

**UNIVERSIDADE FEDERAL DE SANTA CATARINA
DEPARTAMENTO DE ENGENHARIA MECÂNICA**

Eduardo Yuji Sakurada

**METODOLOGIA PARA ANÁLISE DE CONFIABILIDADE
DINÂMICA**

Florianópolis

2013

Eduardo Yuji Sakurada

**METODOLOGIA PARA ANÁLISE DE CONFIABILIDADE
DINÂMICA**

Tese submetida ao Programa de Pós-Graduação em Engenharia Mecânica para a obtenção do Grau de Doutor em Engenharia Mecânica.

Orientador: Prof. Acires Dias, Dr. Eng.

Coorientador: Prof. Bernardo Luís Rodrigues de Andrade, Dr. Eng.

Florianópolis

2013

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

S111m Sakurada, Eduardo Yuji
Metodologia para análise de confiabilidade dinâmica /
Eduardo Yuji Sakurada ; orientador, Acires Dias ; co-
orientador, Bernardo Luís Rodrigues de Andrade. -
Florianópolis, SC, 2013.
259 p.

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

Inclui referências

1. Engenharia mecânica. 2. Confiabilidade dinâmica. 3.
Análise de falhas. 4. Modelagem de sistemas. I. Dias,
Acires. II. Andrade, Bernardo Luís Rodrigues de. III.
Universidade Federal de Santa Catarina. Programa de Pós-
Graduação em Engenharia Mecânica. IV. Título.

CDU 621

Eduardo Yuji Sakurada

**METODOLOGIA PARA ANÁLISE DE CONFIABILIDADE
DINÂMICA**

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

Florianópolis, 08 de abril 2013.

Prof. Júlio César Passos, Dr. Eng.
Coordenador do Curso

Prof. Acires Dias, Dr. Eng.
Orientador

Prof. Bernardo Luís Rodrigues de Andrade, Dr. Eng.
Coorientador

Banca Examinadora:

Prof. Acires Dias, Dr. Eng.
Presidente

Prof. Gilberto Martha de Souza, Ph.D.

Banca Examinadora (continuação):

Prof. Cristiano Vasconcellos Ferreira, Dr. Eng.

Prof. Leonam dos Santos Guimarães, Ph.D.

Prof. Ubirajara Franco Moreno, Dr. Eng.

Prof. Victor Juliano De Negri, Dr. Eng.

À Taliana e à Ayumi, pelo amor e felicidade
que me proporcionam.

AGRADECIMENTOS

Aos estimados professores Acires Dias e Bernardo Luís Rodrigues de Andrade pela orientação e pelo apoio ao longo do desenvolvimento deste trabalho.

Aos professores que participaram da banca de defesa do exame de qualificação e da defesa de tese: Armando Albertazzi Gonçalves Júnior, André Ogliari, Victor Juliano De Negri, Ubirajara Franco Moreno, Leonam dos Santos Guimarães, Gilberto Martha de Souza e Cristiano Vasconcellos Ferreira, pelas observações e sugestões valiosas que contribuíram para a melhoria do trabalho final.

Ao professor Jonny Carlos da Silva por auxiliar com os conceitos relacionados à modelagem e simulação de sistemas.

Aos amigos Luís Fernando Peres Calil, Heitor Azuma Kagueiama, Rodrigo Rizzi Starr e Luis Antonio Pereira de Lima pelo companheirismo, pela parceria nos estudos e valorosas discussões.

Aos colegas do Núcleo de desenvolvimento Integrado de Produtos (NeDIP), especialmente à Cindy Ibarra por auxiliar na representação da metodologia e Juliano Mazute pelo suporte momentos antes da apresentação do trabalho.

Aos colegas Luiz Fernando Segalin de Andrade, Henrique Cezar Pavanati e Rogério Pereira, do IFSC, pelo apoio.

À Taliana pela paciência, carinho e confiança depositada em mim.

À família, em especial aos meus pais, Tetsuya e Sada, pelo carinho, educação e incentivo.

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

Reunir-se é um começo, permanecer juntos é um progresso, e trabalhar juntos é sucesso.

Henry Ford

RESUMO

A análise de confiabilidade dinâmica é bastante recente e está sendo demandada para análise de confiabilidade em sistemas complexos, mas até o momento há poucas publicações no Brasil. As primeiras publicações fora do país iniciaram na década de 1980, mas foi na década de 1990 que o assunto ganhou mais volume. Por ser uma nova abordagem da confiabilidade, muitas análises são dependentes dos especialistas e os aplicativos criados estão vinculados aos sistemas para os quais foram desenvolvidos. Existem vários aspectos que caracterizam uma análise de confiabilidade dinâmica, tais como: análise instantânea da confiabilidade, taxa de falha com degradação, avaliação dos fatores humanos, avaliação do comportamento dinâmico das variáveis de processo, entre outros. Em princípio, a técnica permite modelar sistemas de maneira mais realista para os propósitos da análise de confiabilidade, risco e segurança. No entanto, por considerar uma quantidade maior de variáveis, interações entre sistemas, entre outros fatores, a análise de confiabilidade dinâmica exige uma maior quantidade de informações, modelagem mais complexa, maior custo de processamento computacional e tempo. Isso faz com que se dê preferência em trabalhar com a análise de confiabilidade estática. Todavia, tem-se observado ao longo da história, incidentes graves em sistemas como usinas nucleares, aeronaves, grandes embarcações, etc, que são sistemas complexos com grande potencial catastrófico. Portanto, não se satisfazem com a análise estática de confiabilidade, ou seja, para uma taxa de falha definida num tempo estabelecido. Por causa disso, a análise de confiabilidade dinâmica começou a ser incorporada dentro das metodologias para avaliação de risco e segurança, agregando mais informação para as análises. O presente trabalho apresenta uma proposta de metodologia para a análise de confiabilidade dinâmica, na qual são consideradas: o comportamento dinâmico do sistema devido às falhas, ações de manutenção e atualização do modelo ao longo do tempo. Para isso, a metodologia se fundamenta no método de Monte Carlo e na modelagem a eventos discretos com comportamento semi-markoviano. Adicionalmente, são utilizados alguns métodos e técnicas para dar suporte como: Análise do modo de falha, efeitos e criticidade (FMECA), Análise de eventos por rede causal (CNEA), Diagramas de blocos para confiabilidade e Manutenção centrada em confiabilidade (MCC). Deseja-se com o uso da metodologia facilitar a análise de confiabilidade dinâmica de sistemas e, por consequência, obter modelos de confiabilidade mais próximos da realidade e atualizados. Foram feitas duas aplicações da metodologia: a primeira num problema clássico proposto no *workshop* organizado pela associação italiana

3ASI (*Associazione degli Analisti dell'Ambiente, dell'Affidabilità e della Sicurezza Industriale*) em 2004, de análise de confiabilidade dinâmica; a segunda num “sistema real” – sistema hidráulico de governo de um navio petroleiro.

Palavras-chave: Confiabilidade dinâmica, análise de falhas, modelagem de sistemas.

ABSTRACT

Dynamic reliability analysis is quite recent and is becoming a demand for the reliability analysis on complex systems, but so far there are not as many publications on the subject in Brazil. The first publications are dated from the 1980's, but it was only in the 1990's that the subject gained more volume. Since it is a new approach in reliability, many analyses are dependent on specialists and the computer systems created are linked to the system for which they were developed. There are many aspects that characterize a dynamic reliability analysis, such as: instant reliability analysis, failure rate with degradation, human factor evaluation, evaluation of the dynamic behavior of process variables, among others. In principle, the technique allows the system modeling in a more realistic way for the reliability, risk and safety analysis purposes. On the other hand, since the analysis demand the consideration of a larger number of variables, systems interactions, among other factors, the dynamic reliability analysis requires a larger amount of information, a more complex model, higher cost in computer processing and time. This makes it preferable to work with a static reliability analysis. However, it may be observed in history that severe incidents in systems such as nuclear power plants, aircrafts, large vessels etc., which are complex systems with great catastrophic potential. Therefore, it is not enough to use the static reliability analysis, using a defined failure rate in a specific time. For this reason, the dynamic reliability analysis began to be incorporated in risk and safety evaluation methodologies, adding more information to the analysis. This work presents a methodology proposal for the dynamic reliability analysis, in which are considered: failure dynamic behavior and the model update over time. With this purpose, the methodology is grounded on the Monte Carlo method and discrete events with semi-markovian behavior modeling. Additionally, methods and techniques are used to support the analysis, like: Failure mode, event and criticality analysis (FMECA), Causal network event analysis (CNEA), Reliability block diagrams and Reliability centered maintenance (MCC). The use of this methodology aims to facilitate the system dynamic reliability analysis, consequently, reaching reliability models closer to reality and updated. Two applications were made: the first in a classic problem proposed in the workshop on dynamic reliability analysis organized by the Italian association 3ASI (Associazione degli Analisti dell'Ambiente, dell'Affidabilità e della Sicurezza Industriale) in 2004; and the second in a existing system – the hydraulic system of a oil tanker rudder.

Keywords: Dynamic reliability, failure analysis, system modeling.

LISTA DE FIGURAS

Figura 1.1	Estados do sistema técnico	45
Figura 2.1	Representação do comportamento dinâmico em função dos estados dos componentes (i_1, i_2, \dots) e do tempo t	50
Figura 2.2	Estrutura geral de uma plataforma para confiabilidade dinâmica	55
Figura 2.3	Modelo para predição da confiabilidade	56
Figura 3.1	Exemplo de tabela para FMECA	61
Figura 3.2	Diagrama de uma análise de eventos por rede causal (CNEA)	63
Figura 3.3	Taxonomia da CNEA	64
Figura 3.4	Exemplo de uma caixa e setas	65
Figura 3.5	Exemplo de aplicação de IDEF0	66
Figura 3.6	Configuração em série	67
Figura 3.7	Configuração em paralelo	67
Figura 3.8	Configuração em ponte	68
Figura 3.9	(a)Delta-estrela (b)R-em-N (c)Trimodular (d) <i>Stand-by</i>	68
Figura 3.10	Fluxograma para simulação de Monte Carlo	70
Figura 3.11	Procedimento de referência para implantação da MCC	71
Figura 4.1	Classificação do modelo comportamental utilizado pela metodologia	76
Figura 4.2	Modelo de referência para cada etapa da metodologia	77
Figura 4.3	Metodologia para análise de confiabilidade dinâmica (ACoDi)	78
Figura 4.4	Processo de desenvolvimento integrado de produtos – PRODIP	79
Figura 4.5	Relação da metodologia ACoDi com o PRODIP	79
Figura 4.6	Relação da metodologia com todo o ciclo de vida do produto	81
Figura 4.7	Atividades da etapa 1	83
Figura 4.8	Critérios para o uso da confiabilidade dinâmica	85
Figura 4.9	Relações determinísticas para avaliar a aceitação do risco	87
Figura 4.10	Relações determinísticas para escolha da análise de confiabilidade dinâmica	88
Figura 4.11	Atividade da etapa 2	90
Figura 4.12	Atividades da etapa 3	91

Figura 4.13	Priorização da análise	92
Figura 4.14	Desdobramento da função global	93
Figura 4.15	Variação de temperatura após falha do sistema de refrigeração	97
Figura 4.16	Mudança no nível da variável de controle	97
Figura 4.17	Comportamento do sistema de segunda ordem em função de ξ	99
Figura 4.18	Atividades da etapa 4	101
Figura 4.19	Sistema com componentes C_1 e C_2 (reserva)	102
Figura 4.20	Diagrama de blocos para confiabilidade com sensor, controlador e atuador	102
Figura 4.21	Exemplo de análise de sistema a partir do controle do nível de fluido do reservatório	104
Figura 4.22	Diagrama de blocos para análise de um sistema de controle realimentado	104
Figura 4.23	Regiões de operação do sistema	105
Figura 4.24	Tempo de reação para início da manutenção preditiva	107
Figura 4.25	Atuação sobre o avanço da variável de controle	109
Figura 4.26	Manutenção em série	111
Figura 4.27	Manutenção em paralelo	112
Figura 4.28	Manutenção mista	113
Figura 4.29	Atividades da etapa 5	115
Figura 4.30	Exemplo de simulação realizada manualmente	116
Figura 4.31	Representação do fluxo de informação do <i>software</i>	117
Figura 4.32	Fluxograma para desenvolvimento do <i>software</i>	119
Figura 4.33	Válvula direcional com falha do tipo aberta e fechada	122
Figura 4.34	Fluxograma para avaliação da “Condição de falha nos componentes” no <i>software</i> (Figura 4.32)	124
Figura 4.35	Variáveis de entrada e saída do controlador	125
Figura 4.36	Ação do controlador diante da posição da variável de controle y	126
Figura 4.37	Atividade da etapa 6	128
Figura 4.38	Cenário com sucesso da missão	129
Figura 4.39	Relatório para o cenário apresentado na Figura 4.38	131
Figura 4.40	Obtenção da função densidade de falha	132
Figura 4.41	Rotina para gerar um conjunto de funções densidade de falha	133
Figura 4.42	Relação entre a metodologia ACoDi e a MCC	135
Figura 4.43	Procedimento de análise de segurança	136
Figura 5.1	Problema proposto	139
Figura 5.2	Desdobramento da função global do sistema técnico	142

Figura 5.3	Estados dos componentes	144
Figura 5.4	Regiões de operação para o reservatório	148
Figura 5.5	Cenário com falha na bomba P1	150
Figura 5.6	Cenário com falha na bomba P2	150
Figura 5.7	Cenário com falha oculta na bomba P2	151
Figura 5.8	Comportamento dinâmico de um teste de simulação	152
Figura 5.9	Relatório ponto a ponto ao longo de um tempo de missão	153
Figura 5.10	Histogramas de falhas em 10 mil testes	154
Figura 5.11	Função distribuição acumulada de falhas	155
Figura 5.12	Distribuição de pontos para transbordamento	156
Figura 5.13	Distribuição de pontos para esvaziamento	156
Figura 5.14	Distribuição amostral de X	157
Figura 5.15	Função distribuição acumulada de falhas para trans- bordamento	158
Figura 5.16	Função distribuição acumulada de falhas para esva- ziamento	159
Figura 5.17	Modelo do sistema com GSPN	160
Figura 5.18	Modelo do sistema com FSPN	162
Figura 5.19	Função distribuição acumulada de falhas para trans- bordamento	163
Figura 5.20	Função distribuição acumulada de falhas para esva- ziamento	164
Figura 5.21	Correlação entre os pontos – Transbordamento	165
Figura 5.22	Correlação entre os pontos – Esvaziamento	165
Figura 6.1	Circuito hidráulico do sistema de governo do leme .	168
Figura 6.2	Análise funcional do SHA para os subsistemas de primeiro nível	170
Figura 6.3	Diagrama estrutural do sistema hidráulico de aciona- mento do leme	171
Figura 6.4	Diagrama de blocos para confiabilidade – Máquina do leme	172
Figura 6.5	Estados dos componentes reparáveis	173
Figura 6.6	Estados dos componentes não reparáveis	174
Figura 6.7	Regiões de operação com tempo limite para falha e comutação	176
Figura 6.8	Comportamento com falha oculta	177
Figura 6.9	Comportamento do sistema e dos componentes	179
Figura 6.10	Parte do relatório ponto a ponto para a Figura 6.11	181
Figura 6.11	Comportamento dinâmico para simulação para $t_{Limite} =$ 30 minutos	182

Figura 6.12	Ampliação da Figura 6.11 nas etapas 2, 3, 4 e 5 da simulação	183
Figura 6.13	Ampliação da Figura 6.11 nas etapas 6 e 7 da simulação	183
Figura 6.14	Ampliação da Figura 6.11 nas etapas 9, 10, 11 e 12 da simulação	184
Figura 6.15	Histograma de falhas para sistema de governo do leme ($t_{Limite} = 30$ minutos)	185
Figura 6.16	Função distribuição acumulada de falhas($t_{Limite} = 30$ minutos)	186
Figura 6.17	Probabilidade de falha em função do tempo de missão	188
Figura 6.18	Probabilidade de falha em função do tempo limite sem vazão	188
Figura 6.19	Probabilidade de falha sem manutenção	189
Figura 6.20	Probabilidade de falha em função das taxas de reparo	190
Figura 6.21	Probabilidade de falha em função das taxas de reparo (10mil horas)	190
Figura A.1	Sistema massa-mola – modelo comportamental estático	210
Figura A.2	Sistema massa-mola – modelo comportamental dinâmico	211
Figura A.3	Classificação dos modelos comportamentais	212
Figura A.4	Função densidade de probabilidade de falha hipotética $f(x)$ em função da vida x	216
Figura A.5	Confiabilidade em função do tempo para distribuição exponencial	218
Figura A.6	Correlação entre confiabilidade, manutenibilidade e disponibilidade para produtos reparáveis	219
Figura A.7	Comportamento da variável $X(t)$ ao longo do tempo	220
Figura A.8	Desencadeamento de um incidente	222
Figura A.9	Funções amostra ou realizações do processo	223
Figura A.10	Possíveis estados de um componente	224
Figura A.11	Possíveis estados do sistema	225
Figura A.12	Mudanças de estados de um componente	227
Figura C.1	Probabilidade de falha por transbordamento – P1P2V	235
Figura C.2	Probabilidade de falha por esvaziamento – P1P2V .	236
Figura C.3	Probabilidade de falha por transbordamento – VP1P2	236
Figura C.4	Probabilidade de falha por esvaziamento – VP1P2 .	237
Figura D.1	Problema exemplo	241
Figura D.2	Diagrama de blocos para confiabilidade	241
Figura E.1	Árvore de eventos discreta dinâmica	249
Figura E.2	(a) Uma simples rede de Petri (b) Depois do disparo de T1	251

Figura E.3	Redes de Petri temporizadas	253
Figura E.4	Estados e eventos de um DRBD	256

LISTA DE TABELAS

Tabela 6.1	Valores de probabilidade de falha (ACoDi)	186
Tabela 6.2	Valores de confiabilidade e probabilidade de falha (Confiabilidade estática)	187
Tabela 6.3	Valores de probabilidade de falha para análise sem manutenção	189
Tabela B.1	Dados para transbordamento (Metodologia ACoDi)	231
Tabela B.2	Dados para esvaziamento (Metodologia ACoDi)	231
Tabela B.3	Dados para transbordamento (Redes de Petri)	232
Tabela B.4	Dados para esvaziamento (Redes de Petri)	232
Tabela D.1	Probabilidades de falha e confiabilidade de cada componente	243

LISTA DE QUADROS

Quadro 3.1	Referências bibliográficas recomendadas para técnicas de suporte	59
Quadro 5.1	Funções dos componentes do sistema técnico	143
Quadro 5.2	Características dos componentes	144
Quadro 5.3	Taxa de variação do nível H	145
Quadro 5.4	Configurações do sistema em função do nível	146
Quadro 5.5	Discretização do nível H	161
Quadro 6.1	Vazão disponível para o sistema	174
Quadro 6.2	Taxas de falhas dos componentes	187
Quadro A.1	Sistema dinâmico	213
Quadro A.2	Elementos da definição da norma NBR 5462	215
Quadro A.3	Condição funcional e operacional dos componentes . .	224
Quadro D.1	Possíveis configurações no sistema reservatório baseado em árvore de eventos	244
Quadro E.1	Portas lógicas dinâmicas	251
Quadro E.2	Eventos, condições e portas da estrutura ESD	254

LISTA DE SIGLAS

ACH	Análise de confiabilidade humana
ACoDi	Análise de confiabilidade dinâmica
CNEA	<i>Causal network event analysis</i> (Análise de evento por redes causais)
DFM	<i>Dynamic flowgraph methodology</i> (Metodologia do fluxograma dinâmico)
DETA	<i>Dynamic event tree analysis</i> (Análise por árvore de eventos dinâmica)
DETAM	<i>Dynamic event tree analysis method</i> (Método da análise por árvore de eventos dinâmica)
DFTA	<i>Dynamic fault tree analysis</i> (Análise por árvore de falhas dinâmica)
DRBD	<i>Dynamic reliability block diagram</i> (Diagrama de blocos para confiabilidade dinâmica)
DYLAM	<i>Dynamic logical analytical methodology</i>
DoD	<i>Department of Defense</i> (Departamento de defesa)
ESD	<i>Event sequence diagram</i> (Diagrama sequencial de eventos)
FESD	<i>Functional event sequence diagram</i> (Diagrama sequencial de eventos funcionais)
ETA	<i>Event tree analysis</i> (Análise por árvore de eventos)
FMEA	<i>Failure mode and effects analysis</i> (Análise do modo de falha e seus efeitos)
FMECA	<i>Failure modes, effects and criticality analysis</i> (Análise do modo de falha, efeitos e criticidade)
FTA	<i>Fault tree analysis</i> (Análise por árvore de falha)
FSPN	<i>Fluid Stochastic Petri Nets</i> (Redes de Petri Fluidas e Estocásticas)

GSPN	<i>Generalized Stochastic Petri Nets</i> (Redes de Petri Estocásticas Generalizadas)
HRA	<i>Human reliability analysis</i> (Análise de confiabilidade humana)
IDEFO	<i>Integration definition for function modeling</i>
LabRisco	Laboratório de análise, avaliação e gerenciamento de risco
LASHIP	Laboratório de Sistemas Hidráulicos e Pneumáticos
MCC	Manutenção centrada em confiabilidade
MTBF	<i>Mean time between failures</i> (Tempo médio entre falhas)
MTTR	<i>Mean time to repair</i> (Tempo médio de reparo)
NPR	Número de prioridade de risco (<i>Risk priority number</i>)
NeDIP	Núcleo de Desenvolvimento Integrado de Produtos
PRA	<i>Probabilistic risk assessment</i> (Avaliação probabilística de risco)
PRODIP	Processo de desenvolvimento integrado de produtos
PSA	<i>Probabilistic safety assessment</i> (Avaliação probabilística de segurança)
RBD	<i>Reliability block diagram</i> (Diagramas de blocos para confiabilidade)
SA	Subsistema de atuação
SED	Sistema a eventos discretos
SI	Subsistema de isolamento
SP1	Subsistema de potência 1
SP2	Subsistema de potência 2
TB	Tubulações do sistema hidráulico de governo do leme
UFSC	Universidade Federal de Santa Catarina
USP	Universidade de São Paulo
VE	Válvulas esfera do sistema hidráulico de governo do leme

LISTA DE SÍMBOLOS

$D(t)$	Disponibilidade instantânea para um tempo t
D	Disponibilidade estacionária
$f(x)$	Função densidade de probabilidade de falha da variável x
$F(t)$	Função distribuição de probabilidade de falha ou função distribuição acumulada de falhas da variável t
$IC_{1-\alpha}(\mu)$	Intervalo de confiança de um parâmetro μ , para uma probabilidade $(1 - \alpha)$
$P(j \rightarrow i y)$	Probabilidade de transição de j para i , dado estado y
$Q(x)$	Probabilidade de falha para um tempo de vida x
$R(x)$	Confiabilidade para um tempo de vida x
t	Variável tempo em horas
μ	Taxa de reparo [reparos/hora]
λ	Taxa de falha [falhas/hora]

SUMÁRIO

1	INTRODUÇÃO	37
1.1	Justificativa	41
1.2	Objetivos	43
1.2.1	Objetivo geral	43
1.2.2	Objetivos específicos	43
1.2.3	Resultados esperados	43
1.3	Definições e conceitos preliminares	43
1.3.1	Definição de confiabilidade dinâmica	44
1.3.2	Os modelos para a análise de confiabilidade estática e dinâmica	44
1.4	Estrutura do documento	45
2	CONFIABILIDADE DINÂMICA	47
2.1	Diferentes abordagens para análise de confiabilidade dinâmica	47
2.2	Comportamento dinâmico dos sistemas	49
2.3	Comportamento determinístico e estocástico	51
2.4	Área de aplicação	52
2.5	Estrutura geral de uma análise de confiabilidade dinâmica . .	55
2.6	Considerações do capítulo	57
3	PRINCIPAIS TÉCNICAS PARA DAR SUPORTE À METODOLOGIA	59
3.1	Análise do modo de falha, efeitos e criticidade (FMECA) . .	60
3.2	Análise de eventos por rede causal (CNEA)	62
3.3	<i>Integration definition for function modeling</i> (IDEF0)	64
3.4	Diagramas de blocos para confiabilidade	66
3.5	Método de Monte Carlo	69
3.6	Manutenção centrada em confiabilidade (MCC)	69
3.7	Considerações do capítulo	72
4	METODOLOGIA PROPOSTA PARA ANÁLISE DE CONFIABILIDADE DINÂMICA	75
4.1	Caracterização do sistema abordado pela metodologia	75
4.1.1	Variáveis de estado do sistema	75
4.1.2	Estado do sistema	75
4.2	Modelo de referência	76
4.3	Atualização do modelo	80

4.4	Etapa 1: Análise inicial do sistema técnico para confiabilidade dinâmica	82
4.4.1	Atividade 1.1: Análise quanto ao comportamento dinâmico	82
4.4.2	Atividade 1.2: Análise da criticidade do sistema . . .	83
4.4.3	Atividade 1.3: Análise da disponibilidade do sistema	84
4.4.4	Atividade 1.4: Análise do sistema	85
4.5	Etapa 2: Definição da equipe	88
4.6	Etapa 3: Análise do sistema, subsistemas e componentes . .	89
4.6.1	Atividade 3.1: Desdobramento das funções do sistema	91
4.6.2	Atividade 3.2: Caracterização dos subsistemas e componentes	94
4.6.3	Atividade 3.3: Descrição comportamental do sistema	96
4.7	Etapa 4: Análise da manutenção do sistema técnico	100
4.7.1	Atividade 4.1: Caracterização dos sensores, controlador e atuadores	101
4.7.2	Atividade 4.2: Definição das regiões de operação . .	105
4.7.3	Atividade 4.3: Modelagem do comportamento em função da manutenção	106
4.7.3.1	Tempo de reação	107
4.7.3.2	Atuação sobre o avanço da variável de controle	108
4.7.3.3	Manutenção preditiva com o sistema em operação	109
4.7.3.3.1	Modelagem em série da manutenção	111
4.7.3.3.2	Modelagem em paralelo da manutenção	111
4.7.3.3.3	Modelagem mista da manutenção	112
4.7.3.3.4	Modelagem sem manutenção . .	113
4.7.3.4	Falhas ocultas	114
4.8	Etapa 5: Modelagem e simulação	114
4.8.1	Atividade 5.1: Representação do comportamento dinâmico do sistema	114
4.8.2	Atividade 5.2: Estrutura para implementação	116
4.8.2.1	Diagrama de fluxo do <i>software</i>	118
4.8.2.2	Inicialização das variáveis	118
4.8.2.2.1	Armazenamento dos dados do sistema	120
4.8.2.2.2	Armazenamento dos dados dos componentes	121

4.8.2.3	Sorteio de: tipos de falha, tempos de falha e reparo	122
4.8.2.4	Ordenação cronológica das falhas dos componentes	123
4.8.2.5	Tempo de missão ($t_{missão}$) e falha do sistema	123
4.8.2.6	Condição de falha dos componentes	123
4.8.2.7	Ações do controlador	124
4.8.2.8	Cálculo dy/dt para definir a variação do sistema	126
4.8.2.9	Determinação do próximo evento e tempo associado	126
4.8.2.10	Próximo tempo t e estado y	127
4.9	Etapa 6: Análise de resultados	127
4.9.1	Atividade 6.1: Geração de relatórios ponto a ponto e cenários de simulação	128
4.9.1.1	Cenários de simulação	128
4.9.1.2	Relatório ponto a ponto	129
4.9.2	Atividade 6.2: Cálculo da probabilidade de falha e confiabilidade do sistema técnico	130
4.10	Relação entre a metodologia ACoDi e a MCC	134
4.11	Relação entre a metodologia ACoDi e a Análise de Segurança de Sistemas	135
4.12	Considerações do capítulo	137

5 APLICAÇÃO EM UM PROBLEMA CLÁSSICO 139

5.1	Etapa 1: Análise inicial do sistema técnico para confiabilidade dinâmica	140
5.2	Etapa 2: Definição da equipe	141
5.3	Etapa 3: Análise do sistema, subsistemas e componentes	141
5.3.1	Atividade 3.1: Desdobramento das funções do sistema	142
5.3.2	Atividade 3.2: Caracterização dos subsistemas e componentes	143
5.3.3	Atividade 3.3: Descrição comportamental do sistema	145
5.4	Etapa 4: Análise da manutenção do sistema técnico	146
5.4.1	Atividade 4.1: Caracterização dos sensores, controlador e atuadores	146
5.4.2	Atividade 4.2: Definição das regiões de operação	147
5.4.3	Atividade 4.3: Modelagem do comportamento em função da manutenção	148
5.4.3.1	Tempo de reação	148

5.4.3.2	Atuação sobre o avanço da variável de controle H	148
5.4.3.3	Manutenção preditiva com o sistema em operação	149
5.5	Etapa 5: Modelagem e simulação	149
5.6	Etapa 6: Análise de resultados	151
5.6.1	Atividade 6.1: Geração dos relatórios ponto a ponto e cenários de falha	152
5.6.2	Atividade 6.2: Cálculo da probabilidade de falha e confiabilidade do sistema técnico	154
5.7	Análise com redes de petri	158
5.8	Análise comparativa entre os resultados	161
5.8.1	Quanto à implementação computacional	161
5.8.2	Resultados numéricos	163
5.9	Considerações do capítulo	166
6	APLICAÇÃO EM UM SISTEMA REAL	167
6.1	Etapa 1: Análise inicial do sistema técnico para confiabilidade dinâmica	167
6.1.1	Atividade 1.1: Análise quanto ao comportamento dinâmico	169
6.1.2	Atividade 1.2: Análise da criticidade do sistema	169
6.1.3	Atividade 1.3: Análise da disponibilidade do sistema	169
6.1.4	Atividade 1.4: Análise do sistema	169
6.2	Etapa 2: Definição da equipe	170
6.3	Etapa 3: Análise do sistema, subsistema e componentes	170
6.3.1	Atividade 3.1: Desdobramento das funções do sistema	170
6.3.2	Atividade 3.2: Caracterização dos subsistemas e componentes	173
6.3.3	Atividade 3.3: Descrição comportamental do sistema	174
6.4	Etapa 4: Análise da manutenção do sistema técnico	175
6.4.1	Atividade 4.1: Caracterização dos sensores, controlador e atuadores	175
6.4.2	Atividade 4.2: Definição das regiões de operação	175
6.4.3	Atividade 4.3: Modelagem do comportamento em função da manutenção	175
6.4.3.1	Tempo de reação	175
6.4.3.2	Atuação sobre o avanço da variável de controle	176
6.4.3.3	Manutenção preditiva com o sistema em operação	176

6.4.4	Falhas ocultas	178
6.5	Etapa 5: Modelagem e simulação	178
6.6	Atividade 5.1: Representação do comportamento dinâmico do sistema	178
6.7	Atividade 5.2: Estrutura para implementação	178
6.8	Etapa 6: Análise de resultados	180
6.8.1	Atividade 6.1: Geração dos relatórios ponto a ponto e cenários de falha	180
6.8.2	Atividade 6.2: Cálculo da probabilidade de falha e confiabilidade do sistema técnico	185
6.8.3	Análise de confiabilidade estática	186
6.8.4	Análise comparativa entre a confiabilidade estática e a metodologia ACoDi	187
6.9	Considerações do capítulo	191
7	CONCLUSÕES E RECOMENDAÇÕES PARA TRABALHOS FUTUROS	193
7.1	Quanto aos objetivos	194
7.2	Resultados e contribuições	195
7.3	Recomendações para trabalhos futuros	197
	REFERÊNCIAS	199
	APÊNDICE A – Conceitos e definições	209
	APÊNDICE B – Valores obtidos na simulação do problema clássico	231
	APÊNDICE C – Simulação do problema clássico com componentes reparáveis em série	235
	APÊNDICE D – Análise do reservatório: confiabilidade clássica	241
	APÊNDICE E – Técnicas e ferramentas adicionais	249

1 INTRODUÇÃO

A norma NBR 5462/1994 define a confiabilidade como sendo “a capacidade de um item desempenhar uma função requerida sob condições especificadas, durante um dado intervalo de tempo” (ABNT, 1994). Porém, a mensuração da confiabilidade geralmente está associada a um valor de probabilidade, o que permite, desta forma, avaliar quantitativamente a capacidade do item (sistema ou componente) de realizar sua função.

A análise de confiabilidade se desdobra em aplicações diversas como: na análise de falhas de sistemas e componentes, nos projetos para confiabilidade, na manutenção centrada em confiabilidade (MCC), na elaboração dos períodos de garantia, entre outras atividades – buscando melhorar a qualidade dos produtos e serviços.

Existem duas abordagens para a confiabilidade: estrutural e funcional. A primeira tem seu foco voltado para as estruturas dos sistemas técnicos. Nesse tipo de análise, para uma dada condição inicial de carregamento, verifica-se os valores de tensão, deformação e deslocamento que podem ocorrer nas estruturas. Para essa abordagem, utiliza-se técnicas de simulação numérica como elementos finitos, elementos de contorno, diferenças finitas, entre outras. Sabe-se que os valores de solicitação e resistência não são perfeitamente definidos, pois variam dentro de um intervalo de forma probabilística. Desta forma, a probabilidade dos sistemas resistirem, ou não, depende das funções densidade de probabilidade – dos valores de primeiro momento, de segundo momento, etc – associadas à solicitação, à resistência e aos ciclos aplicados ao longo da vida.

Da Rosa (2002) apresenta aspectos estruturais dos projetos mecânicos, particularmente a mecânica da fratura e fadiga. No texto o autor discute o processo clássico de projeto – que faz uso de coeficientes de segurança – e a análise com enfoque probabilístico, que considera a dispersão dos valores das variáveis de projeto. O autor apresenta a seguinte definição de confiabilidade:

[...] é a probabilidade de que um componente, ou sistema, operando dentro dos limites de projeto, não falhe durante o período de tempo previsto para a sua vida, dentro das condições de agressividade do meio (DA ROSA, 2002, p.32).

Por outro lado, a confiabilidade funcional está centrada na função do sistema, inter-relacionando as várias tecnologias presentes nos sistemas técnicos. Com base nos modos de falhas e nas taxas de falhas dos componentes – obtidos em testes laboratoriais ou observações em campo – estima-se as probabilidades do sistema funcionar, ou falhar, para um dado período de

tempo.

Tanto em um caso quanto no outro – estrutural ou funcional – poderá ser desenvolvida uma análise de confiabilidade estática, a mais comum, ou dinâmica. O que é chamado de confiabilidade estática, ou simplesmente confiabilidade, é caracterizada pela visão de se desenvolver uma análise num momento definido, a partir da elaboração de um modelo de confiabilidade e de uma taxa de falha para cada um dos componentes que compõem o sistema técnico em análise. Para esse tipo de modelo, no momento em que ocorre a falha, o sistema fica fora de operação, período em que são realizadas as manutenções.

Na análise de confiabilidade dinâmica a condição do sistema não fica definida somente por “falha” e “não-falha”, ou seja, o sistema ainda pode trabalhar em uma condição de “falha parcial” antes de chegar à “falha total”. Basicamente, quando se tem uma falha parcial e esta é detectada, ocorre a ação de um controlador para restabelecer o sistema para sua condição normal de operação. Ou seja, dado que se identificou uma condição fora do normal, é disparado um comando para que outros componentes entrem ou saiam de operação. Os sistemas que possuem falhas em seus componentes e, ainda assim, desempenham sua função são conhecidos como “sistemas tolerantes a falhas”. No trabalho de Domínguez-García et al. (2008) o autor apresenta uma metodologia para trabalhar de forma integrada a confiabilidade e a análise de desempenho de sistemas tolerantes a falhas. Para isso, na modelagem do comportamento dinâmico são consideradas as informações como sobressinal (*overshoot*), tempo de acomodação (*settling time*), entre outros parâmetros, junto com as cadeias de Markov, que representam as diferentes configurações do sistema.

Paralelamente às mudanças de configuração do sistemas tolerantes a falhas, pode-se, além disso, incluir a execução da manutenção “a quente”¹ dos componentes em falha. Desta forma, mesmo que as taxas de falha dos componentes permaneçam constantes, a confiabilidade do sistema pode mudar, bastando que se tenha sensores para identificar os componentes em falha, controlador para disparar a ação e a possibilidade de executar a manutenção do sistema durante a operação. Tais ações podem influenciar diretamente no aumento da confiabilidade do sistema, visto que haveria menos componentes em falha.

No artigo publicado por Wang et al. (2012), a análise confiabilidade de dinâmica é realizada em sistemas eletrônicos com o objetivo de capturar o processo de envelhecimento de *hardware*. Para isso é feito um monitoramento com sensores que indicam o processo de degradação do equipamento, obtendo o valor da confiabilidade atual do sistema. Com esses dados torna-se possível

¹Manutenção a quente é o serviço de manutenção com o sistema em operação.

tomar medidas para prolongar a vida e prevenir falhas do equipamento.

A análise dinâmica tem um custo maior porque exige um maior monitoramento do sistema, um esforço computacional maior, maior conhecimento sobre o sistema, entre outros fatores. Por causa desse trabalho mais exigente, as aplicações são destinadas a sistemas complexos com grande potencial catastrófico como nas áreas nuclear, aviação, petroquímica, entre outras.

No entanto, esse cenário restrito vem mudando, sendo um dos fatores que contribuem para o uso da confiabilidade dinâmica é a evolução na capacidade de processamento dos computadores. Segundo Manno et al. (2012) essa melhoria no esforço computacional tem incentivado o uso de modelagens com métodos numéricos para resolução dos problemas, pois são mais simples e flexíveis em comparação com as soluções analíticas. Manno et al. (2012) utiliza o método de Monte Carlo combinado com a análise por árvore de falhas (FTA) para resolver problemas de análise de confiabilidade dinâmica, sendo a plataforma de desenvolvimento o *Simulink* – ambiente de simulação com diagramas de blocos do *software* Matlab.

A confiabilidade dinâmica está fortemente ligada à metodologia PRA (Avaliação Probabilística de Risco), onde além da falha do sistema técnico, existe a preocupação com as consequências da falha sobre o meio ambiente, população, imagem da empresa, continuidade operacional, entre outros aspectos. Todas essas variáveis fazem com que o número de cenários possíveis atinjam um grande volume de possibilidades, o que torna as formas tradicionais de análise difíceis de serem aplicadas. De acordo com Hu (2005), a quantidade crescente de subsistemas e componentes constituintes, combinada com a complexidade da interação entre *hardware*, *software* e ações humanas, faz com que seja difícil obter os cenários de risco com os métodos tradicionais de PRA, ou seja, deve-se então fazer uso de metodologias que levem em consideração os aspectos dinâmicos do sistemas de forma evidente onde se vê o comportamento dinâmico das variáveis, a mudança de configuração do sistema, entre outras características.

Com a análise de alguns incidentes ocorridos no passado, verifica-se que a modelagem de confiabilidade estática não é suficiente para representar os cenários de falhas e modelar adequadamente os sistemas. Geralmente, os incidentes ocorrem devido a uma combinação de vários eventos. Desta forma, a ordem e o tempo com que ocorrem os eventos, bem como a interação humana são fatores fundamentais na modelagem da propagação das falhas. Com isso, percebe-se a necessidade de analisar as falhas considerando tais fatores para uma melhor representação do cenário de falhas. O uso da análise de confiabilidade dinâmica irá facilitar a proposição de barreiras na busca de impedir que falhas catastróficas ocorram ou propor ações alternativas que atenuem os efeitos das falhas.

Verifica-se que essa forma de análise traz vários benefícios, no entanto, a divulgação da técnica foi limitada pela complexidade dos sistemas envolvidos (como sistemas eletrônicos, mecânicos, *software*, fatores ambientais e humanos) e também pela falta de aplicativos para auxiliar no desenvolvimento da análise. Em face disso, a confiabilidade dinâmica no Brasil ainda é pouco conhecida, inclusive no meio acadêmico. Alguns trabalhos estão relacionados com o arcabouço teórico da confiabilidade dinâmica, todavia não são explicitamente tratados como tal. Neste contexto, encontram-se as pesquisas relacionadas com a análise de confiabilidade humana (HRA) (MENEZES; DROGUETT, 2007; MATURANA, 2011), sistemas tolerante a falhas (MOURA, 2006; DOMÍNGUEZ-GARCÍA et al., 2008) e análise probabilística do risco com atualização dinâmica das probabilidades (RODRIGUEZ, 2012) – o dinamismo está presente nas ações humanas, ou nas configurações do sistema ou nas atualização das informações do modelo.

Internacionalmente, os primeiros trabalhos sobre confiabilidade dinâmica foram publicados na década de 1980 com os trabalhos de Ladde e Siljak (1981) e Tanaka et al. (1989). A partir da década de 1990 houve um salto no número de publicações, destacando-se os trabalhos de: Siu (1994), Xue e Yang (1995), Devooght (1997), Marseguerra et al. (1998), Swaminathan e Smidts (1999c), Labeau et al. (2000), Distefano e Xing (2006), Codetta-Raiteri e Bobbio (2006) e Chiacchio et al. (2012).

Entre as técnicas mais utilizadas para a modelagem das falhas nos sistemas destacam-se a DFTA (Análise por árvore de falhas dinâmica), DETA (Análise por árvore de eventos dinâmica) e DRBD (Diagrama de blocos para confiabilidade dinâmica), que são baseadas nas técnicas tradicionais: FTA (Análise por árvore de falhas), ETA (Análise por árvore de eventos) e RBD (Diagrama de blocos para confiabilidade). A principal diferença entre as técnicas tradicionais e as dinâmicas é a implementação de elementos adicionais que consideram ordem cronológica e o tempo de ocorrência dos eventos. Além dessas técnicas, vale ainda citar a análise de Monte Carlo, Redes de Petri, ESD (Diagrama sequencial de eventos) e *Go-flow*.

Assim, a proposta deste trabalho é apresentar uma metodologia para análise de confiabilidade dinâmica e discutir os conceitos dessa nova abordagem, bem como as técnicas que podem ser utilizadas para a modelagem dos sistemas. Pretende-se com a metodologia proposta contemplar duas características dinâmicas: comportamento dinâmico causado pelas falhas e a atualização do modelo do sistema técnico ao longo do tempo.

1.1 JUSTIFICATIVA

Embora os estudos relacionados com a análise de confiabilidade dinâmica tenham iniciado há mais de 20 anos, o conhecimento sobre o assunto ainda não atingiu maturidade suficiente, ou seja, grande parte de sua utilização está no meio acadêmico e fora deste ambiente ainda é bastante restrita.

No Brasil o conhecimento sobre o assunto é mais restrito, pois até o presente momento foram encontradas poucas publicações que abordam o assunto.

Desta forma, existe a necessidade de obter informações como:

- Quando e como começa a análise?
- Quais as etapas de desenvolvimento?
- Quais as informações que devem ser coletadas para o desenvolvimento da análise?
- Como os resultados são apresentados e utilizados?

Assim, em vista das questões apresentadas acima, a relevância deste trabalho é ter uma metodologia para auxiliar no desenvolvimento sistematizado da análise de confiabilidade dinâmica de sistemas.

Visto que as análises são realizadas para sistemas com potencial catastrófico como usinas nucleares, aeronaves, navios de grande porte, que são sistemas complexos, reforça-se a necessidade de se ter uma metodologia para auxiliar o desenvolvimento da análise. Desta forma, mediante a essa dificuldade, busca-se sistematizar o processo de análise e assim reduzir a chances de cometer erros, já que as análises de confiabilidade são muito dependentes dos especialistas. Além disso, deseja-se disseminar o conhecimento para que outros trabalhos possam dar continuidade a essa nova linha pesquisa.

Particularmente, uma das linhas de pesquisas desenvolvidas no NeDIP (Núcleo de Desenvolvimento Integrado de Produtos) e LASHIP (Laboratório de Sistemas Hidráulicos e Pneumáticos) são voltadas para o desenvolvimento de metodologias de projeto de sistemas. Nos últimos dez anos, nos laboratórios citados têm surgido trabalhos relacionados com confiabilidade e manutenibilidade, como:

- Alves (2001) desenvolveu um sistema especialista para diagnóstico de falhas em um sistema de governo de navio, visando o planejamento da manutenção das embarcações.
- Vinadé (2003) desenvolveu um sistema especialista para sistematizar o projeto para confiabilidade e manutenibilidade aplicado à reguladores de velocidade de usinas hidrelétricas.

