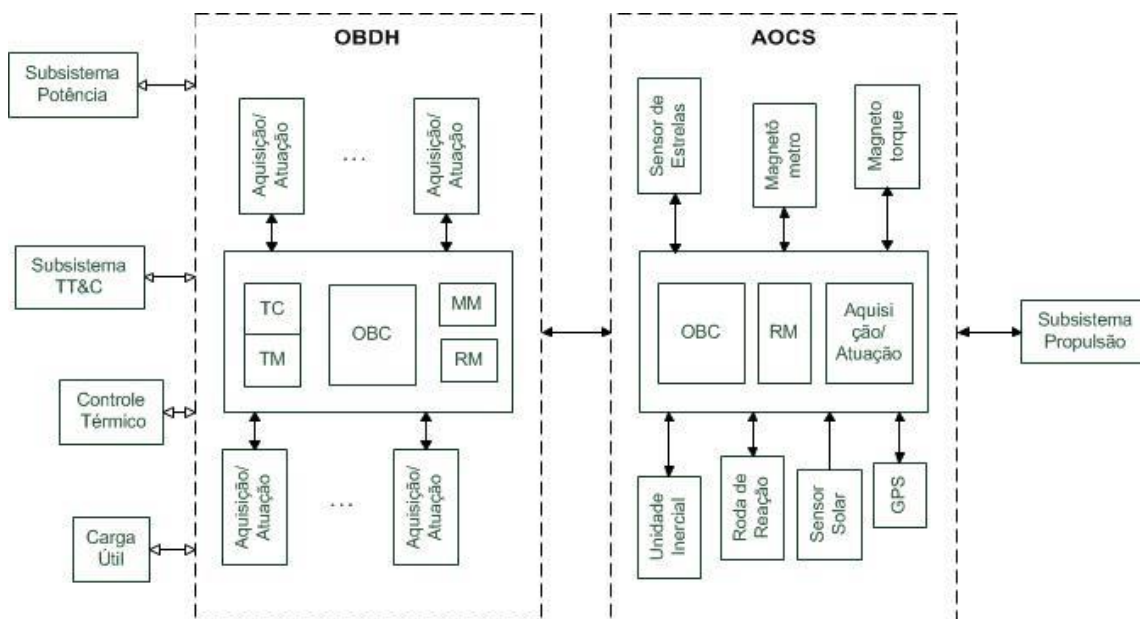
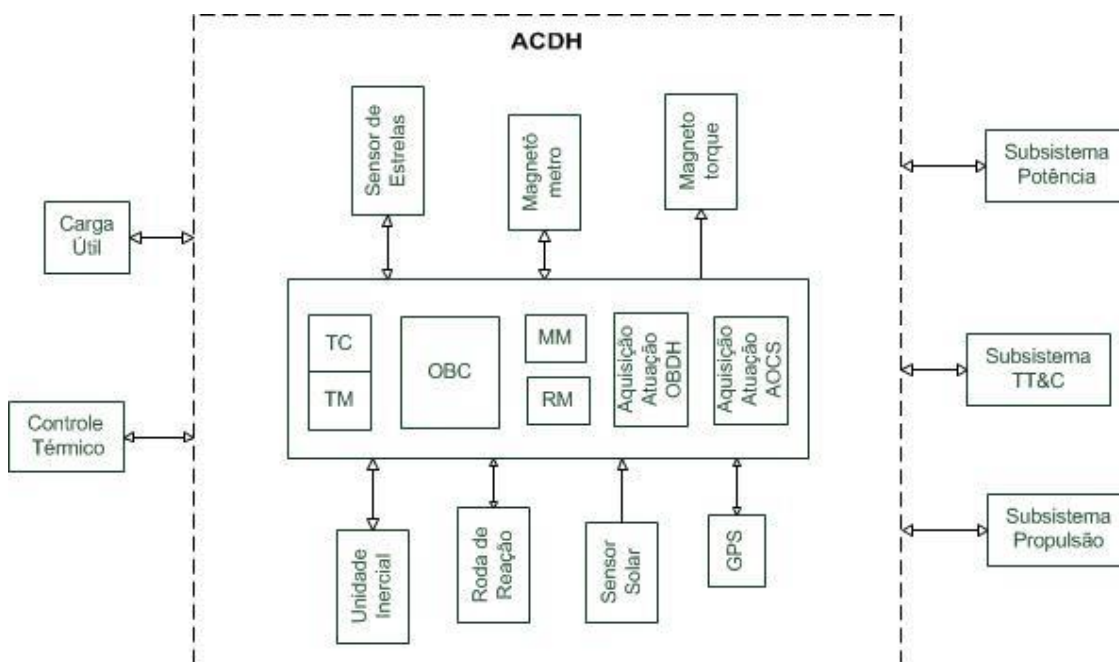


Figura 2.7 – Arquitetura inovada do sistema com o subsistema ACDH.



2.5 Autonomia

De acordo com Everett (2011), há pelo menos três razões para a introdução de autonomia no segmento espacial: reduzir os custos de operação, executar

funções críticas da missão quando o segmento solo não estiver disponível, proteger a espaçonave de eventos inesperados ou falhas.

Eickhoff (2012) aponta que, atualmente, praticamente todo satélite inclui alguma funcionalidade autônoma a bordo a qual visa, principalmente, a execução de operações durante os períodos sem contato com as estações terrenas. Nestas situações, a espaçonave deve ser capaz de gerenciar os casos de falhas garantindo, no mínimo, a transição para um modo seguro.

A implementação de autonomia a bordo das naves espaciais depende dos requisitos e restrições específicos de cada missão tais como, a cobertura proporcionada pelas estações terrenas, o tempo aceitável de interrupção da missão, o período máximo previsto de indisponibilidade do Segmento Solo e pode variar de um nível muito baixo, com a maior parte das tarefas realizadas pelo segmento solo, a um alto nível, com a maioria das tarefas realizadas a bordo.

Conforme mencionado na seção 1.2, a norma ECSS-E-ST-70-11C (2008), classifica a operação autônoma em três grandes áreas. A Tabela 2.4 apresenta a classificação dos níveis de autonomia para a execução das operações nominais da missão, de acordo com a ECSS-E-ST-70-11C (2008).

Tabela 2.4 – Níveis de autonomia para a execução da missão.

Nível	Descrição	Funções
E1	Execução da missão sob controle do segmento solo; capacidade a bordo limitada a questões de segurança	Controle em tempo real do segmento solo nas operações nominais Execução de comandos temporizados em questões de segurança
E2	Execução a bordo de operações da missão pré-planejadas e definidas pelo segmento solo	Capacidade para armazenar comandos com base no tempo em um escalonador embarcado
E3	Execução de forma adaptativa a bordo de operações da missão	Operações autônomas com base em eventos Execução a bordo de procedimentos de controle de operações
E4	Execução a bordo de operações da missão com base em objetivos	Replanejamento da missão com base em objetivos

Fonte: Adaptado de ECSS-E-ST-70-11C (2008).

A Tabela 2.5 apresenta os níveis de autonomia para o gerenciamento de dados da missão, de acordo com a ECSS-E-ST-70-11C (2008).

Tabela 2.5 – Níveis de autonomia para o gerenciamento de dados.

Nível	Descrição	Funções
D1	Armazenagem a bordo de dados essenciais da missão após uma situação de falência ou uma indisponibilidade do segmento solo	Armazenagem e recuperação de relatórios de eventos Armazenagem do gerenciamento
D2	Armazenagem a bordo de todos os dados da missão, i.e. o segmento espacial é independente do segmento solo	Funções realizadas em D1, mais armazenagem e recuperação de todos os dados da missão

Fonte: Adaptado de ECSS-E-ST-70-11C (2008).

A Tabela 2.6 apresenta os níveis de autonomia para o gerenciamento de falhas a bordo, de acordo com a ECSS-E-ST-70-11C (2008).

Tabela 2.6 – Níveis de autonomia para o gerenciamento de falhas a bordo.

Nível	Descrição	Funções
F1	Estabelece configuração segura do segmento espacial após uma falência a bordo	Identifica as anomalias e relata para o segmento solo Reconfigura os sistemas embarcados para isolar os equipamentos ou funções falidas Coloca o segmento espacial em um modo seguro
F2	Reestabelece operações nominais da missão após uma falência a bordo	Além das funções realizadas em F1, reconfigura para uma configuração operacional nominal Retoma a execução das operações nominais Retoma geração dos produtos da missão

Fonte: Adaptado de ECSS-E-ST-70-11C (2008).

2.6 Falha, Erro e Falência (“Fault, Error and Failure”)

No artigo *Fault Management Guiding Principles* (NEWHOUSE et al., 2011) consta “As discussões relacionadas ao gerenciamento de falhas são repletas de confusão resultante de diferenças na terminologia”. Na mesma referência consta ainda: “Requisitos são frequentemente escritos com usos contraditórios dos termos *fault* e *failure*”. Considerando que os autores pertencem ou ao *Jet Propulsion Laboratory* ou ao *Marshall Space Flight Center*, isso mostra, em primeiro lugar, que, mesmo na língua inglesa e na área de gerenciamento de falhas, não há consenso quanto à terminologia e conceitos, em especial, quanto ao emprego dos termos *fault* e *failure*. Mostra ainda a preocupação que uma organização do porte da NASA tem pelo assunto.

Entre os autores nacionais as divergências têm início na tradução dos termos *fault*, e *failure*. Um breve levantamento realizado por Pessotta (1999) aponta algumas dessas diferenças. Três delas são: “Martini (1993), por exemplo, considera que os defeitos (*faults*) são as causas dos erros (*errors*) que, por sua vez, são as causas das falhas (*failures*). Já Martins (1993) considera que as falhas (*faults*) são as causas dos erros (*errors*) que são as causas dos defeitos (*failures*). Outras definições são ainda utilizadas como, por exemplo, em Alonso (1998), onde as faltas (*faults*) são consideradas as causas dos erros (*errors*) os quais são considerados as causas das falhas (*failures*)”.

Face ao quadro descrito acima, **neste trabalho os termos *fault*, *error* e *failure* em Inglês são, respectivamente, considerados equivalentes à falha, erro e falência em Português.** Embora não seja usual a utilização do termo falência no contexto de tratamento de falhas, o termo vem sendo proposto e adotado pelo professor Marcelo Lopes de Oliveira e Souza e seus orientados, em analogia com a terminologia usada em medicina, como um equivalente apropriado para o termo *failure*.

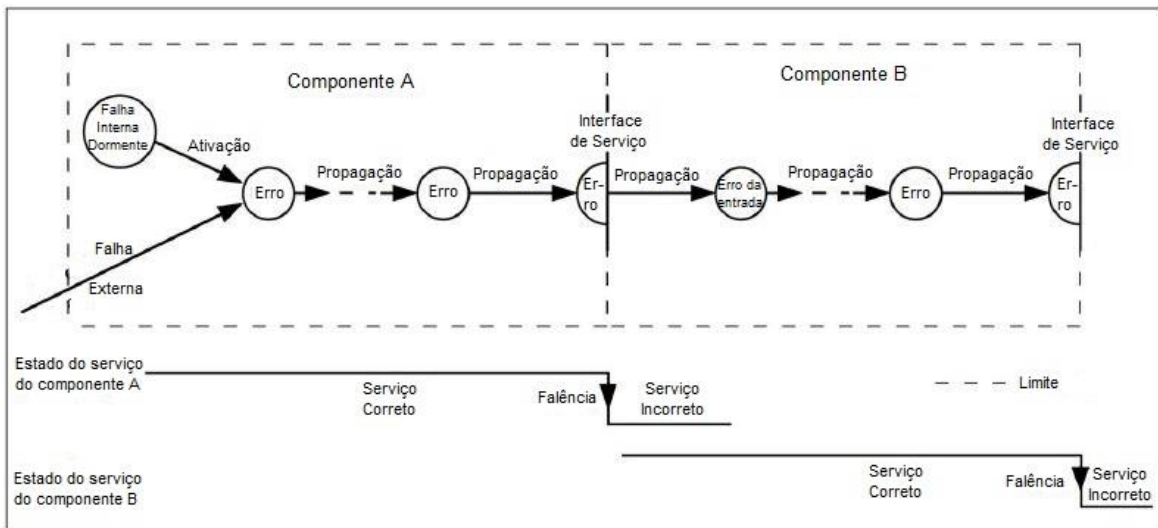
Na literatura existem diferentes abordagens para os conceitos e encadeamentos de falha, erro e falência, ex.: 1) Computação e Comunicação Digitais; e 2) Controle e Automação

Na Computação e Comunicação Digitais, os erros causam as falhas; e estas causam as falências. Por exemplo, os esforços para a definição dos conceitos associados à Dependabilidade e Tolerância a Falhas de sistemas computacionais datam de 1980 quando um comitê conjunto sobre Conceitos Fundamentais e Terminologia foi formado pelo *IEEE Computer Society Technical Committee on Fault-Tolerant Computing* (IEEE CS TC-FTC) e pelo *IFIP Working Group 10.4 on Dependable Computing and Fault Tolerance* (IFIP EG 10.4). O artigo *Basic Concepts and Taxonomy of Dependable and Secure Computing* (AVIZIENIS et al., 2004), apresenta as definições, conceitos e atributos relativos a falhas, erros e falências.

Para Avizienis et al. (2004), uma **falência** do serviço ou, abreviadamente, falência, é um evento que ocorre quando o serviço fornecido desvia inaceitavelmente e definitivamente do serviço correto ou, em outras palavras, uma falência é uma transição inaceitável e definitiva do serviço correto para o serviço incorreto. O desvio do serviço correto pode assumir formas diferentes as quais são denominadas **modos de falência** do serviço. Os modos de falência podem ser classificados de acordo com as severidades da falência. Um **erro** é a parte do estado total do sistema que pode levar a uma subsequente falência do serviço. Uma **falha** é a causa determinada ou hipotética de um erro. Para os autores, o **serviço** fornecido por um sistema é o seu comportamento como ele é percebido por seus usuários.

A Figura 2.8 mostra os mecanismos de criação/ativação, propagação e manifestação em encadeamentos de falhas, erros e falências de acordo com Avizienis et al. (2004) aos quais os autores se referem como **patologia da falência**.

Figura 2.8 – Propagação do erro em sistemas computacionais.



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

Uma **falha** está **ativa** quando produz um erro. Uma falha é ativada quando uma entrada é aplicada a um componente fazendo com que uma **falha dormiente** torne-se ativa.

A **propagação** de um erro no interior de um componente é causada pelo processo de computação. A propagação do erro do componente A ao componente B ocorre quando o erro atinge a interface de serviço do componente A. Neste momento, o serviço fornecido pelo componente A ao componente B torna-se incorreto e a resultante falência do serviço de A manifesta-se como uma falha externa para B.

A **falência** de um componente causa uma falha transiente ou permanente no sistema que contém o componente. A falência do serviço de um sistema causa uma falha externa transiente ou permanente no(s) sistema(s) que recebe(m) o serviço.

Os mecanismos descritos possibilitam o **encadeamento de falhas, erros e falências** por meio das relações de causalidade indicada pelas setas na Figura 2.9.

Figura 2.9 – Encadeamento de falhas, erros e falências em sistemas computacionais.



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

Um erro é detectado se sua presença é indicada por uma mensagem ou por um sinal. Erros que são presentes, mas não são detectados são **erros latentes**.

Uma falência de serviço é detectada por **mecanismos de detecção** no sistema que verificam a correção do serviço fornecido para o usuário na interface de serviço. Falências são consideradas **sinalizadas** quando as perdas de função são detectadas e sinalizadas por meio de um **sinal de advertência**. Caso contrário, são falências não sinalizadas. Os mecanismos de detecção têm, eles mesmos, dois modos de falência: a) Modo 1: sinalização da perda de uma função quando não ocorre nenhuma falência (**falso alarme**); b) Modo 2: não sinalização da perda de uma função quando ocorre uma falência (**perda de alarme**).

O exemplo a seguir (AVIZIENIS et al., 2004) mostra a relação entre falha, erro e falência. Um curto-circuito no interior de um circuito integrado é uma falência (com respeito à função do circuito). A consequência (uma conexão presa em 0 ou 1, a modificação da função do circuito, etc.) é uma falha que permanecerá latente enquanto não for ativada. Após sua ativação (acessando o componente e expondo a falha por meio de uma configuração apropriada de entrada) a falha torna-se ativa e produz um erro o qual provavelmente se propagará e criará outros erros. Se e quando o(s) erro(s) propagado(s) afetar(em) o serviço fornecido (no conteúdo da informação e/ou no tempo de fornecimento), ocorre uma falência.

Ainda na Computação e Comunicação Digitais, Lala e Harper (1994) abordam a presença das **falhas de modo comum**, apresentam uma classificação das mesmas e propõem formas para o seu tratamento.

Diferentemente da Computação e Comunicação Digitais, nos modelos adotados em outras áreas da tecnologia como Controle e Automação, inexistente o conceito de erro como elo causal entre falha e falência.

Em Controle e Automação, as falhas são consideradas as causas das falências. Por exemplo, a *International Federation of Automatic Control – IFAC* (IFAC, 2017) define **falha** como “um desvio não permitido de ao menos uma propriedade ou parâmetro característico de um sistema da condição aceitável/usual/padrão” e **falência** como “uma interrupção permanente da capacidade do sistema desempenhar uma função requerida em condições operacionais especificadas”. Isermann (2006) observa que:

- Uma falha é um estado dentro do sistema;
- Uma falência é um evento;
- Uma falência resulta de uma ou mais falhas;
- Uma falha pode causar a redução ou perda da capacidade de uma unidade funcional realizar uma função requerida;
- Falhas são frequentemente difíceis de detectar.

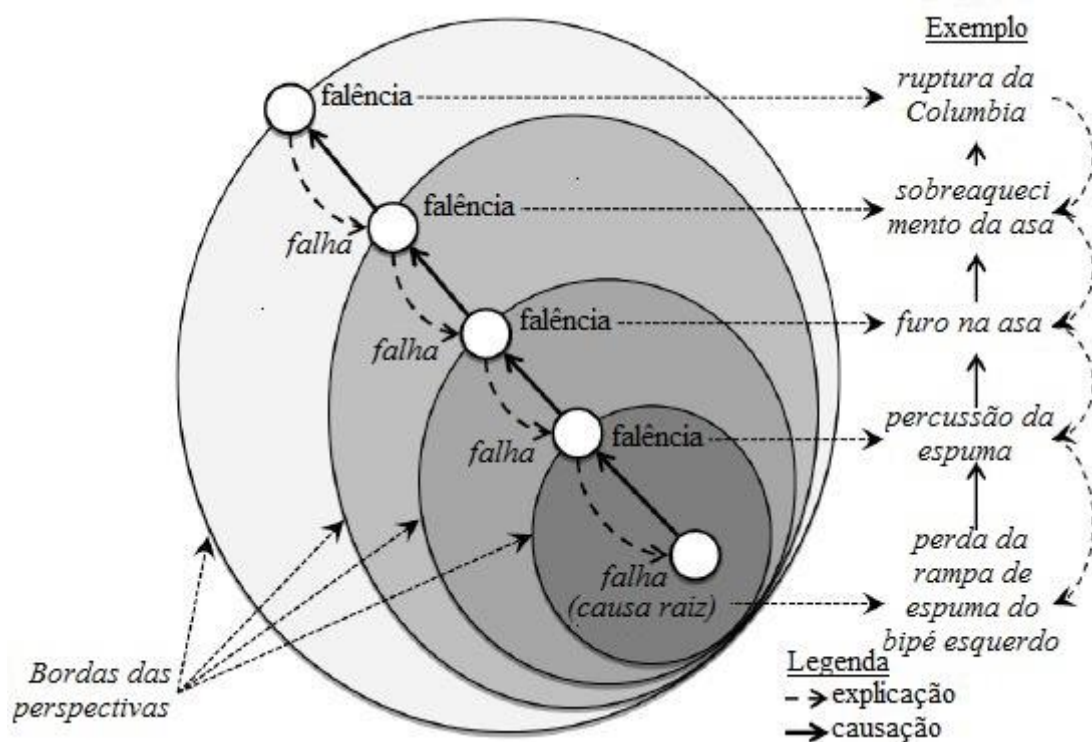
Na área espacial, o *Glossary of Terms* (ECSS, 2012) define **falha** como “estado de um item caracterizado pela incapacidade de apresentar o desempenho requerido”. O glossário define **falência** como “evento que resulta em um item incapaz de realizar sua função requerida”. Uma falha pode gerar uma falência.

O *Fault Management Handbook* (NASA, 2012), define **falência** como o “desempenho inaceitável de uma função”. Falência é um efeito que pode resultar de causas internas ou de causas externas ao sistema. **Falha** é definida

como uma causa interna da falência. Falhas e falências são, portanto, conectadas por uma relação de causa e efeito.

No *Handbook* é ressaltado, no entanto, que uma causa de uma perspectiva é frequentemente vista como um efeito de outra perspectiva o qual é o evento a ser explicado por uma causa mais profunda. Uma **causa raiz** é o primeiro evento em uma cadeia de eventos falência; uma causa precedente é o último evento causal na cadeia. Várias causas raízes podem interagir assim como várias causas precedentes podem interagir para produzir uma falência. Os conceitos de falha e falência são ligados de forma hierárquica e recursiva, como mostra a Figura 2.10.

Figura 2.10 – Encadeamento de eventos falha/falência no acidente do ônibus espacial Columbia.



Fonte: Adaptado de NASA (2012).

Os conceitos de falha, erro e falência usados neste trabalho são apresentados na seção 3.1.

2.7 FMEA/FMECA

Na literatura são encontradas várias ferramentas e técnicas para identificação das falhas potenciais de um sistema. Conforme a seção 2.8.8, onde são descritos exemplos de estratégias de FDIR, as ferramentas usualmente empregadas na área espacial para a identificação das falências potenciais são a FMEA/FMECA (Análise dos Modos de Falência e seus Efeitos / Análise dos Modos de Falência, seus Efeitos e Criticidade) e a FTA (Análise da Árvore de Falhas).

Estas ferramentas são aplicadas isoladamente ou de forma combinada. Quando aplicadas de forma combinada como, por exemplo, em Rice (2008), a FTA é usada em análises *top/down* da missão, dos subsistemas e chega até os níveis mais baixos (internos aos subsistemas) com o objetivo de identificar as interações das falhas no nível baixo com os modos de falência do nível sistema enquanto que a FMEA/FMECA é usada com o objetivo de identificar os modos de falência dos níveis mais baixos.

Em geral, quando apenas uma das ferramentas é usada, a ferramenta FMEA/FMECA é aplicada nas análises para identificação dos modos de falência como, por exemplo, em Bak et al. (1996); Bøgh e Blanke (1997).

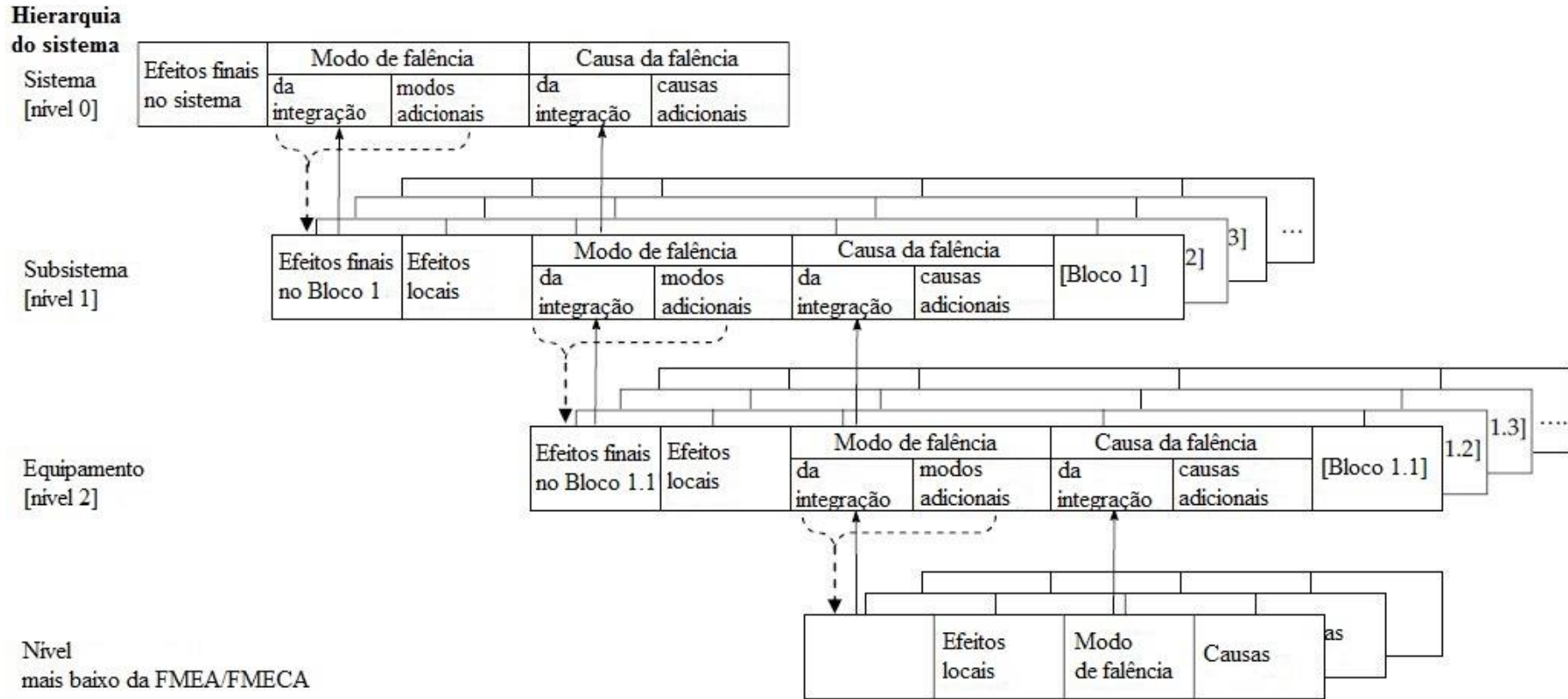
A ferramenta FMEA/FMECA tem sido utilizada nos programas de satélites do INPE com o objetivo principal de identificar todos os potenciais modos de falência e seus efeitos, de tal maneira que as falências de maior severidade ou de maior criticidade possam ser eliminadas ou minimizadas (RABELLO, 2017).

De acordo com ECSS (2009a), a FMEA e a FMECA são aplicadas para sistematicamente identificar os modos de falências potenciais em produtos e processos e avaliar os seus efeitos no sistema tendo em vista definir ações de mitigação. Os modos de falência identificados por meio da FMEA são classificados de acordo com a severidade de seus efeitos. A FMECA é uma extensão da FMEA na qual os modos de falência são classificados com base

na sua criticidade, ou seja, na probabilidade de ocorrência da falência multiplicado pela severidade do efeito dessa falência.

A análise dos modos de falência é aplicada no nível hierárquico do sistema no qual os efeitos das falências estão sendo avaliados. Na integração de análises realizadas em diferentes níveis, os efeitos finais identificados em cada nível hierárquico tornam-se os modos de falência do nível imediatamente superior. Já os modos de falência identificados em cada nível hierárquico tornam-se as causas da falência, i.e., as falhas, do nível imediatamente superior. A Figura 2.11 apresenta uma representação gráfica da integração entre FMEAs de diferentes níveis.

Figura 2.11 – Representação gráfica da integração de FMEAs de diferentes níveis hierárquicos.



Fonte: Adaptado de ECSS (2009a)

2.7.1 FMEA Funcional

FMEAs funcionais e FMEAs mistas, i.e. FMEA que misturam o funcional com o físico são empregadas nas fases iniciais dos projetos quando as informações sobre os componentes físicos ainda não estão disponíveis ou estão parcialmente disponíveis. A ECSS-Q-ST-30-02C (ECSS, 2009), por exemplo, recomenda que a FMEA/FMECA de sistemas complexos deve inicialmente ser realizada utilizando uma abordagem funcional a qual deve ser seguida por uma FMEA/FMECA física assim que informações sobre os principais blocos estejam disponíveis.

2.7.2 Modos de Falência de uma Função

Denson (2010) define seis possíveis modos de falência para uma função:

- a) Não realizar a função;
- b) Realizar a função parcialmente;
- c) Realizar a função intermitentemente;
- d) Realizar a função não intencionalmente;
- e) Realizar a função excessivamente;
- f) Realizar a função de forma degradada.

A distinção entre a realização parcial e a realização de forma degradada de uma função está no fato de que no primeiro caso, parte da função não é realizada desde o início enquanto no segundo caso a função é realizada integralmente no início e degrada-se com o decorrer do tempo.

Outros autores como, por exemplo, Burge (2010) adotam apenas cinco modos de falência para as funções, excluindo o item f ('Realizar a função de forma degradada'). Outras abordagens são, no entanto, encontradas na literatura. Marshall (2011/2012), por exemplo, adota cinco modos de falência mas

substitui o modo 'Realizar a função mais do que é necessário' por 'Realizar a função fora de especificação'.

Burge (2010) afirma que nem todos os modos de falência são aplicáveis para uma função específica. Assim, a aplicação dos modos de falência deve ser contextualizada e sua aplicabilidade decidida em função do que faz a função, de quais são suas saídas e entradas típicas. Burge (2010) ressalta ainda que para uma dada função é necessário indicar qual é o significado exato dos seus modos de falência, ou seja, o significado de cada modo deve também ser contextualizado considerando o que faz a função analisada, suas entradas e saídas.

2.8 FDIR (Fault Detection, Isolation and Recovery)

2.8.1 Introdução

De acordo com Gessner et al. (2004), as funções de tratamento de falhas são necessárias para atender às necessidades de autonomia, confiabilidade e disponibilidade de uma missão. Olive (2010) acrescenta que o tratamento de falhas é parte crítica do projeto de um satélite com impacto nos custos e desempenho de uma missão.

Na literatura, o tratamento de falhas é referenciado por diferentes nomes, entre os quais: 'Detecção, Isolação, Identificação e Recuperação de Falhas' (*Fault Detection, Isolation and Recovery*– FDIR), 'Gerenciamento de Falhas' (*Fault Management* – FM), 'Proteção contra Falhas' (*Fault Protection* – FP), 'Gerenciamento de Redundâncias' (*Redundancy Management* – RM), 'Gerenciamento da Saúde' (*Health Management*- HM).

Neste trabalho, o termo FDIR é preferencialmente utilizado. No entanto, as designações 'Gerenciamento de Falhas'; (FM) e 'Proteção contra Falhas' (FP) as quais são adotadas em muitos trabalhos são também utilizadas. A designação 'Proteção contra Falhas' é adotada tradicionalmente pelo JPL enquanto que 'Gerenciamento de Falhas' vem sendo adotada de forma crescente pela NASA e sua utilização é recomendada em NASA (2012).

O FDIR provê para o segmento espacial a capacidade de detecção, isolamento/identificação e recuperação de falhas que podem comprometer a operação nominal da missão.

De acordo com NASA (2012), o gerenciamento de falhas é a parte da Engenharia de Sistemas dedicada à detecção de falhas e à acomodação tanto do sistema como do subsistema a um comportamento não nominal o qual deve ser projetado, desenvolvido, integrado, testado e operado.

2.8.2 Detecção, Isolação, Identificação e Recuperação

Há várias definições para detecção, isolamento, identificação e recuperação de falhas. Nesta tese serão adotadas as definições apresentadas em Wander e Förstner (2012).

- A detecção de falhas é a determinação da presença de falhas no sistema e do tempo em que ocorreu;
- A isolamento de falhas é a determinação de seu tipo e de sua localização;
- A identificação de falhas tem por objetivo determinar a sua magnitude e comportamento temporal assim como estimar sua severidade e possíveis efeitos no sistema;
- A recuperação do sistema compensa a presença das falhas reconfigurando o sistema por meio, por exemplo, da comutação para uma redundância.

Outro termo comumente usado, FDD (Detecção e Diagnose de Falha), inclui a detecção, a isolamento e a identificação da falha, i.e. todas as tarefas de um FDIR à exceção da recuperação. Já FDI (Detecção e Isolação de Falha), termo mais utilizado na análise da saúde de um sistema, inclui apenas a detecção e isolamento de falha. A Figura 2.12 sumariza estas definições.

Figura 2.12 – Sumário das definições de FDI, FDD e FDIR.



Fonte: Adaptado de Wander e Förstner (2012).

2.8.3 Processo de Desenvolvimento do Tratamento de Falhas (FDIR)

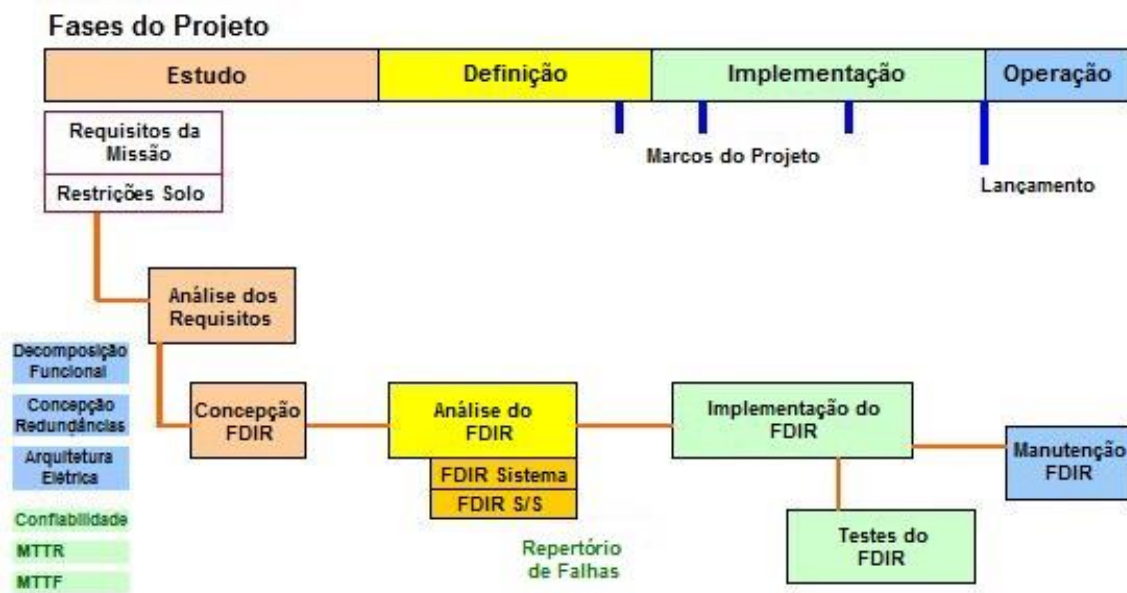
O processo de desenvolvimento do tratamento de falhas, ou seja, de estratégias para a detecção, isolamento / identificação e recuperação (FDIR) tem início na fase de estudos conceituais da missão e estende-se pelas fases seguintes do seu ciclo de vida (GESSNER et al., 2004; NASA, 2012).

As principais tarefas do desenvolvimento de um FDIR, assim como a sua distribuição ao longo do ciclo de vida, são mostradas na Figura 2.13 (GESSNER et al., 2004). Na figura, as fases do ciclo são aglutinadas em quatro grupos:

- a) Fase de Estudos: Compreende o desenvolvimento dos requisitos e projeto conceitual do FDIR. Esta fase pode ser correlacionada à Fase 0 (Análise da Missão e Identificação das Necessidades) e Fase A (Viabilidade), de acordo com as definições estabelecidas no documento ECSS (2009);

- b) Fase de Definição: Compreendem as análises, avaliações e projeto do FDIR no nível sistema e subsistema. Da mesma forma que em a), esta fase pode ser correlacionada à Fase B (Definição Preliminar) e Fase C (Definição Detalhada), de acordo com as definições estabelecidas no documento ECSS (2009);
- c) Fase de Implementação: Compreende a implementação e testes do FDIR. Da mesma forma que em a), esta fase pode ser correlacionada à Fase D (Qualificação e Produção), de acordo com as definições estabelecidas no documento ECSS (2009);
- d) Fase de Operação: Operação e Manutenção. Da mesma forma que em a), esta fase pode ser correlacionada à Fase E (Operação / Utilização) e Fase F (Descarte), de acordo com as definições estabelecidas no documento ECSS (2009).

Figura 2.13 – Desenvolvimento de um FDIR ao longo das fases do ciclo de vida.



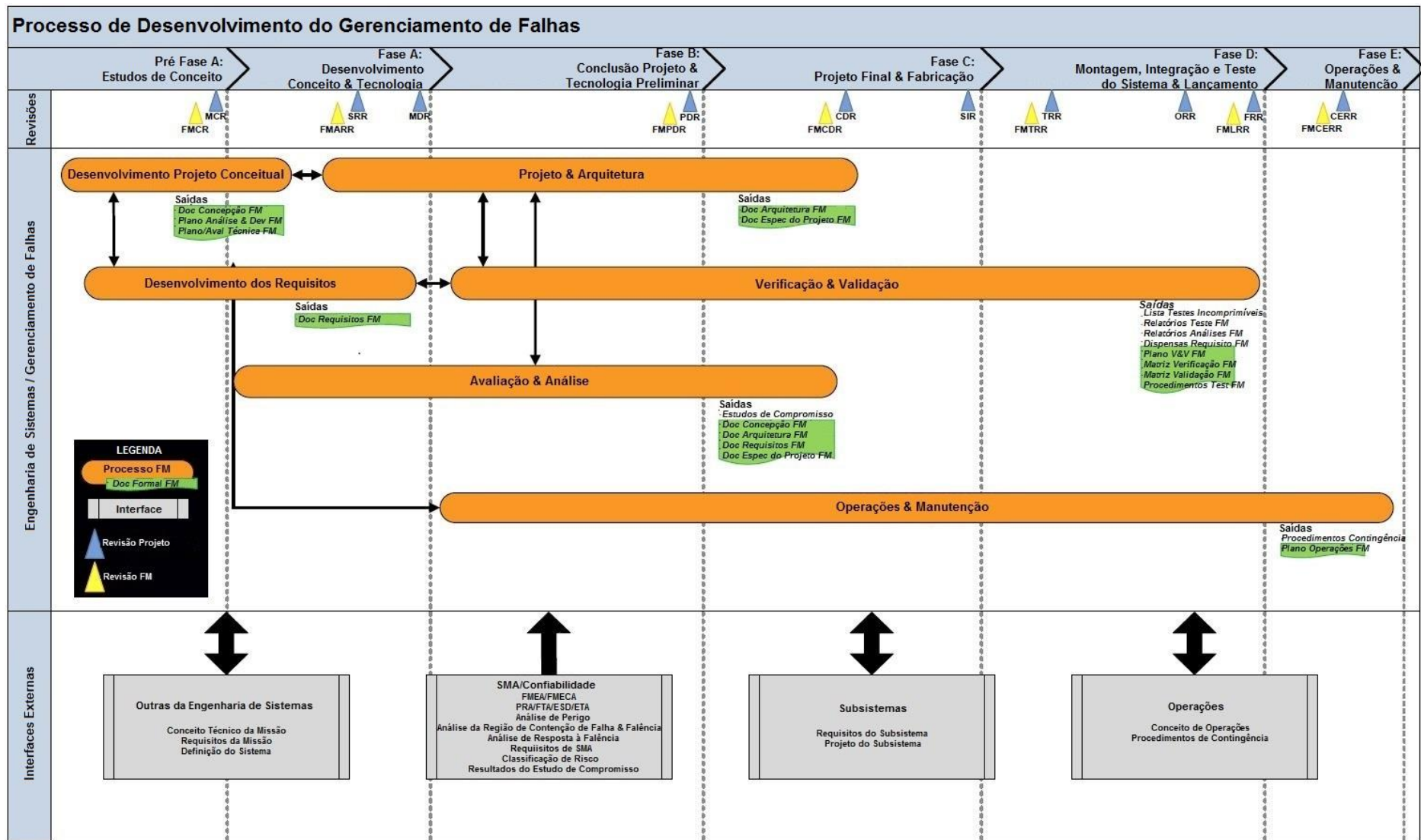
Fonte: Adaptado de Gessner et al. (2004).

O repertório de falhas (Figura 2.13) consiste no conjunto de falhas que será tratado. O repertório é gerado por meio da aplicação de análises que contam usualmente com ferramentas como FMEA, FMECA, FTA para identificação das falhas.

De acordo com NASA (2012), além das ferramentas mencionadas, outras ferramentas e técnicas são também utilizadas tanto na identificação das falhas como na avaliação das mesmas e de seus tratamentos, tais como: PRA (*Probabilistic Risk Assessment*), FEPP (*Failure Effects Propagation Paths*), *Hazard Analysis*, *Event Sequence Diagrams / Event Tree Analysis*, *Failure Containment Region (FCR) Analysis*, *Failure Response Analysis*, *Failure Detection and Isolation Analysis*, *Failure Prognostics Analysis*.

A Figura 2.14 apresenta em detalhes as tarefas para o desenvolvimento do gerenciamento de falhas, seus inter-relacionamentos, interfaces externas e sincronização com as revisões sistêmicas ao longo do ciclo de vida da missão (NASA, 2012).

Figura 2.14 – Processo de gerenciamento de falhas como parte do processo de engenharia de sistemas.



Fonte: Adaptado de NASA (2012).

2.8.4 Recursos e Mecanismos de um FDIR

De acordo com Wander e Föstner (2012, 2013), tradicionalmente o gerenciamento de falhas conta com redundâncias e algoritmos associados com verificações de consistência, mecanismos de votação e técnicas de estimação. Limiares fixos são usados para reconhecimento de comportamento não nominal.

As ações de detecção e isolamento são definidas após avaliação na fase de projeto dos possíveis cenários de falhas e falências por meio de ferramentas como Análise de Árvore de Falhas (FTA) e Análise dos Modos de Falência, seus Efeitos e Criticidade (FMECA). Com base nos resultados destas análises, os eventos críticos são identificados e os procedimentos de recuperação são definidos.

Se, durante a operação, uma falha previamente identificada é detectada e isolada pelo FDIR, o procedimento de recuperação previamente definido é aplicado o que, de forma geral, resulta na comutação para uma redundância ou na mudança do modo de operação da nave para o Modo Seguro. No Modo Seguro, a diagnose da falha, a recuperação do sistema e o retorno da espaçonave ao Modo Nominal de operação são realizados pelo Segmento Solo.

2.8.4.1 Redundância

De acordo com Gessner et al. (2004), as redundâncias em um sistema determinam em grande parte os recursos de um FDIR. O manejo das várias configurações baseadas nos recursos redundantes é um aspecto importante nas considerações relativas à autonomia e FDIR.

As redundâncias podem ser classificadas em: física, funcional/analítica, informacional e temporal. A redundância física consiste no uso de cópia idêntica do *hardware*. A redundância funcional/analítica consiste no uso de *hardware*, *software* ou procedimentos de operação dissimilar para realizar funções idênticas. A redundância informacional utiliza informação extra para

detectar e potencialmente recuperar de certos tipos de falência. A redundância temporal consiste na repetição de uma função quando ocorrer falência na sua primeira execução (NASA, 2012).

2.8.4.2 Modo Seguro de Operação

O Modo Seguro ou Modo de Sobrevivência representa a última reação do FDIR de uma espaçonave a uma falha. No Modo Seguro, a espaçonave é configurada de forma que possa permanecer em segurança sem a intervenção do Segmento Solo por um período determinado de tempo. Todas as unidades ou subsistemas não essenciais são desligados para reduzir o consumo de energia e evitar interferência em outros subsistemas. A espaçonave é orientada para uma atitude (termicamente segura) com relação ao Sol ou a Terra. Um ou mesmo todos os subsistemas são comutados para suas redundâncias (WANDER; FÖSTNER, 2012).

De acordo com Gessner et al. (2004), tipicamente, as seguintes funcionalidades devem ser mantidas:

- Suprimento de energia;
- Controle térmico de equipamentos relevantes;
- Comunicação com o Segmento Solo;
- Altitude da órbita.

2.8.5 Estratégias de FDIR

A expressão **estratégia de FDIR** é frequentemente utilizada na literatura para se referir à arquitetura e aos métodos (ou técnicas, ou modelos) de detecção, isolamento e recuperação (por exemplo, estratégia de FDIR) de um FDIR. A expressão é, no entanto, também empregada referindo-se apenas aos métodos (por exemplo, estratégia de FDD, estratégia de FDI, etc). Neste trabalho, a expressão é usada na primeira acepção para se referir à arquitetura mais os métodos de um FDIR.

2.8.6 Arquiteturas de FDIR

Tradicionalmente, as arquiteturas de FDIR, assim como as estratégias utilizadas, são definidas em função dos requisitos e restrições da missão. Fatores como, por exemplo, restrições orçamentárias podem impor limitações no uso de recursos, como as descritas em RICE et al. (2008).

Basicamente, as arquiteturas podem ser centralizadas, descentralizadas/distribuídas e hierárquicas. Estas arquiteturas podem, no entanto, ser combinadas em um único FDIR como, por exemplo, a utilização de uma arquitetura descentralizada para a detecção e a identificação de falhas em cada subsistema e de uma arquitetura centralizada para isolamento e recuperação das falhas (ALANA et al., 2012).

A Secção 0 trata em maiores detalhes as arquiteturas hierárquicas; e a Secção 2.8.6.2 apresenta arquitetura de FDIR com capacidade decisória visando sistemas autônomos complexos.

2.8.6.1 Arquiteturas Hierárquicas

A norma ECSS-E-ST-70-11C (ECSS-E-ST-70-11C, 2008) estabelece que as funções de FDIR sejam implementadas de forma hierárquica a fim de que a detecção, isolamento e recuperação de falhas ocorram no nível mais baixo possível de implementação.

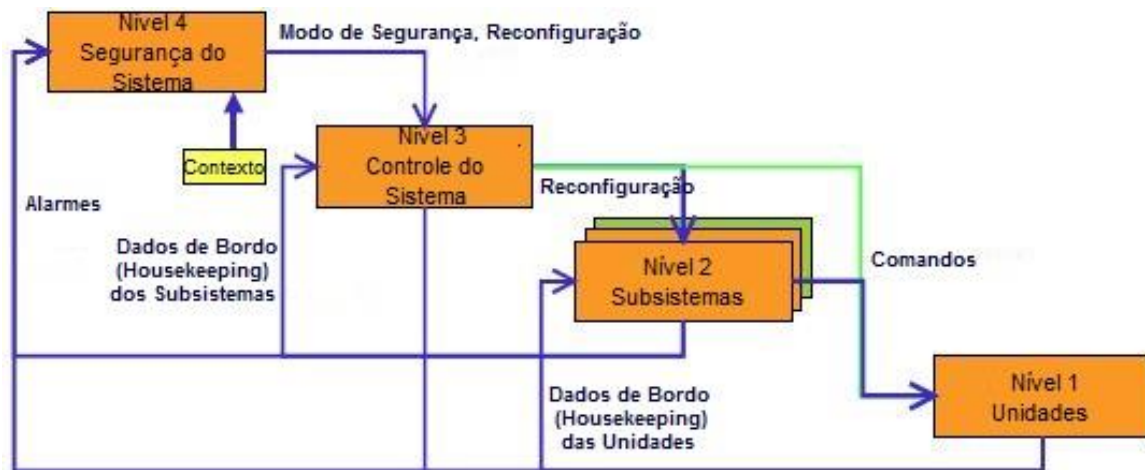
Em consonância com essa norma, Gessner et al. (2004) propõem uma arquitetura hierárquica para o FDIR fundamentado em razões técnicas, de desenvolvimento e programáticas.

- a) Técnicas: a arquitetura hierárquica permite o estabelecimento de uma estrutura de controle com interfaces claramente definidas entre todas as instâncias do FDIR;
- b) Desenvolvimento: a arquitetura hierárquica possibilita distribuir os testes do FDIR de acordo com o plano de desenvolvimento do projeto;

- c) Programáticas: a arquitetura hierárquica permite compatibilizar os diferentes níveis hierárquicos com a organização do projeto.

A Figura 2.15 apresenta um diagrama IDEF0 com a decomposição hierárquica funcional de um FDIR.

Figura 2.15 – Decomposição hierárquica funcional de um FDIR.



Fonte: Adaptado de Gessner et al. (2004).

De acordo com Gessner et al. (2004), a decomposição funcional tem por base os seguintes critérios:

- O nível mais alto da hierarquia é a salvaguarda do sistema que atua reconfigurando o sistema ou colocando a nave no modo seguro;
- O controle do sistema é separado do controle do subsistema em função de requisitos de isolamento de falhas;
- As unidades dentro de um subsistema reportam-se a instâncias mais altas;
- Dependendo dos requisitos de tempo de reação do sistema, é permitido ignorar a hierarquia.

De acordo com Gessner et al. (2004), de forma geral, as instâncias de um FDIR executam funções de comando e controle do nível hierárquico imediatamente abaixo usando os dados de bordo (*housekeeping data*) ou os

alarmes como entradas. Como o nível mais alto da hierarquia (nível 4) não tem nenhuma instância imediatamente superior, o que é especificamente verdadeiro para as missões interplanetárias, as funcionalidades deste nível são normalmente implementadas com redundância “a quente”, ou seja, são implementadas por meio de duas ou mais réplicas que executam simultaneamente as mesmas funções. No nível 2 e no nível 3, as funções de FDIR são implementadas por *software* o que faz com que possam ser facilmente modificadas pelo Segmento Solo. Já no nível hierárquico mais alto (nível 4), as funções de FDIR são, em geral, implementadas por *hardware*. Estas funções geram os comandos para reconfigurar o sistema.

Para fins de implementação de um projeto, é essencial o desenvolvimento de um modelo abrangente do FDIR, o que requer uma decomposição hierárquica funcional completa e suficientemente detalhada das funções de FDIR nos níveis de sistema, subsistema e unidades (GESSNER et al., 2004).

A decomposição funcional apresentada na Figura 2.15 considera apenas as instâncias tratadas a bordo da nave espacial. No caso da recuperação da falha não ser possível nessas instâncias, a nave espacial é colocada no modo seguro e o tratamento da falha é realizado em uma instância superior pelo Segmento Solo. A Figura 2.16 apresenta, para um satélite hipotético, um diagrama com todas as instâncias, inclusive o Segmento Solo, no qual são indicados exemplos de falhas em cada instância e quem é o responsável pelo seu tratamento.

Figura 2.16 – Exemplo de hierarquia de FDIR para um satélite hipotético.

Nível 4 Tratado pelo Segmento Solo	Falências maiores do sistema Falências na comunicação Falências na abertura de painéis Etc.		
Nível 3 Tratado pela Unidade de Reconfiguração (HW) do Computador	Alarmes gerados pelo HW Múltiplos alarmes gerados pelo EDAC Falências na potência da espaçonave Etc.		
Nível 2 Tratado pelo SW do Sistema da Espaçonave	Mau funcionamento do sistema Inconsistências no cálculo da atitude Falências na potência da espaçonave Etc.		
Nível 1 Tratado pelo SW do Subsistema	Mau funcionamento dos subsistemas Falências de equipamentos do subsistema Falências na comunicação interna do subsistema Etc.		
Nível 0 Tratado Internamente pela Unidade	Mau funcionamento interno da unidade Falências recuperáveis internamente como a do EDAC ou similares Etc.	Mau funcionamento interno da unidade Falências que requerem recuperação imediata como proteção contra curto circuito Etc.	Mau funcionamento do barramento de dados Falências recuperáveis por meio de repetições da comunicação Etc.

Fonte: Adaptado de Eickhoff (2012).

A Tabela 2.7 apresenta um sumário do impacto das falhas no sistema de acordo com o nível em que elas ocorrem, como as falhas são detectadas e quais as ações podem ser executadas pelo sistema de controle da espaçonave.

Tabela 2.7 – Detecção e recuperação de falhas nos níveis hierárquicos do FDIR.

Nível Falha/Falência	Impacto	Detecção da Falha	Recuperação do Sistema
Nível 0	Nenhum impacto no desempenho do sistema	Verificação local interna da unidade; verificação do dado transmitido; verificação da consistência.	Repetição local de comando da unidade, reinicialização da unidade, recarga
Nível 1	Desempenho degradado do subsistema	Verificação dos limites de parâmetros da unidade, verificação da plausibilidade	Chaveamento por meio do subsistema para unidade redundante, repetição de comando, recarga
Nível 2	Perda de desempenho do subsistema	Vários alarmes provenientes da verificação de consistência de unidades do nível 0	Chaveamento para redundâncias no nível da plataforma, repetição de comando
Nível 3		Falhas nas unidades de FDIR	
Nível 4	Perda de desempenho do sistema; interrupção da missão	Vários alarmes do nível 2 e 3, alarmes de <i>hardware</i> e.g. Sol/Terra fora do campo do sensor, propulsor preso em aberto	Comutação do modo operacional para o modo de segurança, intervenção do Segmento Solo para recuperação do sistema e retorno ao modo nominal

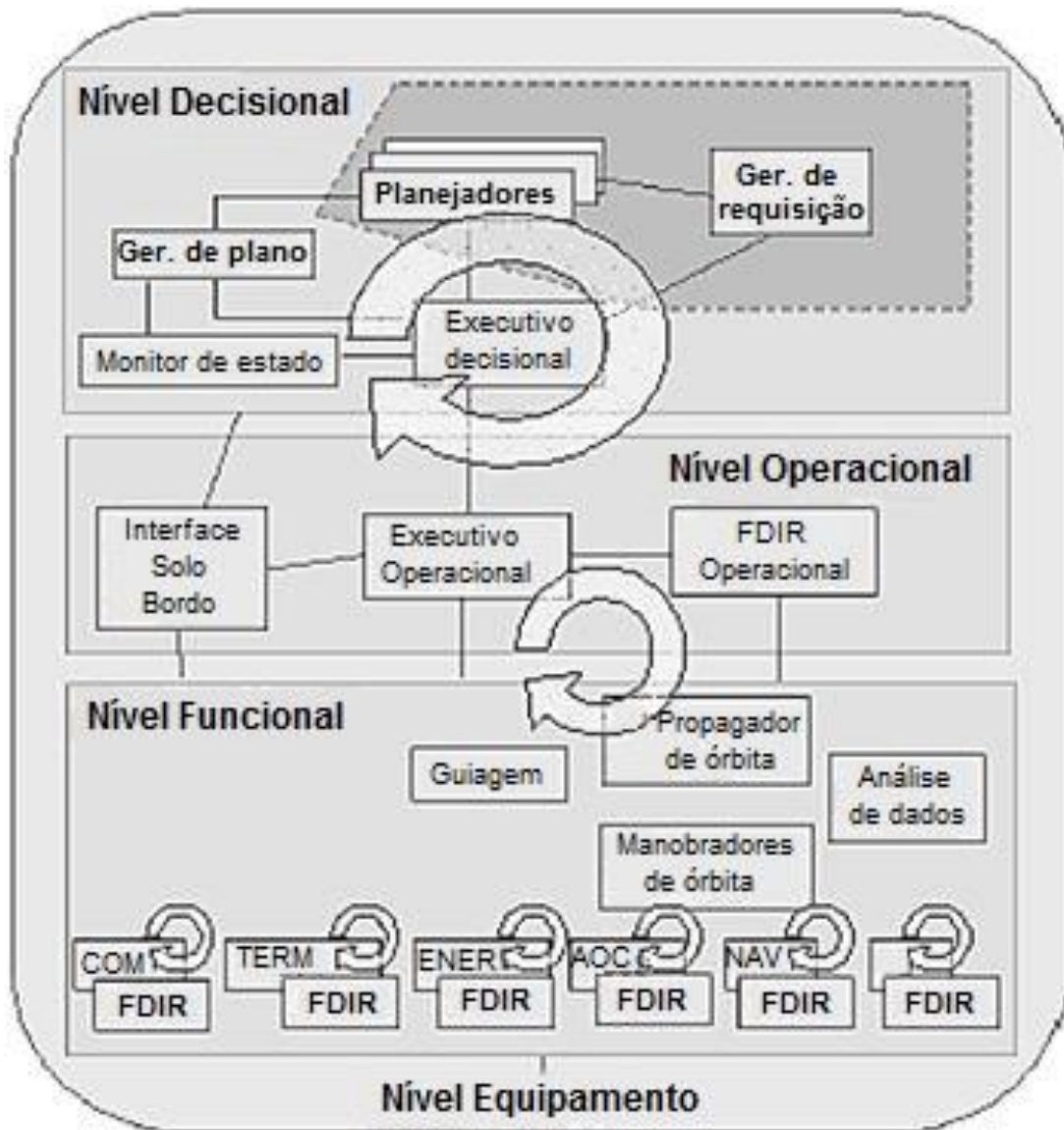
Fonte: Adaptado de Wander e Förstner (2012).

2.8.6.2 Arquitetura com Capacidade Decisória

De acordo com Olive (2012), a necessidade crescente de aumento da autonomia das missões científicas e de observação da Terra com o objetivo de redução do tempo de reação e da tomada de decisões a bordo, oferece oportunidades de introdução de novos conceitos de FDIR a bordo das espaçonaves.

Com foco em missões de observação da Terra e missões científicas e no desenvolvimento de sistemas autônomos complexos, Olive (2012) propõe, com base em Lemai et al. (2006), uma arquitetura com capacidade decisória, organizada em três níveis hierárquicos, conforme mostra a Figura 2.17 possibilitando o desenvolvimento de estratégias de FDIR que sejam ao mesmo tempo centralizadas, de forma a prover em um único local uma visão sintética do estado do satélite para a tomada de decisões a bordo, e distribuída, de forma a manter o FDIR local no nível do subsistema e da unidade.

Figura 2.17 – Arquitetura com capacidade decisória.



Fonte: Adaptado de Olive (2012).

Esta estratégia é compatível com a arquitetura hierárquica descrita na seção anterior, onde os níveis 0, 1, 2 são cobertos pelas partes distribuídas e os níveis 3 e 4 são cobertos pela parte centralizada.