- Calil (2009) propôs uma metodologia para gerenciamento de risco com foco na segurança e na continuidade, sendo utilizada várias técnicas de análise de falhas² de forma integrada a fim de capturar melhor os cenários de falhas e assim, propor barreiras e procedimentos mais eficazes.
- Porciúncula (2009) desenvolveu uma metodologia para cálculo da confiabilidade que leva em consideração o regime de trabalho diferenciado dos componentes do sistema, obtendo dessa forma um valor de confiabilidade mais próximo da realidade. O objetivo é, com essa informação, definir uma manutenibilidade diferenciada para cada campo de aplicação do sistema hidráulico. Isso permite programar a produção e também a gestão da manutenção, na fase de projeto, pelo fabricante do sistema hidráulico.
- Sanabria (2012) desenvolveu uma metodologia para análise de confiabilidade em robôs, cujo objetivo é garantir a confiabilidade estabelecida nas fases iniciais de projeto.

Além do mais, nos laboratórios ora mencionados procura-se desenvolver códigos computacionais que permitam aplicar as teorias desenvolvidas. Também observa-se a integração de várias técnicas, explorando-se adequadamente as vantagens de cada uma. No entanto, apesar dos avanços ora mencionados, a análise de confiabilidade tem sido realizada de forma puramente estática.

Para contribuir com a linha de pesquisa em confiabilidade e manutenibilidade, desenvolveu-se a simulação das falhas nos modelos com base no método de Monte Carlo e nos processos semi-Markovianos. O método de Monte Carlo é utilizado em simulações estocásticas e não necessita de uma interface gráfica para o seu desenvolvimento, como DFTA ou DRBD. Já os processos semi-Markovianos serão usados para modelar estados dos componentes – mudanças da condição normal para falha e vice-versa. A implementação numérica será no *software* Matlab, que é ferramenta bastante conhecida no meio acadêmico. Espera-se com o uso destas técnicas e ferramentas divulgar e facilitar o uso da metodologia.

²FMECA, FTA, ETA, ESD e CNEA.

1.2 OBJETIVOS

1.2.1 Objetivo geral

Neste trabalho objetiva-se propor uma metodologia para análise de confiabilidade dinâmica, contemplando o comportamento dinâmico de falhas e atualização do modelo de análise ao longo do tempo.

1.2.2 Objetivos específicos

Para o cumprimento do objetivo geral deste trabalho, têm-se os seguintes objetivos específicos:

- Estruturar uma metodologia que permita o desenvolvimento da análise de confiabilidade dinâmica para identificar: início da análise, etapas de análise, informações requeridas e resultados.
- Sistematizar o uso das técnicas para análise da confiabilidade dinâmica.
- Sistematizar uma ferramenta computacional para auxiliar na implementação do modelo de análise.
- Avaliar a metodologia para um problema clássico de confiabilidade dinâmica e comparar o resultado com as análises de outros pesquisadores.

1.2.3 Resultados esperados

Deseja-se com o uso da metodologia facilitar a análise de confiabilidade dinâmica de sistemas, obter modelos de confiabilidade mais próximos da realidade e atualizados. Além disso, as informações geradas pela análise serão utilizadas para visualizar os cenários de falhas mais críticos, para os quais devem ser propostas ações – de manutenção ou barreiras – para impedir ou mitigar as consequências das falhas.

1.3 DEFINIÇÕES E CONCEITOS PRELIMINARES

Inicialmente apresenta-se alguns conceitos preliminares fundamentais para a compreensão do texto da tese.

1.3.1 Definição de confiabilidade dinâmica

Confiabilidade dinâmica é uma análise de confiabilidade aplicada em sistemas cuja **modelagem comportamental** tem características dinâmicas, onde ocorrem **mudanças ao longo do tempo** na configuração do sistema, nas variáveis de estado do sistema ou em alguma característica³ de seus componentes, que em função das mudanças observadas, **ações são tomadas** ao longo do tempo a fim de impedir a falha do sistema técnico.

Portanto, destaca-se que não basta que o modelo comportamental do sistema técnico tenha características dinâmicas, também é necessário que se tenha tempo para a tomada de ações, que podem ser humanas ou via *hardware/software*. Assim, nos sistemas que possuem um comportamento muito rápido, em que não há tempo hábil para agir, só é possível utilizar a análise de confiabilidade estática.

1.3.2 Os modelos para a análise de confiabilidade estática e dinâmica

Os itens a seguir apresentam as principais diferenças entre os modelos para a análise de confiabilidade estática e dinâmica:

- Quanto ao modelo comportamental

Geralmente, um diagrama de blocos para a análise de confiabilidade estática é suficiente para a análise. Na análise de confiabilidade dinâmica é preciso ter modelos que descrevam o comportamento dinâmico das variáveis de estado do sistema, cujos valores definem o estado do sistema. Assim, muitas vezes, a **variável de estado do sistema** será denominada no texto de **variável de controle**, pois seu valor caracteriza o estado do sistema.

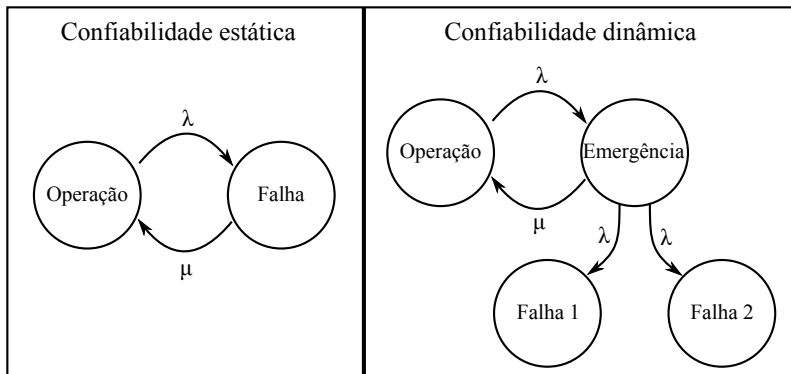
- Quanto aos estados do sistema técnico

O número de estados do sistema técnico para análise de confiabilidade dinâmica é maior do que para análise de confiabilidade estática. A Figura 1.1 apresenta os possíveis estados para uma análise de confiabilidade estática e dinâmica.

Geralmente, para a análise de confiabilidade estática a falha do sistema técnico é caracterizada como o não cumprimento da função. Desta forma, os estados do sistema ficam resumidos em **operação** e **falha**.

³Por exemplo: taxas de falha, taxas de reparo, função densidade de falha.

Figura 1.1 – Estados do sistema técnico



Já na análise de confiabilidade dinâmica, a falha pode ter mais de um estado. Como é feito um acompanhamento das variáveis de estado do sistema, os valores observados podem ultrapassar um limite superior, caracterizando um tipo de falha, ou um limite inferior, segundo tipo de falha do sistema técnico. Na Figura 1.1 estão apresentados apenas **Falha 1** e **Falha 2**. No entanto, poderiam ter outras falhas, quando se utiliza para controle do sistema, um número maior de variáveis de estado.

O estado de **emergência** é uma condição em que o sistema está fora do estado normal de operação, mas também não está em falha. No estado de emergência, o sistema ainda pode voltar para a condição normal, que é uma condição desejada, ou passar para o estado de falha. Estas transições dependem das políticas de manutenção do sistema, dos sistemas de controle de falha, entre outros fatores. O estado de emergência é uma condição do sistema que exige uma ação (humana ou não) para impedir que o sistema alcance o estado de falha.

Os textos apresentados nesta introdução tem por objetivo esclarecer um pouco sobre a análise de confiabilidade dinâmica. No Capítulo 2 a análise de confiabilidade dinâmica é abordada com um maior detalhamento.

1.4 ESTRUTURA DO DOCUMENTO

Este documento está dividido em sete capítulos, conforme apresentados a seguir.

No Capítulo 2 é tratada a análise de confiabilidade dinâmica específica-

mente.

No Capítulo 3 faz-se uma apresentação sucinta das técnicas mais conhecidas para a análise de confiabilidade dinâmica.

O Capítulo 4 traz a metodologia proposta para a análise de confiabilidade dinâmica.

No Capítulo 5 é apresentado um estudo aplicado a um problema clássico proposto especificamente para os estudos em análise de confiabilidade dinâmica, que é um sistema dinâmico para controle de nível de fluido em um reservatório. Os resultados obtidos são comparados com a metodologia com redes de petri estocásticas generalizadas e fluidas, GSPN e FSPN respectivamente.

No Capítulo 6 é apresentado um estudo aplicado em um sistema hidráulico de governo do leme em um navio petroleiro.

No Capítulo 7 são apresentadas as conclusões e propostas para trabalhos futuros.

No Apêndice A são apresentadas as definições básicas relacionadas com a teoria de confiabilidade em sistemas e análise de risco.

O Apêndice B apresenta os valores utilizados para gerar os gráficos das funções distribuição de probabilidade de falhas para o problema do Capítulo 5. Nesta análise foi considerado que os componentes não são reparáveis, ou seja, enquanto o sistema está em operação, não são realizadas manutenções.

Diante disso, houve a curiosidade de se analisar o problema do reservatório, Capítulo 5, considerando a existência de manutenção dos componentes durante a operação. Esta análise foi realizada no Apêndice C, em que verificou-se a influência da sequência de manutenção dos componentes sobre a probabilidade de falha do sistema. Posteriormente, foi realizado no Apêndice D uma análise de confiabilidade estática para o mesmo problema.

No Apêndice E são apresentadas, de maneira sucinta, algumas técnicas utilizadas atualmente para análise de confiabilidade dinâmica. Desta forma, para a obtenção de maiores detalhes deve-se consultar as bibliografias específicas referenciadas no texto.

2 CONFIABILIDADE DINÂMICA

A presente seção apresenta as diferentes abordagens para análise de confiabilidade dinâmica, área de aplicação, limitações e estrutura de análise.

2.1 DIFERENTES ABORDAGENS PARA ANÁLISE DE CONFIABILIDADE DINÂMICA

Um dos primeiros trabalhos em que se encontrou o termo confiabilidade dinâmica foi no livro escrito por Siljak (1978), e o autor refere-se ao termo “confiabilidade dinâmica” como sendo a confiabilidade aplicada a sistemas dinâmicos.

A definição apresentada por Devooght (1997) é bem próxima de Siljak (1978): “confiabilidade dinâmica é o termo utilizado para a teoria de confiabilidade relacionada com sistemas dinâmicos”.

As definições de Siljak (1978) e Devooght (1997) associam a análise de confiabilidade à aplicação, que é em sistemas dinâmicos. No entanto, uma análise em um sistema dinâmico ainda pode ser uma análise de confiabilidade estática e não dinâmica.

A visão de sistema dinâmico na qual os autores se referem é que, nas análises, são levadas em consideração alguns dos itens a seguir:

- variação do comportamento dinâmico das variáveis de saída, ou
- mudanças no arranjo dos seus componentes (configuração do sistema), alterando o estado dos componentes, ou
- variação de alguma característica como, por exemplo, a taxa de falhas ou de reparo dos componentes ao longo do tempo.

Desta forma, não basta somente que o sistema seja dinâmico, faz-se necessário **acompanhar alguma mudança** no sistema ao longo do tempo. Caso não sejam levadas em consideração tais mudanças, ou não seja possível **tomar ações diante das mudanças**, a análise de confiabilidade do sistema dinâmico será estática.

No Apêndice A é apresentado a definição de sistema, sendo discutido as diferenças entre um sistema estático e dinâmico. O que se deseja destacar é que mesmo que o sistema seja dinâmico, a análise de confiabilidade ainda pode ser estática ou dinâmica. Para executar uma análise de confiabilidade dinâmica, proposta nesta tese, deve-se acompanhar as mudanças que ocorrem

no sistema e tomar ações com o objetivo de controlar a progressão da falha e restaurar o sistema para a condição de operação normal.

Por meio da revisão bibliográfica, foi possível constatar que existem outras abordagens para a análise de confiabilidade dinâmica:

- **Avaliação ao longo do tempo:** São feitas avaliações ao longo do tempo, com isso, atualiza-se o modelo confiabilístico com informações de campo ou experimentos, permitindo identificar mudanças nos valores das taxas de falha dos produtos.

As melhorias nos processos de produção, qualidade dos materiais, mão de obra, tecnologia, entre outros fatores, reduzem os valores das taxas de falha, que podem ser percebidas durante as reavaliações da confiabilidade (COLLAS, 1991).

Basicamente, nessa abordagem a avaliação da confiabilidade é dinâmica, visto que ao longo do ciclo de vida do produto, são feitas várias análises dos parâmetros. Neste grupo encontram-se trabalhos com o tema “confiabilidade crescente” (*growing reliability*).

Todavia poderia ser incluído aqui, não somente as análises que identificam a “confiabilidade crescente” dos produtos, mas também aquelas que levam em consideração o aumento da taxa de falhas com o tempo, o que resultaria em uma “confiabilidade decrescente”. Assim, neste caso, estaria associado um processo de degradação do produto, causando um aumento em sua taxa de falhas.

Portanto, tornando essa abordagem mais ampla, pode-se considerar como uma avaliação ao longo do tempo. Consequentemente, são identificadas mudanças na taxa de falha, aumento ou redução, e em função de tais mudanças são realizadas ações como: alterações de projeto, dos processos de fabricação, operação ou manutenção.

- **Avaliação que leva em consideração fatores humanos e ambientais:** A análise de confiabilidade estática tem o foco sobre o equipamento. Por outro lado, na análise de confiabilidade dinâmica os fatores externos são levados em consideração, onde após a falha do equipamento é feita uma análise das consequências. Nesse contexto estão os estudos relacionados com avaliação de risco, que é uma das linhas de pesquisa de Swaminathan e Smidts (1999c), onde os autores definem confiabilidade dinâmica como sendo “o estudo probabilístico dos sistemas homem-máquina-*software* afetados por um processo físico subjacente”.

Segundo Marseguerra et al. (1998) e Devooght e Smidts (1996) a confiabilidade dinâmica visa complementar as metodologias clássicas da avaliação probabilística do risco (*Probabilistic Risk Assessment – PRA*)

quando o comportamento dinâmico do sistema precisa ser levado em consideração.

A abordagem que será adotada neste trabalho segue próxima das duas abordagens apresentadas.

2.2 COMPORTAMENTO DINÂMICO DOS SISTEMAS

Segundo Devooght e Smidts (1996), o comportamento dinâmico de um sistema pode ser descrito por um conjunto de equações de primeira ordem como:

$$\frac{dy}{dt} = f_i(y, t) \quad (2.1)$$

A variável y representa as variáveis de estado que descrevem o comportamento do sistema, o índice i de $f_i(y, t)$ varia de $i = 1$ até $i = M^N$, sendo M o número de estados dos N componentes do sistema¹.

No Apêndice A, Figura A.10, é ilustrado os possíveis estados de um componente e as transições que ocorrem de um estado para outro. Cada círculo representa um estado e cada seta uma transição. Assim, para aquele componente da Figura A.10 estão apresentados seis estados e quatorze transições. Dependendo do problema que está sendo analisado e do componente, o número de estados e transições podem ser diferentes.

Desta forma, supondo que um sistema possua apenas 4 componentes, cada um podendo estar em 6 estados, resulta que o sistema pode ter uma combinação 1296 de estados de componentes. O comportamento dinâmico do sistema, descrito pela Equação 2.1, é influenciado pelos estados dos componentes do sistema. Isso não significa que a falha de um componente necessariamente irá afetar diretamente a dinâmica do sistema. Uma falha oculta em um componente, por exemplo, só irá prejudicar o sistema quando o sistema demandar uma mudança de estado. Por exemplo, se o componente estiver ligado e o mesmo travar na posição ligado, não terá problema enquanto não surgir um comando para desligar.

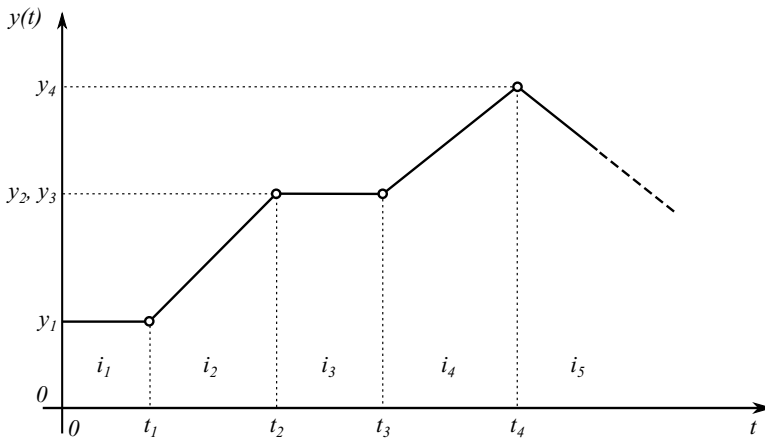
O comportamento dinâmico da variável y é monitorado nos estudos de PSA, onde é investigado em que condições a variável ultrapassa determinados limites de segurança, e quando possível, quantificar a probabilidade dessa transição ocorrer.

¹O número de configurações do sistema, is , calculado em função de M e N , tem como hipótese que todos os componentes possuem os mesmos estados.

Segundo Devooght e Smidts (1996), o histórico de transientes do sistema é uma sucessão de estados (y_1, i_1, t_1) , (y_2, i_2, t_2) ... (y_k, i_k, t_k) ... onde a transição no tempo t_k o sistema está no estado (y_k, i_k) . A transição $i_k \rightarrow i_{k+1}$, que representa a mudança de estados de um componente, ocorre de forma instantânea. Essa consideração geralmente é adequada, no entanto, se for necessário considerar por exemplo um processo de degradação progressivo, pode-se adicionar estados intermediários.

Graficamente, pode-se representar o comportamento dinâmico de um sistema conforme a Figura 2.1. O estado i_1 corresponde ao intervalo $0 \leq t < t_1$, o estado i_2 ao intervalo $t_1 \leq t < t_2$ e assim por diante. Ou seja, a mudança entre os estados, i_s , é instantânea, mas o comportamento da variável y pode ser gradual, dependendo do sistema – neste exemplo, o comportamento da variável y muda linearmente ao longo do tempo.

Figura 2.1 – Representação do comportamento dinâmico em função dos estados dos componentes (i_1, i_2, \dots) e do tempo t



A maneira como Devooght e Smidts (1996) representa os estados do sistema, em função de (y, i, t) , pode gerar uma quantidade muito grande de estados, dificultando a análise. Nesta tese, os estados do sistema serão tratados sob uma visão mais externa, consequentemente, o número de estados do sistema será menor, facilitando a análise do problema. Basicamente, nesta tese o estado do sistema fica definido em função da variável de estado y e do tempo t , reduzindo os estados do sistema em “condição normal” de operação, “condição de emergência” e “condição de falha” do sistema.

As mudanças dos estados dos componentes (i_1, i_2, \dots) podem ser causadas por (DEVOOGHT; SMIDTS, 1996):

- falha ou mal funcionamento de componentes
- dispositivos de controle que agem sob influência de y
- intervenção humana

De acordo com Devooght e Smidts (1996) alguns processos na análise dinâmica podem ser tratados pela modelagem Markoviana. Os autores citam como exemplo os processos de envelhecimento, mas salientam que nem todos os processos podem ser tratados dessa forma. Assim, muitas vezes é utilizada a modelagem semi-Markoviana, que é mais genérica e portanto mais flexível.

No Apêndice A é apresentada a Equação A.16, que representa o conceito de um processo Markoviano. De acordo com a equação, a probabilidade condicional do sistema no tempo t_n , depende apenas do valor x no tempo t_{n-1} . Os valores de x para os tempos anteriores, t_{n-2} em diante, não importam porque não tem influência para o tempo t_n . Assim, a futura evolução do sistema depende apenas do valor atual de (y, i, t) , sem considerar os valores do passado. A Equação A.16 vale tanto para os processos Markovianos, como semi-Markovianos.

Ouhbi e Limnios (2003) e Devooght e Smidts (1996) destacam que pelo fato dos modelos Markovianos exigirem que a transição entre os estados seja distribuída exponencialmente, torna-se uma limitação para muitos casos reais, sendo recomendado desta forma, a modelagem com modelos semi Markovianos.

As probabilidades de transição $P(j \rightarrow i|y)$ são condicionalmente dependentes, em geral, a alguns valores da variável de estado y . Assim, dependendo do valor de y o sistema pode mudar de estado, ligando/desligando componentes para trazer o sistema para uma condição mais segura.

2.3 COMPORTAMENTO DETERMINÍSTICO E ESTOCÁSTICO

Marseguerra et al. (1998) apresenta uma breve descrição de como abordar o comportamento determinístico e o estocástico em conjunto. Segundo os autores, para prever os estados futuros, a análise deve iniciar com a evolução determinística da configuração inicial do sistema. Posteriormente, considera-se a ocorrência de um evento estocástico (evento inicial) e verifica-se o comportamento determinístico com essa nova configuração de cenário. Em um sistema dinâmico, esse comportamento pode ocorrer repetidamente ao longo da duração do incidente.

Formalmente, o problema pode ser estruturado em termos da dinâmica probabilística (MARSEGUERRA et al., 1998 apud DEVOOGHT; SMIDTS, 1992) que

dá subsídios para o relacionamento entre a evolução dinâmica de um sistema e a transição entre seus estados. As características dinâmicas da evolução da planta podem ser levadas em consideração por meio da introdução de modelos físicos adequados, em geral, cada um correspondendo a uma configuração particular do sistema.

O comportamento estocástico está associado aos acontecimentos como: tempo que ocorrerá a falha, tipo de falha (aberta ou fechada) e – se for considerada ações de manutenção no modelo – o tempo de reparo de componentes em falha. Já o comportamento determinístico está associado à evolução, ou variação, da variável de controle do sistema ao longo do tempo que é dirigida por uma equação que relaciona a contribuição de cada componente no comportamento desta variável.

2.4 ÁREA DE APLICAÇÃO

A confiabilidade dinâmica tem sido utilizada principalmente na PRA² e PSA³ para analisar os riscos e a segurança em áreas como: usinas nucleares, indústrias químicas, indústria aeroespacial, entre outras. Foi observado que somente com uso das técnicas tradicionais de árvore de eventos/falhas estáticas não era possível modelar o comportamento dinâmico dos processos e a interação humana.

O contexto industrial e científico sob os quais tais estudos aparecem está claramente o campo do PRA e PSA, usados por exemplo nos estudos de segurança do reator nuclear, cuja espinha dorsal é a metodologia árvore de eventos/falhas (DEVOOGHT, 1997, p.215).

Alguns acidentes no passado reforçam a necessidade de utilização da abordagem dinâmica. Marseguerra et al. (1998) relata que muitos acidentes ocorreram porque não se previu a forte interação entre a evolução das variáveis do processo, a ação de intervenção dos sistemas de proteção (ou controle) e as ações dos operadores para recuperação do sistema.

Por exemplo, o acidente nuclear de *Three Mile Island* em 1979. Após a falha de uma bomba do circuito de resfriamento, houve aumento da temperatura e da pressão dentro do reator. Ao atingir o limite de pressão, ocorreu a abertura da válvula de alívio, no entanto, esta continuou aberta mesmo depois da pressão ter voltado ao normal, pois ficou emperrada. Os operadores não sabiam que a válvula permanecia aberta, visto que o sistema havia mandado sinal para fechá-la, mas não informava o seu estado real. Essa falha e mais

²Probabilistic risk analysis.

³Probabilistic safety analysis.

alguns erros humanos na operação, fizeram com que o acidente se desenvolvesse de uma forma totalmente inesperada. Durante um acidente, um papel importante é representado pelos operadores humanos que são chamados para intervir e recuperar os sistemas. O sucesso ou falha das ações dos operadores são fortemente dependentes dos valores que as variáveis do processo assumem, pois eles são influenciados pelo nível de tensão que estão trabalhando (MARSEGUERRA et al., 1998).

Na análise feita, eram conhecidas as taxas de falha de cada um dos componentes, possivelmente sendo também consideradas as condições de falhas abertas e fechadas. Contudo, não se tinha por certo todos os cenários para as distintas condições. Além do mais, todo nível de taxa de falha foi contextualizado dentro de um nível de confiança. Ou seja, aquele cenário levantado pode não se efetivar. Então para se construir mais cenários, é preciso dispor de instrumentos eficientes para simulação das condições operacionais ao longo do ciclo de vida.

De acordo com Marseguerra et al. (1998), a análise da situação apresentada no exemplo deve ser executada por meio de modelos preditivos que levem em consideração a ocorrência de eventos de transição de vários tipos no equipamento. A predição de estados futuros do sistema exige que se inicie a análise seguindo a evolução determinística da configuração inicial do sistema. Depois disso, considera-se a ocorrência de um evento inicializador no equipamento – estocástico e repentino – e após essa entrada, prossegue-se com a análise dando continuidade a evolução determinística do sistema para a nova configuração do cenário. Em um sistema dinâmico, tal esquema pode ocorrer repetidamente ao longo da duração do acidente.

A geração de cenários de forma manual para um sistema dinâmico pode se tornar muito trabalhosa, tendo em vista a quantidade de combinações de eventos que podem ocorrer. Os cenários dos eventos dependem da ordem cronológica com que ocorrem as falhas, comportamento dinâmico da variável de controle (que muda em função das falhas), tempo e política de manutenção (se for considerada manutenção no modelo), tempo entre as falhas, entre outros fatores.

Desta forma, faz-se necessário que se tenha uma ferramenta computacional para gerar cenários automaticamente, para que um analista possa visualizar e identificar possíveis falhas nos sistemas de proteção. Como exemplo pode-se citar o trabalho de Nejad-Hosseinian (2007) que apresenta uma metodologia para gerar cenários automaticamente com base nos diagramas sequenciais de eventos (ESD).

O artigo de Swaminathan e Smidts (1999a) segue a mesma linha de trabalho de Nejad-Hosseinian (2007), mostrando que algumas vezes alguns cenários importantes podem passar despercebidos. Desta forma os autores

apresentam uma metodologia para identificar cenários que faltaram no modelo, mas que deveriam ser considerados.

Com relação ao gerenciamento de riscos e segurança em sistemas, Guimarães (2003) apresenta um procedimento de análise de segurança, que utiliza como informações preliminares:

- (a) conjunto de cenários de incidentes identificados pela Análise Preliminar de Risco; e
- (b) probabilidade de ocorrência de eventos inicializadores destes cenários.

Desta forma, pode-se – como a Análise Preliminar de Risco – utilizar a análise de confiabilidade dinâmica como etapa preliminar para fornecer, por meio das simulações comportamentais dos sistemas técnicos, os cenários de incidentes para a análise de segurança. Além disso, a análise de confiabilidade dinâmica permite avaliar as “barreiras de segurança” da etapa 2 (Segurança implantada) e as “ações de contenção” do evento indesejado na etapa 3 (Salvaguarda), contidas nos Procedimentos de Análise de Segurança. No Capítulo 4 a relação entre o procedimento de análise de segurança e confiabilidade dinâmica serão tratados com maiores detalhes.

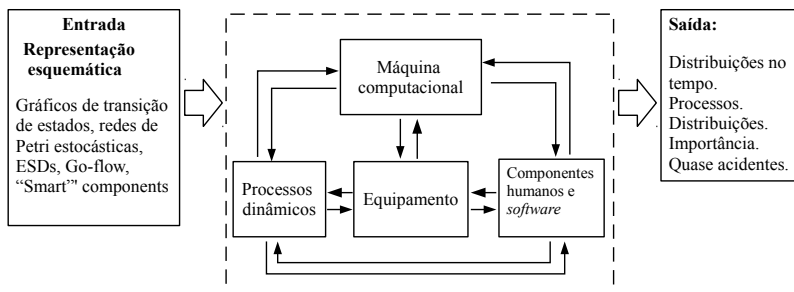
A análise de confiabilidade humana (ACH) também é uma área relacionada com a confiabilidade dinâmica, visto que as reações humanas são dinâmicas e interferem na performance do sistema. Neste contexto, destacam-se trabalhos como:

- Pallerosi et al. (2011) apresenta os conceitos básicos, metodologias qualitativas e quantitativas, aborda aspectos relacionados com a psicologia, administração e engenharia;
- Souza et al. (2010) realiza uma profunda revisão bibliográfica onde é apresentada a evolução das metodologias neste tipo de análise, quantidade de publicações ao longo dos anos e sua importância;
- A análise de confiabilidade humana é realizada com o uso de redes bayesianas (MATURANA, 2011; MENEZES; DROGUETT, 2007; DROGUETT; MOSLEH, 2006);
- Moré (2004) realiza análise de confiabilidade humana com uso de lógica fuzzy; e
- Begosso (2005) propõe um simulador do comportamento humano, com o objetivo de produzir de forma aleatória estados de erro humano.

2.5 ESTRUTURA GERAL DE UMA ANÁLISE DE CONFIABILIDADE DINÂMICA

Labeau et al. (2000) propõe uma estrutura, Figura 2.2, para a análise de confiabilidade dinâmica formada por três módulos: Entrada (Representação esquemática), máquina computacional e saída.

Figura 2.2 – Estrutura geral de uma plataforma para confiabilidade dinâmica



Fonte: Labeau et al. (2000, p.221, tradução nossa)

Na entrada estão as representações esquemáticas, técnicas que relacionam os estados dos componentes dos sistemas em forma de diagramas. Elas permitem visualizar e estruturar o problema a ser resolvido. São exemplos dessas técnicas: diagramas de estados, redes de Petri, *Go-flow*, diagramas de eventos, etc.

Na máquina computacional estão os métodos utilizados para a solução do problema e nela são realizadas as simulações do sistema, agindo como um condutor para os modelos físicos, humano e *software*. A máquina computacional pode ser desde um elaborado método de integração para função densidade de probabilidade, para uma dada distribuição de probabilidade do sistema, até algoritmos de simulação (LABEAU et al., 2000).

A saída são os resultados utilizados pelo analista. De acordo com Labeau et al. (2000) podem ser:

- Frequência total de acidentes em função do tempo.
- Frequência do estado final⁴ em função do tempo.
- Frequência média dos grupos de corte (*Cut set*) para um dado intervalo de tempo.

⁴Estado final são modos de falha particulares do sistema.

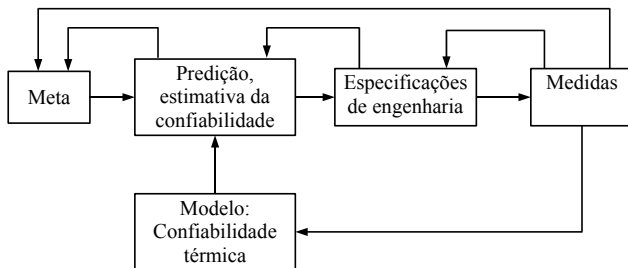
- Frequência de cenários de acidentes discretizados em função do tempo.

Collas (1991) apresentou uma análise de confiabilidade para componentes eletrônicos realizada na Bull S.A.⁵, na qual identificou um comportamento crescente da confiabilidade ao longo do ciclo de vida do produto. Esse processo foi visto como um tipo de confiabilidade dinâmica e foi atribuída à evolução da organização, dos processos de produção, da assistência técnica entre outros fatores. Vale salientar aqui que esta abordagem não será adotada neste trabalho, mas está apresentada aqui para esclarecer ao leitor que existe este outro ponto de vista, que considera análises do produto ao longo do tempo, realimentando o modelo para aproximá-lo do produto real.

Segundo Collas (1991), as abordagens tradicionais para predição da confiabilidade do produto são baseadas nos modelos de taxa de falha dos componentes, definidas apenas em termos dos parâmetros tecnológicos intrínsecos do produto, desconsiderando assim a evolução desses parâmetros durante o seu ciclo de vida – o que faz com que, com o passar dos anos, o modelo fique obsoleto.

O modelo utilizado por Collas (1991) é apresentado na Figura 2.3. O grupo de *marketing* define a “meta” de confiabilidade para o produto. Uma vez definido esse valor, os modelos térmicos e funcionais de confiabilidade são usados para calcular: as estimativas de taxas de falha, especificações de engenharia e medidas derivadas como disponibilidade, demanda de manutenção e requerimentos de peças sobressalentes. Todos esses cálculos são realizados iterativamente com realimentação de uma análise complementar até um balanço satisfatório nas características do componente e sistemas ser alcançado.

Figura 2.3 – Modelo para predição da confiabilidade



Fonte: Collas (1991, p.302, tradução nossa)

⁵<http://www.bull.com/>

A taxa de falha intrínseca do componente foi determinada utilizando um padrão interno da Bull, que leva em consideração: tecnologia, complexidade do circuito integrado, temperatura da junção, ambiente e nível de qualidade. O modelo adotado era mais simples do que outros padrões, exceto pela inclusão de um novo parâmetro que representa a maturidade da tecnologia.

As comparações das taxas de falha estimadas com as observadas foram realizadas para cada tipo de componente, de família e de tecnologia. Com base nessas comparações, foram construídas curvas de ajuste para modificar os parâmetros dos modelos de taxa de falha. Os fatores de ajuste, utilizados para revisar as taxas de falha e a confiabilidade, foram baseados em observações de amostras de clientes ao longo de intervalos de tempos variados, como sucessivos meses ou semestres (COLLAS, 1991).

A partir do trabalho publicado por Collas (1991) percebe-se a necessidade de ajustar os modelos para cada aplicação e para isso é muito importante a disponibilidade de dados colhidos de campo para realimentar o modelo, e assim, fazer os ajustes para uma condição mais próxima da realidade.

2.6 CONSIDERAÇÕES DO CAPÍTULO

O presente capítulo apresentou os aspectos encontrados na análise de confiabilidade ser dinâmica e as diferentes abordagens que podem ser feitas.

A presente seção apresentou diferentes abordagens de análise de confiabilidade dinâmica, que podem estar relacionadas com o comportamento das variáveis de saída do sistema, mudanças na configuração do sistema, mudanças dos parâmetros dos componentes, análise dinâmica – avaliações e reavaliações ao longo do tempo – e atuação humana. O presente trabalho contempla as mudanças na configuração do sistema e o comportamento das variáveis de estado do sistema. As atuações humanas estarão representadas pelas taxas de reparo do componentes, que estão associados com o tempo de manutenção dos componentes.

O comportamento dinâmico está associado com o comportamento determinístico e estocástico do sistema, que são ditados pelos estados dos componentes do sistema. O comportamento estocástico estão relacionados com as falhas e reparos dos componentes.

Neste trabalho, a função densidade de falha do sistema $\pi(y, i, t)$ será obtida por meio de simulação numérica, utilizando o método de Monte Carlo.

As aplicações da análise de confiabilidade dinâmica são muito utilizadas nos estudos de PSA e PRA. Embora não tenha sido relatada na seção, há um grande potencial para aplicação na manutenção de sistemas onde, com as informações geradas, auxiliam o mantenedor na tomada de decisões como

priorizar a manutenção de componentes, elaboração de procedimentos para identificar as falhas ocultas dos componentes e estabelecimento de barreiras para impedir a propagação de falhas.

O modelo apresentado por Collas (1991) é bem diferente do modelo de Labeau et al. (2000). Embora ambos sejam consideradas análises de confiabilidade dinâmica, os objetivos propostos são diferentes. O primeiro busca obter atualizações constantes do modelo, a fim de obter valores dos parâmetros mais adequados, que caracterizem com boa representação o sistema real, ou seja, a avaliação é dinâmica, realizada de tempos em tempos. O modelo de Labeau et al. (2000) é mais alinhado às propostas desta tese e consideram os aspectos dinâmicos relacionados com a configuração do sistema, com os fatores humanos e *software*.

3 PRINCIPAIS TÉCNICAS PARA DAR SUPORTE À METODOLOGIA

A metodologia apresentada neste trabalho passa por diversas etapas nas quais são identificados o comportamento do sistema (dinâmico ou estático), modos de falha, efeitos, criticidade quanto às falhas, disponibilidade e limites de operação do sistema, procedimentos de operação e manutenção, entre outras informações. Para isso, são utilizadas algumas técnicas de suporte que irão auxiliar na coleta de informações, na organização do conhecimento e na modelagem do sistema.

Para a metodologia, sugere-se o uso das seguintes técnicas: FMECA, CNEA, IDEF0, diagramas de bloco para confiabilidade, método de Monte Carlo e MCC. A sugestão se deve às potencialidades oferecidas pelas técnicas, facilidade de uso e também por fazerem parte do arcabouço teórico usado pelos pesquisadores do NeDIP.

Nesta seção é apresentada uma descrição sucinta de cada uma das técnicas. Para uma leitura mais aprofundada sugere-se as bibliografias referenciadas no Quadro 3.1

Quadro 3.1 – Referências bibliográficas recomendadas para técnicas de suporte

Técnica de suporte	Referências
FMECA	Dias et al. (2011), Bertsche (2008), Sakurada (2001), Stamatis (1995), USA/DOD (1980), SAE (2000)
CNEA	Dias et al. (2011), Calil (2009), Kagueiama (2012)
IDEF0	NIST (1993), Dias et al. (2011), Calil (2009), Kagueiama (2012), Belan (2007), Presley (1997)
Diagramas de bloco para confiabilidade	Sanabria (2012), Vinadé (2003), Dias (1996), Billinton e Allan (1992)
Método de Monte Carlo	Billinton e Allan (1992), Sobol (1983), Lobo (2000)
MCC	Dias et al. (2011), Moubray (1997), Smith (2001), Rigoni (2009), SAE (1999), NASA (2008), Siddiqui A. W.; Ben-Daya (2009)

3.1 ANÁLISE DO MODO DE FALHA, EFEITOS E CRITICIDADE (FMECA)

A FMECA é uma técnica indutiva de análise de falhas em sistemas, amplamente utilizada nas áreas de confiabilidade, manutenção, análise de risco e qualidade. A sigla vem do termo em inglês “*Failure modes, effects and criticality analysis*” e foi desenvolvida pelo departamento de defesa dos Estados Unidos (DoD – *Department of Defense*) para avaliação das operações militares.

A partir dos anos de 1970 a técnica foi aplicada no contexto das indústrias automobilísticas e, atualmente, é utilizada em diversos setores com o objetivo de identificar, analisar e avaliar as falhas de produtos e serviços.

A técnica FMECA comumente é também denominada de FMEA. No entanto, esta última tem uma abordagem qualitativa e a outra permite, por meio do índice *NPR* (número de prioridade de risco), quantificar a criticidade da falha. O índice é calculado por meio da Equação 3.1.

$$NPR = S \cdot O \cdot D \quad (3.1)$$

sendo,

S: índice de severidade (1–10)

O: índice de ocorrência (1–10)

D: índice de detecção (1–10)

O índice de severidade está relacionado com os impactos que a falha pode gerar no sistema técnico, ao homem ou ao meio ambiente. As falhas que ameaçam a segurança ou podem gerar grandes prejuízos, recebem valores maiores.

O índice de ocorrência está relacionado com a frequência de ocorrência da falha. Desta forma, as falhas que raramente ocorrem recebem valores baixos e as que ocorrem com muita frequência recebem valores altos.

O índice de detecção está relacionado com os meios de descobrir ou perceber a falha, então representa a dificuldade de se detectar a falha. Se uma falha é facilmente detectável recebe valor baixo, e no caso oposto, quando é difícil de detectar recebe valor elevado.

Portanto, o número de prioridade de risco, *NPR*, é um valor que varia de um até mil e representa a criticidade da falha. Vale destacar que o valor obtido com o *NPR* serve para orientar a equipe quanto à priorização das falhas. Assim, depois de ter as falhas classificadas pelo índice, ainda é necessário que sejam analisadas cuidadosamente, principalmente, para os casos em que o índice de severidade (*S*) é elevado – mesmo que tenham o *NPR* baixo.

A Figura 3.1 apresenta um exemplo de uma tabela FMECA, que é divi-

dida em duas partes. A primeira é o cabeçalho onde são incluídas informações gerais que identificam o sistema, a equipe e o documento – representados pelos números (1), (2) e (3). A segunda parte da tabela FMECA corresponde aos campos utilizados para a análise de falhas dos componentes do sistema, identificados pelos números (4) até (17).

Figura 3.1 – Exemplo de tabela para FMECA

Sistema: _____ (1)			Participantes: _____ (2)				Página: _____ de _____ Data de início: _____ Data de revisão: _____ (3)										
Componente	Função	Modo de falha	Efeitos	S	Causas	O	Controles atuais	D	N P R	Ações recomendadas	Responsável / data limite	Resultados das ações					
												Ações tomadas	S	O	D	N P R	
(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	(15)	(16)	(17)				

Fonte: Adaptado de SAE (2000)

A seguir, uma breve descrição dos campos numerados na Figura 3.1 é apresentada:

- (1) Identificação do sistema.
- (2) Nome dos participantes da reunião.
- (3) Registro da página do formulário, data de início do projeto FMECA e data da reunião atual.
- (4) Identificação do componente.
- (5) Função que o componente deve desempenhar.
- (6) Possíveis modos de falha.
- (7) Possíveis efeitos que podem ser causados no sistema.
- (8) Valor de 1 a 10 do índice de severidade. Este valor é determinado em função dos possíveis efeitos gerados no sistema.
- (9) As causas que podem ter gerado o modo de falha.

- (10) Valor de 1 a 10 do índice de ocorrência.
- (11) Métodos para identificar e controlar as falhas.
- (12) Valor de 1 a 10 do índice de detecção da falha. Este valor é determinado em função dos métodos existentes listados no campo (11).
- (13) Número de prioridade de risco, NPR.
- (14) Ações recomendadas pelo grupo para a eliminação da falha.
- (15) Nome da pessoa responsável em implementar a ação e data limite para conclusão das ações.
- (16) Ação que foi utilizada para a eliminação da falha.
- (17) Reavaliação dos índices e cálculo do novo NPR.

A análise de falhas por meio da FMECA é um procedimento contínuo, aplicado no sistema técnico ao longo do seu ciclo de vida. O documento deve estar sempre atualizado, refletindo cada alteração relacionado ao produto, seja no projeto, processo de fabricação, operação ou manutenção.

Os resultados e os benefícios de sua aplicação são documentos que apresentam as características críticas dos sistema, recomendações para melhoria do projeto/operação/manutenção, orientação para testes e ensaios para análise de falhas, entre outras informações.

Além dos documentos gerados na análise, o maior benefício da técnica é a uniformização do conhecimento gerado durante as reuniões, uma vez que conta com a participação de especialistas (confiabilidade, projeto, operação, manutenção) e usuários do sistema técnico.

3.2 ANÁLISE DE EVENTOS POR REDE CAUSAL (CNEA)

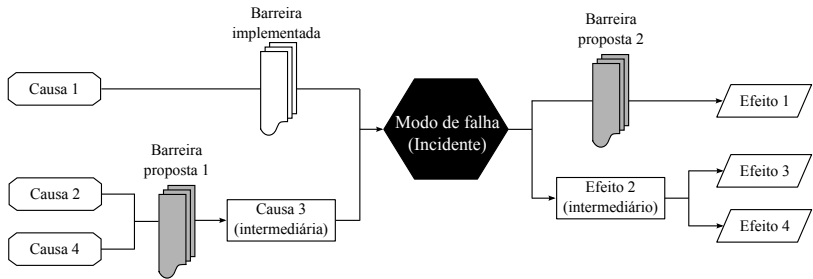
Na seção anterior foi apresentada a técnica FMECA que, basicamente, faz uso de uma tabela para o gerenciamento das informações sobre as falhas de um determinado componente ou sistema. Tal representação apresenta alguns inconvenientes quanto a representação do conhecimento. Para contornar esse problema, buscou-se uma maneira que pudesse representar as relações entre modos de falha, causas e efeitos.

A técnica CNEA (*Causal Network Event Analysis*) foi desenvolvida no Núcleo de Desenvolvimento Integrado de Produtos (NeDIP) – da Universidade Federal de Santa Catarina (UFSC) – durante o projeto MitiSF₆ e as atividades de pesquisa de Calil (2009). O principal objetivo da técnica é representar o

encadeamento entre as falhas, bem como as barreiras, em forma de diagrama – tendo em vista as limitações no uso das tabelas FMECA.

A Figura 3.2 é um exemplo de diagrama. Na parte central localiza-se o modo de falha ou incidente que se deseja analisar. As causas do modo de falha estão dispostos à esquerda do evento central e os efeitos ou consequências à direita. Assim, o ponto forte da técnica é a representação gráfica de todos os eventos relacionados com o evento central, inclusive as causas intermediárias, efeitos intermediários e as barreiras para a contingência dos eventos de falha.

Figura 3.2 – Diagrama de uma análise de eventos por rede causal (CNEA)



Fonte: Kagueiama (2012)



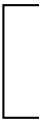
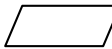
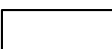
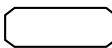


O uso da técnica permite uma melhor compreensão das relações entre eventos de uma rede causal (modos de falha, causas, efeitos, barreiras). Consequentemente, facilita o desenvolvimento das análises de falha, a comunicação entre os especialistas e o preenchimento das tabelas FMECA.

A técnica CNEA foi utilizada para a análise de risco nos trabalhos desenvolvidos no NeDIP (DIAS et al., 2011; CALIL, 2009). A semelhança dos diagramas gerados com a CNEA com a Figura A.8, que representa o modelo de desencadeamento de um incidente, permitiu uma forte interação com a análise de risco, facilitando a representação de cenários críticos de falha e a proposição de barreiras para bloquear ou mitigar efeitos das falhas.

No trabalho desenvolvido por Kagueiama (2012) é apresentado uma sistematização de técnicas de análise de falhas e projeto para confiabilidade: FMECA, CNEA, IDEFO, redes bayesianas e FTA. No estudo foi evidenciado as características de cada uma das técnicas e como podem ser integradas em uma análise de falhas e confiabilidade. A técnica CNEA mostrou-se bastante flexível apresentando boa integração, não somente com a FMECA, mas também com FTA e redes bayesianas.

A Figura 3.3 apresenta uma breve descrição dos elementos utilizados nos diagramas.

Figura 3.3 – Taxonomia da CNEA

FIGURA	DESCRIÇÃO	FIGURA	DESCRIÇÃO
	Evento a se analisar: Um incidente ou modo de falha.	 ou 	Barreira preventiva já implementada que objetiva evitar a ocorrência do evento central ou mitigar seus efeitos.
	Efeito potencial que o evento central pode gerar.		
	Causa ou efeito intermediário		
	Causa raiz para a ocorrência do evento central.	 ou 	Barreira preventiva proposta que deverá ser implementada.

Fonte: Dias et al. (2011)

3.3 *Integration definition for function modeling* (IDEF0)

A técnica IDEF0 é utilizada para representar a estrutura funcional de um sistema e faz parte de uma família de técnicas de modelagem denominadas por IDEF (*integrated definition for function modeling*), que são baseadas em uma linguagem gráfica denominada SADT (*structured analysis and design technique*) (PRESLEY, 1997).

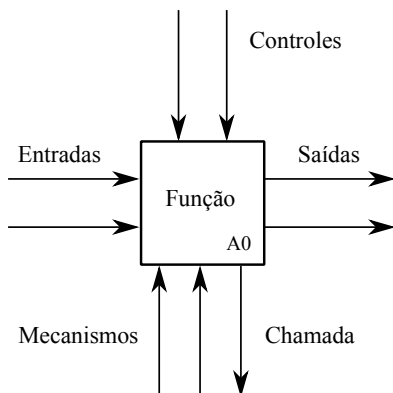
A técnica, durante a análise de sistemas, auxilia na identificação das funções e dos recursos necessários para executá-las, bem como facilita na verificação dos pontos corretos e incorretos do sistema (NIST, 1993; CALIL, 2009).

Os principais componentes utilizados no IDEF0 são as caixas e setas, que podem ser vistos na Figura 3.4.

As caixas representam as funções e as setas são dados ou objetos relacionados às funções a serem executadas. As principais setas são as de entrada, controle, mecanismo e saída. As setas de entrada representam as entradas necessárias para o desenvolvimento da função especificada na caixa e as de saída representam os dados ou objetos que foram produzidos. Setas de controle definem as condições requeridas para a produção das saídas adequadas. As setas de mecanismo definem os meios ou ferramentas através dos quais será exercida a função especificada pela caixa (DIAS et al., 2011).

A Figura 3.5 apresenta um exemplo de diagrama IDEF0 desenvolvido durante o projeto MitiSF₆. O diagrama contém três funções (A21, A22 e

Figura 3.4 – Exemplo de uma caixa e setas



Fonte: NIST (1993), Dias et al. (2011)

A23) relacionadas com o processo de manipulação do gás SF₆ utilizados nos disjuntores de alta tensão da empresa Eletrosul.

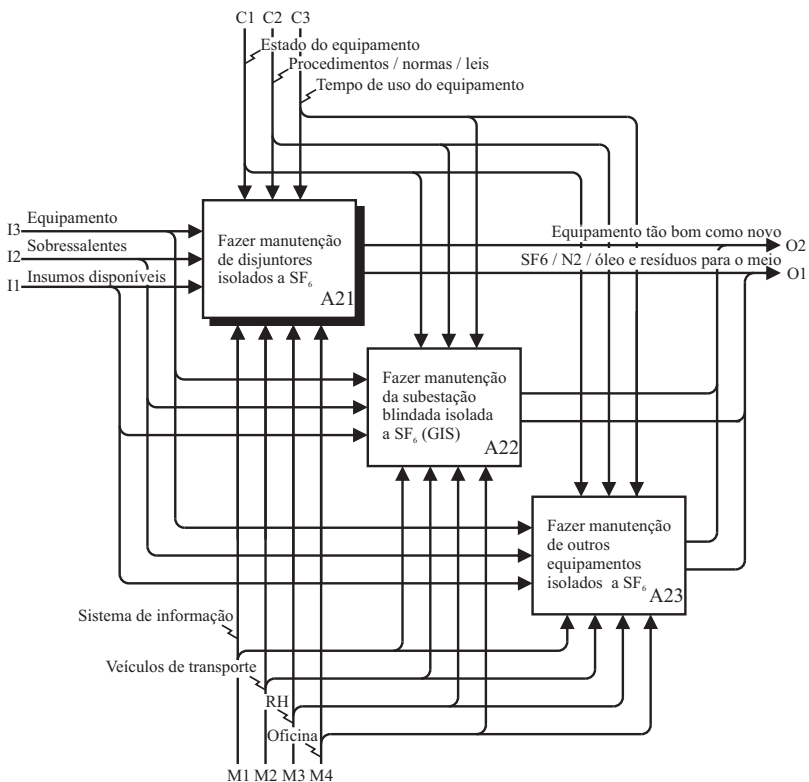
- Função A21: Fazer manutenção nos disjuntores isolados a SF₆
- Função A22: Fazer manutenção da subestação blindada isolada a SF₆
- Função A23: Fazer manutenção de outros equipamentos isolados a SF₆

Todas as funções apresentadas neste exemplo compartilham das mesmas entradas, controles, mecanismos e saídas. No entanto, cada uma apresenta particularidades como diferentes quantidades de perda de gás, procedimentos de operação, procedimentos de manutenção, peças sobressalentes entre outras características que devem ser estudadas a fim de mitigar a perda de SF₆.

Cada função pode ser desdobrada em outras subfunções a fim de se explorar os problemas de cada processo com maiores detalhes. Dado que alguma saída esteja fora dos padrões estipulados pelos controles, são realizadas análises dos procedimentos, documentos e ferramentas a fim de melhorar o processo.

Portanto, a técnica permite mapear as funções de um processo, de forma estruturada. Tal característica traz benefícios como o ganho de conhecimento sobre o processo, os procedimentos, as ações humanas, entre outras atividades – sendo uma técnica de suporte recomendada para as atividades de projeto e controle de processos.

Figura 3.5 – Exemplo de aplicação de IDEF0



Fonte: MT-PR-RT-NE-01 (UFSC/NEDIP, 2008, Apêndice A, p.21)

3.4 DIAGRAMAS DE BLOCOS PARA CONFIABILIDADE

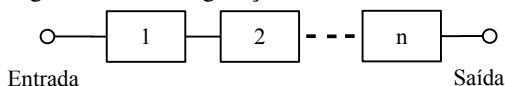
Para se calcular a confiabilidade de um sistema é preciso saber a relação funcional entre componentes, isto é, como irão operar para atender os requisitos do sistema. Uma forma muito utilizada para representação da relação entre os componentes de sistemas é por meio dos diagramas de blocos.

Tais diagramas, no contexto de confiabilidade, são conhecidos como diagramas de blocos para confiabilidade. Basicamente, é uma rede de blocos conectados funcionalmente, isto é, se houver um caminho interligando os blocos da entrada do sistema até a saída, significa que o sistema executa sua função, caso contrário estará em falha.

Cada bloco do diagrama pode representar um componente ou um conjunto de componentes na forma de um subsistema. Logicamente, a confiabilidade do sistema possui uma relação direta não só com a taxa de falha dos componentes, mas também com a configuração formada por esses blocos.

As configurações mais conhecidas são em série e em paralelo. Na configuração em série, Figura 3.6, a falha de qualquer componente da rede resulta na falha do sistema.

Figura 3.6 – Configuração em série

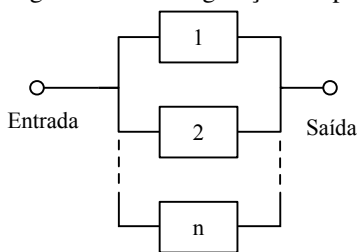


O cálculo da confiabilidade de um sistema em série, R_s , pode ser feito com o uso da Equação 3.2, onde $R_i(t)$ é a confiabilidade de cada componente i .

$$R_s(t) = \prod_{i=1}^n R_i(t) \quad (3.2)$$

Por outro lado, se os componentes estão em paralelo, Figura 3.7, é preciso que todos os componentes nesta configuração estejam em falha para que o sistema também falhe.

Figura 3.7 – Configuração em paralelo



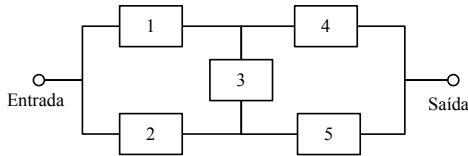
Para o cálculo da confiabilidade em paralelo, R_p , pode-se fazer uso da Equação 3.3.

$$R_p(t) = 1 - \prod_{i=1}^n [1 - R_i(t)] \quad (3.3)$$

Além destas configurações série/paralelo, existem outras mais complexas, como por exemplo a configuração do tipo ponte. Aqui existe um componente especial que dá flexibilidade para o sistema trabalhar com uma combinação maior de componentes.

Por exemplo, a Figura 3.8 é um sistema com configuração ponte, cujo componente especial é o item 3. A falha desse componente especial não causa a falha do sistema, mas reduz as possibilidades de combinações entre os componentes.

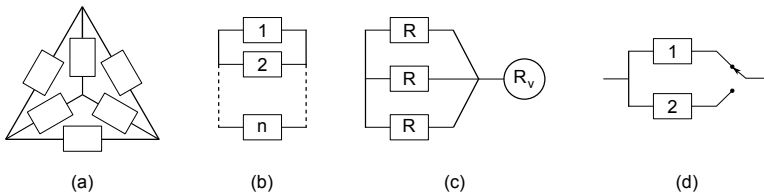
Figura 3.8 – Configuração em ponte



Fonte: Adaptado de Billinton e Allan (1992, p.101)

Outras configurações mais complexas apresentadas na Figura 3.9, podem ser vistas no trabalho de Vinadé (2003) e Billinton e Allan (1992).

Figura 3.9 – (a)Delta-estrela (b)R-em-N (c)Trimodular (d)Stand-by



Fonte: Vinadé (2003)

Assim, uma das primeiras etapas para se determinar a confiabilidade de um sistema é conhecer seu funcionamento, ou seja, a relação entre seus componentes e subsistemas. Comumente, busca-se desenvolver a modelagem, agrupando os componentes e subsistemas, ou analisando por partes, de forma a trazer para uma configuração série/paralelo, que é a mais simples, facilitando assim a análise e a coleta de resultados.

Com as informações geradas na análise de confiabilidade é possível planejar as paradas de manutenção, planejar a compra de peças sobressalentes, identificar pontos de monitoramento de falhas, entre outras atividades, as quais resultarão em um sistema com maior disponibilidade, visto que as ações irão atuar na confiabilidade e na manutenibilidade do sistema.

3.5 MÉTODO DE MONTE CARLO

Segundo Sobol (1983) o Método de Monte Carlo é um método de simulação numérica que tem como base a utilização de variáveis aleatórias. A primeira publicação sobre o método foi em 1949, no artigo “*The Monte Carlo method*”, sendo escrito por J. von Neumann e S. Ulam.

Segundo Hu (2005), enquanto as árvores de eventos dinâmicas, para eventos discretos, ocorrem somente em tempos pré-definidos, a simulação de Monte Carlo pode ocorrer em qualquer momento, e pode ser aplicada a sistemas reais – que são muitas vezes complexos –, usar taxas de falha variável, incluir atrasos (*delay*) como variável aleatória, entre outras características. Assim, a técnica apresenta grande flexibilidade o que a torna bastante atraente.

O comportamento do sistema é descrito por um conjunto de variáveis aleatórias, sendo que estas podem ser obtidas por meio de tabelas, sorteios realizados por *software* matemáticos, planilhas eletrônicas, roleta etc.

A Figura 3.10 apresenta um fluxograma simplificado do procedimento para a simulação de Monte Carlo proposto por Werner (1996). A simulação foi realizada fornecendo duas entradas (*INPUTs*): a primeira (INPUT 1) define a distribuição estatística de cada componente e a segunda (INPUT 2) estabelece a relação entre os componentes e o desempenho do sistema.

Desta forma, a medida que são obtidos os valores aleatórios dos componentes, em INPUT 1, estes são usados para calcular o desempenho do sistema, pois foi estabelecido uma relação entre componente e sistema em INPUT 2. O resultado da simulação, saída (*OUTPUT*), é um conjunto de valores que representam o desempenho do sistema, que são tratados estatisticamente.

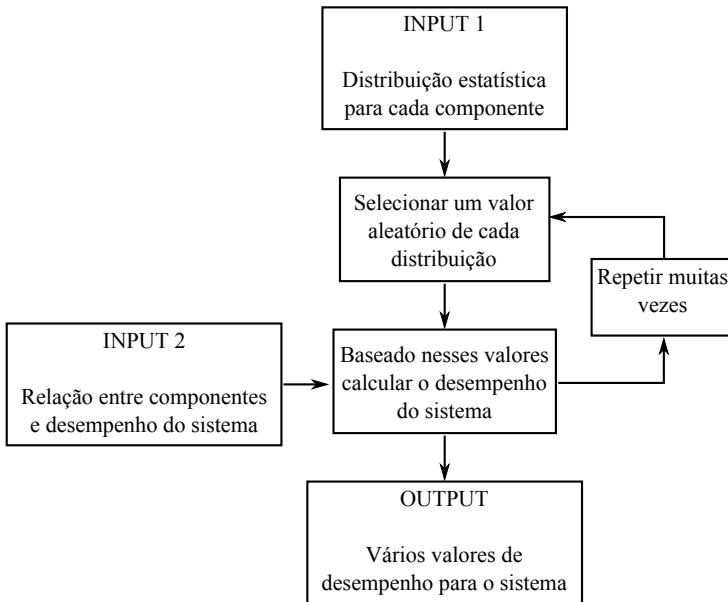
3.6 MANUTENÇÃO CENTRADA EM CONFIABILIDADE (MCC)

A manutenção centrada em confiabilidade é uma concepção de gestão de manutenção que combina, basicamente, várias técnicas e ferramentas para a administração da manutenção tais como as árvores de decisão (FTA, ETA, IDEFO) e análise do modo de falha e efeitos (FMEA, FMECA), de forma sistemática, para apoiar efetiva e eficientemente as decisões de manutenção (DIAS et al., 2011; FUENTES, 2006).

Segundo Fuentes (2006) a MCC busca, fundamentalmente, a:

- Preservação da função do sistema.
- Identificação das falhas funcionais e dos modos de falha dominantes.
- Priorização das falhas funcionais de acordo com as suas consequências.

Figura 3.10 – Fluxograma para simulação de Monte Carlo



Fonte: Werner (1996)

- Seleção das tarefas de manutenção aplicáveis e de custo eficiente favoráveis.

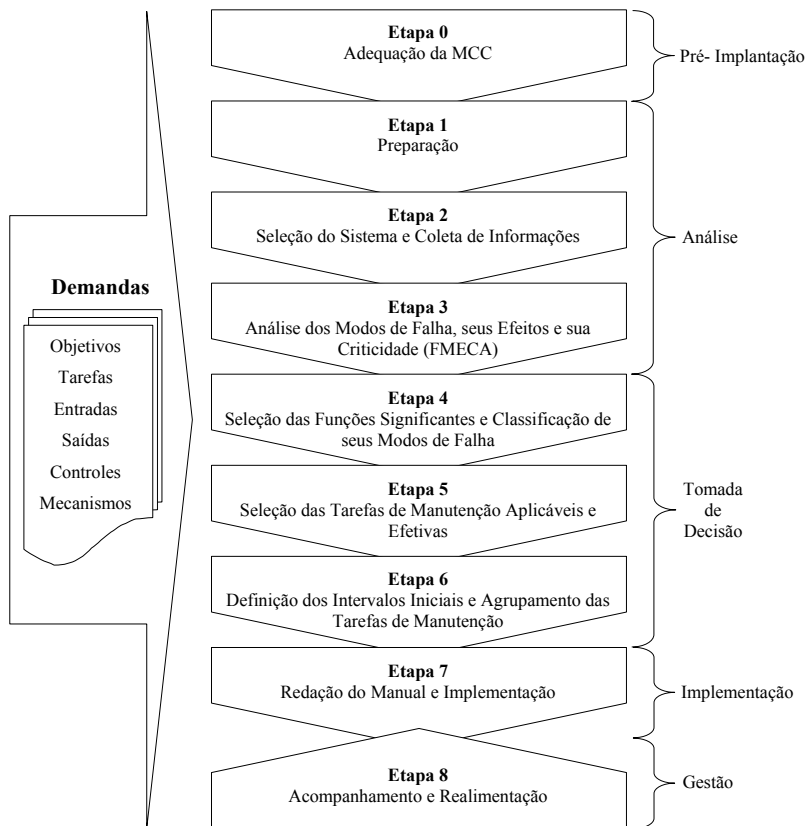
Existem diversos programas para implantação da MCC (Moubray (1997), Smith (2001), SAE (1999), NASA (2008), entre outras). No trabalho de Rigoni (2009) foi realizada uma extensa revisão na literatura sobre o tema, constituindo-se em um referencial teórico consistente e atualizado. Por esse motivo, esta metodologia para implantação de MCC será adotada neste trabalho, Figura 3.11, como uma das técnicas de suporte para análise de confiabilidade dinâmica.

A MCC apresentada é constituída de oito etapas. Algumas destas etapas possuem atividades e documentos importantes para a preparação e execução de uma análise de confiabilidade dinâmica – destacadamente as etapas 3, 4, 5 e 6.

Segundo Fuentes (2006), a MCC permite buscar respostas para as seguintes questões:

- Quais são as funções e os níveis normais de eficiência dos equipamentos

Figura 3.11 – Procedimento de referência para implantação da MCC



Fonte: Rigoni (2009)

em seu atual contexto operacional?

- Qual é o estágio da falha para haver perda da sua função?
- Qual é a causa de cada falha funcional?
- O que sucede quando cada falha ocorrer?
- De que forma cada falha se manifesta?
- O que se pode fazer para prevenir cada falha?

- O que se deveria fazer se uma tarefa preventiva adequada não pode ser executada?

As respostas para tais questões são fundamentais para a etapa de modelagem da manutenção na análise de confiabilidade dinâmica. Pois, na implementação computacional serão utilizadas informações como: efeito da falha do sistema, taxa de reparo, mecanismos de detecção da falha, caracterização da falha do sistema entre outras informações.

3.7 CONSIDERAÇÕES DO CAPÍTULO

Nesta seção foram apresentadas as técnicas de suporte FMECA, CNEA, IDEF0, diagramas de bloco para confiabilidade e MCC, consideradas como as mais relevantes para a análise de confiabilidade dinâmica neste trabalho. Evidentemente, existem outras técnicas podem colaborar no desenvolvimento (ETA, FTA, redes de petri, ESD, entre outras). Todavia as técnicas apresentadas neste capítulo já atendem as necessidades da metodologia para análise de confiabilidade dinâmica.

Algumas técnicas estão inter-relacionadas, como é o caso da FMECA e MCC. Ou seja, a análise do modo de falha e efeitos faz parte de uma das etapas da manutenção centrada em confiabilidade – no caso da metodologia apresentada por Rigoni (2009) a FMECA é realizada na etapa 3. Assim, dado que se tenha executado uma FMECA inicialmente, tem-se uma maior facilidade e rapidez na implantação da manutenção centrada em confiabilidade.

Em princípio, a CNEA poderia ser utilizada após a criação das tabelas FMECA. Mas foi durante o desenvolvimento do projeto MitiSF₆, que foi possível perceber que o uso da CNEA é bastante eficiente em identificar inconsistências nas tabelas FMECA. Por apresentar de forma clara o encadeamento dos eventos relacionadas com falha (causas → modos de falha → efeitos, barreiras propostas e implementadas), recomenda-se seu uso antes da execução da FMECA.

A técnica IDEF0 é utilizada no desdobramento funcional de processos. O uso da técnica junto com a MCC ajudará no mapeamento dos procedimentos e recursos (humanos, equipamentos) da manutenção.

Os diagramas de blocos para confiabilidade auxiliam na visualização da configuração do sistema. Nesta seção, foi apresentada como realizar o cálculo para as configurações em série e paralelo. No entanto, vale salientar que as equações apresentadas são utilizadas para análise de confiabilidade estática. Assim, servem apenas para obter valores de referência para serem comparados com a análise de confiabilidade dinâmica. O maior benefício da técnica aqui está relacionado com a visualização das configurações de operação do sistema,

e não com os valores que podem ser obtidos com os diagramas.

Os principais objetivos das técnicas estão relacionados com a aquisição, a organização e a representação do conhecimento.

4 METODOLOGIA PROPOSTA PARA ANÁLISE DE CONFIABILIDADE DINÂMICA

Esta seção apresenta uma metodologia para análise de confiabilidade dinâmica, sendo desenvolvida para sistemas que utilizam modelos comportamentais com características dinâmicas. Ou seja, é preciso que se tenha características que variam ao longo do tempo e com base nos valores assumidos são tomadas ações para impedir a falha do sistema.

Este capítulo inicia com a caracterização do sistema, posteriormente apresenta-se a relação com o projeto e o ciclo de vida e a descrição das etapas da metodologia.

4.1 CARACTERIZAÇÃO DO SISTEMA ABORDADO PELA METODOLOGIA

Os tópicos seguintes apresentam uma breve descrição sobre as “variáveis de estado do sistema” e os “estado do sistema”, utilizados pela metodologia proposta.

4.1.1 Variáveis de estado do sistema

As variáveis de estado são utilizadas para identificar o estado do sistema. Como o sistema é dinâmico, a variável de estado **tempo** é a principal variável a ser considerada. As outras variáveis dependem da aplicação, por exemplo: temperatura, pressão, vazão, posição, velocidade, força, etc.

As variáveis de estado tratadas pela metodologia podem ser contínuas ou discretas.

4.1.2 Estado do sistema

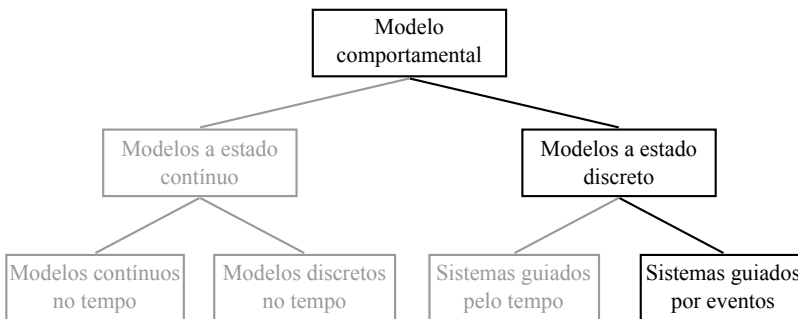
A metodologia é recomendada para sistemas com estados discretos. Assim, com base nos valores das variáveis de estado, o sistema pode estar, por exemplo, em sua **condição normal** de operação, em **emergência** ou em **falha**. Para calcular a confiabilidade do sistema (ou a probabilidade de falha) é verificado, ao final do tempo de missão, se o sistema está ou não em **falha**. Desta forma, para as análises de confiabilidade, o sistema deve ser representado por pelo menos dois estados: um que caracteriza como “bom” e outro como

“falha”. Dependendo da aplicação, em função da necessidade, pode-se criar outros estados além destes apresentados.

Ainda dentro do conceito de modelos a estado discreto, o sistema fica caracterizado como sistema **guiado a eventos**. Desta forma, se ao longo de um tempo de missão, ocorrem poucos eventos, a simulação demanda um menor tempo de processamento. Os principais eventos que influenciam nas simulações para o cálculo da confiabilidade dinâmica são: falha de componente, alterações de estados dos componentes realizados pelo controlador, conclusão do tempo de missão e ações de manutenção.

Portanto, os modelos comportamentais atendidos pela metodologia são os modelos a estados discretos, guiados por eventos, cuja classificação é apresentada na Figura 4.1.

Figura 4.1 – Classificação do modelo comportamental utilizado pela metodologia



Fonte: De Negri e Santos (2007)

4.2 MODELO DE REFERÊNCIA

Para a compreensão dos elementos contidos nas figuras apresentadas na metodologia é apresentado um modelo de referência na Figura 4.2, utilizado para representar cada etapa, sendo identificado um número “x” e um título contendo uma breve descrição na parte superior da figura.

As “Entradas” são informações ou pré-requisitos necessários para o início da etapa e ficam localizadas à esquerda da figura, sendo conectadas por setas na primeira atividade da etapa.

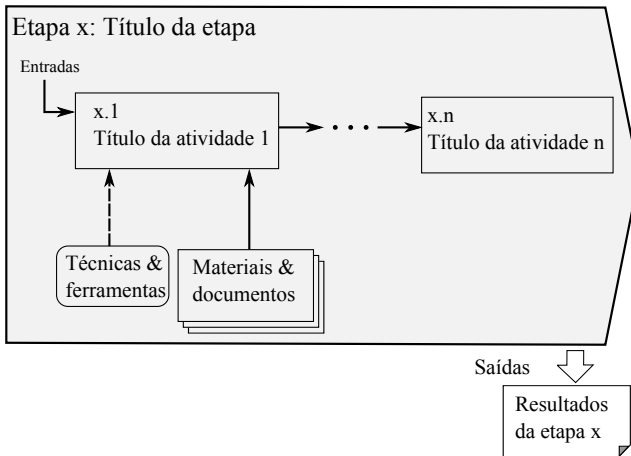
As atividades são ações ou procedimentos necessárias para a realização

da etapa. No modelo, a **Etapa x** possui n atividades (**x.1** até **x.n**) representadas por retângulos. Geralmente, cada etapa será constituída de várias atividades, as quais podem, ou não, compartilhar das mesmas técnicas & ferramentas e materiais & documentos.

As “Técnicas & ferramentas” de suporte estão dispostas na parte inferior de cada atividade, as quais estão representadas dentro de caixas com bordas arredondadas e conectadas às atividades por setas com linhas tracejadas.

Os “Materiais & documentos” também estão dispostos abaixo de cada atividade, sendo representados por um conjunto de folhas e setas com linha contínua. Os “Resultados” de cada etapa estão representados no canto inferior direito da figura, identificados como “Saídas”.

Figura 4.2 – Modelo de referência para cada etapa da metodologia

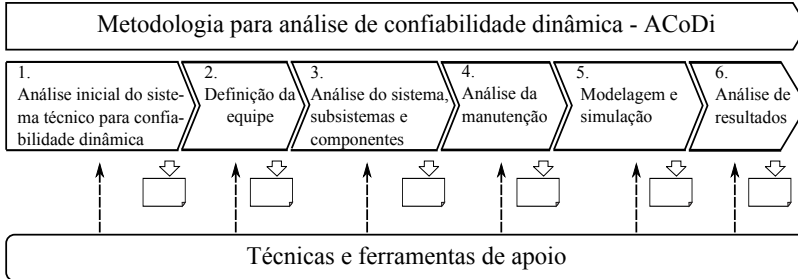


A seguir, a Figura 4.3 sintetiza as etapas principais do processo metodológico para análise de confiabilidade dinâmica, denominada por ACoDi, cujas etapas são:

1. Análise inicial do sistema técnico para confiabilidade dinâmica)
2. Definição da equipe
3. Análise do sistema, subsistemas e componentes
4. Análise da manutenção
5. Modelagem e simulação computacional da falha no sistema técnico
6. Análise de resultados

As etapas da metodologia para análise de confiabilidade dinâmica são suportadas por técnicas e ferramentas de apoio como apresentadas no Capítulo 3 e por outras como, por exemplo: *brainstorming*, questionários estruturados e não estruturados, análise funcional, etc.

Figura 4.3 – Metodologia para análise de confiabilidade dinâmica (ACoDi)



A metodologia ACoDi é uma variante do Processo de Desenvolvimento Integrado de Produtos – PRODIP – desenvolvido por Back et al. (2008), Figura 4.4. Neste caso, por mais complexo que seja o sistema, há que organizar o rito de análise dentro do ciclo de vida, para o atributo de confiabilidade. Este atributo, sofre influência de todos os requisitos e necessidades estabelecidas desde o planejamento, mas sua análise é recomendável a partir do projeto preliminar.

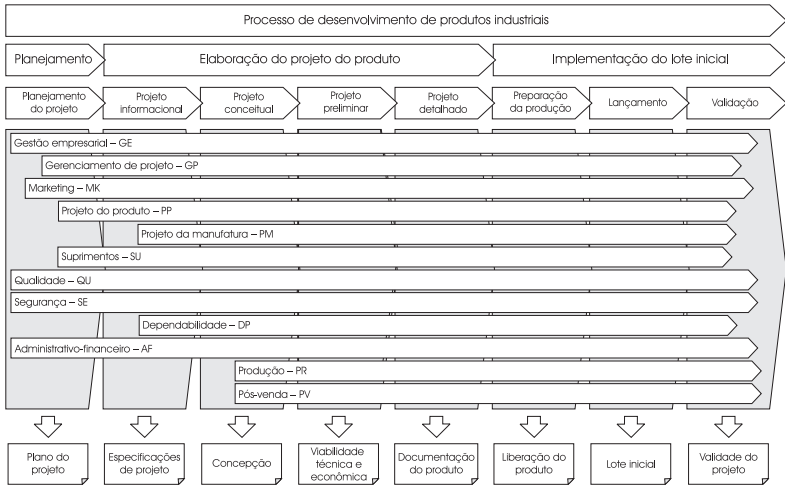
A confiabilidade é entendida, dentro da metodologia PRODIP, como um atributo do produto e no caso está associado ao processo de desenvolvimento do produto. Nesta tese, a análise pode servir para avaliação de produtos em desenvolvimento ou já em uso. Assim, a metodologia proposta vai além do que está contextualizado na Figura 4.4.

No caso da confiabilidade dinâmica, por exigir ainda mais informações do que uma análise estática, depende também do projeto detalhado por ter que considerar, além da estrutura física do sistema técnico, também os *softwares* embarcados, os planos de operação e de manutenção que só ficam concluídos ao final da fase de projeto detalhado.

A Figura 4.5 mostra a relação da metodologia ACoDi com o processo de desenvolvimento de produtos PRODIP. Assim, as saídas do projeto conceitual, preliminar e detalhado são as informações de entrada para a metodologia, que traz como saída: função densidade de falha do sistema para as falhas evidentes e ocultas, probabilidade de falha do sistema, confiabilidade, cenários de falha mais críticos, manutenibilidade e gestão da manutenção.

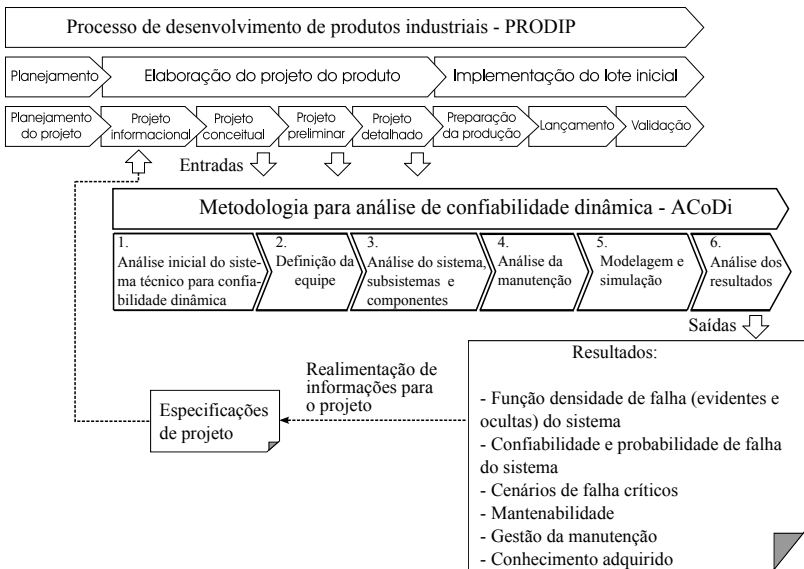
Os resultados obtidos com a metodologia visam dar suporte ao produto no ciclo de vida, a fim de obter melhores resultados para a confiabilidade do

Figura 4.4 – Processo de desenvolvimento integrado de produtos – PRODIP



Fonte: Back et al. (2008)

Figura 4.5 – Relação da metodologia ACoDi com o PRODIP



sistema como: incluir novas funções relacionadas à segurança e proteção do sistema, substituição de alternativas de solução na etapa do projeto conceitual, propor mudanças nos planos de operação/manutenção, incluir outros dispositivos de monitoramento para o sistema, etc. Ou seja, a análise de confiabilidade dinâmica gera informações que irão propor mudanças, desde especificações de projeto – na etapa do projeto informacional – até ações de operação e manutenção durante a etapa de uso.

Vale ressaltar que, embora a metodologia para análise de confiabilidade dinâmica possa ser aplicada desde a fase do projeto preliminar, é na etapa de uso que se tem a maior quantidade de informações, o que conseqüentemente facilita a sua aplicação.

Para melhor relacionar a metodologia proposta com a do PRODIP, tomou-se o ciclo de vida de um item como sendo do planejamento do item ao descarte. A Figura 4.6 sintetiza esta abordagem. As informações da fase de uso e descarte, que servem de entrada de dados para as análises de confiabilidade, no contexto da metodologia estão, relacionados com as taxas de falha e reparo dos componentes, testes realizados em campo, histórico de falhas, etc. Tais informações aproximam o modelo de confiabilidade do comportamento do sistema real.

4.3 ATUALIZAÇÃO DO MODELO

A presente metodologia divide a análise de confiabilidade dinâmica em quatro elementos fundamentais: processos dinâmicos, equipamentos, ações humanas e *software*.

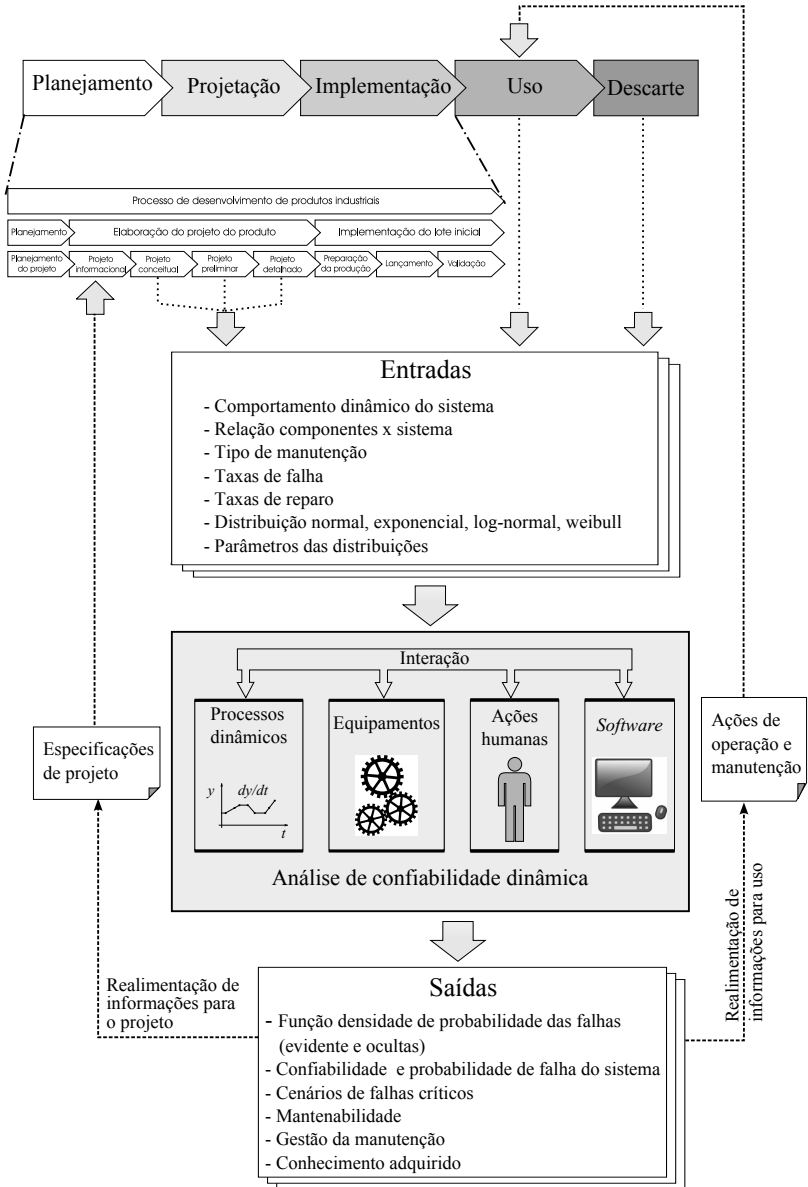
Os processos dinâmicos são ditados pelas relações entre os componentes e o sistema. Os equipamentos possuem características como carga de trabalho, sequências de operação, ambiente de instalação, taxas de falha dos seus componentes entre outras características que influenciam os componentes, logo, agem também sobre o comportamento dinâmico do sistema.

As ações humanas sobre os equipamentos, bem como as reações destes frente a determinados comportamentos dinâmicos dos sistemas estão relacionados. Por fim, o *software* faz a compilação de todas essas informações. A forma que foi desenvolvido tem reflexos na apresentação dos dados e também nas implementações futuras.

Todos esses elementos estão relacionados e fazem parte de uma análise de confiabilidade dinâmica. A Figura 4.6 apresenta os elementos constituintes da análise. À medida que as análises são desenvolvidas, ao longo de meses, é possível refinar o modelo tornando-o mais próximo da realidade.

Com isso, os valores de **entrada** da análise sofrerão alterações – podem

Figura 4.6 – Relação da metodologia com todo o ciclo de vida do produto



haver mudanças na representação dinâmica do sistema, nas funções adotadas (normal, exponencial, log-normal, weibull) ou em seus parâmetros etc – obtendo outras **saídas**. Mostra-se nesta etapa de atualização do modelo, o papel de grande importância do *software*. Assim, deve-se prever estas atualizações, sendo portando recomendado a utilização da filosofia de programação orientada a objetos.

As seções que se seguem apresentam as etapas para o desenvolvimento da metodologia de análise de confiabilidade proposta.

4.4 ETAPA 1: ANÁLISE INICIAL DO SISTEMA TÉCNICO PARA CONFIABILIDADE DINÂMICA

A etapa 1, representada pela Figura 4.7, corresponde a uma análise do sistema técnico para verificar se existe a necessidade de realizar a análise de confiabilidade dinâmica, ou se uma análise estática é suficiente. Os principais critérios para a tomada de decisão são: a análise quanto ao comportamento dinâmico, à criticidade e à disponibilidade do sistema.

Desta forma, cada um dos critérios são descritos como atividades da etapa, que ao final irão dar suporte à tomada de decisão: uso da confiabilidade estática ou dinâmica. As atividades desta etapa são:

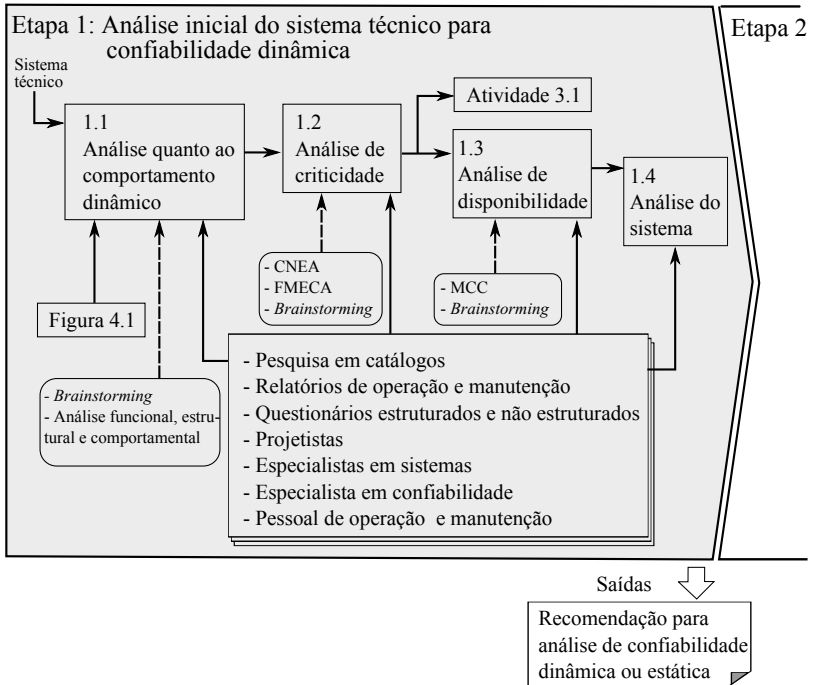
- Atividade 1.1: Análise quanto ao comportamento dinâmico
- Atividade 1.2: Análise da criticidade do sistema
- Atividade 1.3: Análise da disponibilidade do sistema
- Atividade 1.4: Análise do sistema

Cada uma das atividades desta etapa inicial serão abordadas a seguir.

4.4.1 Atividade 1.1: Análise quanto ao comportamento dinâmico

O comportamento dinâmico pode estar relacionado com o processo de degradação dos componentes, às mudanças de configuração do sistema, às ações humanas durante a operação e a manutenção. Nas análises em que se deseja levar em conta tais variações (características dos componentes, configuração, tempo das ações) recomenda-se a análise de confiabilidade dinâmica. Nesta atividade pode-se contar com a participação de projetistas, especialistas em modelagem de sistemas, profissionais responsáveis pela operação e manutenção do sistema.

Figura 4.7 – Atividades da etapa 1



Pode-se tomar como exemplo o caso em que se deseja avaliar o efeito na confiabilidade do sistema, em função do tempo de reação da equipe de operação/manutenção. Equipes com maior capacitação técnica realizam tarefas em menos tempo e com menores chances de erros, o que consequentemente irá refletir na confiabilidade do sistema.

No apêndice A é apresentada uma seção sobre as diferenças entre um sistema representado por um modelo comportamental estático e dinâmico. Em resumo, dependendo da forma com o problema será abordado, pode-se considerar que o sistema é estático ou dinâmico. Assim, recomenda-se uma leitura naquela seção para maiores esclarecimentos.

4.4.2 Atividade 1.2: Análise da criticidade do sistema

Para a avaliação da criticidade recomenda-se usar a técnica FMECA – Análise dos modos de falhas, efeitos e criticidade. A criticidade do sistema leva em consideração a frequência de ocorrência (O), a dificuldade de detecção

(*D*) e a severidade das falhas (*S*). Além deste parâmetro, a técnica traz benefícios como evidenciar as características críticas ou significativas dos sistemas, permite obter listas de procedimentos para detecção de falhas, direcionar a elaboração de testes, destaca potenciais problemas de segurança, entre outras informações que servirão como entrada de dados para esta etapa.

Destaca-se que, na análise de criticidade, é importante avaliar cuidadosamente a severidade do modo de falha. Embora o NPR (índice de criticidade ou número de prioridade de risco) possa ter um baixo valor – quando os índices de ocorrência e detecção são baixos –, deve-se também considerar o sistema como sendo crítico aqueles que possuem modos de falha que podem conduzir danos ao homem e ao meio ambiente.

Esta análise é importante pela premissa básica de que a aplicação da confiabilidade dinâmica é requerida apenas para sistemas cujas falhas podem ter consequências ambientais, humanas ou do empreendimento. Em grande parte dos casos a Severidade (*S*) se constitui no aspecto mais importante nesta análise. Contudo, devido as implicações de uma falha e a dificuldade de detecção (*D*) da mesma, pode gerar nos sistemas complexos, condições de falhas ocultas que pode comprometer o sistema. Se levar em consideração que na maioria dos casos se requer que o sistema técnico não tenha descontinuidade de operação, tal fato potencializa em muito as exigências para esta análise.