2.8.7 Métodos de Detecção, Isolamento, Identificação e Recuperação

Os métodos tradicionais de detecção, isolamento, identificação e recuperação fazem uso de técnicas simples como, por exemplo, verificações de consistência, mecanismos de votação, técnicas simples de estimação. Limites fixos são também usados para um rápido reconhecimento de uma condição

fora de tolerância. Métodos avançados têm, no entanto, sido aplicados no ambiente espacial ou encontram-se em estudo e desenvolvimento visando sua utilização no espaço. Entre outros, podem ser mencionados os métodos baseados em modelos, métodos baseados em dados, métodos baseados em Lógica *Fuzzy* e métodos baseados em Redes Bayesianas, e até o filtro de Kalman.

2.8.7.1 Métodos Baseados em Modelos

A redundância analítica explora as relações matemáticas entre variáveis medidas e variáveis estimadas para detectar possíveis falhas. O conjunto de métodos que resultaram desta abordagem é conhecido como métodos baseados em modelos (MARZAT et al., 2012), onde modelo deve ser entendido como modelo dinâmico baseado no conhecimento. Marzat et al (2012), apresentam um levantamento dos métodos quantitativos baseados em modelos para a diagnose de falhas na área aeroespacial. Zolghadri (2012) discute algumas tendências e avanços em métodos de detecção, isolamento e recuperação de falhas baseados em modelos para aplicações espaciais.

Exemplo da utilização de métodos baseados em modelos é encontrado em Muscettola et al. (1998). O componente Identificação e o componente Reconfiguração de Modo do *Remote Agent Experiment*, experimento da sonda *Deep Space One*, lançada pela NASA em 1998, são providos por um controlador discreto Livingstone (Figura 2.18). Livingstone é um sistema de diagnose baseado em modelos que usa um modelo qualitativo dos componentes de um sistema e as suas interações, tanto em condições nominais de operação como na presença de falhas.

O componente Identificação do Modo (MI) do controlador provê a capacidade de rastrear mudanças na configuração da sonda devido a comandos do Executivo e falhas de componentes. O MI usa o modelo da sonda e os comandos executivos para prever a próxima configuração nominal. Os valores previstos são comparados com os valores reais monitorados e discrepâncias entre eles indicam uma falência. Neste caso, o MI isola a falha e realiza a

diagnose de sua causa usando algoritmos adaptados da diagnose baseada em modelos. Quando a configuração corrente deixa de satisfazer os objetivos da configuração ativa, o componente Reconfiguração de Modo do controlador Livingstone pode identificar um conjunto com custo mínimo de procedimentos de controle que configure a sonda de forma a satisfazer os objetivos.

Figura 2.18 – Diagrama de blocos da arquitetura Livingstone.



Fonte: Adaptado de Muscettola et al. (1998).

2.8.7.2 Métodos que Utilizam Redes Bayesianas

Uma rede Bayesiana é um modelo da distribuição conjunta de probabilidade *a posteriori* do domínio do problema. Assim, os valores observados de algumas das variáveis do domínio podem ser usados como entrada do modelo para atualizar o valor de variáveis não observadas. Na literatura podem ser encontrados trabalhos que utilizam as redes Bayesianas em estratégias de FDIR.

Holsti (2001); Paakko et al. (2001) apresentam o projeto *Advanced FDIR* (AFDIR). Patrocinado pela ESA e coordenado pela Astrium SAS, o projeto foi desenvolvido pela *Space Systems Finland Ltd* com a colaboração da *University of Helsinki* e emprega dois métodos de diagnose: raciocínio probabilístico usando Redes Bayesianas e diagnose baseada em modelos que usa Redes Causais. O AFDIR foi aplicado no satélite hipotético ASOS (*Advanced Smart*

Observation Satellite), similar a um satélite pequeno de observação da Terra, com um subsistema de controle de atitude composto por sensores autônomos de estrelas, GPS, magnetômetros, magnetotorques e rodas de reação.

O projeto *Anomaly Resolution and Prognostic Health Management for Autonomy* (ARPHA) é outra iniciativa patrocinada pela ESA envolvendo a aplicação de Redes Bayesianas em FDIR (CODETTA-RAITERI; PORTINALE, 2010). O projeto, desenvolvido pela Thales/Alenia Italy em colaboração com a Università' del Piemonte Orientale, explora as capacidades de modelagem e inferência das Redes Bayesianas Dinâmicas no projeto e implementação de um FDIR para uma nave autônoma. O método permite realizar a diagnose de uma falha e a recuperação do sistema (recuperação reativa) e o prognóstico de uma falha e a recuperação preventiva do sistema. Codetta-Raiteri e Portinale (2015) apresentam os resultados obtidos em um estudo de caso do ARPHA envolvendo a análise do FDIR do sistema de suprimento de energia do robô ExoMars em diferentes cenários simulados de anomalias e falhas.

2.8.7.3 Métodos que Utilizam Lógica Fuzzy

Guiotto et al. (2003) apresentam o trabalho SMART-FDIR patrocinado pela ESA e desenvolvido pela Alenia Spazio e Politecno di Milano, o qual contempla a implementação de um FDIR usando métodos com base nas tecnologias de Inteligência Artificial tais como: *Fuzzy Inductive Reasoning* na detecção; *Possibilistic Reasoning* na isolação e identificação; e *State Variable Transition e Multi-criteria Decision Making* na recuperação.

2.8.7.4 Métodos Baseados em Automação Cognitiva

Com foco em missões interplanetárias e na presença de falhas não previstas, Wander e Fostner (2012) analisam o emprego de métodos de detecção e diagnose utilizados em aplicações industriais e que têm sido objeto de estudos visando sua utilização no espaço, como os baseados em modelos (*model based*), e métodos de *soft-computing*, tais como Lógica Fuzzy, Redes Bayesianas Dinâmicas, Redes Neurais, Teoria da Evidência de Dempster-

Shafer (D-S-E) e Automação Cognitiva. A análise conclui que a Automação Cognitiva é o método mais promissor resultando na proposição, em Wander e Fostner (2013), de um estudo aplicando esta metodologia ao subsistema de potência de uma nave interplanetária.

2.8.7.5 Métodos Baseados em TFPG (Timed Failure Propagation Graph)

Introduzido por Misra (1994), o Grafo Temporizado de Propagação de Falências (TFPG) é um grafo dirigido cujos nós representam os modos de falência e os efeitos dos modos de falência (i.e. as discrepâncias) e as setas representam a progressão temporal das falências e discrepâncias no sistema. As setas são rotuladas com o tempo de propagação entre os nós. As setas podem também ser rotuladas com os modos de operação permitindo que o grafo capture o comportamento na presença de falência para diferentes configurações do sistema.

Formalmente (BITTNER et al., 2017), um TFPG é representado como a ênupla

$$G = (F, D, E, M, ET, EM, DC) \quad (2.1)$$

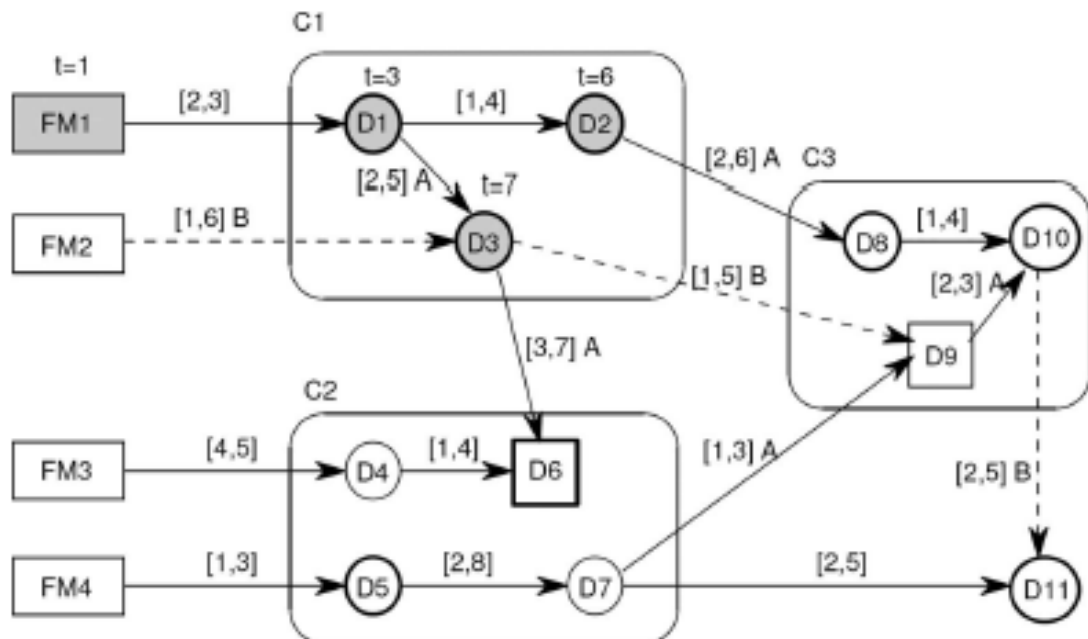
onde:

- F é um conjunto não vazio de modos de falência;
- D é um conjunto não vazio de discrepâncias;
- $E \subseteq V \times V$ é um conjunto não vazio de setas conectando o conjunto de nós $V = F \cup D$;
- M é um conjunto não vazio de modos do sistema (é suposto que, em cada instante de tempo, o sistema está precisamente em um modo);
- $ET: E \rightarrow I$ é um mapa que associa toda seta em E com um intervalo de tempo $[tmin, tmax] \in I$ indicando o tempo de propagação mínimo e máximo da seta (onde $I \in \mathbb{R}_{\geq 0} \times (\mathbb{R}_{\geq 0} \cup \{+\infty\})$ e $tmin \leq tmax$);

- $EM : E \rightarrow 2^M$ é um mapa que associa toda seta em E a um conjunto de modos em M (é suposto que $EM(e) \neq \emptyset$ para toda seta $e \in E$);
- $DC : D \rightarrow \{AND, OR\}$ é um mapa definindo o tipo da discrepância;

A Figura 2.19 é um exemplo de TFPG extraído de Abdelwahed et al. (2009). Na figura, os retângulos representam os modos de falência, os círculos representam as discrepâncias do tipo OR (OU inclusivo - nós disjuntivos) e os quadrados representam as discrepâncias do tipo AND (E - nós conjuntivos). As setas são parametrizadas com o intervalo de propagação (t_{min} , t_{max}) e com os modos de operação nos quais a propagação ocorre (A e B). C1, C2 e C3 representam componentes do sistema. O modo de falência FM1 e as discrepâncias D1, D2 e D3 (preenchidos com a cor cinza) estão ativos. Os tempos t , associados a FM1, D1, D2 e D3, indicam o instante em que os nós tornaram-se ativos.

Figura 2.19 – Exemplo de um TFPG.



Fonte: Abdelwahed et al. (2009).

O TFPG modela prevalentemente o comportamento temporal de uma grande variedade de sistemas na presença de falências. Misra (1994); Abdelwahed et al. (2006) utilizam o TFPG para a diagnose de sistemas enquanto que

Mahadevan et al. (2010) propõem a sua utilização na diagnose de sistemas hierárquicos complexos. Já Abdelwahed et al. (2009) investigam a utilização do TFPG para o prognóstico de falências e discrepâncias e Troiano et al. (2012) propõem a sua extensão de forma a incorporar a recuperação ao modelo. Bittner et al. (2017) utilizam o TFPG no projeto de sistemas críticos para a modelagem da propagação de falências e suporte a avaliação e implementação das funções para detecção, isolamento e recuperação.

Em aplicações espaciais, Ofsthun e Abdelwahed (2007) tratam as falências no sistema de combustível de um satélite, Dubey et al. (2011) descrevem o sistema de gerenciamento da saúde de um satélite com base no TFPG e Hayden et al. (2006) avaliam para a NASA a utilização de TFPG no tratamento das falências da propulsão do lançador Ares I. Ainda em aplicações espaciais, Bittner et al. (2014) utilizam o TFPG no FAME (*Failure and Anomaly Management Engineering*), um processo integrado, baseado em modelos para o projeto de FDIR desenvolvido para a ESA; e Bittner et al. (2017) apresentam três estudos de caso nos quais aplicam o TFPG na análise da segurança e validação do FDIR da sonda Solar Orbiter (SOLO) da ESA.

Além da sua utilização no processo de detecção, isolamento e recuperação, o TFPG oferece outras possibilidades (TROIANO et al., 2012), tais como:

- Modelar como uma falha se propaga em função do tempo de latência, modos de operação e fase do sistema;
- Analisar o tempo de resposta em termos da capacidade de detecção do sensor, da confirmação da detecção e do tempo total, do início da falência até a sua detecção e confirmação;
- Auxiliar o projetista revelando problemas no projeto no estágio inicial de desenvolvimento;
- Apoiar as equipes técnica e operacional na identificação da falência e definição da melhor estratégia de recuperação.

2.8.7.6 Trabalhos Desenvolvidos no INPE

No INPE, têm sido desenvolvidos trabalhos no âmbito do Curso de Pós-Graduação em Engenharia e Tecnologia Espaciais (ETE), Área de Concentração em Mecânica Espacial e Controle abordando detecção, diagnose e reconfiguração de falhas em Sistemas de Controle de Atitude e Órbita-SCAOs de satélites entre os quais podem ser citados: Melo (1991), Teixeira (2005), Leite (2007; 2012), Amaral (2008; 2013), Manelli (2011), Gayarre (2015) e Siqueira (2016). Além desses, os trabalhos de Alonso (1998), Arias (1999; 2012), Pessotta (1999) e Kucinskis (2007; 2012) desenvolvidos por integrantes da ETE no âmbito dos programas de pós-graduação do INPE e do ITA, tratam de sistemas computacionais tolerantes a falhas e sistemas computacionais autônomos.

2.8.8 Algumas Estratégias de FDIR Utilizadas em Missões Espaciais

Nesta seção são revistas algumas estratégias FDIR disponíveis na literatura com o objetivo de apresentar soluções que têm sido adotadas, assim como o estado atual da arte e projetos de pesquisa propostos e em andamento.

2.8.8.1 Satélite Ørsted

O microssatélite dinamarquês Ørsted (BØGH; BLANKE, 1997; BAK et al., 1996), lançado em 1999 com uma massa total de 62 kg, tem como característica marcante a operação autônoma e tolerante a falhas do subsistema ACS (Attitude Control System) com uma quantidade mínima de redundância de *hardware*. O satélite é estabilizado nos três eixos, possui quatro tipos de sensores de atitude (Magnetômetro, Imageador de Estrelas, GPS, Sensor Solar) e tem como atuador dois conjuntos de Magnetotorques. Nesta seção são destacados pontos apresentados em Bøgh e Blanke (1997) e em Bak et al. (1996) considerados relevantes para o desenvolvimento deste trabalho.

O ACS é responsável pelo controle e pela estimação de atitude, validação dos dados dos sensores, gerenciamento dos comandos operacionais, monitoramento das informações e tratamento das falhas.

Para facilitar a realização dessas funções foi adotada a estrutura, já mostrada na Figura 1.1, com três níveis:

- O nível mais baixo contempla entradas e saídas e a malha de controle;
- O nível intermediário contempla os algoritmos de detecção e recuperação de falhas;
- O terceiro nível contempla a lógica de supervisão.

A autonomia é obtida por meio de algoritmos de controle e determinação de atitude reconfiguráveis em tempo real, permitindo sua adaptação às mudanças de fase da missão, às contingências e às falhas. O Supervisor monitora o estado do satélite e reconfigura os algoritmos de ACS de forma a otimizar o desempenho do sistema.

Devido às restrições de custo e massa, a abordagem adotada para dependabilidade inclui:

- Ausência de requisito de falha em segurança;
- Tolerância para a degradação de desempenho em consequência de uma falha;
- Aceitação de redundância de *hardware* para poucos componentes.

A estratégia adotada para a definição do Supervisor consiste de:

1. Realização de uma FMEA de todos os equipamentos envolvidos, a qual, combinada com uma análise completa de todo satélite, indica os efeitos finais no nível do satélite;

2. Efeitos finais são classificados de acordo com sua severidade para seleção daqueles que serão tratados pelo Supervisor;
3. Alternativas para recuperação das falhas são avaliadas;
4. Localização das falhas que originam os efeitos finais é realizada por meio da análise reversa da FMEA;
5. Algoritmos para detecção de falhas são definidos;
6. Ações para recuperação das falhas são definidas;
7. Regras de inferência para o Supervisor são definidas usando as informações sobre falhas/efeitos detectados e de como eles são recuperados. O Supervisor determina as ações mais apropriadas a partir das condições presentes dos comandos recebidos.

2.8.8.2 Satélite WISE

Em Rice et al. (2008), é apresentada a estratégia de proteção contra falhas adotada na missão WISE (*Wide-field Infrared Survey Explorer*) da NASA. A missão inclui um satélite de médio porte com massa de 750 kg, lançado em dezembro de 2009 portando um telescópio espacial na faixa do infravermelho.

Devido aos recursos financeiros limitados, a estratégia tradicional de utilização de redundância para todos os equipamentos mostrou-se inviável para a missão. Apoiada em características da missão como sua curta duração, a herança de equipamentos e da arquitetura para aceitar riscos que não poderiam ser aceitos em outras circunstâncias, a WISE pôde limitar a abrangência da proteção contra falhas e a utilização de redundâncias a bordo do satélite.

O desenvolvimento do projeto da proteção contra falhas tem início com o estabelecimento das prioridades e características da proteção contra falhas da missão. Em primeiro lugar, a proteção contra falhas na WISE procura proteger a saúde e segurança da Plataforma e preservar os itens consumíveis da

missão como, por exemplo, o hidrogênio para resfriamento da ótica e do detector.

A proteção contra falhas é implementada com o objetivo de reduzir o risco para a missão sempre que viável, detectando as falhas que podem ter impacto na saúde do sistema e respondendo, quando o tempo de resposta for crítico, por meio da isolação da falha e da colocação do satélite em uma configuração segura. Respostas autônomas somente tentam recuperar o desempenho necessário para proteger a saúde do sistema. A recuperação do desempenho da carga útil é sempre realizada pelo segmento solo.

Como segunda prioridade, a proteção contra falhas tenta preservar a integridade dos requisitos da carga útil. Devido à sensibilidade da missão com relação ao tempo de inatividade, a proteção contra falhas é projetada para minimizar o tempo de recuperação onde for possível, minimizando a reconfiguração necessária para a retomada da operação da carga útil e maximizando as informações disponíveis para um rápido diagnóstico das falhas.

Para garantir que as falhas mais críticas são consideradas e que as mitigações conseguem uma redução real do risco, é implantado um processo para compilar o repertório de falhas da missão o mais abrangente possível. Para a produção do repertório é utilizada uma combinação da Análise da Árvore de Falhas (FTA) e da Análise dos Modos de Falência, seus Efeitos e Criticidade (FMECA).

A FTA é aplicada no nível da missão e do satélite. No nível da missão, a FTA foi aplicada nos seus eventos. No nível da Plataforma e Carga Útil, a FTA é aplicada nas funções de seus subsistemas até o nível de montagem. O objetivo da FTA é identificar os modos de falência no nível do sistema e as interações das falhas no nível baixo no âmbito da operação do sistema.

A FMECA é aplicada em todas as montagens com o objetivo de identificar os modos de falência no nível baixo os quais foram mapeados na FTA com o

objetivo de criar uma análise completa e consistente de todas as falhas possíveis e de suas interações com o sistema. Para ampliar o repertório de falhas, é ainda utilizado o conhecimento proveniente da experiência com os equipamentos e a arquitetura herdada de outras missões. A Figura 2.20 apresenta o fluxo de trabalho para definição do repertório de falhas.

Figura 2.20 – Fluxo de trabalho para definição do repertório de falhas da missão WISE.



Fonte: Adaptado de Rice et al. (2008).

A partir dos resultados das análises é gerada uma matriz de falhas com aproximadamente 600 falhas onde, a cada falha, foi associado um risco para os objetivos de alto nível da missão com base na probabilidade da falha ocorrer e no impacto da falha no sucesso da missão resultando numa classificação com quatro níveis de criticidade. As falhas são ainda avaliadas tendo em vista o tempo máximo em que a resposta deve ser executada antes que o desempenho do sistema seja impactado.

A identificação de mitigações para as falhas tem início com as falhas de mais alto risco para, a seguir, serem tratadas as falhas de mais baixo risco. Em muitos casos, as medidas de tolerância a falhas intrínsecas ao subsistema permitem dispensar mitigações adicionais. Onde a mitigação é considerada necessária, uma solução preliminar é definida e, se reduz significativamente o impacto da falha, mantida no projeto. Se apresentar nenhum ou pouco impacto na redução do risco, a solução é substituída por medidas que podem ter um impacto melhor ou a detecção e resposta a falhas são realocadas para a operação da missão.

O resultado é um sistema com algumas redundâncias funcionais e de *hardware* e mecanismos de tolerância a falhas que proporcionam a redução de risco mais econômica possível. A proteção contra falhas é distribuída pelo sistema. No nível baixo, funções de *hardware* provêm alguma proteção em condições de risco. O *software* de proteção contra falhas é implantado primariamente no computador principal do satélite. Uma unidade de processamento independente monitora a saúde da unidade principal e é capaz de manter o apontamento e a segurança térmica em caso de falha que impacte o *software* de bordo.

A maior parte dos subsistemas são estruturas *single-string* onde algumas redundâncias foram adicionadas para aumentar a tolerância a falhas em áreas mais sensíveis, como o controle de atitude. Como a WISE é sensível a restrições de apontamento, muitas das redundâncias e da degradação progressiva estão no sistema de apontamento.

A carga útil não possui nenhuma unidade de processamento que realize funções de monitoramento e resposta. Assim a proteção contra falhas é realizada somente pelo *software* de bordo.

2.8.8.3 Missão Cassini-Huygens

A missão Cassini-Huygens, composta pelas naves Cassini (orbitador) e Huygens (sonda) foi lançada em outubro de 1997 e entrou em órbita de Saturno em julho de 2004. A Huygens pousou na superfície de Titã em dezembro de 2004, após se separar da Cassini (WIKIPEDIA, 2016). A massa total da Cassini-Huygens no lançamento era de aproximadamente 4.637 kg, dividido entre o Orbitador (1.925 kg), a Sonda (312 kg) e o combustível (2.400 kg) (BROWN; DONALDSON, 1994).

Nesta seção é abordada a estratégia de proteção contra falhas da Cassini, com foco na Proteção contra Falhas no Sistema - *System Fault Protection (SFP)* e na proteção contra falhas nos subsistemas Comando e Dados - *Command and*

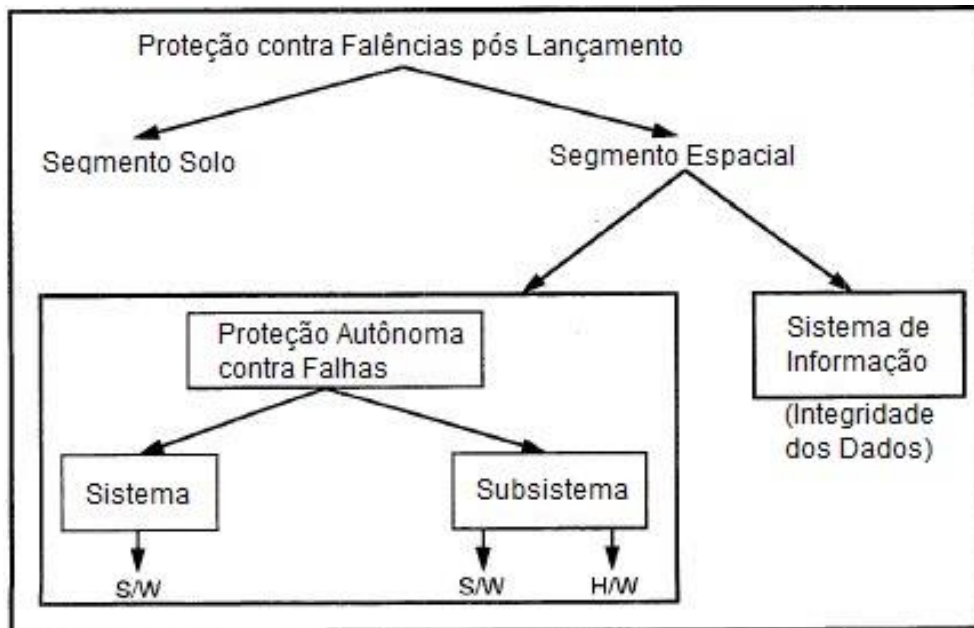
Data Subsystem (CDS) e Controle da Atitude e da Articulação - Attitude and Articulation Control Subsystem (AACCS).

Diferentemente dos casos anteriores (Ørsted e WISE), o requisito primário do SFP da Cassini estabelece que nenhum possível ponto de falência simples deve impedir a missão de atingir seus objetivos ou resultar numa degradação significativa da missão. Embora o requisito primário seja proteger contra falhas simples, a meta do SFP é recuperar o sistema de falhas múltiplas, desde que elas estejam localizadas em regiões de contenção independentes (SLONSKI, 1996).

De acordo com Slonski (1996), a responsabilidade pela recuperação de falhas na Cassini é dividida entre o Segmento Solo e o Segmento Espacial. Quando uma resposta de solo não é viável ou quando essa resposta deve ser fornecida em um período de até duas semanas, a proteção contra falhas é realizada de forma autônoma a bordo. A responsabilidade pela recuperação autônoma de falhas a bordo é dividida entre o SFP e os subsistemas.

O SFP monitora e protege funções nas áreas de telecomunicação, potência, térmica, computador de bordo e propelente. Os subsistemas são, em geral, responsáveis pela recuperação de suas funcionalidades. Quando o subsistema não tem capacidade de realizar a sua recuperação ou a sua recuperação necessitar de ações específicas de outro subsistema o SFP é envolvido. A Figura 2.21 mostra a alocação de responsabilidades concernente à proteção contra falhas na Cassini.

Figura 2.21 – Alocação de responsabilidades para proteção contra falhas na Cassini.



Fonte: Adaptado de Slonski (1996).

O SFP é hospedado no subsistema *Command and Data Subsystem* (CDS). A disponibilidade do SFP é garantida pela proteção contra falhas internas ao CDS que conta com um CDS redundante que pode assumir o papel do CDS primário no caso do mesmo vir a falhar. O SFP está embutido no *software* do CDS e consiste de uma estrutura composta de monitores, respostas e um gerenciador para a coordenação. A ocorrência de uma falência do sistema levará o monitor relacionado à mesma, após avaliação dos dados da falha, a definir a resposta ou as respostas que devem ser executadas (SLONSKI, 1996).

A proteção contra falhas no subsistema CDS – *CDS Fault Protection* (CFP) é baseada nos conceitos de designação e classificação dos erros. Cada erro associado ao CDS recebe uma designação que especifica o serviço ou os serviços providos pelo subsistema que são afetados pelo erro. A classificação especifica a localização e a criticidade do erro. A associação de um erro ao serviço que ele afeta é permanente e função da arquitetura do subsistema. A classificação, i.e. a severidade de um erro, depende da fase da missão (BROWN; DONALDSON, 1994)

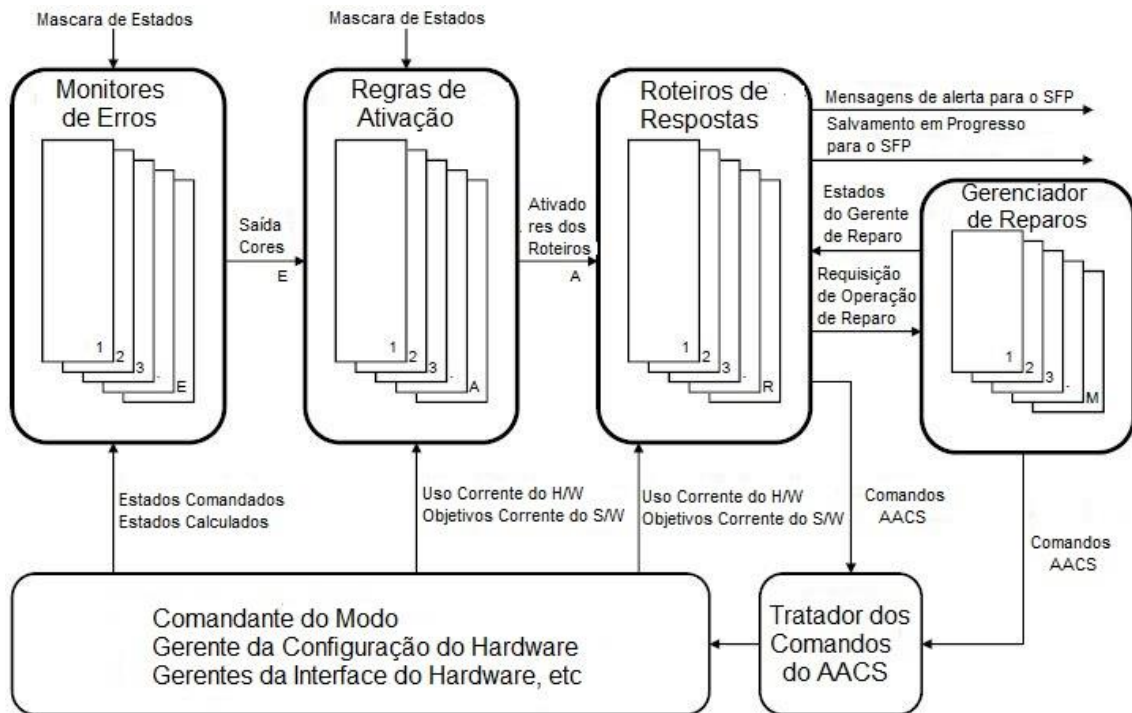
Conforme Brown e Donaldson (1994), o CFP segue a abordagem de monitoramento e resposta. Quando ocorre uma falha o sistema detecta uma violação na sua funcionalidade que resulta na geração de um erro. Estes erros são detectados de forma distribuída pelos componentes *hardware* e *software* do sistema. Dado que os subsistemas são projetados usando decomposição funcional, cada função é relevante para um ou mais dos serviços do CDS. Como o erro é mapeado na designação do serviço que é afetado e o serviço é mapeado na sua criticidade durante uma fase específica da missão, a resposta a um erro será ajustada apropriadamente durante a missão.

A arquitetura da proteção contra falhas no subsistema AACS – *AACS Fault Protection* (AACS FP) é composta por monitores de erro, regras de ativação, roteiros de resposta, gerenciadores de reparo e gerenciadores de redundância (Figura 2.22).

Os monitores de erros detectam desvios do desempenho esperado e sumarizam sua opinião como uma cor. As regras de ativação usam o conhecimento da configuração corrente do *hardware* junto com os objetivos do subsistema para diagnosticar a fonte e a severidade do problema e, a seguir, ativar um ou mais roteiros de resposta. Os roteiros de resposta restauram o subsistema a uma condição segura e funcional por meio de comandos e mensagens de alerta adequados e/ou dirigindo as ações dos gerenciadores de reparo.

Os gerenciadores de reparo aplicam ações corretivas nos componentes físicos individuais e provêm os históricos de reparo para os roteiros de reparo. Os gerenciadores de redundância coordenam e acompanham as mudanças nos conjuntos primários. O AACS FP contém 317 monitores de erro, 310 regras ativação e 221 roteiros de resposta (MEAKIN, 2008).

Figura 2.22 – Diagrama de blocos da arquitetura do AACS FP.



Fonte: Adaptado de Meakin (2008).

De acordo com Meakin (2008), os monitores de erros estão embutidos em três níveis do *software* de voo do AACS. No nível mais baixo, os monitores de erro monitoram os gerenciadores de interface de *hardware*. Os monitores de baixo nível consistem, em geral, de testes simples do *hardware*, são responsáveis pela detecção da maioria das falhas e podem usualmente prover a localização das mesmas.

No nível intermediário, os monitores de erros de estimação e controle monitoram o desempenho dos algoritmos de AACS. Estes monitores não fornecem uma região de falhas restrita como a dos monitores de nível mais baixo, pois podem ser ativados por diversas falhas.

O nível mais alto de monitores de erros são os testes funcionais. Estes monitores mapeiam regiões mais abrangentes, consistem de *time-outs* ou *give-ups* e provêm pouca localização das falhas. Grosso modo, no subsistema AACS existem centenas de monitores de erros de nível baixo, dezenas de monitores de erros de estimação e controle e dez testes funcionais com monitores de erros.

2.8.8.4 Formação de Satélites TerraSAR-X e TanDEM-X

O TerraSAR-X é um satélite alemão de observação da Terra por meio de sensor radar na banda X com massa de 1230 kg lançado em 15 de junho de 2007. O satélite TanDEM-X, gêmeo quase idêntico do TerraSAR-X, foi lançado em 21 de junho de 2010 com massa de 1330 kg. Os satélites podem operar individualmente para geração dos produtos da missão TerraSAR-X ou em conjunto, voando em uma formação controlada com os satélites distando tipicamente menos de 150 m um do outro, para a geração de imagens tridimensionais da Terra (SCHWAB et al., 2012; DLR, 2014a; DLR 2014b). Nesta seção são destacados pontos apresentados em Schwab et al. (2012) considerados relevantes para o desenvolvimento deste trabalho.

O FDIR da missão conjunta TerraSAR-X e TanDEM-X é composto pelos Segmentos Solo e Espacial. No Segmento Espacial, o FDIR é composto pelo FDIR individual dos satélites e pelo FDIR integrado global do Segmento Espacial abrangendo a formação e as interações entre os satélites.

O FDIR individual dos satélites tem por base uma concepção multicamadas, hierárquica e distribuída na qual cada camada realiza sua própria detecção, isolamento e recuperação de falências. Se a recuperação da falência não puder ser realizada na camada em que foi detectada é gerado um relatório do evento e a camada imediatamente superior se encarregará das ações para recuperação.

A Figura 1.3, apresentada na Seção 1, mostra a estrutura hierárquica dos processos aplicativos do satélite TerraSAR X. A modularidade do sistema é obtida pela decomposição funcional do sistema global em processos aplicativos provendo individualmente funções dedicadas, as quais são embutidas em um conjunto comum de serviços operacionais para as funções padrões. Este conjunto de serviços provê comandabilidade e observabilidade para as aplicações individuais assim como para a aplicação específica de FDIR.

De acordo com Schwab et al. (2012), a hierarquia das aplicações mostrada na Figura 1.3 assegura um roteamento eficiente e transparente dos pacotes de telecomandos e telemetrias e o tratamento eficiente de falências no tempo mais curto e no nível mais baixo possível. A aplicação Controle do Sistema (*System Control*), aplicação de nível mais alto a bordo do satélite, é responsável pelo FDIR global assim como pela distribuição de comandos e envio de telemetrias do/para o Segmento Solo (*MOS – Mission Operation Segment*). As aplicações *Bus Controle* AOCS provêm todos os serviços e funções necessários para a plataforma e o satélite como um todo. A aplicação Gerenciamento da Carga Útil (*Payload Manager*) provê funções de suporte, inclusive FDIR, para a Carga Útil, composta por aplicações adicionais distribuídas em diferentes unidades de *hardware*. O FDIR interno de cada aplicação é constituído por um conjunto configurável de serviços com base na ECSS-E-70-41A – *Packet Utilization Standard* (PUS).

O FDIR de cada um dos satélites cobre, além das falências do *hardware* identificadas na FMECA, erros operacionais e funcionais e falências transientes como, por exemplo, as causadas por SEU em memórias ou por EMI durante a transmissão de dados. O FDIR integrado global cobre a operação conjunta da formação a qual, devido à proximidade dos satélites, envolve risco de colisão e risco de iluminação mútua pelo feixe principal das antenas do radar.

2.8.8.5 Formação Autônoma de Satélites

Castel et al (2006) analisam estratégias de FDIR para uma formação autônoma de satélites. No trabalho são consideradas anomalias que afetam a geometria da formação, a missão científica e as comunicações. Três estratégias centralizadas, uma mista e duas distribuídas de FDIR são caracterizadas por meio de simulações baseadas em redes de Petri.

2.8.8.6 Satélites CBERS 3&4

A arquitetura do tratamento de falhas nos satélites da série CBERS é descentralizada e distribuída. A recuperação de falhas da Plataforma é

parcialmente realizada pelo Segmento Espacial cabendo o restante ao Segmento Solo. Já as falhas relativas às Cargas Úteis, são totalmente tratadas pelo Segmento Solo.

O tratamento de falhas sistêmicas da Plataforma coloca o satélite em modo de segurança quando ocorre falência do controle de atitude ou do controle de órbita. O FDIR do subsistema AOCS é responsável por colocar o satélite em um dos dois modos de segurança previstos para a missão. No modo “Global Attitude Acquisition”, a atitude do satélite é controlada pelo computador do subsistema AOCS o qual utiliza todos os sensores e todos os atuadores. No modo “Emergency”, a atitude do satélite é controlada por um módulo de emergência, independente do computador do subsistema, o qual utiliza apenas os “Thrusters” e os “Giros” para manter o satélite seguro.

No nível subsistema, somente falhas dos subsistemas OBDH e AOCS que necessitam de ação imediata para não comprometer a operação dos subsistemas ou a segurança do satélite são tratadas a bordo pelos seus FDIRs. No nível equipamento, as falhas que podem comprometer a operação do equipamento ou a segurança do satélite também são tratadas a bordo.

A Tabela 2.8 apresenta alguns métodos de detecção e recuperação para falências das funções de processamento, comunicação e tempo de bordo do subsistema OBDH. Na tabela são considerados três modos de falência: a) não realiza a função; b) realiza a função intermitentemente; c) realiza a função com erro.

Tabela 2.8 – Detecção de Falências e Recuperação do Subsistema OBDH dos Satélites CBERS

Item	Falências	CBERS	
		Detecção	Recuperação
1	Perda da capacidade de processamento	Em bordo: <i>Watch Dog</i> .	Em bordo: reset, comutação para <i>hardware</i> redundante; Em solo: carregamento de nova versão do <i>software</i> .
2	Processamento intermitente	Abaixo de determinado tempo não será detectado; Acima será detectado e recuperado como no item 1 (Perda da capacidade de processamento).	
3	Erro no processamento;	Em solo: Telemetria.	Em solo: comutação para <i>hardware</i> redundante; carregamento de nova versão do <i>software</i> .
4	Perda de canal de comunicação;	Em solo: Telemetria.	Em solo: comutação para <i>hardware</i> redundante.
5	Canal de comunicação intermitente;	Abaixo de determinado tempo não será detectado; Acima será detectado e recuperado como no item 4 (Perda canal de comunicação).	
6	Erro no canal de comunicação;	Em solo: Telemetria.	Em solo: comutação para <i>hardware</i> redundante
7	Perda da referência de tempo	Em bordo: verificação de consistência do tempo do GPS com relação ao relógio de bordo; Em solo: Telemetria.	Em bordo: interrupção da atualização do relógio de bordo a partir do GPS; Em solo: comutação para GPS redundante.
8	Referência de tempo intermitente	Abaixo de determinado tempo não será detectado; Acima será detectado e recuperado como no item 7 (Perda da referência de tempo).	
9	Erro na referência de tempo	Em bordo: verificação de consistência do tempo do GPS com relação ao relógio de bordo (erro >20ms); Em solo: Telemetria (erro <20ms).	Em bordo: interrupção da atualização do relógio de bordo a partir do GPS; Em solo: comutação para GPS redundante.

Com relação aos demais subsistemas: a) Todos os equipamentos do subsistema Suprimento de Energia possuem redundância interna quente, o que garante que o subsistema é tolerante a falhas simples; b) No caso do subsistema de Telecomunicação de Serviço, a cadeia de telecomandos possui redundância interna “a quente” que garante a sua operação em caso de falha simples.

A Tabela 2.9 sumariza como se dá o tratamento de falhas na Plataforma dos satélites CBERS.

Tabela 2.9 – Sumário do tratamento de falhas da Plataforma nas missões CBERS.

Nível		Segmento	
		Solo	Espacial
Equipamento		X	X
Subsistema	OBDH e AOCS	X	X
	Outros subsistemas	X	
Sistema		X	

Os satélites CBERS 1, 2, e 2B ultrapassaram a vida útil prevista para as missões. No entanto, os satélites apresentaram falhas ao longo do tempo em que estiveram em operação, as quais, em alguns casos, impuseram restrições à sua operação. Todos os satélites permaneceram em operação até a ocorrência de falências que causaram o final das missões. As causas prováveis dessas falências são discriminadas abaixo:

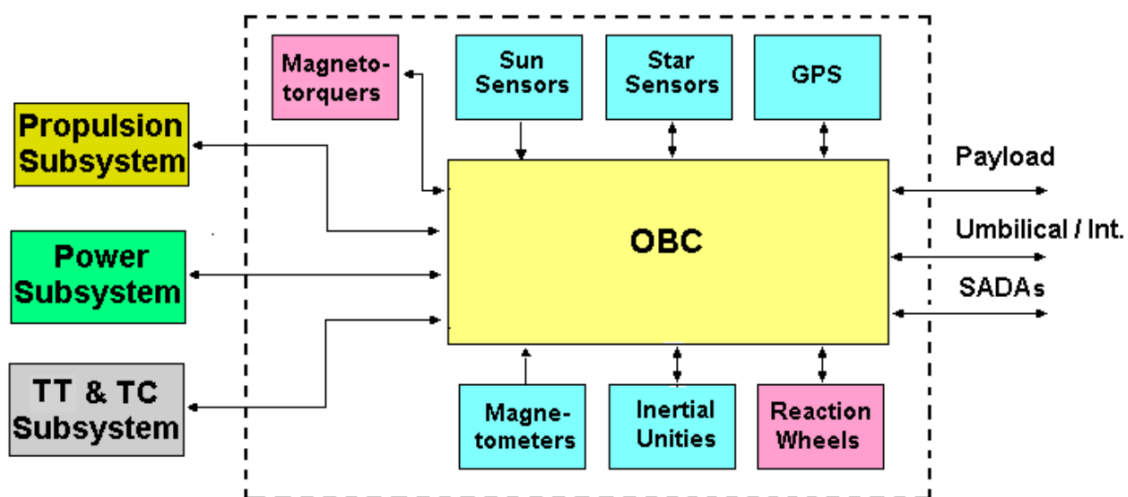
- CBERS 1: Falência do controle da atitude causou a perda do apontamento dos painéis solares que causou falta de energia. Em consequência, os subsistemas OBDH e AOCS e as cargas úteis deixaram de operar;
- CBERS 2: Falência das Baterias causada por provável avalanche térmica;
- CBERS 2B: Falência dos Giros causou a falência do Controle de Atitude que levou ao consumo de todo o seu combustível.

2.8.8.7 PMM e o Satélite Amazonia 1

Embora as futuras missões brasileiras devam ter por base a arquitetura originalmente proposta para a PMM, a qual prevê a integração das funções de AOCS e OBDH em um único subsistema, o subsistema Controle de Atitude e

Tratamento de Dados – ACDH (Figura 2.23), o satélite Amazonia-1 mantém a arquitetura tradicional (Figura 2.6) com um subsistema de Controle de Atitude e Órbita (AOCS) e um subsistema de Tratamento de Dados (OBDH).

Figura 2.23 – Diagrama de blocos do subsistema ACDH e suas principais interfaces com subsistemas da Plataforma e Carga Útil.



Fonte: INPE (2001).

Assim como nos satélites CBERS, o tratamento de falhas das Cargas Úteis do satélite Amazonia 1 é realizado pelo Segmento Solo. O tratamento de falhas da Plataforma é dividido entre o Segmento Solo e o Segmento Espacial.

O FDIR da Plataforma tem uma estrutura hierárquica com mecanismos de tratamento de falhas implantados no nível equipamento, no nível subsistema e no nível sistema. O FDIR do sistema está hospedado no computador do subsistema OBDH.

No nível subsistema, somente as falhas dos subsistemas OBDH, AOCS e PSS (*Power Supply Subsystem*) são tratadas a bordo do satélite. O FDIR do subsistema OBDH é hospedado em seu computador assim como o FDIR do AOCS é hospedado no computador do seu subsistema.

No nível equipamento, as falhas que necessitam de ação imediata para não comprometer a segurança e operação do satélite são tratadas a bordo. No caso do subsistema de Telecomunicação de Serviço, a cadeia relativa a telecomandos possui redundância interna “a quente” que garante a sua

operação em caso de falha simples. A Tabela 2.10 sumariza como se dá o tratamento de falhas na Plataforma do satélite Amazonia 1.

Tabela 2.10 – Sumário do tratamento de falhas da Plataforma no satélite Amazonia 1.

Nível		Segmento	
		Solo	Espacial
Equipamento		X	X
Subsistema	OBDH, AOCS e PSS	X	X
	Outros subsistemas	X	
Sistema		X	X

2.8.9 Sumário das Arquiteturas e Métodos de FDIR Revisitos

A Tabela 2.11 apresenta um sumário das arquiteturas e métodos de FDIR analisados nessa revisão.

Tabela 2.11 – Sumário das arquiteturas e métodos analisados nesta revisão.

Referência	Arquitetura Proposta	Métodos	Análises e Modelamentos	Métricas / Repertório Falhas	Aplicação (Massa, Ano Lançamento)
Bøgh, S. A.;Blanke, M. (1997) Bak, T. et al. (1996)	Arquitetura do subsistema ACS (<i>attitude and control system</i>) com 3 níveis: 1) entrada/saída e <i>loop</i> de controle; 2) algoritmos para detecção e acomodação de falhas; 3) supervisão	Detecção: Verificação da variação e taxa dos sinais dos sensores; Isolação: Filtro de Kalman estendido para o sensor solar; Recuperação: Seleção dos algoritmos de controle, habilitação/desabilitação redundâncias, ativação/desativação do controlador; Supervisão: Regras de inferência.	FMECA		Ørsted (62 kg, 1999)
Castel, C (2006)	Centralizadas (3 estratégias); Mista (1) e Distribuídas (2 estratégias)	Os métodos não são tratados. Cada estratégia é caracterizada pelo conhecimento e algoritmos de Detecção, Isolação, Reconfiguração necessários, onde são implementados e os requisitos de comunicação entre as naves.	Petri net		Simulação das estratégias usando o ambiente de <i>software</i> ProCoSA
Codetta-Raiteri, D.; Portinale, L (2010)		Dynamic Decision Network (DDN). Uma classe de Probabilistic Graphical Models, as DDNs são essencialmente DBNs(Dynamic Bayesian Networks) expandidas com nós de decisão e funções de utilidade.	Modelamento de falhas: EDFT (<i>Extended Dynamic Fault Tree</i>) Modelamento da arquitetura do <i>software</i> : UML		Protótipo do ARPHA avaliado em sistema composto por Leon 3 e RTEMS usando como estudo de caso o cenário e a simulação de um rover para exploração planetária.
Gessner, R. et all (2004)	Hierárquica		IDEF0 (modelamento do FDIR)		Mars Express (1.123 kg, 2003) GOCE (1.077 kg, 2009) ADM-AEOLUS (1.366 kg, 2018)

(continua)

Tabela 2.11 – Continuação.

Referência	Arquitetura Proposta	Métodos	Análises e Modelamentos	Métricas / Repertório Falhas	Aplicação (Massa, Ano Lançamento)
Guiotto, A (2003)		<p>Detecção: Fuzzy Inductive Reasoning</p> <p>Identificação/Isolação: Possibilistic Reasoning</p> <p>Recuperação: State Variable Transition + MADM (Multiple Attribute Decision Making Under Uncertainty)</p>	MATLAB-SIMULINK (modelamento e linguagem de programação)		<p>Simulação</p> <p>Os cenários de validação são os subsistemas Electrical Power Subsystem e Attitude Control Subsystem do satélite GOCE.</p> <p>O protótipo do SMART-FDIR é executado em ambiente com o sistema operacional Windows 2000</p>
Holsti, N.; Paakko, M. (2001) Paakko, M. et all (2001)		<p>Detecção: métodos tradicionais (limit monitoring, correlation tests, trending,, transient filtering, etc.) + Kalman filtering, Weighted Sum-Squared Residual test, Generalized Likelihood Test, Random Sample Consensus</p> <p>Diagnose: Raciocínio probabilístico usando Bayesian Networks e diagnose baseada em modelos usando Causal Networks</p>			<p>Aplicado no satélite hipotético ASOS, "Advanced Smart Observation Satellite", similar a um satélite pequeno de observação da Terra.</p>
Kumar, V. et all (2012)	FDIR (Fault Detection Isolation and Re-configuration) + ESR (Emergency Sun Re-acquisition) Arquitetura do FDIR é hierárquica e multicamadas	Bayesian networks.			ISRO GEO Spacecrafts

(continua)

Tabela 2.11 – Continuação.

Referência	Arquitetura Proposta	Métodos	Análises e Modelamentos	Métricas / Repertório Falhas	Aplicação (Massa, Ano Lançamento)
Muscettola, N. et all (1998)	Arquitetura do sistema integra 3 componentes hierárquicos: 1) sistema de planejamento; 2) sistema executivo; 3) sistema de identificação e reconfiguração	O sistema de identificação e reconfiguração é baseado em modelos analíticos			Deep Space One (373 kg, 1998)
Olive, X. (2012)	Arquitetura do sistema com 3 níveis: 1) decisório; 2) operacional; 3) funcional. FDIR: Hierárquica e distribuída nos subsistemas e equipamentos (níveis 0, 1, 2) e centralizada nos níveis decisório e operacional (níveis 3, 4)				
Rice, E.B.; Lev-Tov, J. (2008)			Nível de missão/plataforma/carga útil: FTA Níveis inferiores: FMECA		WISE (750 kg, 2009)
Schwab, A et all (2012)	Hierárquica, multicamada, distribuída				Formação das naves TSX e TDX. TDX (1230 kg, 2007); TSX (1330 kg, 2010)

(continua)

Tabela 2.11 – Conclusão.

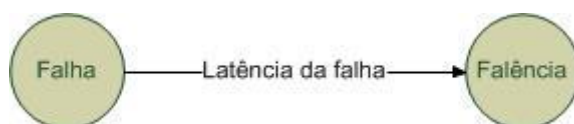
Referência	Arquitetura Proposta	Métodos	Análises e Modelamentos	Métricas / Repertório Falhas	Aplicação (Massa, Ano Lançamento)
Slonski, J. P. (2015) Meakin, P. C. (2008)				Stellar Reference Units (SRUs) CCD temperature (Meakin);	Cassini (1.925 kg, 1997)
Wander, A.; Förstner, R. (2013)	Hierárquica	Cognitive automation			Simulação do Subsistema de potência de nave interplanetária em órbita de Mercúrio
INPE (2001) INPE (2010)	Hierárquica.	Métodos tradicionais (verificação de limites, verificação de consistência, cão de guarda – <i>hardware</i> e <i>software</i> , etc)	FMEA/FMECA		Satélite Amazonia 1 (500kg, 2018)

3 PROPOSTA DE ESTRATÉGIA PARA O TRATAMENTO DE FALHAS

3.1 Conceitos de Falha, Erro e Falência usados neste Trabalho

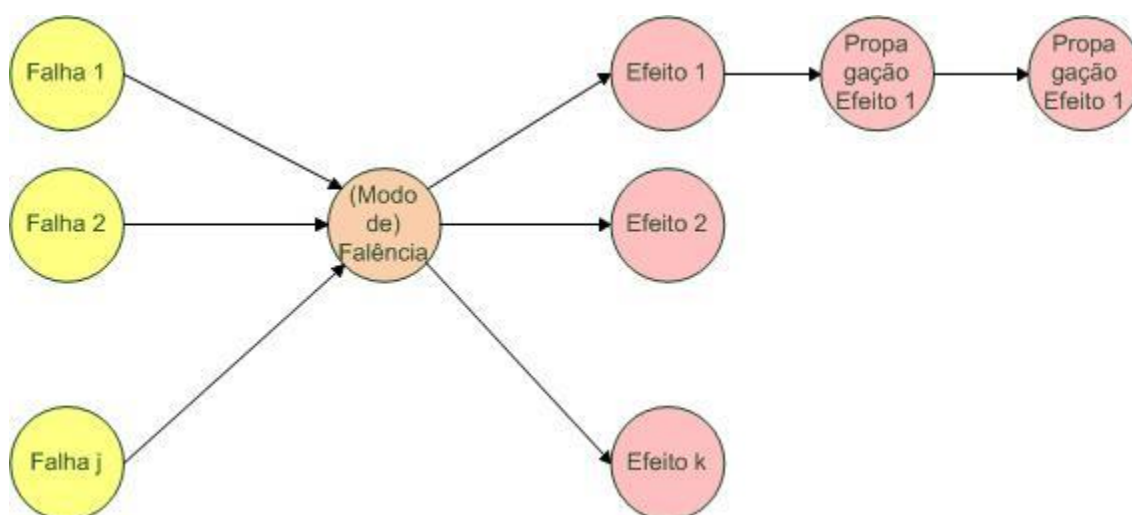
Neste trabalho não é adotado o conceito de erro como elo causal entre falha e falência uma vez que, para a abordagem funcional (Seção 3.3.1) adotada nesta tese para o tratamento de falhas, a sua utilização não se mostrou útil. Neste trabalho, as falhas são consideradas as causas das falências, conforme mostra a Figura 3.1. A latência de uma falha é definida como o intervalo de tempo entre a ocorrência da falha e o aparecimento da falência.

Figura 3.1 – Relação entre falha e falência.



Uma falência ocorre quando o desempenho de uma função não está conforme a especificação. Uma falência pode se manifestar de modos diferentes, os modos de falência. Um modo de falência pode ser causado por mais de uma falha e produzir efeitos (também referidos neste trabalho como discrepâncias), os quais podem se propagar no sistema. A Figura 3.2 resume estes conceitos.

Figura 3.2 – Relação entre falha, falência e efeito.



3.2 Implicações do Tratamento de Falhas Sistêmicas na Fase C da Missão, como atualmente adotado no INPE

No INPE, as atividades relacionadas ao desenvolvimento de satélites podem ser divididas em gerenciamento, engenharia de sistemas, engenharia de subsistemas e engenharia da qualidade, as quais estão estabelecidas em processos (RABELLO, 2017). A Tabela 3.1 apresenta os macroprocessos das atividades de engenharia de sistemas e de engenharia de subsistemas nas fases B e C do ciclo de vida das missões que impactam no tratamento de falhas dos subsistemas OBDH e AOCS.

A Tabela 3.1 mostra que o tratamento das falhas sistêmicas nas missões brasileiras tem, como regra geral, seu início na fase C das missões. Na fase B, a definição da arquitetura do sistema contempla basicamente o atendimento dos requisitos de confiabilidade estabelecidos para a missão em face de possíveis falências de equipamentos.

Os documentos de especificação utilizados nos processos de contratação da aquisição ou do desenvolvimento dos subsistemas e equipamentos da PMM (INPE, 2001) e do ACDH do satélite Amazônia 1 (INPE, 2010), por exemplo, limitam-se, de modo geral, à inclusão da quantidade de unidades redundantes que devem ser fornecidas.

Tabela 3.1 – Macroprocessos que Implementam os Subsistemas OBDH e AOCS.

Macroprocessos para a Implementação dos Subsistemas OBDH e AOCS			
Atividade	Objetivos e Documentos	Fase B	Fase C
Engenharia de Sistemas	Objetivos dos Macroprocessos	<ul style="list-style-type: none"> - Levantar requisitos do OBDH e AOCS; - Alocar confiabilidade para OBDH e AOCS. 	<ul style="list-style-type: none"> - Integração e testes ME dos subsistemas no satélite; - Definir FDIR do sistema.
	Documentos de Entrada dos Macroprocessos	<ul style="list-style-type: none"> - Requisitos da Missão; - Requisitos do satélite; - Concepção da missão e da operação; - Arquitetura do satélite; - <i>Design and Construction Specification</i>; - <i>Environmental Specification</i>; - <i>EMI/EMC Specification</i> 	<ul style="list-style-type: none"> - Requisitos de OBDH e de AOCS; - Lista preliminar de TC e TM; - Interface com o Segmento de Controle; - Interface com o Segmento Aplicação; - Requisitos de teste de OBDH e AOCS.
	Documentos de Saída dos Macroprocessos	<ul style="list-style-type: none"> - Requisitos de OBDH e de AOCS; - Lista preliminar de TC e TM; - Interface com o Segmento de Controle; - Interface com o Segmento Aplicação; - Requisitos de teste de OBDH e AOCS. 	<ul style="list-style-type: none"> - Especificação do FDIR do sistema; - Listas de TC e TM detalhadas e consolidadas; - Relatórios dos testes integrados.
Engenharia de Subsistemas	Objetivos dos Macroprocessos	<ul style="list-style-type: none"> - Especificar os subsistemas e equipamentos, incluindo os seus FDIRs; - Especificar os testes dos subsistemas e equipamentos; - Gerar documentos de fabricação. 	<ul style="list-style-type: none"> - Fabricação dos equipamentos dos subsistemas; - Testes dos equipamentos e dos subsistemas, incluindo seus FDIRs.
	Documentos de Entrada dos Macroprocessos	Requisitos do OBDH e do AOCS	<ul style="list-style-type: none"> - Especificação dos subsistemas e equipamentos (incluindo os seus FDIRs); - Especificação dos testes dos subsistemas e equipamentos; - Documentos de fabricação.
	Documentos de Saída dos Macroprocessos	<ul style="list-style-type: none"> - Especificação dos subsistemas e equipamentos (incluindo os seus FDIRs); - Especificação dos testes dos subsistemas e equipamentos; - Documentos de fabricação. 	<ul style="list-style-type: none"> - Relatórios de fabricação dos equipamentos; - Relatório de testes dos equipamentos.

O tratamento de falhas na fase C impõe restrições na definição de estratégias para missão. Nesta fase, a arquitetura física do satélite já está estabelecida e os subsistemas e equipamentos já foram especificados e, ou estão sendo adquiridos, ou estão em desenvolvimento.

As estratégias propostas nesta fase para o tratamento de falhas sistêmicas têm então, como principal recurso, o uso das réplicas dos equipamentos mais os mecanismos implantados nos equipamentos pelos seus fornecedores e os mecanismos passíveis de serem incluídos no *software* de bordo.

A adição generalizada de redundâncias físicas pode, em função de seu custo, não ser a melhor estratégia ou mesmo não ser uma solução viável para satélites de pequeno e médio porte. Especialmente em missões científicas, o uso desta alternativa pode ser agravado por orçamentos ainda mais limitados, como mostrado na seção 2.8.8.2 deste trabalho, que analisa o satélite WISE.