4.4.3 Atividade 1.3: Análise da disponibilidade do sistema

Existem sistemas em que é fundamental que a disponibilidade tenha valor extremamente elevado¹. Nesse caso, as manutenções devem ser realizadas com o sistema em operação (manutenção a quente). Para isso, é importante que se tenha componentes redundantes para que, durante a operação do componente reserva, seja realizada a manutenção do componente principal o mais rápido possível, a fim de garantir que sempre haja um componente reserva pronto para ser usado.

A implantação de uma manutenção centrada em confiabilidade (MCC) e o uso da FMECA ou técnicas da análise de risco, priorizam as funções críticas do sistema técnico que devem ser mantidas. Assim, uma análise de confiabilidade dinâmica pode dar suporte para as tomadas de decisão, por exemplo, apresentando para um dado tempo, quais itens devem ser testados para identificação de falhas ocultas no sistema que tem comportamento di-

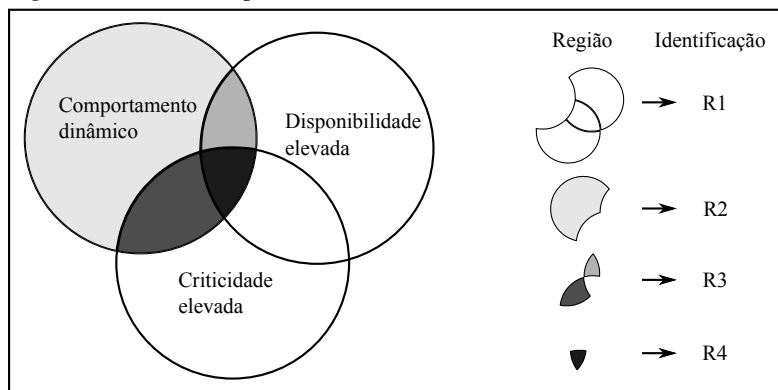
¹A disponibilidade neste caso está relacionada com o gerenciamento da continuidade do negócio, que tem como objetivo de não permitir a interrupção das atividades do negócio e proteger os processos críticos, como por exemplo o fornecimento de energia elétrica, água, serviço aéreo, etc. Mesmo que a probabilidade de ocorrência (*O*) seja pequena, para esses sistemas, deve-se cuidar, tendo em vista o impacto da falta da disponibilidade do sistema técnico ou dos serviços.

nâmico. Ou seja, com esta análise é possível fazer simulações para testar a garantia de continuidade, mesmo que alguns dos itens da função principal do sistema estejam em falha ou em manutenção.

4.4.4 Atividade 1.4: Análise do sistema

A condição essencial para o uso da confiabilidade dinâmica é que o sistema tenha um comportamento dinâmico. Todavia, dependendo da disponibilidade e criticidade do sistema, ainda é possível fazer uso da análise de confiabilidade estática mesmo tendo o sistema um comportamento dinâmico. A Figura 4.8 representa os critérios para se adotar a análise de confiabilidade dinâmica.

Figura 4.8 – Critérios para o uso da confiabilidade dinâmica



A análise inicial considera que um sistema está configurado, para efeito de aplicação de confiabilidade dinâmica, na condição de ter comportamento dinâmico, disponibilidade elevada e criticidade elevada. Contudo, nem todo sistema está simultaneamente nas três condições. Assim, é requerido que se proceda uma análise para tomada de decisão quanto a aplicação de confiabilidade dinâmica ou estática. A maioria dos sistemas requerem apenas análise de confiabilidade estática, definido pela região R1, por não terem comportamento dinâmico.

Se tiver comportamento dinâmico, ainda assim pode não ser requerido a análise de confiabilidade dinâmica, como apontada pela região R2. Os sistemas que se encontram nessa região possuem comportamento dinâmico, no entanto, não possuem criticidade ou disponibilidade elevada. Assim, o uso da análise de confiabilidade dinâmica para esses sistemas é opcional.

A região R3 é definida para os sistemas que tenham comportamento dinâmico e estejam na região de disponibilidade elevada ou criticidade elevada. Nesta região é fortemente recomendada a análise de confiabilidade dinâmica.

Por último na região R4, é obrigatório o uso da análise de confiabilidade dinâmica, visto que estes sistemas além do comportamento dinâmico, exigem disponibilidade elevada e possuem criticidade elevada.

A condição necessária para o uso da análise de confiabilidade dinâmica é que o sistema tenha comportamento dinâmico. Portanto, a disponibilidade elevada e a criticidade são critérios adicionais que irão refinar a decisão de se realizar uma análise de confiabilidade dinâmica ou não. Para a tomada de decisão, pode-se criar uma matriz semelhante à matriz de risco, que é uma forma de avaliar os riscos de um sistema técnico. A matriz apresentada na Figura 4.9 (DIAS et al., 2011), é uma proposta de avaliar o risco em complementação ou substituição ao índice NPR (Número de prioridade de risco).

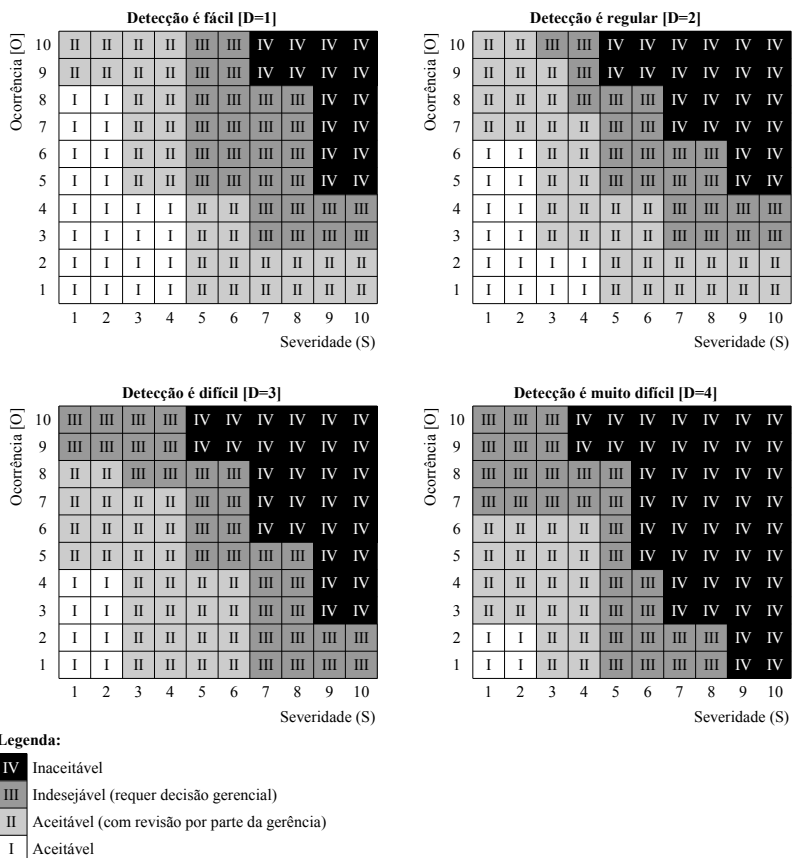
A avaliação do risco apresentada por Dias et al. (2011), Figura 4.9, é realizada por um conjunto de 4 matrizes, sendo que cada uma representa um grau de detecção das falhas. Cada matriz por sua vez é uma combinação dos índices de ocorrência (O) e severidade (S). Portanto, de acordo com os índices de “detecção” (D), “ocorrência” (O) e “severidade” (S), pode-se avaliar o risco como aceitável, indesejável e inaceitável.

Vale ressaltar a importância de se destacar o índice de severidade. Portanto, ao observar a forma como a criticidade do sistema é avaliada comumente nas análises de FMECA, considerando somente o NPR, verifica-se que a severidade (S) fica mascarada por estar embutida dentro do índice de criticidade ($NPR = S \cdot O \cdot D$). Para evidenciar sua importância e manter o mesmo critério utilizado nas análises FMECA, pode-se fazer uso de quatro matrizes – como apresentado por Dias et al. (2011) – ao invés de uma, fazendo uma distinção quanto ao impacto dos efeitos gerados com a falha: severidade baixa, média, perigosa e catastrófica.

A Figura 4.10 é um exemplo de matriz que poderia ser utilizada para a tomada de decisão na escolha da análise de confiabilidade estática ou dinâmica. A figura foi desenvolvida a partir da matriz de risco de Dias et al. (2011), onde os índices de ocorrência (O) e severidade (S) foram substituídos pela disponibilidade e criticidade do sistema.

Na Figura 4.10 apresenta-se a matriz para avaliar os sistemas dinâmicos, no qual pondera-se os aspectos de disponibilidade e criticidade do sistema. Para os sistemas em que é exigida baixa disponibilidade e criticidade, a análise de confiabilidade dinâmica é opcional, região I (R2). Na proporção em que os critérios vão sendo mais exigentes, a análise pode se tornar “recomendada” – região II (R3) –, “fortemente recomendada” – região III (R3) – e “obrigatória” – região IV (R4) –. As identificações dentro dos parênteses (R2, R3 e R4)

Figura 4.9 – Relações determinísticas para avaliar a aceitação do risco



Fonte: Dias et al. (2011)

foram incluídas nas Figura 4.10 para relacionar a matriz com a Figura 4.8.

A matriz apresentada é uma sugestão para auxiliar a tomada de decisão. Dependendo do sistema técnico e da equipe de trabalho, as regiões (I, II, III e IV) irão sofrer mudanças, sendo alocadas mais espaços para uma região ou outra.

Figura 4.10 – Relações determinísticas para escolha da análise de confiabilidade dinâmica

Disponibilidade	10	IV	IV	IV	IV	IV	IV	IV	IV	IV	
	9	IV	IV	IV	IV	IV	IV	IV	IV	IV	
	8	III	III	III	III	III	IV	IV	IV	IV	
	7	III	III	III	III	III	IV	IV	IV	IV	
	6	II	II	II	II	III	III	III	IV	IV	
	5	II	II	II	II	II	III	III	III	IV	
	4	II	II	II	II	II	III	III	IV	IV	
	3	I	I	I	II	II	II	III	III	IV	
	2	I	I	I	II	II	II	III	III	IV	
	1	I	I	I	II	II	II	III	III	IV	
		1	2	3	4	5	6	7	8	9	10
		Criticidade									

Legenda:

Uso da análise de confiabilidade dinâmica	}	IV	Obrigatória	→ R4	} R3
		III	Fortemente recomendada		
		II	Recomendada		
		I	Opcional	→ R2	

Fonte: Adaptado de Dias et al. (2011)

4.5 ETAPA 2: DEFINIÇÃO DA EQUIPE

A equipe deve ser definida com profissionais que tenham conhecimento para estabelecer os critérios de análise como recomendado na Figura 4.8 e tomadas de decisão como o indicado na Figura 4.10. Em qualquer que seja a condição há que conhecer tecnicamente o item (componente, subsistema ou sistema) em análise e as técnicas demandadas para uma análise de confiabilidade.

A equipe deve ser constituída por profissionais com conhecimentos em diversas áreas e características como:

- Conhecimento do item em análise
- Conhecimento do atributo confiabilidade
- Segurança humana, ambiental e física do sistema
- Análise de risco
- Gestão da operação
- Gestão da manutenção
- Análise de falhas
- Análise e desenvolvimento computacional

Em outras palavras, a equipe deve ser constituída por profissionais que possam fornecer informações sobre: projeto, procedimentos de operação, configurações de operação (normal e emergência), alarmes, tempo de falha de componentes, tempo de reparo, tratamento e dados estatísticos, implementação computacional, entre outras informações.

A Figura 4.11 representa a etapa de definição da equipe de analistas, que será definida em função do sistema técnico a ser modelado. Esta etapa apresenta apenas uma atividade, 2.1, onde se procede a seleção dos profissionais ou das habilidades envolvidas com o sistema, requeridos para auxiliar na análise de confiabilidade dinâmica.

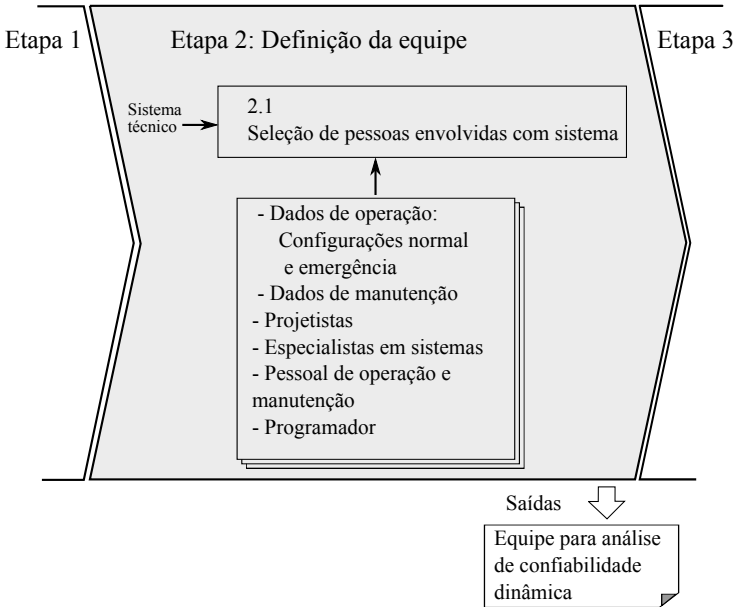
A presença de um profissional em informática na equipe se torna importante não somente pelo tempo gasto na implementação, mas também para a documentação e desenvolvimento de um sistema flexível que torne fácil realizar modificações futuras, construir um banco de dados, entre outras atividades que deverão ser realizadas ao longo do ciclo de vida.

Por fim, é preciso que se tenha conhecimentos de estatística para o processamento das informações: análise do gerador de números aleatórios, construção dos histogramas de falhas e análise das dispersão dos resultados. A recomendação é que o grupo seja constituído de 5 a 8 analistas, sendo requerido da equipe, prioridade de conhecimento em confiabilidade, no sistema técnico e em análise computacional.

4.6 ETAPA 3: ANÁLISE DO SISTEMA, SUBSISTEMAS E COMPONENTES

É a partir deste cenário que, após montar a equipe, inicia-se efetivamente a análise do sistema técnico sob o ponto de vista da confiabilidade. A

Figura 4.11 – Atividade da etapa 2



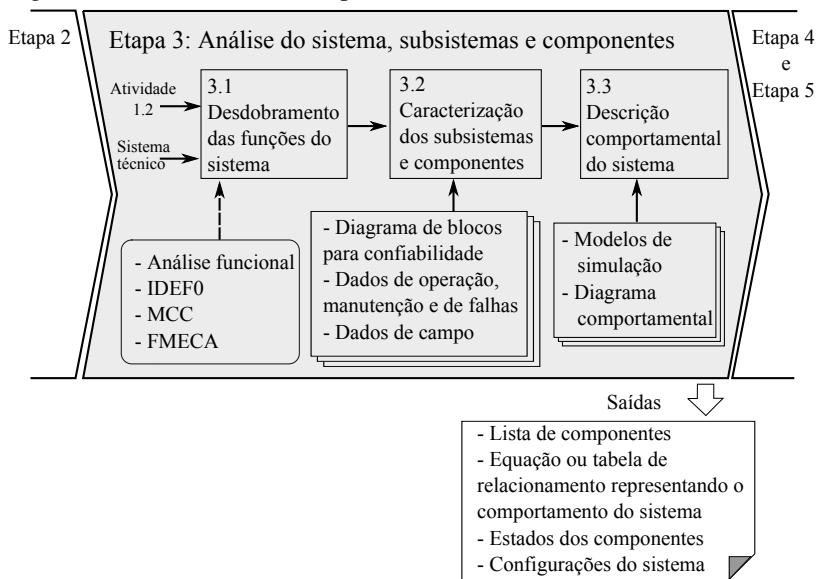
consideração do atributo da confiabilidade, como se sabe, deve ser feita durante o projeto. Contudo, por causa de incidentes passados ocorridos na operação ou por exigência legal devido atualização da legislação, também se deflagre o processo de análise no ciclo de vida de uso. Muitas vezes, a consideração das restrições legais, os eventos de falha ocorridos, o investimento financeiro feito e a visão e missão do empreendimento também influenciam a opção por análise de confiabilidade dinâmica.

Esta etapa é constituída de três atividades, cuja sequência pode ser vista na Figura 4.12:

- Atividade 3.1: Desdobramento das funções do sistema
- Atividade 3.2: Caracterização dos subsistemas e componentes
- Atividade 3.3: Descrição comportamental do sistema

Basicamente, é realizada a discretização do problema, buscando os principais subsistemas e componentes. Posteriormente, são obtidas informações da operação/manutenção dos subsistemas e componentes, sendo avaliada

Figura 4.12 – Atividades da etapa 3



a influência de cada uma das partes sobre a função global do sistema técnico.

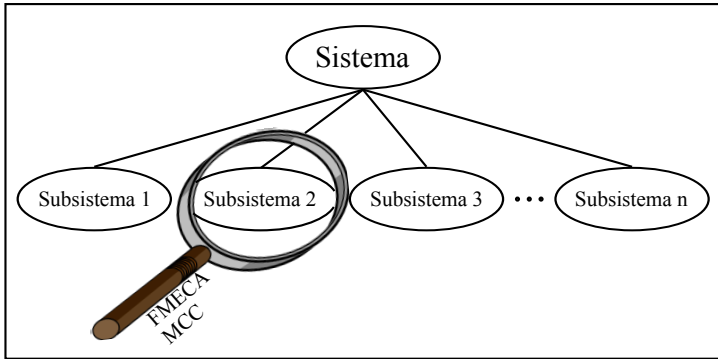
4.6.1 Atividade 3.1: Desdobramento das funções do sistema

Geralmente, os sistemas são compostos por uma quantidade muito grande de componentes e subsistemas. Desta forma, é preciso organizar quais componentes ou subsistemas que irão participar do estudo. A atividade 1.2 realizada para avaliar a criticidade do sistema é uma das entradas para esta etapa. Para desenvolver a atividade 3.1 há que se utilizar de técnicas que proporcionem a explicitação do conhecimento da equipe de análise (definida na Etapa 2) na forma de documentos racionalizados para uma futura implementação computacional, com vistas a manter continuidade da análise e também obter, tanto quanto possível, informações quantificáveis.

A primeira atividade da equipe é determinar se a análise será realizada em todo o sistema técnico, avaliado na etapa 1, ou será em uma parte do sistema. A Figura 4.13 apresenta esta situação, onde existe um sistema composto por n subsistemas.

A realização da FMECA na etapa 1 (atividade 1.2: Análise quanto à criticidade), avaliou a criticidade do sistema. Considerando que o sistema

Figura 4.13 – Priorização da análise



possui uma criticidade elevada, deve-se avaliar neste momento se a análise será realizada para todo o sistema ou em algum subsistema específico. Para essa decisão, pode-se revisar os documentos da FMECA, CNEA e relatórios de falhas da MCC.

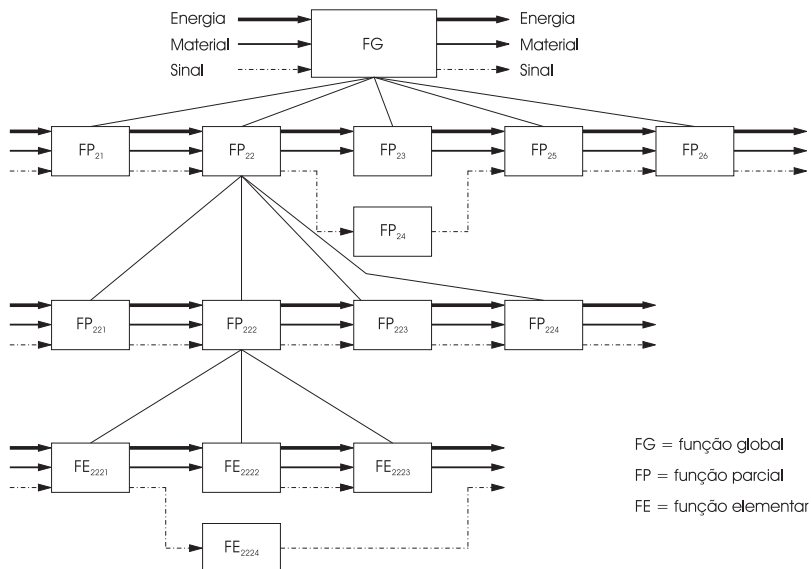
O objetivo desta análise inicial é racionalizar os esforços, buscando identificar as partes mais importantes do sistema. A análise será realizada prioritariamente nos subsistemas que possuem maior influência na função principal do sistema, ou quando estiver relacionado com os sistemas de segurança e proteção. A escolha feita pela equipe poderá ser: analisar o sistema todo, ou se restringir a um, ou mais, subsistema.

A partir da escolha de qual subsistema a ser analisado, a próxima ação é o desdobramento das funções do sistema ou subsistema. A análise começa com a função global do sistema (FG), ou do subsistema, sendo desdobrada em funções mais simples, denominadas funções parciais (FP). O nível mais detalhado das funções é denominado de funções elementares (FE). A Figura 4.14 ilustra o desdobramento da função global apresentada por Back et al. (2008). Além das funções, são representadas os fluxos de energia, material e sinal.

A IDEF0 é uma técnica recomendada para realizar análise funcional de processos. Da mesma forma que o desdobramento funcional, a técnica também permite o desdobramento funcional em níveis, e permite visualizar a comunicação entre uma função e outra, bem como o fluxo de informações dos controles, mecanismos, entradas e saídas. Portanto, o uso desta técnica torna-se fortemente recomendado para essa atividade.

Após o desdobramento das funções, tem-se uma estrutura funcional do sistema ou subsistema. Esta representação facilita a comunicação entre os membros da equipe e permite segregar as funções mais importantes para o processo, que podem ser utilizadas para o desenvolvimento de um novo

Figura 4.14 – Desdobramento da função global



Fonte: Back et al. (2008)

FMECA ou MCC, mais detalhado, ou realimentar as antigas análises.

Para sistemas já em uso, por exemplo, serão utilizadas informações como: relatórios de manutenção, histórico de incidentes, dados de taxas de falha, componentes e subsistemas com características críticas, entrevistas com especialistas, analogia com sistemas semelhantes, entre outras fontes. Tais informações são obtidas na etapa de uso do ciclo de vida do desenvolvimento de produtos.

Para projetos novos, durante o desenvolvimento do projeto conceitual, é realizada a análise funcional do sistema, obtendo a estrutura de funções. Para cada função são investigados diferentes princípios de solução, resultando na construção da matriz morfológica. Destaca-se que, mesmo um produto encontrando-se na etapa de projeção, pode-se obter as funções ou subfunções mais críticas, que serão utilizadas nesta atividade de desdobramento.

Com a lista de componentes mais críticos do sistema ou daqueles que tem influência no comportamento do sistema, pode-se então realizar uma subdivisão e organização do sistema em subsistemas e componentes.

As funções dos sistemas e componentes são uma das mais importantes informações para as técnicas FMECA, CNEA e MCC, principalmente, quando a análise é realizada com uma abordagem funcional, em que o modo de falha

é definido como uma “não função” do componente.

Após obter a estrutura funcional é preciso relacionar as funções com os subsistemas e componentes. Com isso, tem-se um mapeamento dos componentes e subsistemas mais importantes para a função global, permite ter um melhor entendimento sobre o funcionamento do sistema e uniformização do conhecimento entre os participantes da análise.

4.6.2 Atividade 3.2: Caracterização dos subsistemas e componentes

Após realizar o desdobramento do sistema, é possível analisar o comportamento do sistema em função dos possíveis estados dos subsistemas e componentes². Portanto, a caracterização dos subsistemas e componentes inicia com a análise dos possíveis estados que os itens podem assumir.

A Figura A.10, apresentada no Apêndice A, é um exemplo de diagrama de estados de um item, que ao longo do seu ciclo de vida pode assumir qualquer um dos seis estados, que são obtidos com a combinação de três condições funcionais (sem falha, com falha evidente, com falha oculta) com duas condições operacionais (ligado, desligado):

- Sem falha

O item pode estar sem falha e sua condição operacional pode ser desligado ou ligado.

- Com falha evidente

O item com falha evidente pode estar travado na posição “ligado” ou “desligado”. Está caracterizado como falha evidente porque sua condição operacional atual difere da condição normal de operação. Ou seja, o item deveria estar na condição ligado e agora está desligado. Essa diferença com a condição de operação permite detectar a falha.

- Com falha oculta

A falha oculta é difícil de ser detectada, visto que o componente está travado na posição em que coincide com a condição de operação normal. Ou seja, na condição normal o item deveria estar ligado e a falha faz com que o item fique travado na posição ligado. Este tipo de falha só é percebido quando é exigida uma mudança de estado do item. Somente

²Os subsistemas e componentes serão tratados como item. Segundo a norma NBR 5462 (ABNT, 1994) item é definido como “qualquer parte, subsistema, sistema ou equipamento que possa ser considerado individualmente e ensaiado separadamente.”

nesse momento a falha deixa de ser oculta e passa a ser uma falha evidente.

A falha oculta pode ser detectada com manutenções preventivas, em que os itens do sistema são verificados com uma frequência pré-determinada de período de inspeção.

Vale ressaltar que os estados apresentados na Figura A.10 servem apenas para orientação. O número de estados de um item pode ser bem maior do que seis. Por exemplo, se ao invés de duas, fossem três (aberto, fechado, parcialmente aberto) as condições operacionais. A combinação com as três condições funcionais (sem falha, com falha evidente, com falha oculta) poderiam gerar um total de nove estados.

Assim, com base nos dados de operação, manutenção e de falha, deve-se estabelecer os possíveis estados de cada item obtido na atividade 3.1.

A combinação dos estados dos componentes têm influência sobre o sistema, sua variável de controle e derivadas. Devido aos fatores dinâmicos dos sistemas – mudança de configuração, estados e características dos componentes e tempo –, à elevada quantidade de componentes e estados, é desaconselhável analisar o efeito no comportamento do sistema para cada combinação sem o auxílio de uma implementação computacional. Isso porque, mais do que a análise o importante é a permanência e a repetitividade da análise.

Assim, na implementação computacional cria-se uma variável denominada “componente” com informações do tipo: nome do componente, estado atual, taxa de falha, tempo para a falha, estado inicial, taxa de reparo, entre outras informações. Durante a simulação induz-se mudanças nos componentes e consequentemente no sistema, que pode falhar ou atingir o tempo de missão, ou seja, sucesso. Toda esta racionalidade de análise efetuada a partir do conhecimento sistematizado do sistema e das informações dos especialistas, permite tomada de decisão onde a descontinuidade da função fica mitigada. Maiores detalhes serão apresentados na seção de implementação computacional.

Cada componente será identificado por um nome, condição de operação inicial (ligado ou desligado), efeito funcional no sistema, possíveis estados, função densidade de falha, taxa de falha, função densidade de reparo, taxa de reparo, entre outras informações. Para obter esses detalhes, deve-se recorrer a fontes como:

- Relatórios de manutenção
- Análise em sistemas similares
- Testes

- Dados de campo
- Histórico de incidentes
- Dados de taxa de falhas
- Entrevistas com especialistas
- Requisitos legais
- Política institucional

4.6.3 Atividade 3.3: Descrição comportamental do sistema

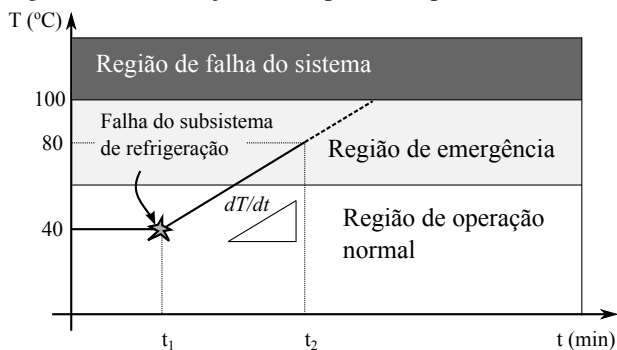
O principal objetivo nesta etapa é descrever o comportamento do sistema em função dos elementos que se encontram nos níveis hierárquicos que estão abaixo, sejam eles componentes ou subsistemas. Para isso, deve-se ter conhecimento da influência de cada componente sobre o sistema, isto é, como a variável de saída do componente afeta o comportamento dinâmico do sistema.

Por exemplo, seja um sistema cuja temperatura deva ser controlada e mantida em torno dos 40°C. A falha do subsistema de refrigeração vai conduzir ao aumento da temperatura. A Figura 4.15 representa o comportamento dinâmico da temperatura do sistema (variável de controle) após a falha, que aumenta gradualmente a uma taxa dT/dt . Assim, na descrição comportamental é preciso que a variação de temperatura do sistema esteja definida em função dos estados do subsistema de refrigeração e dos outros subsistemas que podem agir sobre essa variável de controle.

Basicamente, é preciso identificar os fatores que desencadeiam a mudança da variável de controle e também os fatores que levam a variável de controle a estabilizar em um patamar específico, ou retornar ao ponto de início. Em geral, o início do processo tem origem em falhas nos componentes, ou ação indevida durante a operação, e o patamar de estabilização está associado aos dispositivos de segurança que impedem que a variável de controle atinja valores críticos. A Figura 4.15 apresenta apenas o início do aumento da temperatura, ou seja, ainda seria preciso definir os processos que levariam a temperatura a estabilizar ou retornar ao valor original.

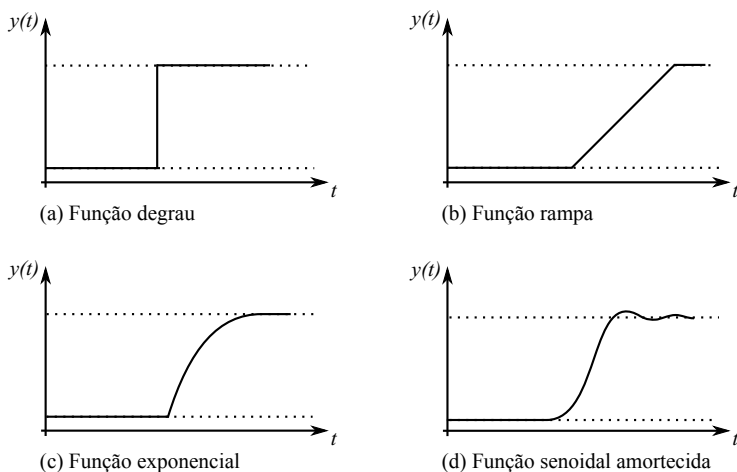
A estrutura funcional do sistema, desenvolvida no projeto conceitual, é uma das principais fontes de informação para esta etapa. Tendo uma estrutura de funções bem documentada é possível relacionar os componentes com as

Figura 4.15 – Variação de temperatura após falha do sistema de refrigeração



funções e avaliar a interferência de cada componente sobre a função global. O comportamento dinâmico do sistema é descrito por uma variável de controle, que é a variável de estado do sistema. A Figura 4.16 apresenta alguns exemplos de funções que podem ser adotadas para representar as mudanças de nível da variável de controle, $y(t)$. Tais mudanças podem estar relacionadas à falha ou reparo de um componente, ação do controlador e ações humanas.

Figura 4.16 – Mudança no nível da variável de controle



- O item (a) da Figura 4.16 ilustra uma mudança instantânea – função degrau – na variável de controle, $y(t)$, sendo utilizada para representar os casos em que as variações são muito rápidas em relação ao tempo.

Por exemplo, a ação de um operador ao ligar uma fonte de energia: o valor parte de zero até o valor nominal de tensão.

- O item (b) da figura ilustra uma mudança que segue uma função do tipo rampa; representa uma variação gradual no valor da variável de controle. Como exemplo, pode-se supor que esteja sendo monitorada a pressão em um reservatório de gás. A falha de um componente (início da rampa) dá início a um aumento gradual da pressão. Ao atingir um certo valor limite, é acionada uma válvula limitadora de pressão, que impede o aumento da pressão – final da rampa.

O comportamento neste caso é regido por uma equação de reta do tipo:

$$y(t) = At + B \quad (4.1)$$

Desta forma é importante definir os parâmetros A e B da Equação 4.1 em função dos estados dos componentes do sistema.

- O item (c) ilustra uma mudança que segue uma função exponencial. Um exemplo clássico para esse comportamento é o processo de carga de um capacitor elétrico. Os sistemas descritos por esse comportamento, na área de controle de sistemas, são denominados de sistemas de primeira ordem e seguem uma equação do tipo:

$$y(t) = (1 - e^{-\frac{t}{\tau}})u(t) \quad (4.2)$$

Os elementos da Equação 4.2 correspondem à variável $u(t)$, que representa uma variável de entrada, e τ , conhecida como constante de tempo – seu valor está relacionado com a velocidade com que ocorre a variação de $y(t)$ no tempo³.

- O item (d) ilustra uma mudança que segue uma função senoidal amortecida. O amortecimento do sistema obedece uma curva exponencial e a oscilação segue os parâmetros definidos pela função senoidal. O sistemas descritos por esse comportamento, na área de controle de sistemas, são denominados de sistemas de segunda ordem e obedecem uma equação do tipo:

$$y(t) = \left[1 - \frac{e}{\sqrt{1 - \xi^2}} e^{-\frac{t}{\tau}} \text{sen}(\omega_d t + \psi) \right] u(t) \quad (4.3)$$

³Quanto menor for o valor de τ , maior a velocidade com que ocorre a variação de $y(t)$ no tempo.

onde,

ξ : razão de amortecimento

ω_n : frequência natural

τ : constante de tempo

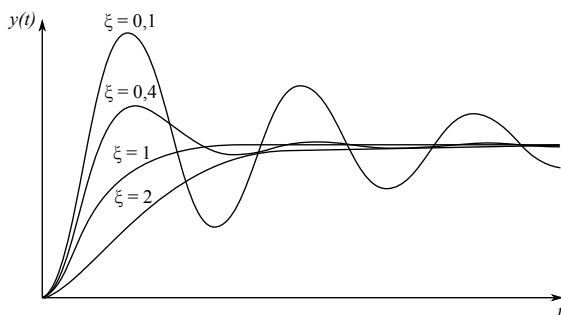
$$\tau = \xi \omega_n$$

$$\omega_a = \omega_n \sqrt{1 - \xi^2}$$

$$\Psi = \arccos(\xi)$$

Dependendo do valor assumido pelo parâmetro ξ , o comportamento da curva pode ficar próximo de um sistema de primeira ordem, ou seja, sem sobressinal. Isso pode ser observado na Figura 4.17, onde é apresentado um gráfico para quatro valores de ξ (0,1 – 0,4 – 1 – 2)⁴. A teoria de controle de sistemas dinâmicos relacionados com modelos de primeira e segunda ordem podem ser encontradas em Franklin et al. (1994) e Ogata et al. (2003).

Figura 4.17 – Comportamento do sistema de segunda ordem em função de ξ



O modelo mecânico clássico de sistema de segunda ordem é representado por massa, mola e amortecedor.

Os itens (c) e (d) são bastante utilizados na análise de sistemas de controle, onde o comportamento durante o transiente possui influência significativa na performance do sistema. Assim, dependendo das características do sistemas que estão sendo modelados, das informações disponíveis e dos requisitos de projeto pode-se considerar os comportamentos descritos pelos itens (a), (b), (c) ou (d).

⁴Quando $\xi = 1$ é denominado sistema com amortecimento crítico. Para $\xi > 1$ é denominado sistema superamortecido e para $0 < \xi < 1$ subamortecido.

Além da variável de controle, muitas vezes os valores de suas derivadas devem ser controlados. Por exemplo, se a variável que estiver sendo monitorada for uma posição “x” de um atuador, dependendo do problema é necessário monitorar a velocidade com que o atuador está se movimentando e também sua aceleração. Para esses casos, estará sendo avaliada mais de uma variável de controle. Assim, a falha do sistema pode ocorrer quando qualquer uma das variáveis alcançar a região de falha do sistema. Consequentemente, à medida que o número de variáveis aumenta, a complexidade da análise também aumenta.

A falha do sistema técnico fica caracterizada quando a variável de estado alcançar a região de falha. Por outro lado, o sucesso da missão fica caracterizado quando o tempo de simulação atinge o tempo de missão sem que a variável de controle alcance a região de falha.

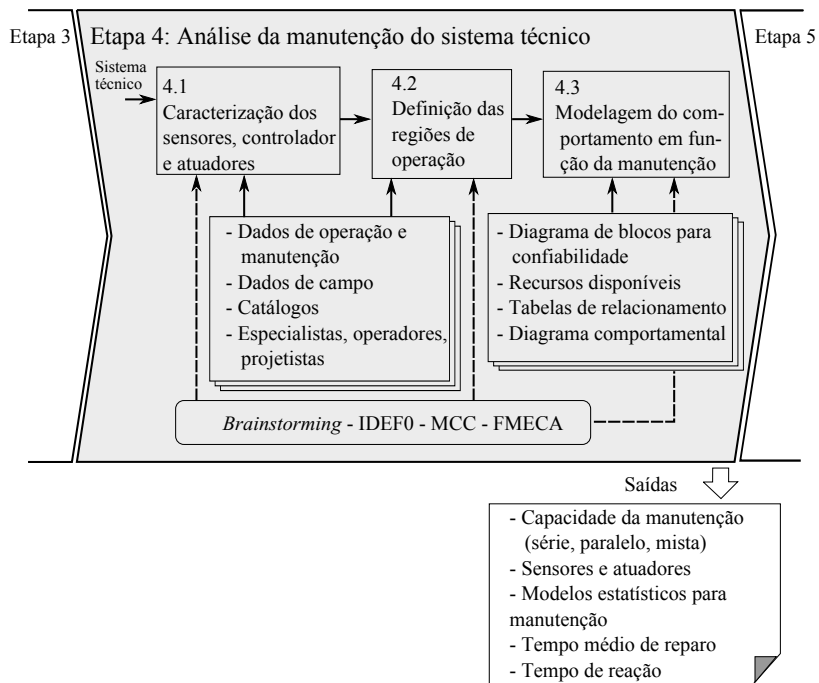
4.7 ETAPA 4: ANÁLISE DA MANUTENÇÃO DO SISTEMA TÉCNICO

Nesta etapa, Figura 4.18, a manutenção centrada em confiabilidade (MCC) é a principal técnica de suporte a ser utilizada. Serão obtidas informações como tempo médio de reparo dos componentes, modelo estatístico das ações de manutenção (função densidade de reparo), sensores que detectam a falha, valores limites da variável de controle, priorização das ações de manutenção, manutenção em série e paralelo, recursos (equipamentos e mão de obra) disponíveis, etc.

Durante as reuniões, as técnicas *Brainstorming*, IDEF0 e FMECA irão auxiliar fornecendo informações como funções, processos e componentes mais críticos do sistema; histórico de falhas; procedimentos de operação e manutenção; entre outras. A Figura 4.18 apresenta as atividades realizadas na etapa de análise da manutenção do sistema:

- Atividade 4.1: Caracterização dos sensores, controlador e atuadores
- Atividade 4.2: Definição das regiões de operação
- Atividade 4.3: Modelagem do comportamento em função da manutenção

Figura 4.18 – Atividades da etapa 4



4.7.1 Atividade 4.1: Caracterização dos sensores, controlador e atuadores

Os sensores são os elementos que irão monitorar a variável de controle constantemente. A partir do momento que ocorre uma falha, o comportamento dinâmico do sistema faz com que a variável deixe a região de operação normal.

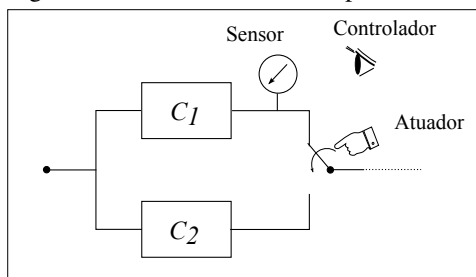
A detecção de que o valor está fora da região normal é percebida por um controlador, que faz a leitura do sensor e dependendo da informação obtida, dispara ações para os atuadores. Portanto, é preciso definir quais são os elementos do sistema que operam como sensores, os limites em que fica caracterizado que o comportamento está fora do normal, o controlador e os atuadores.

A partir do momento que o sensor indica que a variável de controle está fora da região de operação, o controlador faz o acionamento dos atuadores, que são os elementos responsáveis em impedir que a variável atinja os limites

críticos que determinam a falha total do sistema.

Para ilustrar melhor estes conceitos é apresentado um exemplo, Figura 4.19. O sistema é constituído de dois componentes, C_1 e C_2 ligados em paralelo, e um medidor para obter a saída do componente C_1 .

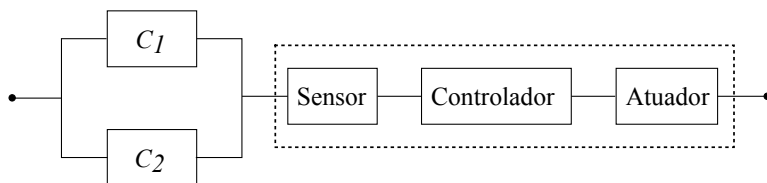
Figura 4.19 – Sistema com componentes C_1 e C_2 (reserva)



Supondo que em um dado momento, o medidor instalado junto ao componente C_1 indica que o sinal fornecido está abaixo de um valor limite. Ao perceber a informação, o controlador aciona o atuador que realiza a comutação para o componente C_2 , que é o componente reserva. O sensor deste sistema é composto pelo medidor, o controlador e atuador são representados pelo operador, que deve visualizar no medidor que o sinal está baixo e realizar a comutação para o componente reserva.

Embora o sistema apresentado no exemplo possua um componente reserva, a ação de recuperar o sistema ainda pode falhar, pela probabilidade de falha do sensor, do controlador ou do atuador. Uma análise de confiabilidade pode ser desenvolvida com o uso de diagramas de blocos para confiabilidade, como apresentado na Figura 4.20. O sensor, controlador e o atuador podem entrar como componentes montados em série, visto que a falha de qualquer um deles pode conduzir a falha no sistema.

Figura 4.20 – Diagrama de blocos para confiabilidade com sensor, controlador e atuador



Um caso simples como no exemplo citado, pode gerar várias análises

e soluções. Esse tipo de problema, é bastante aderente à análise de confiabilidade dinâmica, onde é possível simular vários cenários⁵. Geralmente, na análises de confiabilidade estática, o conjunto (sensor, controlador e atuador) é considerado perfeito, ou seja, nenhum dos três elementos falha – portanto, não entram na representação dos diagramas de blocos para a confiabilidade.

Na análise de confiabilidade dinâmica os sensores, o controlador e os atuadores são itens importantes, pois são necessários para a representação do comportamento dinâmico do sistema. Assim, mesmo se forem considerados perfeitos, ainda devem estar presentes nos modelos para realizar mudanças de estados nos componentes para impedir a falha do sistema. Além disso, mesmo considerando que não falhem, suas características como o valor definido para acionamento, tempo de resposta (para leitura do controlador e acionamento dos atuadores), entre outras, irão influenciar na confiabilidade do sistema.

Caso os sensores, controlador e atuadores forem suscetíveis à falhas, será preciso ter uma função densidade de falha que represente o sensor e o atuador, bem como os seus possíveis estados – análogo aos estados definidos para os componentes.

Deve-se salientar que um sensor, no contexto deste trabalho, não tem função somente de realizar a leitura da variável de controle. Além disso, deve apresentar a informação para que seja interpretada pelo controlador e com isso sejam tomadas ações para evitar a falha.

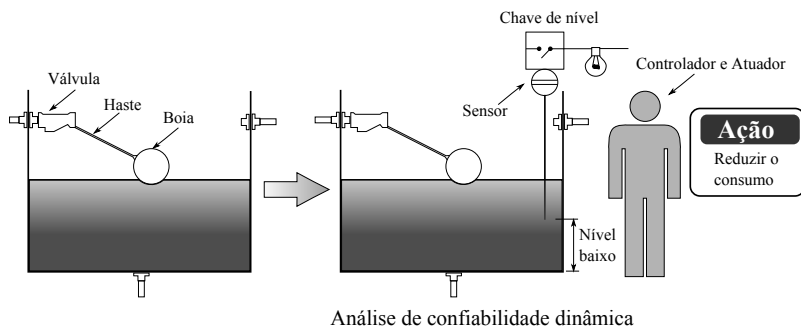
Assim, considere o exemplo apresentado na Figura 4.21. O sistema pode ser caracterizado como um sistema dinâmico no qual a variável de controle que está sendo monitorada é o nível do reservatório. Pode-se pensar inicialmente que a boia é um sensor/controlador e a haste acoplada à válvula é o atuador. Na medida que o nível de líquido baixa, a boia faz o papel de sensor e controlador porque faz a leitura e aciona a válvula por meio da haste.

No entanto, do ponto de vista da análise de confiabilidade dinâmica, se for considerado que a falha do sistema é quando ocorre o esvaziamento do reservatório, então, para realizar a análise deve-se incluir um elemento que, por exemplo, quando o nível do reservatório chegar em 50%, um alerta é emitido informando a situação. O controlador, de posse dessa informação comanda uma ação de atuação – redução do consumo –. Para esse caso, a função do controlador e atuador estão representados pelo homem, que com a informação que o nível está baixo e toma a ação de reduzir o consumo.

Embora a boia, a haste e a válvula sejam elementos que fazem parte do sistema que controla o enchimento do reservatório, estes não podem ser

⁵Poderia ser simulado um sensor com falha oculta, ou seja, está travado em uma posição de leitura. Ou ainda, simular a ação do operador cujo tempo de reação segue uma dada distribuição de probabilidade – nesse caso seria avaliado a confiabilidade do sistema em função do tempo de reação do operador.

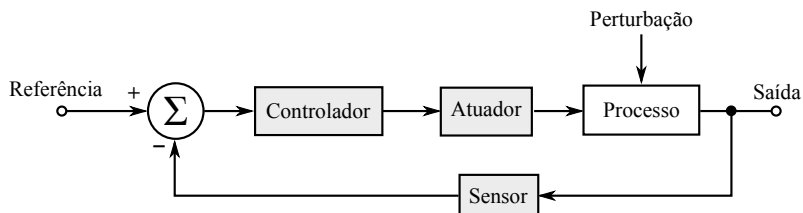
Figura 4.21 – Exemplo de análise de sistema a partir do controle do nível de fluido do reservatório



caracterizados como sensor, controlador e atuador. As taxas de falha destes elementos entram na análise e terão impacto na confiabilidade do sistema, mas participam da modelagem somente como componentes do sistema.

O sensor, o controlador e o atuador são elementos que estão presentes nas teorias de controle clássico. A Figura 4.22 apresenta um diagrama de blocos para análise de um sistema de controle realimentado (também denominado de sistema em malha fechada) em que é possível observar a disposição dos três elementos. O sensor faz a leitura da saída do processo e se houver diferença com o valor de referência do sistema, o controlador – por meio do atuador – toma ações sobre o processo para manter a variável nos limites estabelecidos no projeto. As perturbações são interferências externas que agem sobre o processo e podem afastar o valor de saída do sistema do valor de referência.

Figura 4.22 – Diagrama de blocos para análise de um sistema de controle realimentado



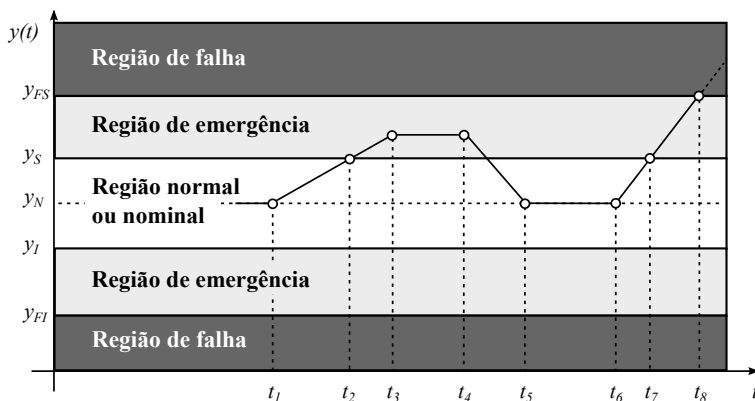
Fonte: Adaptado de Ogata et al. (2003)

4.7.2 Atividade 4.2: Definição das regiões de operação

A atividade de definição dos limites de operação consiste em definir os valores que caracterizam: a falha do sistema, a condição de emergência e a operação normal.

No exemplo apresentado na Figura 4.21, a condição considerada normal seria do nível 50% até o reservatório cheio (100%). A condição de emergência seria para valores abaixo dos 50% e falha quando estivesse vazio. A atividade de definição dos limites está relacionada diretamente com a caracterização dos sensores e atuadores. Ou seja, durante a definição dos sensores e atuadores, naturalmente se inicia a definição dos limites de operação.

Figura 4.23 – Regiões de operação do sistema



A Figura 4.23 apresenta um gráfico que representa o comportamento dinâmico de uma variável de controle, $y(t)$. A figura representa um caso genérico que será utilizada para explicar como cada ponto pode migrar para cada uma das regiões:

- Condição normal de operação: Nesse caso, variável de controle $y(t)$, opera dentro de um limite superior, y_S , e um limite inferior, y_I . O valor y_N é um valor de referência que representa o valor nominal de projeto. Desta forma, os pontos identificados no tempo t_1 , t_5 e t_6 , representam o sistema na condição normal de operação.
- Condição de emergência: O sistema avança para a região de emergência quando ocorre falha em um ou mais componentes. No momento que a variável de controle atinge os limites da condição normal (y_S ou y_I), o

sensor envia uma informação ao controlador de que, pelo menos, um componente está em falha. Os pontos que se encontram no tempo t_2 , t_3 , t_4 , t_7 e t_8 são condições em que um alerta está sendo emitido e que ações são necessárias para recuperar o sistema.

A saída da condição normal e o ingresso para a região de emergência está associado com a taxa de falha de um ou mais itens do sistema e como os seus estados influenciam a variável de controle. Desta forma, quanto maior for a taxa de falha dos componentes, maior será a frequência com que ocorrerá esta passagem.

- Falha do sistema: O sistema falha quando o valor da variável de controle atinge o limite superior, y_{FS} , ou o limite inferior, y_{FI} . A ocorrência de falha do sistema vai depender da velocidade com que a variável de controle avança para a região de falha e também da qualidade dos sensores, do controle e dos atuadores. A qualidade destes elementos está relacionada com os equipamentos de proteção, a capacitação da equipe de manutenção, os programas de manutenção, entre outros pontos que são abordados pela manutenção centrada em confiabilidade.

Assim, as chances do sistema migrar da região de emergência para a região de falha estão associadas com os tempos para as ações de manutenção, mão de obra da equipe e recursos disponíveis para instalação de barreiras (proteções). Estas ações quando não puderem trazer o sistema para a condição normal, devem pelo menos reduzir a velocidade de avanço da variável de controle do sistema, a fim de que possa ser feita a manutenção e impedir que se atinja a região de falha.

4.7.3 Atividade 4.3: Modelagem do comportamento em função da manutenção

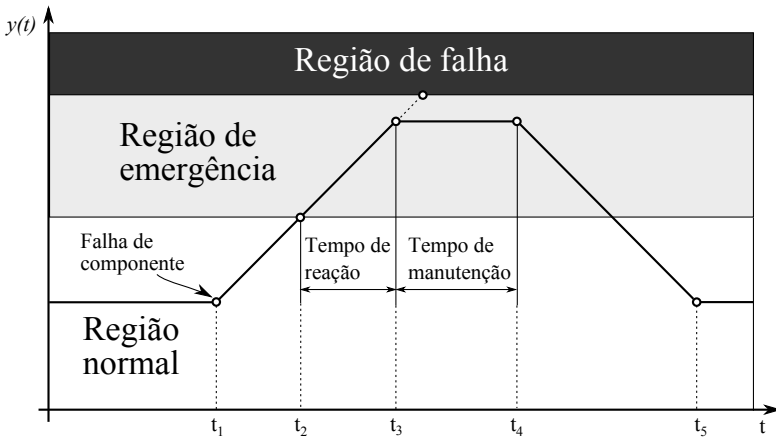
Os possíveis estados dos componentes, e portanto, das falhas foram definidas na atividade 3.2 (Caracterização dos componentes). A atividade a ser realizada nesta etapa se resume em caracterizar como as ações de detecção e manutenção influenciam a variável de controle, e portanto, a confiabilidade do sistema. As informações advindas da manutenção centrada em confiabilidade (MCC) são fundamentais nesta etapa, pois estão fortemente relacionadas com o procedimentos de manutenção, tempos de reparo, equipamentos de suporte disponíveis, mão de obra, etc.

4.7.3.1 Tempo de reação

A partir do momento que a variável de controle alcança a região de emergência, o sensor informa a situação ao controlador. O período de tempo entre o momento de entrada na região de emergência até o início do procedimento de manutenção é denominado de tempo de reação.

A Figura 4.24 apresenta uma variável de controle, $y(t)$, que após a falha de um componente no tempo t_1 , alcança a região de emergência no tempo t_2 ; nesse momento o sensor informa o estado da variável $y(t)$ para o controlador. Após um dado tempo – tempo de reação – entra em operação um atuador que interrompe o avanço da variável de controle em direção à falha do sistema.

Figura 4.24 – Tempo de reação para início da manutenção preditiva



Dependendo da complexidade do sistema, do tipo de falha e dos controles disponíveis, o tempo de reação implementado no modelo pode ser nulo ou ser tão longo que não há tempo para o controlador acionar os atuadores, consequentemente ocorrerá a falha do sistema.

O tempo de reação pode ser determinístico ou estocástico:

- Caso seja determinístico, é preciso ter a função que descreve o tempo de reação para computar o início da manutenção. Essa função pode ser dependente do componente, da equipe de manutenção, da variável de controle, entre outros elementos.
- Caso seja estocástico, deve-se informar a função densidade que descreve o tempo para que possa realizar o sorteio e obter o valor do tempo de

reação. Quanto maior for o tempo de reação, maiores são os riscos do sistema falhar. O tempo de reação está relacionado com os dispositivos de sinalização dos sensores e com a capacitação da equipe de manutenção.

Nessa atividade, é muito importante a presença de especialistas no sistema, como os projetistas, pessoal de operação e manutenção, que irão dar informações para construir a função ou fornecer o modelo estatístico que descreve o tempo de reação.

4.7.3.2 Atuação sobre o avanço da variável de controle

Antes de iniciar a manutenção de algum componente, alguns sistemas possuem elementos que fazem o bloqueio da variável de controle, impedindo o avanço em direção à região de falha do sistema. Paralelamente, são iniciadas as ações para detecção das falhas e manutenção preditiva dos componentes.

Deve-se buscar mecanismos que façam o bloqueio, principalmente, quando a mudança da variável de controle é considerada rápida em relação às ações de manutenção. Por outro lado, se a mudança da variável de controle é bastante lenta, pode-se buscar a manutenção direta dos componentes. Mas além da taxa de variação, deve-se levar em consideração os recursos disponíveis (equipamentos, mão de obra, etc), os possíveis efeitos que a falha pode gerar, a probabilidade de detecção e recuperação dos componentes em falha, entre outros fatores.

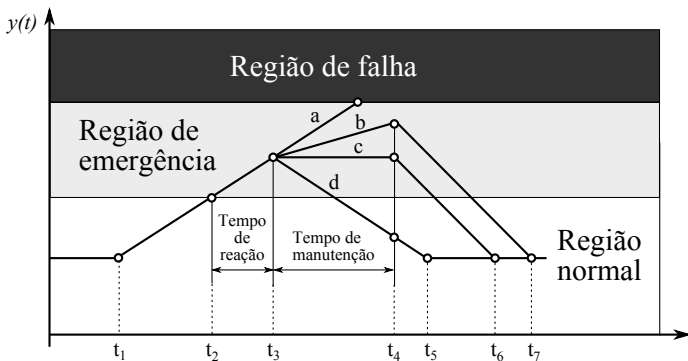
Na Figura 4.25, após o tempo de reação do sistema de controle, são apresentados quatro caminhos de manutenção preditiva para a variável $y(t)$ identificadas por “a”, “b”, “c” e “d”:

- No caminho “a” não foi realizada nenhuma ação sobre a variável. Embora, as ações de manutenção já tivessem iniciado – no tempo t_3 – não foi possível impedir a falha do sistema.
- No caminho “b” foi feita uma ação sobre o sistema que permitiu uma queda no comportamento dy/dt , que foi suficiente para que a manutenção do sistema fosse concluída e levasse o sistema a retornar para as condições normais de operação em t_6 . Todavia, nesse caso uma demora maior na manutenção do sistema ainda poderá conduzi-lo a falha.
- No caminho “c” o avanço da variável foi totalmente interrompido. Em relação aos casos “a” e “b”, essa situação é a mais favorável, visto que o sistema já não avança em direção à falha. Consequentemente, o trabalho da equipe de manutenção é realizado sob uma pressão um pouco menor

nesse caso. No entanto, vale chamar a atenção que ainda é uma situação crítica, pois no caso de alguma nova falha, o tempo disponível para qualquer ação é bem menor, tendo em vista a proximidade com os limites da região de emergência com a região de falha.

- No caminho “d” foi realizada uma ação que permitiu a variável retornar para a região de operação normal. Isso pode ocorrer, por exemplo, para os sistemas que possuem componentes redundantes. Assim, dado que ocorreu uma falha no componente principal, ao ser detectada esta condição, é realizada a comutação para o componente reserva, que recupera o sistema. Paralelamente, pode ser realizada a manutenção do componente em falha, que após o reparo pode entrar em operação novamente, ou ficar na condição de reserva.

Figura 4.25 – Atuação sobre o avanço da variável de controle



Assim a análise de confiabilidade procura caracterizar os cenários a partir da dinâmica das falhas dos itens, dos estados de falha do sistema e do tempo de reação da manutenção, como forma de sistematizar barreiras para impedir ou reduzir o avanço para a região de falha. Tais proteções, junto com as ações de manutenção aumentam as chances de recuperação do sistema, e consequentemente, a confiabilidade.

4.7.3.3 Manutenção preditiva com o sistema em operação

Como visto no capítulo de revisão, a gestão da MCC está estruturada para agir na forma de: manutenção corretiva e manutenção preventiva, baseada no tempo ou baseada na condição. Um problema crítico para sistemas

dinâmicos está associado às falhas ocultas. É nestes casos que a análise de confiabilidade dinâmica é mais apropriado, e para que não haja perda de continuidade a manutenção é feita com o sistema em operação, sinalizada de forma preditiva.

Em alguns instantes do ciclo de vida dos sistemas serão detectadas falhas em mais de um item. Isso pode ser mais crítico se existirem falhas ocultas no sistema. No momento em que componentes com falha oculta recebem uma solicitação para mudança de estado (de ligado para desligado, ou de desligado para ligado), as falhas deixam de ser ocultas. Essas não conformidades fazem o sistema operar em condições desfavoráveis, conseqüentemente, as variáveis de estado do sistema irão ultrapassar os limites de segurança, tendendo o sistema a ir para uma condição de falha. A existência de dois ou mais componentes em falha torna a situação mais complicada do ponto de vista da manutenção. Para esses casos, pergunta-se: em quais componentes se deve iniciar a manutenção?

A resposta para a pergunta vai depender dos recursos disponíveis, da função e tempo de reparo de cada componente, entre outros fatores. O que se quer é manter o sistema operando, mesmo que se detectou a falha de um componente. As prioridades definidas pela organização estão nas informações geradas pela MCC e nela estará definido o tipo de manutenção do sistema, que pode ser em série, em paralelo, misto ou sem manutenção. Vale ressaltar que a manutenção do componente é realizada com o sistema em operação – sem desligar o equipamento –. Assim, a manutenção deve ser executada de forma mais rápida possível para que a variável de controle retorne à sua faixa de operação, afastando-se dos limites máximos ou mínimos que poderiam levar à falha do sistema.

As seções seguintes apresentam as possíveis modelagens para conduzir a manutenção de conjuntos de componentes que estão em falha, que são:

- Manutenção em série

- Manutenção em paralelo

- Manutenção mista

- Sem manutenção

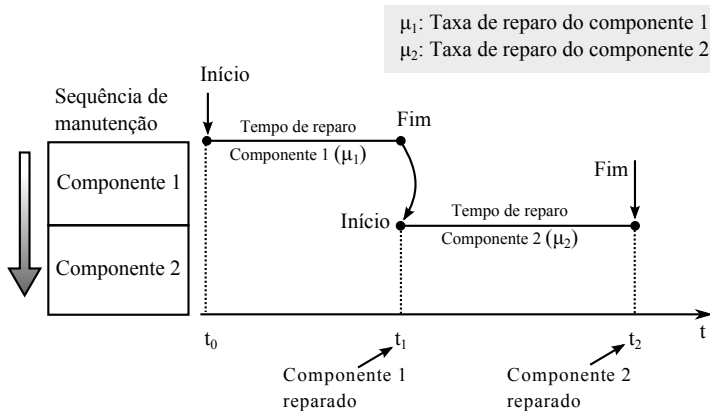
A caracterização das modelagens de manutenção é muito importante para a análise de confiabilidade dinâmica do sistema técnico, principalmente quanto ao comportamento dinâmico do sistema após as falhas nos componentes.

4.7.3.3.1 Modelagem em série da manutenção

Na manutenção em série os reparos serão realizados em um componente de cada vez. Consequentemente é um processo mais lento. A maneira como é conduzida a manutenção dos componentes terá um impacto direto no valor da confiabilidade do sistema, pois se o sistema de manutenção é mais eficiente, é possível trazê-lo para a condição normal mais rapidamente, evitando assim que os valores limites que caracterizam as falhas sejam alcançados.

A Figura 4.26 representa graficamente a manutenção em dois componentes. A manutenção do componente 1 inicia em t_0 e termina em t_1 . A manutenção do componente 2 tem início somente depois da manutenção do componente 1 em t_1 , finalizando em t_2 .

Figura 4.26 – Manutenção em série



Na manutenção em série deve-se especificar a ordem com que será realizada a manutenção, cuja sequência foi definida em função das taxas de reparo, ou taxas de falha, ou grau de influência do componente sobre a variável de estado do sistema, ou custo de manutenção do componente etc.

Esta modelagem ocorre para itens dependentes na estrutura funcional e é feita das decisões de projeto.

4.7.3.3.2 Modelagem em paralelo da manutenção

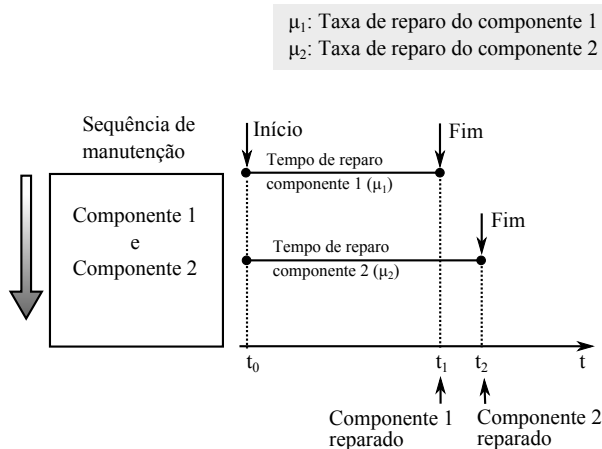
Na manutenção em paralelo o tempo para o início da manutenção é igual, diferindo-se na finalização para cada componente.

Após a manutenção, tanto em série quanto em paralelo, pode-se especi-

ficar um coeficiente de degradação do componente que irá atuar na sua taxa de falha. Ou pode-se considerar o componente recuperado tão bom quanto novo, neste caso não há degradação do componente.

Na Figura 4.27 estão dois componentes sendo reparados em paralelo. Neste tipo de manutenção, os componentes iniciam a manutenção no mesmo tempo, t_0 . No tempo t_1 finaliza-se a manutenção do componente 1 e do componente 2 em t_2 .

Figura 4.27 – Manutenção em paralelo



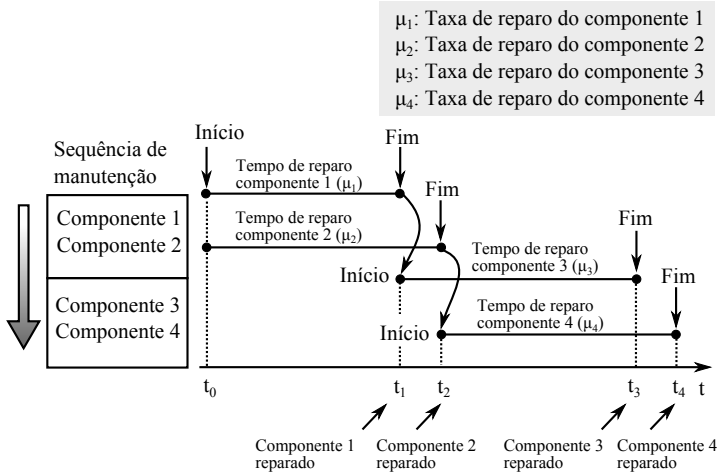
Verifica-se que há uma sobreposição nos processos de manutenção, conseqüentemente, tem-se todos os componentes que estavam em falha sendo reparados, o que implica em tempo menor de reparo do sistema, quando comparados com a manutenção em série.

4.7.3.3 Modelagem mista da manutenção

Na modelagem da manutenção mista combina-se a manutenção em série e paralelo. Nesta manutenção, grupos de componentes são reparados em série. Dentro de cada grupo a manutenção é realizada em paralelo. A Figura 4.28 apresenta um exemplo em que quatro componentes estão em falha: componentes 1, 2, 3 e 4.

A manutenção inicia com os componentes 1 e 2. Dado que a manutenção de um dos componentes foi concluída (componente 1), inicia-se a manutenção do componente do segundo grupo, que é o componente 3. Assim, pode-se concluir que a capacidade de manutenção deste sistema é de dois

Figura 4.28 – Manutenção mista



componentes por vez. Na existência de mais componentes em falha, estes ficam em espera.

Ou seja, a manutenção em série seria um caso particular em que cada grupo é constituído por apenas um componente. Em contrapartida, a manutenção em paralelo seria também um caso particular em que é composto por um único conjunto composto por todos os componentes.

4.7.3.3.4 Modelagem sem manutenção

Alguns sistemas não permitem que a manutenção seja realizada com o sistema em operação. Mas para evitar a parada do sistema, possuem mecanismos, ou barreiras, para impedir ou mitigar a progressão da variável de controle. Com isso, conseguem interromper o avanço da variável em direção à região de falha, ou retardar o avanço, para que medidas que reduzam o impacto dos efeitos sejam tomadas.

Vale destacar que, mesmo que os componentes não sejam reparáveis ainda necessitam de sensores, controladores e atuadores para fazerem a predição.

4.7.3.4 Falhas ocultas

A falha oculta irá ocorrer sempre que o tipo de falha, aberta ou fechada, coincidir com o estado de operação exigido pelo sistema. Por exemplo, considere que uma válvula de alívio, na sua operação normal, deva permanecer fechada. Em um dado tempo, por algum problema, a válvula permanece trancada na posição fechada – se a função da válvula não for exigida e ela está trancada, tem-se o caso de uma falha oculta. A sua condição de falha só será percebida quando o sistema necessitar que a válvula mude de estado para aberta.

Durante a simulação, para a determinação da confiabilidade dinâmica do sistema é possível identificar e registrar os componentes com falha oculta e também o momento da ocorrência. Com o número de ocorrências e tempo, é possível obter uma função densidade de probabilidade para falhas ocultas. Esta informação obtida das simulações, pode ser usada pelo mantenedor para organizar seu cronograma de inspeções dos componentes de acordo com o período mais provável que as falhas irão ocorrer, a fim de identificar tais falhas no sistema real e evitar surgimento de problemas durante a demanda de operação.

4.8 ETAPA 5: MODELAGEM E SIMULAÇÃO

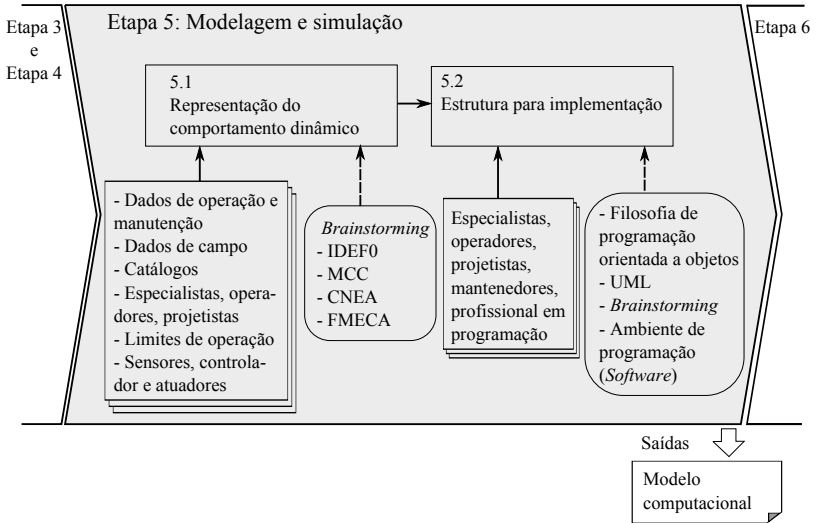
As informações obtidas nas etapas 3 e 4 são utilizadas para a modelagem e simulação computacional do sistema técnico. A Figura 4.29 apresenta as atividades realizadas nesta etapa.

4.8.1 Atividade 5.1: Representação do comportamento dinâmico do sistema

O comportamento dinâmico do sistema é descrito pelas variáveis de estado, y , que indicam valores, quantidades ou condições que são utilizados em um processo – servem para controlar, modificar ou supervisionar. Temperatura, pressão, densidade, concentração e peso são efeitos cujas de variáveis podem ser monitoradas para disparar alarmes – quando o sistema ultrapassa o limite de sua condição normal de operação –, ou caracterizar a falha do sistema. Assim, deve-se estabelecer os valores limites: faixa normal de operação, valores máximos e mínimos que definirão a falha do sistema.

A Equação 2.1, dy/dt , apresentada no capítulo 2, mostra que ocorrerão

Figura 4.29 – Atividades da etapa 5



variações devido aos estados dos componentes i e suas propriedades⁶, ao tempo t e também pela própria variável y .

Assim, deve-se escrever como os componentes influenciam na variável de controle do sistema. Para implementação computacional recomenda-se inicialmente modelar os gráficos que representem o comportamento dinâmico ao longo do tempo, para adquirir sensibilidade da análise.

A Figura 4.30 é um exemplo de simulação onde é possível acompanhar o comportamento dinâmico do sistema diante à ocorrência de falhas. A figura foi elaborada considerando um sistema com dois componentes C1 e C2 ligados em paralelo, no qual o primeiro é o componente principal e o segundo é o reserva (redundante).

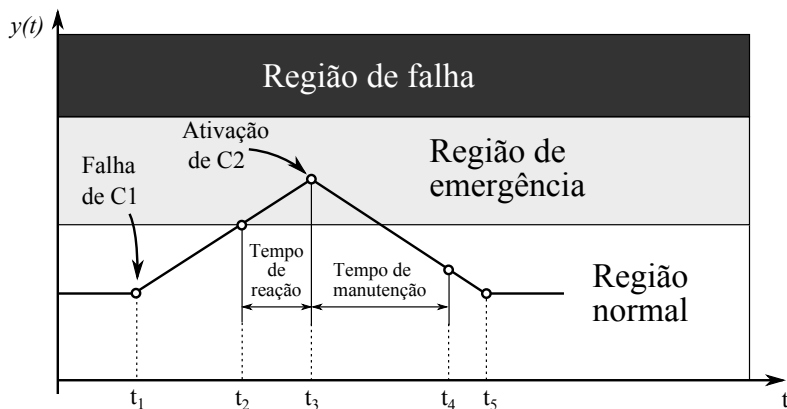
Inicialmente um componente C1 tem uma falha no tempo t_1 . Quando o sistema ultrapassa o limite da região normal, no tempo t_2 , o sensor envia a informação ao controlador. Após o tempo de reação em t_3 , o atuador faz a comutação, ativando o componente C2. Com isso, o sistema consegue trazer a variável $y(t)$ para a região normal de operação em t_5 . A manutenção do componente C1 é concluída no tempo t_4 .

À medida que os componentes são reparados, seus estados são alterados e sorteios de novos tempo de falha e de reparo são realizados.

Diagramas que mostram o comportamento do sistema são muito im-

⁶Taxas de falha, taxa de reparo, condições de operação etc

Figura 4.30 – Exemplo de simulação realizada manualmente



portantes para a orientação na implementação computacional e também para a equipe que está trabalhando no problema. Nessa atividade, são revisados os limites de condição normal de operação e quando a falha no sistema ocorre. Também verifica-se as ações do controlador sobre os atuadores, os componentes e analisa-se as políticas de manutenção do sistema.

4.8.2 Atividade 5.2: Estrutura para implementação

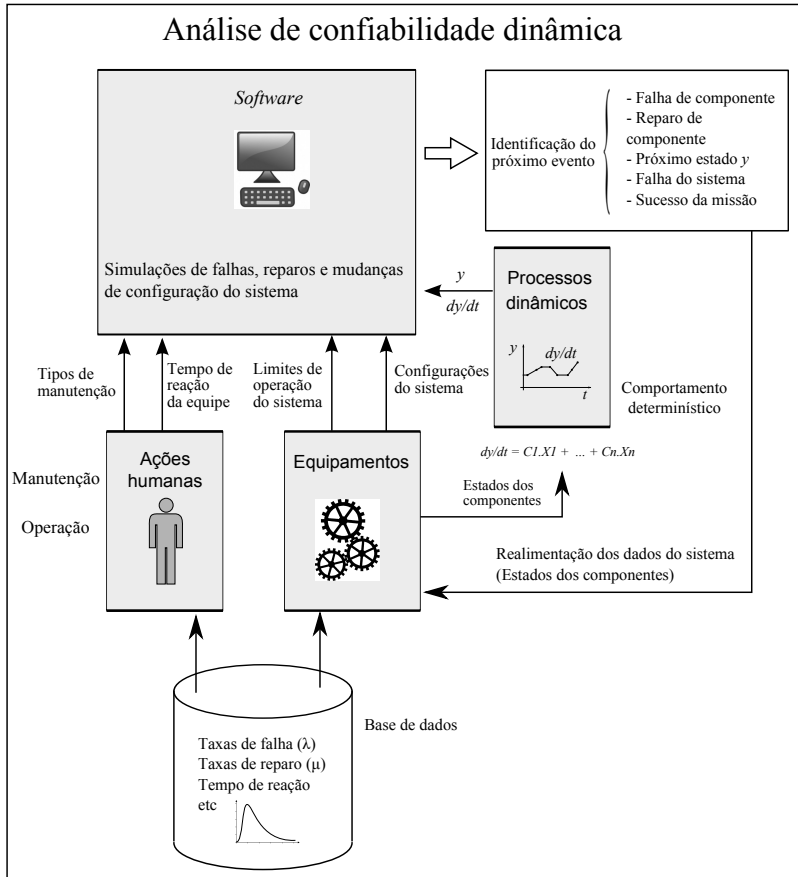
A implementação computacional de uma análise de confiabilidade dinâmica pode ser estruturada com os seguintes elementos: sistema, componentes, controlador e manutenção. A comunicação entre os elementos está apresentada na Figura 4.31.

O elemento principal do sistema é o controlador, que concentra todas as informações vindas do sistema e ações de manutenção. Na Figura 4.31, o controlador é representado pelo *software*, tendo como função identificar quais os próximos eventos que irão ocorrer no sistema, que podem ser: falha ou reparo de componente, falha do sistema ou sucesso da missão, próximo estado da variável de controle.

O comportamento dinâmico da variável de controle, y , é regido pelos comandos do controlador (*software*) sobre os atuadores que agem sobre os componentes, pelas respostas do sistema e falhas/reparos dos componentes.

O comportamento aleatório está vinculado às taxas de falha e de reparo. Para cada componente são sorteados o tempo da próxima falha, tipo de falha e o tempo gasto com a manutenção. No momento que o tempo “ t ” de simulação

Figura 4.31 – Representação do fluxo de informação do *software*



coincide com o tempo de falha ou de reparo, o componente muda de estado.

O comportamento determinístico é ditado pela equação do sistema que relaciona os estados dos componentes com a variável de controle. Dado que ocorreu uma falha, se não for oculta, o estado do componente irá mudar passando de aberto para fechado ou de fechado para aberto, influenciando diretamente os valores da variável de controle ao longo do tempo.

Portanto, o comportamento da variável de controle possui uma parcela determinística e outra estocástica. Considera-se determinística porque depende dos estados dos componentes que são alterados pelo controlador e estocástica porque a ocorrência da falha e o tempo gasto com a manutenção possuem comportamento aleatório.

4.8.2.1 Diagrama de fluxo do *software*

A Figura 4.32 apresenta o fluxograma para auxiliar na implementação computacional, sendo recomendado o uso de linguagem orientada a objetos, ou que possam utilizar variáveis do tipo estrutura onde seja possível armazenar vários tipos de informações em um mesmo elemento. Desta maneira, torna-se mais fácil a implementação e mudanças futuras, seja acrescentando outros componentes ou mudando o valor de suas variáveis.

O fluxograma representa que a rotina será executada em um número de “ n ciclos” de simulação, definido pela variável n_{ciclos} . Cada ciclo representa um teste cujo resultado pode ser uma falha do sistema – em um tempo – ou sucesso da missão. O conjunto de n ciclos é usado para construir um único histograma de falhas do sistema. Desta forma, se na entrada de dados da análise for estipulado “ k ” histogramas, o fluxograma apresentado se repetirá um número de “ k ” vezes.

Desta forma, este ciclo deve ser repetido exaustivamente. Na Figura 4.32 a variável que representa os milhares de ciclos está nomeada como n_{ciclos} . Nas aplicações realizadas neste trabalho, foram realizadas 10^4 ciclos para a construção de cada histograma. Portanto, o algoritmo deve estar dentro de um laço de repetição, para a construção de vários histogramas de falhas, permitindo assim analisar a dispersão dos resultados dos histogramas.

Cada um dos blocos apresentados na Figura 4.32 possui rotinas de programação associadas. Algumas das rotinas podem depender do tempo, $f(t)$, da variável de estado do sistema, $f(y)$, e do estado dos componentes, $f(componentes)$.

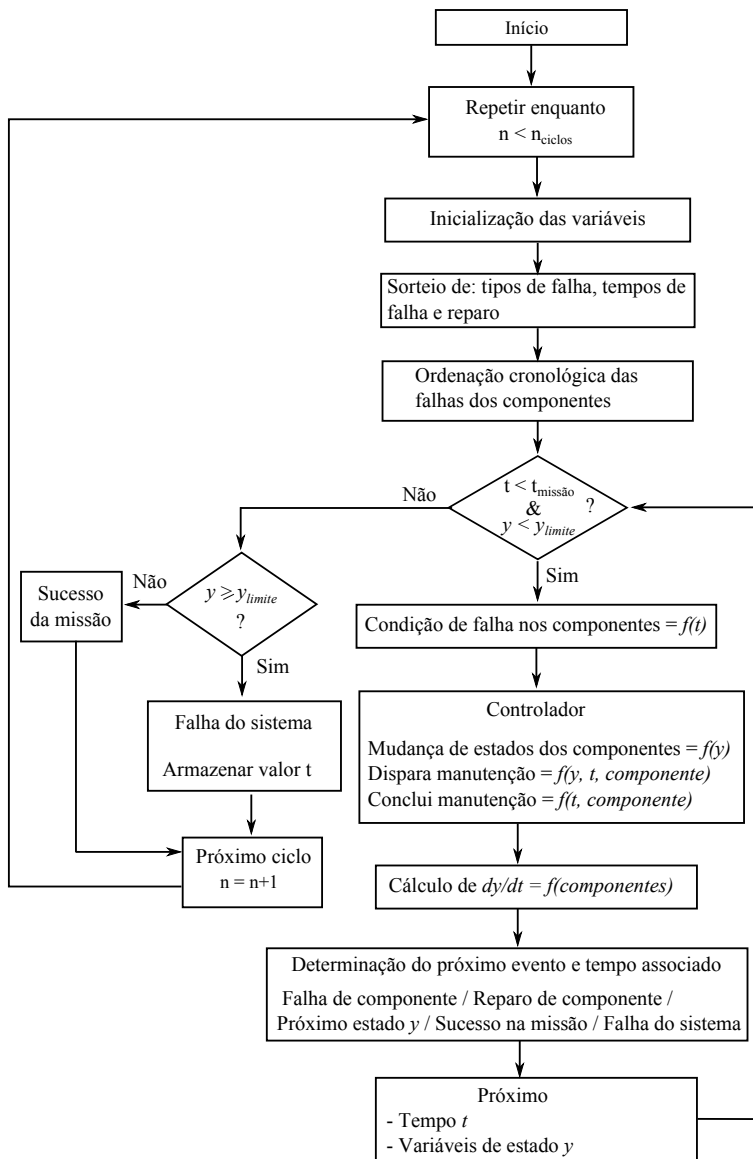
Nas seções seguintes serão descritos os principais pontos da Figura 4.32 para a implementação computacional.

4.8.2.2 Inicialização das variáveis

A primeira rotina para implementação computacional é a inicialização das variáveis. É preciso estabelecer as condições iniciais das variáveis utilizadas na simulação. Ou seja, o sistema deve ter os estados dos componentes, dos sensores, da variável de controle e de suas derivadas definidas para um tempo inicial $t_0 = 0$.

Os estados dos componentes, sensores e variável de controle devem receber valores iniciais que representem as condições normais de operação. Desta forma, no tempo $t_0 = 0$ o sistema não apresenta falhas, a variável de controle se encontra no valor nominal de projeto, os sensores indicam condição normal, os componentes principais ativados e os redundantes desativados.

Figura 4.32 – Fluxograma para desenvolvimento do *software*



Nas seções seguintes é apresentada uma sugestão para criação das variáveis sistema e componentes.

4.8.2.2.1 Armazenamento dos dados do sistema

Ao longo da simulação a variável sistema deve trocar diversas informações com o controlador para ativar/desativar a manutenção e ligar/desligar componentes. Os itens apresentados a seguir são informações que podem ser armazenadas na variável sistema e servem para a orientação na implementação computacional.

- Próximo evento e o tempo em que irá ocorrer.

Esta informação será proveniente do controlador que, com as informações do sistema e manutenção poderá inferir qual será o próximo evento e quando irá ocorrer. Como o controlador é responsável por ler os sensores e comandar os atuadores, processar os dados, esta informação será armazenada dentro da variável sistema para que não se perca.

- Componente que está sendo reparado.
- Tipo de manutenção adotado: série, paralelo, mista ou sem manutenção.
- Sequência de manutenção de componentes.

Se for escolhida a manutenção em série deve-se ter a priorização com que a manutenção será executada nos componentes. Caso a manutenção do sistema seja do tipo mista, deve-se ter a priorização dentro de cada grupo de componentes.

- Tempo de reação.

Tempo intermediário entre o momento em que a variável de controle y entra na região de emergência e o início da manutenção de componente. Em algumas aplicações o tempo de reação pode ser considerado nulo, como por exemplo, em sistemas que executam a comutação automática entre o componente principal e reserva.

- Tempo de início da manutenção.

Tempo que começa a ser contado a partir do tempo de reação.

- Tempo final da manutenção.
- Estado do alarme: ligado ou desligado.

O alarme fica ligado quando a variável de controle se encontra na região de emergência e é desligado quando não há mais falhas e a variável de controle retorna para o seu valor nominal.

- Região de emergência.

Valores limites da variável de controle que informam ao controlador que o sistema está fora da condição normal. Nesses casos, após o tempo de reação, o controlador comanda os atuadores para o início da manutenção de componentes.

- Região de falha.

Valores limites da variável de controle que caracterizam a falha do sistema. Quando o sistema atinge esses valores é feito o registro do tipo de falha e o momento em que ocorreu.

4.8.2.2.2 Armazenamento dos dados dos componentes

Em relação ao componente, este pode armazenar as seguintes informações:

- Nome do componente.
- Estado operacional: o componente pode estar ligado ou desligado.
- Último comando recebido pelo controlador: pode ser ligado ou desligado.
- Condição atual. Inicialmente a condição do componente é “sem falha”.
- Taxa de falha (λ): Valor utilizado para calcular quando ocorrerá a falha.
- Taxa de reparo (μ): Valor utilizado para calcular o intervalo de tempo para recuperar o componente.
- O valor de saída para o sistema: máximo e mínimo.

De acordo com a condição do componente, o valor pode variar de um valor mínimo até um máximo. O valor terá influência no comportamento dinâmico do sistema, dy/dt .

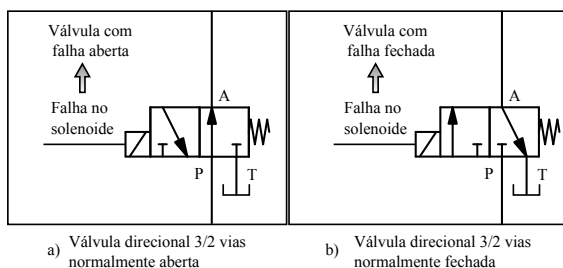
Destaca-se aqui a diferença entre estado operacional e condição do componente. O estado operacional é o modo como o componente está operando, que pode ser ligado ou desligado. Por outro lado, a condição do componente está relacionado com os possíveis estados do componente, definido na atividade 3.2 “Caracterização dos componentes”, onde são gerados diagramas representando os estados dos componentes. A condição de cada componente pode ser: sem falha, com falha evidente ou com falha oculta.

4.8.2.3 Sorteio de: tipos de falha, tempos de falha e reparo

Nessa rotina, com a função densidade de probabilidade e os valores de taxa de falha, calcula-se o tempo que a falha irá ocorrer. Além disso deve-se considerar o tipo de falha, ou seja, sortear se a falha será aberta ou fechada. As probabilidades associadas ao tipo de falha podem ser iguais, ou não, isso dependerá das características construtivas de cada componente e a maneira como está instalado no sistema.

A Figura 4.33 apresenta um exemplo em que uma válvula direcional 3/2 vias faz parte de um circuito hidráulico. A válvula é acionada por meio de um solenoide. Na Figura 4.33 (a), a falha do solenoide faz com que a válvula tenha uma falha aberta, ou seja, na tentativa de fechar a válvula, esta permaneceu aberta por causa da falha do solenoide. Em contrapartida, na Figura 4.33 (b), a falha do solenoide gera uma falha fechada na válvula. Ou seja, aciona-se o solenoide para abrir a válvula, mas esta permanece fechada⁷.

Figura 4.33 – Válvula direcional com falha do tipo aberta e fechada



Portanto, nesse caso, os detalhes construtivos da válvula direcional 3/2 vias definem o modo de falha do solenoide na válvula, ou seja, o modo falha deste componente pode ser uma falha aberta ou fechada.

O tempo de reparo também é uma variável aleatória que será calculada em função da taxa de reparo. O tempo de reparo é uma forma de considerar fatores humanos na simulação. De acordo com a capacitação da equipe de manutenção, número de colaboradores, equipamentos utilizados, alarmes, entre outros fatores, os valores das taxas de reparo irão variar mais ou menos.

Cada componente que sofrer uma manutenção, terá um novo tempo de falha, tipo de falha e tempo de reparo. É possível adicionar uma função de degradação nas taxas de falha, que irá influenciar o tempo de falha, fazendo com que a próxima ocorrência de falha seja num tempo menor do que em um

⁷Pode-se dizer então que, uma falha aberta é uma falha que ocorre em uma ação de fechar e uma falha fechada é uma falha que ocorre em uma ação de abrir.

componente “novo”.

4.8.2.4 Ordenação cronológica das falhas dos componentes

Após o cálculo dos tempos de falha é preciso organizar os componentes por ordem de ocorrência de falha, ou seja, qual componente irá falhar primeiro, qual o segundo e assim por diante. Esta ordenação se faz necessária, pois durante a simulação são realizadas verificações para identificar qual o próximo evento. Assim, se o evento for “falha de componente”, é preciso identificar o componente que irá falhar e quando irá ocorrer.

4.8.2.5 Tempo de missão ($t_{miss\tilde{a}o}$) e falha do sistema

O tempo de missão e a falha do sistema são dois eventos que interrompem a simulação. Se o tempo de missão for atingido e a variável de estado do sistema não atingiu o limite que caracteriza a falha, significa que houve sucesso na missão.

Por outro lado, se a variável de estado atingir o valor limite que caracteriza a falha do sistema, interrompe-se a simulação e registra-se a falha e o tempo t de ocorrência. O conjunto de valores, falha e tempo, de várias rodadas de simulação são utilizados na etapa final para construção dos histogramas e cálculo das probabilidades de falha.