A adição generalizada de redundâncias não é, no entanto, a única desvantagem desta abordagem. De acordo com Bouricius et al. (1969), a confiabilidade de um sistema é altamente sensível a variações da cobertura do tratamento de falhas onde, a cobertura é definida como a probabilidade do sistema se recuperar dado que ocorreu uma falência, ou seja:

$$c = \text{Pr} [\text{recuperação do sistema} \mid \text{falência do sistema}]$$

De acordo com Bouricius et al. (1969) “*muitas técnicas para o aumento da confiabilidade (como, por exemplo, a adição de mais unidades reservas) são inúteis em vista de uma cobertura inadequada. A adição de mecanismos de diagnóstico, verificação, etc. para melhorar a cobertura das falências é a técnica mais vantajosa*”. A cobertura é, portanto diretamente dependente dos mecanismos de tratamento de falhas, ou seja, detecção, isolamento, identificação e recuperação. A expressão para cobertura pode então ser reescrita como:

$$c = \text{Pr} [\text{detectar a falência, isolar a falha, identificar a falha, recuperar o sistema} \mid \text{falência do sistema}]$$

Do exposto, pode-se concluir que o início do tratamento de falhas sistêmicas na fase C tem as seguintes implicações:

- 1) A quantidade de falhas tratáveis é limitada pela abrangência dos mecanismos e recursos disponíveis nos equipamentos e por aqueles passíveis de serem incluídos no *software* de bordo;
- 2) A cobertura proporcionada pelas estratégias de tratamento adotadas passa a ser função dos mecanismos e recursos para detecção, isolamento, identificação e recuperação disponíveis nos equipamentos ou passíveis de serem incluídos no *software* de bordo;
- 3) As falhas não tratáveis a bordo usando os recursos e mecanismos disponíveis nos equipamentos e por aqueles passíveis de serem incluídos no *software* de bordo devem ser tratadas pelo Segmento Solo;
- 4) O nível de autonomia do tratamento de falhas e, por conseguinte, o nível de autonomia da execução da missão e o nível de autonomia do gerenciamento de dados são limitados pelos mecanismos e recursos disponíveis nos equipamentos e por aqueles passíveis de serem incluídos no *software* de bordo.

3.3 Abordagens para a Definição da Estratégia

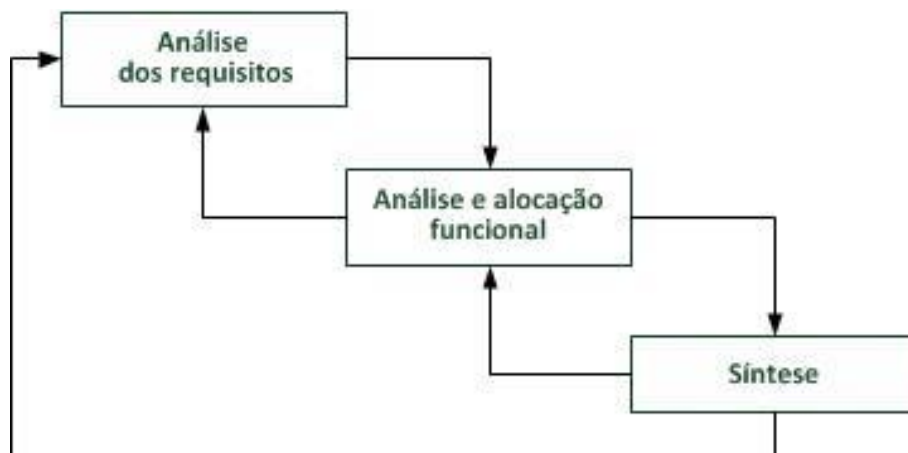
3.3.1 Descrição Funcional da Arquitetura do Subsistema

O processo de engenharia de sistemas inclui (DOD, 2001) a análise de requisitos, a análise funcional/alocação e a síntese do produto, conforme mostrado na Figura 3.3. Na análise funcional/alocação, as funções de nível mais alto, identificadas por meio da análise de requisitos, são decompostas em funções de níveis mais baixos enquanto os requisitos de desempenho associados ao nível superior são alocados às funções de nível mais baixo. Do processo de análise/alocação resulta a arquitetura funcional que descreve o sistema em termos do que ele faz logicamente e em termos de desempenho.

A síntese é o processo de definição do produto em termos de elementos físicos e de *software* que resulta na sua arquitetura física. Cada componente da arquitetura física deve atender ao menos um (ou parte de um) requisito funcional. Em projetos modulares os componentes da arquitetura física realizam uma única função independente, tem pontos únicos de entrada e de saída e são testáveis separadamente. Assim, no caso de um projeto modular, cada módulo da arquitetura funcional é mapeado em um módulo da arquitetura física.

Em áreas de pesquisa relacionadas a tratamento de falhas, a arquitetura do sistema é comumente descrita em termos funcionais e/ou físicos. Misra (1994), por exemplo, em sua tese de doutorado, que trata da diagnose de sistemas dinâmicos com base em sensores, modela hierarquicamente tanto a estrutura física como a estrutura funcional do sistema, associando os modos de falência à estrutura física e os seus efeitos à estrutura funcional.

Figura 3.3 – Processo de engenharia de sistemas.



Fonte: Adaptado de DOD (2001).

Neste trabalho, a antecipação da definição de estratégias para o tratamento de falhas para o final da fase A e/ou início da fase B da missão requer que a definição seja realizada após a conclusão da alocação funcional e, portanto antes da síntese da arquitetura física. Isso implica que o subsistema seja descrito funcionalmente e que a definição de estratégias para o tratamento de

falhas, assim como os modos de falência e seus efeitos, sejam associados às funções.

Durante o processo de síntese da arquitetura física, etapa seguinte do processo de engenharia de sistemas, não incluída no escopo deste trabalho, as estratégias definidas funcionalmente devem ser detalhadas e aplicadas considerando as características dos componentes da arquitetura física.

Neste trabalho, arquiteturas físicas típicas de um subsistema ACDH são usadas como referência para caracterizar sinais e/ou dados associados comumente às funções analisadas e usados na detecção das falências das funções.

3.3.2 Descrição do Comportamento do Sistema por meio de Modelos de Falhas

Para fins de tratamento de falhas, o comportamento do sistema pode ser descrito a partir de modelos nominais, os quais descrevem o comportamento do sistema na ausência de falhas; ou por meio de modelos de falhas, os quais descrevem o comportamento do sistema na presença de falhas (MISRA, 1994). Tais modelos podem usar lógicas de tratamento de dados (aquisição, armazenamento, processamento, decisão, etc.) para extrair informações de falhas conforme a Tabela 3.2:

Tabela 3.2 - Modelos de tratamento de dados de falhas

Modelo	Características
Combinacional	Estático, instantâneo, todas as informações sobre os efeitos está disponível.
Sequencial	Cinemático, não instantâneo, acumula informações sobre as características assíncronas/por eventos dos efeitos.
Temporal	Cinemático, não instantâneo, acumula informações sobre as características síncronas/por tempo dos efeitos.
Informacional	Não instantâneo, acumula informações sobre as características assíncronas/por eventos e características síncronas/por tempo das causas e efeitos de fluxos informacionais.
Dinâmico	Não instantâneo, acumula informações sobre as características assíncronas/por eventos e características síncronas/por tempo das causas e efeitos de fluxos físicos.

Neste trabalho, a descrição do comportamento do sistema na presença de falhas é realizada por meio de modelos de falhas.

A descrição do comportamento **totalmente estático** emprega a FMEA (*Failure Modes and Effects Analysis*) funcional, introduzida na seção 2.7, o diagrama de propagação instantânea correspondente, numa **lógica combinacional**, e origina a Abordagem 1 (Abordagem por Teoria e Análise) da seção 3.3.4.

A descrição do comportamento **prevalentemente cinemático** emprega a FMEA (*Failure Modes and Effects Analysis*) funcional, introduzida na seção 2.7, o diagrama de propagação não instantânea correspondente, numa **lógica sequencial**, e origina a Abordagem 2 (Abordagem por Modelagem e Simulação) da seção 3.3.5.

A descrição do comportamento **prevalentemente temporal** emprega o TFPG (*Timed Failure Propagation Graph*), introduzido na seção 2.8.7.5, o diagrama de propagação não instantânea correspondente, numa **lógica temporal**, e origina a caso da literatura da seção 4.2.

As vantagens da utilização de modelos de falhas e, em especial, do TFPG, para o modelamento do comportamento prevalentemente temporal de sistemas complexos na presença de falhas são discutidas em detalhes em Misra (1994),

Como o comportamento na presença de falhas é analisado apenas para o modo nominal de operação do subsistema, a ênupla que representa o TFPG, expressão (2.1), reduz-se a:

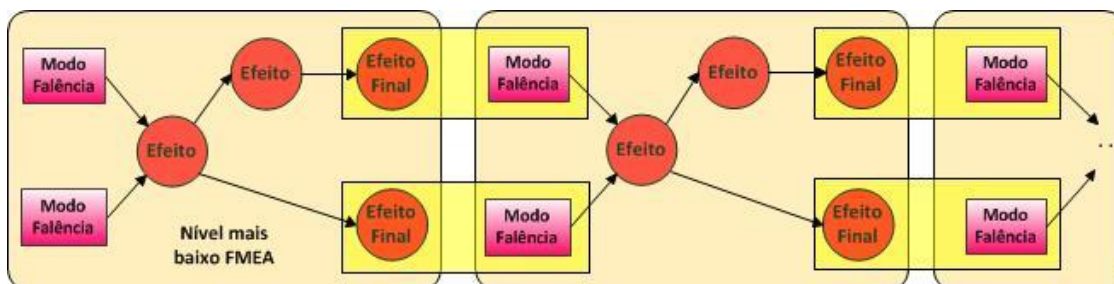
$$G = (F, D, E, ET, DC) \quad (3.1)$$

onde:

- F é um conjunto não vazio de modos de falência;
- D é um conjunto não vazio de discrepâncias;
- $E \subseteq V \times V$ é um conjunto não vazio de setas conectando o conjunto de nós $V = F \cup D$;
- $ET : E \rightarrow I$ é um mapa que associa toda a seta em E com um intervalo de tempo $[tmin, tmax] \in I$ indicando o tempo de propagação mínimo e máximo da seta (onde $I \in \mathbb{R}_{\geq 0} \times (\mathbb{R}_{\geq 0} \cup \{+\infty\})$ e $tmin \leq tmax$);
- $DC : D \rightarrow \{AND, OR\}$ é um mapa definindo o tipo da discrepância;

A descrição do comportamento do sistema é realizada por níveis hierárquicos, integrando FMEA e TFPG em cada nível. A propagação para o nível imediatamente superior segue o fluxo previsto para integração de FMEAs de diferentes níveis hierárquicos, descrito na Seção 2.7, ou seja, o efeito final num dado nível se propaga para o nível imediatamente superior como modo de falência, conforme mostrado na Figura 3.4.

Figura 3.4 – Integração FMEA e TFPG em uma Arquitetura Hierárquica.



Para descrever o comportamento do sistema, inicialmente os modos de falência, os efeitos e as causas identificados na FMEA são associados aos nós de um TFPG. Num segundo momento, os nós são conectados seguindo o fluxo de propagação de cada modo de falência. Em seguida, os tempos estimados de propagação são associados às setas. Por último, os monitores são alocados aos nós.

3.3.3 Tratamento de Falências Funcionais

Na seção 2.7.2 são apresentados os modos potenciais de falência de uma função mencionados na literatura. Neste trabalho são tratados os três seguintes modos de falência:

- Não realizar a função;
- Realizar a função fora de especificação; e
- Realizar a função de forma intermitente.

De modo geral, estes modos de falência podem ser caracterizados como se segue.

3.3.3.1 Modo de Falência ‘Não Realizar a Função’

O modo de falência “não realizar a função” ocorre quando nenhuma das saídas é fornecida de forma aceitável.

3.3.3.2 Modo de Falência ‘Realizar a Função Fora de Especificação’

O modo de falência “realizar a função fora de especificação” ocorre quando uma ou mais saídas da função são fornecidas de forma não aceitável.

As análises realizadas para o modo de falência ‘realizar a função fora de especificação’ pode ser aplicada, sem perda de generalidade, para os modos de falência ‘realizar a função parcialmente’, ‘realizar a função excessivamente’ e ‘realizar a função não intencionalmente’. Estes modos de falência podem de fato ser considerados casos particulares do modo de falência ‘realizar a função fora de especificação’. Para a função ‘fornecer comando direto’, por exemplo, pode-se caracterizar a ocorrência desses modos de falência considerando que: a) a realização parcial da função implica o fornecimento de um pulso de comando com duração e/ou amplitude inferior ao requerido; b) a realização excessiva da função implica o fornecimento de um pulso de comando com duração e/ou amplitude superior ao requerido; e c) a realização não intencional da função implica o fornecimento de um pulso de comando quando não requerido por um dispositivo.

3.3.3.3 Modo de Falência ‘Realizar a Função Intermitentemente’

O modo de falência “realizar a função de forma intermitente” ocorre quando a função não é realizada a intervalos aleatórios de tempo.

De acordo com o dicionário Aurélio, intermitente é o “que apresenta interrupções ou suspensões”. A intermitência pode ser caracterizada pelo intervalo de ocorrência das interrupções e pela duração da interrupção.

Syed et al. (2013) consideram as falhas intermitentes como sintomas da degradação de um sistema. Neste caso, a duração da intermitência aumenta e o intervalo de ocorrência da intermitência diminui à medida que a degradação aumenta, ou seja, as falhas intermitentes tendem a falhas permanentes ao longo do tempo.

Syed et al. (2013) consideram as falhas intermitentes como sintomas da degradação de um sistema. Neste caso, a duração da intermitência aumenta e o intervalo de ocorrência da intermitência diminui à medida que a degradação aumenta, ou seja, as falhas intermitentes tendem a falhas permanentes ao longo do tempo.

Neste trabalho, considera-se que uma mesma falência pode ocorrer tanto de forma permanente como de forma intermitente e que, uma falência quando ocorre de modo intermitente, provoca os mesmos efeitos provocados quando ocorre de modo permanente. Assim, a descrição do comportamento do sistema por meio de FMEA e TFPG não depende do modo de falência ativo.

A identificação do modo de falência ativo só é necessária quando as causas do modo de falência permanente e do modo de falência intermitente estiverem em regiões que podem ser tratadas de forma independente (Figura 3.5). Quando as causas do modo de falência permanente e as causas do modo de falência intermitente não puderem ser tratadas de forma independente (Figura 3.6) a isolamento da falência é suficiente para o tratamento. Assim, tratamos os casos:

- 1) Duração da intermitência é insuficiente para sua propagação (o tempo mínimo de propagação é maior que a duração da intermitência) e a intermitência não se propaga;
- 2) Duração da intermitência é suficiente para sua completa propagação espacial (o tempo máximo de propagação é menor que a duração da intermitência);
- 3) A causa da intermitência está localizada na mesma região que causa uma falência permanente.

Figura 3.5 – Causas dos modos de falência localizadas em regiões que podem ser tratadas de forma independente.

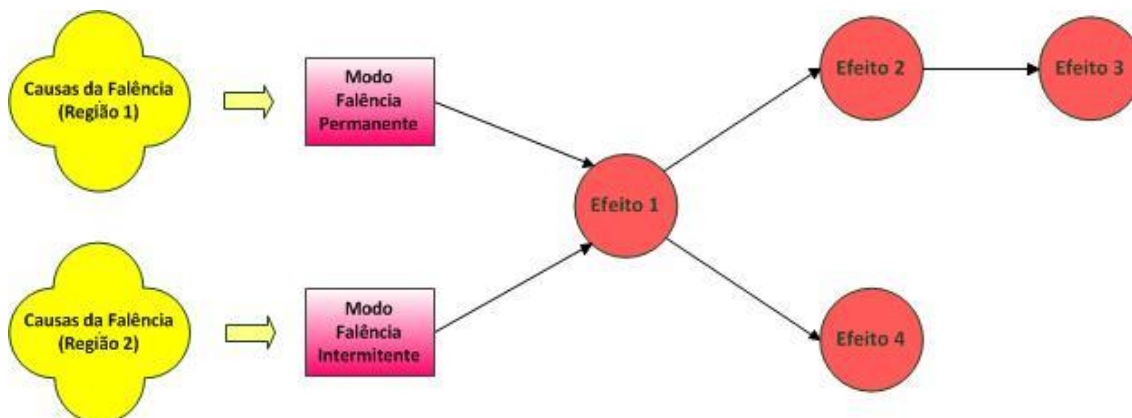
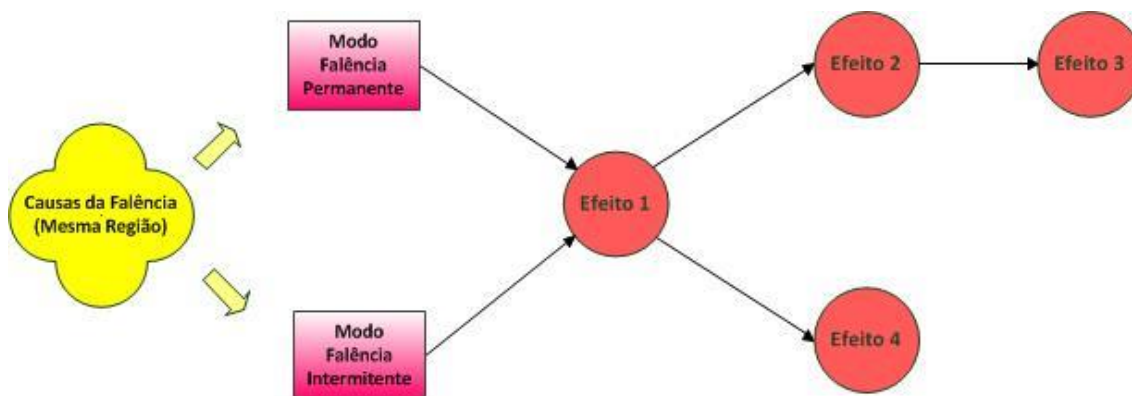


Figura 3.6 – Causas dos modos de falência intermitente e dos modos de falência permanente localizadas na mesma região.



3.3.4 Abordagem por Teoria e Análise para a Diagnose de Falências no Domínio Espacial

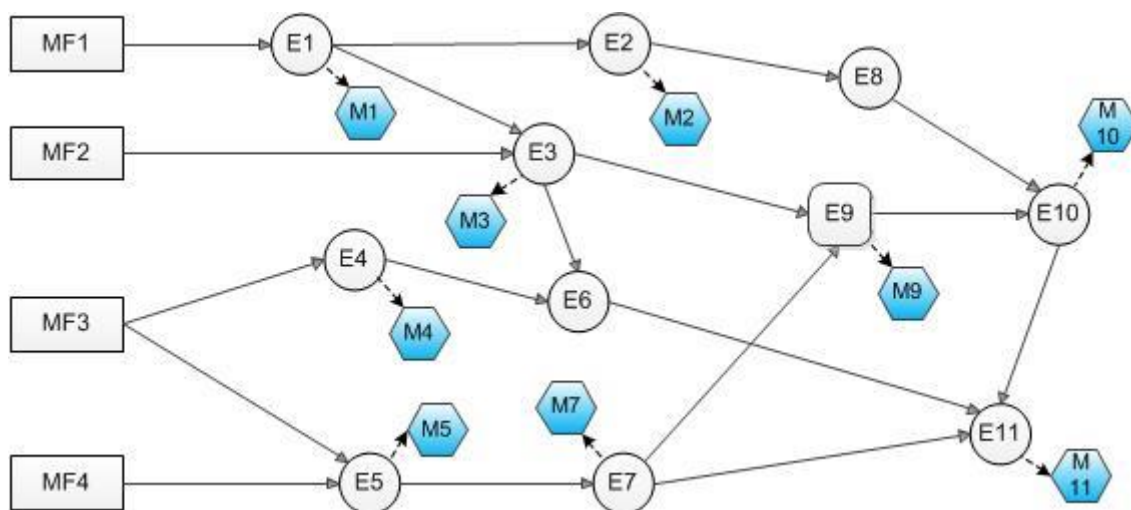
Esta abordagem é prevalentemente combinacional, conforme estabelecido na Tabela 3.2. Nesta abordagem, a isolação e/ou identificação de falências, ou seja, a lógica inversa é realizada por meio de lógicas combinacionais baseadas na assinatura no domínio espacial dos modos de falência. A assinatura no domínio espacial pode ser obtida por meio da modelagem da propagação de cada modo de falência pela estrutura do sistema. As hipóteses estabelecidas na seção 3.3.4.1 serão válidas para esta abordagem.

A propagação de Modos de Falência (*MF*) pelo sistema gera Efeitos (*E*) em diversas regiões de sua estrutura (funcional ou física) que podem ser

monitorados por monitores (M). O conjunto de Efeitos Monitorados (EM) gerados por um MF constitui a manifestação (ou assinatura) **espacial** do MF a qual é representada neste trabalho pelo vetor (\vec{a}). Os monitores fornecem informações sobre o estado de um efeito. Por razões como dificuldades de acesso, de implementação, de prazo e custo, nem sempre o monitoramento do efeito é viável.

O grafo dirigido mostrado na Figura 3.7, cujos nós representam os modos de falência, os efeitos e os monitores, ilustra a propagação dos modos de falência quando se considera apenas o domínio espacial.

Figura 3.7 – Exemplo de propagação de modos de falência pela estrutura do sistema.



Na Figura 3.7, os retângulos representam os modos de falência, os círculos e o quadrado representam os efeitos dos modos de falência e os hexágonos representam os monitores. Os círculos representam nós disjuntivos, i.e. discrepâncias que são ativadas sempre que uma das falências que se propaga até o nó é ativada. Os quadrados representam nós conjuntivos, i.e. discrepâncias que são ativadas somente quando todas as falências que se propagam até o nó são ativadas.

Conforme dito no início da seção 3.3.2 e na Tabela 3.2, a propagação de falências pode igualmente se manifestar em outros domínios: **na sequência de ocorrência de seus efeitos, no tempo, na informação**. Todas essas

manifestações podem ser usadas de forma isolada ou combinada na diagnose, i.e., na isolação e/ou identificação da sua causa.

O tempo de ocorrência, por exemplo, é essencial na diagnose por meio do TFPG. Contudo, o domínio temporal não é o único domínio utilizado. O método se vale ainda dos domínios **espacial** (encadeamento dos efeitos) e **informacional** (indicação da ocorrência ou da ativação de causas e efeitos).

Além da ativação ou ocorrência do efeito, do domínio **informacional** podem ser extraídas informações de dados e de sinais. Vamos explorá-los a seguir.

3.3.4.1 Hipóteses para a Diagnose de Falências no Domínio Espacial

Para a análise da diagnose no domínio espacial, as seguintes hipóteses são estabelecidas:

- Hipótese 1: Quando o efeito de uma falência atinge um determinado nó, o estado desse nó muda de forma permanente (ABDELWAHED; KARSAL, 2006);
- Hipótese 2: Existem m Modos de Falência MF , $1 < m < \infty$, modelados como “0” ou “1”, inacessíveis fisicamente (não são monitoráveis); o modo normal é modelado como “0”; os modos de falência ocorrem com maior probabilidade de forma mutuamente exclusiva (modo simples); os modos de falência ocorrem com probabilidade decrescente em duplas, triplas, . . . enuplas (modo simultâneo);

A atribuição de uma probabilidade de ocorrência aos modos de falência permite limitar o número de modos que são analisados de acordo com um critério de corte.

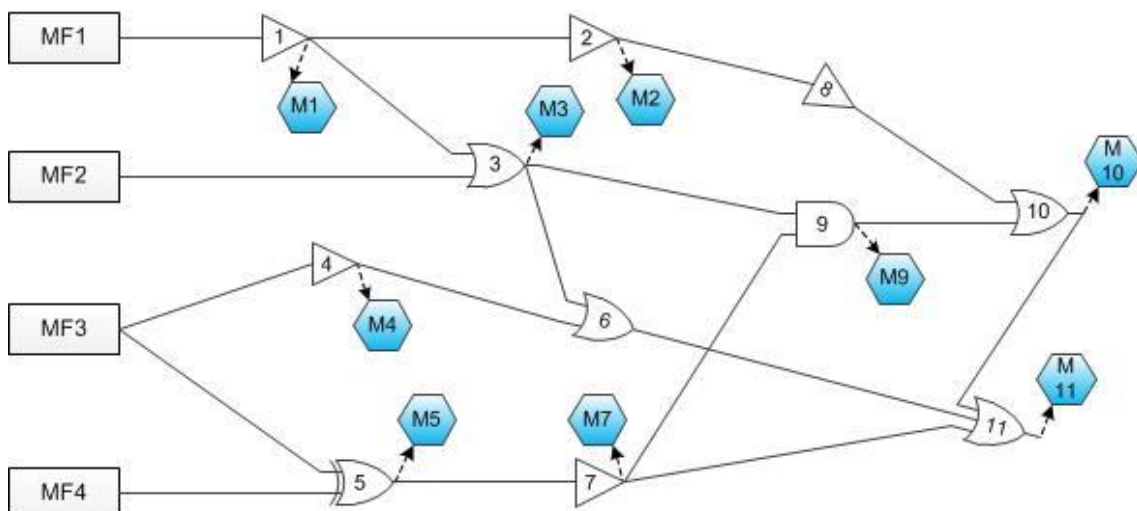
- Hipótese 3: Um MF causa pelo menos um Efeito Monitorado EM ;
- Hipótese 4: Existem k Efeitos E , $1 \leq k < \infty$, modelados como “0” ou “1”;

- Hipótese 5: Existem p Monitores M , $1 \leq p \leq k$, modelados como “0” ou “1”;
- Hipótese 6: $\exists n$ vetores \vec{a} , $1 \leq n < 2^p$, cada qual composto por k EM;
- Hipótese 7: Os MFs se propagam até os Ms por meio de uma rede espacial, combinatória de propagação no intervalo (t_{min} , t_{max});
- Os efeitos são representados por portas lógicas onde, as **portas não inversoras** representam o efeito que tem uma única causa possível. As **portas OU inclusivo** representam o efeito causado por uma ou mais das causas possíveis. As **portas OU exclusivo** representam o efeito causado por uma única das causas possíveis. As **portas E** representam o efeito causado por todas as causas possíveis. A Hipótese 8: O MF_i se propaga no intervalo de tempo (t_{imin} , t_{imax});

Figura 3.8 mostra uma rede combinatória derivada do grafo dirigido mostrado na Figura 3.7 onde nós que representam os efeitos foram substituídos por portas.

- Hipótese 8: O MF_i se propaga no intervalo de tempo (t_{imin} , t_{imax});

Figura 3.8 – Exemplo de propagação de modos de falência por uma rede combinatória.



- Hipótese 9: Os monitores podem apresentar falências ou mesmo, uma cadeia causal completa;
- Hipótese 10: Nas análises realizadas neste trabalho em que são considerados falências de monitores, apenas dois modos de falência são admitidos para os monitores: a) Fornecer um alarme falso positivo; e b) Fornecer um alarme falso negativo. O falso positivo ocorre quando o monitor sinaliza a ocorrência de um efeito que de fato não ocorreu. O falso negativo ocorre quando o monitor não sinaliza a ocorrência de um efeito que de fato ocorreu.

3.3.4.2 Propagação e Diagnose no Domínio Espacial Modeladas como Funções Direta e Inversa

A propagação e a diagnose de falências no domínio espacial podem ser modeladas como funções direta e inversa. Por estes modelos, a assinatura espacial \vec{a}_i do modo de falência MF_i , é expressa pela função direta $f : MF \rightarrow EM$ de acordo com a expressão

$$\vec{a}_i = f(MF_i) \quad (3.2)$$

A aplicação da função direta ao conjunto de modos de falência produz o conjunto de assinaturas espaciais desses modos. A Figura 3.9 apresenta uma representação funcional da propagação dos modos de falência pela estrutura do sistema onde:

Figura 3.9 – Representação funcional da propagação dos modos de falência.



- As entradas MF_1, MF_2, \dots, MF_m representam os m Modos de Falência;

- As saídas $\vec{a}_1, \vec{a}_2, \dots, \vec{a}_n$ representam os n conjuntos de assinaturas gerados pelos m modos de falência;
- A Função Direta f é realizada por um conjunto de funções f_i .

Quando os modos de falência são mutuamente exclusivos (Hipótese 1) o número mínimo de assinaturas para identificar o modo de falência ativo é igual ao número de modos de falência, ou seja,

$$n \geq m \quad (3.3)$$

A remoção da condição de mútua exclusividade da Hipótese 1, ou seja, quando múltiplos modos de falência são admitidos faz com o número mínimo de assinaturas para os modos de falência ativos cresça exponencialmente com o número de MFs, ou seja,

$$n \geq 2^m - 1 \quad (3.4)$$

A **diagnose** (identificação; ou, pelo menos, isolamento) é o **problema inverso** da propagação. A partir da assinatura de uma falência deve ser identificado qual o modo de falência ativo. Dessa forma, a **identificação** do MF_i ativo pode ser expressa por uma **função inversa** $f^{-1} : EM \rightarrow MF$ de acordo com a expressão

$$MF_i = f^{-1}(\vec{a}_i) \quad (3.5)$$

A Figura 3.10 apresenta uma representação funcional da diagnose.

Figura 3.10 – Representação da identificação do modo de falência ativo a partir de sua assinatura.



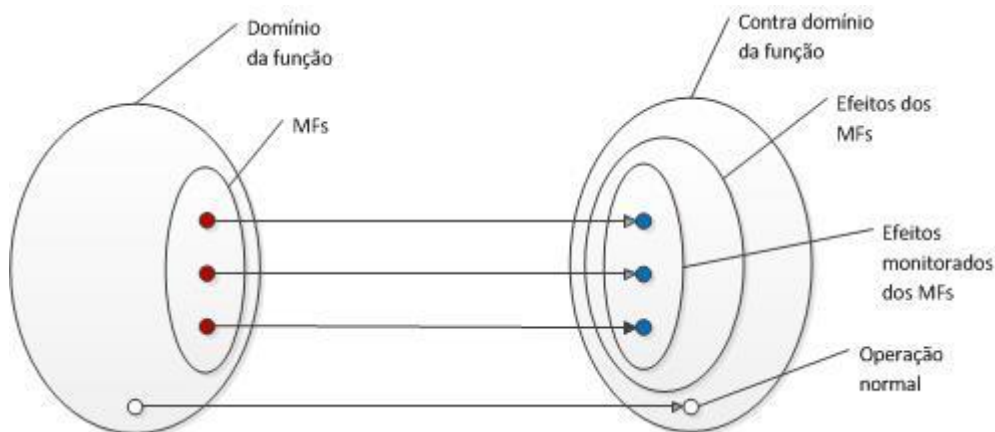
Nem sempre, no entanto, existe uma função inversa. Um exemplo é a situação em que a assinatura apresenta **ambiguidades**. A menos que a assinatura seja desambiguada, não é possível definir-se a função inversa. Só há a **isolação**.

Neste trabalho, conforme as hipóteses 2 e 7 a função direta é expressa por uma lógica digital combinacional direta (“**lógica direta**”); e a função inversa pode ser expressa por uma lógica digital combinacional inversa (“**lógica inversa**”).

A analogia entre a propagação de modos de falência e os tipos de função contribui para uma melhor compreensão do problema da diagnose.

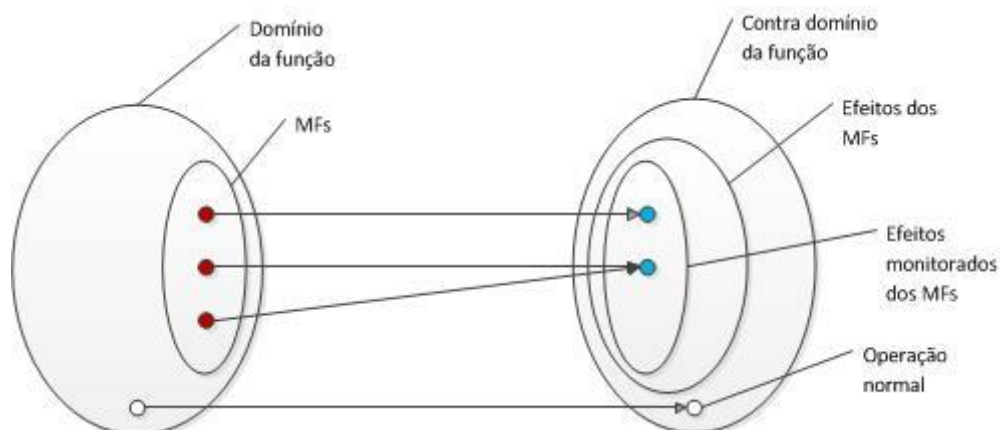
1) Função bijetora $MF \rightarrow EM$: A analogia com uma **função bijetora** (Figura 3.11), por exemplo, ilustra a situação em que sempre é possível definir-se uma função inversa. Nesse caso, a função direta é bijetora e a função inversa sempre existe. Cada modo de falência causa biunivocamente uma assinatura, portanto não existe ambiguidade. Enquadra-se nesta situação a propagação de MF_1 e MF_2 na Figura 3.7. Há a **identificação**.

Figura 3.11 – Analogia entre função bijetora e propagação dos modos de falência.



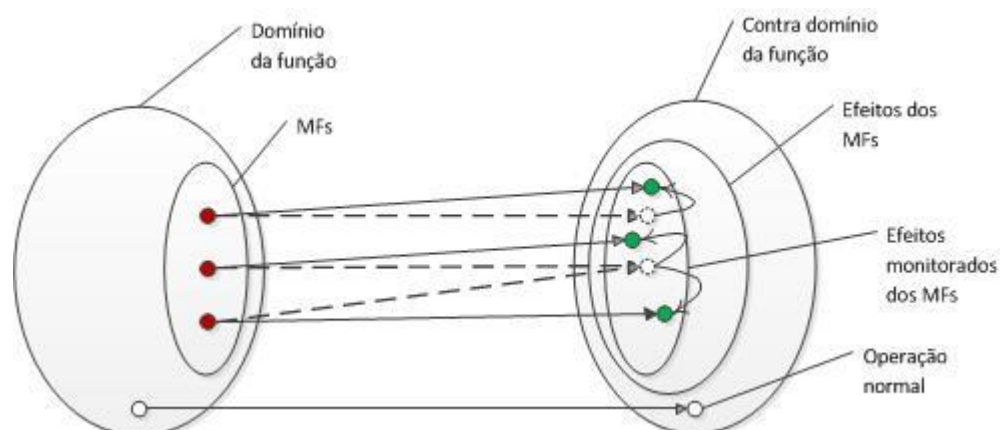
2) Função sobrejetora $MF \rightarrow EM$: A analogia da propagação de modos de falência com uma **função sobrejetora** (Figura 3.12) ilustra uma situação em que não existe função inversa. Nesse caso, existe ambiguidade na assinatura: dois ou mais modos de falência possuem a mesma assinatura. Só há a **isolação**.

Figura 3.12 – Analogia entre função sobrejetora e propagação dos modos de falência caracterizando a ambiguidade de assinaturas.



Para desambiguar é necessário acrescentar ao vetor que representa as assinaturas um ou mais efeitos monitorados de forma que sejam geradas assinaturas distintas para cada um dos modos de falência. A Figura 3.13 mostra o deslocamento das assinaturas originais (setas e assinaturas pontilhadas) para as novas assinaturas. Para que a desambiguação seja possível devem existir efeitos monitoráveis que atendam às condições mencionadas acima, o que nem sempre é viável. Seus casos básicos são: OU exclusivo, OU inclusivo, E. Os demais são combinações lógicas (“álgebra inversa”) destes.

Figura 3.13 – Desambiguação de assinaturas transformando a função sobrejetora em bijetora.



Para tratá-los e generalizá-los por Indução propomos o processo e as noções a seguir:

Processo geral de desambiguação: é a redução ou até a eliminação das ambiguidades, pelos passos: **1)** modelagem da propagação dos modos de falência conforme Hipóteses 1 a 10; **2)** identificação das ambiguidades existentes; **3)** introdução de elementos lógicos (espaciais, temporais, informacionais, etc.) sem ambiguidades ou com ambiguidades distintas das já existentes; **4)** compatibilização dos mapas de Karnaugh da lógica direta; **5)** construção dos mapas de compatibilidade da lógica inversa; **6)** construção dos mapas de Karnaugh da lógica inversa; **7)** otimização destes.

Compatibilidade dos mapas: é a exigência de que os efeitos, mesmo diferentes, mas em condições/posições correspondentes em mapas diferentes, sejam produzidos pelas mesmas causas correspondentes àquelas condições/posições.

A compatibilidade dos mapas reduz ou elimina as ambiguidades presentes em tais mapas pela intersecção delas, aproxima ou permite a inversão da lógica direta. A lógica inversa identifica os modos de falência ativos a partir dos efeitos monitorados. A lógica inversa pode ser expressa por mapas de compatibilidade.

Mapas de compatibilidade expressa os modos de falência ativos a partir dos efeitos monitorados.

Vamos exemplificá-los com seus casos básicos: OU exclusivo, OU inclusivo, E.

2a) Porta OU exclusivo:

Passo 1: Um exemplo simples é a desambiguação da assinatura da porta OU exclusivo produzida por dois modos de falência (MF_1 , MF_2) que produzem de forma mutuamente exclusiva o efeito E monitorado pelo monitor M , conforme mostra a Figura 3.14 (a).

Passo 2: A Figura 3.14 (b) mostra o Mapa de Karnaugh do efeito E , onde é realçada a situação de **dupla ambiguidade** da assinatura.

Figura 3.14 – (a) Efeito monitorado EM causado pela propagação mutuamente exclusiva de MF_1 e MF_2 . (b) Mapa de Karnaugh para o efeito E .

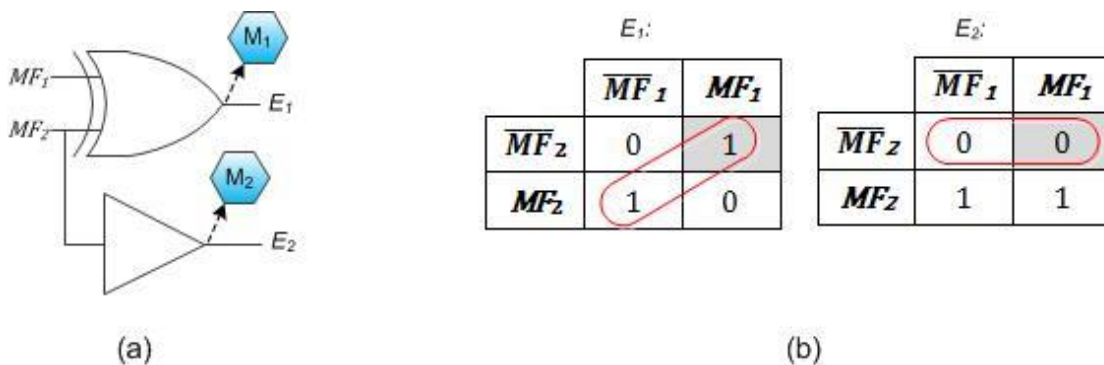


Nesse caso, o vetor \vec{a} é composto somente pelo elemento EM . Assim, a assinatura produzida por MF_1 , $\vec{a}_1 = 1$, é igual à assinatura produzida por MF_2 , $\vec{a}_2 = 1$.

Passo 3: A maneira mais simples de **desambiguar** é acrescentar um efeito monitorado (representado por uma porta não inversora) que seja independente de um dos modos de falência, como mostrado na Figura 3.15 (a).

Passo 4: Na nova configuração espacial, o vetor \vec{a} passa a ser composto por E_1M_1 e por E_2M_2 e a assinatura produzida por MF_1 , $\vec{a}_1 = (1\ 0)$, passa a ser diferente da assinatura produzida por MF_2 , $\vec{a}_2 = (1\ 1)$, eliminando a ambiguidade, como mostrado na Figura 3.15 (b).

Figura 3.15 – (a) Adição do efeito monitorado E_2M_2 independente de MF_1 . (b) Mapa de Karnaugh para os efeitos E_1 e E_2 .



Passo 5: O mapa de compatibilidade da Figura 3.16 (a) é construído a partir da compatibilidade dos mapas da Figura 3.15 (b).

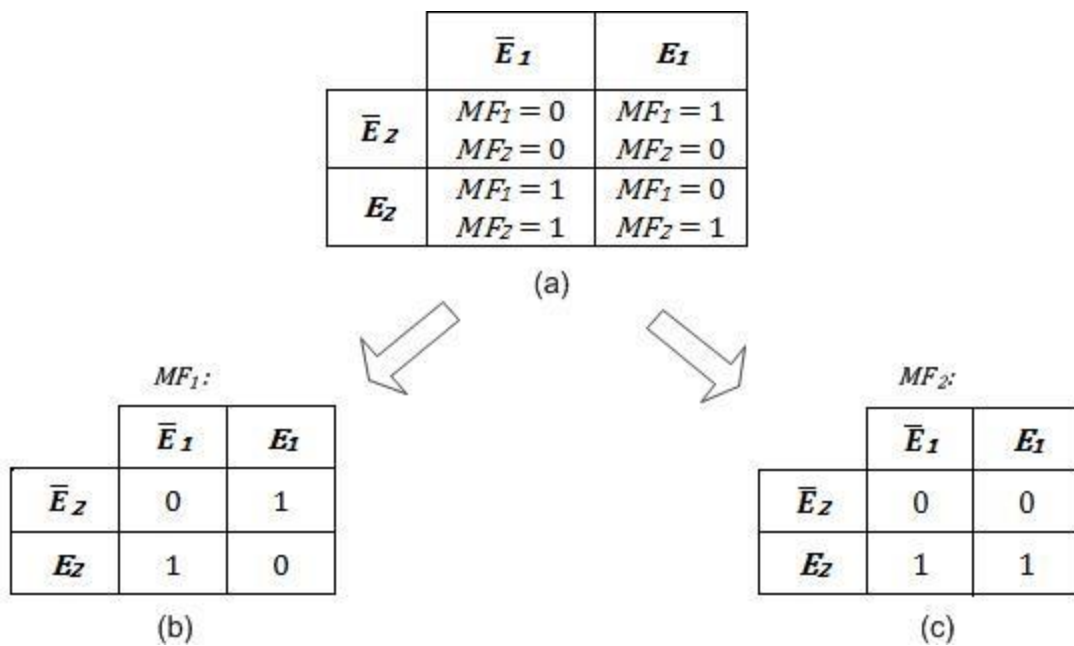
Passo 6: Os mapas de Karnaugh da Figura 3.16 (b) e (c) são construídos a partir do mapa de compatibilidade da Figura 3.16 (a).

Passo 7: As lógicas inversa otimizadas para MF_1 e MF_2 são geradas a partir dos mapas de Karnaugh da Figura 3.16 (b) e (c), conforme mostra as expressões (3.6) e (3.7).

$$MF_1 = E_1\bar{E}_2 + \bar{E}_1E_2 \quad (3.6)$$

$$MF_2 = E_2 \quad (3.7)$$

Figura 3.16 – (a) Mapa de compatibilidade da função OU Exclusivo desambiguada. (b) Mapa de Karnaugh de MF_1 . (c) Mapa de Karnaugh de MF_2 .



2b) Porta OU inclusivo:

Passo 1: Outro exemplo é a desambiguação da assinatura produzida por dois modos de falência (MF_1 , MF_2) que produzem de forma disjuntiva inclusiva o efeito E monitorado pelo monitor M , conforme mostra a Figura 3.17(a).

Passo 2: A Figura 3.17(b) mostra Mapa de Karnaugh do efeito E , onde é realçada a situação de **tripla ambiguidade** da assinatura.

Figura 3.17 – (a) Efeito monitorado EM causado pela propagação inclusiva de MF_1 e MF_2 ; (b) Mapa de Karnaugh para o efeito E .

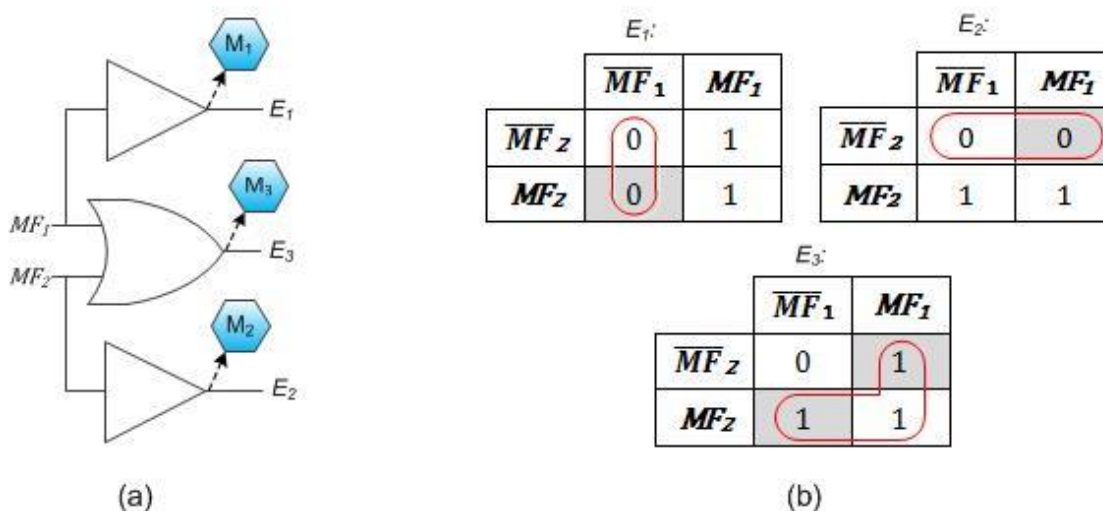


Nesse caso, a assinatura produzida por MF_1 , $\vec{a}_1 = 1$, é igual à assinatura produzida por MF_2 , $\vec{a}_2 = 1$, que é igual à assinatura produzida conjuntamente por MF_1 e MF_2 , $\vec{a}_3 = 1$.

Passo 3: Uma maneira de desambiguar é acrescentar dois efeitos monitorados, um independente de MF_1 e o outro independente de MF_2 , como mostrado na Figura 3.18 (a).

Passo 4: Na nova configuração espacial, o vetor \vec{a} passa a ser composto por E_1M_1 , E_2M_2 e E_3M_3 e a assinatura produzida por MF_1 , $\vec{a}_1 = (1\ 1\ 0)$, a assinatura produzida por MF_2 , $\vec{a}_2 = (0\ 1\ 1)$, e a assinatura produzida conjuntamente por MF_1 e MF_2 , $\vec{a}_3 = (1\ 1\ 1)$, eliminando a ambiguidade, como mostrado na Figura 3.18 (b).

Figura 3.18 – (a) Adição do efeito monitorado E_1M_1 independente de MF_2 , e de E_2M_2 independente de MF_1 ; (b) Mapa de Karnaugh para os efeitos E_1 , E_2 e E_3 .



Passo 5: O mapa de compatibilidade da Figura 3.19 (a) é construído a partir da compatibilidade dos mapas da Figura 3.18 (b).

Passo 6: Os mapas de Karnaugh da Figura 3.19 (b) e (c) são construídos a partir do mapa de compatibilidade da Figura 3.19 (a).

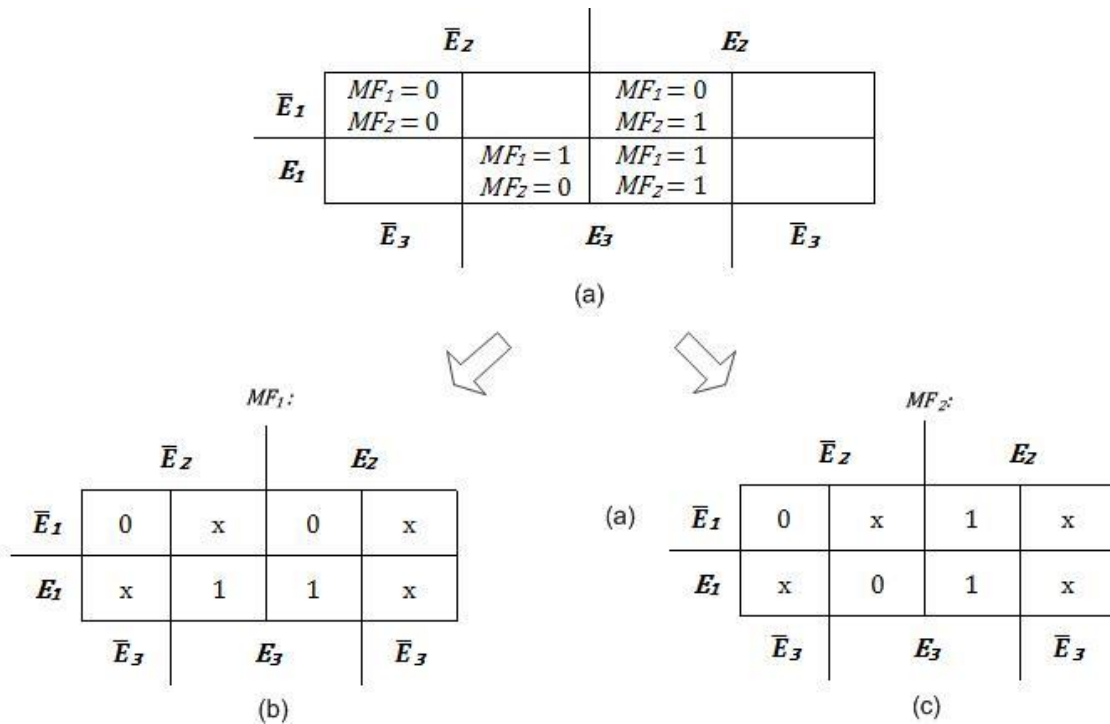
Passo 7: As lógicas inversa otimizadas para MF_1 e MF_2 são geradas a partir dos mapas de Karnaugh da Figura 3.19 (b) e (c), conforme mostra as expressões (3.8) e (3.9).

$$MF_1 = E_1 \quad (3.8)$$

$$MF_2 = E_2 \quad (3.9)$$

O monitor M_3 pode ser dispensado, pois as expressões que definem as lógicas inversas não necessitam do efeito monitorado E_3M_3 para identificar o modo de falência ativo.

Figura 3.19 – (a) Mapa de compatibilidade da função OU inclusivo desambiguada. (b) Mapa de Karnaugh de MF_1 . (c) Mapa de Karnaugh de MF_2 .



2c) Porta E:

Passo 1: Por fim, um terceiro exemplo é a desambiguação da assinatura produzida por dois modos de falência (MF_1, MF_2) que produzem de forma conjuntiva o efeito E monitorado pelo monitor M , conforme mostra a Figura 3.20(a).

Passo 2: A Figura 3.20(b) mostra Mapa de Karnaugh do efeito E , onde é realçada a situação de **tripla ambiguidade** da assinatura.

Figura 3.20 – (a) Efeito monitorado EM causado pela propagação conjuntiva de MF_1 e MF_2 ; (b) Mapa de Karnaugh para o efeito E .

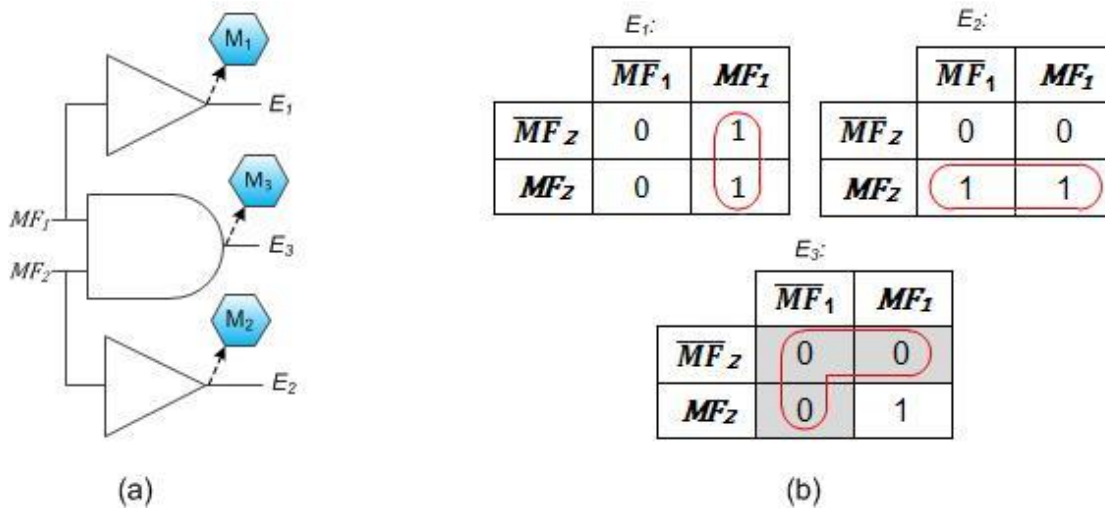


Nesse caso, a assinatura produzida por MF_1 quando MF_2 está inativo, $\vec{a}_1 = 0$, é igual à assinatura produzida por MF_2 quando MF_1 está inativo, $\vec{a}_2 = 0$, que é igual à assinatura produzida conjuntamente por MF_1 e MF_2 , quando ambos estão inativos, $\vec{a}_3 = 0$.

Passo 3: Uma maneira de desambiguar é acrescentar dois efeitos monitorados, um independente de MF_1 e o outro independente de MF_2 , como mostrado na Figura 3.21(a).

Passo 4: Na nova configuração espacial, o vetor \vec{a} passa a ser composto por E_1M_1 , E_2M_2 e E_3M_3 e a assinatura produzida por MF_1 quando MF_2 está inativo, $\vec{a}_1 = (1\ 0\ 0)$, a assinatura produzida por MF_2 quando MF_1 está inativo, $\vec{a}_2 = (0\ 0\ 1)$, e a assinatura produzida conjuntamente por MF_1 e MF_2 , quando ambos estão inativos, $\vec{a}_3 = (0\ 0\ 0)$, eliminando a ambiguidade, como mostrado na Figura 3.21(b).

Figura 3.21 – (a) Adição do efeito monitorado E_1M_1 independente de MF_2 e de E_2M_2 independente de MF_1 ; (b) Mapa de Karnaugh para os efeitos E_1 , E_2 e E_3 .



Passo 5: O mapa de compatibilidade da Figura 3.22 (a) é construído a partir da compatibilidade dos mapas da Figura 3.21 (b).

Passo 6: Os mapas de Karnaugh da Figura 3.22 (b) e (c) são construídos a partir do mapa de compatibilidade da Figura 3.22 (a).

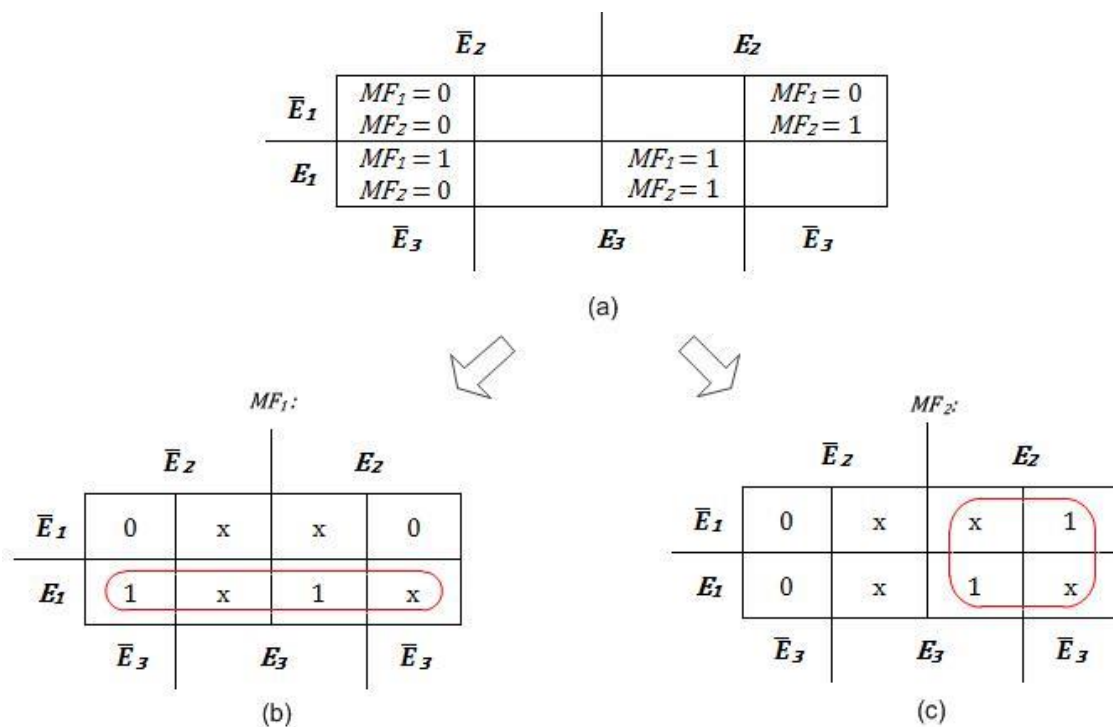
Passo 7: As lógicas inversa otimizadas para MF_1 e MF_2 são geradas a partir dos mapas de Karnaugh da Figura 3.22 (b) e (c), conforme mostra as expressões (3.10) e (3.11).

$$MF_1 = E_1 \quad (3.10)$$

$$MF_2 = E_2 \quad (3.11)$$

O monitor M_3 pode ser dispensado, pois as expressões que definem as lógicas inversas não necessitam do efeito monitorado E_3M_3 para identificar o modo de falência ativo.

Figura 3.22 – (a) Mapa de compatibilidade da função E desambiguada. (b) Mapa de Karnaugh de MF_1 . (c) Mapa de Karnaugh de MF_2 .



A desambiguação no domínio espacial também pode ser realizada combinando a assinatura no domínio espacial com a assinatura em outros domínios como, por exemplo, o domínio temporal.