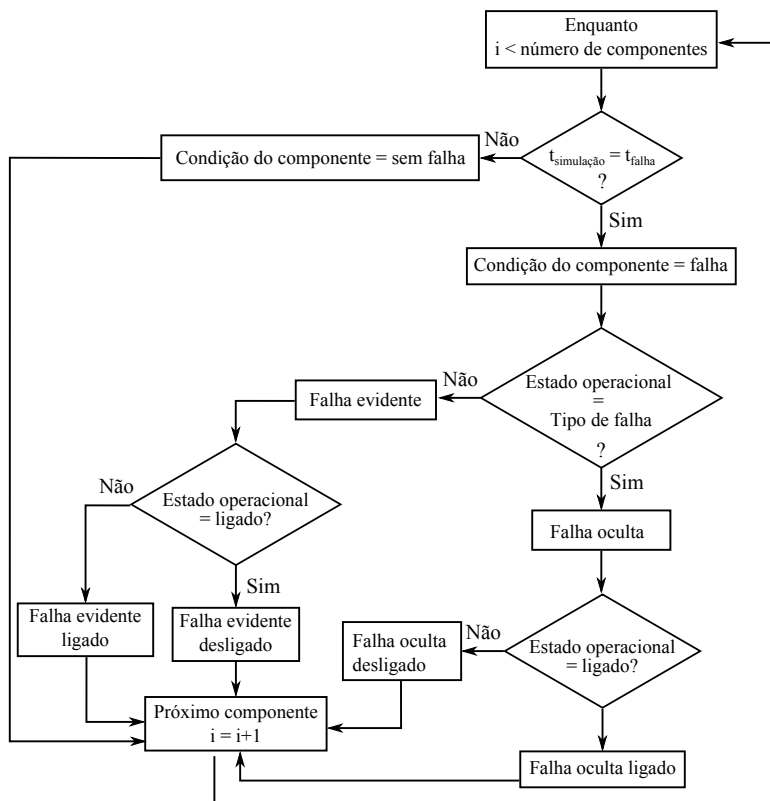
4.8.2.6 Condição de falha dos componentes

Nesta rotina, o tempo t de simulação será comparado com o tempo de falha dos componentes. Se os valores forem iguais, muda-se o estado do componente para falha.

Posteriormente é necessário verificar se a falha é aberta ou fechada. Se o estado operacional antes da falha do componente for aberto e ocorrer uma falha aberta, tem-se uma falha oculta aberta. Por outro lado, se o estado operacional do componente antes da falha for fechado e ocorrer uma falha fechada, tem-se uma falha oculta fechada.

Assim, as informações de entrada nesta rotina são: o tempo t de simulação, o tempo de falha, o tipo de falha e o estado operacional do componente. A Figura 4.34 apresenta um fluxograma para auxiliar na implementação da rotina.

Figura 4.34 – Fluxograma para avaliação da “Condição de falha nos componentes” no *software* (Figura 4.32)

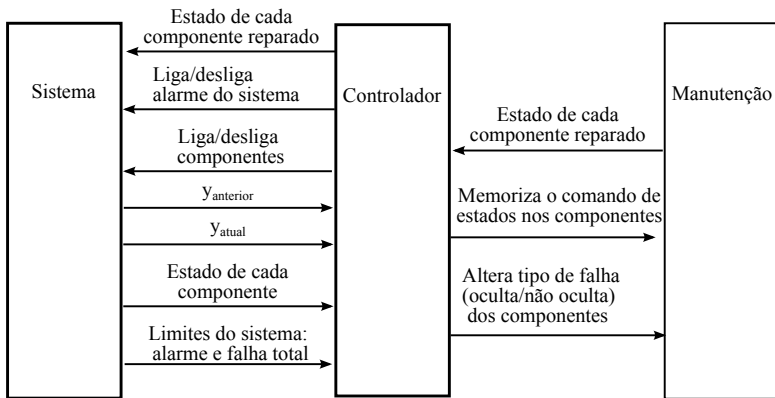


4.8.2.7 Ações do controlador

De acordo com o valor da variável de controle, y , uma rotina denominada “controlador” irá executar comandos para ligar e desligar os componentes. Além disso, irá disparar ações de manutenção e alterar o estado dos componentes quando forem reparados. A Figura 4.35 ilustra as variáveis que devem ser fornecidas para o controlador (variáveis de entrada) e as informações retornadas por ele.

Quando a variável de controle sai da região de operação normal, o controlador deve disparar um alarme (sinal) para indicar que existe falha em algum componente. Além disso deve alterar a condição do sistema informando que está em reparo – nesse momento, o tempo de início de reparo é ajustado.

Figura 4.35 – Variáveis de entrada e saída do controlador



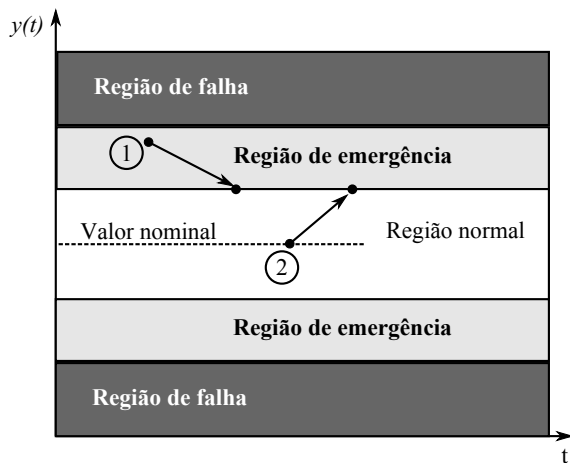
O tempo para finalização do reparo é obtido com o sorteio da taxa de reparo (μ) do componente.

Quando o tempo para finalização do reparo for igual ao tempo de simulação t , o estado do componente é alterado de acordo com o último estado definido pelo próprio controlador. Assim, o último comando do controlador (ligar/desligar) sobre o componente deve ficar registrado, para que depois da manutenção, este estado seja ajustado no componente reparado.

Ao final do reparo o componente não tem mais falha, no entanto, é preciso sortear novos tempos de falha e reparo. Após cada reparo de componente, é feita uma reordenação dos componentes em função dos tempos de falha. Com os componentes sem falha, o sistema retorna para as condições normais de operação, sendo então desligado o alarme que indica a condição de emergência.

Outra consideração importante é saber o estado anterior da variável de controle, y . A Figura 4.36 ilustra esse caso. Quando a variável de controle, y , está fora da faixa normal de operação, ponto (1), e posteriormente atinge o limite da condição normal, nenhum comando para mudança de estado é realizado. Por outro lado, se ocorre da variável de controle estar dentro da faixa normal de operação, ponto (2), e no momento seguinte alcança a linha limite, o controlador dispara um alarme e após o tempo de reação, muda o estado de alguns componentes para impedir a progressão da variável de controle em direção aos limites que caracterizam a falha do sistema.

Assim, para um mesmo valor de y , é possível que o sistema tenha dois comportamentos distintos. Um comportamento para o sistema saindo da condição normal e outro para quando estiver retornando.

Figura 4.36 – Ação do controlador diante da posição da variável de controle y 

4.8.2.8 Cálculo dy/dt para definir a variação do sistema

Nesta rotina, em função dos estados dos componentes, calcula-se a derivada da variável de estado do sistema, dy/dt . Com esse valor e os limites operacionais do sistema (condição normal, emergência e falha) é possível determinar para qual região a variável de estado do sistema – ou variável de controle – está avançando e verificar o tempo demandado para alcançar essa região.

4.8.2.9 Determinação do próximo evento e tempo associado

A simulação tem um comportamento markoviano, ou seja, dado que se conhece o estado do sistema no presente, é possível saber qual será o seu próximo estado futuro. Desta forma, sabendo como está ocorrendo a variação do sistema, dy/dt , bem como os tempos de falha e de reparo dos componentes, é possível determinar qual será o próximo evento.

Assim, a simulação se desenvolve gerenciada por eventos, que podem ser:

- Falha de um componente
- Reparo de um componente
- Valor limite da região de segurança da variável de controle

- Valor nominal de operação da variável de controle
- Sucesso da missão
- Falha do sistema, tendo a variável de controle atingido o valor crítico.

Se os valores da variável de controle forem constantes ao longo do tempo na simulação, $dy/dt = 0$, a análise dos resultados se torna mais restrita e dessa forma os resultados para o próximo evento podem ser: falha ou reparo de algum componente ou sucesso da missão.

No entanto, se a variação da variável de controle for diferente de zero, então é preciso verificar qual o valor atual e quanto tempo levará para chegar ao próximo limite (segurança, valor nominal ou falha do sistema). Este tempo deve ser comparado com o tempo de falha e reparo dos componentes para que o menor tempo seja o próximo evento.

4.8.2.10 Próximo tempo t e estado y

Esta é a última rotina do ciclo de simulação para coleta dos tempos de falha do sistema. Neste momento é atualizado o incremento, Δt , que será dado ao tempo de simulação t . Tal incremento é obtido com a rotina “Determinação do próximo evento e tempo associado”. Assim, a simulação segue orientada a eventos, que pode ser uma falha, um reparo ou um valor de referência da variável de estado y .

4.9 ETAPA 6: ANÁLISE DE RESULTADOS

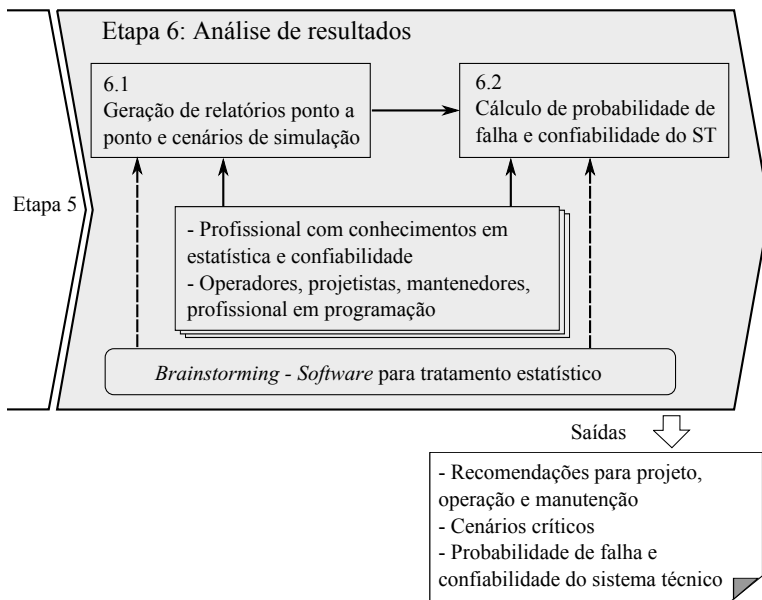
A Figura 4.37 representa a etapa de resultados, onde são realizadas as seguintes atividades:

- Atividade 6.1: Geração de relatórios ponto a ponto e cenários de falha
- Atividade 6.2: Cálculo da probabilidade de falha e confiabilidade do sistema técnico

Espera-se, como resultados, ter um modelo que represente o sistema em suas configurações variadas, ter um modelo de confiabilidade mais próximo da realidade, servir como material de apoio a decisões para o gerenciamento de ativos, planejamento da manutenção e atualização tecnológica dos equipamentos.

Com a metodologia busca-se facilitar o papel do analista e também reduzir a dispersão das análises, visto que elas são muito dependentes dos

Figura 4.37 – Atividade da etapa 6



especialistas. Assim, o desenvolvimento estruturado da análise visa reduzir a chance de erros e também facilitar a aplicação da análise de confiabilidade dinâmica.

4.9.1 Atividade 6.1: Geração de relatórios ponto a ponto e cenários de simulação

A utilização de relatórios ponto a ponto e cenários permitem visualizar o comportamento dinâmico da variável de estado do sistema. De posse do relatório e do gráfico verifica-se há coerência do comportamento do sistema para identificar eventuais erros na modelagem ou implementação.

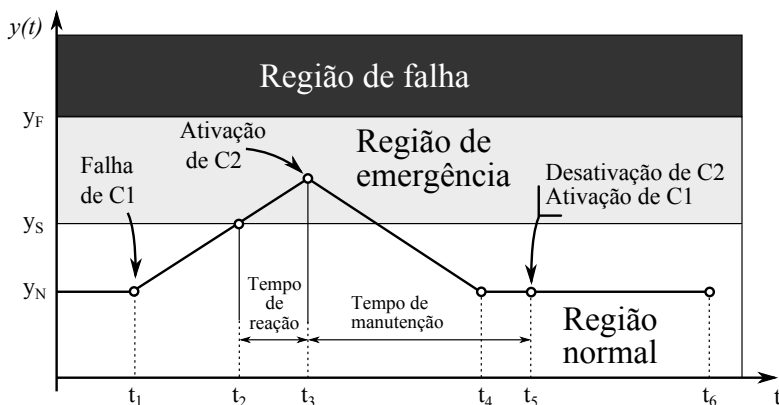
4.9.1.1 Cenários de simulação

A Figura 4.38 apresenta um exemplo de um cenário que pode ocorrer como resultado de uma simulação. Para o exemplo foi considerado um sistema com dois componentes, sendo um principal (C1) e outro reserva (C2).

No tempo t_1 , ocorre a falha de C1 e com isso a variável de controle $y(t)$

avança para a região de emergência. Após ter passado o tempo de reação em t_3 , o componente (C2) entra em operação, trazendo o sistema para a região normal em T_4 . Depois de ter sido concluída a manutenção do componente em falha, em t_5 , é realizada a comutação entre os componentes – desativação de C2 e ativação de C1.

Figura 4.38 – Cenário com sucesso da missão



Assim, a Figura 4.38 representa o comportamento dinâmico do sistema para um resultado de simulação. Os textos incluídos no gráfico foram adicionados manualmente com a intenção de explicar o comportamento da variável no gráfico. No entanto, todos os gráficos devem vir acompanhados de relatórios ponto a ponto, a fim de verificar a coerência do comportamento do modelo em relação ao sistema real.

4.9.1.2 Relatório ponto a ponto

Os relatórios ponto a ponto são utilizados junto com os gráficos de cenários da simulação. Nele, cada ponto do gráfico é identificado trazendo as informações das condições dos sistema e componentes. Além disso, apresenta qual será o próximo evento e quando este irá ocorrer.

A Figura 4.39 apresenta parte do relatório, contendo apenas o “ponto 0” e “ponto 1”, que poderia ser gerado para o exemplo apresentado na Figura 4.38. O presente relatório seria composto por sete pontos – seis pontos apresentados no gráfico mais o ponto inicial ($t = 0, y = y_n$).

Desta forma, os relatórios devem apresentar as seguintes informações:

- Ponto de referência

Número sequencial que indica cada ponto no gráfico de cenário, sendo identificado por um tempo e um valor da variável de controle do sistema (t_i, y_i) .

- Tempo t e variável de controle y

Corresponde aos valores t_i e y_i para o ponto de referência

- Estados dos componentes

Os estados dos componentes permitem inferir sobre o comportamento da variável de controle, dy/dt . Assim, o analista, quando percebe uma variação dy/dt fora dos padrões esperados, deve observar qual os estados dos componentes para verificar se o comportamento está coerente.

- Alarme do sistema para não-conformidade

O alarme indica quando a variável de controle alcançou o início da região de emergência. Significa que o sistema está deixando a região de operação normal, conseqüentemente, há alguma não conformidade. Esta informação serve para dar início do tempo de reação, tempo gasto para iniciar a identificação e manutenção dos componentes em falha.

- Próximo evento e tempo

Com as informações dos estados dos componentes, tempos de falha/reparo, y e dy/dt é possível avaliar qual será o próximo evento e quando irá ocorrer. Apresenta-se esta informação no relatório, para cada ponto de referência, para verificar se a seqüência de eventos está coerente com os eventos reais.

4.9.2 Atividade 6.2: Cálculo da probabilidade de falha e confiabilidade do sistema técnico

A falha do sistema é caracterizada quando a variável de controle alcança a região de falha. Esta informação é armazenada em uma variável junto com o tempo t em que ocorreu a falha. Um conjunto de falhas distribuídas ao longo do tempo permite construir um histograma e com isso obter a probabilidade de falha e a confiabilidade do sistema.

A Figura 4.40 ilustra a seqüência de passos para obter a função densidade de falha de um sistema. No exemplo são realizadas doze simulações até

Figura 4.39 – Relatório para o cenário apresentado na Figura 4.38

```

***** Ponto 0 *****
t = 0     e     y = yN

----- Estados dos componentes -----
C1: Sem falha (ligado)
C2: Sem falha (desligado)

----- Alarme de não conformidade -----
Alarme = desligado

----- Próximo evento -----
Próximo evento ==> Falha evidente de C1 (desligado)
Próximo tempo t ==> t = t1

*****
***** Ponto 1 *****
t = t1    e     y = yN

----- Estados dos componentes -----
C1: Falha evidente (desligado)
C2: Sem falha (desligado)

----- Alarme de não conformidade -----
Alarme = desligado

----- Próximo evento -----
Próximo evento ==> Nível yE
Próximo tempo t ==> t = t2

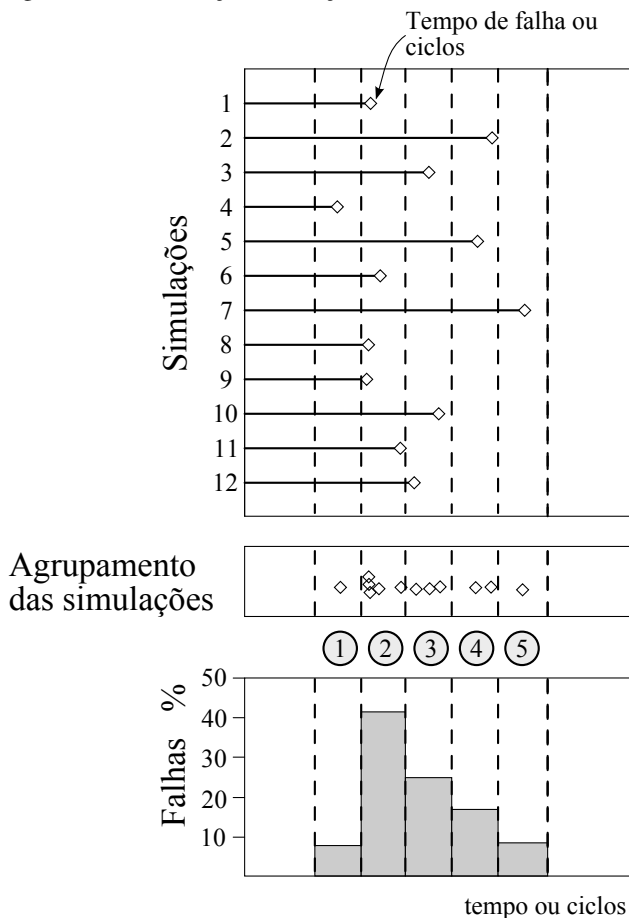
```

a falha, as quais são agrupadas em cinco classes. A contagem das falhas em cada classe permite obter as frequências relativas de falhas, em porcentagem

Todavia, muitas vezes se deseja ter um conjunto de histogramas, com o objetivo de realizar uma análise de dispersão dos resultados (histogramas ou funções densidade de falha). Assim, para se obter mais funções, basta repetir o processo. A Figura 4.41 apresenta um fluxograma que pode ser utilizado para gerar vários histogramas ou funções densidades de falha, permitindo realizar uma análise de dispersão dos dados. O número de histogramas é definido pela variável $n_{funcoes}$ e o número de simulações para gerar cada um dos histogramas é definido pela variável $n_{simulacoes}$.

Pode-se reduzir a dispersão com aumento na quantidade de simulações – para construção de cada histograma – e no número de repetições. Em contrapartida, haverá um maior custo em processamento computacional, demandando um tempo maior para a obtenção dos resultados.

Figura 4.40 – Obtenção da função densidade de falha



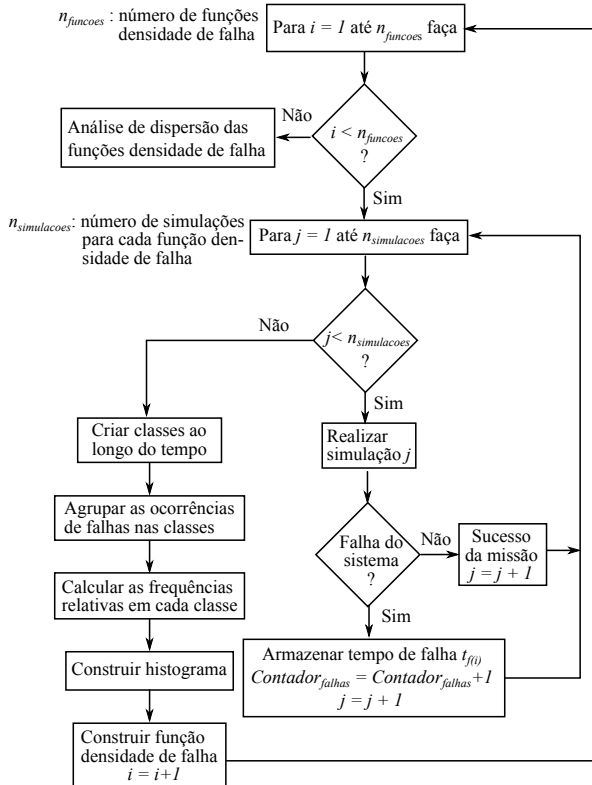
Fonte: Adaptado de Bertsche (2008)

O aumento da quantidade de simulações e de classes⁸, torna as diferenças de falhas entre as classes mais suave, melhorando a visualização dos histogramas.

Outra informação importante que pode ser obtida durante as simulações é a probabilidade de falha oculta dos componentes. Ou seja, dado que ocorreu uma falha oculta, registra-se a ocorrência e o tempo. Com essas informações, constrói-se histogramas e obtém a probabilidade de falha oculta dos compo-

⁸O aumento do número de classes permite que o intervalo de tempo, ou ciclo, para cada classe fique menor. Consequentemente, há uma maior discretização do gráfico, tornando-o mais suave.

Figura 4.41 – Rotina para gerar um conjunto de funções densidade de falha



mentes. Tal informação pode ser usada pelos mantenedores na busca de falhas ocultas pelo sistema.

Com relação à detecção de falha oculta, Assis (2012) propõe uma maneira de estimar a periodicidade de inspeção, em componentes responsáveis pela proteção do sistema sujeitos à falhas ocultas. No artigo, o autor leva em consideração aspectos de custos de manutenção para determinar o período ótimo para a realização das inspeções.

A análise parte da consideração de que inspeções mais frequentes possuem maiores chances de detectar as falhas e, logo, menores serão os custos com as consequências das falhas. No entanto, a realização das inspeções também têm um custo envolvido. Então, pressupõe-se que existe um período ótimo para as inspeções, no qual o custo total é mínimo. As simulações são realizadas orientadas a eventos, usando como base o método de Monte Carlo.

Portanto, como a metodologia proposta neste trabalho permite obter a função densidade de falhas ocultas, pode-se futuramente adicionar uma implementação envolvendo custos, de forma que seja possível – da mesma maneira que foi proposto por Assis (2012) –, calcular um período ótimo para a realização das inspeções no sistema.

4.10 RELAÇÃO ENTRE A METODOLOGIA ACODI E A MCC

Percebe-se com as etapas da metodologia ACoDi, uma proximidade com os processos de manutenção, especificamente a manutenção centrada em confiabilidade MCC. Desta forma, nesta seção apresenta os pontos que relacionam as duas metodologias.

A Figura 4.42 apresenta a relação entre a metodologia MCC proposta por Rigoni (2009) e a metodologia para análise de confiabilidade dinâmica proposta neste trabalho. As etapas 3, 4, 5 e 6 da metodologia para MCC fornecem informações para as etapas 1, 3 e 4 da análise de confiabilidade dinâmica.

A seguir, é apresentada uma breve descrição das etapas da análise de confiabilidade dinâmica que são dependentes das informações da MCC:

- Etapa 1: Análise inicial do sistema técnico para confiabilidade dinâmica

Nesta etapa, são necessárias informações para análise de criticidade do sistema. Assim, as informações desenvolvidas na etapa 3 da MCC (FMECA) dão suporte para a análise do sistema e tomada de decisões.

- Etapa 3: Análise do sistema, subsistemas e componentes

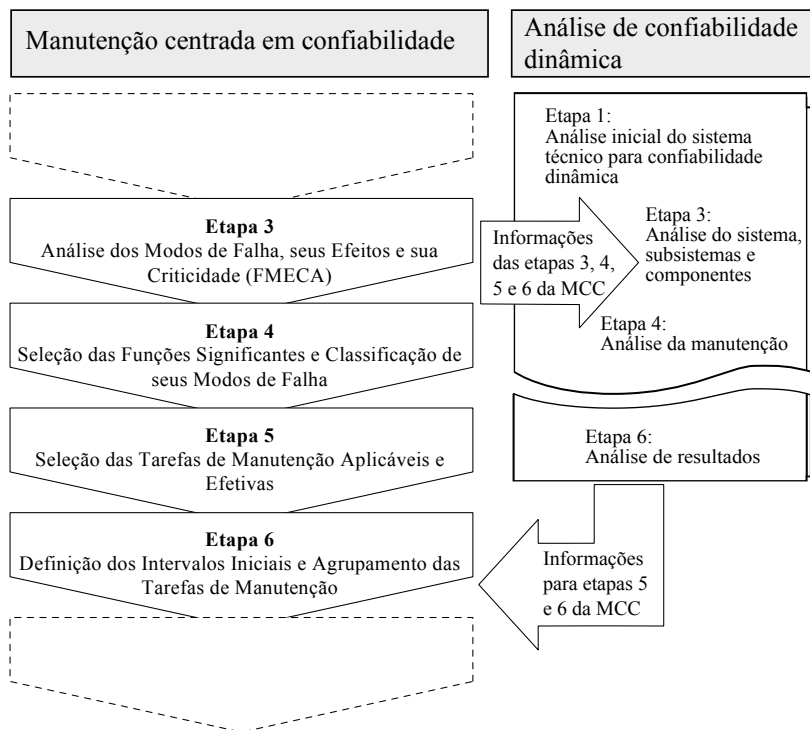
As informações dos componentes e subsistemas, funções críticas, modos de falhas e efeitos, desenvolvidas na MCC são utilizadas na modelagem comportamental do sistema. As falhas que podem ocorrer nos componentes possuem influência direta sobre o comportamento dinâmico do sistema.

- Etapa 4: Análise da manutenção

As manutenções tem grande peso na confiabilidade do sistema na análise de confiabilidade dinâmica. Assim, as informações sobre os procedimentos de manutenção, tempo de execução das tarefas entre outras informações geradas nas etapas 5 e 6 da MCC, são necessárias para a modelagem da manutenção.

Os resultados da análise de confiabilidade dinâmica obtida na etapa 6 (Análise de resultados), podem servir como informações de suporte para

Figura 4.42 – Relação entre a metodologia ACoDi e a MCC



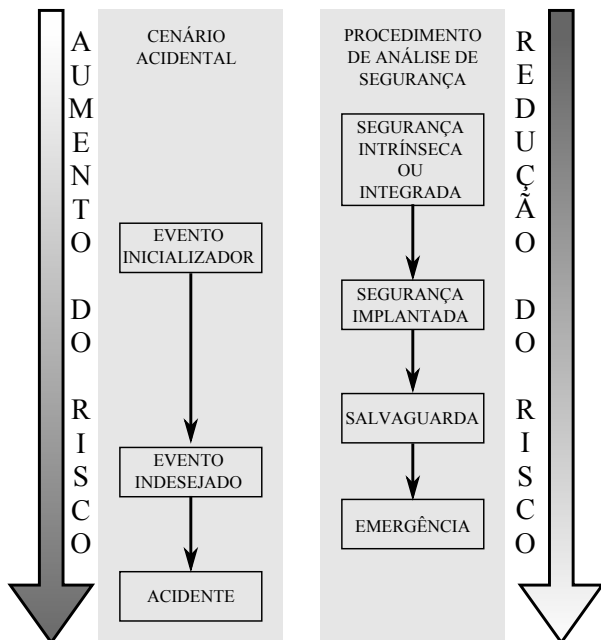
a MCC, especificamente, nas etapas 5 e 6. Assim, pode-se atualizar as informações da MCC, fechando um ciclo com melhoria contínua. Ou seja, as informações geradas pela MCC são fornecidas para a análise de confiabilidade dinâmica, que retorna quais pontos do processo de manutenção poderiam ser melhorados. Com isso, faz-se a implementação das mudanças propostas e realiza-se uma nova avaliação do sistema, tanto no contexto da MCC como na confiabilidade dinâmica.

4.11 RELAÇÃO ENTRE A METODOLOGIA ACoDi E A ANÁLISE DE SEGURANÇA DE SISTEMAS

Guimarães (2003) apresenta na Figura 4.43, um procedimento geral de análise de segurança de sistemas, constituído de quatro etapas: segurança intrínseca, segurança implantada, salvaguarda e emergência.

De acordo com a Figura 4.43, à proporção que as etapas são implantadas ocorre a redução do risco. Em contrapartida, dado que se deflagrou o evento inicializador e ocorre a progressão do cenário acidental, tem-se um aumento do risco.

Figura 4.43 – Procedimento de análise de segurança



Fonte: Adaptado de Guimarães (2003)

Pode-se relacionar as regiões de operação do sistema da Figura 4.23, com o cenário acidental apresentado por Guimarães (2003). Quando a variável de controle avança para a “região de falha” apresentada na Figura 4.23 corresponde ao avanço do cenário acidental em direção ao “acidente”. Assim, quanto maior for a região de emergência, na Figura 4.23, mais distante a região de falha estará da região normal ou nominal. Conseqüentemente, um tempo maior será disponível para o acionamento das “barreiras de segurança” ou “ações de contenção” contidas nos procedimentos de segurança, o que aumentam as chances de impedir ou retardar o avanço para a região de falha.

Os dispositivos de alarme e os procedimentos de análise de segurança, têm influência na confiabilidade dinâmica do sistema técnico. Durante os estudos e implantação dos procedimentos de segurança, principalmente nas etapas de “segurança implantada” e “salvaguarda”, pode-se realizar simulações

(alterando as regiões de operação, alarmes, controles, etc) a fim de se obter maior confiabilidade do sistema técnico, resultando em uma maior eficiência das alterações propostas no sistema técnico.

4.12 CONSIDERAÇÕES DO CAPÍTULO

O presente capítulo apresentou a proposta de metodologia para a análise de confiabilidade dinâmica. Na Etapa 1 (Análise inicial do sistema técnico para confiabilidade dinâmica) foram apresentados alguns critérios para o uso da metodologia, que depende fundamentalmente das características do sistema técnico que está sendo analisado. Ao longo do desenvolvimento do estudo percebe-se que é preciso conhecer bem o sistema que está sendo analisado, e para isso é necessário saber como os componentes ou subsistemas funcionam e como estão relacionados, para melhor caracterizar as falhas (modos de falhas e efeitos).

Para os casos em que, inicialmente, se tem pouco conhecimento sobre o sistema recomenda-se fortemente a utilização da técnica FMECA pois, neste tipo de análise parte-se da análise funcional dos componentes, e posteriormente analisa-se as possíveis falhas dos componentes e os efeitos que poderiam gerar no sistema. Esse procedimento indutivo possibilita adquirir conhecimento profundo sobre o sistema, obter lista de subsistemas e componentes mais importantes, conhecimento sobre as falhas dos componentes e, por fim, a criticidade do sistema, que é um dos critérios de avaliação para o uso da metodologia.

Outra técnica recomendada é a CNEA, semelhante à técnica FMECA, contudo ao invés de trazer as informações em forma de tabela, faz uso de diagramas para representar sequências de eventos de falha. Com isso, facilita a discussão e a compreensão sobre as relações de modos de falha, causas e efeitos de falha. Na Etapa 3 (Análise do sistema e componentes) e Etapa 4 (Análise da manutenção do sistema técnico) o comportamento do sistema é descrito em função das falhas e das manutenções. Por causa disso, o uso de análise de falhas como técnica de suporte nessas etapas se torna fundamental.

Dado que se tenha um pouco mais de conhecimento sobre as relações de causa e efeitos, pode-se também utilizar a técnica FTA. Esta técnica possui uma estrutura onde o evento de topo é uma falha do sistema e abaixo deste evento estão todas as possíveis causas relacionadas por portas lógicas.

No trabalho de Kagueiyama (2012) o autor disserta sobre várias técnicas utilizadas na análise de confiabilidade⁹ e como podem ser utilizadas em conjunto.

⁹IDEF0, FMECA, FTA, CNEA e redes bayesianas.

Outra consideração importante a ser ressaltada é a forte interação da metodologia proposta com a MCC. Tão importante quanto as técnicas de análise de falhas, a manutenção centrada em confiabilidade é uma das principais fontes de informação para a modelagem do sistema, principalmente, nas etapas 3 e 4, pois o comportamento dinâmico do sistema está fortemente relacionado com os sensores, alarmes e ações de operação/manutenção.

Desta forma, quanto maior for a quantidade de informações obtidas com a MCC, mais fácil se dará a implementação e maior será a proximidade do modelo com o sistema real. Destaca-se também a relação da metodologia com a análise de segurança de sistemas. Alguns conceitos (como alarmes, controles sobre as falhas, etc) são semelhantes aos adotados na área de segurança de sistemas. Conseqüentemente, pode-se utilizar a metodologia para auxiliar nos estudos de segurança de sistemas.

Um dos problemas observados por diversos autores é a falta de um modelo para facilitar a aplicação da análise de confiabilidade dinâmica. Assim, um dos desafios desse trabalho é, além de desenvolver uma metodologia para a análise, tornar a aplicação da técnica mais simples.

A modelagem utilizando a filosofia de sistemas orientados a eventos é bastante adequada para os problemas de análise de confiabilidade dinâmica. Uma das vantagens disso é a velocidade na execução das simulações que fica bastante rápida, quando comparada com simulações que executam com incremento de passo no tempo, Δt , constante. Outro problema de executar o incremento de tempo constante é que se o valor for muito grande, pode-se perder alguns eventos. E para valores muito pequenos o tempo de simulação pode ficar muito demorado.

Assim, o presente trabalho identifica o próximo evento e quando irá ocorrer, e por isso, o valor do incremento de tempo, Δt , é variável. Portanto, quando há poucos eventos entre o início da simulação e o tempo de missão, o tempo gasto na simulação é bem curto.

A metodologia será aplicada em um problema clássico de confiabilidade dinâmica, apresentado no Capítulo 5. Posteriormente, a metodologia será aplicada a um sistema real, sendo os resultados comparados com a análise de confiabilidade estática.

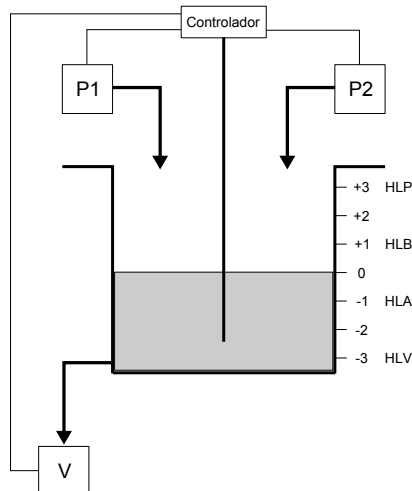
Finalmente, destaca-se que existe uma preocupação com relação à capacidade dos *softwares* em gerar números aleatórios, que na realidade são números pseudo-aleatórios, visto que a partir de um dado limite a série de valores começa a se repetir. Assim, verificou-se que, teoricamente, no Matlab é possível gerar mais do que 2^{1492} valores antes de começar a se repetir (MOLER, 2004). Desta forma, as simulações geradas nos capítulos seguintes serão realizadas com mais de um milhão de sorteios em cada análise, a fim de se obter melhores resultados numéricos.

5 APLICAÇÃO EM UM PROBLEMA CLÁSSICO

Nesta seção, a metodologia ACoDi será aplicada em um estudo de caso apresentado em um *workshop* de análise de confiabilidade dinâmica, cujo intuito era comparar várias técnicas de confiabilidade dinâmica existentes.

O *workshop* foi organizado em 2004 pela associação italiana 3ASI (*Associazione degli Analisti dell'Ambiente, dell'Affidabilità e della Sicurezza Industriale*), no qual foi apresentado o problema da Figura 5.1.

Figura 5.1 – Problema proposto



O sistema é composto por um reservatório contendo fluido, duas bombas (P1 e P2) para encher o reservatório, uma válvula (V) para esvaziá-lo e um controlador para monitorar o nível (H) do fluido e acionar as bombas e a válvula.

Inicialmente o nível H se encontra em 0, a bomba P1 ligada, a válvula V aberta e a bomba P2 desligada. A vazão fornecida pelas bombas é a mesma da válvula. Dessa forma, enquanto nenhum componente falha, o sistema mantém o nível constante em 0. A falha consiste em travar um dos componentes no estado ligado ou desligado. A probabilidade de falha obedece a distribuição exponencial.

Se H atingir o nível HLB (+1) há o risco do fluido transbordar pelo reservatório; este evento ocorre quando H excede o nível HLP (+3). Para evitar isso o controlador comanda o desligamento das duas bombas e abertura da válvula com o objetivo de reduzir H. Se um componente está travado, ele não

obedece o controlador e mantém o seu estado atual.

O outro cenário indesejado é o esvaziamento do reservatório, que ocorre quando H está abaixo de HLV (-3). Para evitar isso, quando o nível atinge HLA (-1), o controlador ordena o acionamento das duas bombas e o fechamento da válvula V , com o objetivo de aumentar o nível H .

Assim, a falha do sistema fica caracterizado pelos dois cenários: reservatório com fluido transbordando e reservatório esvaziando.

Com isso, objetivo desta seção é apresentar a metodologia passo a passo para resolver esse problema e comparar com os resultados obtidos por outros pesquisadores.

5.1 ETAPA 1: ANÁLISE INICIAL DO SISTEMA TÉCNICO PARA CONFIABILIDADE DINÂMICA

Nesta etapa são realizadas quatro atividades cujo objetivo é avaliar o comportamento dinâmico do sistema, a criticidade e a disponibilidade do sistema técnico.

- Atividade 1.1: Análise quanto ao comportamento dinâmico

O problema proposto apresenta comportamento dinâmico do nível do reservatório, que varia em função dos estados dos componentes e do tempo t .

Outro comportamento dinâmico é em relação à configuração do sistema. Nas condições normais de operação, tem-se a bomba PI acionada, fornecendo vazão para o reservatório, funcionando junto com a válvula V , drenando o reservatório. Dado que o nível H passa para HLB (+1) ou HLA (-1), a configuração do sistema, com os componentes em operação irá mudar em função das ações do controlador.

- Atividade 1.2: Análise da criticidade do sistema

Não é anunciado que o sistema é crítico. Além disso, o problema não está colocado em nenhum contexto que apresente risco ao homem, ao meio-ambiente, ou custo elevado. Assim, pode-se assumir que este problema é de baixa criticidade.

Assim, ao observar a Figura 4.10 com as relações determinísticas para a escolha da análise de confiabilidade dinâmica, no eixo das abscissas, o sistema estaria entre as colunas 1 e 3.

- Atividade 1.3: Análise da disponibilidade do sistema

Da mesma forma que a análise realizada na Atividade 1.2 (criticidade), o contexto apresentado para o problema não permite afirmar se é um sistema que exige alta disponibilidade ou não. Da maneira como está apresentado, sem uma contextualização se o reservatório faz parte de um sistema de abastecimento de água de uma cidade, ou de uma empresa, ou uma residência, ou um processo de fabricação, etc, não é possível definir qual a disponibilidade exigida pelo sistema.

Como não foi contextualizado, será assumido que o sistema não exige disponibilidade, podendo parar ocasionalmente para realizações de manutenção. Assim, será assumido que a disponibilidade exigida possui nota mínima de 1 e máxima de 3.

- Atividade 1.4: Análise do sistema

Por fim, conclui-se que o sistema possui comportamento dinâmico em que a variável de controle, nível H , muda ao longo do tempo em função dos estados dos componentes. As variações do nível ocorrem em função dos estados dos componentes, que por sua vez sofrem influência das taxas de falha e da própria variável de controle H .

Assim, mesmo que não tenha criticidade elevada ou seja exigida alta disponibilidade já se pode realizar uma análise de confiabilidade dinâmica neste sistema, tendo em vista a presença do comportamento dinâmico. Este sistema está localizado na região R2 da Figura 4.8 e a aplicação da confiabilidade dinâmica seria opcional conforme a Figura 4.10.

5.2 ETAPA 2: DEFINIÇÃO DA EQUIPE

Como a aplicação será feita em um sistema bastante simples, nesse caso, a formação da equipe não é tão relevante. Aqui a equipe está constituída apenas pelo pesquisador sendo a programação realizada no *software* Matlab.

5.3 ETAPA 3: ANÁLISE DO SISTEMA, SUBSISTEMAS E COMPONENTES

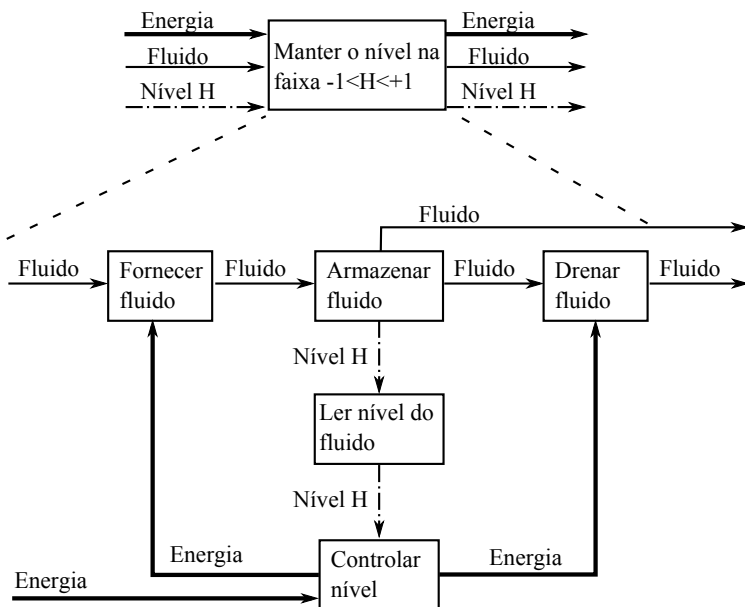
Nesta etapa são realizadas as seguintes atividades:

- Atividade 3.1: Desdobramento das funções do sistema
- Atividade 3.2: Caracterização dos subsistemas e componentes
- Atividade 3.3: Descrição comportamental do sistema

5.3.1 Atividade 3.1: Desdobramento das funções do sistema

O desdobramento das funções do sistema foi realizado conforme a Figura 5.2. Iniciou-se com a função global do sistema (manter o nível na faixa $-1 < H < +1$), sendo levado em consideração os fluxos de energia, matéria e sinal.

Figura 5.2 – Desdobramento da função global do sistema técnico



Na Figura 5.1 é possível identificar os seguintes componentes deste sistema: bomba P1, bomba P2, reservatório, válvula V e controlador. Desta forma, com o desdobramento da funcional do sistema e a lista de componentes do sistema faz-se o relacionamento dos componentes com as funções elementares identificadas, Quadro 5.1.

O reservatório e o controlador serão considerados como elementos perfeitos, que não sofrem falha. Esta consideração foi feita no trabalho de Codetta-Raiteri e Bobbio (2006), que será usado para comparação dos resultados, o que faz com que os modelos tenham os mesmos componentes.