2d) Portas de múltiplas entradas:

O tratamento das portas OU exclusivo, OU inclusivo e E com múltiplas entradas podem ser simplificado reduzido-se o número de entradas (por exemplo, para duas entradas) empregando-se a propriedade associativa, conforme ilustrado pelas expressões abaixo:

$$MF_1 \oplus MF_2 \oplus \dots \oplus MF_n = MF_1 \oplus (MF_2 \oplus \dots \oplus MF_n); \quad (3.12)$$

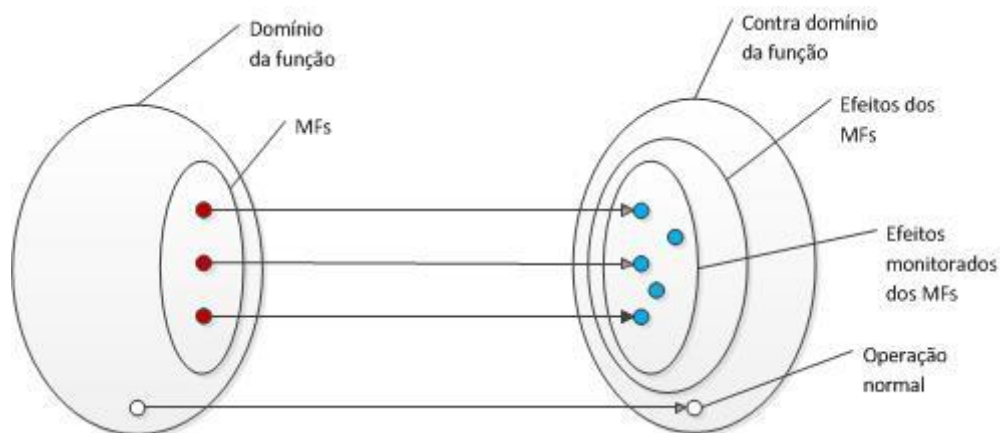
$$MF_1 + MF_2 + \dots + MF_n = MF_1 + (MF_2 + \dots + MF_n); \quad (3.13)$$

$$MF_1.MF_2.\dots.MF_n = MF_1.(MF_2.\dots.MF_n); \quad (3.14)$$

3) Função injetora $MF \rightarrow EM$: A analogia da propagação de modos de falência com uma **função injetora** (Figura 3.23) ilustra outra situação em que não é possível definir uma função inversa, pois existem uma ou mais assinaturas que não são produzidas por nenhum dos modos de falência.

Nessa situação, o processo equivalente a desambiguação é a eliminação de todas as assinaturas que não podem ser causadas pelos modos de falência do contradomínio da função, ou seja, limitar o contradomínio à imagem da função direta.

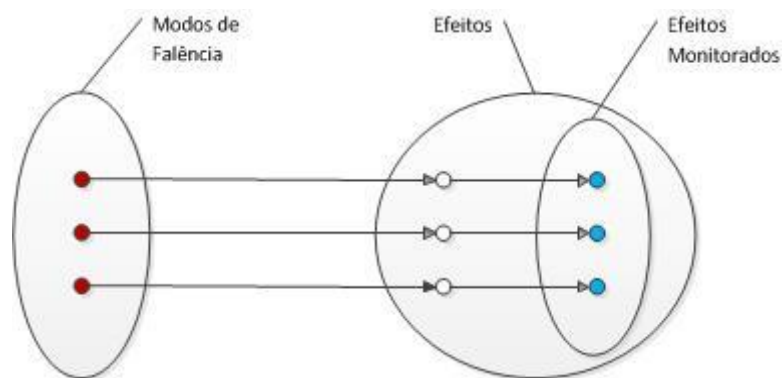
Figura 3.23 – Analogia entre função injetora e a propagação dos modos de falência.



A analogia entre a propagação dos modos de falência e os tipos de função contribui também para uma melhor compreensão dos efeitos provocados pela falência de um monitor.

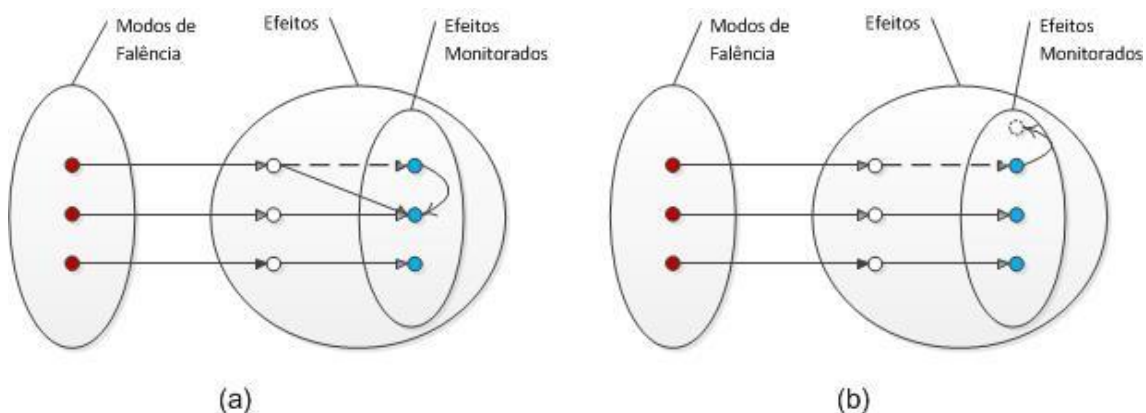
4) Função bijetora $E \rightarrow EM$: O monitoramento de um efeito pode ser expresso por uma **função bijetora** $f : E \rightarrow EM$, conforme mostrado na Figura 3.24. Quando os monitores não apresentam falências, a aplicação da função a um efeito E_i produz biunivocamente um efeito monitorado E_iM_i .

Figura 3.24 – Analogia entre função bijetora e o monitoramento de efeitos quando os monitores não apresentam falências.



A falência do monitor M_i altera o efeito monitorado E_iM_i e, por conseguinte, altera a assinatura \vec{a}_i . Com a alteração, a assinatura resultante pode coincidir com uma assinatura já existente causando uma ambiguidade (conforme mostra a Figura 3.25(a)). A assinatura resultante pode também não fazer parte da imagem da função direta (conforme mostra a Figura 3.25(b)).

Figura 3.25 – Analogia entre função bijetora e o monitoramento de efeitos: (a) quando a falência do monitor causa ambiguidade na assinatura; ou (b) quando a falência do monitor causa assinatura que não faz parte da imagem da função direta.



Teorema 1: Dadas as hipóteses 1 a 6, um *MF* ativo é identificável se existir um conjunto $n = m$ de assinaturas biunivocamente associadas aos m *MFs*.

Corolário: Dadas as hipóteses 1 a 6, um *MF* ativo é identificável se existir um conjunto $n = m$ de *EM* biunivocamente associadas aos m *MFs*.

3.3.5 Abordagem por Modelagem e Simulação para a Diagnose de Falências no Domínio Espacial

Esta abordagem é prevalentemente sequencial, conforme estabelecido na Tabela 3.2. Nesta abordagem, a isolamento e/ou identificação de falências, ou seja, a lógica inversa é realizada por meio de lógicas algorítmicas baseadas na assinatura no domínio espacial dos modos de falência. A assinatura no domínio espacial pode ser obtida por meio da modelagem da propagação de cada modo de falência pela estrutura do sistema. As hipóteses estabelecidas na seção 3.3.4.1 são igualmente válidas para esta abordagem.

A diagnose pode ser realizada quando ocorre um evento, ou seja, quando uma discrepância é detectada. A diagnose pode também ser aplicada de forma temporal (periodicamente ou aleatoriamente) ou ainda por uma combinação de evento e tempo.

Nas seções 3.3.5.1, 3.3.5.2 e 3.3.5.3 são propostas lógicas que, respectivamente, realizam a diagnose por diferença de assinaturas, por biunivocidade e por biunivocidade e verificação de precedência. Embora sejam a princípio, acionadas por eventos, essas lógicas podem ser adaptadas para serem acionadas temporalmente.

Na seção 3.3.5.4 é apresentado um exemplo de lógica que realiza a diagnose nos domínios espacial e temporal.

3.3.5.1 Lógica para Isolação e/ou Identificação por Diferença de Assinaturas

Esta lógica compara a assinatura observada com a assinatura prevista dos modos de falência após a ocorrência de uma discrepância e usa, como critério de decisão, a diferença entre ambos. Isso significa que:

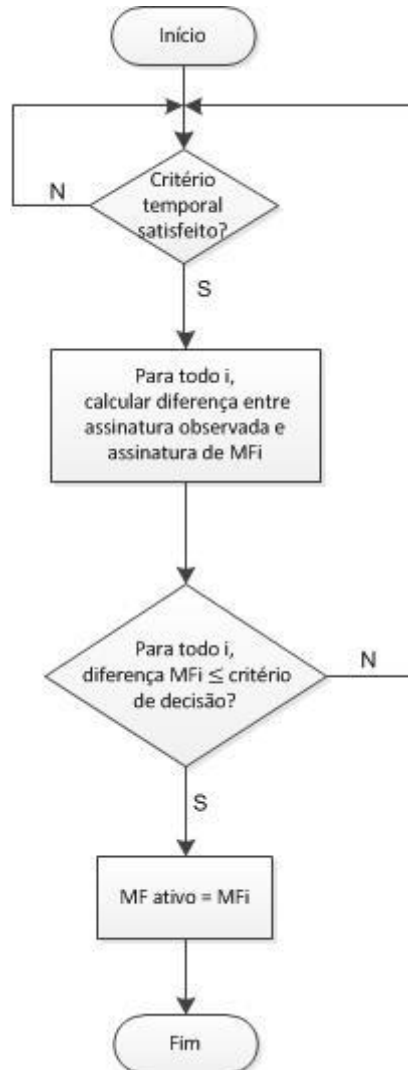
- a) Com diferença tolerável (limiar) igual a zero, para identificar corretamente o modo de falência ativo na ausência de falências de monitores devem ocorrer todas as discrepâncias monitoradas do modo de falência ativo;
- b) Com diferença tolerável (limiar) diferente de zero, o aumento do valor da diferença usada como critério de decisão tem dois efeitos: a) permite antecipar a identificação do modo de falência ativo, na hipótese de ausência de falência de monitores; b) permite identificar o modo de falência ativo na presença de falência de monitores. O incremento do valor aumenta, no entanto, o risco de erro de identificação e de identificação ambígua. Um fluxograma básico dessa lógica é mostrado na Figura 3.26.

Figura 3.26 – Fluxograma básico de lógica acionada por evento para isolamento e/ou identificação por diferença de assinaturas.



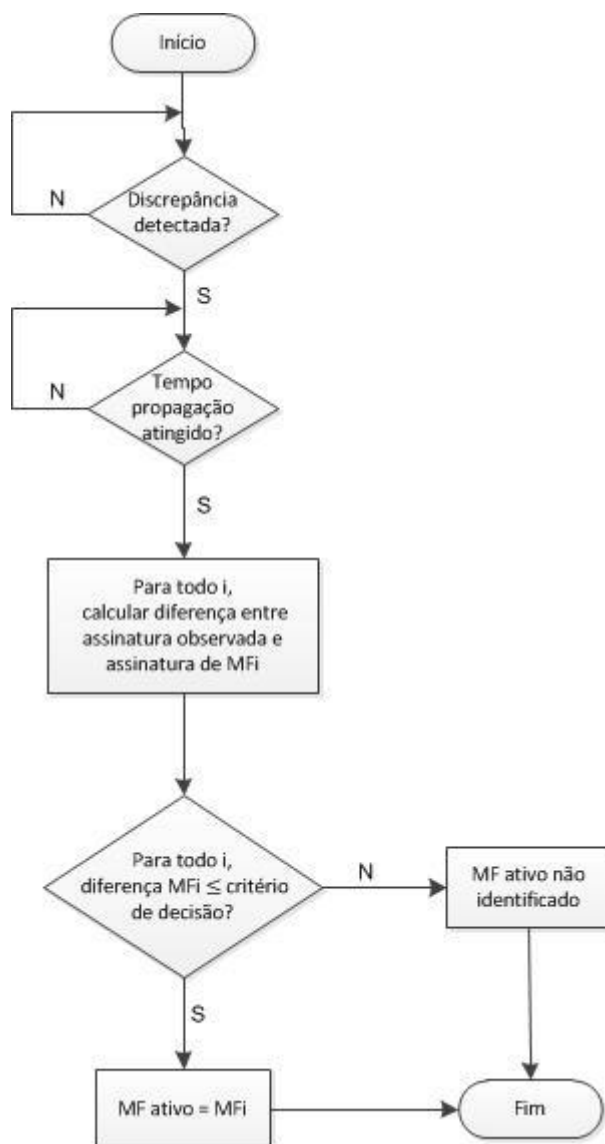
Na Figura 3.26 o acionamento da lógica é realizado por um evento, a detecção de uma discrepância. A Figura 3.27 mostra adaptação dessa lógica para o acionamento temporal. Esta adaptação pode ser igualmente aplicada às lógicas propostas nas seções 3.3.5.2 e 3.3.5.3.

Figura 3.27 – Fluxograma básico de lógica acionada temporalmente para isolamento e/ou identificação por diferença de assinaturas.



Um exemplo de combinação das duas lógicas tratadas nesta seção é a lógica para diagnose após a propagação dos modos de falência, simulada como referência na seção 5. A Figura 3.28 mostra fluxograma básico dessa lógica a qual combina o acionamento por evento e o acionamento temporal para diagnose por diferença de assinaturas.

Figura 3.28 – Fluxograma básico de lógica que combina acionamento por evento e acionamento temporal para isolamento e/ou identificação por diferença de assinaturas após a propagação dos modos de falência.



3.3.5.2 Lógica para Isolamento e/ou Identificação por Biunivocidade

Esta lógica identifica o modo de falência ativo procurando por uma assinatura biunívoca. Para tanto, após a ocorrência de uma discrepância, compara a assinatura observada com a assinatura prevista para os modos de falência e descarta os modos de falência cujas assinaturas não contêm a discrepância. Um fluxograma para realização dessa lógica é mostrado na Figura 3.29.

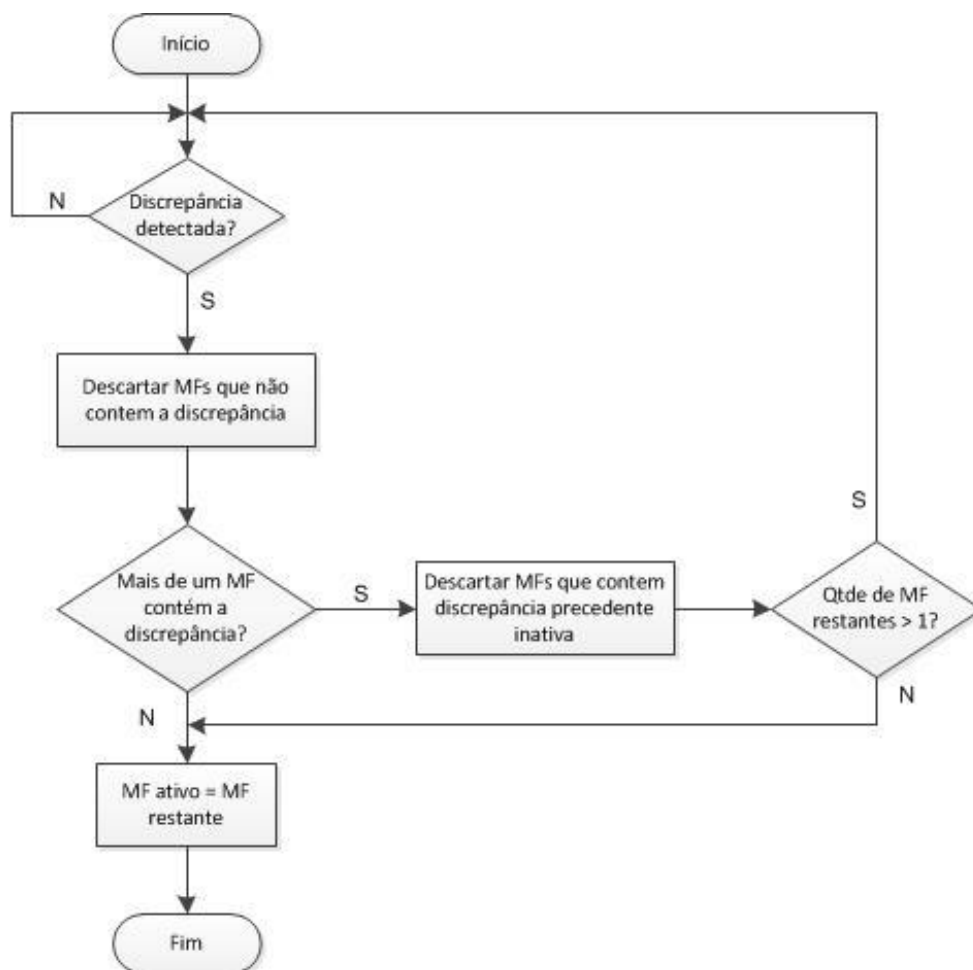
Figura 3.29 – Fluxograma básico para isolamento e/ou identificação com critério de biunivocidade.



3.3.5.3 Lógica para Isolamento e/ou Identificação por Biunivocidade e Verificação de Precedência

Esta lógica agrega um segundo critério à lógica proposta na seção anterior. Como ocorre na seção anterior, após a ocorrência de cada discrepância, a assinatura observada é comparada com a assinatura de cada modo de falência e os modos de falência cujas assinaturas não contêm a discrepância são descartados. Para os modos de falência restantes, as ambiguidades são, tentativamente, resolvidas descartando os modos de falência cujas assinaturas contêm discrepâncias precedentes inativas. Um fluxograma para realização dessa lógica é mostrado na Figura 3.30.

Figura 3.30 – Fluxograma básico para isolamento e/ou identificação com critério de biunivocidade e verificação de precedência.



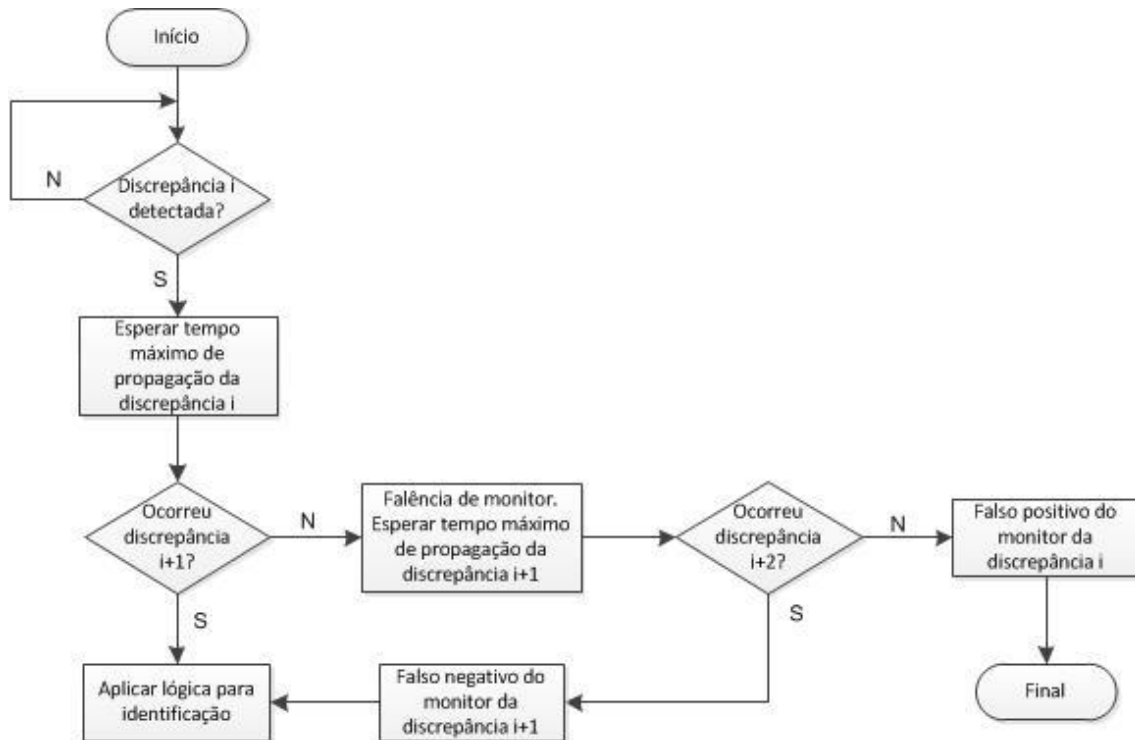
3.3.5.4 Isolação e/ou Identificação nos Domínios Espacial / Temporal

Nesta seção é apresentado um exemplo de lógica que realiza a isolamento/identificação combinando o domínio espacial (representado pela posição relativa das discrepâncias na estrutura do sistema) e o domínio temporal (representado pelo tempo de propagação dos modos de falência na estrutura do sistema).

Basicamente, quando uma discrepância é detectada, a lógica verifica, após o tempo máximo (t_{max}) de propagação previsto para a esta discrepância, se a discrepância sucessora foi ativada. Esta abordagem permite identificar a falência de monitores e pode ser combinada com as lógicas propostas nas

seções anteriores. A Figura 3.31 apresenta um fluxograma básico para isolamento e/ou identificação combinando os domínios espacial e temporal.

Figura 3.31 – Fluxograma básico para isolamento e/ou identificação combinando os domínios espacial e temporal.



3.4 Sumário da Estratégia para o Tratamento de Falhas Sistêmicas

- 1) A arquitetura funcional é definida a partir dos requisitos funcionais do sistema. Um subsistema ACDH típico é o estudo de caso deste trabalho;
- 2) As funções são caracterizadas e decompostas. Os sinais e/ou dados associados a elas numa arquitetura física típica são identificados e caracterizados;
- 3) Os modos de falência funcionais assim como as suas causas (falhas) e os seus efeitos (discrepâncias) são identificados por meio de FMEA funcional;
- 4) O repertório de falhas é constituído;

- 5) O comportamento do sistema na presença de falhas funcionais é descrito por meio de um TFPG (BITTNER et al., 2017);
- 6) As discrepâncias usualmente monitoradas são identificadas;
- 7) As discrepâncias que usualmente não são monitoradas, mas são monitoráveis, são identificadas e selecionadas mediante uma cuidadosa tomada de decisão;
- 8) As assinaturas dos modos de falências nos domínios espacial, temporal e informacional são caracterizadas;
- 9) O cenário de referência compreende: a ocorrência de um único modo de falência, todas as discrepâncias são monitoradas, todos os monitores funcionam corretamente, inexistem ruídos ou incertezas no tempo e na informação;
- 10) Uma lógica combinacional e/ou sequencial e/ou temporal para detecção, isolamento e identificação (FDII) das falências é construída com base nas assinaturas das falências;
- 11) Uma lógica combinacional e/ou sequencial para recuperação do sistema é construída com base nas causas prováveis ou identificadas da falência;

O processo de recuperação pode avaliar o tempo de reação, o impacto na arquitetura funcional e o grau de autonomia proporcionado (TROIANO et al., 2012);

- 12) Adicionalmente, para robustecer esta abordagem pode-se testa-la em cenários que compreendam: i) a ocorrência de um único modo de falência, algumas discrepâncias são monitoradas, todos os sensores funcionam corretamente, a inexistência de ruídos ou de incertezas no tempo e na informação; ii) a ocorrência de um único modo de falência, algumas discrepâncias são monitoradas, um dos sensores não funciona corretamente, a inexistência de ruídos ou de incertezas no tempo e na

informação; iii) a ocorrência de um único modo de falência, algumas discrepâncias são monitoradas, dois dos sensores não funcionam corretamente, a inexistência de ruídos ou de incertezas no tempo e na informação; iv) a ocorrência de mais de um modo de falência, algumas discrepâncias são monitoradas, um dos sensores não funciona corretamente, a inexistência de ruídos ou de incertezas no tempo e na informação;

O teste nesses cenários permite identificar e corrigir falhas na lógica proposta e, dessa forma, aumentar a sua cobertura.

3.5 Avaliação da Originalidade da Proposta

A Tabela 3.3 apresenta os resultados mais relevantes do levantamento bibliográfico e os compara com a proposta do trabalho, situando a originalidade desta proposta em relação à literatura. Basicamente, a estratégia proposta combina uma abordagem funcional e hierárquica com uma descrição estática (FMEA) e prevalentemente temporal (TFPG) do comportamento do sistema para definir lógicas para diagnose com base na compatibilidade de mapas e na assinatura espacial.

Tabela 3.3 – Avaliação da Originalidade da Proposta

Referências	Conceitos	Cadeias Causais	Descrição do Sistema		Arquitetura	
			Funcional	Física	Sistema	FDIR
Avizienis et al. (2004)	Falha; Erro (estado); Falência (evento)	Falha > Erro > Falência				
NASA (2012)	Falha; Falência	Falha > Falência	Enquanto descrição física não disponível			
ECSS (2012)	Falha (estado); Falência (evento)	Falha > Falência	Enquanto descrição física não disponível			Recomenda hierárquica
IFAC (2017)	Falha (estado); Falência (evento)	Falha > Falência				
Misra (1994)	Falência; Discrepância	Falência > Discrepância	Discrepâncias associadas à descrição funcional	Modos de falência associados a descrição física	Hierárquica	
Gessner et al. (2004)				X		Hierárquica
Codetta-Raiteri et al. (2015)	Falha; Falência; Anomalia					
Wander et al. (2012)						
Guiotto et al. (2003)						
Rice et al. (2008)				X		
Ofsthun et al. (2007)	Falência; Discrepância	Falência > Discrepância		X		
Abdelwahed et al. (2009)	Falência; Discrepância	Falência > Discrepância		X		

(continua)

Tabela 3.3 – Continuação

Referências	Conceitos	Cadeias Causais	Descrição do Sistema		Arquitetura	
			Funcional	Física	Sistema	FDIR
Alana et al. (2012)	Síntese de FDIR; Projeto baseado em modelo; Métodos formais					Menciona que a ferramenta suporta estruturas hierárquica, descentralizada ou centralizada
Schwab et al. (2012)		Não menciona falha. Só menciona falência		X	Hierárquica, multicamada;	Hierárquica, multicamada, distribuída
Bittner et al. (2014)	Síntese de FDIR; Projeto baseado em modelo; Métodos formais			X		
Troiano, et al. (2012)	Falência; Discrepância	Falência > Discrepância				
Esta Tese	Falha; Falência; Discrepância	Falha > Falência > Discrepância	X		Hierárquica	Hierárquica

(continua)

Tabela 3.3 – Continuação

Referências	Identificação das Falhas do Repertório	Repertório de Falhas	Assinatura das Falências	Propagação de Falências	Lógica Detecção	Lógica Isolamento e Identificação	Lógica Recuperação
Avizienis et al. (2004)							
NASA (2012)	FMECA, FTA						
ECSS (2012)							
IFAC (2017)							
Misra (1994)						Temporal, espacial (TFPG)	
Gessner et al. (2004)	FMECA						
Codetta-Raiteri et al. (2015)						Temporal, espacial (Redes Bayesianas Dinâmicas)	Temporal, espacial (Redes Bayesianas Dinâmicas)
Wander et al. (2012)	Método visa falhas não identificadas					Informacional (Automação Cognitiva)	
Guiotto et al. (2003)					Informacional (<i>Fuzzy Inductive Reasoning</i>)	Informacional (<i>Possibilistic Reasoning</i>)	Informacional (<i>State Variable Transition e Multi-criteria Decision Making</i>)
Rice et al. (2008)	FMECA, FTA, Experiência	Composto por aproximadamente 600 falhas					
Ofsthun et al. (2007)		Lista as discrepâncias monitoradas		Utiliza TFPG		Temporal, espacial (TFPG)	
Abdelwahed et al. (2009)				Utiliza TFPG		Temporal, espacial (TFPG)	

(continua)

Tabela 3.3 – Conclusão

Referências	Identificação das Falhas do Repertório	Repertório de Falhas	Assinatura das Falências	Propagação de Falências	Lógica Detecção	Lógica Isolação e Identificação	Lógica Recuperação
Alana et al. (2012)	FMEA, FTA						
Schwab et al. (2012)		Menciona algumas falências			Não apresenta lógica; Usa serviços do PUS.	Não apresenta lógica; Usa serviços do PUS.	Não apresenta lógica; Usa serviços do PUS.
Bittner et al. (2014)	FMEA, FTA, HAZARD	Exemplo menciona possíveis falhas e discrepâncias		Utiliza TFPG			
Troiano, et al. (2012)	FMECA, FTA	Exemplo menciona possíveis falhas e discrepâncias		Utiliza TFPG		Temporal, espacial (TFPG)	Temporal, espacial (TFPG)
Esta Tese	FMEA funcional hierárquico	Composto por Falhas funcionais do ACDH	X	TFPG	Informacional e Temporal	Compatibilidade dos mapas e Assinaturas Espacial, (generalizável para temporal e informacional)	

4 APLICAÇÃO DA ESTRATÉGIA A UM ACDH BASEADO NA PMM DO INPE, E A UM CASO DA LITERATURA

4.1 Aplicação da Estratégia a um ACDH baseado na PMM do INPE

A aplicação da estratégia a um ACDH baseado na PMM do INPE é primeiramente realizada utilizando a abordagem por Modelagem e Simulação e, a seguir, a aplicação da estratégia é realizada utilizando a abordagem por Teoria e Análise, portanto, na ordem inversa em que as abordagens são introduzidas na seção 3. A opção por esta sequência decorre da abordagem por Modelagem e Simulação ser aplicada no modelo completo da função e a abordagem por Teoria e Análise ser aplicada em um modelo reduzido da função, o qual é derivado do modelo completo.

4.1.1 Arquitetura Funcional do ACDH

4.1.1.1 Funções do ACDH

Conforme descrito na seção 2.4, o ACDH é resultado da integração dos subsistemas AOCS e OBDH. Assim as funções de um ACDH incluem as funções dos dois subsistemas as quais podem ser resumidas em comandar, tratar os dados de bordo e, controlar a atitude e a órbita do satélite.

Com base nas especificações do ACDH da PMM (INPE, 2001) e nas especificações do ACDH do satélite Amazonia 1 (INPE, 2010) as funções de um ACDH podem ser decompostas em um segundo nível nas seguintes subfunções:

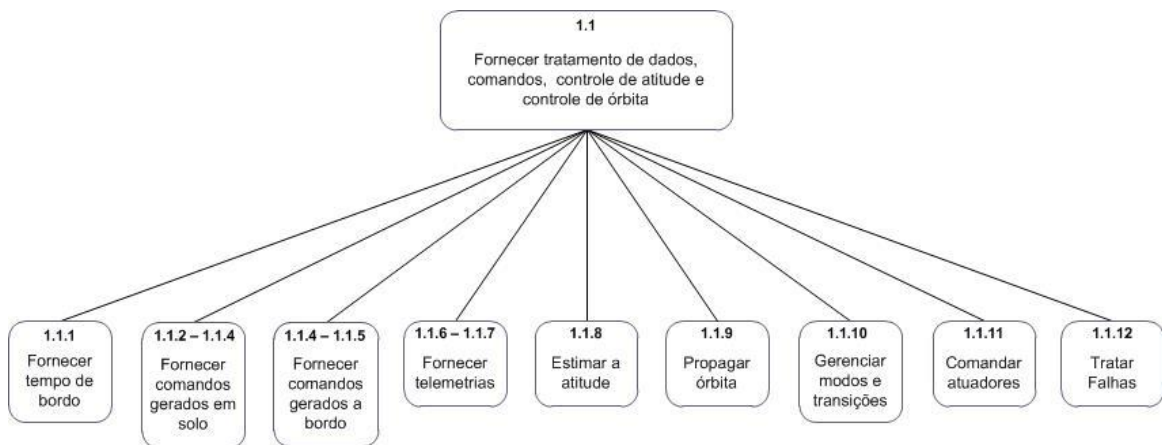
- Fornecer Tempo de Bordo;
- Fornecer Comandos;
- Fornecer Telemetrias;
- Estimar Atitude;
- Propagar Órbita;

- Comandar Atuadores;
- Gerenciar Modos e Transições;
- Tratar Falhas.

Embora não tenha sido explicitada como função nos documentos mencionados acima, o tratamento de falhas sistêmicas está implícito nas especificações do subsistema ACDH, tanto no documento da PMM como no do satélite Amazônia 1. Não é, no entanto, objetivo deste trabalho tratar a subfunção ‘Tratar Falhas Sistêmicas’, de forma a evitar a recorrência representada pelo tratamento de falhas da função ‘Tratar Falhas’.

A Figura 4.1 apresenta os dois primeiros níveis da decomposição funcional do ACDH.

Figura 4.1 – Nível 1 e nível 2 da arquitetura funcional hierárquica do subsistema ACDH.



Embora a decomposição funcional possa ser continuada até atingir o nível mais baixo que se deseje analisar, a decomposição é realizada até o nível 4, pois ao exercitar o modelo de decomposição, verificou-se que os níveis inferiores não são relevantes para este trabalho uma vez que a maior parte das subfunções de nível 3 são decompostas nas subfunções ‘Prover Processamento’ e ‘Prover Comunicação’ no nível 4.

As subfunções 'Prover Processamento' e 'Prover Comunicação' são abstrações com o objetivo de ocultar informações desnecessárias (COLBURN et al., 2007) relativas aos recursos para execução das funções de nível superior, assim como dos recursos para troca de informações entre as próprias funções do ACDH e, entre as funções do ACDH e as funções externas. O processo de síntese da arquitetura física pode produzir subfunções 'Prover Processamento' e 'Prover Comunicação' com características diferentes para cada uma das funções do subsistema.

Neste trabalho, a subfunção 'Prover Processamento' e a subfunção 'Prover Comunicação', assim como outras subfunções localizadas no nível hierárquico mais baixo da decomposição funcional, são consideradas componentes atômicos da arquitetura funcional e não são, portanto, decompostas nem determinadas as causas de suas falências.

Com fins ilustrativos, a FMEA mista (funcional/física) da função 'Prover Processamento' é apresentada na Tabela C1 do Apêndice C.

Dando continuidade à decomposição funcional, a seguir as subfunções de nível 2 das funções 'Fornecer Tempo de Bordo', 'Fornecer Comando Direto' e 'Fornecer Comando Roteado Imediato' são decompostas nos níveis 3 e 4. A decomposição das demais funções é realizada no Apêndice A.

4.1.1.2 Função 'Fornecer Tempo de Bordo'

1) Descrição da função

A função Fornecer Tempo de Bordo gera e distribui o Tempo de Bordo (TB) para os subsistemas da Plataforma e para as Cargas Úteis. O TB é sincronizado periodicamente com uma Referência de Tempo (RT). No intervalo entre as sincronizações, o TB é atualizado localmente pela função 'Fornecer Tempo de Bordo'.

O TB é usado pelas funções do ACDH Fornecer Comando Temporizado, Fornecer Telemetria de Tempo Real, Fornecer Telemetria Armazenada e Propagar Órbita, as quais são descritas nas seções seguintes.

2) Formato do Tempo de Bordo

A codificação do tempo de bordo utilizada neste trabalho segue o formato *CCSDS Unsegmented Time Code (CUC)*, um dos cinco diferentes formatos previstos na norma *Time Code Formats* (CCSD, 2002), o qual é adotado para o satélite Amazonia 1. O formato prevê dois campos e é configurável pelo usuário. Neste trabalho é utilizada a configuração adotada pela PMM na qual:

- Campo T (tempo): 4 octetos para *coarse time* ("segundos"), o que dá um período de aproximadamente 136 anos, e 2 octetos para *fine time* ("subsegundos"), o que dá uma resolução aproximada de 15 μ s;
- Campo P (preâmbulo): Implícito, ou seja, o destinatário do tempo de bordo deve conhecer a priori o formato do tempo.

3) Decomposição Funcional

A função "Fornecer Tempo de Bordo" é decomposta em dois níveis funcionais, os quais são identificados como nível 3 e nível 4 em vista de suas posições na estrutura hierárquica funcional do subsistema.

No nível 3, a função é decomposta nas seguintes subfunções:

- Subfunção Adquirir Referência de Tempo;
- Subfunção Gerar Tempo de Bordo;
- Subfunção Distribuir Tempo de Bordo;

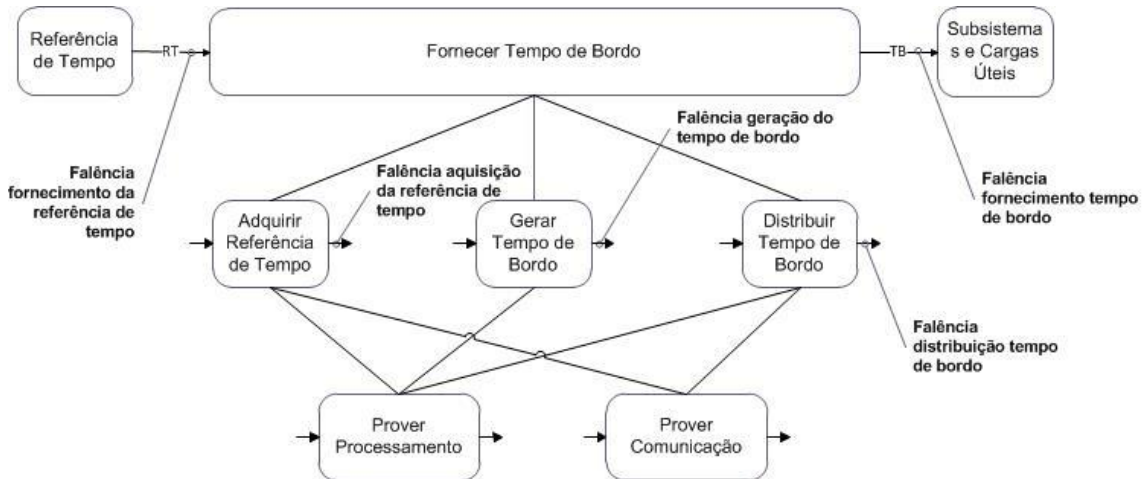
No nível 4, a função é decomposta nas seguintes subfunções:

- Subfunção Prover Processamento;

- Subfunção Prover Comunicação.

A Figura 4.2 apresenta o diagrama da decomposição funcional da função “Fornecer Tempo de Bordo”.

Figura 4.2 - Decomposição funcional da função ‘Fornecer Tempo de Bordo’.



4) Entradas da função

- Referência de Tempo (RT):

A RT pode ser fornecida pelas estações de controle do Segmento Solo ou pode ser fornecida por um GPS localizado no Segmento Espacial. Quando fornecida pelo Segmento Solo, a RT é composta por um dado que representa o horário de referência. Quando fornecida pelo Segmento Espacial, a RT consiste de um dado que define o horário de referência mais um sinal de sincronização com frequência de um segundo o qual periodicamente sincroniza o TB com a RT. Para simplificação da análise, neste trabalho é considerado que a RT é fornecida pelo Segmento Solo.

5) Saídas da função

- Tempo de Bordo (TB):

O TB pode ser fornecido para os subsistemas e cargas úteis de duas formas: a) horário atualizado (dado); b) horário atualizado (dado) mais o sinal de sincronização. Da mesma forma que no item anterior, para simplificação da análise, neste trabalho é tratada a forma descrita no item a.

6) Caracterização dos modos de falência da função 'Fornecer Tempo de Bordo'

Considerando que o tempo de bordo consiste de um dado que representa o horário, os modos de falência da função podem ser caracterizados como:

- O **tempo de bordo não é fornecido** quando o dado que representa o horário fornecido no instante t é igual ao dado fornecido no instante $t-1$;
- O **tempo de bordo é fornecido de forma intermitente** quando o tempo de bordo é fornecido a intervalos aleatórios de tempo;
- O **tempo de bordo é fornecido fora da especificação** quando $TB_i \neq TB_{i-1} + \Delta t$, onde TB_i é o dado que representa o tempo de bordo fornecido no instante t_i , TB_{i-1} é o dado que representa o tempo de bordo fornecido no instante t_{i-1} e Δt é o intervalo de tempo $t_i - t_{i-1}$.

Os modos de falência 'Fornecer Tempo de Bordo Fora da Especificação' 'Fornecer Tempo de Bordo Intermitentemente' não são tratados neste trabalho.

7) Causas dos modos de falência da função 'Fornecer Tempo de Bordo'

A partir da decomposição funcional e da caracterização dos modos de falência, as causas potenciais da falência podem ser determinadas para cada modo de falência e nível hierárquico da função.

No nível 2,

- O tempo de bordo não é fornecido quando:
 - TB não é gerado;

- TB não é distribuído;
- O tempo de bordo é fornecido de forma intermitente quando:
 - TB é gerado a intervalos aleatórios de tempo;
 - TB é distribuído a intervalos aleatórios de tempo;
- O tempo de bordo é fornecido fora da especificação quando:
 - TB é gerado fora da especificação;
 - TB é distribuído fora da especificação;
 - RT não é adquirida;
 - RT é adquirida fora da especificação;

No nível 3,

- O tempo de bordo não é fornecido quando:
 - Processamento não é provido;
 - Comunicação não é provida.
- O tempo de bordo é fornecido de forma intermitente quando:
 - Processamento é provido a intervalos aleatórios de tempo;
 - Comunicação é provida a intervalos aleatórios de tempo.
- O tempo de bordo é fornecido fora da especificação quando:
 - Processamento é provido fora de especificação;
 - Comunicação é provida fora de especificação.

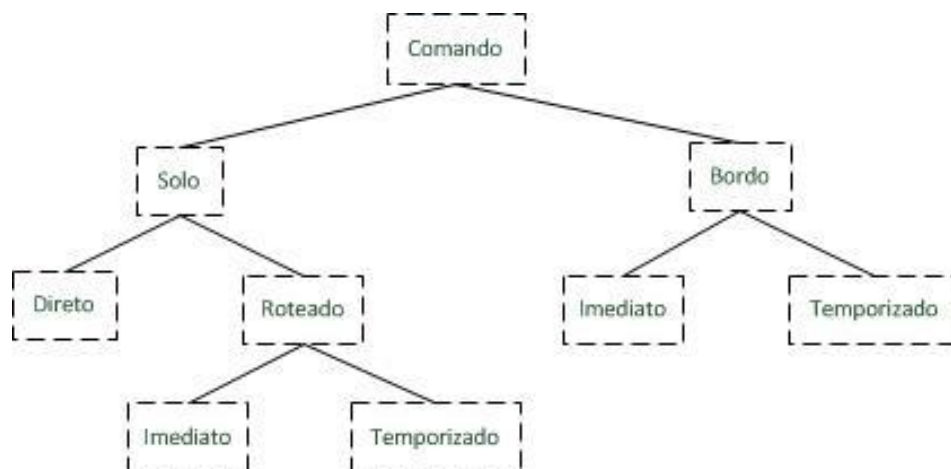
4.1.1.3 Função ‘Fornecer Comandos’

Os comandos fornecidos pelo ACDH podem ser classificados de acordo com a sua origem (Solo ou Bordo), forma de distribuição (Direto ou Roteado) e o tempo de execução (Imediato ou Temporizado), conforme sumarizado na Figura 4.3. Os comandos diretos são telecomandos recebidos de solo e distribuídos de forma imediata em bordo. Os comandos roteados são telecomandos recebidos de solo que passam por processamento em bordo antes de serem distribuídos. Os comandos temporizados são distribuídos de acordo com um agendamento que atende às necessidades de operação do satélite posteriormente ao seu recebimento (quando originados no solo) ou a sua geração (quando originados em bordo).

Os comandos podem ser de dois tipos: discretos ou seriais. Os comandos discretos consistem de pulsos de amplitude e duração fixas. Os comandos seriais consistem de dados (BERGET, 2005).

Neste trabalho, os comandos são tratados de acordo com a classificação apresentada na Figura 4.3, uma vez que os modos de falência podem diferir, conforme a origem, forma de distribuição e tempo de execução do comando.

Figura 4.3 – Classificação de comandos de acordo com sua origem, forma de distribuição e tempo de atuação.



4.1.1.4 Comandos Gerados em Solo

i) Função 'Fornecer Comando Direto'

1) Descrição da função

Os comandos diretos são gerados pelo Segmento Solo e transmitidos para o Segmento Espacial na forma de telecomandos. Os comandos diretos são comandos discretos usados para acionar dispositivos em bordo. A função 'Fornecer Comando Direto' recebe e distribui os comandos gerados em solo, acionando diretamente dispositivos nos subsistemas e cargas úteis do satélite.

2) Decomposição Funcional

A função 'Fornecer Comando Direto' é decomposta em dois níveis funcionais os quais são identificados como nível 3 e nível 4 em vista de suas posições na estrutura hierárquica funcional do subsistema.

No nível 3, a função é decomposta nas seguintes subfunções:

- Subfunção 'Receber Telecomando'

A subfunção 'Receber Telecomando' demodula e decodifica os telecomandos.

- Subfunção 'Distribuir Comando Direto'

A subfunção 'Distribuir Comando Direto' aciona os dispositivos endereçados pelo comando nos subsistemas e cargas úteis.

No nível 4, a subfunção 'Receber Telecomando' é decomposta nas seguintes subfunções:

- Subfunção 'Demodular Telecomando'

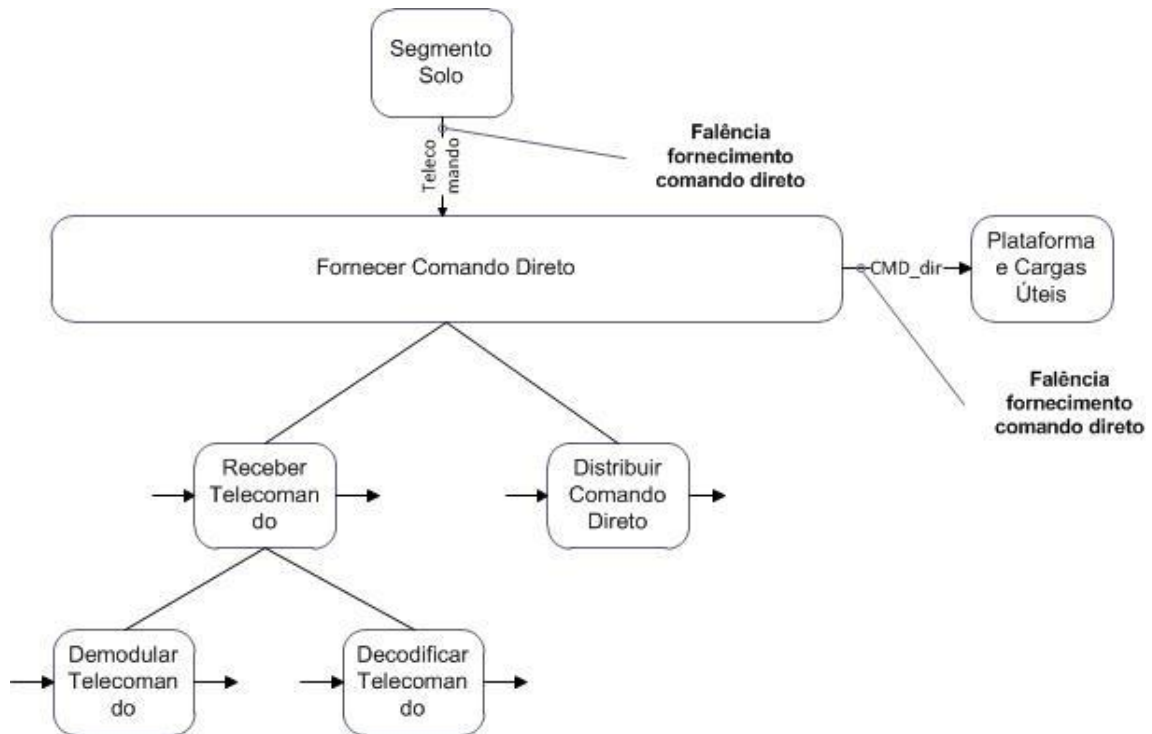
A subfunção 'Demodular Telecomando' demodula os telecomandos extraíndo os quadros de dados.

- Subfunção 'Decodificar Telecomando'

A subfunção 'Decodificar Telecomando' decodifica as informações e identifica os endereços dos dispositivos que devem ser acionados.

A Figura 4.4 apresenta o diagrama da decomposição funcional da função Fornecer Comando Direto.

Figura 4.4 – Decomposição funcional da função ‘Fornecer Comando Direto’.



3) Entradas da função

- Telecomandos fornecidos pelo Segmento Solo;

4) Saídas da função

- Comandos Diretos;

5) Caracterização dos modos de falência da função ‘Fornecer Comando Direto’

- O comando direto não é fornecido quando o pulso de acionamento não é fornecido;
- O comando direto é fornecido de forma intermitente quando o comando direto é fornecido a intervalos aleatórios de tempo;
- O comando direto é fornecido fora de especificação quando o pulso de acionamento não é fornecido de forma aceitável (e.g. aciona dispositivo

não especificado, fornece pulso com amplitude não especificada, fornece pulso com duração não especificada).

6) Causas dos modos de falência da função 'Fornecer Comando Direto'

A partir da decomposição funcional e da caracterização dos modos de falência, as causas potenciais da falência da função podem ser determinadas para cada modo de falência e nível hierárquico da função.

No nível 2,

- O comando direto não é fornecido quando:
 - Telecomando não é recebido;
 - Comando direto não é distribuído;
- O comando direto é fornecido de forma intermitente quando:
 - Telecomando é recebido intermitentemente;
 - Comando direto é distribuído intermitentemente;
- O comando direto é fornecido fora da especificação:
 - Telecomando é recebido fora da especificação;
 - Comando direto é distribuído fora da especificação.

No nível 3,

- O comando direto não é fornecido quando:
 - Telecomando não é demodulado;
 - Telecomando não é decodificado.
- O comando direto é fornecido de forma intermitente quando:
 - Telecomando é demodulado intermitentemente;

- Telecomando é decodificado intermitentemente.
- O comando direto é fornecido fora da especificação:
 - Telecomando é decodificado fora de especificação;

ii) Função 'Fornecer Comando Roteado Imediato'

1) Descrição da função

Os comandos roteados imediatos são gerados pelo Segmento Solo e transmitidos para o Segmento Espacial na forma de telecomandos. Os comandos roteados são comandos seriais. A função 'Fornecer Comando Roteado Imediato' distribui imediatamente os comandos roteados recebidos de solo para os subsistemas e cargas úteis do satélite.

2) Decomposição Funcional

A função 'Fornecer Comando Roteado Imediato' é decomposta em dois níveis funcionais os quais são identificados como nível 3 e nível 4 em vista de suas posições na estrutura hierárquica funcional do subsistema.

No nível 3, a função é decomposta nas seguintes subfunções:

- Subfunção 'Receber Telecomando';

A subfunção 'Receber Telecomando' demodula e decodifica os telecomandos.

- Subfunção 'Distribuir Comando Roteado Imediato';

A subfunção 'Distribuir Comando Roteado Imediato' aciona os dispositivos endereçados pelo comando nos subsistemas e cargas úteis.

No nível 4, a função é decomposta nas seguintes subfunções:

- Subfunção 'Demodular Telecomando'

A subfunção 'Demodular Telecomando' demodula os telecomandos extraindo quadros de dados.

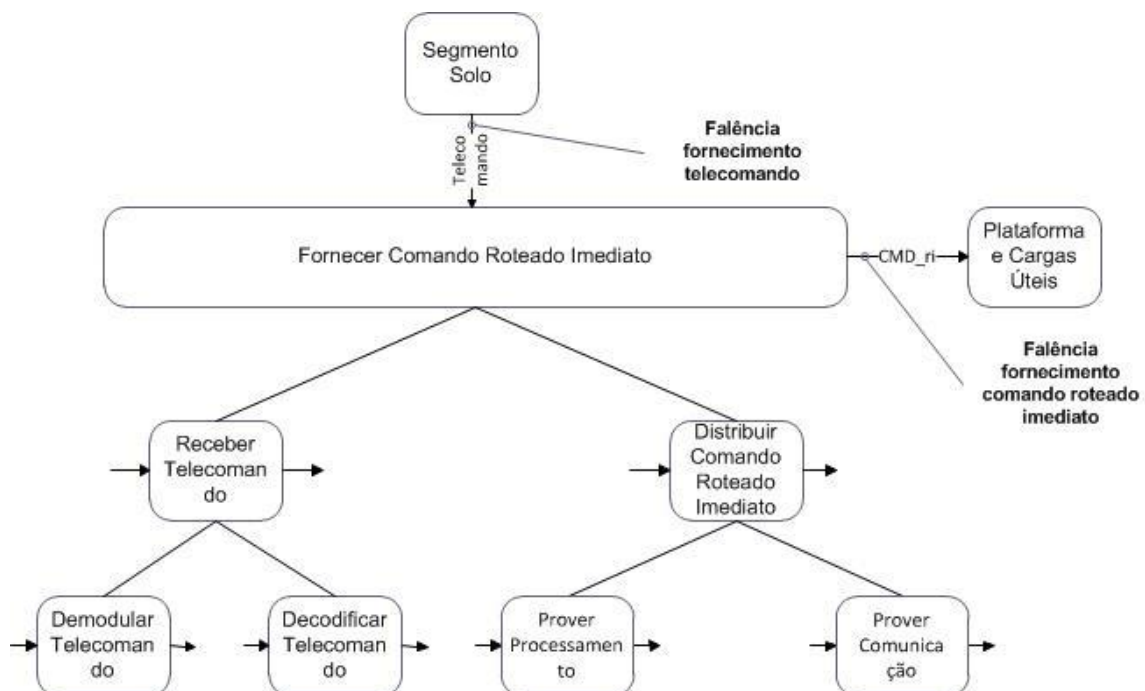
- Subfunção 'Decodificar Telecomando'

A subfunção 'Decodificar Telecomando' decodifica os telecomandos e identifica os endereços dos dispositivos que devem ser acionados.

- Subfunção 'Prover Processamento';
- Subfunção 'Prover Comunicação';

A Figura 4.5 apresenta o diagrama da decomposição funcional da função Fornecer Comandos Roteados Imediatos.

Figura 4.5 – Decomposição funcional da função Fornecer Comando Roteado Imediato.



3) Entradas da função

- Telecomandos fornecidos pelo Segmento Solo;

4) Saídas da função

- Comandos Roteados Imediatos;
- 5) Caracterização dos modos de falência da função 'Fornecer Comando Roteado Imediato'
- O comando roteado imediato não é fornecido quando os dados do comando não são fornecidos;
 - O comando roteado imediato é fornecido de forma intermitente quando os dados do comando são fornecidos a intervalos aleatórios de tempo;
 - O comando roteado imediato é fornecido fora da especificação quando os dados do comando não são fornecidos conforme o especificado.
- 6) Causas dos modos de falência da função 'Fornecer Comando Roteado Imediato'

A partir da decomposição funcional e da caracterização dos modos de falência, as causas potenciais da falência da função podem ser determinadas para cada modo de falência e nível hierárquico da função.

No nível 2,

- O comando roteado imediato não é fornecido quando:
 - Telecomando não é recebido;
 - Comando roteado imediato não é distribuído;
- O comando roteado imediato é fornecido de forma intermitente quando:
 - Telecomando é fornecido a intervalos aleatórios de tempo;
 - Comando roteado imediato é distribuído a intervalos aleatórios de tempo;
- O comando roteado imediato é fornecido fora da especificação:

- Telecomando é recebido fora da especificação;
- Comando roteado imediato é distribuído fora da especificação;

No nível 3,

- O comando roteado imediato não é fornecido quando:
 - Telecomando não é demodulado;
 - Telecomando não é decodificado.
- O comando roteado imediato é fornecido de forma intermitente quando:
 - Telecomando é demodulado a intervalos aleatórios de tempo;
 - Telecomando é decodificado a intervalos aleatórios de tempo.
- O comando roteado imediato é fornecido fora da especificação:
 - Telecomando é decodificado fora de especificação;

4.1.1.5 Consolidação da Arquitetura Funcional do ACDH

A Figura 4.6 agrupa as funções decompostas de um ACDH destacando os componentes comuns à maior parte das funções: as subfunções Prover Processamento e Prover Comunicação. A Figura 4.7 apresenta a arquitetura funcional hierárquica do subsistema ACDH consolidada. Na Figura 4.7, as subfunções Prover Processamento e Prover Comunicação, comuns à maior parte das funções, são consolidadas.

Figura 4.6 – Decomposição das funções do subsistema ACDH.

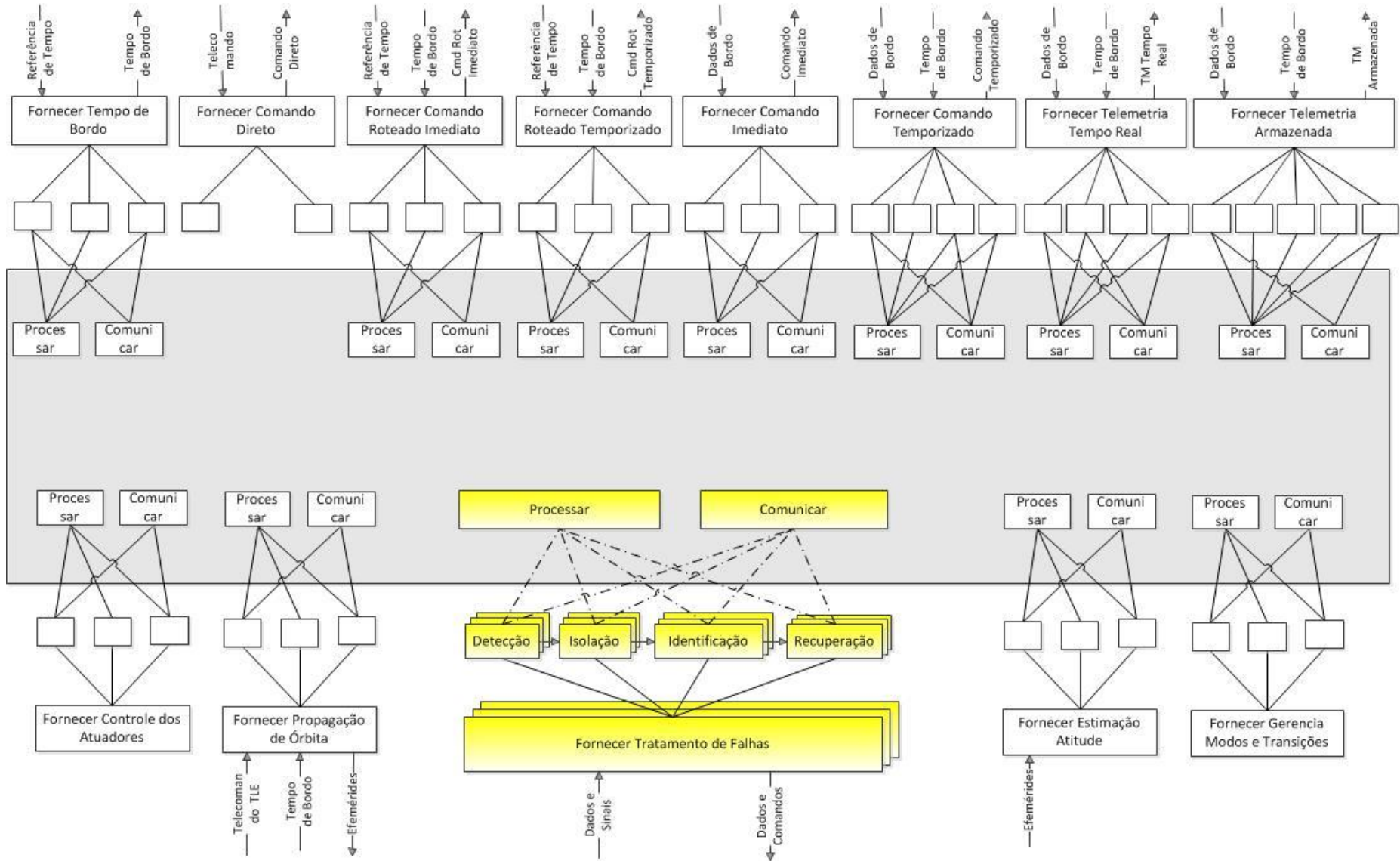
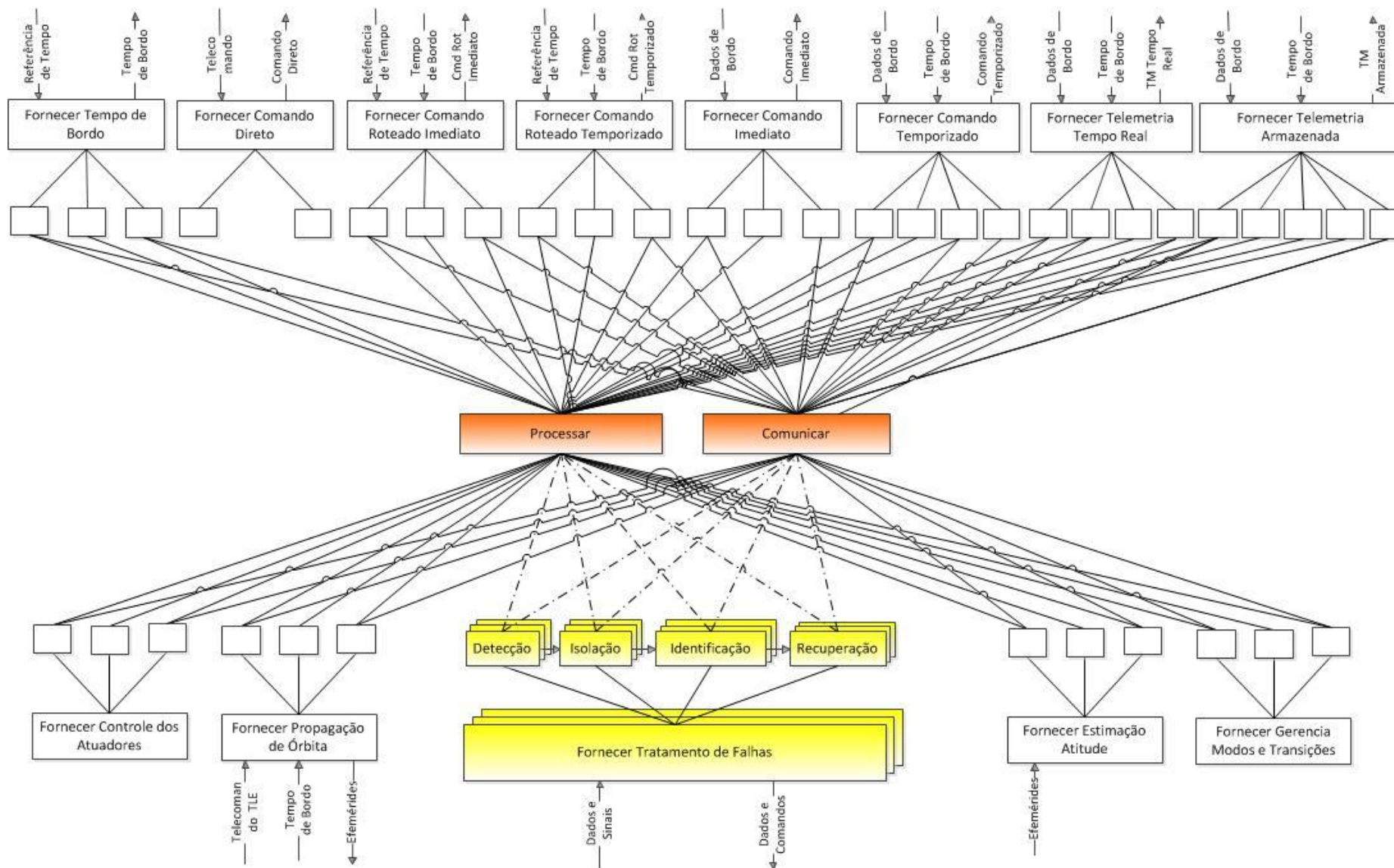


Figura 4.7 – Arquitetura funcional hierárquica do subsistema ACDH.



4.1.2 FMEA Funcional Hierárquica do ACDH

A decomposição funcional realizada na Seção 4.1 fornece os elementos necessários para a elaboração da FMEA funcional hierárquica do ACDH. A FMEA é aplicada por função, respeitando os níveis funcionais definidos na decomposição funcional, de forma a identificar, para cada nível funcional, os modos potenciais de falência, suas causas e seus efeitos.

A elaboração da FMEA tem como base o modelo de tabela e os critérios estabelecidos pela norma ECSS-Q-ST-30-02C (2009). As colunas Método de Detecção da Falência/Sintomas Observáveis, Provisão para Compensação, Recomendações e Observações são preenchidas considerando as soluções adotadas no âmbito das missões com participação brasileira e servem como referência para este trabalho.

Os resultados da aplicação da FMEA nas funções do ACDH são apresentados nas seguintes tabelas:

- Tabela 4.1 – Função ‘Fornecer Tempo de Bordo’;
- Tabela 4.2 – Função ‘Fornecer Comando Direto’;
- Tabela 4.3 – Função ‘Fornecer Comando Roteado Imediato’;

- Tabela B.1 – Função ‘Fornecer Comando Roteado Temporizado’;
- Tabela B.2 – Função ‘Fornecer Comandos Imediatos’;
- Tabela B.3 – Função ‘Fornecer Comandos Temporizados’;
- Tabela B.4 – Função ‘Fornecer Telemetria de Tempo Real’;
- Tabela B.5 – Função ‘Fornecer Telemetria Armazenada’;
- Tabela B.6 – Função ‘Estimar Atitude’;
- Tabela B.7 – Função ‘Propagar Órbita’;
- Tabela B.8 – Função ‘Comandar Atuadores’;
- Tabela B.9 – Função ‘Gerenciar Modos e Transições’.

Tabela 4.1 – Análise Funcional Hierárquica dos Efeitos dos Modos de Falências da Função ‘Fornecer Tempo de Bordo’.

Identificação	Nível	Função	Modo de Falência	Causa da Falência	Fase da Missão/ Modo de Operação	Efeitos da Falência	Severidade	Método de Detecção da Falência/ Sintomas Observáveis	Provisão para Compensação	Recomendações	Observações
1	2	Fornecer tempo de Bordo	Não fornece tempo de bordo	Não distribui TB; Não gera TB;	LEOP e fases operacionais;	Efemérides desatualizadas; Comandos temporizados não executados; Telemetria armazenada com tempo desatualizado; Telemetria de tempo real com tempo desatualizado; Dados auxiliares com erro; Atitude estimada com erro; Não gera imagem;	Catastrófica	Telemetria, OBSW	Recarga e execução do OBSW; Redundância física Redundar função		
2			Fornecer tempo de bordo de forma intermitente	Gera TB intermitente; Distribui TB intermitente;	Idem acima;	Efemérides atualizadas intermitentemente; Comandos temporizados executados intermitentemente; Telemetria armazenada com tempo atualizado intermitentemente; Telemetria de tempo real com tempo atualizado intermitentemente; Dados auxiliares sem erro intermitentemente; Atitude estimada sem erro intermitentemente; Gera imagem intermitentemente.	Catastrófica	Telemetria, OBSW	Recarga e execução do OBSW; Redundância física		

(continua)

Tabela 4.1 – Continuação

Identificação	Nível	Função	Modo de Falência	Causa da Falência	Fase da Missão/ Modo de Operação	Efeitos da Falência	Severidade	Método de Detecção da Falência/ Sintomas Observáveis	Provisão para Compensação	Recomendações	Observações	
3	2	Fornecer tempo de Bordo	Fornecer tempo de bordo fora da especificação	Gera TB fora da especificação; Distribui TB fora da especificação; Não adquire RT; Adquire RT fora da especificação;	Idem acima;	Efemérides com erro; Comandos temporizados não executados no tempo especificado; Telemetria armazenada com erro no tempo; Telemetria de tempo real com erro no tempo; Dados auxiliares com erro; Atitude estimada com erro; Gera imagem de local não especificado.	Catastrófica	Telemetria, OBSW	Recarga e execução do OBSW; Redundância física Redundar função			
4	3	Adquirir Referência de Tempo	Não adquire RT	Não processa; Não comunica;	Idem acima;	Fornecer TB fora da especificação;						
5			Adquire RT intermitente	Processa intermitentemente; Comunica intermitentemente;	Idem acima;	Fornecer TB fora da especificação intermitentemente (*);						
6			Adquire RT fora da especificação	Processa fora da especificação; Comunica fora da especificação;	Idem acima;	Fornecer TB fora da especificação;						
7			Gerar Tempo de Bordo	Não gera TB	Não processa;	Idem acima;	Não fornece TB;					
8			Gerar Tempo de Bordo	Gera TB intermitente	Processa intermitentemente	Idem acima;	Fornecer TB intermitentemente;					

(continua)

Tabela 4.1 – Continuação

Identificação	Nível	Função	Modo de Falência	Causa da Falência	Fase da Missão/ Modo de Operação	Efeitos da Falência	Severidade	Método de Detecção da Falência/ Sintomas Observáveis	Provisão para Compensação	Recomendações	Observações
9	3	Gerar Tempo de Bordo	Gera TB fora especificação	Processa fora da especificação;	Idem acima;	Fornece TB fora especificação;					
10		Distribuir Tempo de Bordo	Não distribui TB	Não processa; Não comunica;	Idem acima;	Não fornece TB;					
11			Distribui TB intermitente	Processa intermitentemente; Comunica intermitentemente;	Idem acima;	Fornece TB intermitentemente;					
12			Distribui TB fora da especificação;	Processa fora da especificação; Comunica fora da especificação;	Idem acima;	Fornece TB fora da especificação;					
13	4	Prover Processamento	Não processa	(**)	Idem acima;	Não adquire RT; Não gera TB; Não distribui TB;					
14			Processa intermitente	(**)	Idem acima;	Adquire RT intermitente; Gera TB intermitente; Distribui TB intermitente;					
15			Processa fora de especificação	(**)	Idem acima;	Adquire RT fde; Gera TB fde; Distribui TB fde;					

(continua)

Tabela 4.1 – Conclusão

Identificação	Nível	Função	Modo de Falência	Causa da Falência	Fase da Missão/ Modo de Operação	Efeitos da Falência	Severidade	Método de Detecção da Falência/ Sintomas Observáveis	Provisão para Compensação	Recomendações	Observações
16	4	Prover Comunicação	Não comunica	(**)	Idem acima;	Não adquire RT; Não distribui TB;					
17			Comunica intermitentemente	(**)	Idem acima;	Adquire RT intermitente; Distribui TB intermitente;					
18			Comunica fora de especificação	(**)	Idem acima;	Adquire RT fde; Distribui TB fde;					

(*) Os modos de falência ‘Fornecer Tempo de Bordo Fora da Especificação’ ou ‘Fornecer Tempo de Bordo Intermitentemente’ não são tratados neste trabalho.

(**) Conforme a Seção 4.1.1.1, as causas das falências das subfunções ‘Prover Processamento’ e ‘Prover Comunicação’ não são determinadas.

Tabela 4.2 – Análise Funcional Hierárquica dos Efeitos dos Modos de Falências da Função 'Fornecer Comando Direto'.

Identificação	Nível	Função	Modo de Falência	Causa da Falência	Fase da Missão/ Modo de Operação	Efeitos da Falência	Severidade	Método de Detecção da Falência/ Sintomas Observáveis	Provisão para Compensação	Recomendações	Observações
1	2	Fornecer Comando Direto	Não fornece comando direto	Perda da capacidade de recepção de telecomando; Perda da capacidade de distribuição de comando direto.	LEOP e fases operacionais;	Perda da comandabilidade do satélite;	Catastrófica	Telemetria	Redundância física		
2			Fornecer comando direto intermitente	Recepção intermitente de telecomando; Distribuição intermitente de comando direto.	Idem acima	Perda/atraso na comandabilidade do satélite;	Catastrófica	Telemetria	Redundância física		
3			Fornecer comando direto fora do especificado	Recepção de telecomando fora de especificação; Distribuição fora de especificação de comando direto.	Idem acima	Perda da comandabilidade do satélite;	Catastrófica	Telemetria	Redundância física		
4	3	Receber Telecomando Direto	Não recebe telecomando direto	Não demodula telecomando; Não decodifica telecomando.	Idem acima	Não fornece comando direto					
5			Recebe telecomando direto intermitente	Demodulação intermitente de telecomando; Decodificação intermitente de telecomando.	Idem acima	Fornecer comando direto intermitente					
6			Recebe telecomando direto fora de especificação	Demodulação de telecomando fora de especificação; Decodificação de telecomando fora de especificação.	Idem acima	Fornecer comando direto fora de especificação					

(continua)

Tabela 4.2 – Conclusão

Identificação	Nível	Função	Modo de Falência	Causa da Falência	Fase da Missão/ Modo de Operação	Efeitos da Falência	Severidade	Método de Detecção da Falência/ Sintomas Observáveis	Provisão para Compensação	Recomendações	Observações
7	3	Distribuir Comando Direto	Não distribui comando direto	(*)	Idem acima	Não fornece comando direto					
8			Distribui comando direto intermitente	(*)	Idem acima	Fornecer comando direto de forma intermitente					
9			Distribui comando direto fora da especificação	(*)	Idem acima	Fornecer comando direto fora de especificação					
10	4	Demodular Telecomando	Não demodula telecomando	(*)	Idem acima	Não recebe telecomando direto					
11			Demodula telecomando intermitente	(*)	Idem acima	Recebe telecomando direto intermitente					
12			Demodula telecomando fora da especificação	(*)	Idem acima	Recebe telecomando direto fora de especificação					
13		Decodificar Telecomando	Não decodifica telecomando	(*)	Idem acima	Não recebe telecomando direto					
14			Decodifica telecomando intermitente	(*)	Idem acima	Recebe telecomando direto intermitente					
15			Decodifica telecomando fora da especificação	(*)	Idem acima	Recebe telecomando direto fora de especificação					

(*) Conforme a seção 4.1.1.1, as causas das falências das subfunções do nível hierárquico mais baixo da decomposição funcional são consideradas componentes atômicos da arquitetura funcional e não são decompostas nem são determinadas as causas de suas falências.

Tabela 4.3 – Análise Funcional Hierárquica dos Efeitos dos Modos de Falências da Função ‘Fornecer Comando Roteado Imediato’.

Identificação	Nível	Função	Modo de Falência	Causa da Falência	Fase da Missão/ Modo de Operação	Efeitos da Falência	Severidade	Método de Detecção da Falência/ Sintomas Observáveis	Provisão para Compensação	Recomendações	Observações
1	2	Fornecer Comandos Roteados Imediatos	Não fornece comandos roteados imediatos;	Perda da capacidade de recepção de telecomando; Perda da capacidade de distribuição de Comando Roteado.	LEOP e fases operacionais;	Perda da comandabilidade do satélite	Catastrófica	Telemetria	Redundância física Recarga e execução do OBSW;		
2			Fornecer comandos roteados imediatos de forma intermitente;	Recepção intermitente de telecomando; Distribuição intermitente de Comando Roteado Imediato;	Idem acima	Perda/Atraso na comandabilidade do satélite	Catastrófica	Telemetria	Redundância física Recarga e execução do OBSW;		
3			Fornecer comandos roteados imediatos fora de especificação	Recepção de telecomando fora de especificação; Distribuição de Comando Roteado Imediato fora de especificação;	Idem acima	Perda da comandabilidade do satélite	Catastrófica	Telemetria	Redundância física Recarga e execução do OBSW;		

(continua)

Tabela 4.3 – Continuação

Identificação	Nível	Função	Modo de Falência	Causa da Falência	Fase da Missão/ Modo de Operação	Efeitos da Falência	Severidade	Método de Detecção da Falência/ Sintomas Observáveis	Provisão para Compensação	Recomendações	Observações
4	3	Receber Telecomando Direto	Não recebe telecomando direto	Não demodula telecomando; Não decodifica telecomando.	Idem acima	Não fornece comando roteado imediato					
5			Recebe telecomando direto intermitente	Demodulação intermitentemente de telecomando; Decodificação intermitentemente de telecomando.	Idem acima	Fornece comando roteado imediato intermitentemente					
6			Recebe telecomando direto fora de especificação	Demodulação de telecomando fora de especificação; Decodificação de telecomando fora de especificação.	Idem acima	Fornece comando roteado imediato fora de especificação					
7		Distribuir Comando Roteado Imediato	Não distribui comando roteado imediato	Não processa; Não comunica;	Idem acima	Não fornece comando roteado imediato					

(continua)

Tabela 4.3 – Continuação

Identificação	Nível	Função	Modo de Falência	Causa da Falência	Fase da Missão/ Modo de Operação	Efeitos da Falência	Severidade	Método de Detecção da Falência/ Sintomas Observáveis	Provisão para Compensação	Recomendações	Observações
8	3	Distribuir Comando Roteado Imediato	Distribui comando roteado imediato intermitente	Processa intermitentemente; Comunica intermitentemente;	Idem acima	Fornecer comando roteado imediato de forma intermitente					
9			Distribui comando roteado imediato fora da especificação	Processa fora da especificação; Comunica fora da especificação;	Idem acima	Fornecer comando roteado imediato fora de especificação					
10	4	Demodular Tele comando	Não demodula telecomando	(*)	Idem acima	Não recebe telecomando direto					
11			Demodula telecomando intermitente	(*)	Idem acima	Recebe telecomando direto intermitente					
12			Demodula telecomando fora da especificação	(*)	Idem acima	Recebe telecomando direto fora de especificação					

(continua)

Tabela 4.3 – Continuação

Identificação	Nível	Função	Modo de Falência	Causa da Falência	Fase da Missão/ Modo de Operação	Efeitos da Falência	Severidade	Método de Detecção da Falência/ Sintomas Observáveis	Provisão para Compensação	Recomendações	Observações
13	4	Decodificar Telecomando	Não decodifica telecomando	(*)	Idem acima	Não recebe telecomando direto					
14			Decodifica telecomando intermitente	(*)	Idem acima	Recebe telecomando direto intermitente					
15			Decodifica telecomando fora da especificação	(*)	Idem acima	Recebe telecomando direto fora de especificação					
16		Prover Processamento	Não processa	(*)	Idem acima	Não distribui comando roteado imediato					
17			Processa intermitente	(*)	Idem acima	Distribui comando roteado imediato intermitente					
18			Processa fora de especificação	(*)	Idem acima	Distribui comando roteado imediato fora da especificação					

(continua)

Tabela 4.3 – Conclusão

Identificação	Nível	Função	Modo de Falência	Causa da Falência	Fase da Missão/ Modo de Operação	Efeitos da Falência	Severidade	Método de Detecção da Falência/ Sintomas Observáveis	Provisão para Compensação	Recomendações	Observações
19	4	Prover Comunicação	Não comunica	(*)	Idem acima	Não distribui comando roteado imediato					
20			Comunica intermitentemente	(*)	Idem acima	Distribui comando roteado imediato intermitente					
21			Comunica fora de especificação	(*)	Idem acima	Distribui comando roteado imediato fora da especificação					

(*) Conforme a seção 4.1.1.1, as causas das falências das subfunções do nível hierárquico mais baixo da decomposição funcional, são consideradas componentes atômicos da arquitetura funcional e não são decompostas nem são determinadas as causas de suas falências.

4.1.3 Repertório de Falhas do ACDH

O domínio das falhas de um sistema inclui todas as suas falhas potenciais. Nem todas as falhas pertencentes ao domínio das falhas são, no entanto, identificáveis. O conjunto das falhas potenciais pertencentes ao domínio das falhas do sistema que são identificadas constitui o Repertório de Falhas do sistema.

Neste trabalho o domínio das falhas é limitado ao subsistema ACDH e o Repertório de Falhas é constituído pelas falhas funcionais identificadas. Na Tabela 4.4 são apresentadas as falhas identificadas por meio da aplicação FMEA funcional às funções 'Fornecer tempo de bordo', 'Fornecer comando direto', 'Fornecer comando roteado imediato'. A Tabela 4.4 apresenta o número de funções que podem ser afetadas por cada falha, o número de modos de falência dessas funções que podem ser causados por cada falha e quantidade de efeitos que podem ser causados por cada falha.

Tabela 4.4 – Falhas Identificadas na FMEA Funcional do ACDH para as Funções ‘Fornecer tempo de bordo’, ‘Fornecer comando direto’, ‘Fornecer comando roteado imediato’.

Item	Falhas	Funções Afetadas	Modos de Falência Causados pela Falha	Efeitos Causados pela Falha
1	Não distribui TB	1	1	7
2	Não gera TB	1	1	7
3	Gera TB intermitente	1	1	7
4	Distribui TB intermitente	1	1	7
5	Gera TB fora da especificação	1	1	7
6	Distribui TB fora da especificação	1	1	7
7	Não adquire RT	1	1	7
8	Adquire RT fora da especificação	1	1	7
9	Não processa	3	3	2
10	Não comunica	2	2	2
11	Processa intermitentemente	3	3	1
12	Comunica intermitentemente	2	2	1
13	Processa fora da especificação	3	3	1
14	Comunica fora da especificação	2	2	1
15	Perda da capacidade de recepção de telecomando	2	2	1
16	Perda da capacidade de distribuição de comando direto	1	1	1
17	Recepção intermitente de telecomando	2	2	2
18	Distribuição intermitente de comando direto	1	1	2
19	Recepção de telecomando fora de especificação	2	2	1
20	Distribuição fora de especificação de comando direto	1	1	1
21	Não demodula telecomando	1	1	1
22	Não decodifica telecomando	1	1	1
23	Demodulação intermitentemente de telecomando	1	1	1
24	Decodificação intermitentemente de telecomando	1	1	1
25	Demodulação de telecomando fora de especificação	1	1	1
26	Decodificação de telecomando fora de especificação	1	1	1
27	Perda da capacidade de distribuição de Comando Roteado Imediato	1	1	1
28	Distribuição intermitente de Comando Roteado Imediato	1	1	1
29	Distribuição de Comando Roteado Imediato fora de especificação	1	1	1

4.1.4 Tratamento da Função ‘Fornecer Tempo de Bordo’

Falhas e falências podem ocorrer em qualquer nível da estrutura funcional e seus efeitos podem se propagar e afetar tanto o subsistema quanto o sistema e

a missão. Numa missão de imageamento, a falência da função 'Fornecer Tempo de Bordo' pode ter impacto no produto da missão. O não fornecimento ou o fornecimento do tempo fora da especificação para a função 'Propagar Órbita' resulta em erro no cálculo dos elementos orbitais que se propagam para os dados auxiliares, uma vez que tanto o tempo como os elementos orbitais fazem parte dos dados auxiliares. Como os dados auxiliares são gravados na imagem e utilizados para sua recuperação em solo, a falência no fornecimento do tempo de bordo inviabiliza o fornecimento das imagens pela missão.

4.1.4.1 Comportamento Cinemático do ACDH na Presença de Falências da Função 'Fornecer Tempo de Bordo'

Para descrever o comportamento cinemático do ACDH na presença de falências da função 'Fornecer Tempo de Bordo', as informações relativas aos modos de falência e aos efeitos disponíveis na FMEA funcional são importadas para o TFPG da função. A seguir, os monitores são definidos e incorporados aos nós e, por último, os nós são interconectados por meio de setas temporizadas. Essa sequência é semelhante à adotada por Bittner et al. (2017) para desenvolver um TFPG a partir da FMEA da arquitetura física de FDIR da sonda Solar Orbiter da ESA com o propósito de avaliar a propagação de falências nos diferentes níveis da arquitetura.

Diferente de Bittner et al. (2017), a descrição do comportamento neste trabalho, é segmentada de acordo com os níveis da arquitetura funcional e da FMEA das funções. Essa abordagem simplifica a descrição e a definição de lógicas de detecção, diagnose e recuperação. A segmentação da descrição do comportamento permite iniciar a descrição do comportamento pelo nível mais baixo ou pelo nível mais alto da decomposição funcional. A opção neste trabalho por iniciar pelo nível mais alto deve-se a este ser o nível onde os modos de falência da função se propagam, evidenciando os seus efeitos nas outras funções do subsistema e no sistema.

i) Descrição do Comportamento no Nível 1

Modos de Falência

Os modos de falência identificados no nível 2 da Tabela 4.1 são importados diretamente para o TFGP:

- Não fornece tempo de bordo (*MF1*);
- Fornece tempo de bordo fora da especificação (*MF2*);
- Fornece tempo de bordo de forma intermitente (*MF3*).

Além dos modos de falência da função 'Fornecer Tempo de Bordo', são importados os modos de falência de funções do ACDH e de funções externas ao ACDH que podem produzir as mesmas discrepâncias produzidas pela função 'Fornecer Tempo de Bordo'.

Modos de falência de outras funções do ACDH:

- Não fornece telemetria de tempo real (*MF4*);
- Fornece telemetria de tempo real fora de especificação (*MF5*);
- Não fornece telemetria armazenada (*MF6*);
- Fornece telemetria armazenada fora de especificação (*MF7*);
- Não propaga órbita (*MF8*);
- Propaga órbita fora de especificação (*MF9*);
- Não fornece comando temporizado (*MF10*).
- Fornece comando temporizado fora de especificação (*MF11*);

Modos de falência de funções externas ao ACDH:

- Câmera não imageia (*MF12*);
- Transponder da câmera não transmite (*MF13*);

Efeitos

Dos efeitos identificados na Tabela 4.1, são importados como discrepâncias para o TFPG:

- Efemérides desatualizadas;
- Efemérides com erro;
- Comandos temporizados não fornecidos;
- Comandos temporizados não fornecidos no tempo especificado;
- Telemetria armazenada com tempo desatualizado;
- Telemetria de tempo real com tempo desatualizado;
- Telemetria armazenada com erro no tempo;
- Telemetria de tempo real com erro no tempo;
- Dados auxiliares com erro;
- Atitude estimada com erro;
- Não gera imagem;
- Gera imagem de local não especificado;
- Imagem com erro nos dados auxiliares;
- Perda da observabilidade satélite;
- Fornece imagem não localizável;
- Fornece Imagem de local não especificado;
- Não fornece imagem.

As discrepâncias são representadas no grafo como nós disjuntivos exclusivos, uma vez que é suposto a ocorrência de apenas modos simples de falência.

Em vista das considerações da seção 3.3.3.3, a propagação dos efeitos dos modos de falência intermitentes são considerados iguais aos da propagação dos efeitos dos modos de falência permanentes e, por essa razão, não são importados para o TFPG.

Definição dos Monitores

A definição dos monitores visa detectar e diagnosticar o modo de falência ativo de forma que o sistema possa ser recuperado autonomamente.

As discrepâncias ‘Perda da observabilidade do satélite’, ‘Fornecer imagem não localizável’, ‘Fornecer imagem de local não especificado’ ‘Não fornecer imagem’ são manifestações no Solo de falências ocorridas no satélite. Como essas discrepâncias **podem ser sempre detectadas** pelo processamento das telemetrias e das imagens no Solo, são associados **monitores** a cada uma delas (o código dos monitores está de acordo a numeração adotada na Figura 4.8):

- *M12*: Perda da observabilidade do satélite;
- *M19*: Fornece imagem não localizável;
- *M111*: Fornece imagem de local não especificado;
- *M112*: Não fornece imagem.

As discrepâncias ‘Comandos temporizados não fornecidos’ e ‘Comandos temporizados não fornecidos no tempo especificado’ **não são monitoráveis**. Para o seu monitoramento é necessário que o monitor que tenha informações relativas à geração e escalonamento do comando e um relógio de bordo independente do relógio que fornece o tempo de bordo.

Também as discrepâncias ‘Não gera imagem’, ‘Gera imagem de local não especificado’ e ‘Imagem com erro nos dados auxiliares’ **não são monitoráveis**. Para o monitoramento, seriam necessários monitores com capacidade para abrir e examinar as imagens.

Já as discrepâncias ‘Efemérides desatualizadas’, ‘Efemérides com erro’, ‘Telemetria armazenada com tempo desatualizado’, ‘Dados auxiliares com erro’, ‘Telemetria armazenada com erro no tempo’, ‘Telemetria de tempo real com erro no tempo’ e ‘Telemetria de tempo real com tempo desatualizado’ **são monitoráveis** embora, não sejam monitoradas em nenhum dos satélites com participação brasileira. Para monitorar estas discrepâncias, o monitoramento é vinculado a um evento periódico de forma que, periodicamente, o valor atual do parâmetro monitorado possa ser comparado com o último valor adquirido. Os **monitores** são associados às discrepâncias como segue:

- *M110*: Efemérides desatualizadas;
- *M16*: Efemérides com erro;
- *M15*: Telemetria armazenada com tempo desatualizado;
- *M13*: Telemetria de tempo real com tempo desatualizado;
- *M18*: Dados auxiliares com erro;
- *M11*: Telemetria de tempo real com erro no tempo;
- *M14*: Telemetria armazenada com erro no tempo;

Definição das Conexões dos Nós

As conexões entre os nós que representam os modos de falência e os nós que representam as discrepâncias são definidas com base nos efeitos listados na Tabela 4.1 e nos documentos INPE (2001), INPE (2010).

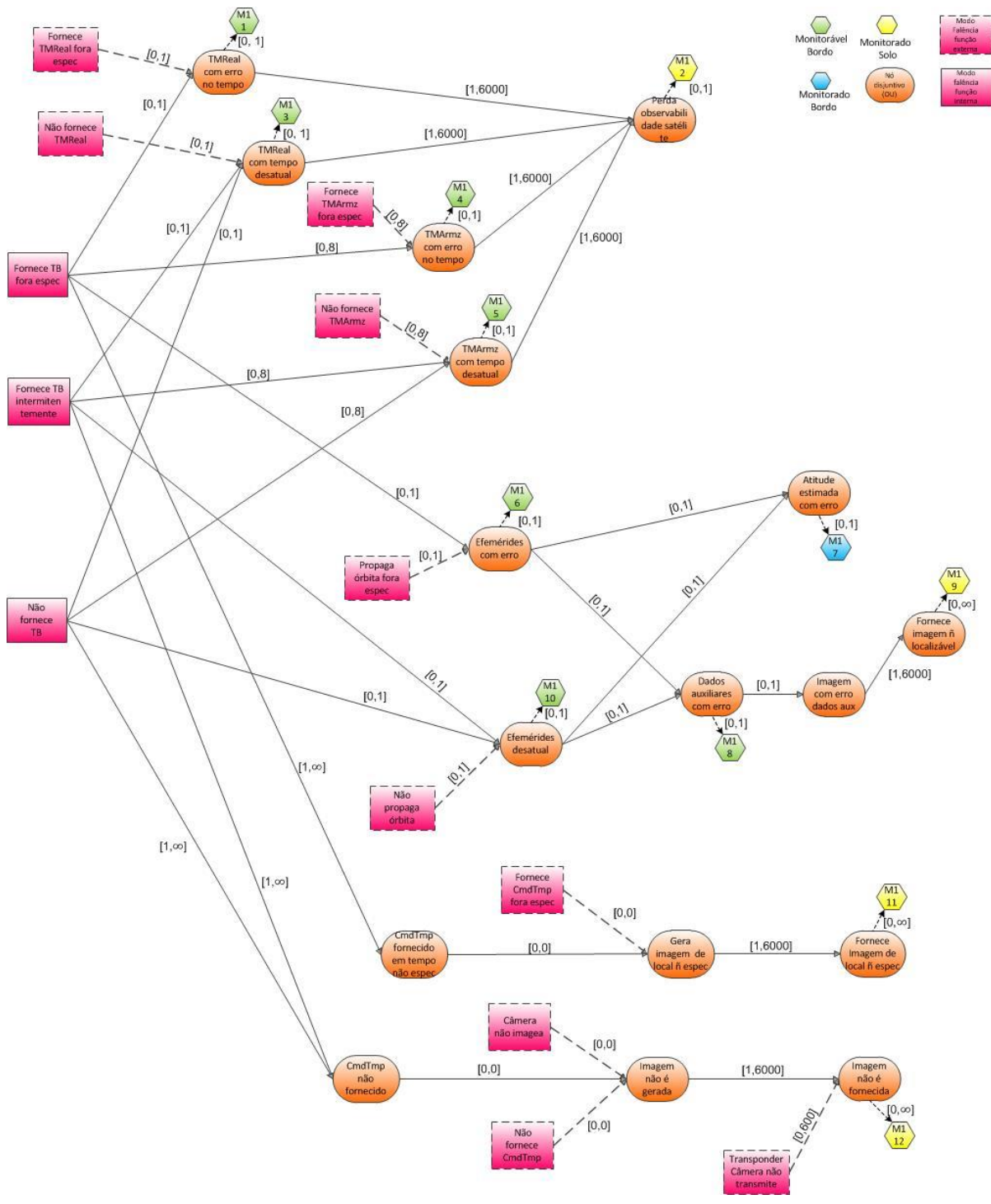
A definição dos tempos de propagação têm como referência os satélites Amazônia-1 e CBERS-3 e 4 com base em informações fornecidas pela equipe de desenvolvimento desses satélites.

Propagação das Falências

Com base nas informações acima é gerado o diagrama de propagação dos modos de falência da função 'Fornecer Tempo de Bordo' no subsistema ACDH (nível 1 da decomposição funcional) apresentado na Figura 4.8.

Na Figura 4.8, os **retângulos de linhas tracejadas** representam **falências de outras funções** que podem resultar nas discrepâncias produzidas pelos modos de falência da função 'Fornecer Tempo de Bordo'. Nessas figuras, os **retângulos de cantos arredondados** representam **discrepâncias do tipo disjuntivo exclusivo**. Os **hexágonos** representam os **monitores** das discrepâncias. Os monitores são identificados por um **número** sendo que o primeiro dígito corresponde ao nível hierárquico em análise e os demais dígitos correspondem ao número de sequência do monitor no nível analisado. Os **hexágonos na cor azul** representam monitores usualmente utilizados na implementação de um **ACDH**. Os **hexágonos na cor amarela** representam monitores usualmente presentes em **solo**. Os **hexágonos na cor verde** representam monitores que usualmente **não são utilizados a bordo**. As **discrepâncias** às quais não está associado um monitor são consideradas **não observáveis**. A dupla $[t_{min}, t_{max}]$ representa o **intervalo de tempo** que a falência ou os seus efeitos podem levar para se propagar do nó precedente ao nó conseqüente.

Figura 4.8 – Diagrama de propagação para função ‘Fornecer Tempo de Bordo’ no nível 1.



ii) Descrição do Comportamento no Nível 2

Modos de Falência

Os modos de falência identificados no nível 3 da Tabela 4.1 são importados diretamente para o TFPG:

- Não adquire RT;
- Adquire RT intermitente;
- Adquire RT fora da especificação;
- Não gera TB;
- Gera TB intermitentemente;
- Gera TB fora especificação;
- Não distribui TB;
- Distribui TB fora da especificação;
- Distribui TB intermitentemente.

Efeitos

Dos efeitos identificados na Tabela 4.1, são importados como discrepâncias para o TFPG:

- Fornece TB fora da especificação;
- Não fornece TB;

As discrepâncias são representadas no grafo como nós disjuntivos exclusivos, uma vez que é suposto a ocorrência de apenas modos simples de falência.

Em vista das considerações da seção 3.3.3.3, a propagação dos efeitos dos modos de falência intermitentes são considerados iguais aos da propagação dos efeitos dos modos de falência permanentes e, por essa razão, não são importados para o TFPG.

Definição dos Monitores

O monitoramento das discrepâncias não é realizado nesse nível funcional. A sua inclusão implica a adição de estruturas funcionais/físicas que reproduzem as existentes nas funções que utilizam o tempo de bordo.

Definição das Conexões dos Nós

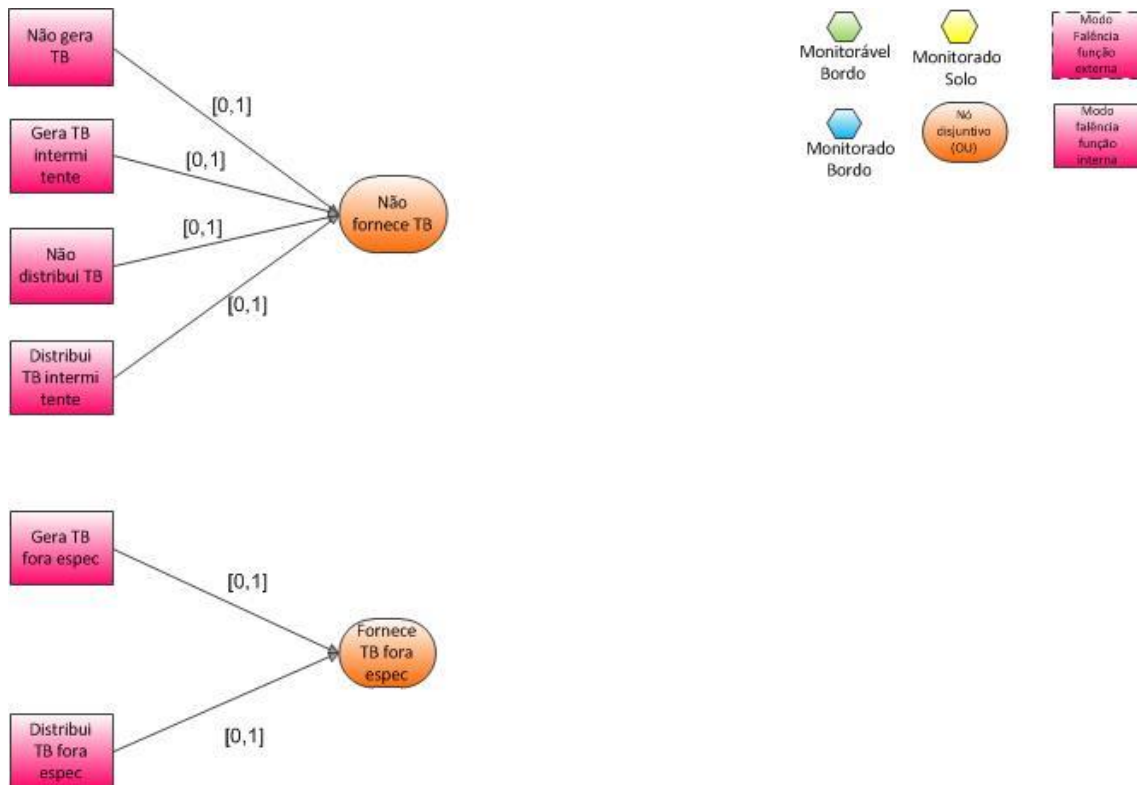
As conexões entre os nós que representam os modos de falência e os nós que representam as discrepâncias são definidas com base nos efeitos listados na Tabela 4.1 e nos documentos INPE (2001) e INPE (2010).

A definição dos tempos de propagação tem como referência os satélites Amazônia-1 e CBERS-3 e 4 com base em informações fornecidas pela equipe de desenvolvimento desses satélites.

Propagação das Falências

Com base nas informações acima é gerado o diagrama de propagação dos modos de falência da função 'Fornecer Tempo de Bordo' no subsistema ACDH (nível 2 da decomposição funcional) apresentado na Figura 4.9.

Figura 4.9 – Diagrama de propagação da função ‘Fornecer Tempo de Bordo’ no nível 2.



iii) Descrição do Comportamento no Nível 3

Modos de Falência

Os modos de falência identificados no nível 4 da Tabela 4.1 são importados diretamente para o TFPG:

- Não processa;
- Processa intermitente;
- Processa fora de especificação;
- Não comunica;
- Comunica fora de especificação;
- Comunica intermitentemente;

Efeitos

Dos efeitos identificados na Tabela 4.1, são importados como discrepâncias para o TFPG:

- Não adquire RT;
- Não gera TB;
- Não distribui TB;
- Adquire RT fora de especificação;
- Gera TB fora de especificação;
- Distribui TB fora de especificação;

As discrepâncias são representadas no grafo como nós disjuntivos exclusivos, uma vez que é suposto a ocorrência de apenas modos simples de falência.

Em vista das considerações da seção 3.3.3.3, a propagação dos efeitos dos modos de falência intermitentes são considerados iguais aos da propagação dos efeitos dos modos de falência permanentes e, por essa razão, não são importados para o TFPG.

Definição dos Monitores

Nesse nível funcional é viável a inclusão de monitores para as discrepâncias 'Não adquire RT' e 'Adquire RT fora de especificação'. O monitoramento das demais discrepâncias não é realizado, pois a sua inclusão implica a adição de estruturas funcionais/físicas que reproduzem as existentes nas funções que utilizam o tempo de bordo.

Definição das Conexões dos Nós

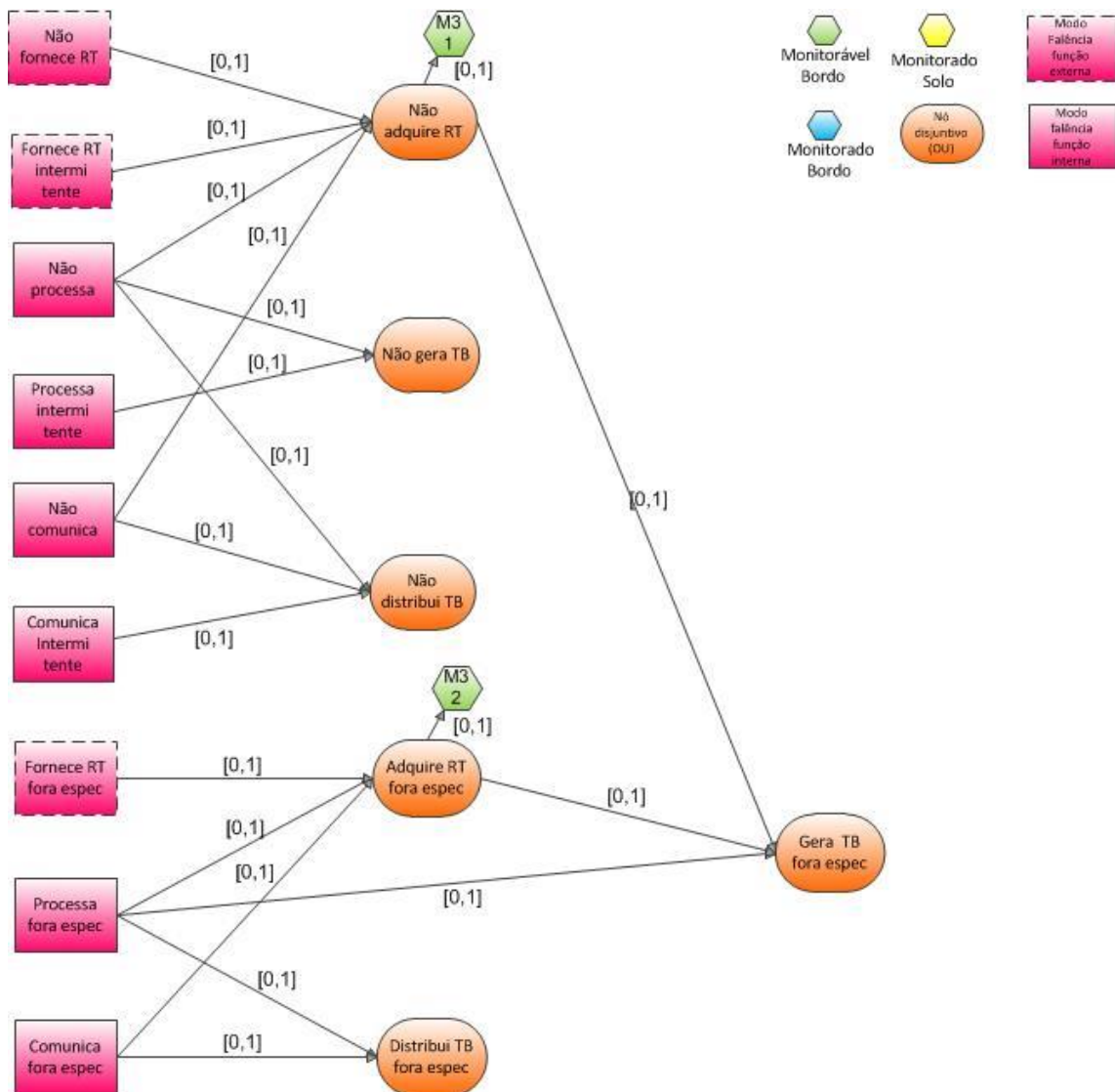
As conexões entre os nós que representam os modos de falência e os nós que representam as discrepâncias são definidas com base nos efeitos listados na Tabela 4.1 e nos documentos INPE (2001) e INPE (2010).

A definição dos tempos de propagação tem como referência os satélites Amazonia-1 e CBERS-3 e 4 com base em informações fornecidas pela equipe de desenvolvimento desses satélites.

Propagação das Falências

Com base nas informações acima é gerado o diagrama de propagação dos modos de falência da função 'Fornecer Tempo de Bordo' no subsistema ACDH (nível 2 da decomposição funcional) apresentado na Figura 4.10.

Figura 4.10 – Diagrama de propagação para função 'Fornecer Tempo de Bordo' no nível 3



4.1.4.2 Detecção e Diagnose

Nesta seção, a detecção e diagnose dos modos de falência no nível 1 é exercitada por meio da aplicação da estratégia proposta.

Conforme tratado na seção 3.3.4, a detecção, isolamento e identificação dos modos de falências podem ser realizados com base nas suas manifestações espaciais, temporais e informacionais.

Escolha do Domínio

A detecção e a diagnose dos modos de falência da função 'Fornecer Tempo de Bordo' são realizadas com base nas manifestações dos modos de falência no domínio espacial. A utilização das manifestações temporais das falências da função 'Fornecer Tempo de Bordo' pela lógica de detecção e diagnose, ou seja, pela função inversa torna-se inviável, pois o tempo utilizado para monitorar o horário de ocorrência das discrepâncias é fornecido pela própria função 'Fornecer Tempo de Bordo'. Essa situação produz um efeito análogo ao produzido pela falência de monitores, tratada na Seção 3.3.4.2 para o domínio espacial, a qual pode resultar em ambiguidade nas assinaturas ou em assinaturas que não pertencem à imagem da função direta e resultar em erro na diagnose do modo de falência ativo.

Definição do Vetor Assinatura no Domínio Espacial

No domínio espacial, o exame do diagrama de propagação mostra a existência em bordo de nove modos de falência que podem causar discrepâncias monitoradas (três relativos à função 'Fornecer Tempo de Bordo', dois relativos à função 'Fornecer Telemetria de Tempo Real', dois relativos à função 'Fornecer Telemetria Armazenada' e dois relativos à função 'Propagar Órbita'). Como o modo de falência intermitente ('Fornecer tempo de bordo intermitentemente') é tratado como permanente, ou seja, é tratado como o modo 'Não fornece tempo de bordo', são considerados apenas oito modos de falência ($m=8$). Isso implica que para identificar o modo de falência ativo devam

existir pelo menos 8 assinaturas biunívocamente associadas aos 8 *MFs* (Teorema 1).

O vetor assinatura deve conter um conjunto de efeitos monitorados que permita cobrir todos os modos de falências. Nesse caso, o conjunto composto pelos monitores *M11*, *M13*, *M14*, *M15*, *M17* (ou *M18*) é o menor conjunto que atende a essa condição. No entanto, a inclusão de *M17* (ou *M18*) no vetor assinatura produz uma ambiguidade: os modos de falência ‘Propaga órbita fora de especificação’ e ‘Não propaga órbita’ produzem a mesma assinatura. Essa ambiguidade pode ser removida pela remoção de *M17* (ou *M18*) e a inclusão de *M16* e *M110*. O vetor assinatura pode então ser definido como:

$$\vec{a} = (M11\ M13\ M14\ M15\ M16\ M110) \quad (4.1)$$

A Tabela 4.5 mostra a assinatura de todos os modos de falência detetáveis do diagrama de propagação nível 1 da função ‘Fornecer Tempo de Bordo’.

Tabela 4.5 – Assinatura no domínio dos modos de falência da função ‘Fornecer Tempo de Bordo’.

Modos de Falência	Assinaturas no Domínio Espacial (Vetor \vec{a})
<i>MF1</i> - Não fornece tempo de bordo	(0 1 0 1 0 1)
<i>MF2</i> - Fornece tempo de bordo fora da especificação	(1 0 1 0 1 0)
<i>MF4</i> - Não fornece telemetria de tempo real	(0 1 0 0 0 0)
<i>MF5</i> - Fornece telemetria de tempo real fora de especificação	(1 0 0 0 0 0)
<i>MF6</i> - Não fornece telemetria armazenada	(0 0 0 1 0 0)
<i>MF7</i> - Fornece telemetria armazenada fora de especificação	(0 0 1 0 0 0)
<i>MF8</i> - Não propaga órbita	(0 0 0 0 0 1)
<i>MF9</i> - Propaga órbita fora de especificação	(0 0 0 0 1 0)

4.1.5 Aplicação da Abordagem por Modelagem e Simulação

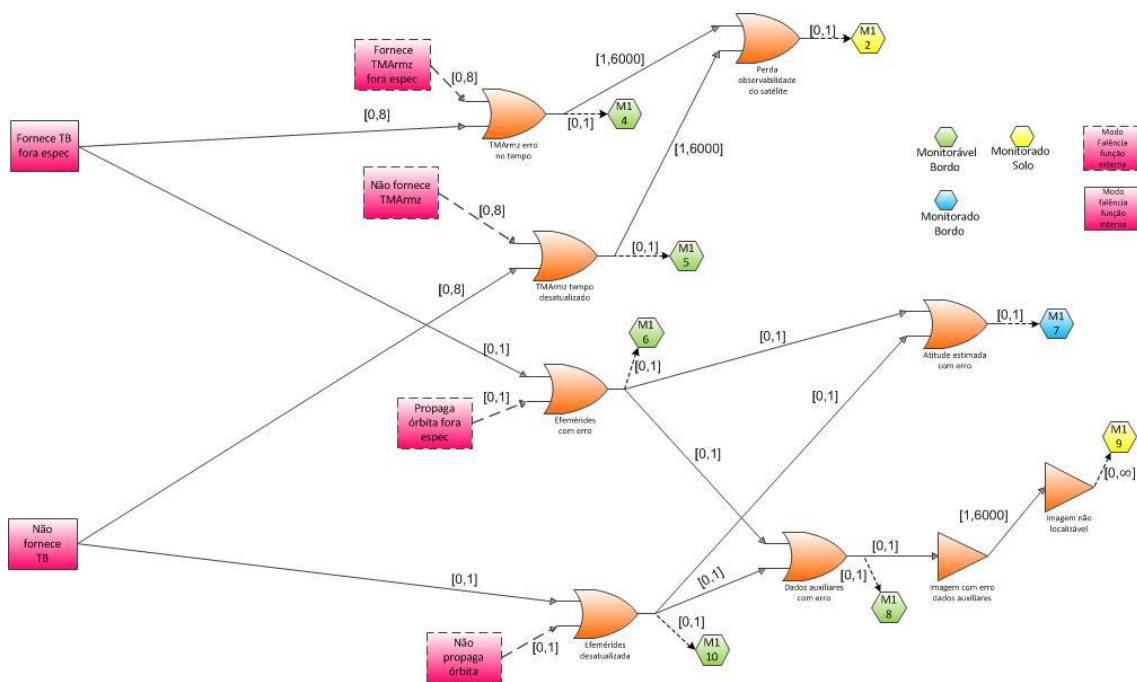
Como os modos de falência da função ‘Fornecer Tempo de Bordo’ afetam o fornecimento do tempo, os resultados da diagnose por amostragem temporal, por utilizar o tempo para sua aplicação, podem ser igualmente afetados. Para evitar essa possibilidade, a diagnose é realizada por eventos. Assim, as três lógicas propostas na seção 3.3.5.1, ou seja, diagnose com critério de diferença de assinaturas, diagnose com critério de biunivocidade e diagnose com critério de biunivocidade e verificação de precedência, são aplicadas para isolar e/ou identificar o modo de falência ativo. Os resultados da simulação da aplicação dessas lógicas à função ‘Fornecer Tempo de Bordo’ são apresentados e analisados no Capítulo 5.

4.1.6 Aplicação da Abordagem por Teoria e Análise

Na condição de monitores isentos de falências, a aplicação da abordagem por teoria e análise segue os passos propostos na seção 3.3.4.2.

Passo 1: Para aplicar a abordagem por teoria e análise, a propagação da função ‘Fornecer Tempo de Bordo’ é, sem perda de generalidade, reduzida conforme o diagrama de propagação mostrado na Figura 4.11.

Figura 4.11 – Diagrama de propagação da função ‘Fornecer Tempo de Bordo’ reduzida.



No diagrama existem seis modos de falência:

- Não fornece tempo de bordo (*MF1*);
- Fornece tempo de bordo fora de especificação (*MF2*);
- Fornece telemetria armazenada fora de especificação (*MF3*);
- Não fornece telemetria armazenada (*MF4*);
- Propaga órbita fora de especificação (*MF5*);

- Não propaga órbita (*MF6*).

Considerando que os modos de falência são mutuamente exclusivos, e analisando as propagações dos 6 modos de falência pelo diagrama da Figura 4.11, conclui-se que, para identificar quatro modos de falência e isolar os outros dois basta o acréscimo de dois monitores (*M14* e *M15*) e utilizar o monitor *M17*, o qual já existe a bordo. Nesse caso, o vetor assinatura é composto por *M14*, *M15* e *M17* e os modos de falência são isolados/identificados conforme a Tabela 4.6.

Tabela 4.6 – Assinaturas e Isolação/identificação dos modos de falência da função ‘Fornecer Tempo de Bordo’ reduzida.

Assinaturas no Domínio Espacial (Vetor \vec{a})	Modos de Falência Isolados/Identificados
(0 0 0)	Nenhum modo de falência ativo, i.e., modo normal
(0 0 1)	Não propaga órbita Propaga órbita fora de especificação
(0 1 1)	Não fornece tempo de bordo
(1 1 1)	Assinatura inválida para modos de falência mutuamente exclusivos
(1 0 1)	Fornece tempo de bordo fora de especificação
(1 0 0)	Fornece telemetria armazenada fora de especificação
(1 1 0)	Assinatura inválida para modos de falência mutuamente exclusivos
(0 1 0)	Não fornece telemetria armazenada

Os modos de falência ‘Não propaga órbita’ e ‘Propaga órbita fora de especificação’ não são identificáveis. A associação de ambos à assinatura (001) indica a ambiguidade.

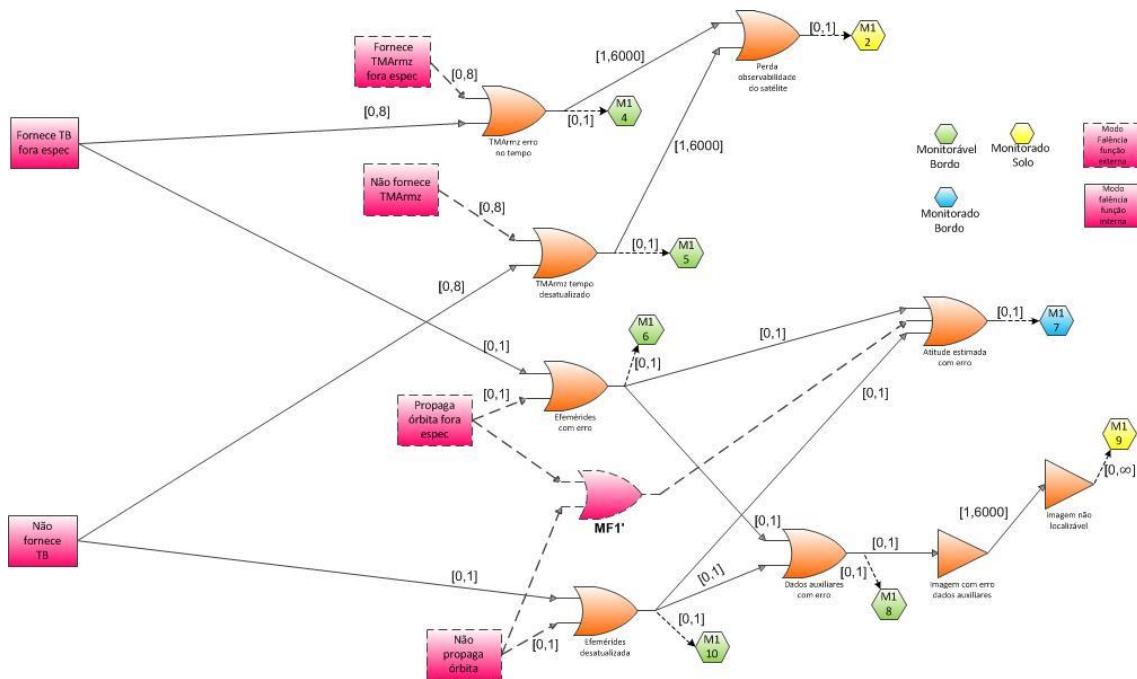
Se pudermos tolerá-la, estes podem ser agrupados num **pseudo modo/modo virtual/modo agrupado *MF1***’ como indicado na Tabela 4.7 e mostrado na

Figura 4.12. Este agrupamento possibilita uma aplicação recursiva dessa abordagem.