Quadro 5.1 – Funções dos componentes do sistema técnico

Componente	Função
Bomba P1	Fornecer fluido
Bomba P2	Fornecer fluido
Reservatório	Armazenar fluido
Válvula V	Drenar fluido
Controlador	Ler nível do fluido e controlar o nível do reservatório

5.3.2 Atividade 3.2: Caracterização dos subsistemas e componentes

A quantidade de estados dos componentes para este caso são seis:

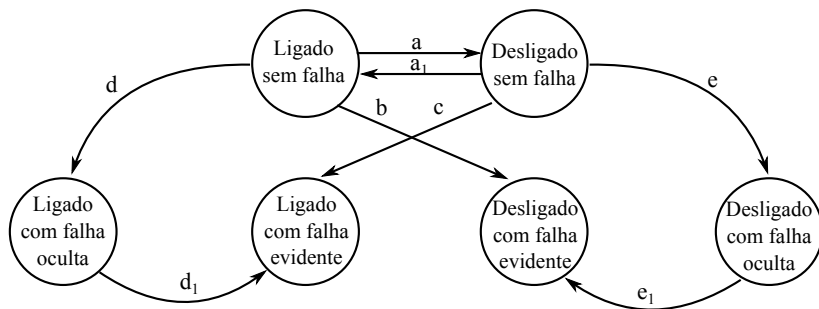
1. Ligado sem falha
2. Desligado sem falha
3. Ligado com falha evidente
4. Desligado com falha evidente
5. Ligado com falha oculta
6. Desligado com falha oculta

Os possíveis estados dos componentes, com suas transições, podem ser vistos na Figura 5.3. Na proposta realizada no *workshop*, os componentes do sistema não são reparáveis, portanto, sem manutenção. Em comparação com a Figura A.10, o número de estados é o mesmo, todavia, existem menos transições tendo em vista que neste estudo de caso não são realizadas manutenções. Assim, uma vez que o componente passa para a condição funcional “com falha evidente ou oculta”, este não retorna para a condição “sem falha”.

As transições de estados “ a_1 ” e “ a ” são determinadas pelo controlador de nível do sistema técnico. Já as transições “ b ”, “ c ”, “ d ” e “ e ” são ocasionadas por falhas que podem ser do tipo comum ou ocultas, abertas (liga quando não deveria) ou fechadas (desliga quando não deveria). As transições “ d_1 ” e “ e_1 ” ocorrem quando o controlador do sistema tenta mudar a condição operacional do componente: ligado → desligado ou desligado → ligado. Nesse momento, a falha que antes era oculta passa a ser evidente.

Os componentes da simulação suscetíveis às falhas são: bomba P1, bomba P2 e válvula V. As taxas de falha e a variação de nível, dH/dt , estão relacionadas no Quadro 5.2.

Figura 5.3 – Estados dos componentes



Quadro 5.2 – Características dos componentes

Componente	Taxa de falha (Falhas/hora)	dH/dt (m/hora)
Bomba P1	0,004566	0,6
Bomba P2	0,005714	0,6
Válvula V	0,003125	-0,6

A obtenção do tempo de falha, se o componente irá falhar travado ligado ou desligado e se a falha será evidente ou oculta é realizada em três etapas:

- Inicialmente realiza-se o sorteio do tempo de falha do componente, com base nas taxas de falha do Quadro 5.2.
- Posteriormente, um segundo sorteio é realizado para definir se o componente irá falhar travado ligado ou desligado. Neste caso, como não foi dada nenhuma informação sobre as probabilidades de falhar ligado ou desligado, considerou-se que as probabilidades de falha, em relação ao estado operacional (ligado ou desligado) são iguais.
- Por fim, verifica-se o estado operacional do componente antes da falha. A falha será oculta se o estado operacional antes da falha coincidir com estado operacional da falha (ligado ou desligado) e evidente quando forem diferentes.

Portanto, para definir o tempo de falha e o estado de falha do componente (oculta/evidente, ligado/desligado) é preciso, além do Quadro 5.2, saber o estado operacional do componente quando estava funcionando.

Embora o controlador seja um componente do sistema, este será analisado em separado na etapa 4, atividade 4.1.

5.3.3 Atividade 3.3: Descrição comportamental do sistema

A variação do nível H pode ser representada pela equação 5.1.

$$\frac{dH}{dt} = C1.Q1 + C2.Q2 + C3.Q3 \quad (5.1)$$

C1, C2 e C3 são os estados dos componentes e indicam se estão ligados (1) ou desligados (0). O componente C1 representa a bomba P1, com Q1 valendo 0,6 m/h. O componente C2 representa a bomba P2 com Q2 valendo 0,6 m/h, e C3 a válvula V com Q3 valendo -0,6 m/h.

O quadro 5.3 apresenta os valores obtidos com a equação 5.1. Desta forma, verifica-se que a taxa de variação do nível H depende do estado operacional dos componentes – pode ser positiva (aumento do nível H), nula, ou negativa. Vale destacar que a variação sendo positiva, ainda pode assumir dois valores: valores 0,6 m/h ou 1,2 m/h.

Quadro 5.3 – Taxa de variação do nível H

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

O nível do reservatório não se altera quando uma das bombas, P1 ou P2, está ligada com a válvula V e também quando todos os componentes estão desligados, situação vista na configuração 3, 5 e 8 do quadro 5.3.

O único modo em que a vazão do reservatório diminui, aparece na configuração 7, quando ambas as bombas estão desligadas e a válvula V ligada.

Para os outros quatro casos (1, 2, 4 e 6), o reservatório apresenta a tendência ao enchimento. Assim, analisando a combinação dos estados dos componentes, percebe-se que há uma tendência maior de ocorrer transborda-

mento do que esvaziamento.

5.4 ETAPA 4: ANÁLISE DA MANUTENÇÃO DO SISTEMA TÉCNICO

Esta etapa é constituída por três etapas:

- Atividade 4.1: Caracterização dos sensores, controlador e atuadores
- Atividade 4.2: Definição das regiões de operação
- Atividade 4.3: Modelagem do comportamento em função da manutenção

5.4.1 Atividade 4.1: Caracterização dos sensores, controlador e atuadores

O sensor e controlador são representados pelo mesmo componente no sistema. Os atuadores são a bomba P1, bomba P2 e válvula V, já descritos na atividade 3.2.

O controlador irá atuar sobre os componentes em função do valor da variável de estado do sistema. Se for percebido que há uma tendência de ocorrer transbordamento, o controlador irá desligar as bombas e ligar a válvula que faz a drenagem do reservatório.

Por outro lado, se houver uma tendência de esvaziamento, ambas as bombas são ligadas e válvula V é fechada.

Na condição normal de operação, nível H entre HLA (-1) e HLB (+1), a bomba P1 fica ligada, a bomba P2 desligada e a válvula V ligada. Assim, pode-se perceber que o sistema assume várias configurações em função da variável de controle H, sendo o controlador o componente responsável por essas mudanças.

O quadro 5.4 resume os estados componentes em função do nível H.

Quadro 5.4 – Configurações do sistema em função do nível

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

No Quadro 5.4 estão apresentadas apenas as configurações do sistema em que todos os componentes estão na condição sem falha. Ou seja, se forem

consideradas todas as configurações possíveis, incluindo as condições com e sem falha, resulta em 216 configurações do sistema. O cálculo é realizado com a seguinte equação:

$$i = M^n$$

sendo,

i: Número de configurações

M: Número de estados de cada componente (6)

n: Número de componentes (3)

5.4.2 Atividade 4.2: Definição das regiões de operação

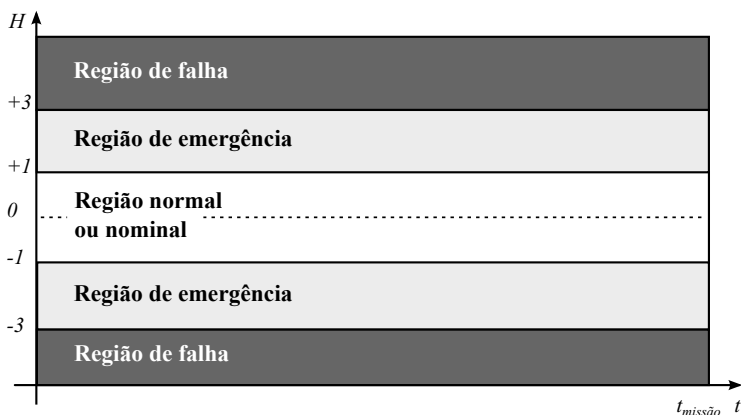
A variável de estado do sistema é o nível do reservatório H, sendo que esta terá cinco pontos característicos.

- H=0 -> Nível nominal de operação. Este é o ponto desejado de operação normal.
- H=HLB (+1) -> Nível limite (superior) da condição normal. Neste ponto existe um risco de ocorrer transbordamento. Para valores de H acima deste valor o sistema entra na região de emergência.
- H=HLA (-1) -> Nível limite (inferior) da condição normal. Neste ponto existe um risco de ocorrer a esvaziamento do reservatório. Para valores de H abaixo deste valor o sistema entra na região de emergência.
- H=HLP (+3) -> Nível máximo do reservatório. Ponto onde é caracterizado o transbordamento, portanto, falha do sistema por transbordamento.
- H=HLV (-3) -> Nível mínimo do reservatório. Ponto onde é caracterizado o esvaziamento completo, portanto, falha do sistema por esvaziamento.

O tempo de missão será 1000 horas, valor utilizado em outras simulações encontradas na literatura como Codetta-Raiteri e Bobbio (2006) e Marseguerra et al. (1998).

A Figura 5.4 apresenta as regiões de operação do sistema técnico, sendo indicadas os limites da variável de controle H para cada região.

Figura 5.4 – Regiões de operação para o reservatório



5.4.3 Atividade 4.3: Modelagem do comportamento em função da manutenção

Neste sistema não será considerada a manutenção. No entanto, ele possibilita conter o avanço da variável de controle H para a região de falha por meio das ações do controlador que altera as configurações do sistema, ativando e desativando componentes do sistema.

5.4.3.1 Tempo de reação

O tempo de reação será utilizado para comutar as configurações do sistema quando a variável de controle atingir os valores de $H=+1$ e $H=-1$. Neste estudo de caso está sendo considerado que o sistema é automático e como as mudanças são muito rápidas, está sendo considerado que o tempo de comutação é nulo.

5.4.3.2 Atuação sobre o avanço da variável de controle H

Quando a variável de controle alcançar os limites da condição normal (+1 ou -1), ocorrerão mudanças de configuração do sistema a fim de impedir o avanço para a região de falha ($H=+3$ ou $H=-3$) e recuperar a variável de controle para a condição nominal, $H=0$.

5.4.3.3 Manutenção preditiva com o sistema em operação

Neste estudo de caso, não está sendo considerada a manutenção dos componentes. Para impedir a falha do sistema é realizada apenas alterações na configuração do sistema, por meio do controlador, a fim de que não ocorra transbordamento ou secagem do reservatório.

5.5 ETAPA 5: MODELAGEM E SIMULAÇÃO

Esta etapa é constituída de duas atividades:

- Atividade 5.1: Representação do comportamento dinâmico do sistema
- Atividade 5.2: Estrutura para implementação

A atividade 5.2 não será descrita, pois a estrutura para implementação é a mesma apresentada no capítulo da proposta da metodologia. Desta forma, será descrita apenas a atividade 5.1 (Representação do comportamento dinâmico do sistema).

Para analisar os gráficos gerados na simulação é importante conhecer antecipadamente alguns possíveis cenários para facilitar a compreensão do comportamento dinâmico do sistema. A Figura 5.5 ilustra o comportamento do sistema quando ocorre a falha na bomba P1. Nesse caso, o nível do reservatório, H , irá oscilar entre o valor $+1$ e -1 , até que ocorra outra falha no sistema.

A Figura 5.6 representa uma falha da bomba P2. Nesse caso, a bomba entra em operação quando não devia. No entanto, ao atingir o nível $H=+1$ o controlador dispara um comando impedindo que ocorra o transbordamento.

Uma falha fechada na válvula V terá o mesmo comportamento apresentado na Figura 5.6, onde há um aumento do nível do reservatório até chegar no valor $H=+1$. Nesse nível, o controlador comanda o desligamento das bombas mantendo o nível estagnado em $H=+1$.

A presença de um controlador torna o sistema bastante robusto, visto que, mesmo ocorrendo falhas nos componentes e sem ter manutenção, ainda é possível com as mudanças de configuração do sistema, impedir o transbordamento ou secagem do reservatório.

A Figura 5.7 é um caso em que ocorreu a falha em dois componentes, P1 e P2. Ainda que dois componentes estivessem em falha, o controlador impede a falha total do sistema. Após o ponto de início é possível verificar a ocorrência de uma falha oculta na bomba P2. Ou seja, a bomba estava desligada e falha mantém o componente nesse mesmo estado (desligado).

Figura 5.5 – Cenário com falha na bomba P1

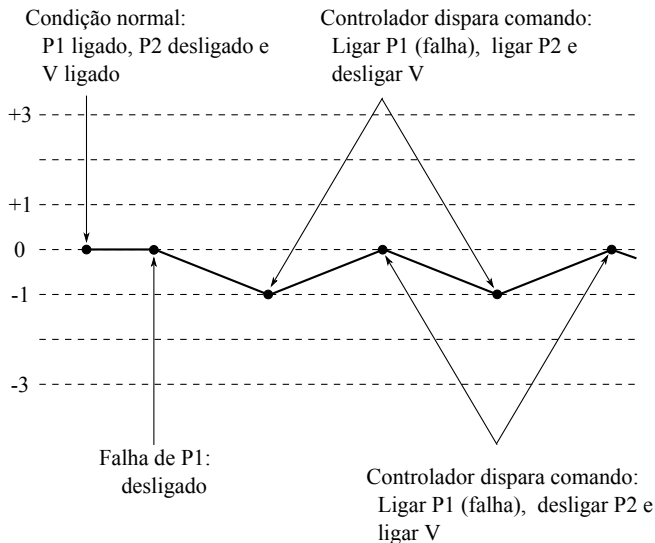
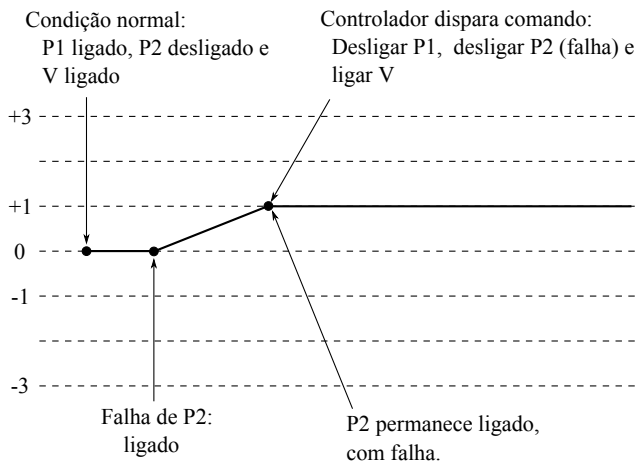
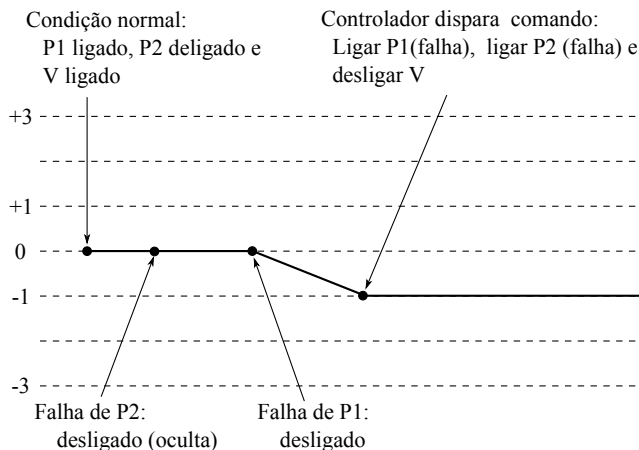


Figura 5.6 – Cenário com falha na bomba P2



Dessa forma, não há variação do nível H. A falha só deixa de ser oculta quando o controlador dispara um comando para ligar as bombas, quando o nível alcança o valor $H=-1$.

Figura 5.7 – Cenário com falha oculta na bomba P2



A representação do comportamento do sistema em função das falhas dá subsídios para o programador verificar a coerência do sistema na simulação numérica na etapa de análise dos resultados. Aqui foram criados apenas três figuras, mas já são suficientes para a compreensão do comportamento. Durante a simulação, vários eventos de falha irão se combinar e possivelmente irão gerar gráficos com uma complexidade maior.

5.6 ETAPA 6: ANÁLISE DE RESULTADOS

Nesta etapa de resultados são apresentadas duas atividades:

- Atividade 6.1: Geração dos relatórios ponto a ponto e cenários de falha
- Atividade 6.2: Cálculo da probabilidade de falha e confiabilidade do sistema técnico

Cada teste de simulação resulta em uma falha ou sucesso da missão do sistema técnico. Inicialmente, para cada teste é gerado um relatório ponto a ponto e um gráfico com o cenário de falha mostrando o comportamento dinâmico da variável de controle H. Posteriormente, após verificar que o comportamento do modelo está coerente com o sistema, são gerados apenas resultados numéricos, não sendo mais gerados os relatórios ponto a ponto e os gráficos de cenários de falha, a fim de que a simulação seja realizada com menor custo de processamento.

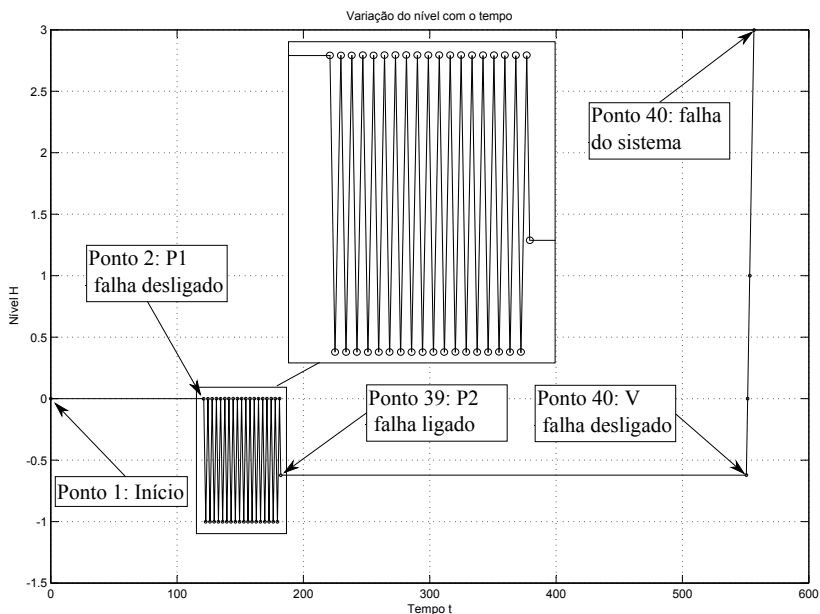
Na seção seguinte será apresentado apenas um gráfico com cenário de falha e parte de um relatório ponto a ponto.

5.6.1 Atividade 6.1: Geração dos relatórios ponto a ponto e cenários de falha

Para auxiliar na interpretação dos dados gerados pelo modelo de simulação, são gerados relatórios ponto a ponto ao longo do tempo, gráficos do comportamento dinâmico da variável de estado do sistema e os histogramas.

A Figura 5.8 apresenta o comportamento dinâmico (cenário de falha) de apenas um teste de simulação. A simulação tem início no ponto 1, com o sistema na condição normal de operação: bomba P1 ligada, P2 desligada, válvula V ligada e nível H em zero.

Figura 5.8 – Comportamento dinâmico de um teste de simulação

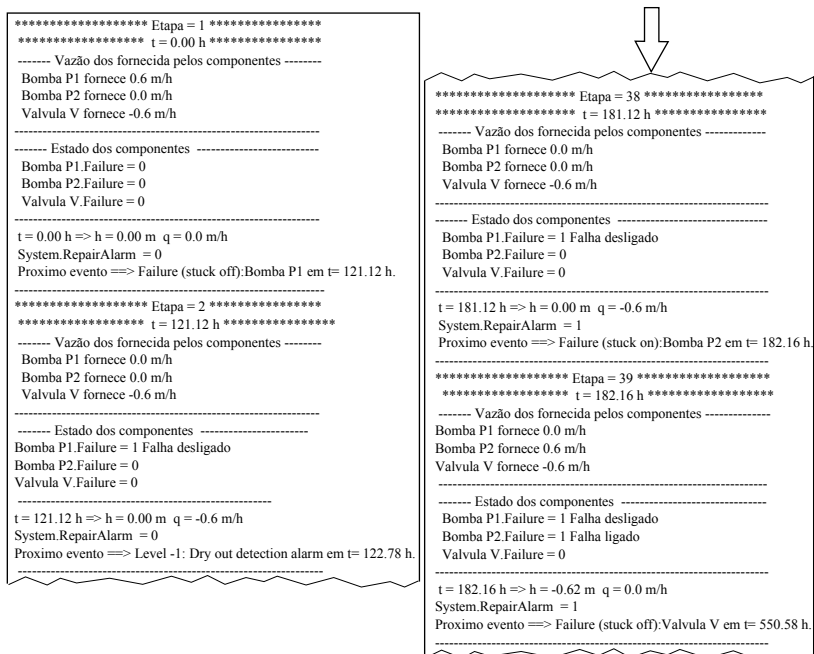


A primeira falha ocorre no tempo $t = 121,12$ h. A bomba P1 falha desligada, fazendo com que o nível do reservatório diminua até atingir $H = -1$. O controlador nesse momento comanda o fechamento da válvula V e acionamento da bomba P2, fazendo o nível do reservatório subir até atingir

$H=0$. Nesse nível o sistema deve operar com a configuração inicial (P1 ligada, P2 desligada e V ligada), mas como a bomba P1 está em falha, o nível do reservatório volta a diminuir. Esse comportamento oscilatório – representado no detalhe com ampliação – repete-se até o ponto 39, quando a bomba P2 falha ligada.

A Figura 5.9 apresenta parte do relatório ponto a ponto gerado em um teste de simulação, que é utilizado para facilitar a leitura do gráfico de comportamento dinâmico do sistema. Cada ponto do gráfico é descrito pelo relatório informando a condição (falha ou não) de cada componente, nível do reservatório, tempo, vazão de cada componente, vazão resultante, próximo evento e quando este irá ocorrer.

Figura 5.9 – Relatório ponto a ponto ao longo de um tempo de missão



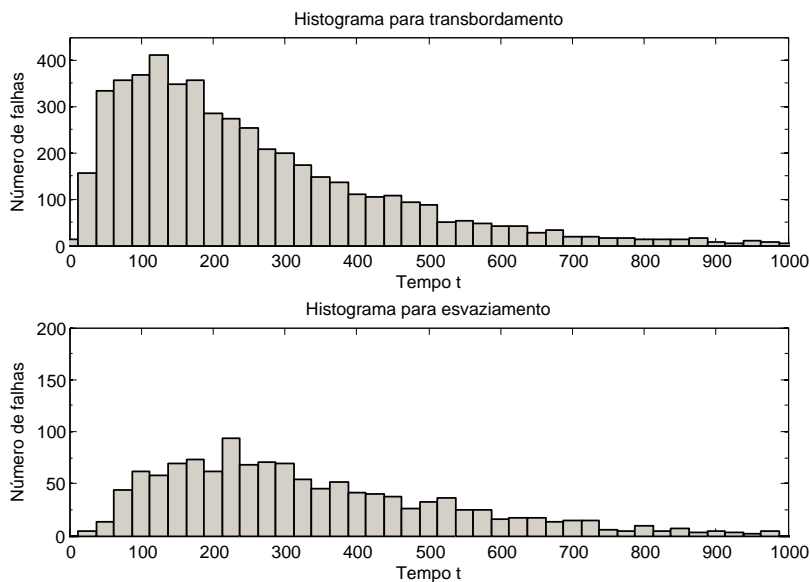
5.6.2 Atividade 6.2: Cálculo da probabilidade de falha e confiabilidade do sistema técnico

Para a construção de um único histograma, foram realizados 10 mil testes, cujo resultado pode ser: falha por transbordamento, falha por esvaziamento ou sucesso da missão. A Figura 5.10 apresenta um histograma para transbordamento e um outro para esvaziamento do reservatório.

Vale destacar que o histograma para transbordamento apresenta uma quantidade de falhas muito maior que a de esvaziamento. Por causa disso, as escalas de número de falhas nos gráficos – eixo vertical – são diferentes. Assim, no histograma de falhas por transbordamento, a escala de falhas é [0 – 450], enquanto que no histograma de falhas por esvaziamento, a escala apresentada é [0 – 200].

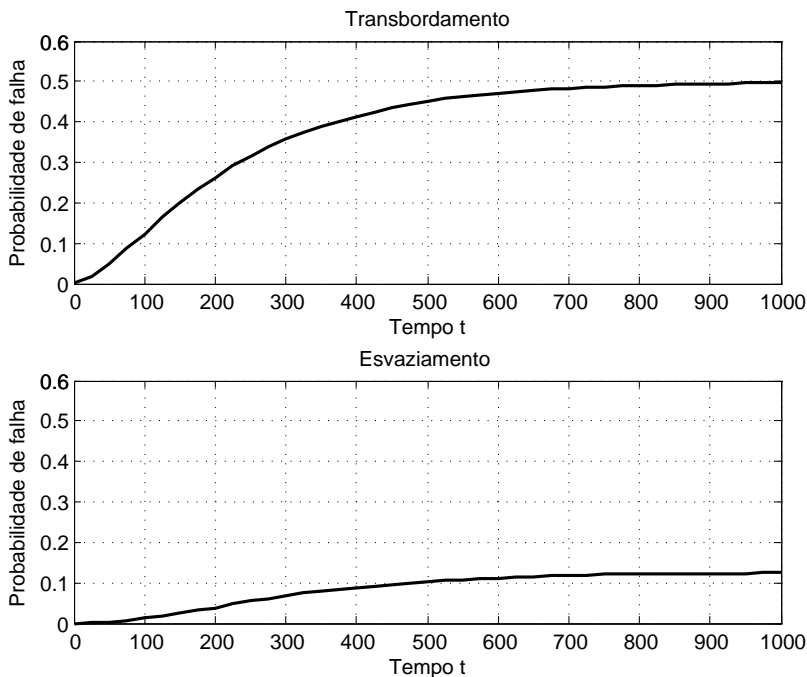
Os gráficos foram gerados com diferença nas escalas com o intuito de facilitar a visualização do gráfico referente ao esvaziamento. É possível verificar ainda que os histogramas possuem contornos que podem ser aproximados à uma função log-normal.

Figura 5.10 – Histogramas de falhas em 10 mil testes



Fazendo-se a integração dos valores contidos nos histogramas de falha no tempo, para o transbordamento e esvaziamento, obtém-se a função distribuição acumulada de falhas, Figura 5.11.

Figura 5.11 – Função distribuição acumulada de falhas



Embora a Figura 5.11 forneça as probabilidades de falha do sistema para tempos de missão de 0 até 1000 horas, ainda é necessário saber a dispersão dos resultados. Para isso, o processo para se obter cada histograma foi repetido 100 vezes, obtendo-se assim 100 curvas de distribuição acumulada de falhas para transbordamento – Figura 5.12 – e esvaziamento – Figura 5.13.

Ao analisar os gráficos da Figura 5.12 e Figura 5.13 é possível verificar que a probabilidade de ocorrer falha por transbordamento fica em torno de 50%, enquanto a probabilidade de ocorrer falha por esvaziamento do reservatório é em torno de 12%.

O valor da probabilidade de falha do sistema é uma estimativa. E como tal, deve-se determinar o intervalo de confiança, $IC_{1-\alpha}(\mu)$, em que possivelmente possa ser encontrado o valor real do parâmetro desejado, que nesse caso é a probabilidade de falha para transbordamento e esvaziamento do reservatório. Para esse cálculo, faz-se uso da Equação 5.2 (NETO, 1977).

$$IC_{1-\alpha}(\mu) \approx \left(\bar{X} - z_{1-\alpha/2} \cdot \frac{S}{\sqrt{n}}, \bar{X} + z_{1-\alpha/2} \cdot \frac{S}{\sqrt{n}} \right) \quad (5.2)$$

Figura 5.12 – Distribuição de pontos para transbordamento

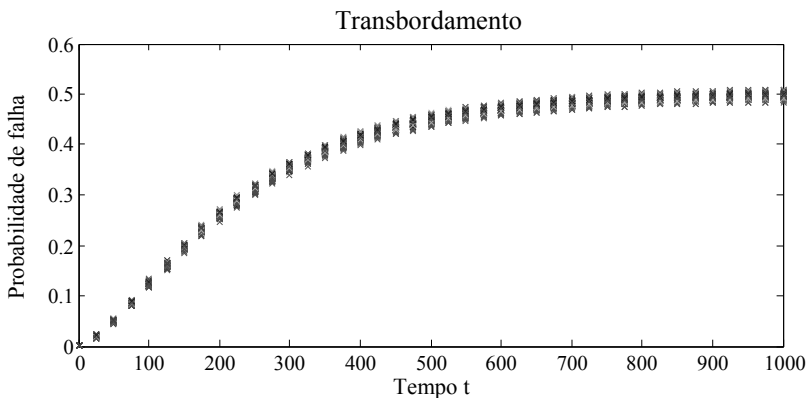
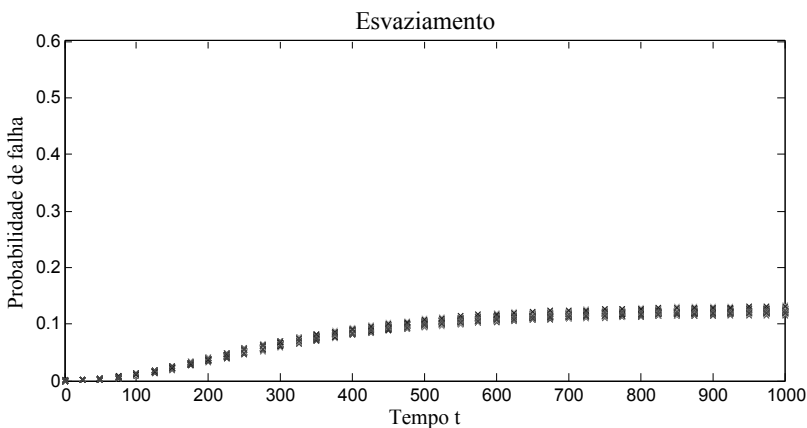


Figura 5.13 – Distribuição de pontos para esvaziamento



Quando o número de amostras é elevado, a curva da distribuição *t-student* fica muito próxima da distribuição normal. Por causa disso, nesta aplicação os limites para o intervalo de confiança foram calculados com base na distribuição normal.

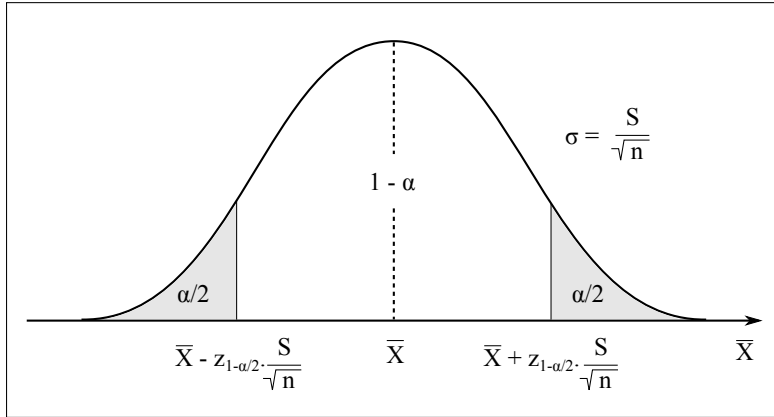
O intervalo de confiança, $IC_{1-\alpha}(\mu)$, está relacionado com a probabilidade de se encontrar o valor real dentro da faixa, sendo esta probabilidade denominada por “nível ou grau de confiança”, expressa como $(1 - \alpha)$.

Desta forma, α é a probabilidade do erro na estimação para o inter-

valo de confiança, isto é, a probabilidade de errar ao afirmar que o valor da probabilidade de falha do sistema está dentro do intervalo de confiança.

A representação gráfica do intervalo de confiança, expressa pela Equação 5.2, está ilustrada na Figura 5.14. A equação representa o limite inferior e o superior, para uma distribuição normal bi-caudal, para um nível de confiança $(1 - \alpha)$.

Figura 5.14 – Distribuição amostral de X



Fonte: Adaptado de Neto (1977)

O cálculo para determinar o intervalo de confiança de 99% em torno da média, no ponto em $t = 1000$ h (tempo de missão) foi realizado com a Equação 5.2.

Os valores utilizados para o cálculo foram:

- Número de pontos, $n = 100$.
- Para intervalo de confiança de 99%, $z = 2,58$.
- Valor médio da probabilidade de transbordamento, $\bar{X} = 0,4962$.
- Desvio padrão para os dados relacionados com o transbordamento, $S = 0,0047$.
- Valor médio da probabilidade de esvaziamento, $\bar{X} = 0,1227$.
- Desvio padrão para os dados relacionados com o esvaziamento, $S = 0,0034$.

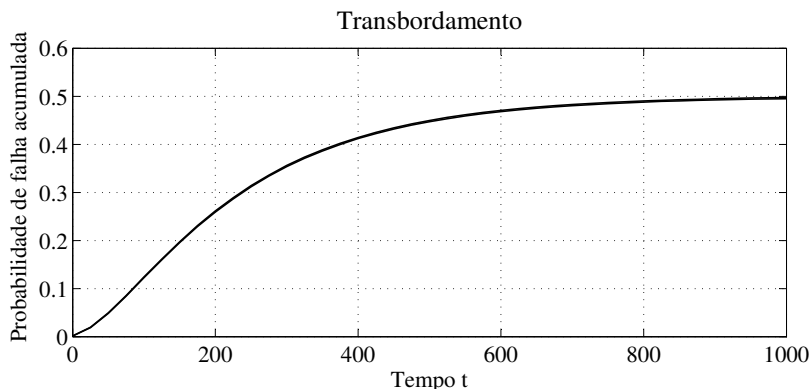
Assim, os intervalos de confiança para as falhas, no tempo $t = 1000$ h, resultam em:

Transbordamento: $IC_{99\%}(\mu) \approx (0,4950; 0,4974)$
 Esvaziamento: $IC_{99\%}(\mu) \approx (0,1218; 0,1236)$

O mesmo processo foi utilizado para determinar o intervalo de confiança para outros pontos, sendo obtidos os gráficos da Figura 5.15 e Figura 5.16. Os valores utilizados para gerar os gráficos estão apresentados no Apêndice B, nas tabelas B.1 e B.2.

Analisando os gráficos é possível perceber que a dispersão dos resultados aumenta com o aumento do tempo t , assim, as maiores diferenças estão no tempo $t = 1000$ h. No gráfico relacionado à falha por transbordamento, Figura 5.15, os limites máximos e mínimos do intervalo de confiança não são perceptíveis, ficando uma curva sobreposta a outra.

Figura 5.15 – Função distribuição acumulada de falhas para transbordamento



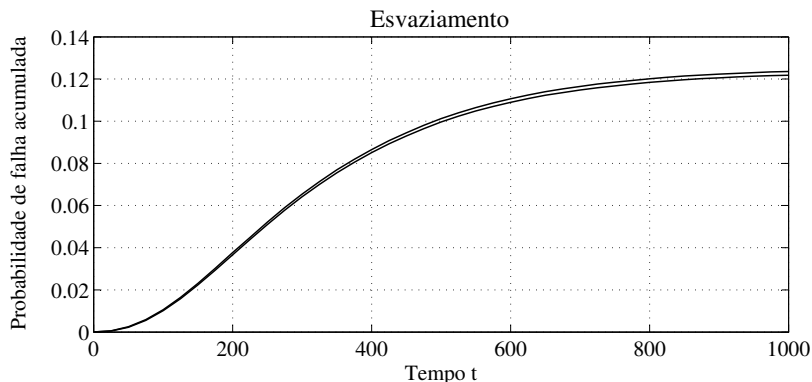
Já no gráfico referente à falha por esvaziamento, Figura 5.16, por ter outra escala nos eixos das ordenadas, os limites máximos e mínimos ainda que bem próximos, são visíveis. Todavia, a dispersão dos valores referente à falha por esvaziamento é maior que a falha por transbordamento.

Na seção seguinte, o problema é resolvido com o uso de redes de petri. Posteriormente, os resultados obtidos com a metodologia ACoDi e redes de petri são comparados.

5.7 ANÁLISE COM REDES DE PETRI

Nesta seção apresenta-se a análise utilizando redes de petri realizada por Codetta-Raiteri e Bobbio (2006). O autor desenvolve o problema utilizando duas técnicas: Redes de Petri Estocásticas Generalizadas – *Generalized*

Figura 5.16 – Função distribuição acumulada de falhas para esvaziamento



Stochastic Petri Nets (GSPN) – e Redes de Petri Fluidas Estocásticas – *Fluid Stochastic Petri Nets* (FSPN).

A Figura 5.17 apresenta o modelo com redes de petri estocásticas generalizadas (GSPN) onde o acompanhamento do comportamento do sistema é feito por meio das fichas (marcas) dentro da rede.

Inicialmente, as fichas estão na posição onde a configuração do sistema indica a operação normal de funcionamento, ou seja, sem falhas, bomba P1 ligada, P2 desligada e válvula V ligada. O nível do reservatório se encontra na posição 0, ou seja, com quatro fichas em “Level”. A relação entre os níveis e a sua discretização para o modelo GSPN estão apresentadas no Quadro 5.5.

Cada um dos componentes pode estar no estado ligado (“on”), desligado (“off”) ou travado (“stuck”), que é definido pela posição da ficha.

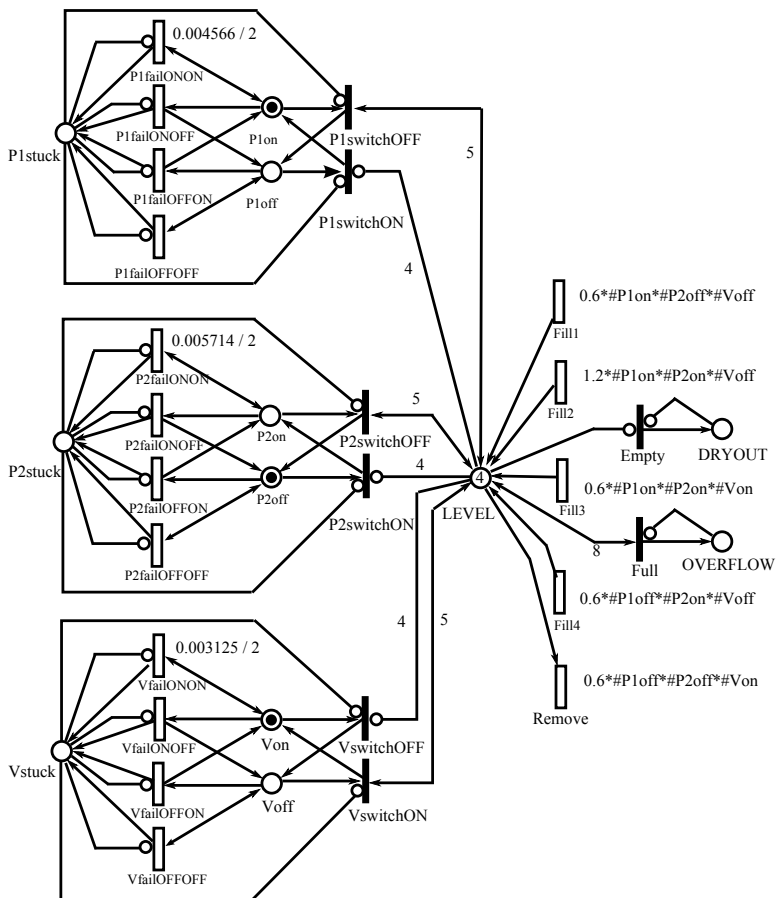
Ao observar a rede, percebe-se que as taxas de falha dos componentes¹ foram divididas por dois. Isso porque nessa análise está sendo considerado que uma parcela da taxa é destinada para falha aberta – componente trava na posição ligado – e outra para falha fechada, quando o componente trava na posição desligado.

As variações do nível do reservatório são modeladas por cinco transições, indicadas por: Fill1, Fill2, Fill3, Fill4 e Remove. Os estados dos componentes (ligado/desligado) influenciam nessas transições e causam a variação do nível do reservatório. Quando o nível do reservatório chega em zero, uma ficha é adicionada na variável DRYOUT. Em contrapartida, se o nível do reservatório atingir valor oito, uma ficha é adicionada na variável OVERFLOW.

A Figura 5.18 corresponde ao modelo de redes de petri fluidas estocásticas (FSPN). Esta ferramenta, além de possuir os elementos utilizados nas redes de petri estocásticas generalizadas (GSPN), possui arcos e posições de rede que podem repre-

¹Corresponde à taxa de transição do estado de componente bom para falha.

Figura 5.17 – Modelo do sistema com GSPN



Fonte: Codetta-Raiteri e Bobbio (2006)

sentar variáveis contínuas como: nível, temperatura e pressão. Os arcos adicionais, encontrados no modelo FSPN, representam tubos ou canalizações. As funções delta de Dirac são utilizadas para executar uma transição quando o nível atinge um determinado valor.

Na modelagem por GSPN e FSPN os níveis do reservatório, foram discretizados de acordo com o Quadro 5.5. Na modelagem FSPN a nova posição de rede “L” representa o nível de líquido no reservatório que, de acordo com o Quadro 5.5, pode variar de 0 até 6. Os arcos adicionais estão representados na figura por setas duplas, \Rightarrow , indicam tubos e modelam a ação das bombas e da válvula sobre o nível

Quadro 5.5 – Discretização do nível H

H	Condição	# fichas Level (GSPN)	Level (FSPN)
>+3	Transbordamento	8	
+3	HLP	7	6
+2		6	5
+1	HLB	5	4
0	Nível inicial	4	3
-1	HLA	3	2
-2		2	1
-3	HLV	1	0
<-3	Esvaziamento	0	

Fonte: Adaptado de Codetta-Raiteri e Bobbio (2006)

do reservatório.

5.8 ANÁLISE COMPARATIVA ENTRE OS RESULTADOS

A presente seção traz os resultados da implementação computacional e os valores obtidos comparados às metodologias GSPN e FSPN (CODETTA-RAITERI; BOBBIO, 2006).

5.8.1 Quanto à implementação computacional

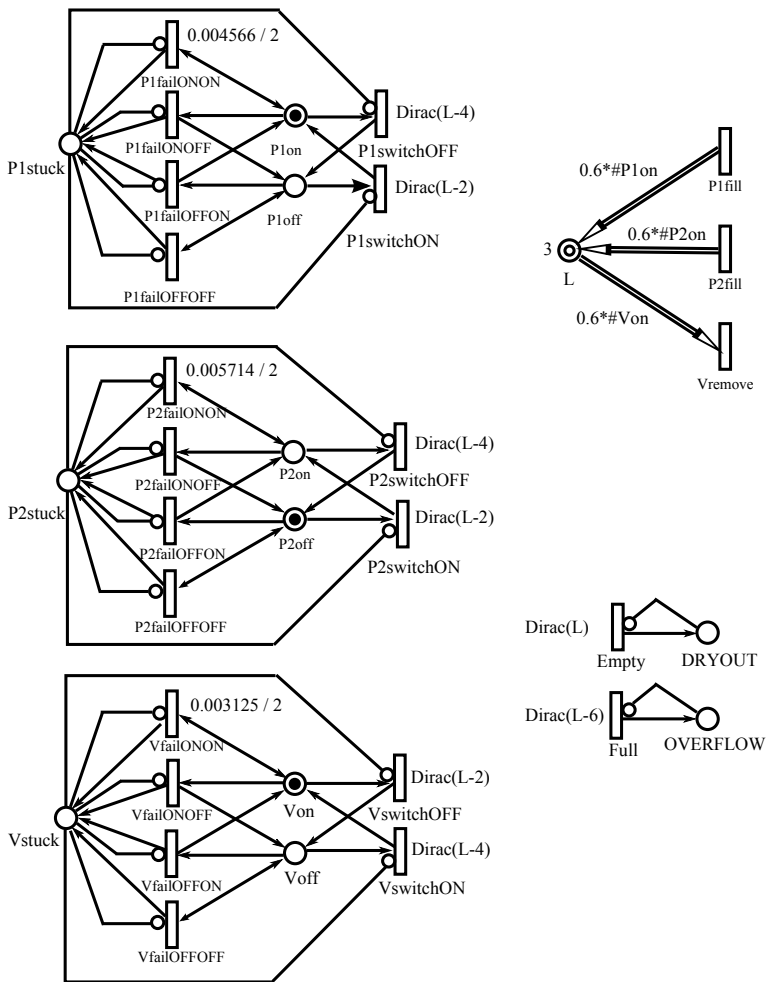
A implementação computacional foi realizada no *Matlab*, que possui uma linguagem própria de programação muito semelhante às linguagens C e Pascal. Foi possível perceber que plataforma de programação desenvolvida facilita a implementação de novos componentes do sistema, bem como a inclusão de rotinas como, por exemplo, para a execução de manutenção no sistema.