Tabela 4.7 – Agrupamento dos dos modos de falência da função ‘Fornecer Tempo de Bordo’ reduzida em pseudos modos de falência.

Pseudo Modos de Falência	Modos de Falência Agrupados
<i>MF1'</i>	Não propaga órbita Propaga órbita fora de especificação

Figura 4.12 – Diagrama de propagação da função ‘Fornecer Tempo de Bordo’ reduzida com os pseudos modos falência.



Se não pudermos tolerá-la, então, sendo ela do tipo “OU inclusivo”, para desambiguá-los, precisa-se de, pelo menos, mais 2 monitores, o *M16* e o *M110*, já que o terceiro, o *M17*, é necessário a para as identificações da Tabela 4.6. Assim, para identificar o modo de falência ativo é necessário acrescentar a bordo ao menos quatro monitores com essa finalidade específica: *M14*, *M15*, *M16* e *M110*, ao *M17*.

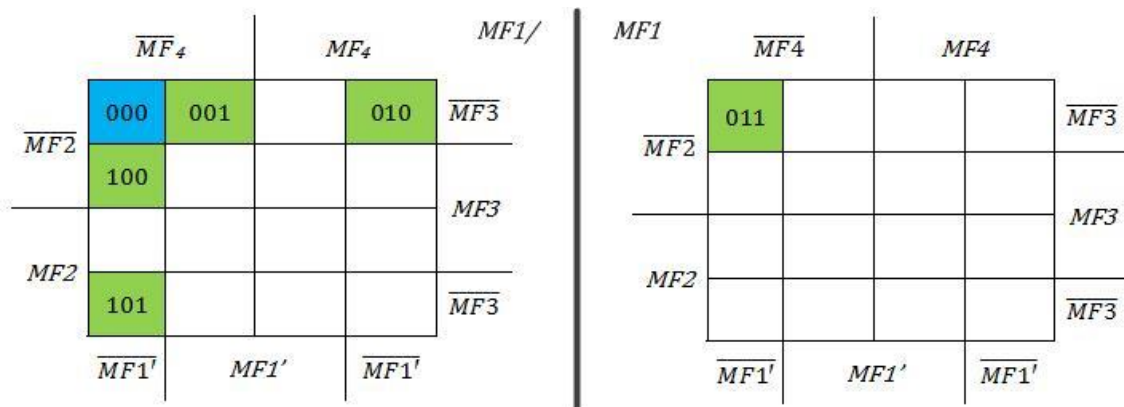
A Tabela 4.6 também mostra que a falência de monitores (Tipo 1 = falso positivo; ou Tipo 2 = falso negativo) pode transformar assinaturas válidas (p.ex.

011) em outras assinaturas válidas (p.ex.: 001) ou inválidas (p.ex.: 111), gerando ambiguidade, dependente da diferença entre o observado e o previsto.

Na sequência, é considerado que os modos de falência ‘Não propaga órbita’ (MF6) e ‘Propaga órbita fora de especificação’ (MF5) podem ser agrupados no pseudo modo MF1’.

Passo 2: A Figura 4.13 mostra o mapa de Karnaugh da assinatura espacial, representada pela tripla ordenada das discrepâncias monitoradas por M14, M15 e M17, dos modos de falência MF1, MF2, MF3, MF4 e do pseudo modo de falência MF1’ da função ‘Fornecer Tempo de Bordo’ reduzida. As células verdes indicam as assinaturas dos modos mutuamente exclusivos. As células brancas indicam as assinaturas dos modos simultâneos. A célula azul indica a assinatura na ausência de falências.

Figura 4.13 – Mapa de Karnaugh da assinatura espacial dos modos e pseudo modo de falência da função ‘Fornecer Tempo de Bordo’ reduzida.



Passo 3 e 4: O mapa de Karnaugh das assinaturas mostra que para falências mutuamente exclusivas não existem ambiguidades nas assinaturas dos modos e pseudo modos de falência .

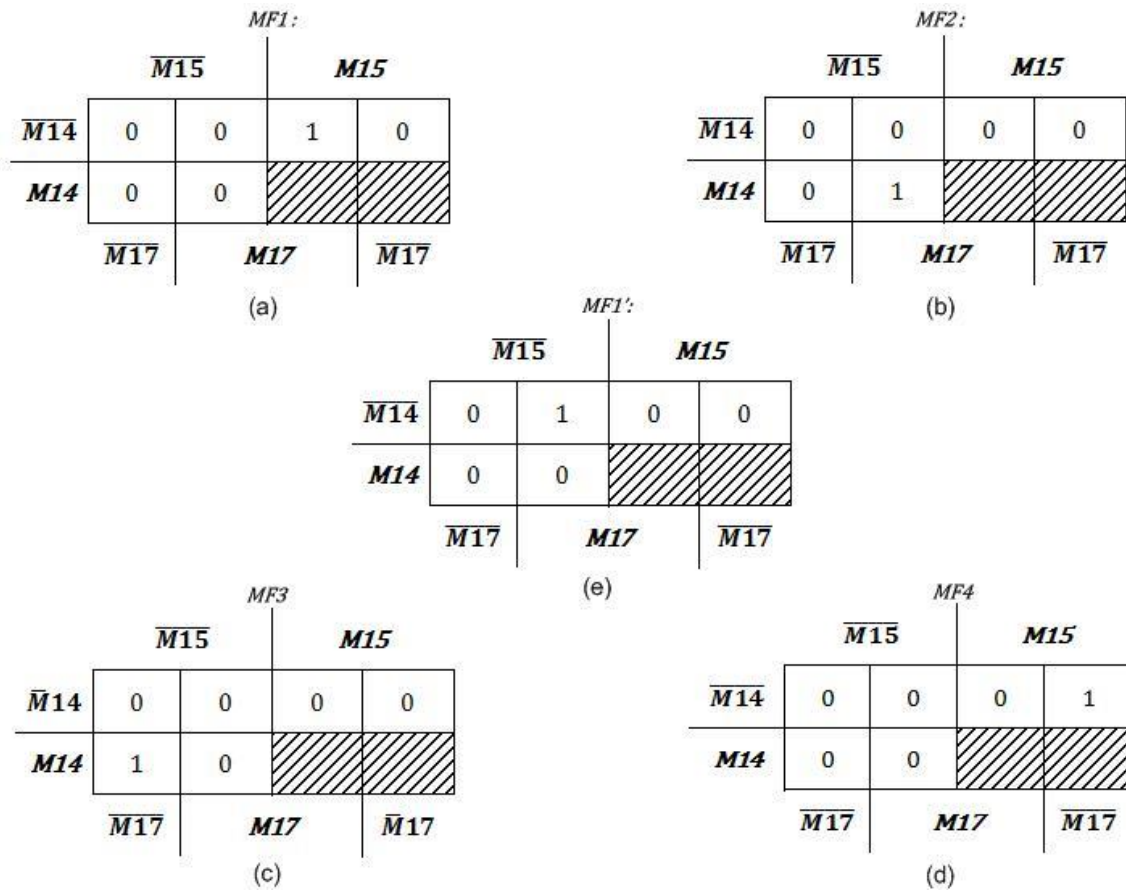
Passo 5: A Figura 4.14 mostra o mapa de compatibilidade dos modos e pseudos modos de falência da função ‘Fornecer Tempo de Bordo’ reduzida. As células hachuradas referem-se aos modos de falência simultâneos.

Passo 6: Os mapas de Karnaugh de $MF1$, $MF2$, $MF3$, $MF4$ e $MF1'$, em função de $M14$, $M15$, e $M17$ são gerados a partir do mapa de compatibilidade (Figura 4.14) e mostrados na Figura 4.15. As células hachuradas referem-se aos modos de falência simultâneos.

Figura 4.14 – Mapa de compatibilidade da função ‘Fornecer Tempo de Bordo’ reduzida.

		$\overline{M15}$		$M15$	
$\overline{M14}$		$MF1 = 0$	$MF1 = 0$	$MF1 = 1$	$MF1 = 0$
		$MF2 = 0$	$MF2 = 0$	$MF2 = 0$	$MF2 = 0$
		$MF3 = 0$	$MF3 = 0$	$MF3 = 0$	$MF3 = 0$
		$MF4 = 0$	$MF4 = 0$	$MF4 = 0$	$MF4 = 1$
		$MF1' = 0$	$MF1' = 1$	$MF1' = 0$	$MF1' = 0$
$M14$		$MF1 = 0$	$MF1 = 0$		
		$MF2 = 0$	$MF2 = 1$		
		$MF3 = 1$	$MF3 = 0$		
		$MF4 = 0$	$MF4 = 0$		
		$MF1' = 0$	$MF1' = 0$		
		$\overline{M17}$		$M17$	$\overline{M17}$

Figura 4.15 – Mapa de Karnaugh para (a) $MF1$, (b) $MF2$, (c) $MF3$, (d) $MF4$ e (e) $MF1'$.



Passo 7: As lógicas inversa otimizadas para $MF1$, $MF2$, $MF3$, $MF4$ e $MF1'$ são geradas a partir dos mapas de Karnaugh (Figura 4.15), conforme as expressões (4.2), (4.3), (4.4), (4.5) e (4.6).

$$MF1 = \overline{M14} M15 M17 \quad (4.2)$$

$$MF2 = M14 \overline{M15} M17 \quad (4.3)$$

$$MF3 = M14 \overline{M15} \overline{M17} \quad (4.4)$$

$$MF4 = \overline{M14} M15 \overline{M17} \quad (4.5)$$

$$MF1' = \overline{M14} \overline{M15} M17 \quad (4.6)$$

4.2 Aplicação da Estratégia a um Caso da Literatura

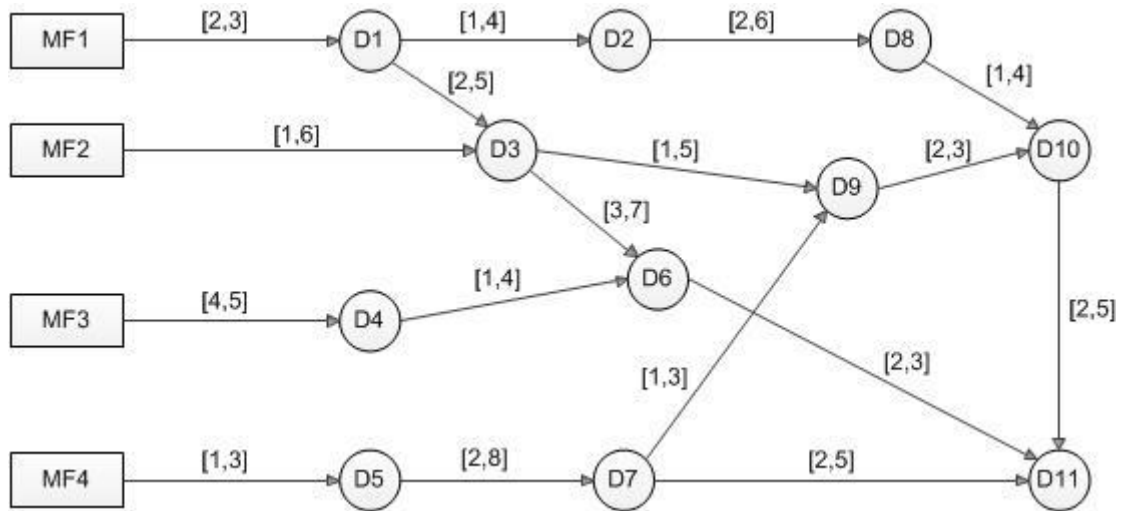
A aplicação da estratégia a um Caso da Literatura é primeiramente realizada utilizando a abordagem por Modelagem e Simulação e, a seguir, a aplicação da estratégia é realizada utilizando a abordagem por Teoria e Análise, portanto, na ordem inversa em que as abordagens são introduzidas na seção 3. A opção por esta sequência decorre da abordagem por Modelagem e Simulação ser aplicada no modelo completo da função e a abordagem por Teoria e Análise ser aplicada em um modelo reduzido da função, o qual é derivado do modelo completo.

4.2.1 Abordagem por Modelagem e Simulação

Nesta seção, a estratégia é parcialmente aplicada a um caso da literatura cujo modelo de falhas exibe um comportamento mais complexo que o exibido pela função 'Fornecer Tempo de Bordo'. Nesse caso, o comportamento da função na presença de falhas é representado pelo grafo temporizado (Figura 4.16) proposto no trabalho *A Consistency-based Robust Diagnosis Approach for Temporal Causal Systems* por Abdelwahed et al. (2005).

A estratégia proposta neste trabalho não é aplicada às etapas que precedem a elaboração do grafo, uma vez que o sistema não é descrito em Abdelwahed et al. (2005).

Figura 4.16 – Diagrama de propagação de um caso da literatura.



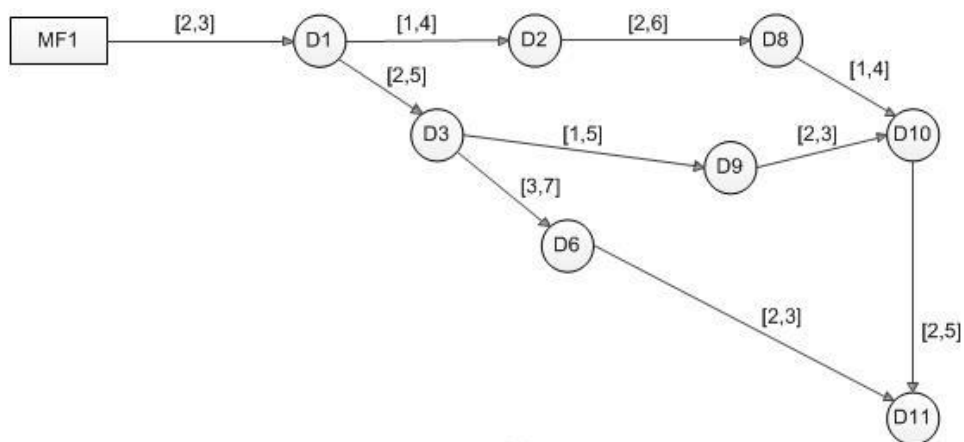
Fonte: Adaptado de Abdelwahed et al. (2005).

Aplicando as hipóteses estabelecidas na seção 3.3.4.1 ao caso da literatura e considerando que todas as discrepâncias são monitoradas, ou seja, a cada discrepância D_i está associado um monitor M_i , pode ser definido um vetor assinatura composto por onze elementos:

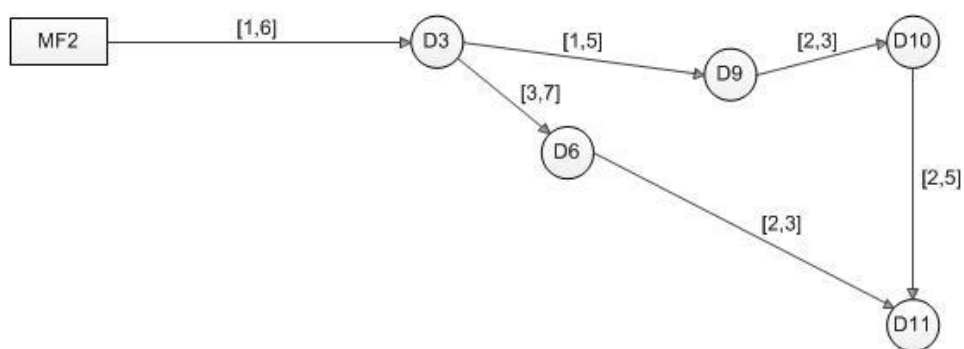
$$\vec{a} = (D1M1 \ D2M2 \ D3M3 \ D4M4 \ D5M5 \ D6M6 \ D7M7 \ D8M8 \ D9M9 \ D10M10 \ D11M11) \quad (4.7)$$

A assinatura de cada modo de falência pode então ser determinada a partir do diagrama de propagação da função, decompondo-o em quatro subdiagramas (Figura 4.17), um para a propagação de cada modo de falência. A Tabela 4.8 mostra a assinatura no domínio espacial de cada modo de falência.

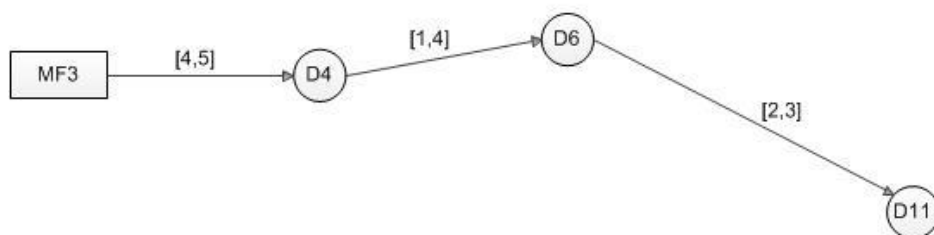
Figura 4.17 – Decomposição do diagrama de propagação do caso da literatura: a) subdiagrama da propagação de *MF1*; b) subdiagrama da propagação de *MF2*; c) subdiagrama da propagação de *MF3*; subdiagrama da propagação de *MF4*.



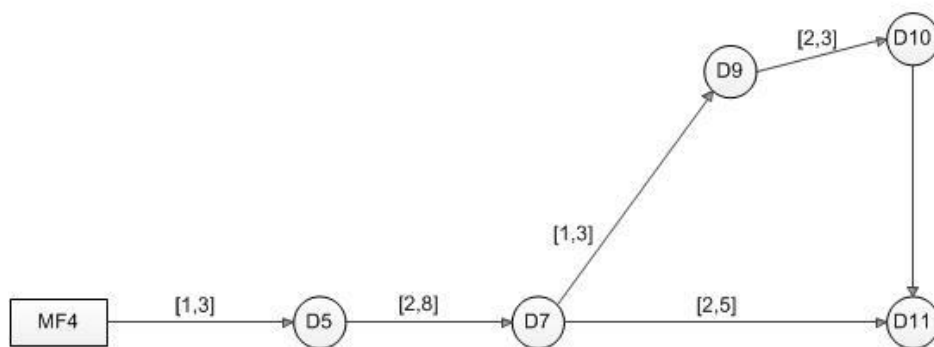
(a)



(b)



(c)



(d)

Tabela 4.8 – Assinaturas no domínio espacial dos modos de falência do caso da literatura.

Modos de Falência	Assinaturas no Domínio Espacial (Vetor \vec{a})
<i>MF1</i>	(1 1 1 0 0 1 0 1 1 1 1)
<i>MF2</i>	(0 0 1 0 0 1 0 0 1 1 1)
<i>MF3</i>	(0 0 0 1 0 1 0 0 0 0 1)
<i>MF4</i>	(0 0 0 0 1 0 1 0 1 1 1)

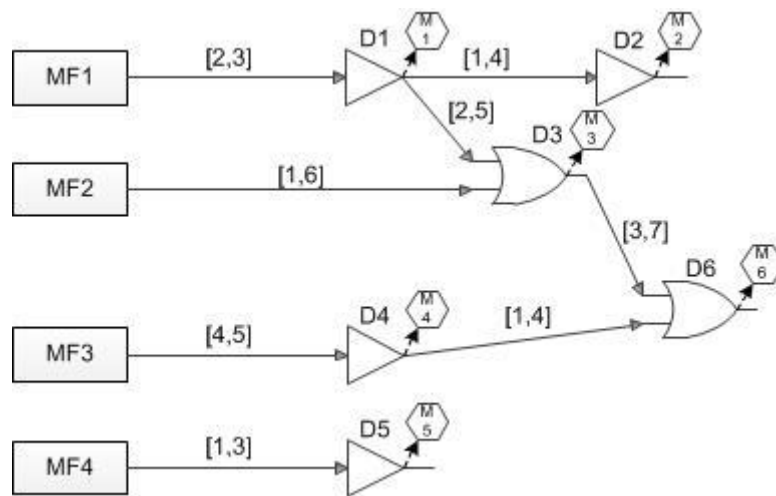
As três lógicas propostas na seção 3.3.5.1 para isolar e/ou identificar o modo de falência ativo a partir da ocorrência de eventos, ou seja, diagnose com critério de diferença de assinaturas, diagnose com critério de biunivocidade e diagnose com critério de biunivocidade e verificação de precedência mais as três lógicas propostas na seção 3.3.5.2 para realizar a diagnose por amostragem temporal, ou seja, amostragem no tempo máximo de propagação das falências, amostragem periódica e amostragem no tempo de propagação das discrepâncias são aplicadas ao do caso da literatura. Os resultados da simulação da aplicação dessas lógicas são apresentados e analisados no Capítulo 5.

4.2.2 Abordagem por Teoria e Análise

Na condição de monitores isentos de falências, a aplicação da abordagem por teoria e análise segue os passos propostos na seção 3.3.4.2.

Passo 1: Para aplicar a abordagem por teoria e análise, a propagação do caso da literatura é, sem perda de generalidade, reduzido às seis primeiras discrepâncias, $D1$, $D2$, . . . $D6$, gerando o diagrama de propagação reduzida mostrado na Figura 4.18.

Figura 4.18 – Diagrama de propagação do caso da literatura reduzido.



Passo 2: A Figura 4.19 mostra o mapa de Karnaugh da assinatura espacial (vetor \vec{a}) representada pela sêxtupla ordenada de discrepâncias monitoradas ($D1M1 D2M2 D3M3 D4M4 D5M5 D6M6$) dos modos de falência do caso da literatura reduzido. Neste caso, as células verdes indicam as assinaturas dos modos de falência mutuamente exclusivos. As células brancas indicam as assinaturas dos modos de falência simultâneos. A célula azul indica a assinatura na ausência de falências.

Quando os modos de falência são supostos mutuamente exclusivos, a função direta não apresenta ambiguidades. Para exercitar a aplicação da abordagem por teoria e análise a ocorrência de modos de falência simultâneos será, no entanto, admitida. Neste caso, existem quatro ambiguidades duplas, as quais são destacadas por círculos na Figura 4.19.

Passo 3: O mapa de Karnaugh das assinaturas mostra que as ambiguidades ocorrem quando $MF1$ está ativo. Neste caso, não é possível identificar no domínio espacial, sem violar a Hipótese 2, se a falência decorre de $MF1$ ativo ou de $MF2$ ativo ou de ambos. Neste caso, só é possível no domínio espacial isolar o modo de falência ativo ($MF1$ ou $MF2$). Para fins de demonstração da aplicação da abordagem por teoria e análise é, no entanto, considerado que existe um efeito monitorável ($D7$) que pode ser incorporado à assinatura espacial, como mostrado na Figura 4.20.

Figura 4.19 – Mapa de Karnaugh da assinatura espacial do caso da literatura reduzido.

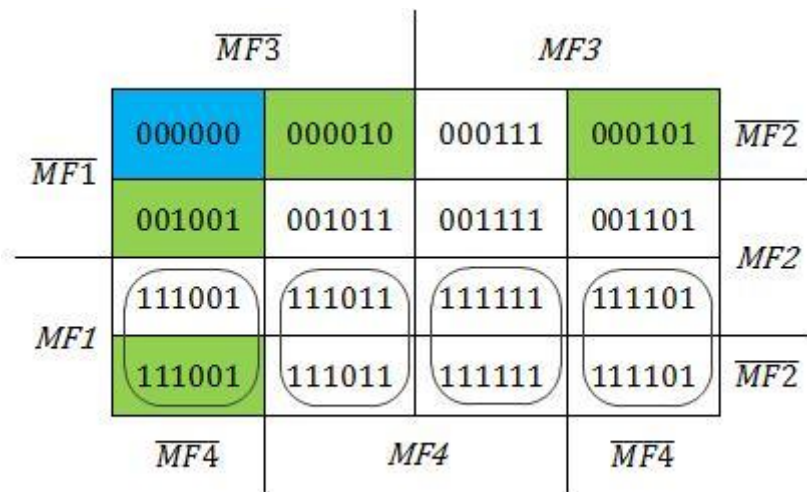
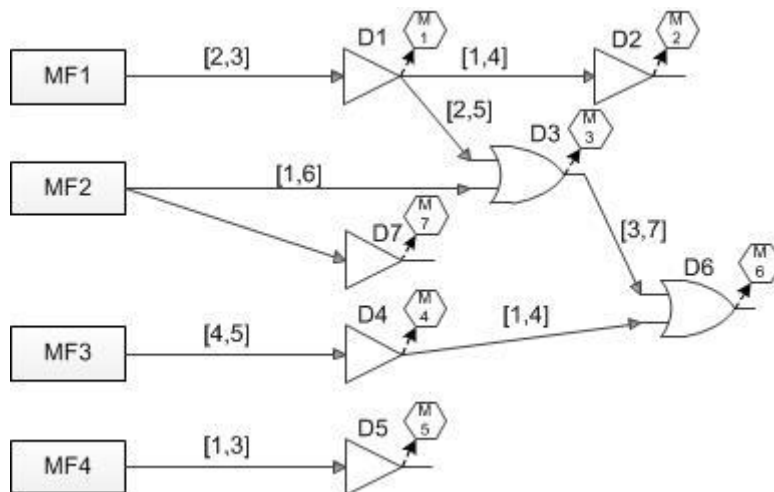


Figura 4.20 – Diagrama de propagação do caso da literatura reduzido desambiguado.



Passo 4: Na nova configuração espacial, a assinatura espacial (vetor \vec{a}) passa a ser representada pela sétupla ordenada ($D1M1 D2M2 D3M3 D4M4 D5M5 D6M6 D7M7$) eliminando as ambiguidades, como mostrado na Figura 4.21.

Figura 4.21 – Mapa de Karnaugh da assinatura espacial do caso da literatura reduzido desambiguado.

	$\overline{MF3}$		$MF3$		
$\overline{MF1}$	0000000	0000100	0001110	0001010	$\overline{MF2}$
	0010011	0010111	0011111	0011011	$MF2$
	1110011	1110111	1111111	1111011	
$MF1$	1110010	1110110	1111110	1111010	$\overline{MF2}$
	$\overline{MF4}$	$MF4$	$MF4$	$\overline{MF4}$	

Passo 5: Para construção do mapa de compatibilidade as discrepâncias $D2$, $D3$ e $D6$ não são consideradas, uma vez que na nova configuração as discrepâncias monitoradas $D2M2$, $D3M3$ e $D6M6$ não são necessárias para a identificação dos modos de falência. A Figura 4.22 mostra o mapa de compatibilidade do caso da literatura reduzido desambiguado.

Passo 6: Os mapas de Karnaugh de $MF1$, $MF2$, $MF3$ e $MF4$ em função de $D1$, $D4$, $D5$ e $D7$ são gerados a partir do mapa de compatibilidade (Figura 4.22) e mostrados na Figura 4.23.

Figura 4.22 – Mapa de compatibilidade do caso da literatura reduzido desambiguado.

	$\overline{D5}$		$D5$		
$\overline{D1}$	$MF1=0$	$MF1=0$	$MF1=0$	$MF1=0$	$\overline{D4}$
	$MF2=0$	$MF2=1$	$MF2=1$	$MF2=0$	
	$MF3=0$	$MF3=0$	$MF3=0$	$MF3=0$	
	$MF4=0$	$MF4=0$	$MF4=1$	$MF4=1$	
$D1$	$MF1=0$	$MF1=0$	$MF1=0$	$MF1=0$	$D4$
	$MF2=0$	$MF2=1$	$MF2=1$	$MF2=0$	
	$MF3=1$	$MF3=1$	$MF3=1$	$MF3=1$	
	$MF4=0$	$MF4=0$	$MF4=1$	$MF4=1$	
$D1$	$MF1=1$	$MF1=1$	$MF1=1$	$MF1=1$	$\overline{D4}$
	$MF2=0$	$MF2=1$	$MF2=1$	$MF2=0$	
	$MF3=1$	$MF3=1$	$MF3=1$	$MF3=1$	
	$MF4=0$	$MF4=0$	$MF4=1$	$MF4=1$	
	$\overline{D7}$	$D7$		$\overline{D7}$	

Passo 7: As lógicas inversa otimizadas para $MF1$, $MF2$, $MF3$ e $MF4$ são geradas a partir dos mapas de Karnaugh (Figura 4.23), conforme as expressões (4.8), (4.9), (4.10) e (4.11).

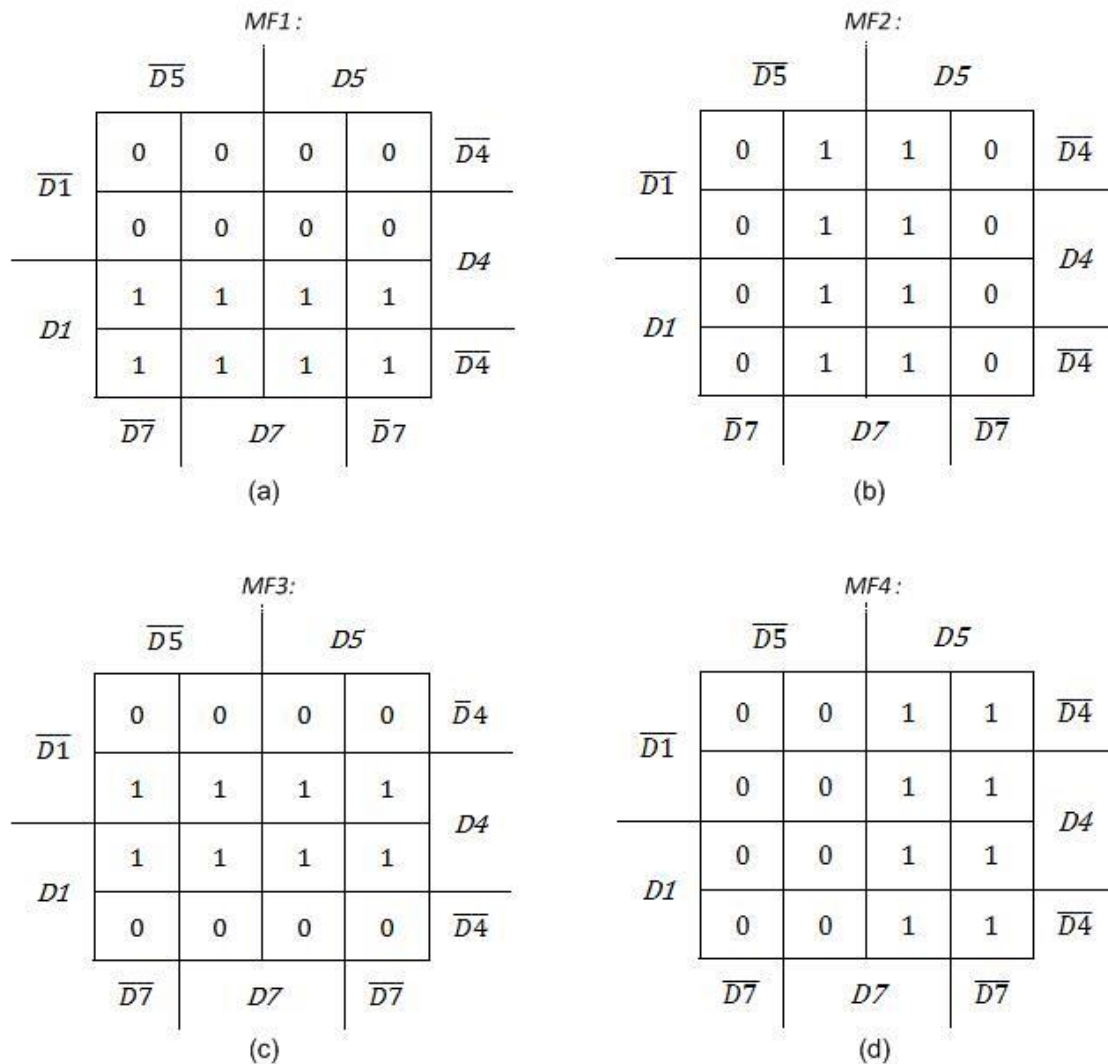
$$MF1 = D1 \quad (4.8)$$

$$MF2 = D7 \quad (4.9)$$

$$MF3 = D4 \quad (4.10)$$

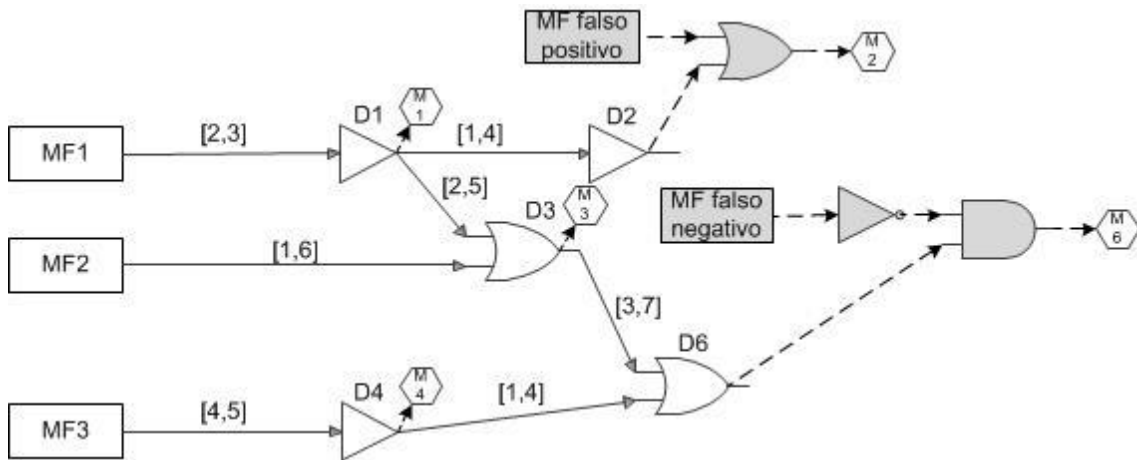
$$MF4 = D5 \quad (4.11)$$

Figura 4.23 – Mapas de Karnaugh para: (a) MF1; (b) MF2; (c) MF3; (d) MF4.



A falência de monitores (Tipo 1 = falso positivo; ou Tipo 2 = falso negativo) pode ser modelada como mostrado na Figura 4.24. A falência do monitor $M2$ como falso positivo é modelada por meio de uma porta OU inclusiva que recebe o modo de falência falso positivo (representado pelo retângulo **MF falso positivo**) e o estado da discrepância $D2$. A falência do monitor $M6$ como falso negativo é modelada por meio de uma porta E que recebe o modo de falência falso negativo (representado pelo retângulo **MF falso negativo**) negado e o estado da discrepância $D6$. Neste caso, considera-se que o monitor $M2$ apresenta somente o modo de falência falso positivo e o monitor $M6$ apresenta somente o modo de falência falso negativo.

Figura 4.24 – Modelamento da falência de monitores como falso positivo e falso negativo.



O modelamento do falso positivo e do falso negativo como modos de falência permite aplicar as abordagens propostas nas seções 3.3.4 e 3.3.5 para o tratamento de falências de monitores.

5 VALIDAÇÃO DA ESTRATÉGIA PARA O TRATAMENTO DE FALHAS

O objetivo desta seção é validar por meio de simulação as lógicas algorítmicas para diagnose propostas na seção 3.3.5: diagnose por diferença de assinaturas, diagnose por biunivocidade e diagnose por biunivocidade e precedência. As lógicas são aplicadas à função 'Fornecer Tempo de Bordo' e ao caso da literatura.

5.1 Ambiente de Modelagem e Simulação

Na ausência de ferramentas específicas para modelagem e simulação relativas aos processos de gerenciamento de falhas no INPE, as simulações realizadas neste trabalho utilizam um ambiente de desenvolvimento da linguagem VHDL (*VHSIC Hardware Description Language*).

O ambiente escolhido é composto pelas seguintes ferramentas:

- Simulador VHDL: GHDL v0.34;
- Visualizador de formas de onda: *GTKWave Analyser* v3.3.84;
- Editor de texto: Notepad++ v7.5.4;
- Ferramenta para automatização da simulação: *GNU Make* v3.81;

Todas as ferramentas são *softwares* livres, que podem ser utilizados sob as condições GNU GPL v2 (*GNU General Public License version 2*).

5.1.1 Simulador GHDL

O simulador GHDL (*G Hardware Design Language*) é um compilador VHDL que pode executar programas VHDL que atendam às revisões de 1987, 1993 e 2002 da norma IEEE 1076 - IEEE Standard VHDL Language Reference Manual (GINGOLD, 2018). O GHDL suporta parcialmente a revisão 2008 da norma IEEE 1076.

O GHDL traduz arquivos VHDL para código de máquina sem o uso de uma linguagem intermediária tal como o C ou o C++. Dessa forma, o código compilado pode ser mais rápido e o tempo de análise pode ser menor que os obtidos com o uso de um compilador que utiliza uma linguagem intermediária.

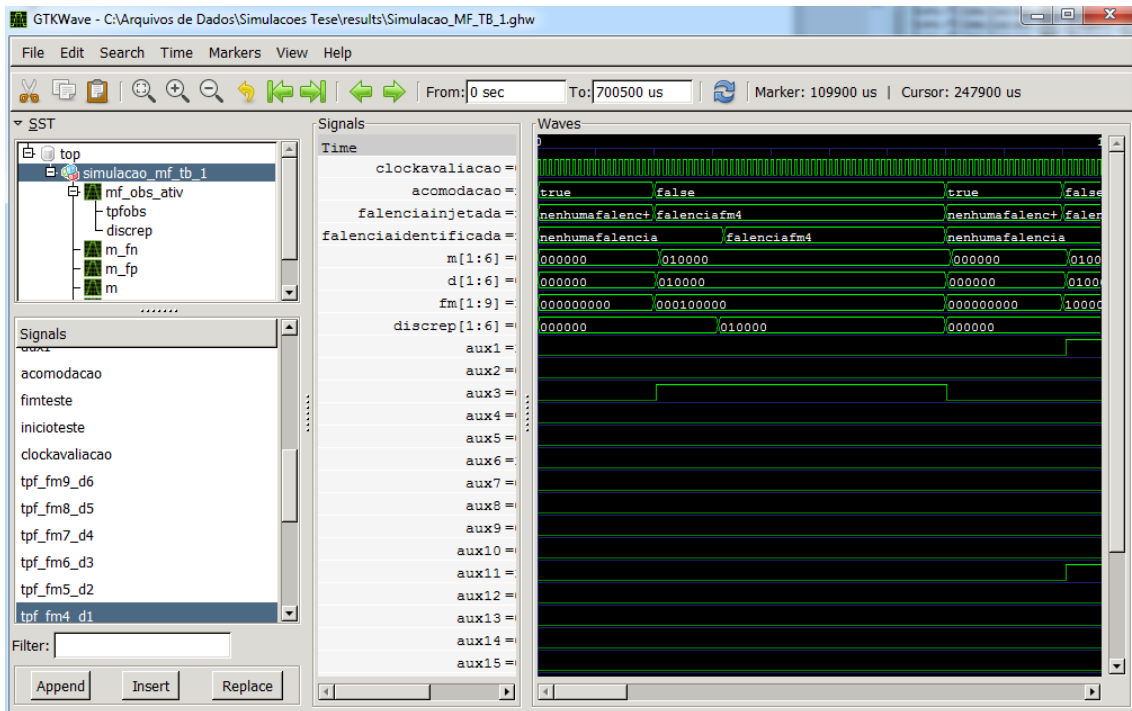
O simulador GHDL não contém um visualizador gráfico. Ele produz, no entanto arquivos de saída nos formatos VCD, GHW e FST os quais podem ser visualizados em visualizadores de forma de onda como, por exemplo, o GTKWave.

5.1.2 Visualizador GTKWave

O GTKWave (BSI, 2018) é uma ferramenta de análise usada para depurar modelos de simulação escritos em VHDL e Verilog. O GTKWave não executa interativamente com a simulação. Ele é executado após a simulação e usa como entrada arquivo de saída do simulador. O GTKWave suporta arquivos nos formatos VCD, LXT, LXT2, VZT, GHW, AET2, IDX, FST, VPD, WLF e FSDB.

A Figura 5.1 mostra a janela principal do GTKWave com formas de onda da simulação da função 'Fornecer Tempo de Bordo'.

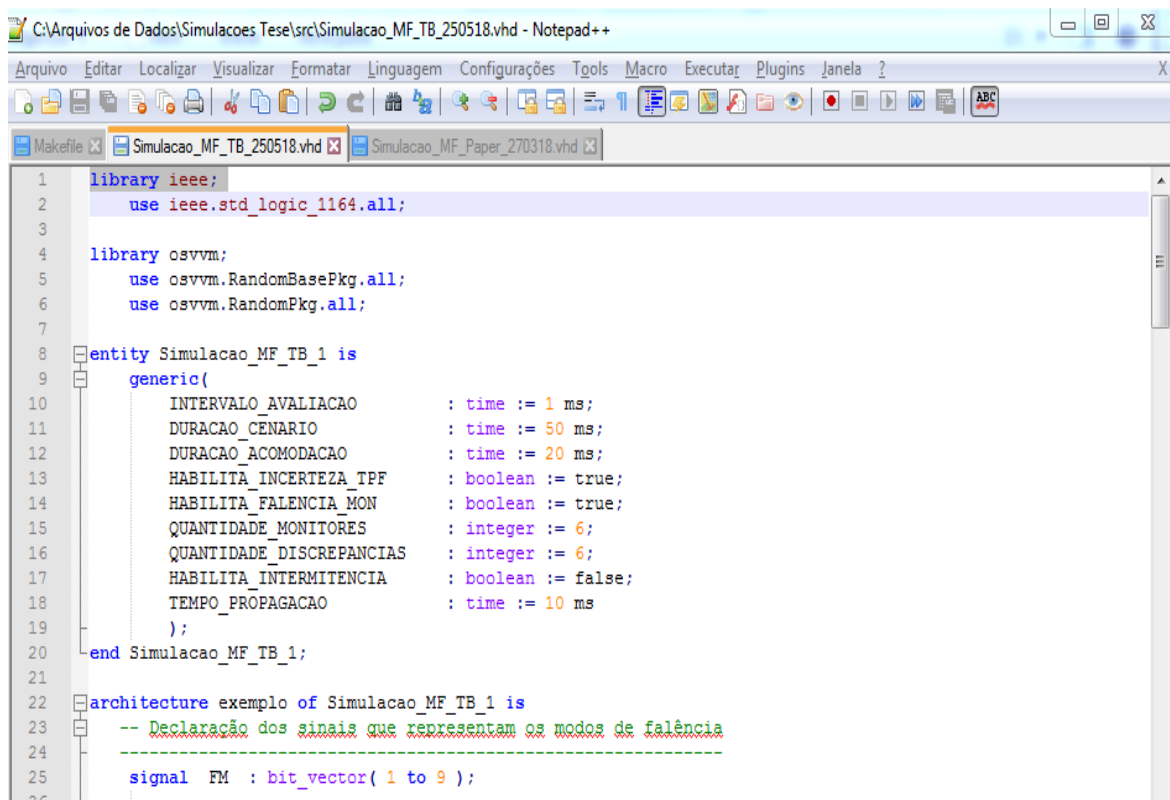
Figura 5.1 – Janela principal do GTKWave com formas de onda da simulação da função ‘Fornecer Tempo de Bordo’.



5.1.3 Notepad++

Notepad++ (<https://notepad-plus-plus.org/>) é um editor de código fonte que suporta 82 linguagens, entre as quais o VHDL e o Makefile. O Notepad++ executa em ambiente Windows. A Figura 5.2 apresenta janela do Notepad++ com trecho inicial do código VHDL da simulação da função ‘Fornecer Tempo de Bordo’.

Figura 5.2 – Janela do Notepad++ com trecho inicial do código VHDL da simulação da função ‘Fornecer Tempo de Bordo’.



```
1 library ieee;
2   use ieee.std_logic_1164.all;
3
4 library osvvm;
5   use osvvm.RandomBasePkg.all;
6   use osvvm.RandomPkg.all;
7
8 entity Simulacao_MF_TB_1 is
9   generic(
10      INTERVALO_AVALIACAO      : time := 1 ms;
11      DURACAO_CENARIO          : time := 50 ms;
12      DURACAO_ACOMODACAO      : time := 20 ms;
13      HABILITA_INCERTEZA_TPF   : boolean := true;
14      HABILITA_FALENCIA_MON    : boolean := true;
15      QUANTIDADE_MONITORES     : integer := 6;
16      QUANTIDADE_DISCREPANCIAS : integer := 6;
17      HABILITA_INTERMITENCIA   : boolean := false;
18      TEMPO_PROPAGACAO        : time := 10 ms
19   );
20 end Simulacao_MF_TB_1;
21
22 architecture exemplo of Simulacao_MF_TB_1 is
23   -- Declaração dos sinais que representam os modos de falência
24   -----
25   signal FM : bit_vector( 1 to 9 );
26
```

5.1.4 GNU Make

O utilitário GNU Make automaticamente determina quais as partes de um programa devem ser recompiladas e executa comandos para sua recompilação (<https://www.gnu.org/software/make/manual/make.html#Overview>). A ferramenta é utilizada para automatizar por meio de um arquivo Makefile as operações de Análise, Elaboração e Execução do simulador GHDL.

5.2 Principais Características do Simulador das Lógicas de Detecção e Diagnose

O simulador utilizado neste trabalho para avaliação do desempenho das lógicas propostas permite:

- Definir a quantidade de cenários simulados;

- Definir os tempos de propagação ou escolher aleatoriamente o tempo no intervalo de propagação;
- Definir o modo de falência ou escolher aleatoriamente a falência que será injetada;
- Simular falência de monitores, definindo os monitores falidos, os seus modos de falência e o tempo de ocorrência da falência ou escolhendo aleatoriamente tanto os monitores falidos quanto os seus modos de falência e os tempos de ocorrência das falências.

5.3 Resultados das Simulações

Nesta seção são apresentados os resultados das simulações das lógicas usadas para detecção e diagnose da função 'Fornecer Tempo de Bordo' e do caso da literatura, ou seja, a diagnose por diferença de assinaturas, a diagnose por biunivocidade e a diagnose por biunivocidade e precedência.

Para a função 'Fornecer Tempo de Bordo', as lógicas foram aplicadas a cada ocorrência de uma nova discrepância. Para o caso da literatura, as lógicas foram aplicadas periodicamente, a cada segundo.

Adicionalmente, como referência, a lógica para diagnose por diferença de assinaturas foi aplicada após o tempo máximo de propagação dos modos de falência previsto para cada uma das funções. Para a função 'Fornecer Tempo de Bordo', o tempo é contado a partir da ocorrência da primeira discrepância. Para o caso da literatura, o tempo é contado a partir da primeira amostragem da assinatura, ou seja, um segundo após o início da simulação.

Para cada combinação do número de falência de monitores e do valor da diferença entre assinaturas são simulados 1000 cenários, onde é aplicada a lógica de diagnose que está sendo validada. Em cada cenário, o modo de falência ativo e os tempos de propagação do modo de falência são escolhidos aleatoriamente.

Quando é admitida a falência de um ou dois monitores, o(s) monitor(es) falido(s) e o(s) seu(s) modo(s) de falência são escolhidos aleatoriamente. As falências dos monitores se manifestam, no entanto, sempre no início da simulação.

5.3.1 Resultados da Simulação da Função ‘Fornecer Tempo de Bordo’

As tabelas 5.1, 5.2 e 5.3 apresentam, respectivamente, os resultados das simulações realizadas para as lógicas por diferença de assinaturas, por biunivocidade e por biunivocidade e precedência propostas na secção 3.3.5. A Tabela 5.4 apresenta o resultado das simulações da aplicação da lógica por diferença de assinaturas após a propagação das falências.

Tabela 5.1 – Resultados das simulações da lógica proposta para a diagnose por diferença de assinaturas e detecção por eventos.

Falência de Monitores	Diferença entre Assinaturas	Identificações Corretas	Identificações Ambíguas	Não Identificadas	Identificações Incorretas	Tempo Máximo (seg)	Tempo Mínimo (seg)	Tempo Médio (seg)
0	0	1000	0	0	0	9	2	3
0	1	1000	0	0	0	9	2	3
0	2	0	1000	0	0	-	-	-
1	0	397	0	25	578	9	0	3
1	1	397	25	0	578	9	0	3
1	2	74	923	0	3	9	2	5
2	0	176	0	186	638	9	0	2
2	1	209	63	98	630	9	0	2
2	2	74	923	0	3	9	2	4

Tabela 5.2 – Resultados das simulações da lógica proposta para a diagnose por biunivocidade e detecção por eventos.

Falência de Monitores	Diferença entre Assinaturas	Identificações Corretas	Identificações Ambíguas	Não Identificadas	Identificações Incorretas	Tempo Máximo (seg)	Tempo Mínimo (seg)	Tempo Médio (seg)
0	0	269	731	0	0	2	2	2
0	1	269	731	0	0	9	2	5
0	2	0	1000	0	0	-	-	-
1	0	186	367	241	206	9	0	2
1	1	188	737	0	75	9	0	3
1	2	74	923	0	3	9	2	5
2	0	150	243	317	290	9	0	2
2	1	152	628	10	210	9	0	3
2	2	74	923	0	3	9	2	4

Tabela 5.3 – Resultados das simulações da lógica proposta para a diagnose por biunivocidade e verificação de precedência e detecção por eventos.

Falência de Monitores	Diferença entre Assinaturas	Identificações Corretas	Identificações Ambíguas	Não Identificadas	Identificações Incorretas	Tempo Máximo (seg)	Tempo Mínimo (seg)	Tempo Médio (seg)
0	0	269	731	0	0	2	2	2
0	1	269	731	0	0	9	2	5
0	2	0	1000	0	0	-	-	-
1	0	186	367	241	206	9	0	2
1	1	188	737	0	75	9	0	3
1	2	74	923	0	3	9	2	5
2	0	150	243	317	290	9	0	2
2	1	152	628	10	210	9	0	3
2	2	74	923	0	3	9	2	4

Tabela 5.4 – Resultados das simulações da lógica proposta para a diagnose por diferença de assinaturas aplicada após a propagação das falências e detecção por eventos.

Falência de Monitores	Diferença entre Assinaturas	Identificações Corretas	Identificações Ambíguas	Não Identificadas	Identificações Incorretas	Tempo Máximo (seg)	Tempo Mínimo (seg)	Tempo Médio (seg)
0	0	1000	0	0	0	18	10	11
0	1	1000	0	0	0	18	10	11
0	2	0	1000	0	0	-	-	-
1	0	444	0	496	60	18	10	11
1	1	515	425	0	60	18	10	11
1	2	71	869	0	60	10	10	10
2	0	224	0	650	126	18	10	11
2	1	284	449	141	126	18	10	10
2	2	70	864	0	66	10	10	10

5.3.2 Resultados das Simulações de um Caso da Literatura

As tabelas 5.5, 5.6 e 5.7 apresentam, respectivamente, os resultados das simulações realizadas para as lógicas por diferença de assinaturas, por biunivocidade e por biunivocidade e precedência propostas na secção 3.3.5 aplicadas a um caso da literatura. Como referência, a Tabela 5.8 apresenta o resultado das simulações da aplicação da lógica por diferença de assinaturas após a propagação das falências.

Tabela 5.5 – Resultados das simulações da lógica proposta para a diagnose por diferença de assinaturas e detecção por amostragem periódica.

Falência de Monitores	Diferença entre Assinaturas	Identificações Corretas	Identificações Ambíguas	Não Identificadas	Identificações Incorretas	Tempo Máximo (seg)	Tempo Mínimo (seg)	Tempo Médio (seg)
0	0	1000	0	0	0	18	7	12
0	1	1000	0	0	0	16	6	10
0	2	1000	0	0	0	15	5	8
1	0	464	0	536	0	19	6	11
1	1	999	0	0	1	18	5	11
1	2	888	13	0	99	17	1	9
2	0	248	0	752	0	18	5	11
2	1	718	0	261	21	18	1	11
2	2	850	23	0	127	18	1	9

Tabela 5.6 – Resultados das simulações da lógica proposta para a diagnose por biunivocidade e detecção por amostragem periódica.

Falência de Monitores	Diferença entre Assinaturas	Identificações Corretas	Identificações Ambíguas	Não Identificadas	Identificações Incorretas	Tempo Máximo (seg)	Tempo Mínimo (seg)	Tempo Médio (seg)
0	0	743	257	0	0	6	2	3
0	1	507	493	0	0	12	4	6
0	2	263	737	0	0	14	6	10
1	0	541	190	55	214	11	1	3
1	1	510	490	0	0	14	3	6
1	2	253	747	0	0	14	5	9
2	0	400	153	161	286	12	1	3
2	1	477	449	14	60	13	1	6
2	2	227	773	0	0	14	4	8

Tabela 5.7 – Resultados das simulações da lógica proposta para a diagnose por biunivocidade e verificação de precedência e detecção por amostragem periódica.

Falência de Monitores	Diferença entre Assinaturas	Identificações Corretas	Identificações Ambíguas	Não Identificadas	Identificações Incorretas	Tempo Máximo (seg)	Tempo Mínimo (seg)	Tempo Médio (seg)
0	0	1000	0	0	0	7	2	4
0	1	1000	0	0	0	12	3	7
0	2	1000	0	0	0	15	5	9
1	0	674	0	184	142	14	1	4
1	1	779	24	61	136	14	1	6
1	2	727	53	44	176	15	1	8
2	0	471	0	351	178	13	1	5
2	1	628	30	126	216	13	1	6
2	2	595	74	78	253	15	1	8

Tabela 5.8 – Resultados das simulações da lógica proposta para a diagnose por diferença de assinaturas aplicada após a propagação das falências e detecção por amostragem periódica.

Falência de Monitores	Diferença entre Assinaturas	Identificações Corretas	Identificações Ambíguas	Não Identificadas	Identificações Incorretas	Tempo Máximo (seg)	Tempo Mínimo (seg)	Tempo Médio (seg)
0	0	1000	0	0	0	23	22	23
0	1	1000	0	0	0	23	22	23
0	2	1000	0	0	0	23	22	23
1	0	464	0	536	0	23	22	23
1	1	1000	0	0	0	23	22	23
1	2	936	64	0	0	23	22	23
2	0	248	0	752	0	23	22	23
2	1	728	0	263	9	23	22	23
2	2	910	90	0	0	23	22	23

5.4 Análise dos Resultados das Simulações

5.4.1 Análise dos Resultados Obtidos para a Função ‘Fornecer Tempo de Bordo’

Com base nos resultados apresentados na seção 5.3.1, a Tabela 5.9 apresenta um sumário da porcentagem de identificações corretas realizadas pelas lógicas de diagnose simuladas. Na Tabela 5.10 é apresentado um sumário dos tempos médios para as identificações corretas.

Tabela 5.9 – Sumário dos resultados corretos da diagnose da função ‘Fornecer Tempo de Bordo’.

Condições da Simulação		Identificações Corretas (%)			
Quantidade de Monitores Falidos	Valor da Diferença entre Assinaturas	Diagnose por Diferença de Assinatura após Propagação	Diagnose por Diferença de Assinaturas	Diagnose por Biunivocidade	Diagnose por Biunivocidade e Verificação de Precedência
0	0	100	100	26,9	26,9
0	1	100	100	26,9	26,9
0	2	0	0	0	0
1	0	44,4	0	18,6	18,6
1	1	51,5	39,7	18,8	18,8
1	2	7,1	7,4	7,4	7,4
2	0	22,4	17,6	15	15
2	1	28,4	20,9	15,2	15,2
2	2	7	7,4	7,4	7,4

A seguir são analisados os resultados com base no número de monitores falidos, ou seja, nenhum monitor falido, um monitor falido e dois monitores falidos.

Tabela 5.10 – Sumário dos tempos médios necessários para a diagnose correta da função ‘Fornecer Tempo de Bordo’ pelas lógicas propostas.

Condições da Simulação		Tempo Médio para Identificações Corretas (seg)			
Quantidade de Monitores Falidos	Valor da Diferença entre Assinaturas	Diagnose por Diferença de Assinatura após Propagação	Diagnose por Diferença de Assinaturas	Diagnose por Biunivocidade	Diagnose por Biunivocidade e Verificação de Precedência
0	0	11	3	2	2
0	1	11	3	5	5
0	2	-	-	-	-
1	0	11		2	2
1	1	11	3	3	3
1	2	10	5	5	5
2	0	11	2	2	2
2	1	10	2	3	3
2	2	10	4	4	4

5.4.1.1 Nenhuma Falência de Monitor

A Figura 5.3 apresenta de forma gráfica o sumário da porcentagem de identificações corretas quando nenhum dos monitores apresenta falência. Quando não existe falência de monitores, a diagnose por diferença de assinaturas aplicada após a propagação dos modos de falência ou aplicada a cada evento identificam corretamente todos os modos de falência quando o valor da diferença entre a assinatura observada e as assinaturas previstas é 0 ou 1 e não identificam corretamente os modos de falência quando o valor da diferença é 2. A diagnose por biunivocidade e a diagnose por biunivocidade e precedência identificam corretamente os modos de falência em 26,9% das simulações quando o valor da diferença entre as assinaturas previstas e observada é 0 ou 1 e também não identificam corretamente os modos de falência quando o valor da diferença é 2.

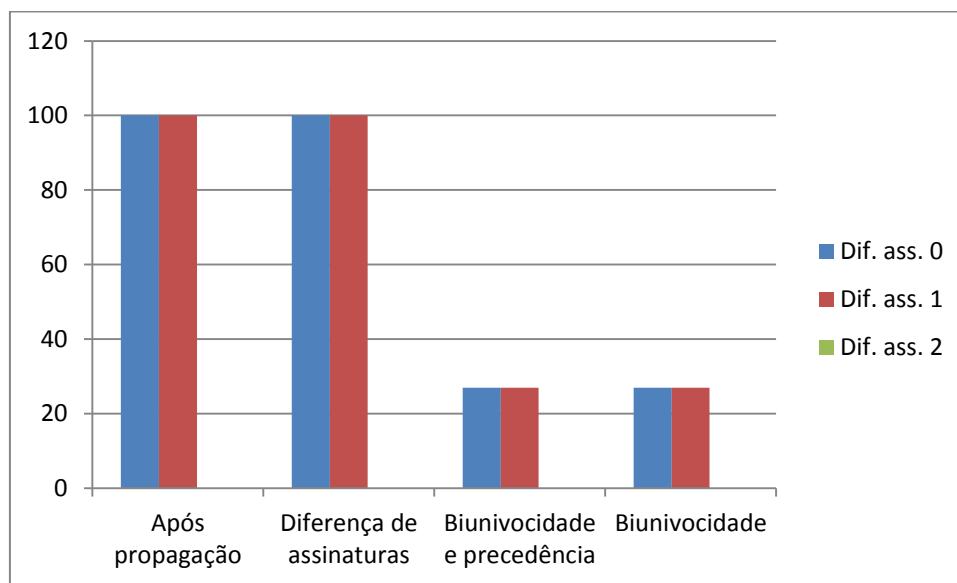
Conforme os resultados apresentados na seção 5.3.1, todos os casos não identificados corretamente foram identificados como ambíguos. Esse

comportamento é explicado pelo fato de que para uma diferença de 2 entre as assinaturas dos modos de falência (Tabela 4.5) e a assinatura observada sempre haverá no mínimo dois candidatos a modo de falência ativo.

A diagnose por biunivocidade e a diagnose por biunivocidade e precedência identificam corretamente aproximadamente 25% dos casos devido a aproximadamente 75% das assinaturas estarem contidas em *MF1* ou *MF2*, conforme Tabela 4.5

A diagnose por biunivocidade e a diagnose por biunivocidade e precedência identificam corretamente o mesmo número de modos de falência devido à inexistência de discrepâncias precedentes na assinatura.

Figura 5.3 – Sumário dos resultados corretos da diagnose da função ‘Fornecer Tempo de Bordo’ quando nenhum dos monitores apresenta falência.



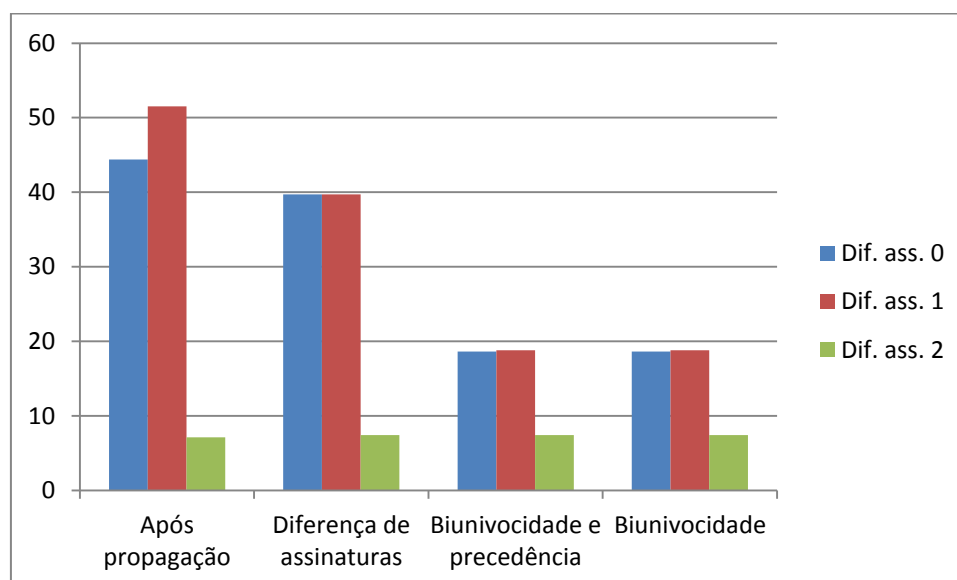
Conforme sumário dos tempos médios para identificações corretas apresentado na Tabela 5.10, a diagnose por biunivocidade e a diagnose por biunivocidade e precedência identificam corretamente no menor tempo médio os modos de falência quando o valor da diferença entre assinaturas é 0 enquanto a diagnose por diferença de assinaturas identifica corretamente os no menor tempo médio quando o valor da diferença entre assinaturas é 1.

5.4.1.2 Uma Falência de Monitor

A Figura 5.4 apresenta de forma gráfica o sumário da porcentagem de identificações corretas quando um dos monitores apresenta falência. Quando ocorre a falência de um monitor, à exceção dos casos em que a diferença de assinatura é 2, a quantidade de identificações corretas cai entre 30% e 60% quando comparado a ausência de falência de monitores. Conforme previsto na seção 3.3.5.1, a queda é menor quando a diferença entre as assinaturas previstas e observada é diferente de 0.

Diferentemente do que ocorre no caso anterior (nenhuma falência de monitor), a falência de um monitor permite identificar corretamente modos de falência quando a diferença aceitável entre as assinaturas previstas e observada é 2. Nesse caso, a ocorrência de um falso positivo (numa posição inativa) em *MF1* ou *MF2* aumenta a diferença entre as assinaturas (Tabela 4.5), fazendo com que a diferença entre *MF1* (ou *MF2*) e *MF2* (ou *MF1*) e os demais modos de falência seja maior do que 2.

Figura 5.4 – Sumário dos resultados corretos da diagnose da função ‘Fornecer Tempo de Bordo’ quando um dos monitores apresenta falência.



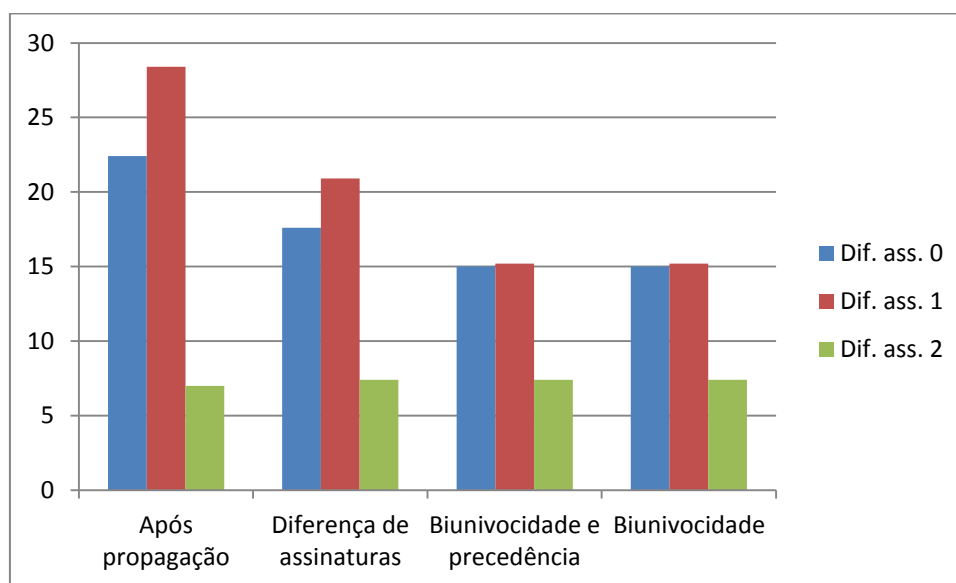
Da mesma forma que ocorre para nenhuma falência de monitor, a diagnose por biunivocidade e a diagnose por biunivocidade e precedência para uma falência

de monitor identificam corretamente o mesmo número de modos de falência devido à inexistência de discrepâncias precedentes na assinatura.

5.4.1.3 Duas Falências de Monitor

A Figura 5.5 apresenta de forma gráfica o sumário da porcentagem de identificações corretas quando dois dos monitores apresentam falência. Quando ocorre a falência de dois monitores, à exceção dos casos em que a diferença de assinatura é 2, a quantidade de identificações corretas cai entre 19% e 56% quando comparado a uma falência de monitor. Conforme previsto na seção 3.3.5.1, a queda é menor quando a diferença entre as assinaturas previstas e observada é diferente de 0.

Figura 5.5 – Sumário dos resultados corretos da diagnose da função ‘Fornecer Tempo de Bordo’ quando dois dos monitores apresentam falência.



Nos casos em que a diferença de assinatura é 2, a quantidade de identificações corretas não se altera quando comparado com a falência de um monitor. Nesse caso, a ocorrência de um falso positivo (numa posição inativa) e um falso negativo (numa posição inativa) em *MF1* ou em *MF2* aumenta a diferença entre as assinaturas (Tabela 4.5), fazendo com que a diferença entre *MF1* (ou *MF2*) e *MF2* (ou *MF1*) e os demais modos de falência seja maior do que 2.

Da mesma forma que ocorre para nenhuma falência de monitor, a diagnose por biunivocidade e a diagnose por biunivocidade e precedência para uma falência de monitor identificam corretamente o mesmo número de modos de falência devido à inexistência de discrepâncias precedentes na assinatura.

5.4.2 Análise dos Resultados Obtidos para o Caso da Literatura

Com base nos resultados apresentados na seção 5.3.2, a Tabela 5.11 apresenta um sumário da porcentagem de identificações corretas realizadas pelas lógicas de diagnose simuladas. Na Tabela 5.12 é apresentado um sumário dos tempos médios para as identificações corretas.

Tabela 5.11 – Sumário dos resultados corretos da diagnose do caso da literatura.

Condições da Simulação		Identificações Corretas (%)			
Quantidade de Monitores Falidos	Valor da Diferença entre Assinaturas	Diagnose por Diferença de Assinatura após Propagação	Diagnose por Diferença de Assinaturas	Diagnose por Biunivocidade	Diagnose por Biunivocidade e Verificação de Precedência
0	0	100,0	100,0	74,3	100,0
0	1	100,0	100,0	50,7	100,0
0	2	100,0	100,0	26,3	100,0
1	0	46,4	46,4	54,1	67,4
1	1	100,0	99,9	51,0	77,9
1	2	93,6	88,8	25,3	72,7
2	0	24,8	24,8	40,0	47,1
2	1	72,8	71,8	47,7	62,8
2	2	91,0	85,0	22,7	59,5

A seguir são analisados os resultados com base no número de monitores falidos, ou seja, nenhum monitor falido, um monitor falido e dois monitores falidos.

Tabela 5.12 – Sumário dos tempos médios necessários para a diagnose correta do caso da literatura pelas lógicas propostas.

Condições da Simulação		Tempo Médio para Identificações Corretas (seg)			
Quantidade de Monitores Falidos	Valor da Diferença entre Assinaturas	Diagnose por Diferença de Assinatura após Propagação	Diagnose por Diferença de Assinaturas	Diagnose por Biunivocidade	Diagnose por Biunivocidade e Verificação de Precedência
0	0	23	12	3	4
0	1	23	10	6	7
0	2	23	8	10	9
1	0	23	11	3	4
1	1	23	11	6	6
1	2	23	9	9	8
2	0	23	11	3	5
2	1	23	11	6	6
2	2	23	9	8	8

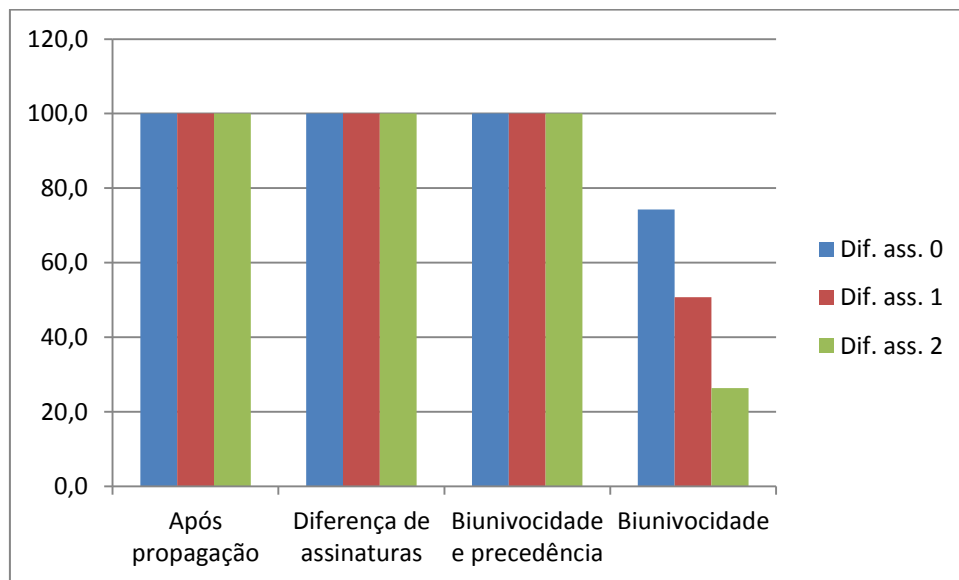
5.4.2.1 Nenhuma Falência de Monitor

A Figura 5.6 apresenta de forma gráfica o sumário da porcentagem de identificações corretas quando nenhum dos monitores apresenta falência. Quando não existe falência de monitores, a diagnose por diferença de assinaturas aplicada após a propagação dos modos de falência ou aplicada periodicamente e a diagnose por biunivocidade e precedência identificam corretamente os modos de falência em todas as simulações.

A diagnose por biunivocidade não identifica corretamente todos os modos de falência devido a *MF2* estar totalmente contido em *MF1*, como pode ser observado na Figura 4.17, resultando em ambiguidade na diagnose. A diagnose por biunivocidade identifica corretamente aproximadamente 74% dos casos quando a diferença de assinaturas é 0, caindo para aproximadamente 51% quando a diferença é 1 e 26% quando a diferença é 2. Esse comportamento é explicado pelo fato de que à medida que a diferença aceitável entre as assinaturas previstas e a assinatura observada aumenta,

também aumenta a probabilidade de uma assinatura observada estar contida em mais de uma assinatura prevista, aumentando a probabilidade de ambiguidade na diagnose. Os resultados da simulação da diagnose por biunivocidade apresentados na Tabela 5.6 confirmam que todos os modos de falência que não foram identificados corretamente por biunivocidade foram considerados ambiguos.

Figura 5.6 – Sumário dos resultados corretos da diagnose do caso da literatura quando nenhum dos monitores apresenta falência.



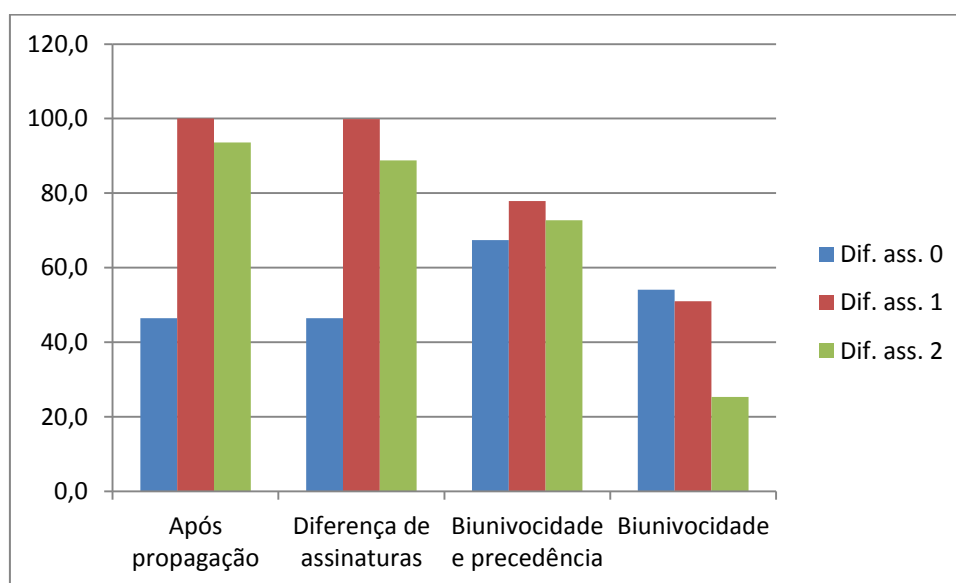
A diagnose por biunivocidade e a diagnose por biunivocidade e precedência são as que apresentam, na maior parte dos casos, o menor tempo para identificação correta dos modos de falência, conforme sumário dos tempos médios para identificações corretas apresentado na Tabela 5.12.

5.4.2.2 Uma Falência de Monitor

A Figura 5.7 apresenta de forma gráfica o sumário da porcentagem de identificações corretas quando um dos monitores apresenta falência. Para diferença entre assinaturas 0, as identificações corretas para a diagnose após a propagação e a diagnose por diferença de assinaturas (46,4% do total em cada caso) são atribuídas a ocorrência de falsos positivos para discrepâncias ativas e falsos negativos para discrepâncias inativas. O aumento da porcentagem de identificações corretas nas diagnoses por biunivocidade e por

biunivocidade e precedência deve-se a essas lógicas poderem realizar a identificação sem que sejam examinados todos os elementos da assinatura, ou seja, o monitor falido pode não ser examinado. O aumento de identificações corretas na diagnose por biunivocidade e precedência é ainda maior (67,4% contra 54,1%) devido à verificação de precedência permitir a eliminação de parte das ambiguidades.

Figura 5.7 – Sumário dos resultados corretos da diagnose do caso da literatura quando um dos monitores apresenta falência.



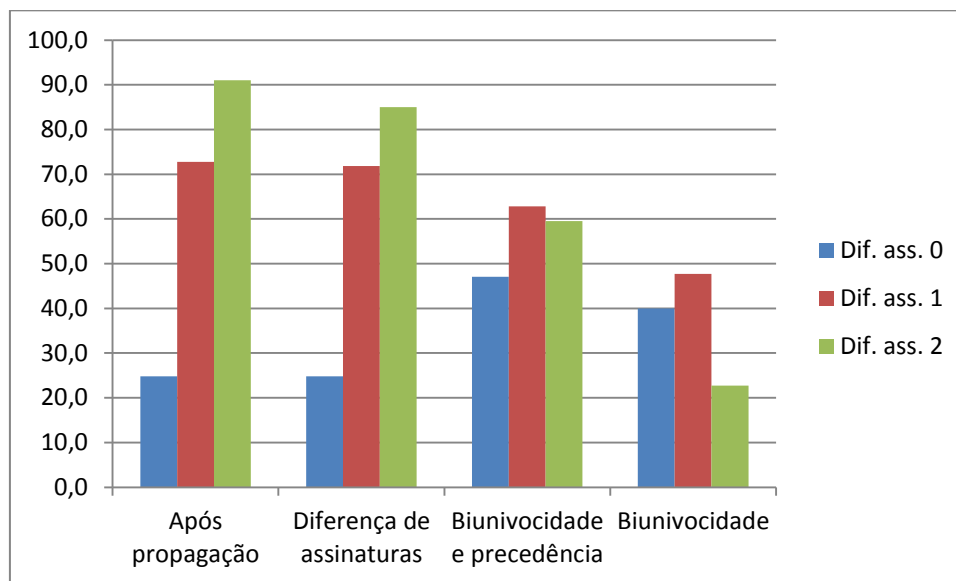
Para diferença entre assinaturas 1, as diagnoses após propagação e por diferença de assinaturas identificam corretamente 100% dos casos devido a diferença entre as assinaturas previstas ser no mínimo 3, ou seja, a diferença entre uma assinatura observada e uma das assinaturas previstas será de no máximo 1, permitindo a identificação correta. A diagnose por biunivocidade identifica corretamente 51% dos casos (os demais são âmbiguos) devido à combinação da realização da identificação sem que sejam examinados todos os elementos da assinatura com uma diferença aceitável entre assinaturas de 1. A diagnose por biunivocidade e precedência identifica corretamente 77,9% dos casos devido à verificação de precedência eliminar a maior parte das ambiguidades.

Para diferença entre assinaturas 2, a porcentagem de identificações corretas diminui quando comparado com as porcentagens atingidas para diferença entre assinaturas 1. O comportamento das lógicas é, no entanto, semelhante ao comportamento para diferença de 1.

5.4.2.3 Duas Falências de Monitor

A Figura 5.8 apresenta de forma gráfica o sumário da porcentagem de identificações corretas quando dois dos monitores apresentam falência. A porcentagem de identificações corretas com duas falências de monitores diminui em todas as situações simuladas quando comparada com a falência de um dos monitores. Chama a atenção neste caso, a porcentagem de identificações corretas pela diagnose após a propagação e a diagnose por diferença de assinaturas apresentarem melhores resultados quando a diferença entre as assinaturas é 2. Esse comportamento deve-se ao fato de que quando a diferença entre assinaturas é 0, a identificação correta somente ocorre quando as duas falências de monitores indicam o estado correto das discrepâncias aos quais estão associados, i.e., são atribuídas a ocorrência de falsos positivos para discrepâncias ativas e falsos negativos para discrepâncias inativas. Quando a diferença entre assinaturas é 1, basta que uma das falências de monitores indique o estado correto das discrepâncias aos quais estão associados e quando a diferença entre assinaturas é 2 não é necessário que nenhum dos monitores indique o estado correto das discrepâncias aos quais estão associados para que ocorra a identificação correta do modo de falência.

Figura 5.8 – Sumário dos resultados corretos da diagnose do caso da literatura quando dois dos monitores apresentam falência.



6 CONCLUSÕES

A luz das motivações mencionadas no capítulo 1, este trabalho teve como objetivo propor uma estratégia para tratamento de falhas sistêmicas (FDIR) em ACDHs de satélites de pequeno e médio porte. Essa estratégia é baseada na análise da arquitetura funcional - em detrimento da física - do satélite, o que permite adiantar o projeto do FDIR para o início da Fase B do ciclo de vida, quando ainda é possível que as considerações de FDIR tenham um impacto mais efetivo no projeto dos subsistemas e do satélite como um todo.

Para tanto, a arquitetura funcional do subsistema foi decomposta e os modos de falência mais significativos das funções, assim como suas causas e efeitos foram identificados por meio de uma FMEA funcional. O comportamento do sistema foi descrito por meio de um grafo temporizado e os efeitos monitoráveis foram identificados. Uma lógica inversa para a isolação e/ou identificação dos modos de falência ativos foi então definida com base: a) na compatibilidade dos mapas de Karnaugh de causa e efeito; b) na assinatura dos modos de falência no domínio espacial (generalizável).

A estratégia foi aplicada em um ACDH típico, que tem como referência o ACDH em desenvolvimento para a PMM e o satélite Amazônia. A arquitetura funcional do subsistema, definida com base nos documentos disponíveis, foi decomposta em doze funções e cada uma dessas funções foi decomposta em dois níveis funcionais. A estratégia foi aplicada na função 'Fornecer tempo de bordo' considerando os modos de falência 'Não fornece tempo de bordo' e 'Fornece tempo de bordo fora de especificação'. Algumas lógicas inversas para detecção e diagnose com base na assinatura espacial dos modos de falência foram propostas e simuladas em diferentes condições para avaliação de seu desempenho.

6.1 Contribuições

- 1) Levantamento bibliográfico abrangente e minucioso do tratamento de falhas em aplicações espaciais.

- 2) Proposta de uma abordagem funcional que pode ser aplicada nas fases iniciais de desenvolvimento, antecipando o tratamento de falhas sistêmicas da missão e permitindo a adoção de soluções que melhoram o FDIR, o que pode, de acordo com a literatura, aumentar a autonomia e facilitar o tratamento de falhas em sistemas complexos/altamente integrados.
- 3) Definição de uma lógica inversa para a isolação e/ou identificação dos modos de falência ativos com base: a) na compatibilidade dos mapas de Karnaugh de causa e efeito; b) na assinatura dos modos de falência no domínio espacial (generalizável para o domínio temporal e/ou domínio informacional).
- 4) Reinserção do tratamento de falhas em satélites como área de pesquisa no âmbito do Grupo de Supervisão de Bordo (SUBORD) da Divisão de Eletrônica Aeroespacial (DEA) do INPE.

6.2 Sugestões para Trabalhos Futuros

- 1) Expansão da generalização da diagnose de falências considerando:
 - i) As combinações de compatibilidade de mapas;
 - ii) As assinaturas no domínio temporal e no domínio informacional;
 - iii) O acionamento das lógicas de diagnose por eventos e/ou por tempo;
 - iv) Outros modos de falência dos monitores;
- 2) Otimização do tempo de diagnose (minimização do tempo necessário para isolação e/ou identificação) por meio de tratamento que considere além do domínio espacial as manifestações dos modos de falência no domínio temporal e/ou no domínio informacional.
- 3) Robustecimento da abordagem por Modelagem e Simulação por meio de testes das lógicas algorítmicas em cenários que compreendam:

- i) Ocorrência de um único modo de falência, discrepâncias parcialmente monitoradas, ausência de falência de sensores, inexistência de ruídos ou de incertezas no tempo e na informação;
- ii) Ocorrência de um único modo de falência, discrepâncias parcialmente monitoradas, falência de um dos sensores, inexistência de ruídos ou de incertezas no tempo e na informação;
- iii) Ocorrência de um único modo de falência, discrepâncias parcialmente monitoradas, falência de dois dos sensores, inexistência de ruídos ou de incertezas no tempo e na informação;
- iv) Ocorrência de mais de um modo de falência, discrepâncias parcialmente monitoradas, falência de um dos sensores, inexistência de ruídos ou de incertezas no tempo e na informação.

REFERÊNCIAS BIBLIOGRÁFICAS

- ABDELWAHED, S.; KARSAI, G. Notions of diagnosability for timed failure propagation graphs. In: AUTOTESTCON, 2006, Anaheim, CA, USA. **Proceedings...** IEEE, 2006. DOI: 10.1109/AUTEST.2006.283740. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4062453>. Acesso em: 22 mar. 2017.
- ABDELWAHED, S.; KARSAI, G.; BISWAS, G. A consistency-based robust diagnosis approach for temporal causal systems. In: INTERNATIONAL WORKSHOP ON PRINCIPLES OF DIAGNOSIS, 16., 2005. **Proceedings...** Disponível em: <https://semanticolístico/b1cd/a6bd7899e80bb43cd8946ae4a1ccd8f38182.pdf>. Acesso em: 19 out. 2017.
- ALANA, E.; NARANJO, H.; YUSHTEIN, Y.; BOZZANO, M.; CIMATTI, A.; GARIO, M.; FERLUC, R.; GARCIA, G. Automated generation of FDIR for the compass integrated toolset (AUTOGEF). In: DATA SYSTEMS IN AEROSPACE CONFERENCE (DASIA), 2012, Dubrovnik, Croatia. **Proceedings...** Disponível em: <https://es-static.fbk.eu/people/bozzano/publications/dasia2012.pdf>. Acesso em: 30 dez. 2016.
- ALONSO, J. D.D. **Guia para padronização do desenvolvimento de software crítico para aplicações espaciais**. Dissertação (Mestrado em Engenharia Eletrônica e Computação) - Instituto Tecnológico da Aeronautica (ITA), São José dos Campos, 1998.
- AMARAL, J. C. **Análise, projeto e simulação de uma arquitetura de controle reconfigurável para a plataforma multi-missão**. 2009. 149p. (INPE-15682-TDI/1456). Dissertação (Mestrado em Engenharia e Tecnologia Espaciais / Mecânica Espacial e Controle) - Instituto Nacional de Pesquisas Espaciais (INPE), São José dos Campos, 2009.
- AMARAL, J. C. **Estudo dos efeitos da reconfiguração sobre o transitório e a estabilidade de sistemas de controle reconfiguráveis**. 2013. 172p. (sid.inpe.br/mtc-m19/2013/07.25.18.55-TDI). Tese (Doutorado em Engenharia e Tecnologia Espaciais / Mecânica Espacial e Controle) - Instituto Nacional de Pesquisas Espaciais (INPE), São José dos Campos, 2013. Disponível em: <http://urlib.net/8JMKD3MGP7W/3EGT738>.
- ARIAS, R. **Estudo do uso de roteamento dinâmico de mensagens em sistemas computacionais tolerantes a falhas baseados em transputers**. Dissertação (Mestrado em Engenharia Eletrônica e Computação) - Instituto Tecnológico da Aeronautica (ITA), São José dos Campos, 1999.
- ARIAS, R. **Um framework de simulação para verificação de requisitos de desempenho de sistemas computacionais de tempo real**. Tese (Doutorado em Engenharia Eletrônica e Computação) - Instituto Tecnológico da Aeronautica (ITA), São José dos Campos, 2012.

ARMELIN, F. B. **Biblioteca de componentes para síntese do protocolo de sincronização e codificação de canal de telemetria recomendado pelo CCSDS**. Dissertação (Mestrado em Engenharia Eletrônica e Computação) - Instituto Tecnológico da Aeronáutica (ITA), São José dos Campos, 2010.

AVIZIENIS, A.; LAPRIE, J-C; RANDELL, B; LANDWEHR, C. Basic concepts and taxonomy of dependable and secure computing. **IEEE Transactions on Dependable and Secure Computing**, v. 1, n. 1, p. 11-33, jan./mar. 2004.

BAK, T.; WISNIEWSKI, R.; BLANKE, M. Autonomous attitude determination and control system for the Ørsted satellite. In: AEROSPACE APPLICATIONS CONFERENCE, 1996, Aspen, USA. **Proceedings ...** DOI: 10.1109/AERO.1996.495975. Disponível em: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=495975&tag=1. Acesso em: 28 dez. 2015.

BERGET, R. T. Command and data handling. In: LARSON, W. J.; WERTZ, J. R. (Eds.). **Space mission engineering**. 3.ed. El Segundo, CA, USA: Microcosm Press, 2005.

BITTNER, B.; BOZZANO, M.; CIMATTI, A.; DE FERLUC, R.; GARIO, M.; GUIOTTO, A.; YUSHTEIN, Y. An integrated process for FDIR design in aerospace. In: ORTMEIER, F.; RAUZY, A. (Eds.). **Model based safety and assessment**. Berlin: Springer, 2014. Disponível em: <https://es-static.fbk.eu/people/bozzano/publications/imbsa2014b.pdf>. Acesso em: 28 abr. 2016.

BITTNER, B.; BOZZANO, M.; CIMATTI, A. Timed failure propagation analysis for spacecraft engineering: the ESA solar orbiter case study. In: BOZZANO, M.; PAPADOPOULOS, Y. (Eds.). **Model based safety and assessment**. Berlin: Springer, 2017. p.255-271. Disponível em: https://www.researchgate.net/publication/318841253_Timed_Failure_Propagation_Analysis_for_Spacecraft_Engineering_The_ESA_Solar_Orbiter_Case_Study. Acesso em: 20 out. 2017.

BØGH, S. A.; BLANKE, M. **Fault-tolerant control - a case study of the Ørsted satellite**. 1997. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=643169>. Acesso em: 06 ago. 2015.

BOURICIUS, W. G.; CARTER, W. G.; SCHNEIDER, P. R. Reliability modeling techniques for self-repairing computer systems. In: ACM NATIONAL CONFERENCE, 24, 1969, New York, NY, USA. **Proceeding ...** p. 295-309. DOI: 10.1145/800195.805940. Disponível em: http://delivery.acm.org/10.1145/810000/805940/p295-bouricius.pdf?ip=150.163.30.28&id=805940&acc=ACTIVE%20SERVICE&key=344E943C9DC262BB%2E84DA360D213EE7B4%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&CFID=721557729&CFTOKEN=31634618&_acm_=1485550830_7718c834fdc28789bdc786206b340ae5. Acesso em: 27 jan. 2017.

BOS, J.F.T.; ZORITA, D.; BACCHETTA, A.; CHLEWICKI, G.; GUICHON, D.; RASMUSSEN, I. ACMS FDIR system for the Herschel / Planck satellites. In: INTERNATIONAL ESA CONFERENCE ON GUIDANCE, NAVIGATION AND CONTROL SYSTEMS, 6., 2006, Loutraki, Greece. **Proceedings...** Disponível em: http://articles.adsabs.harvard.edu/cgi-bin/nph-article_query?2006ESASP.606E..36B&defaultprint=YES&page_ind=0&filetype=.pdf. Acesso em: 17 set. 2015.

BROOKS, P. TOPSAT: high resolution imaging from a small satellite. In: ANNUAL / USU CONFERENCE ON SMALL SATELLITES, 15., 2001, Logan, USA. **Proceedings...** Disponível em: <http://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=1956&context=smallsat>. Acesso em: 01 set. 2015.

BROWN, T. K.; DONALDSON, J. A. Fault protection design of the command and data subsystem on the Cassini spacecraft. In: AIAA / IEEE DIGITAL AVIONICS SYSTEMS CONFERENCE (DASC), 13., 1994, Phoenix, USA. **Proceedings...** 1994. p. 408-413. Disponível em: <http://trs-new.jpl.nasa.gov/dspace/bitstream/2014/33236/1/94-1172.pdf>. Acesso em: 19 ago. 2015.

BSI. **GTKWave 3.3 Wave analyzer user's guide**. 2018. Disponível em: <http://gtkwave.sourceforge.net/gtkwave.pdf>. Acesso em: 26 dez. 2018.

BURGE, S. **Functional failure modes and effects analysis alias system FMEA**. 2010. Disponível em: <http://www.burgehugheswalsh.co.uk/uploaded/1/documents/ffmea-tool-box-v1.2.pdf>. Acesso em: 09 mai. 2016.

CAPÓ-LUGO, P. A.; BAINUM, P. M. **Orbital mechanics and formation flying: a digital control perspective**. Cambridge, UK: Woodhead Publishing Limited, 2011. 438p. Disponível em: <https://books.google.com.br/books?id=GyJtAgAAQBAJ&printsec=copyright#v=onepage&q&f=false>. Acesso em: 14 ago. 2015.

CASTEL, C; GABARD, J-F; TESSIER, C; LABORDE, B; SOUMAGNE, R. **FDIR strategies for autonomous satellite formations - a preliminary report**. 2006. Disponível em: <https://www.aaai.org/Papers/Symposia/Fall/2006/FS-06-07/FS06-07-005.pdf>. Acesso em: 30 abr. 2015.

CAWLEY, S. TOPSAT: Low cost high resolution imagery from space. In: IAA SYMPOSIUM ON SMALL SATELLITES FOR EARTH OBSERVATION, 4., 2003, Berlin, Germany. **Proceedings...** Disponível em: <http://www.dlr.de/Portaldata/49/Resources/dokumente/archiv4/IAA-B4-0801.pdf>. Acesso em: 01 set. 2015.

CODETTA-RAITERI, D.; PORTINALE, L. **ARPHA: an FDIR architecture for autonomous spacecrafts based on dynamic probabilistic graphical models**. Alessandria, Italy: Dipartimento di Informatica Università del Piemonte Orientale

“A. Avogadro”, 2010. 24p. (Technical report tr-inf-2010-12-04-unipmn). Disponível em: <http://www.di.unipmn.it/TechnicalReports/TR-INF-2010-12-04-UNIPMN.pdf>. Acesso em: 26 out. 2015.

CODETTA-RAITERI, D.; PORTINALE, L. Dynamic bayesian networks for fault detection, identification, and recovery in autonomous spacecraft. **IEEE Transactions on Systems, Man, and Cybernetics: Systems**. v. 45, n. 1, p. 13-24, 2015. DOI: 10.1109/TSMC.2014.2323212. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6823144>. Acesso em: 28 jul. 2015.

COLBURN, T; SHUTE, G. **Abstraction in computer science**. 2007. Disponível em: <https://www.d.umn.edu/~tcolburn/papers/Abstraction.pdf>. Acesso em: 07 mar. 2018.

CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEMS (CCSDS). **Time code formats**. 3.ed. Washington, USA: CCSDS Secretariat. 2002. 36p. CCSDS 301.0-B-3.

DENSON, W. **Reliability modeling: the RIAC guide to reliability prediction assessment and estimation**. Utica, USA: Reliability Information Analysis Center, 2010. 432p. (Technical report OMB No. 0704-0188). Disponível em: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.385.6682&rep=rep1&type=pdf>. Acesso em: 9 maio 2016.

DEPARTMENT OF DEFENSE (DOD) – SYSTEMS MANAGEMENT COLLEGE. **Systems engineering fundamentals**. Fort Belvoir, USA: Defense Acquisition University Press, 2001. 222p. Disponível em: https://ocw.mit.edu/courses/aeronautics-and-astronautics/16-885j-aircraft-systems-engineering-fall-2005/readings/sefguide_01_01.pdf. Acesso em: 21 dez. 2016.

DUBEY, A.; KARSAI, G.; MAHADEVAN, N. Model-based software health management for real-time systems. In: AEROSPACE CONFERENCE, 2011, Big Sky, USA. **Proceedings...** 2011, p. 1-18. DOI: 10.1109/AERO.2011.5747559. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5747559>. Acesso em: 19 out. 2017.

EICKHOFF, J. **Onboard computers, onboard software and satellite operations: an introduction**. Berlin, Germany: Springer-Verlag, 2012. 300p. CD-ROM.

EM ÓRBITA. **CBERS-4 colocado em órbita com sucesso**. 2014. Disponível em: <http://www.orbita.zenite.nu/cbers-4-colocado-em-orbita-com-sucesso/>. Acesso em: 09 set. 2015.

ENCYCLOPEDIA OF SCIENCE. **Satellite mass categories**. 2015. Disponível em:

http://www.daviddarling.info/encyclopedia/S/satellite_mass_categories.html.

Acesso em: 14 ago. 2015.

EOPORTAL. **IRS-P6**. 2015a Disponível em

<https://directory.eoportal.org/web/eoportal/satellite-missions/i/irs-p6>. Acesso em: 10 dez. 2015.

EOPORTAL. **FormoSat-2**. 2015b. Disponível em

<https://directory.eoportal.org/web/eoportal/satellite-missions/f/formosat-2>.

Acesso em: 10 dez. 2015.

EUROPEAN COOPERATION FOR SPACE STANDARDIZATION (ECSS).

Space engineering space segment operability. 2.ed. Noordwijk, The Netherlands: ESA Requirements and Standards Division, 2008. 76p. (ECSS-E-ST-70-11C).

EUROPEAN COOPERATION FOR SPACE STANDARDIZATION (ECSS).

Space product assurance failure modes, effects (and criticality) analysis (FMEA/FMECA). 2.ed. Noordwijk, The Netherlands: ESA Requirements and Standards Division, 2009a. 74p. (ECSS-Q-ST-30-02C).

EUROPEAN COOPERATION FOR SPACE STANDARDIZATION (ECSS).

Space project management project planning and implementation. 3.ed. Noordwijk, The Netherlands: ESA Requirements and Standards Division. 2009b. 50p. (ECSS-M-ST-10C Rev. 1).

EUROPEAN COOPERATION FOR SPACE STANDARDIZATION (ECSS).

Glossary of terms. 3.ed. Noordwijk, The Netherlands: ESA Requirements and Standards Division. 2012. 63p. (ECSS-S-ST-00-01C).

EUROPEAN SPACE AGENCY (ESA). **Herschel and planck**. 2009. Disponível em:

http://www.esa.int/Our_Activities/Space_Science/Herschel_and_Planck.

Acesso em: 24 mar. 2016.

EVERETT, D. F. Overview of spacecraft design. In: WERTZ, J. R.; EVERETT, D. F.; PUSCHELL, J.J. (Eds.). **Space mission engineering: the new SMAD**.

Hawthorne, USA: Microcosm Press, 2011. ISBN 978-1-881-883-15-9.

FUQUA, N. B. The applicability of Markov analysis methods to reliability, maintainability, and safety. **START: Selected Topics in Assurance Related Technologies**, v.10, n. 2, p. 1-8, 2003. Disponível em:

<https://src.alionscience.com/pdf/MARKOV.pdf>. Acesso em: 21 set. 2016.

GAYARRE, L. P. **Um algoritmo de clusterização de dados para auxílio à análise de comportamentos de sistemas**. 2015. 157p. (sid.inpe.br/mtc-

m21b/2015/04.23.19.03-TDI). Tese (Doutorado em Engenharia e Tecnologia Espaciais / Mecânica Espacial e Controle) - Instituto Nacional de Pesquisas Espaciais (INPE), São José dos Campos, 2015. Disponível em:

<http://urlib.net/8JMKD3MGP3W34P/3JCFC22>.

GERMAN AEROSPACE CENTER (DLR). **TerraSAR-X - Germany's radar eye in space**. 2014a. Disponível em: http://www.dlr.de/dlr/en/desktopdefault.aspx/tabid-10377/565_read-436/#/gallery/350. Acesso em: 25 fev. 2016.

GERMAN AEROSPACE CENTER (DLR). **TanDEM-X - the Earth in three dimensions**. 2014b. Disponível em: http://www.dlr.de/dlr/en/desktopdefault.aspx/tabid-10377/565_read-436/#/gallery/350. Acesso em: 25 fev. 2016.

GESSNER, R.; KÖSTERS, B.; HEFLER, A.; EILENBERGER, R.; HARTMANN, J.; SCHMIDT, M. Hierarchical FDIR Concepts in S/C Systems. In: INTERNATIONAL CONFERENCE ON SPACE OPERATIONS (SPACEOPS), 8., 2004, Montreal, Canada. **Proceedings....** Disponível em: <http://arc.aiaa.org/doi/pdfplus/10.2514/6.2004-433-249>. Acesso em: 07 abr. 2015.

GINGOLD, TRISTAN. **GHDL documentation**. 2018. Disponível em: <https://media.readthedocs.org/pdf/ghdl/latest/ghdl.pdf>. Acesso em: 25 jan. 2018.

GLOBALSECURITY.ORG. **Zi Yuan CBERS (China-Brazil earth resources satellite)**. 2011. Disponível em: <http://www.globalsecurity.org/space/world/china/zy-1.htm>. Acesso em: 09 set. 2015.

GUIOTTO, A; MARTELLI, A.; PACCAGNINI, C.; LAVAGNA, M. SMART-FDIR: use of artificial intelligence in the implementation of a satellite FDIR. In: DATA SYSTEMS IN AEROSPACE CONFERENCE (DASIA), 2003, Prague, Czech Republic. **Proceedings....** Noordwijk, Netherlands: ESA Publications Division, 2003. Disponível em: <ftp://ftp.estec.esa.nl/pub/wm/anonymous/wme/Web/SmartFDIR2003.pdf>. Acesso em: 27 maio 2015.

HAYDEN, S.; OZA, N.; MAH, R.; MACKKEY, R.; NARASIMHAN, S.; KARSAL, G.; POLL, S.; DEB, S.; SHIRLEY, M. **Diagnostic technology evaluation report for on-board crew launch vehicle**. Hanover, USA: NASA Center for Aerospace Information, 2006. 48p. (NASA/TM-2006-214552). Disponível em: [https://ti.arc.nasa.gov/m/pub-archive/1218h/1218%20\(Hayden\).pdf](https://ti.arc.nasa.gov/m/pub-archive/1218h/1218%20(Hayden).pdf). Acesso em: 18 out. 2017.

HOLSTI, N.; PAAKKO, M. Towards advanced FDIR components. In: DATA SYSTEMS IN AEROSPACE CONFERENCE (DASIA), 2001. **Proceedings...** Disponível em: ftp://ftp.estec.esa.nl/pub/wm/anonymous/wme/Web/DASIA_2001_Towards%20Advanced%20FDIR%20Components.pdf. Acesso em: 16 abr. 2015.

INSTITUTO NACIONAL DE PESQUISAS ESPACIAIS (INPE). **Multi-mission platform Attitude Control and Data Handling (ACDH) subsystem**

specification. São José dos Campos, Brasil: INPE, 2001. 40p. (A828700-SPC-01/04).

INSTITUTO NACIONAL DE PESQUISAS ESPACIAIS (INPE). **Amazonia-1 satellite ACDH subsystem specification.** São José dos Campos, Brasil: INPE, 2010. 45p. (A12700-SPC-01 v02).

ISERMANN, R. **Fault-diagnosis systems:** an introduction from fault detection to fault tolerance. Heidelberg, Germany: Springer-Verlag, 2006. 475p. ISBN 978-3-540-30368-8.

INTERNATIONAL FEDERATION OF AUTOMATIC CONTROL (IFAC). **Terminology in the area of fault management.** Disponível em: <http://tc.ifac-control.org/6/4/terminology/terminology-in-the-area-of-fault-management>. Acesso em: 06 jan. 2017.

JIAXUE, L.; XIANG, Z. Detection method of intermittent faults in electronic systems based on markov model. In: INTERNATIONAL SYMPOSIUM ON COMPUTATIONAL INTELLIGENCE AND DESIGN. 4., 2011. Hangzhou, China. **Proceedings...** 2011, p216-219. DOI: 10.1109/ISCID.2011.62. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6079674>. Acesso em: 27 jun. 2017.

KRAMER, H. J.; CRACKNEL, A. P. An overview of small satellites in remote sensing. **International Journal of Remote Sensing**, v. 29, n. 15, p. 4285–4337, 2008. Disponível em: <http://www.tandfonline.com/doi/pdf/10.1080/01431160801914952>. Acesso em: 04 nov. 2015.

KUCINSKIS, F. N. **Alocação dinâmica de recursos computacionais para experimentos científicos com replanejamento automatizado a bordo de satélites.** 2007. 165 p. (INPE-14798-TDI/1241). Dissertação (Mestrado em Computação Aplicada) - Instituto Nacional de Pesquisas Espaciais, São José dos Campos, 2007. Disponível em: <http://urlib.net/sid.inpe.br/mtc-m17@80/2007/04.23.11.42>. Acesso em: 10 jan. 2017.

KUCINSKIS, F. N. **Uma arquitetura de software embarcado do segmento espacial para habilitar a operação de missões baseada em objetivos.** 2012. 166p. (sid.inpe.br/mtc-m19/2012/03.01.14.50-TDI). Tese (Doutorado em Engenharia e Tecnologia Espaciais) - Instituto Nacional de Pesquisas Espaciais (INPE), São José dos Campos, 2012. Disponível em: <http://urlib.net/8JMKD3MGP7W/3BEQBSP>.

LALA, J.; H.; HARPER, R. E. Architectural principles for safety-critical real-time applications. **Proceedings of the IEEE**, v. 82, n. 1, p. 25-40, 1994.

LAPRIE, J. C. Dependable computing and fault tolerance: concepts and terminology. In: INTERNATIONAL SYMPOSIUM ON FAULT TOLERANT COMPUTING (FTCS), 15., 1985, Ann Arbor, USA. **Proceedings...** 1985.

LEITE, A. C. **Detecção e diagnóstico de falhas em sensores e atuadores da plataforma multi-missão.** 2007. 372p. (INPE-15219-TDI/1313). Dissertação (Mestrado em Engenharia e Tecnologia Espaciais / Mecânica Espacial e Controle) - Instituto Nacional de Pesquisas Espaciais (INPE), São José dos Campos, 2007.

LEITE, A.C. **Detecção, diagnóstico e reconfiguração de falhas para o projeto otimizado de veículos espaciais seguros aplicados à PMM e a rovers planetários.** 2012. 137p. Tese (Doutorado em Engenharia e Tecnologia Espaciais / Mecânica Espacial e Controle) - Instituto Nacional de Pesquisas Espaciais (INPE), São José dos Campos, 2012.

LEMAI, S.; CHARMEAU, M; OLIVE, X. Decisional architecture for autonomous space systems. In: ESA WORKSHOP ON ADVANCED SPACE TECHNOLOGIES FOR ROBOTICS AND AUTOMATION (ASTRA 2006), 9., 2006, Noordwijk, The Netherlands. **Proceedings...** Disponível em: <http://robotics.estec.esa.int/ASTRA/Astra2006/Papers/ASTRA2006-1.3.1.01.pdf>. Acesso em: 06 jul. 2015.

MAHADEVAN, N.; ABDELWAHED, S.; DUBEY, A.; KARSAI, G. Distributed diagnosis of complex systems using timed failure propagation graph models. In: AUTOTESTCON, 2010, Orlando, USA. **Proceedings...** IEEE, 2010. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5613575>. Acesso em: 19 out. 2017.

MANELLI, H. N. **Estudo de requisitos e especificações para a tolerância a falha simples aplicados a sistemas de controle aeroespaciais.** (sid.inpe.br/mtc-m19/2011/02.28.13.08-TDI). Dissertação (Mestrado em Engenharia e Tecnologia Espaciais / Mecânica Espacial e Controle) - Instituto Nacional de Pesquisas Espaciais (INPE), São José dos Campos, 2011. Disponível em: <http://urlib.net/8JMKD3MGP7W/3996485>.

MARSHALL, J. **An introduction to failure modes effects and criticality analysis FME(C)A.** 2011/2012. Disponível em: http://www2.warwick.ac.uk/fac/sci/wmg/ftmsc/modules/modulelist/peuss/slides/section_10b_fmea_lecture_slides_compatibility_mode.pdf. Acesso em: 13 maio 2016.

MARTINI, M. R. B. Avaliação da dependabilidade de sistemas levando em conta falhas hardware e software. In: SIMPÓSIO DE COMPUTADORES TOLERANTES A FALHAS (SCTF), 5., 1993, São José dos Campos, Brasil. **Anais...** 1993.

MARTINS, E. Validação experimental da tolerância a falhas: a técnica de injeção de falhas. In: SIMPÓSIO DE COMPUTADORES TOLERANTES A FALHAS (SCTF), 5., 1993, São José dos Campos, Brasil. **Anais...** 1993.

MARZAT, J.; PIET-LAHANIER, H.; DAMONGEOT, F.; WALTER, E. Model-based fault diagnosis for aerospace systems: a survey. **Proceedings of the**

Institution of Mechanical Engineers, Part G: Journal of Aerospace Engineering, v.226, n.10, 2012. DOI: 10.1177/0954410011421717. Disponível em: <https://hal.archives-ouvertes.fr/hal-00615617/document>. Acesso em: 13 jul. 2015.

MEAKIN, P. C. Cassini attitude control fault protection design: launch to end of prime mission performance. In: AIAA/AAS ASTRODYNAMICS SPECIALIST CONFERENCE, 2008, Honolulu, USA. **Proceedings...** Disponível em: http://trs-new.jpl.nasa.gov/dspace/bitstream/2014/45425/1/08-2559_A1b.pdf. Acesso em: 04 set. 2015.

MELO, A. F. **Detecção e identificação de falhas em sistemas de controles lineares usando uma modificação do filtro de detecção**. 1991. 121p. (INPE-5367-TDI/466). Dissertação (Mestrado em Ciência Espacial / Mecânica Orbital) - Instituto Nacional de Pesquisas Espaciais (INPE), São José dos Campos, 1991.

MISRA, A. **Sensor-based diagnosis of dynamical systems**. 1994. Tese (Doutorado em Engenharia Elétrica) - Vanderbilt University, Nashville, USA, 1994. Disponível em: http://www.isis.vanderbilt.edu/sites/default/files/Misra_A_0_0_1994_Sensor_Bas_0.pdf. Acesso em: 22 mar. 2017.

MORGAN, P. S. Fault protection techniques in JPL spacecraft. In: INTERNATIONAL FORUM ON INTEGRATED SYSTEM HEALTH ENGINEERING AND MANAGEMENT IN AEROSPACE (ISHEM), 1., 2005. Disponível em: <http://trs-new.jpl.nasa.gov/dspace/bitstream/2014/39531/1/05-2750.pdf>. Acesso em: 17 jun. 2015.

MUSCETTOLA, N.; NAYAK, P. P.; PELL, B.; WILLIAMS, B. C. Remote agent: to boldly go where no AI system has gone before. **Artificial Intelligence**, v. 103, n. 1–2, p. 5–47, 1998. Disponível em: http://www.sciencedirect.com/science?_ob=Articulístico&_method=list&_ArticleListID=-822603403&_sort=r&_st=13&_view=c&_md5=49a62fff702c47b108cfac815eb5697d&searchtype=a. Acesso em: 13 jul. 15.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION (NASA). **Fault management handbook**. Washington, USA: NASA, 2012. 203p. NASA-HDBK-1002/DRAFT 2. Disponível em: http://www.nasa.gov/pdf/636372main_NASA-HDBK-1002_Draft.pdf. Acesso em: 05 jul. 2015.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION (NASA). **Small spacecraft technology state of the art**. Hanover, USA: NASA Center for Aero Space Information, 2014. 211p. NASA/TP–2014–216648/REV1. Disponível em: https://www.nasa.gov/sites/default/files/files/Small_Spacecraft_Technology_State_of_the_Art_2014.pdf. Acesso em: 18 ago. 2015.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION (NASA). **NASA system engineering handbook**. 2.ed. Washington, USA: NASA, 2016. 297p. NASA SP-2016-6105 Rev2. Disponível em: https://www.nasa.gov/sites/default/files/atoms/files/nasa_systems_engineering_handbook_0.pdf. Acesso em: 07 ago. 2017.

NASASPACEFLIGHT. **Brazil's CBERS-3 spacecraft lost following Chinese failure**. 2013. Disponível em: <http://www.nasaspaceflight.com/2013/12/chinese-long-march-4b-cbers-3/>. Acesso em: 09 set. 2015.

NASASPACEFLIGHT. **200th long march rocket launches CBERS-4 for Brazil**. 2014. Disponível em: <http://www.nasaspaceflight.com/2014/12/200th-long-march-launches-cbers-4-brazil/>. Acesso em: 09 set. 2015.

NEWHOUSE, M. E.; FRIBERG, K. H.; FESQ, L.; BARLEY, B. Fault management guiding principles. In: AIAA INFOTECH AEROSPACE CONFERENCES, 2011, St. Louis, USA. Disponível em: <http://trs-new.jpl.nasa.gov/dspace/bitstream/2014/42059/1/11-1104.pdf>. Acesso em: 28 ago. 2015.

OFSTHUN, S.C.; ABDELWAHED, S. Practical applications of timed failure propagation graphs for vehicle diagnosis. In: AUTOTESTCON, 2007, Baltimore, USA. **Proceedings...** Disponível em: <http://ieeexplore.ieee.org.ez61.periodicos.capes.gov.br/stamp/stamp.jsp?arnumber=4374226>. Acesso em: 31 mar. 2017.

OLIVE, X. FDI(R) for satellite at Thales Alenia Space how to deal with high availability and robustness in space domain? In: CONFERENCE ON CONTROL AND FAULT TOLERANT SYSTEMS, 2010, Nice, France. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5675942>. Acesso em: 28 maio 2015.

OLIVE, X. FDI(R) for satellite: how to deal with high availability and robustness in space domain? **International Journal of Applied Mathematics and Computer Science**, v. 22, n. 1, p. 99-107, 2012. Disponível em <http://matwbn.icm.edu.pl/ksiazki/amc/amc22/amc2217.pdf>. Acesso em: 26 maio 2015.

PAAKKO, M.; MYLLYMÄKI, P.; HOLSTI, N.; TIRRI, H. Bayesian networks for advanced FDIR. In: ESA WORKSHOP ON ON-BOARD AUTONOMY, 2001, Noordwijk, The Netherlands. **Proceedings...** Disponível em: ftp://ftp.estec.esa.nl/pub/wm/anonymous/wme/Web/ESA_On_Board_Auto_WS_SSF_Artic_2.pdf. Acesso em: 26 maio 15.

PASQUET, J. M.; DE FERLUC, R.; PROVOST-GRELLIER, A.; DELLANDREA, B. FDIR - state of the art and evolutions TAS-F point of view. In: ESA WORKSHOP ON AVIONICS, DATA, CONTROL AND SOFTWARE SYSTEMS (ADCSS), 9., 2015, Noordwijk, The Netherlands. **Proceedings...** Disponível em:

<https://indico.esa.int/indico/event/85/session/7/contribution/133/material/0/0.pdf>.
Acesso em: 08 ago. 2017.

PESSOTTA, F. A. **Análise de arquiteturas de computadores de bordo para missões espaciais de longa duração.** Dissertação (Mestrado em Engenharia Eletrônica e Computação) - Instituto Tecnológico da Aeronautica (ITA), São José dos Campos, 1999.

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. 298p. (sid.inpe.br/mtc-m21b/2016/11.07.17.54-TDI) - Tese (Doutorado em Engenharia e Tecnologia Espaciais / Engenharia e Gerenciamento de Sistemas Espaciais) - Instituto Nacional de Pesquisas Espaciais (INPE), São José dos Campos, 2017. Disponível em: <http://urlib.net/8JMKD3MGP3W34P/3MP6RNL>. Acesso em: 22 mar. 2017.

RICE, E.B.; LEV-TOV, J. Optimized spacecraft fault protection for the wise mission. In: IEEE AEROSPACE CONFERENCE, 2008. **Proceedings...** Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4526482>. Acesso em: 15 jun. 2015.

ROGERS, A. Q.; HUANG, P. M.; WELLS, V. E.; DARRIN, M. A.; SUTER, J. J. Small satellite initiatives: building on success. In: SPACE SYMPOSIUM, 30., 2014, Colorado Springs, USA. Disponível em: http://www.spacefoundation.org/sites/default/files/downloads/A.Rogers_30th_Space_Symposium_Tech_Track.pdf. Acesso em: 02 nov. 2014.

SCHWAB, A; GIESE, C.; ULRICH, D. TDX-TSX - On-board autonomy and FDIR of whispering brothers. In: INTERNATIONAL CONFERENCE ON SPACE OPERATIONS (SPACEOPS), 2012, Stockholm, Sweden. **Proceedings...** Disponível em: <http://www.spaceops2012.org/proceedings/documents/id1290887-Paper-001.pdf>. Acesso em: 17 jul. 2015.

SIQUEIRA, J. E. M. **Uma abordagem no domínio 'frequência-estrutura' para a detecção e diagnóstico de falhas em sistemas de controle reconfiguráveis.** 2016. 450p. (sid.inpe.br/mtc-m21b/2016/05.23.16.38-TDI) - Tese (Doutorado em Engenharia e Tecnologia Espaciais / Mecânica Espacial e Controle) - Instituto Nacional de Pesquisas Espaciais (INPE), São José dos Campos, 2016. Disponível em: <http://urlib.net/8JMKD3MGP3W34P/3LNR7CP>. Acesso em: 25 jan. 2018.

SLONSKI, J. P. System fault protection design for the cassini spacecraft. In: AEROSPACE APPLICATIONS CONFERENCE, 1996, Aspen, USA. **Proceedings...** IEEE, 1996. p. 279-292. ISBN: 0-7803-3196-6. DOI: 10.1109/AERO.1996.495890. Disponível em:

<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=495890>. Acesso em: 19 nov. 2015.

SYED, W. A.; KHAN, S.; PHILLIPS, P.; PERINPANAYAGAM, S. Intermittent fault finding strategies. **Procedia CIRP**, v. 11, p. 74-79, 2013. DOI: 10.1016/j.procir.2013.07.062. Disponível em: http://ac.els-cdn.com/S2212827113005362/1-s2.0-S2212827113005362-main.pdf?_tid=99f3e17c-5b70-11e7-92e5-00000aab0f02&acdnat=1498592663_e7a4bd7da4c95694f99608e30062d2e2. Acesso em: 26 jun. 2017.

TEIXEIRA, A. J. **Detecção, identificação e reconfiguração de falhas múltiplas em sensores de sistemas lineares invariantes no tempo**. 2005. 311p. (INPE-14487-TDI/1168) - Tese (Doutorado em Engenharia e Tecnologia Espaciais / Mecânica Espacial e Controle) - Instituto Nacional de Pesquisas Espaciais (INPE), São José dos Campos, 2005.

TOMAYKO, J. E. **Computers in spaceflight : the NASA experience**. 1988. 409p. (NASA–Wichita State University Contractor Report 182505). Disponível em: https://ia700509.us.archive.org/6/items/nasa_techdoc_19880069935/1988006935.pdf. Acesso em: 26 jun. 2014.

TROIANO, L.; TIPALDI, M.; DI CERBO, A.; HOPING, M.; PASQUALE, D.; BRUENJES, B. Satellite FDIR practices using timed failure propagation graphs. In: IAC INTERNATIONAL ASTRONAUTICAL CONGRESS, 63., 2012, Naples, Italy. **Proceedings...** Disponível em: https://www.researchgate.net/publication/287329869_Satellite_FDIR_Practices_Using_Timed_Failure_Propagation_Graphs. Acesso em: 22 mar. 2017.

WANDER, A.; FÖRSTNER, R. Innovative fault detection, isolation and recovery strategies on-board spacecraft: state of the art and research challenges. In: DEUTSCHER LUFT UND RAUMFAHRTKONGRESS, 2012, Berlin, Germany. **Proceedings...** Disponível em: <http://www.dglr.de/publikationen/2013/281268.pdf>. Acesso em: 31 mar. 2015.

WANDER, A.; FÖRSTNER, R. Innovative fault detection, isolation and recovery strategies on-board spacecraft: study and implementation using cognitive automation. In: CONFERENCE ON CONTROL AND FAULT-TOLERANT SYSTEMS (SYSTOL), 2013, Nice, France. **Proceedings...** Disponível em: <http://ieeexplore.ieee.org.ez61.periodicos.capes.gov.br/stamp/stamp.jsp?tp=&arnumber=6693950>. Acesso em: 28 maio 2015.

WATKINS, C.B. Integrated modular avionics: managing the allocation of shared intersystem resource. In: DIGITAL AVIONICS SYSTEMS CONFERENCE (DASC), 25., 2006, Portland, USA. **Proceedings...** IEEE, 2006. Disponível em: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4106349. Acesso em: 11 jun. 2014.

WEEDEN, B. Small satellite space traffic management. In: BEIJING ORBITAL DEBRIS MITIGATION WORKSHOP, 2010, Beijing, China. **Proceedings...** Disponível em: http://swfound.org/media/99980/Weeden-Smallsat_STM.pdf. Acesso em: 02 set. 2015.

WIKIPEDIA. **Miniaturized satellite**. 2015. Disponível em: https://en.wikipedia.org/wiki/Miniaturized_satellite. Acesso em: 14 ago. 2015.

WIKIPEDIA. **Cassini–Huygens** 2016. Disponível em: <https://en.wikipedia.org/wiki/Cassini%E2%80%93Huygens>. Acesso em: 27 jan. 2016.

ZOLGHADRI, A. Advanced model-based FDIR techniques for aerospace systems: Today challenges and opportunities. **Progress in Aerospace Sciences**, v. 53 p. 18-29, 2012. Disponível em: http://ac.els-cdn.com.ez61.periodicos.capes.gov.br/S0376042112000292/1-s2.0-S0376042112000292-main.pdf?_tid=cbfa9924-e2c6-11e4-82bc-00000aab0f6b&acdnat=1429030598_b6bc18a03e84a22df575535c62a82d4a. Acesso em: 14 abr. 2015.

APÊNDICE A – DECOMPOSIÇÃO FUNCIONAL DAS FUNÇÕES DO ACDH (CONTINUAÇÃO)

A.1 Comandos Gerados em Solo (Continuação)

A.1.1 Função ‘Fornecer Comandos Roteados Temporizados’

1) Descrição da função: Os comandos roteados temporizados são gerados pelo Segmento Solo e transmitidos para o Segmento Espacial na forma de telecomandos. Os comandos roteados são comandos seriais. A função ‘Fornecer Comando Roteado Temporizado’ distribui os comandos recebidos de solo para os subsistemas e cargas úteis do satélite no horário agendado.

2) Decomposição Funcional

A função Fornecer Comandos Roteados Temporizados é decomposta em dois níveis funcionais:

a) Nível 3:

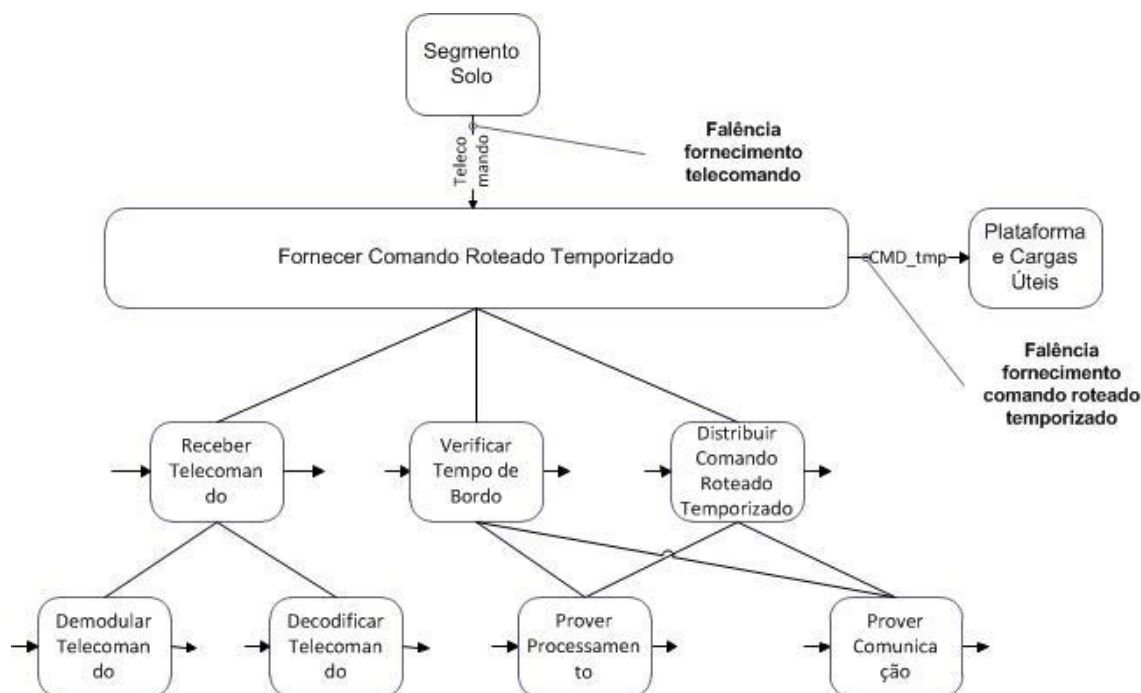
- Subfunção Receber Telecomando;
- Subfunção Armazenar comandos temporizados;
- Subfunção Verificar Tempo de Bordo;
- Subfunção Distribuir Comandos Roteados Temporizados.

b) Nível 4:

- Subfunção Prover Processamento;
- Subfunção Prover Comunicação.

A Figura A.1 apresenta o diagrama da decomposição funcional da função Fornecer Comandos Roteados Temporizados.

Figura A.1 – Decomposição funcional da função Fornecer Comando Roteado Temporizado.



3) Entradas da função

- Telecomandos fornecidos pelo Segmento Solo;
- Tempo de Bordo.

4) Saídas da função

- Comandos Roteados Temporizados.

A.2 Comandos Gerados em Bordo

A.2.1 Função ‘Fornecer Comandos Imediatos’

1) Descrição da função: Os comandos imediatos são gerados em bordo e distribuídos imediatamente para os subsistemas e cargas úteis do satélite. Os comandos imediatos podem ser comandos discretos usados para acionar dispositivos em bordo ou comandos seriais.

2) Decomposição Funcional

A função Fornecer Comandos Imediatos é decomposta em dois níveis funcionais:

a) Nível 3:

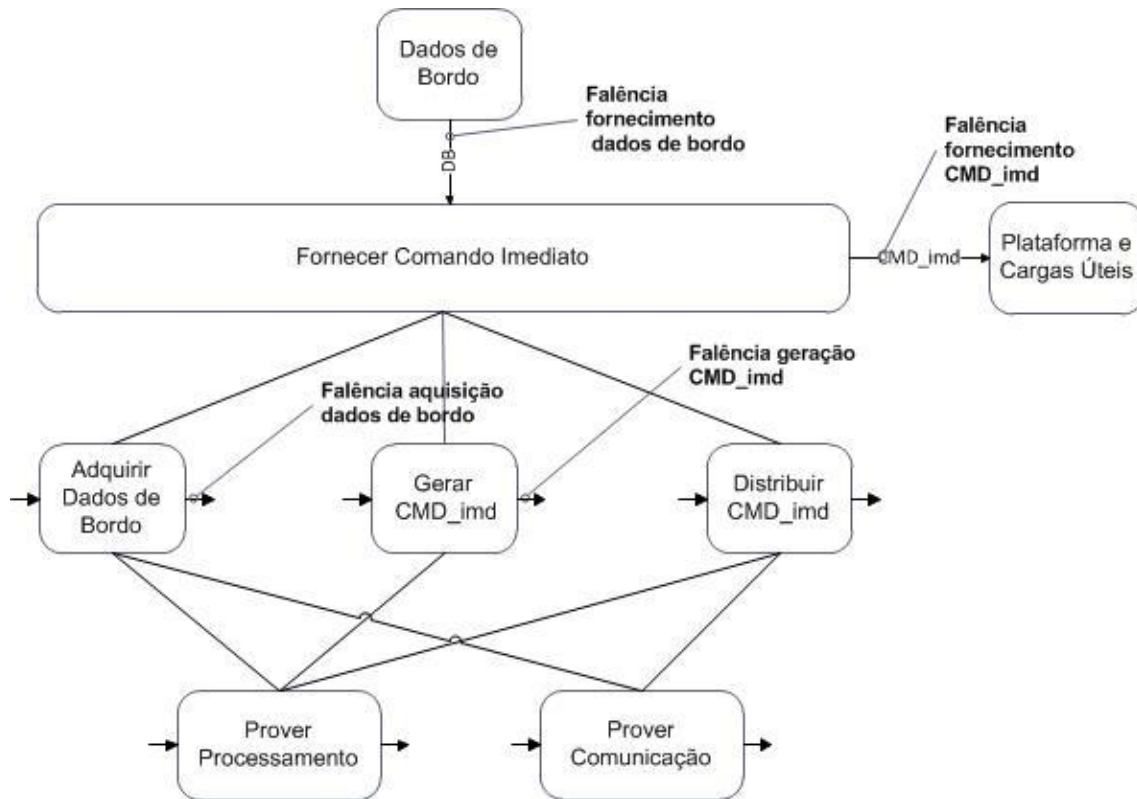
- Subfunção Adquirir Dados de Bordo;
- Subfunção Gerar Comandos Imediatos;
- Subfunção Distribuir Comandos Imediatos.

b) Nível 4:

- Subfunção Prover Processamento;
- Subfunção Prover Comunicação.

A Figura A.2 apresenta o diagrama da decomposição funcional da função Fornecer Comandos Imediatos.

Figura A.2 – Decomposição funcional da função ‘Fornecer Comando Imediato’.



3) Entradas da função

- Dados de Bordo;

4) Saídas da função

- Comandos Imediatos.

A.2.2 Função ‘Fornecer Comandos Temporizados’

1) Descrição da função: Descrição da função: Os comandos temporizados são gerados em bordo e agendados para serem distribuídos para os subsistemas e cargas úteis do satélite. Os comandos temporizados podem ser comandos discretos usados para acionar dispositivos em bordo ou comandos seriais.

2) Decomposição Funcional

A função Fornecer Comandos Temporizados é decomposta em dois níveis funcionais:

a) Nível 3:

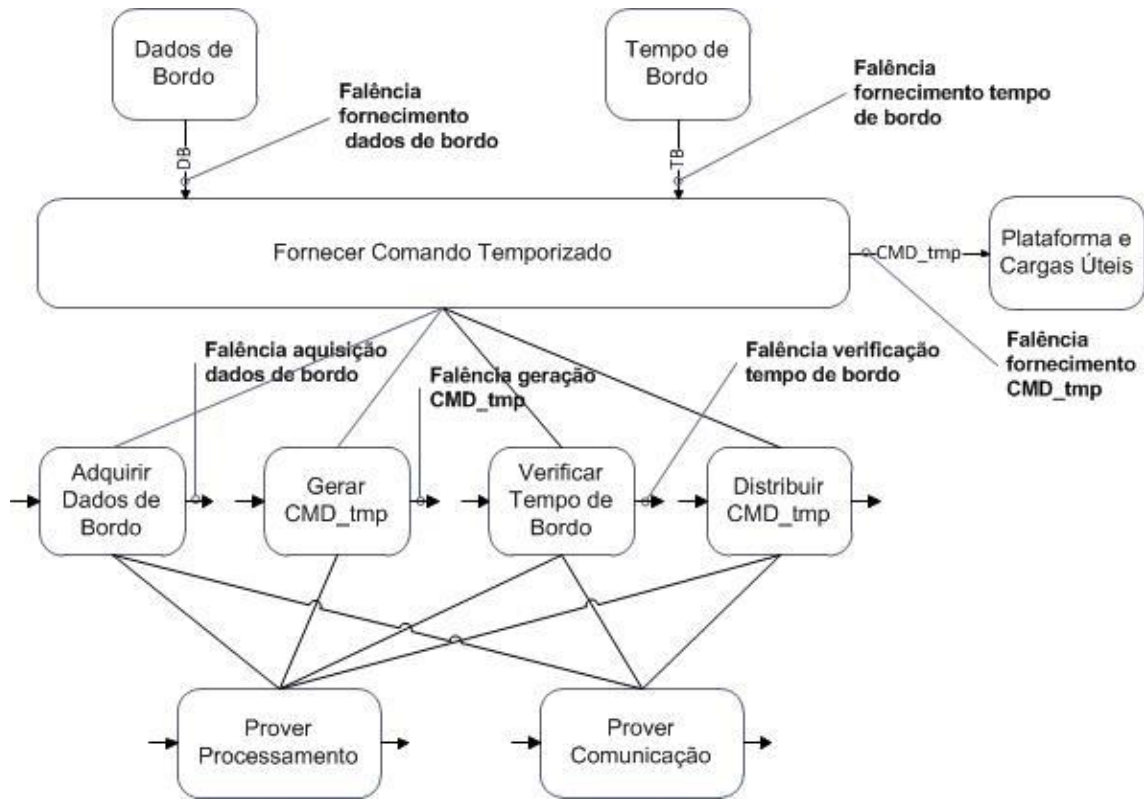
- Subfunção Adquirir Dados de Bordo;
- Subfunção Gerar Comandos Temporizados;
- Subfunção Verificar Tempo de Bordo;
- Subfunção Distribuir Comandos Temporizados.

b) Nível 4:

- Subfunção Prover Processamento;
- Subfunção Prover Comunicação.

A Figura A.3 apresenta o diagrama da decomposição funcional da função Fornecer Comandos Temporizados.

Figura A.3 – Decomposição funcional da função ‘Fornecer Comandos Temporizados’.



3) Entradas da função

- Dados de Bordo;
- Tempo de Bordo.

4) Saídas da função

- Comandos Temporizados.

A.3 Função ‘Fornecer Telemetrias’

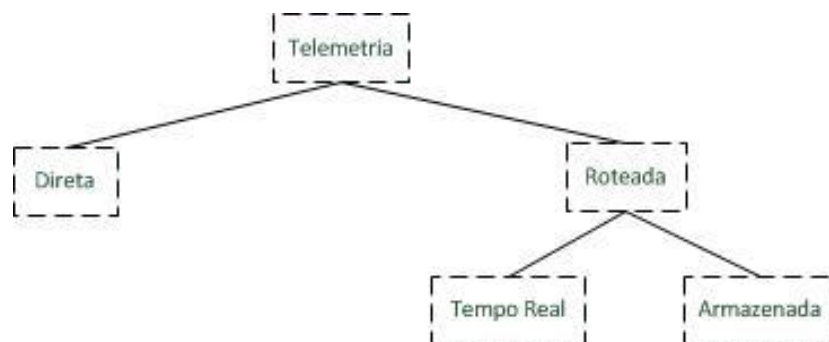
A.3.1 Classificação das Telemetrias e Caracterização dos seus Modos de Falência

Basicamente, uma telemetria é constituída pelos dados adquiridos a bordo e pelo tempo em que os dados foram adquiridos. Estas informações são formatadas em quadros (*frames*), os quais são distribuídos para o Segmento Solo por meio do *transponder* de serviço.

As telemetrias podem ser classificadas de acordo com a sua origem (Direta ou Roteada) e o tempo em que são distribuídas (Tempo Real ou Armazenada), conforme sumarizado na Figura A.4. As telemetrias diretas são fornecidas por módulo dedicado que adquire os dados e o tempo de bordo e, imediatamente, formata e envia para o *transponder* de serviço. As telemetrias roteadas são fornecidas por meio do computador de bordo. Neste caso, as telemetrias podem ser adquiridas e enviadas imediatamente para o *transponder* de serviço (neste caso são denominadas telemetrias de tempo real) ou podem ser adquiridas e armazenadas (neste caso são denominadas telemetrias armazenadas) para serem enviadas posteriormente para o Segmento Solo.

As Telemetrias Diretas não são tratadas neste trabalho, pois com exceção dos satélites da série SCD, as demais missões brasileiras ou com participação do Brasil não possuem esta funcionalidade.

Figura A.4 – Classificação de telemetrias de acordo com a origem e o tempo de transmissão.



Neste trabalho, as telemetrias são tratadas distintamente, de acordo com a sua origem e o tempo em que são distribuídas, uma vez que as causas e os efeitos dos seus modos de falência são diferentes.

A.3.2 Função 'Fornecer Telemetrias de Tempo Real'

1) Descrição da função

A função 'Fornecer Telemetrias de Tempo Real' adquire os dados de bordo e os tempos em que são adquiridos e, imediatamente, formata e distribui para o Segmento Solo e o Segmento Espacial.

2) Decomposição Funcional

A função 'Fornecer Telemetrias de Tempo Real' é decomposta em dois níveis funcionais, os quais são identificados como nível 3 e nível 4 em vista de suas posições na estrutura hierárquica funcional do subsistema. No nível 3, a função é decomposta nas seguintes subfunções:

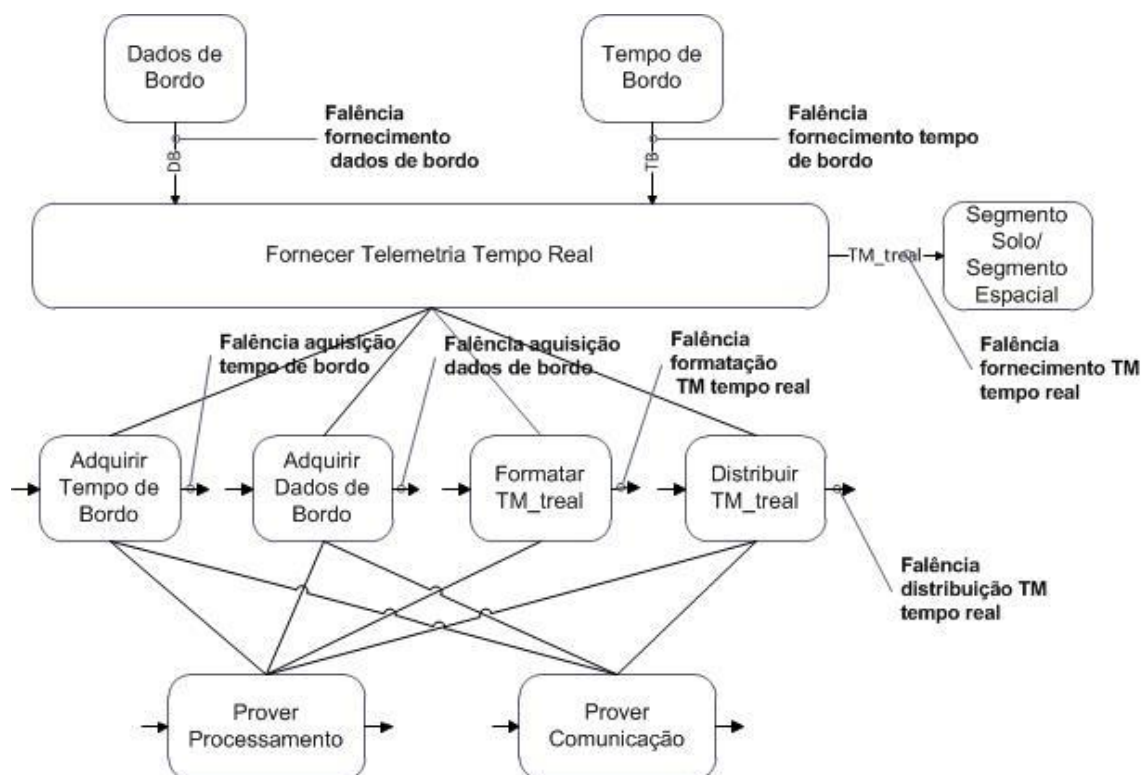
- Subfunção Adquirir Tempo de Bordo;
- Subfunção Adquirir Dados de Bordo;
- Subfunção Formatar Telemetrias de Tempo Real;
- Subfunção Distribuir Telemetrias de Tempo Real.

No nível 4, a função é decomposta nas seguintes subfunções:

- Subfunção Prover Processamento;
- Subfunção Prover Comunicação.

A Figura A.5 apresenta o diagrama da decomposição funcional da função 'Fornecer Telemetrias de Tempo Real'.

Figura A.5 – Decomposição funcional da função ‘Fornecer Telemetria Tempo Real’.



3) Entradas da função

- Dados de Bordo;
- Tempo de Bordo.

4) Saídas da função

- Telemetrias de Tempo Real.

A.3.3 Função ‘Fornecer Telemetrias Armazenadas’

1) Descrição da função

A função ‘Fornecer Telemetrias Armazenadas’ adquire os dados de bordo e os tempos em que são adquiridos, formata e agenda a sua distribuição para o Segmento Solo.

2) Decomposição Funcional

A função Fornecer Telemetrias Armazenadas é decomposta em dois níveis funcionais:

a) Nível 3:

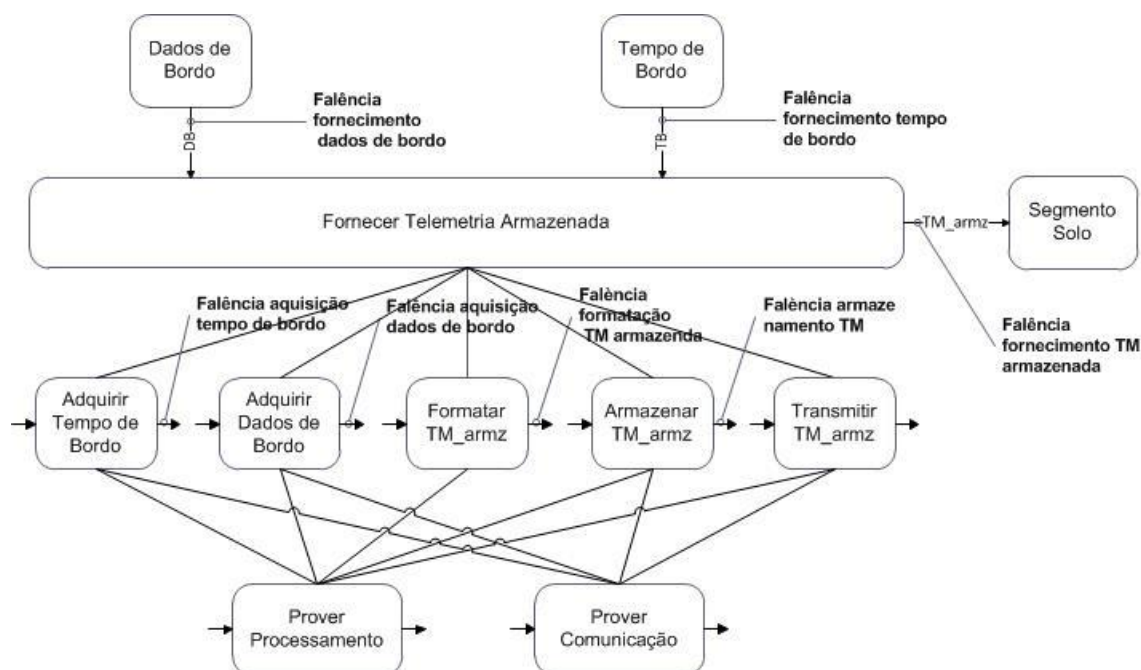
- Subfunção Adquirir Tempo de Bordo;
- Subfunção Adquirir Dados de Bordo;
- Subfunção Formatar Telemetrias;
- Subfunção Armazenar Telemetrias;
- Subfunção Transmitir Telemetrias Armazenadas.

b) Nível 4:

- Subfunção Prover Processamento;
- Subfunção Prover Comunicação.

A Figura A.6 apresenta o diagrama da decomposição funcional da função Fornecer Telemetrias Armazenadas.

Figura A.6 – Decomposição funcional da função ‘Fornecer Telemetria Armazenada’.



3) Entradas da função

- Dados de Bordo;
- Tempo de Bordo.

4) Saídas da função

- Telemetrias de Tempo Real.

A.4 Função ‘Estimar Atitude’

1) Descrição da função

A função ‘Estimar Atitude’ calcula a atitude do satélite a partir das informações fornecidas pelos sensores e das efemérides fornecidas pela função ‘Propagar Órbita’.

2) Decomposição Funcional

A função Estimar Atitude é decomposta em dois níveis funcionais:

a) Nível 3:

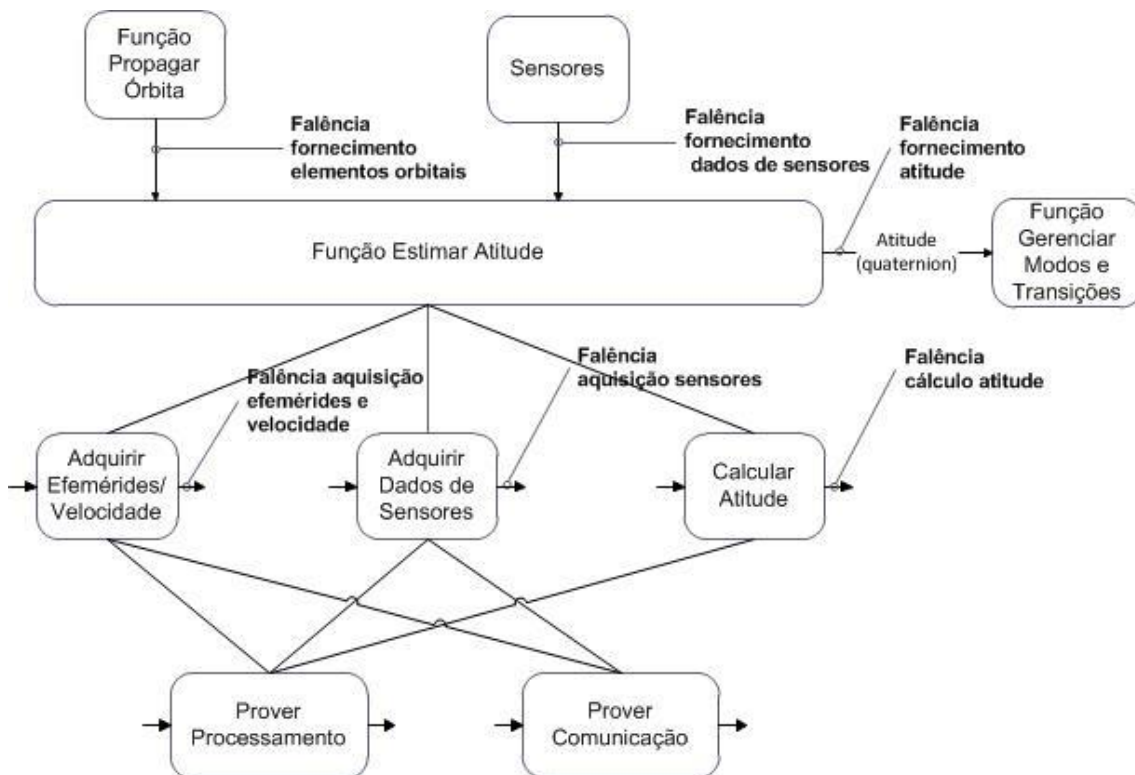
- Subfunção Adquirir Efemérides e Velocidade;
- Subfunção Adquirir Sensores;
- Subfunção Calcular Atitude.

b) Nível 4:

- Subfunção Prover Processamento;
- Subfunção Prover Comunicação.

A Figura A.7 apresenta o diagrama da decomposição funcional da função Estimar Atitude.

Figura A.7 – Decomposição funcional da função Estimar Atitude.



3) Entradas da função

- Elementos orbitais;

- Dados de sensores
- 4) Saídas da função

- Quaternion;

A.5 Função ‘Propagar Órbita’

1) Descrição da função

A função ‘Propagar Órbita’ calcula as efemérides (os elementos orbitais e a velocidade do satélite) para um dado Tempo de Bordo a partir do TLE (*Two Lines Elements*) fornecido por telecomando pelo Segmento Solo. As efemérides são posteriormente utilizadas pela função ‘Estimar Atitude’ no cálculo da atitude do satélite e incluídas nos Dados Auxiliares fornecidos para as Câmeras e gravados nas imagens.

2) Decomposição Funcional

Para os propósitos deste trabalho a função ‘Propagar Órbita’ é decomposta em dois níveis funcionais, os quais são identificados como nível 3 e nível 4 em vista de suas posições na estrutura hierárquica funcional do subsistema. No nível 3, a função é decomposta nas seguintes subfunções:

- Subfunção Adquirir Tempo de Bordo;
- Subfunção Receber TLE (*Two Lines Elements*);
- Subfunção Propagar Órbita.

No nível 4, a função é decomposta nas seguintes subfunções:

- Subfunção Prover Processamento;
- Subfunção Prover Comunicação.

A Figura A.8 apresenta o diagrama da decomposição funcional da função ‘Propagar Órbita’.

- A órbita é propagada de forma intermitente quando a órbita não é propagada a intervalos randômicos de tempo;
- A órbita é propagada fora da especificação quando os valores da velocidade e dos elementos orbitais fornecidos pela função são diferentes dos valores esperados.

6) Causas dos modos de falência da função 'Propagar Órbita'

A partir da decomposição funcional e da caracterização dos modos de falência as causas potenciais da falência podem ser determinadas para cada modo de falência e nível hierárquico da função. No nível 2,

- A órbita não é propagada quando:
 - TB não é adquirido;
 - Propagação orbital não é calculada;
- A órbita é propagada de forma intermitente quando:
 - TB é adquirido de forma intermitente;
 - Propagação orbital é calculada de forma intermitente;
- A órbita é propagada fora da especificação quando:
 - TB é adquirido fora da especificação;
 - TLE é recebido fora da especificação;
 - Propagação orbital é calculada fora da especificação;

No nível 3,

- A órbita não é propagada quando:
 - Processamento não é provido;

- Comunicação não é provida.
- A órbita é propagada de forma intermitente quando:
 - Processamento é provido de forma intermitente;
 - Comunicação é provida de forma intermitente.
- A órbita é propagada fora da especificação quando:
 - Processamento é provido fora de especificação;
 - Comunicação é provida fora de especificação.

A.6 Função ‘Comandar Atuadores’

1) Descrição da função

A função ‘Comandar Atuadores’ calcula os comandos que devem ser enviados para os atuadores a partir dos torques de controle fornecidos pela função ‘Gerenciar Modos e Transições’ e dos dados dos atuadores.

2) Decomposição Funcional

A função Comandar Atuadores é decomposta em dois níveis funcionais:

a) Nível 3:

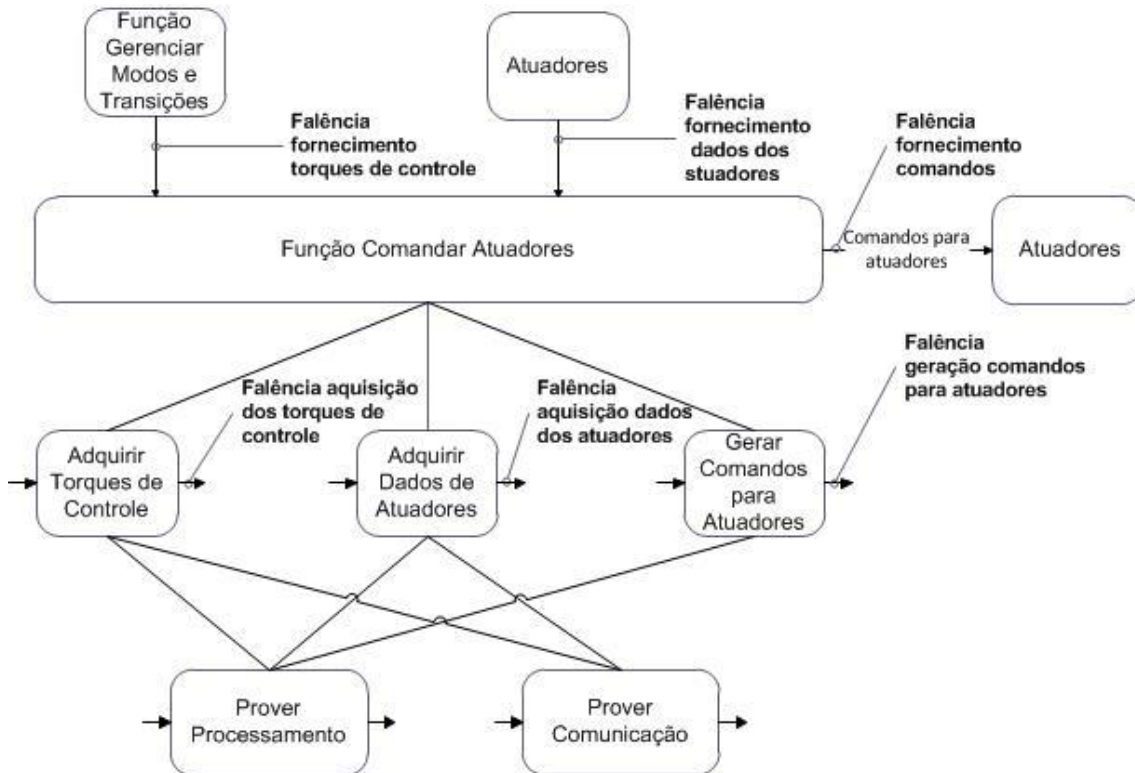
- Subfunção Adquirir Torques de Controle;
- Subfunção Dados de Atuadores;
- Subfunção Gerar Comandos para Atuadores.

b) Nível 4:

- Subfunção Prover Processamento;
- Subfunção Prover Comunicação.

A Figura A.9 apresenta o diagrama da decomposição funcional da função Comandar Atuadores.

Figura A.9 – Decomposição funcional da função ‘Comandar Atuadores’.



3) Entradas da função

- Dados dos torques de controle;
- Dados dos atuadores.

4) Saídas da função

- Comandos para atuadores.

A.7 Função ‘Gerenciar Modos e Transições’

1) Descrição da função

A função ‘Gerenciar Modos e Transições’ calcula os torques de controle que devem ser aplicados aos atuadores a partir dos dados fornecidos pelos

sensores e da atitude estimada (quaternion) fornecida pela função 'Estimar Atitude'.

2) Decomposição Funcional

A função Gerenciar Modos e Transições é decomposta em dois níveis funcionais:

a) Nível 3:

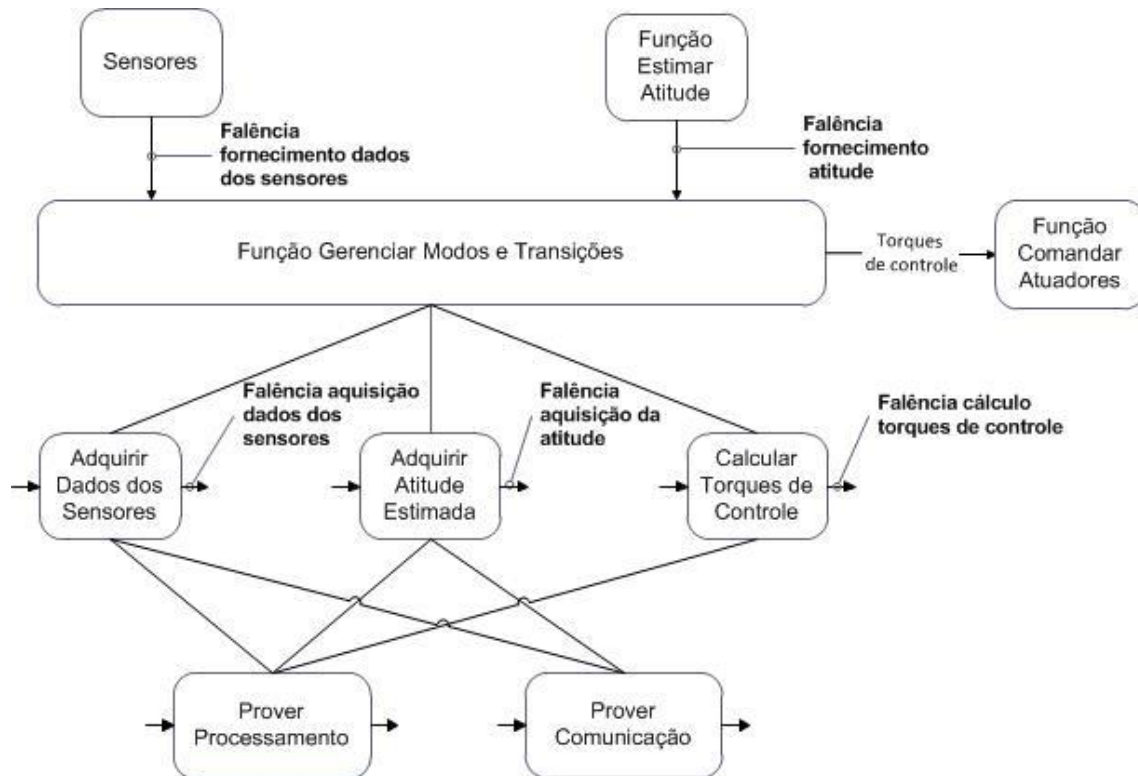
- Subfunção Adquirir Dados dos Sensores;
- Subfunção Adquirir Atitude Estimada;
- Subfunção Calcular Torques de Controle.

b) Nível 4:

- Subfunção Prover Processamento;
- Subfunção Prover Comunicação.

A Figura A.10 apresenta o diagrama da decomposição funcional da função Gerenciar Modos e Transições.

Figura A.10 – Decomposição funcional da função ‘Gerenciar Modos e Transições’.



3) Entradas da função

- Dados de sensores;
- Atitude estimada.

4) Saídas da função

- Torques de controle.

APÊNDICE B – FMEA FUNCIONAL HIERÁRQUICA DO ACDH (CONTINUAÇÃO)

Tabela B.1 – Análise Funcional Hierárquica dos Efeitos dos Modos de Falências da Função ‘Fornecer Comando Roteado Temporizado’

Identificação	Nível	Função	Modo de Falência	Causa da Falência	Fase da Missão/ Modo de Operação	Efeitos da Falência	Severidade	Método de Detecção da Falência/ Sintomas Observáveis	Provisão para Compensação	Recomendações	Observações
1	2	Fornecer Comandos Roteados Temporizados	Não fornece comandos roteados temporizados;	Perda da capacidade de recepção de telecomando; Perda da capacidade de verificação do tempo de bordo; Perda da capacidade de distribuição de Comando Roteado;	LEOP e fases operacionais;	Perda da comandabilidade do satélite	Catastrófica	Telemetria	Redundância física Recarga e execução do OBSW;		
2			Fornecer comandos roteados temporizados de forma intermitente;	Recepção intermitente de telecomando; Verificação intermitente do tempo de bordo; Distribuição intermitente de Comando Roteado;	Idem acima	Atraso na comandabilidade do satélite	Catastrófica	Telemetria	Redundância física Recarga e execução do OBSW;		
3			Fornecer comandos roteados temporizados fora de especificação	Recepção de telecomando fora de especificação; Verificação fora de especificação do tempo de bordo; Distribuição de Comando Roteado fora de especificação;	Idem acima	Perda da comandabilidade do satélite	Catastrófica	Telemetria	Redundância física Recarga e execução do OBSW;		

Tabela B.2 – Análise Funcional Hierárquica dos Efeitos dos Modos de Falências da Função ‘Fornecer Comandos Imediatos’

Identificação	Nível	Função	Modo de Falência	Causa da Falência	Fase da Missão/ Modo de Operação	Efeitos da Falência	Severidade	Método de Detecção da Falência/ Sintomas Observáveis	Provisão para Compensação	Recomendações	Observações
1	2	Fornecer Comandos Imediatos	Não fornece comandos imediatos;	Não adquire dados de bordo; Perda da capacidade de geração de comando imediato; Perda da capacidade de distribuição de comando imediato;	LEOP e fases operacionais;	Perda da comandabilidade do satélite	Catastrófica	Telemetria	Recarga e execução do OBSW; Redundância física		
2			Fornecer comandos imediatos de forma intermitente;	Adquire dados de bordo intermitente; Geração de comando imediato intermitente; Distribuição de comando imediato intermitente;	Idem acima	Atraso na comandabilidade do satélite	Catastrófica	Telemetria	Recarga e execução do OBSW; Redundância física		
3			Fornecer comandos imediatos fora de especificação	Adquire dados de bordo fora de especificação; Geração de comando imediato fora de especificação; Distribuição de comando imediato fora de especificação;	Idem acima	Perda da comandabilidade do satélite	Catastrófica	Telemetria	Recarga e execução do OBSW; Redundância física		

Tabela B.3 – Análise Funcional Hierárquica dos Efeitos dos Modos de Falências da Função ‘Fornecer Comandos Temporizados’

Identificação	Nível	Função	Modo de Falência	Causa da Falência	Fase da Missão/ Modo de Operação	Efeitos da Falência	Severidade	Método de Detecção da Falência/ Sintomas Observáveis	Provisão para Compensação	Recomendações	Observações
1	2	Fornecer Comandos Temporizados	Não fornece comandos temporizados;	Não adquire dados de bordo; Perda da capacidade de geração de comando temporizado; Perda da capacidade de verificação do tempo de bordo; Perda da capacidade de distribuição de comando temporizado;	LEOP e fases operacionais;	Perda da comandabilidade do satélite	Catástrofica	Telemetria	Recarga e execução do OBSW; Redundância física		
2			Fornecer comandos temporizados de forma intermitente;	Adquire dados de bordo intermitente; Geração de comando temporizado intermitente; Verificação intermitente do tempo de bordo; Distribuição de comando temporizado intermitente;	Idem acima	Atraso na comandabilidade do satélite	Catástrofica	Telemetria	Recarga e execução do OBSW; Redundância física		
3			Fornecer comandos temporizados fora de especificação	Adquire dados de bordo fora de especificação; Geração de comando temporizado fora de especificação; Verificação fora de especificação do tempo de bordo; Distribuição de comando temporizado fora de especificação;	Idem acima	Perda da comandabilidade do satélite	Catástrofica	Telemetria	Recarga e execução do OBSW; Redundância física		

Tabela B.4 – Análise Funcional Hierárquica dos Efeitos dos Modos de Falências da Função ‘Fornecer Telemetria de Tempo Real’

Identificação	Nível	Função	Modo de Falência	Causa da Falência	Fase da Missão/ Modo de Operação	Efeitos da Falência	Severidade	Método de Detecção da Falência/ Sintomas Observáveis	Provisão para Compensação	Recomendações	Observações
1	2	Fornecer Telemetrias de Tempo Real	Não fornece telemetrias de tempo real;	Não formata TM tempo real; Não transmite TM tempo real;	LEOP e fases operacionais;	Perda observabilidade do satélite;	Catastrófica	Ausência de Telemetria	Recarga e execução do OBSW; Redundância física		
2			Fornecer telemetrias de tempo real intermitentemente	Transmite TM tempo real intermitentemente; Formata TM tempo real intermitentemente.	Idem acima	Perda ou atraso na observabilidade do satélite	Catastrófica	Telemetria intermitente	Redundância física; Redundância temporal		
3			Fornecer telemetrias de tempo real fora especificação	Não adquire dados de bordo; Não adquire TB; Adquire DB fora especificação; Adquire TB fora especificação; Formata TM_treal fora especificação	Idem acima	Perda observabilidade do satélite	Catastrófica	Telemetria	Recarga e execução do OBSW; Redundância física		

Tabela B.5 – Análise Funcional Hierárquica dos Efeitos dos Modos de Falências da Função ‘Fornecer Telemetria Armazenada’

Identificação	Nível	Função	Modo de Falência	Causa da Falência	Fase da Missão/ Modo de Operação	Efeitos da Falência	Severidade	Método de Detecção da Falência/ Sintomas Observáveis	Provisão para Compensação	Recomendações	Observações
1	2	Fornecer Telemetrias Armazenadas	Não fornece telemetrias armazenadas;	Não adquire dados de bordo; Não adquire tempo de bordo; Não formata TM armazenada; Não armazena TM armazenada; Não transmite TM armazenada;	LEOP e fases operacionais	Perda observabilidade do satélite	Catástrofica	Ausência de Telemetria	Recarga e execução do OBSW; Redundância física		
2			Fornecer telemetrias armazenadas de forma intermitente	Transmite TM armazenada intermitentemente; Formata TM armazenada intermitentemente; Armazena TM armazenada intermitentemente.	Idem acima	Perda ou atraso na observabilidade do satélite	Catástrofica	Telemetria intermitente	Redundância física; Redundância temporal		
3			Fornecer telemetrias armazenadas fora de especificação	Não adquire dados de bordo; Não adquire tempo de bordo; Formata TM armazenada parcialmente; Armazena TM armazenada parcialmente;	Idem acima	Perda observabilidade do satélite	Catástrofica	Telemetria	Recarga e execução do OBSW; Redundância física		

Tabela B.6 – Análise Funcional Hierárquica dos Efeitos dos Modos de Falências da Função ‘Estimar Atitude’

Identificação	Nível	Função	Modo de Falência	Causa da Falência	Fase da Missão/ Modo de Operação	Efeitos da Falência	Severidade	Método de Detecção da Falência/ Sintomas Observáveis	Provisão para Compensação	Recomendações	Observações
1	2	Estimar Atitude	Não estima atitude	Não calcula atitude	LEOP e fases operacionais	Perda da atitude	Catastrófica	Telemetria	Recarga e execução do OBSW; Redundância física		
2			Estimar atitude intermitentemente	Calcula atitude intermitentemente	Idem acima	Perda intermitente da atitude	Catastrófica	Telemetria	Recarga e execução do OBSW; Redundância física		
3			Estimar atitude fora de especificação	Não adquire efemérides; Não adquire dados dos sensores; Adquire efemérides fora da especificação; Adquire dados dos sensores fora da especificação; Calcula atitude fora da especificação.	Idem acima	Atitude fora da especificação	Catastrófica	Telemetria	Recarga e execução do OBSW; Redundância física		

Tabela B.7 – Análise Funcional Hierárquica dos Efeitos dos Modos de Falências da Função ‘Propagar Órbita’

Identificação	Nível	Função	Modo de Falência	Causa da Falência	Fase da Missão/ Modo de Operação	Efeitos da Falência	Severidade	Método de Detecção da Falência/ Sintomas Observáveis	Provisão para Compensação	Recomendações	Observações
1	2	Propagar Órbita	Não propagar órbita	TB não é adquirido; Propagação orbital não é calculada.	Idem acima	Efemerides desatualizadas; Dados auxiliares com erro; Atitude estimada com erro; Não gera imagem;	Catastrófica	Telemetria	Recarga e execução do OBSW; Redundância física		
2			Propagar órbita intermitentemente	TB é adquirido de forma intermitente; Propagação orbital é calculada de forma intermitente.	Idem acima	Efemerides atualizadas intermitentemente; Dados auxiliares sem erro intermitentemente; Atitude estimada sem erro intermitentemente; Gera imagem intermitentemente.	Catastrófica	Telemetria	Recarga e execução do OBSW; Redundância física		
3			Propagar órbita fora de especificação	TB é adquirido fora da especificação; Propagação orbital é calculada fora da especificação; TLE é recebido fora da especificação.	Idem acima	Efemerides com erro; Dados auxiliares com erro; Atitude estimada com erro; Gera imagem de local não especificado.	Catastrófica	Telemetria	Recarga e execução do OBSW; Redundância física		
4	3	Adquirir Tempo de Bordo	TB não é adquirido;	Não processa; Não comunica;	Idem acima	Não propagar órbita					
5			TB é adquirido de forma intermitente;	Processa intermitentemente; Comunica intermitentemente;	Idem acima	Propagar órbita intermitentemente					

(continua)

Tabela B.7 – Continuação

Identificação	Nível	Função	Modo de Falência	Causa da Falência	Fase da Missão/ Modo de Operação	Efeitos da Falência	Severidade	Método de Detecção da Falência/ Sintomas Observáveis	Provisão para Compensação	Recomendações	Observações
6	3	Adquirir Tempo de Bordo	TB é adquirido fora da especificação;	Processa fora da especificação; Comunica fora da especificação;	Idem acima	Propagar órbita fora de especificação					
7		Receber TLE	TLE não é recebido	Não processa; Não comunica;	Idem acima	Propagar órbita fora de especificação					
8			TLE é recebido intermitentemente	Processa intermitentemente; Comunica intermitentemente;	Idem acima	(**)					
9			TLE é recebido fora da especificação	Processa fora da especificação; Comunica fora da especificação;	Idem acima	Propagar órbita fora de especificação					
10		Calcular Propagação Orbital	Propagação orbital não é calculada.	Não processa;	Idem acima	Não propagar órbita					
11			Propagação orbital é calculada de forma intermitente.	Processa intermitentemente;	Idem acima	Propagar órbita intermitentemente					

(continua)

Tabela B.7 – Continuação

Identificação	Nível	Função	Modo de Falência	Causa da Falência	Fase da Missão/ Modo de Operação	Efeitos da Falência	Severidade	Método de Detecção da Falência/ Sintomas Observáveis	Provisão para Compensação	Recomendações	Observações
12	3	Calcular Propagação Orbital	Propagação orbital é calculada fora da especificação;	Processa fora da especificação;	Idem acima	Propagar órbita fora de especificação					
13	4	Prover Processamento	Não processa	(*)	Idem acima	TB não é adquirido; TLE não é recebido; Propagação orbital não é calculada.					
14			Processa intermitente	(*)	Idem acima	TB é adquirido de forma intermitente; TLE é recebido intermitentemente; Propagação orbital é calculada de forma intermitente.					
15			Processa fora de especificação	(*)	Idem acima	TB é adquirido fora da especificação; TLE é recebido fora da especificação; Propagação orbital é calculada fora da especificação;					

(continua)

Tabela B.7 – Conclusão

Identificação	Nível	Função	Modo de Falência	Causa da Falência	Fase da Missão/ Modo de Operação	Efeitos da Falência	Severidade	Método de Detecção da Falência/ Sintomas Observáveis	Provisão para Compensação	Recomendações	Observações
16	4	Prover Comunicação	Não comunica	(*)	Idem acima	TB não é adquirido; TLE não é recebido;					
17			Comunica intermitentemente	(*)	Idem acima	TB é adquirido de forma intermitente; TLE é recebido intermitentemente;					
18			Comunica fora de especificação	(*)	Idem acima	TB é adquirido fora da especificação; TLE é recebido fora da especificação;					

(*) Conforme seção 4.1.1.1, as causas das falências das subfunções do nível hierárquico mais baixo da decomposição funcional, são consideradas componentes atômicos da arquitetura funcional e não são decompostas nem é determinada as causas de suas falências.

(**) Este efeito implica ocorrência de falência dupla, ou seja, propagar órbita fora de especificação intermitentemente.

Tabela B.8 – Análise Funcional Hierárquica dos Efeitos dos Modos de Falências da Função ‘Comandar Atuadores’

Identificação	Nível	Função	Modo de Falência	Causa da Falência	Fase da Missão/ Modo de Operação	Efeitos da Falência	Severidade	Método de Detecção da Falência/ Sintomas Observáveis	Provisão para Compensação	Recomendações	Observações
1	2	Comandar Atuadores	Não comanda atuadores		LEOP e fases operacionais	Perda da atitude	Catastrófica	Telemetria	Recarga e execução do OBSW; Redundância física		
2			Comanda atuadores intermitentemente		Idem acima	Perda intermitente da atitude	Catastrófica	Telemetria	Recarga e execução do OBSW; Redundância física		
3			Comanda atuadores fora de especificação		Idem acima	Atitude fora da especificação	Catastrófica	Telemetria	Recarga e execução do OBSW; Redundância física		

Tabela B.9 – Análise Funcional Hierárquica dos Efeitos dos Modos de Falências da Função ‘Gerenciar Modos e Transições’

Identificação	Nível	Função	Modo de Falência	Causa da Falência	Fase da Missão/ Modo de Operação	Efeitos da Falência	Severidade	Método de Detecção da Falência/ Sintomas Observáveis	Provisão para Compensação	Recomendações	Observações
1	2	Gerenciar Modos e Transições	Não gerencia modos e transições		LEOP e fases operacionais	Perda da atitude	Catastrófica	Telemetria	Recarga e execução do OBSW; Redundância física		
2			Gerencia intermitentemente modos e transições		Idem acima	Perda intermitente da atitude	Catastrófica	Telemetria	Recarga e execução do OBSW; Redundância física		
3			Gerencia fora de especificação modos e transições		Idem acima	Atitude fora da especificação	Catastrófica	Telemetria	Recarga e execução do OBSW; Redundância física		

APENDICE C – FMEA FUNCIONAL/FÍSICA DA FUNÇÃO ‘PROVER PROCESSAMENTO’

Na elaboração desta FMEA são utilizados o modelo de tabela e os critérios básicos estabelecidos pela norma ECSS-Q-ST-30-02C (2009). As colunas Método de Detecção da Falência/Sintomas Observáveis, Provisão para Compensação, Recomendações e Observações são preenchidas considerando as soluções adotadas no âmbito das missões com participação brasileira para servirem como referência para este trabalho. A coluna Severidade é preenchida de acordo com os critérios estabelecidos na norma ECSS-Q-ST-30-02C (2009).

Tabela C.1 – Análise Funcional/Física dos Efeitos dos Modos de Falência da Função ‘Prover Processamento’

Identificação	Nível	Função	Modo de Falência	Causa da Falência	Fase da Missão/ Modo de Operação	Efeitos da Falência		Severidade	Método de Detecção da Falência/ Sintomas Observáveis	Provisão para Compensação	Recomendações	Observações
						a) Efeito Local	b) Efeito Final					
1	4	Prover Processamento	Não provê processamento	Perda do micro processador; Perda da PROM; Perda da EEPROM; Perda da RAM	LEOP e fases operacionais;	Local: Não executa <i>software</i> Final: ACDH não fornece tempo de bordo; não provê comunicação; não fornece telecomandos diretos; não fornece telecomandos roteados; não fornece comandos gerados a bordo; não fornece telemetrias; não recupera de falhas no nível 1; não recupera de falhas no nível 2; temperatura fora de controle, atitude fora de controle; órbita fora de controle;	Catastrófica	Cão de guarda	Redundância física			

(continua)

Tabela C.1 – Conclusão

Identificação	Nível	Função	Modo de Falência	Causa da Falência	Fase da Missão/ Modo de Operação	Efeitos da Falência		Severidade	Método de Detecção da Falência/ Sintomas Observáveis	Provisão para Compensação	Recomendações	Observações
						a) b)	Efeito Local Efeito Final					
2	4	Prover Processamento	Provê processamento intermitente	Falha intermitente do microprocessador; Falha intermitente da RAM;	LEOP e fases operacionais;	Local: Executa <i>software</i> de forma intermitente Final: ACDH fornece tempo de bordo de forma intermitente; provê comunicação de forma intermitente; fornece tecomandos diretos de forma intermitente; fornece telecomandos roteados de forma intermitente; fornece comandos gerados a bordo de forma intermitente; fornece telemetrias de forma intermitente;	Catastrófica	Telemetria, OBSW	Redundância física			
3			Provê processamento fora do especificado	Erro no <i>software</i> ;	LEOP e fases operacionais;	Local: Executa <i>software</i> errado Final: ACDH fornece tempo de bordo errado; provê comunicação com erro; fornece comandos gerados a bordo errados; fornece telemetrias com erro; erro no controle da temperatura; erro no controle da atitude; erro no controle da órbita.	Catastrófica	Telemetria, OBSW, Cão de guarda;	Recarga e execução do OBSW;			