Nesta etapa, os resultados foram comparados considerando que os componentes não são reparáveis. No Apêndice C estão os resultados de uma simulação para os componentes reparáveis, sendo a manutenção realizada em série. No entanto, para o caso da simulação considerando manutenção em série, não foram encontradas análises na literatura para serem comparadas.

Uma das principais etapas observadas durante o estudo de caso foram:

- A caracterização da falha, ou seja, quais são as condições que o sistema se encontra em falha. No início das análises não se tem muitas informações, assim, esse é um dos passos principais, ter de forma clara as condições que conduzem o sistema a falha.

Figura 5.18 – Modelo do sistema com FSPN



Fonte: Codetta-Raiteri e Bobbio (2006)

- O desenvolvimento de gráficos que representem o comportamento dinâmico do sistema de forma manual. Neste momento são descritos as mudanças de estados dos componentes ao longo do tempo, em função das variáveis de controle, das falhas e/ou reparo dos componentes.

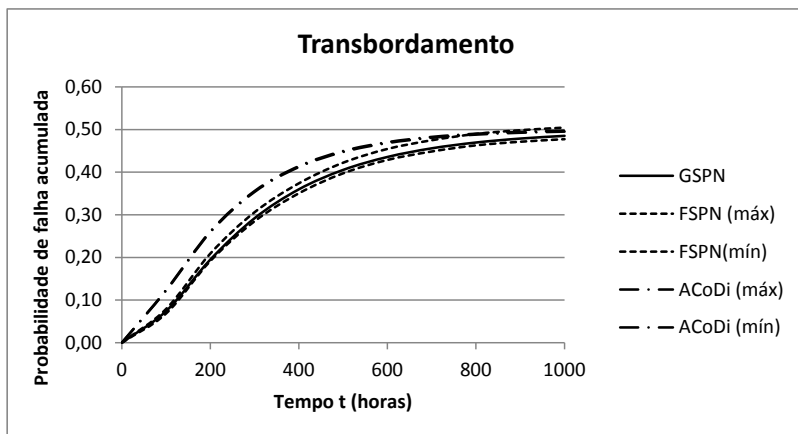
A grande vantagem da metodologia está na flexibilidade da implementação, podendo ser realizada em diferentes linguagens de programação. Vale salientar que as

linguagens de programação com filosofia orientadas a objeto potencializam a implementação de novas rotinas.

5.8.2 Resultados numéricos

Os resultados obtidos com as redes de petri estão apresentados junto com os da metodologia ACoDi. A Figura 5.19 apresenta a probabilidade de falha acumulada considerando o transbordamento do reservatório ao longo do tempo. Os valores obtidos com a metodologia ACoDi, inicialmente, são maiores que os valores obtidos com as redes de petri. No entanto, percebe-se uma convergência na medida que os valores se aproximam do tempo de missão, $t = 1000$ h.

Figura 5.19 – Função distribuição acumulada de falhas para transbordamento



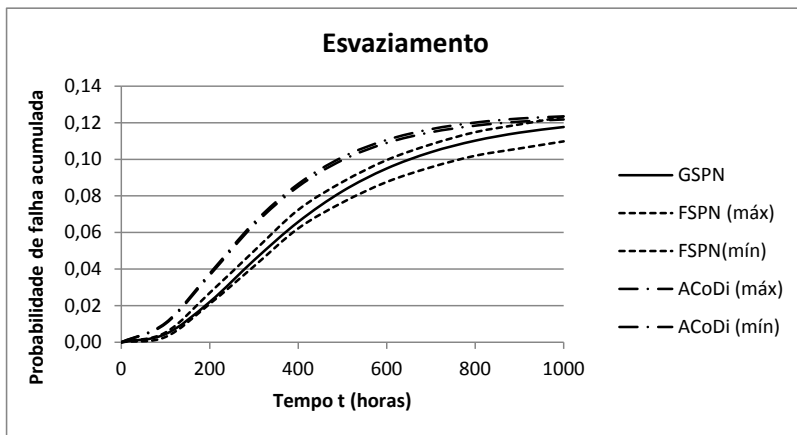
A Figura 5.20 apresenta a probabilidade de falha acumulada considerando o esvaziamento do reservatório ao longo do tempo. Nesse gráfico, também se percebe que há uma diferença inicial, mas quando os valores se aproximam do tempo de missão $t = 1000$ h, essa diferença se reduz consideravelmente.

Algumas inferências foram pensadas para avaliar as diferenças entre os resultados:

1. O uso de variáveis de precisão simples (*float*), precisão dupla (*double*) bem como os arredondamentos utilizados na programação podem ter influência.
2. O *software* gerador de números aleatórios do Matlab pode também influenciar nos resultados. É preciso um estudo nos algoritmos e modelos para geração de números aleatórios e pseudoaleatórios utilizados pelo programa.

As hipóteses levantadas (1 e 2) podem ter influência para os tempos de missão abaixo de 500 horas. No entanto, na medida que o tempo de missão aumenta, tem-se um período disponível maior para que ocorram os comportamentos dinâmicos do

Figura 5.20 – Função distribuição acumulada de falhas para esvaziamento



sistema (falhas e mudanças de estados dos componentes comandados pelo controlador). Neste caso, as diferenças numéricas de implementação acabam tendo menos influência, em comparação com a dinâmica do sistema.

Em função do objetivo da tese, embora tenha-se pesquisado para mitigar as diferenças, considera-se que a mesma não é significativa para o objeto da pesquisa, tendo em vista que a hipótese mais provável é que o problema seja de modelamento matemático e computacional, e não de engenharia.

Os valores obtidos com as redes de petri estocásticas generalizada (GSPN) são analíticos. Por este motivo, estes foram usados para verificar o coeficiente de correlação, R^2 , comparando-se com os resultados da metodologia ACoDi. A Figura 5.21 apresenta um gráfico que relaciona os valores do modelo GSPN e da metodologia para o caso de falha por transbordamento do reservatório. O valor do coeficiente de correlação está junto ao gráfico, $R^2 = 0,9709$. Ou seja, as variações dos valores obtidos com a metodologia são explicados em 97,09% pela variação dos valores obtidos com a GSPN.

Da mesma forma, a Figura 5.22 apresenta um gráfico que relaciona os valores do modelo GSPN com os obtidos com a metodologia ACoDi, sendo considerada a falha por esvaziamento do reservatório. O valor obtido foi $R^2 = 0,9635$, ou seja, os valores obtidos com a metodologia são explicados com 96,35% dos valores obtidos com a GSPN.

Ao comparar os valores médios obtidos com a metodologia ACoDi, com os valores obtidos com o modelo GSPN, para o tempo $t = 1000$ h, calculou-se um erro relativo de 2,3% para falha por transbordamento e 4,2% para esvaziamento. Os valores são satisfatórios, tendo em vista que são os valores mais baixos justamente no tempo de missão desejado. Os valores dos resultados, tanto da metodologia quanto das redes de petri, estão organizados em tabelas e podem ser vistos no Apêndice B.

Por outro lado, para os valores de t baixos, em torno de 100 h observou-se uma

Figura 5.21 – Correlação entre os pontos – Transbordamento

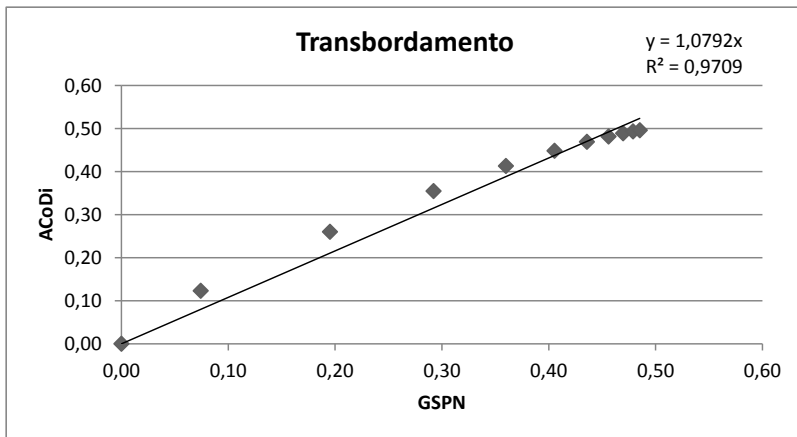
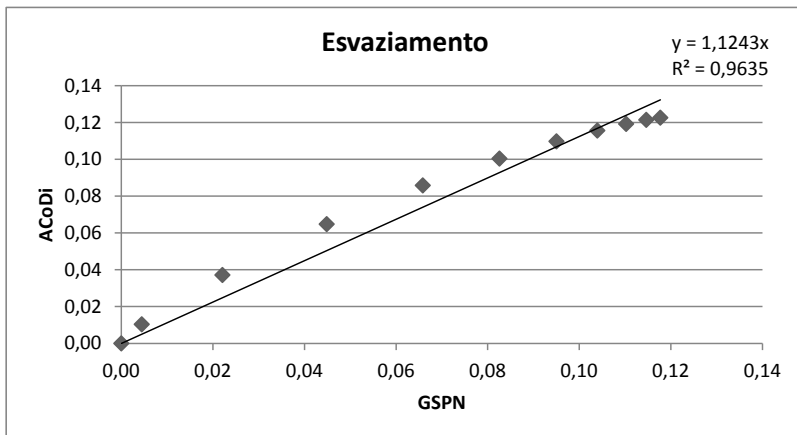


Figura 5.22 – Correlação entre os pontos – Esvaziamento



diferença mais acentuada entre os valores da metodologia em relação aos obtidos com o modelo GSPN. A diferença decai rapidamente alcançando 4,2% (transbordamento) e 2,3% (esvaziamento) no tempo $t = 1000$ h. Esse comportamento ainda deve ser estudado, visando melhorar os resultados para os tempos iniciais.

5.9 CONSIDERAÇÕES DO CAPÍTULO

O presente capítulo apresentou a aplicação da metodologia ACoDi para um problema clássico. Observou-se que os valores obtidos pela metodologia ACoDi é mais conservativo, na faixa 4,2% para esvaziamento e 2,3% para esvaziamento. Este fato poderia ser interpretado para a análise de risco em sistemas. Como já comentado, mais casos ainda precisam ser estudados para adquirir mais confiança sobre a proposição.

Contudo permite-se afirmar que a solução apresentada, traz no desenvolvimento a aderência a uma metodologia de projeto, e por isso poderá ser muito apropriada aos projetistas que desenvolvem produtos ou fazem atualizações buscando melhorar a confiabilidade e redução dos riscos existentes nos sistemas já em operação.

A etapa que mais demandou tempo no desenvolvimento da análise de confiabilidade dinâmica do reservatório foi implementação computacional. A utilização dos relatórios que descrevem a simulação ponto a ponto, junto com os gráficos que apresentam o comportamento dinâmico da variável de estado do sistema foram fundamentais para as validações iniciais do modelo.

Cada histograma de falhas foi gerado com 10 mil testes, sendo que o resultado de cada teste poderia ser: sucesso, transbordamento ou esvaziamento do reservatório. O tempo de processamento de 10 mil testes foi de aproximadamente sete minutos, sendo a configuração do computador: Windows Vista, Processador Intel Core 2 Duo T7500 (2.2GHz, 4MB L2 Cache, 800MHz), Memória de 3GB DDR2 667MHz. Uma das razões para o rápido processamento é que o incremento de tempo, Δt , é variável. Na simulação, busca-se identificar qual será o próximo evento (falha, reparo, nível) e quando irá ocorrer. Consequentemente, a execução da simulação se torna muito mais rápido do que um incremento de tempo constante, que se for muito grande, corre-se o risco de perder algum evento.

A dispersão dos histogramas foi feita com 100 histogramas para cada falha, sendo considerada um intervalo de confiança para 99%. Ao observar os gráficos percebe-se que os valores tiveram pouca dispersão. Por causa disso, permite-se para futuras simulações, realizar uma quantidade de testes menor.

6 APLICAÇÃO EM UM SISTEMA REAL

Nesta seção é apresentado um estudo de caso realizado em um sistema real. A aplicação foi realizada em um sistema de governo convencional de um navio para transporte de produtos derivados de petróleo que opera na costa brasileira.

Entre os vários sistemas constituintes do navio petroleiro, a análise foi realizada no sistema de governo do leme, denominada de máquina do leme, que é comandado hidráulicamente.

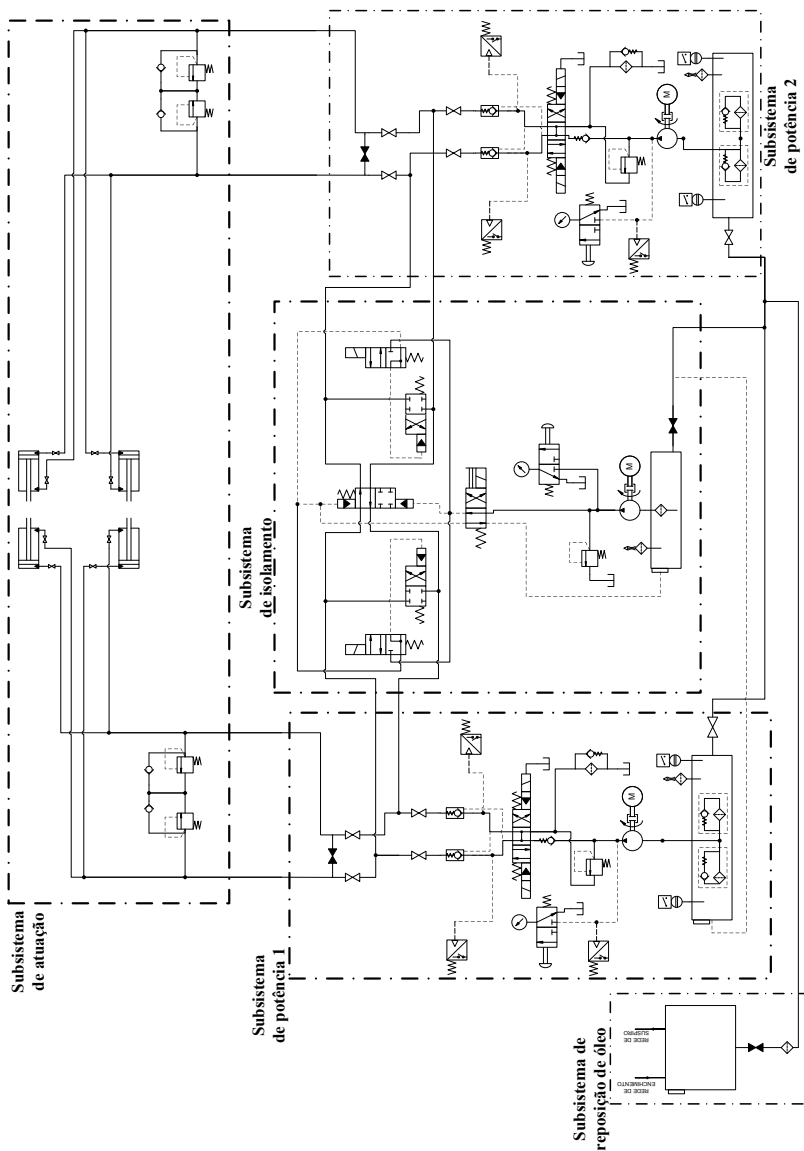
6.1 ETAPA 1: ANÁLISE INICIAL DO SISTEMA TÉCNICO PARA CONFIABILIDADE DINÂMICA

A Figura 6.1 apresenta o circuito hidráulico do sistema de governo do leme do navio. Em uma análise de confiabilidade estática considera-se que a falha do sistema ocorre no momento em que este fica indisponível, ou seja, no instante em que a embarcação fica a deriva. No final deste capítulo, os resultados com o uso da metodologia ACoDi são comparados com os valores obtidos com a análise de confiabilidade estática.

No entanto, é possível realizar uma análise em que se pode considerar um tempo de limite em que a embarcação fica sem o sistema de governo. Deseja-se avaliar qual a confiabilidade do sistema para os tempos limites de 40, 20, 10, 5 e 2 minutos.

Portanto, somente será considerado “falha do sistema do leme” se houver indisponibilidade da função do leme em um tempo maior que o tempo limite. Desta forma, a realização destas simulações podem ser utilizadas para avaliar a capacidade da equipe de manutenção e de seus procedimentos.

Figura 6.1 – Circuito hidráulico do sistema de governo do leme



Fonte: Sakurada e Andrade (2007)

6.1.1 Atividade 1.1: Análise quanto ao comportamento dinâmico

O sistema possui um comportamento dinâmico do ponto de vista de mudança da configuração do sistema. Dado que ocorre falha no sistema subsistema principal de potência (SP1), entra em operação o subsistema de potência reserva (SP2). Paralelamente, tem início a manutenção de SP1, que após ser recuperado volta a fornecer vazão para o sistema, retornando o subsistema de potência SP2 para a condição de elemento reserva.

Desta forma, o sistema muda de configuração em função das falhas e manutenções dos subsistemas de potência SP1 e SP2.

Outro comportamento dinâmico observado é a vazão fornecida ao sistema. Enquanto o subsistema de potência SP1 está sem falha, há vazão disponível a ser fornecida para o sistema. Dado que ocorra a falha, enquanto não é realizada a comutação para SP2, o sistema fica com vazão disponível nula. Após a comutação para SP2, o sistema volta a ter vazão disponível. Assim, a vazão disponível para o sistema pode ter o valor nominal de projeto ou pode ser nula, dependendo dos estados dos subsistemas SP1/SP2 e também do tempo de transição de um sistema para outro.

6.1.2 Atividade 1.2: Análise da criticidade do sistema

Os navios petroleiros são sistemas que possuem criticidade elevada tendo em vista as consequências que podem ocorrer em caso de um incidente. Entre os vários sistemas existentes na embarcação, o sistema de governo do leme é um dos mais importantes. A indisponibilidade da função do sistema de governo pode conduzir a efeitos catastróficos, sendo uma ameaça à segurança do homem e do meio ambiente.

6.1.3 Atividade 1.3: Análise da disponibilidade do sistema

A função do sistema de governo é constantemente exigida, principalmente, na entrada de canais ou em baías. Durante a navegação nessas regiões é exigida elevada disponibilidade do sistema, tendo em vista o limitado espaço para manobras, proximidade com outras embarcações, estruturas portuárias, etc.

6.1.4 Atividade 1.4: Análise do sistema

Com as informações levantadas nas atividades 1.1, 1.2 e 1.3 conclui-se que é um sistema dinâmico, crítico em que é exigida elevada disponibilidade. Portanto, de acordo com a Figura 4.8, este sistema se encontra na região R4 onde o uso da análise de confiabilidade dinâmica é obrigatório.

6.2 ETAPA 2: DEFINIÇÃO DA EQUIPE

O sistema de governo do leme foi analisado em um projeto do NeDIP – do Departamento de Engenharia Mecânica da UFSC – com LabRisco – do Departamento de Engenharia Naval e Oceânica da USP. Neste desenvolvimento, foram realizadas consultas com técnicos da embarcação e engenheiros de ambas as instituições. Com isso, foi possível obter informações sobre o funcionamento da máquina do leme.

6.3 ETAPA 3: ANÁLISE DO SISTEMA, SUBSISTEMA E COMPONENTES

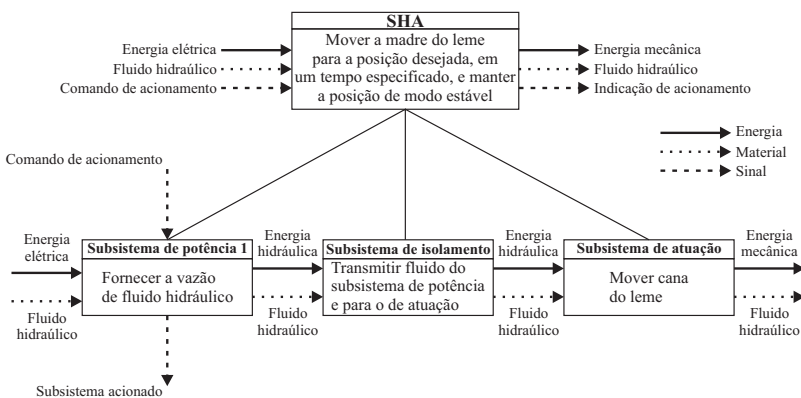
Esta etapa é constituída das seguintes atividades:

- Atividade 3.1: Desdobramento das funções do sistema
- Atividade 3.2: Caracterização dos subsistemas e componentes
- Atividade 3.3: Descrição comportamental do sistema

6.3.1 Atividade 3.1: Desdobramento das funções do sistema

O desdobramento funcional do sistema de governo foi apresentado no trabalho de Kagueiama (2012), Figura 6.2. A função global o principal do sistema foi descrita como: Mover a madre do leme para a posição desejada, em um tempo especificado e manter a posição de modo estável.

Figura 6.2 – Análise funcional do SHA para os subsistemas de primeiro nível



Fonte: Kagueiama (2012)

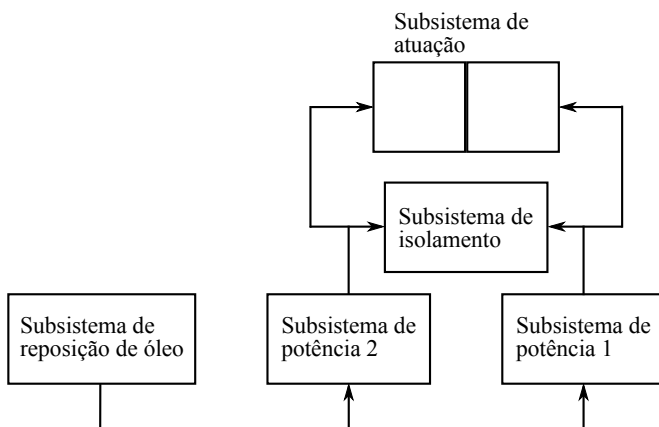
Com o desdobramento da função global foram identificados os principais

subsistemas presentes: subsistema de potência, de isolamento, de reposição de óleo e o de atuação.

- Subsistema de potência – É o subsistema que apresenta a maior quantidade de componentes. Fornece vazão para o sistema e é constituído com duas unidades denominadas de SP1 e SP2.
- Subsistema de isolamento – É constituído por um conjunto de válvulas que permite que o sistema possa operar com dois ou quatro cilindros hidráulicos. Este subsistema possui seu próprio reservatório, motor elétrico, bomba e conjunto de válvulas.
- Subsistema de atuação – É constituído por dois pares de cilindros hidráulicos e um conjunto de válvulas de alívio. Convertem a energia hidráulica em energia mecânica atuando sobre a cana do leme.
- Subsistema de reposição de óleo – É constituído de um reservatório de mil litros e válvulas de bloqueio. Tem a função de abastecer os reservatórios dos subsistemas de potência e de isolamento, quando o nível de óleo se encontra muito baixo. Desta forma, esse subsistema somente é acionado durante as ações de manutenção periódica.

Desta forma, o circuito hidráulico apresentado na Figura 6.1 foi organizado em quatro subsistemas, conforme a Figura 6.3.

Figura 6.3 – Diagrama estrutural do sistema hidráulico de acionamento do leme



Fonte: Sakurada e Andrade (2007)

A quantidade de componentes existentes e a função desempenhada pelo subsistema de potência faz com que este subsistema seja o mais importante na movimentação

do leme. Portanto, por uma questão de segurança, os subsistemas SP1 e SP2 são idênticos. Com isso, na ocorrência de falha do subsistema SP1, é realizada a comutação para o subsistema SP2 para garantir a disponibilidade de vazão de óleo.

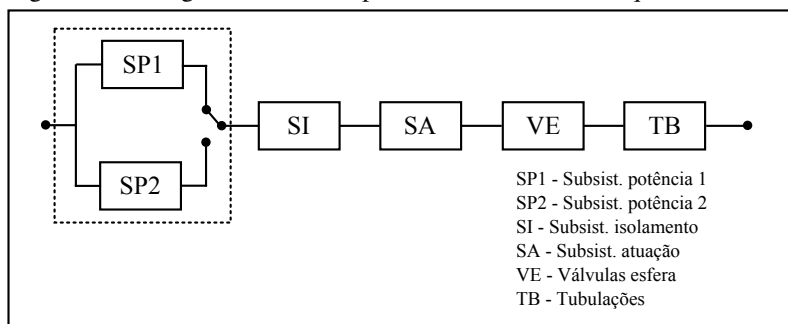
Na análise de confiabilidade Biasotto (2008) não foi considerado o subsistema de reposição de óleo, tendo em vista que é um sistema em paralelo, ligado aos reservatórios de óleo apenas quando é verificado que o nível do óleo está baixo.

Em contrapartida, um conjunto de válvulas esferas (VE) e tubulações (TB) foram incluídas na análise do sistema de governo. As válvulas esfera são acionadas manualmente e são operadas em condições de emergência, quando se deseja isolar alguma parte do sistema do leme, sendo operadas no caso de uma pane elétrica do sistema. Como a ocorrência de falha em alguma dessas válvulas, bem como nas tubulações, pode comprometer a função principal do sistema, tais componentes foram incluídos na análise.

A Figura 6.4 é o diagrama de blocos para análise de confiabilidade do sistema de governo do leme. Nessa configuração, o sistema opera com o subsistema SP1, subsistema de isolamento (SI), subsistema de atuação (SA), conjunto de válvulas esfera (VE) e tubulações (TB).

No caso de uma falha do subsistema SP1, ocorre a comutação para o subsistema SP2, o que torna possível realizar manutenções em SP1 com a máquina do leme ainda em operação. Por outro lado, o mesmo não acontece quando a falha ocorre em SI e SA – nesses casos é necessário que máquina do leme fique fora de operação.

Figura 6.4 – Diagrama de blocos para confiabilidade – Máquina do leme



A partir deste ponto a máquina do leme será tratada como sistema técnico em análise tendo como componentes: SP1, SP2, SI, SA, VE e TB.

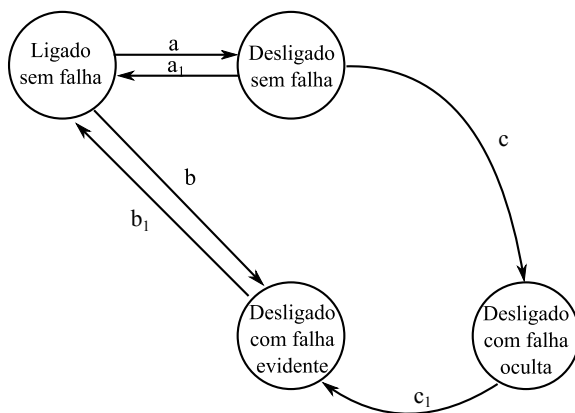
Para a análise de confiabilidade dinâmica, será considerada como variável de controle do sistema o “tempo que o sistema fica sem vazão disponível”, t_{sv} . Tal situação ocorre quando houver falhas nos componentes SP1 e SP2. A vazão não é fornecida para os cilindros a todo momento. Ou seja, quando os cilindros estão parados, a vazão gerada pela bomba hidráulica é devolvida para o reservatório. Todavia, se houver necessidade de movimentação, a válvula direcional 4/3 vias alimentará os cilindros hidráulicos. Por causa disso, utiliza-se o termo “vazão disponível”, que é a vazão gerada pelo sistema e pode, ou não, ser direcionada para os cilindros.

A partir disso, define-se a falha do sistema: será quando o tempo que o sistema fica sem vazão for maior que o tempo limite, ou seja, se $t_{sv} > t_{limite}$ tem-se a falha no sistema. As simulações serão realizadas para os tempo limites, t_{limite} : 40, 30, 20, 10, 5 e 2 minutos.

6.3.2 Atividade 3.2: Caracterização dos subsistemas e componentes

A Figura 6.5 apresenta os possíveis estados dos componentes reparáveis, ou seja, SP1 e SP2. Assim, esses componentes quando estão ligados, fornecendo vazão, podem parar de fornecer – caminho “b”. Caso estejam desligados, podem ter uma falha oculta – caminho “c”. Desta forma, quando houver uma demanda será percebida a ocorrência de uma falha oculta. Nesse caso, a falha irá deixar de ser oculta e será uma falha comum – caminho “c₁”.

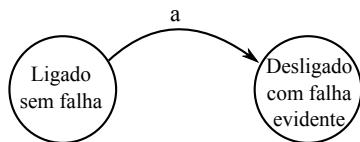
Figura 6.5 – Estados dos componentes reparáveis



Não serão consideradas falhas do tipo: entrar em operação quando não deveria. Por causa disso, não há falhas evidentes do tipo “ligado”. Desta forma, todas as falhas que ocorrem com os componentes SP1 e SP2 são no sentido de não fornecer vazão.

Os componentes SI, SA, VE e TB só podem ser reparados quando a máquina do leme estiver fora de operação. Assim, serão tratados como componentes não reparáveis. A Figura 6.6 representa os possíveis estados desses componentes: ligado (sem falha) e desligado (com falha). Como não são reparáveis, a falha desses componentes conduzem à falha do sistema.

Figura 6.6 – Estados dos componentes não reparáveis



6.3.3 Atividade 3.3: Descrição comportamental do sistema

Nesta análise estará sendo verificado se os componentes SP1 e SP2 tem vazão disponível ou não. A partir do momento que ambos os componentes estão em falha, a vazão disponível é nula. Então, o comportamento que será observado nos gráficos gerados na simulação são do tipo degrau, Figura 4.16 (a). Portanto, quando a houver vazão disponível, o valor da variável de controle, Q , será 1. Caso contrário, a o valor de Q será 0.

A equação 6.1 será utilizada para verificar a vazão disponível para o sistema. A vazão pode ser fornecida pelo componente SP1 ou SP2. Assim, quando o componente estiver em operação (ativado) seu valor será igual a 1, do contrário, será 0. O operador deve selecionar se deseja operar com o componente SP1 ou SP2 (SetSP1 ou SetSP2).

As variáveis FuncQ1 e FuncQ2 indicam que o componente está funcionando (1) ou com falha (0).

$$Q = \text{SetSP1} \cdot \text{FuncQ1} + \text{SetSP2} \cdot \text{FuncQ2} \quad (6.1)$$

Assim, para um componente fornecer vazão para o sistema, ele deve estar ativado e ligado. O Quadro 6.1 representa a vazão disponível para o sistema, Q , em função dos componentes SP1 e SP2. Se SP1 estiver com falha FuncQ1 será zero – visto que está desligado –, a mesma consideração é adotada para SP2.

Quadro 6.1 – Vazão disponível para o sistema

Q	SetSP1	FuncQ1	SetSP2	FuncQ2	Observação
1	1	1	0	0	SP1 ativado operando normalmente
1	0	0	1	1	SP2 ativado operando normalmente
0	1	0	0	0	SP1 ativado, mas sem vazão
0	0	0	1	0	SP2 ativado, mas sem vazão

6.4 ETAPA 4: ANÁLISE DA MANUTENÇÃO DO SISTEMA TÉCNICO

6.4.1 Atividade 4.1: Caracterização dos sensores, controlador e atuadores

A detecção de falhas de falhas em SP1 e SP2 ocorre quando os componentes deixam de ter vazão disponível.

O sensor e controlador serão considerados como sendo o mesmo componente nesta simulação. Quando ocorre a falha em SP1 (componente principal), decorre um tempo para ativação de SP2, denominado tempo de comutação.

O tempo de reparo dos componentes (SP1 e SP2) segue uma distribuição exponencial com taxa de reparo sendo 0,2 reparos/hora.

Quando ocorrer a falha de SP1, o papel do controlador nesse sistema será de, simultaneamente, realizar a comutação para SP2 e disparar o comando para manutenção. Após a manutenção de SP1, desliga-se o alarme – já que o sistema retornou à condição normal de operação – e realiza-se a comutação de SP2 para SP1.

6.4.2 Atividade 4.2: Definição das regiões de operação

A Figura 6.7 representa as regiões de operação do sistema: região normal, de emergência e de falha do sistema.

A região normal de operação é quando não há falhas ou para um período de tempo curto sem vazão, no qual é utilizado para realizar a comutação do subsistema de potência principal, SP1, para o subsistema de potência reserva, SP2. Se por algum motivo, o tempo de indisponibilidade do sistema for maior que o tempo de comutação, tem se uma condição de emergência.

No momento em que não há vazão disponível, inicia-se a contagem para verificar se o tempo limite sem vazão será alcançado. Essa situação indica que o sistema se encontra em uma condição de emergência e que está se aproximando da região de falha.

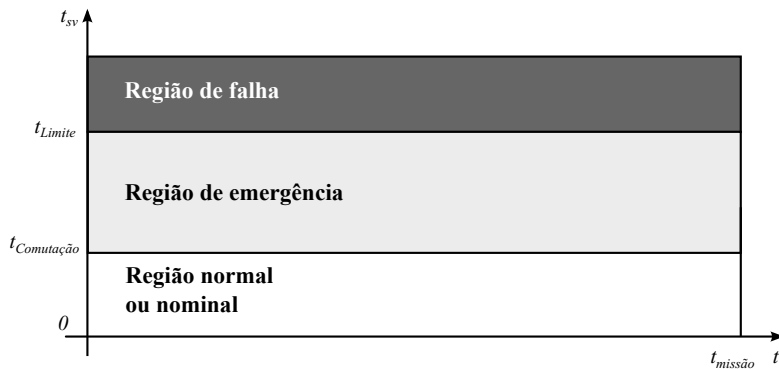
6.4.3 Atividade 4.3: Modelagem do comportamento em função da manutenção

As falhas e reparos de componentes tem influência no comportamento dinâmico da variável de controle, Q , do sistema.

6.4.3.1 Tempo de reação

O tempo de reação aqui será considerado nulo. Ou seja, a partir do momento que ocorrer a falha de um componente principal, inicia se o processo para a comutação

Figura 6.7 – Regiões de operação com tempo limite para falha e comutação



para o componente reserva. Paralelamente, inicia-se o processo de manutenção dos componentes em falha.

O tempo de comutação foi considerado constante, sendo atribuído o valor de 30 segundos. O valor foi atribuído em função da facilidade de ativação de um subsistema para outro.

6.4.3.2 Atuação sobre o avanço da variável de controle

No momento que vazão disponível for nula, percebe-se que há falha do sistema. Consequentemente, tem início as ações de manutenção do sistema, que são: comutação para o componente reserva e início da manutenção do componente principal.

Portanto, ocorre o monitoramento de duas variáveis: a vazão (Q) e o tempo que o sistema fica com vazão nula (t_{sv}). Mas o acompanhamento da variável t_{sv} só é realizado enquanto $Q = 0$.

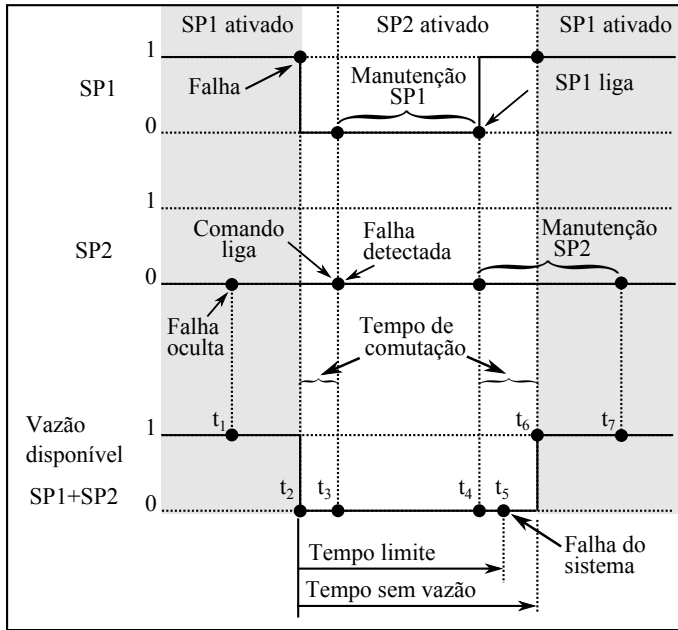
6.4.3.3 Manutenção preditiva com o sistema em operação

Entre os componentes do sistema de governo, somente será realizada manutenção preditiva em SP1 e SP2. Pois, enquanto um destes componentes estiver em manutenção, o outro pode estar suprindo o sistema com vazão de óleo. Para que seja considerada falha do subsistema de potência é necessário que ambos os componentes SP1 e SP2 estejam sem vazão disponível por um tempo maior que o tempo limite, $t_{sv} > t_{limite}$.

Os outros componentes SI, SA, VE e TB, por não possuírem elementos redundantes, necessitam que o sistema seja desligado para a realização de manutenções. Assim, na falha de um destes componentes, será considerada a falha do sistema.

A manutenção será em série, ou seja, se ambos os componentes (SP1 e SP2) estiverem em falha, a manutenção será realizada inicialmente em SP1 e posteriormente em SP2. A Figura 6.8 ilustra essa situação onde inicialmente é feita a manutenção de SP1, posteriormente de SP2. As regiões em cinza destacam os instantes que SP1 está ativado e SP2 desativado.

Figura 6.8 – Comportamento com falha oculta



Observa-se na Figura 6.8 que SP2 está com falha oculta no tempo t_1 . O componente SP1 deixa de funcionar em t_2 , exigindo a comutação para SP2 – a falha no componente reserva será percebida somente neste momento. É um cenário crítico, onde ambos os componentes responsáveis por fornecer vazão estão em falha. No entanto, se um dos componentes for recuperado e ativado antes do tempo limite, t_5 , o sistema estará salvo. Neste exemplo ocorreu a falha do sistema porque o tempo que o sistema voltou a ter vazão foi em t_6 , ultrapassando o tempo limite t_5 .

No exemplo, destaca-se que embora um dos componentes tenham sido reparados antes do tempo limite, ocorreu a falha no sistema pois a comutação demandou um tempo que ultrapassou o tempo limite.

6.4.4 Falhas ocultas

As falhas ocultas podem ocorrer somente com SP2, sendo do tipo desligado. Esta falha deixa de ser oculta e passa a ser uma falha evidente ao tentar ligar o componente. Na Figura 6.8 a falha oculta ocorreu em t_1 e foi percebida somente em t_3 , após o tempo de comutação.

6.5 ETAPA 5: MODELAGEM E SIMULAÇÃO

A implementação computacional será realizada no *software* Matlab. A estrutura desenvolvida para o estudo de caso do problema clássico (controle do nível do reservatório), será usada como base para este desenvolvimento.

6.6 ATIVIDADE 5.1: REPRESENTAÇÃO DO COMPORTAMENTO DINÂMICO DO SISTEMA

O comportamento dinâmico que será observado são, principalmente, os estados dos componentes SP1 e SP2. As falhas e manutenções sobre estes componentes são os principais responsáveis pelo comportamento do sistema de governo do leme. Alguns diagramas comportamentais do sistema, Figuras 6.8 e 6.9, serão utilizadas para compreender o comportamento do sistema.

Na Figura 6.9 é possível visualizar um cenário no qual ocorre a falha de SP1 no tempo t_1 . A comutação entre os componentes ocorre nos intervalos t_1-t_2 e t_3-t_4 . O sistema volta a ser alimentado por SP1 em t_4 . Destaca-se que a ativação de um componente para outro não é realizada instantaneamente, deve-se considerar o “tempo de comutação”.

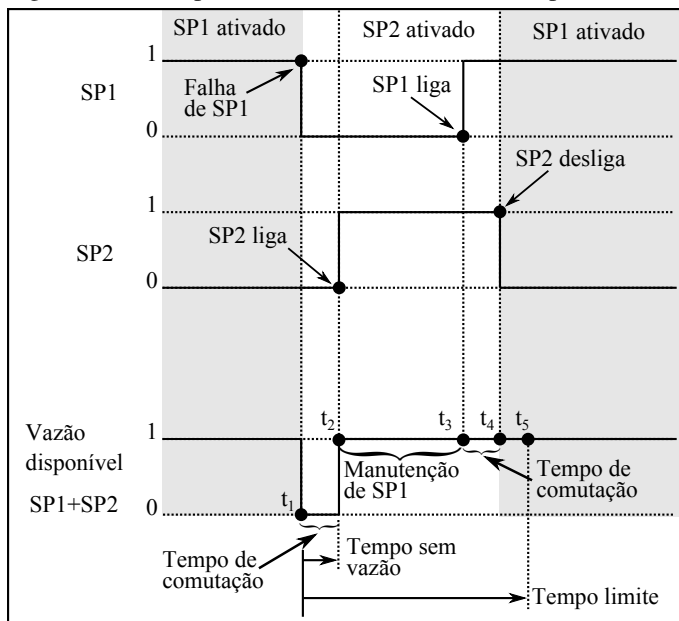
No intervalo t_3-t_4 ambos os componentes estão em funcionamento. No entanto, somente SP2 está ativado – fornecendo vazão para o sistema. O tempo t_5 representa o tempo máximo que o sistema pode ficar sem vazão. Nesse caso, como foi feita a comutação com o componente reserva, o tempo que o sistema ficou sem fornecimento de óleo é muito menor que o tempo limite. A vazão disponível para o sistema será monitorada, junto com os tempos de comutação e reparo dos componentes.

6.7 ATIVIDADE 5.2: ESTRUTURA PARA IMPLEMENTAÇÃO

A estrutura para implementação do *software* segue conforme descrito na proposta da metodologia, ou seja, utiliza o fluxograma apresentado na Figura 4.32 como estrutura geral para a implementação do *software*; os tempos de falha e de reparo são obtidos por sorteio, posteriormente é feita a ordenação das falhas conforme a ordem cronológica de ocorrência; e o processo é dirigido a eventos.

As variáveis armazenadas nos componentes reparáveis são:

Figura 6.9 – Comportamento do sistema e dos componentes



- Nome: SP1 e SP2
- A condição atual: sem falha ligado, sem falha desligado, com falha evidente, com falha oculta
- O último estado definido pelo controlador
- Taxa de falha: $93,9133 \cdot 10^{-6}$ falhas/hora. Valor obtido do relatório técnico de Biasotto (2008)
- Taxa de reparo: 0,2 reparos/hora
- Tempo de reparo: Valor obtido a partir da taxa de reparo
- Valor de saída: ligado (1) ou desligado (0)
- Próxima condição: Falha ou reparo
 - As variáveis armazenadas nos componentes não reparáveis são:
- Nome: SI, SA, VE e TB
- A condição atual: ligado sem falha, desligado com falha comum
- O último estado definido pelo controlador. Não se aplica aqui, visto que o componente não é reparável
- Taxa de falha: Valores obtidos do relatório técnico de Biasotto (2008)
 - SI: $20,6187 \cdot 10^{-6}$ falhas/hora

SA: $4,3304 \cdot 10^{-6}$ falhas/hora

VE: $1,7366 \cdot 10^{-6}$ falhas/hora

TB: $1,0435 \cdot 10^{-6}$ falhas/hora

- Taxa de reparo: Não se aplica aqui para estes componentes
- Tempo de reparo. Não se aplica aqui para estes componentes
- Valor de saída: ligado (1) ou desligado (0)
- Próxima condição: Falha evidente

6.8 ETAPA 6: ANÁLISE DE RESULTADOS

6.8.1 Atividade 6.1: Geração dos relatórios ponto a ponto e cenários de falha

Os relatórios ponto a ponto e cenários de falha são usados para verificar apenas a coerência do comportamento dinâmico. Dado que os cenários e relatórios apresentam comportamentos avaliados como adequados, esta função não é mais executada. Pois, em uma simulação com 10 mil testes, seriam gerados 10 mil relatórios e gráficos, exigindo muito do processamento computacional o que tornaria a simulação muito lenta.

Os relatórios ponto a ponto são textos gerados automaticamente e trazem informação de cada ponto do gráfico de cenário de falhas. A Figura 6.10 traz a parte inicial do relatório ponto a ponto para a simulação apresentada na Figura 6.11. Cada ponto no gráfico é descrito no relatório como etapa, sendo informado o subsistema de potência que está ativo, valor da variável de controle Q , tempos de falha de reparo dos componentes e o evento que irá ocorrer na próxima etapa.

Figura 6.10 – Parte do relatório ponto a ponto para a Figura 6.11

```

***** Etapa = 1 *****
***** t = 0.00 h *****
----- Estado dos componentes SP1 e SP2 -----
SP1 = 1 (0)Desligado (1)Ligado
SP2 = 0
-----

----- Condição dos componentes -----
SP1.Failure = 0
SP2.Failure = 0
SI.Failure = 0
SA.Failure = 0
TB.Failure = 0
VE.Failure = 0
-----

t = 0.00 h => Q = 1.00 dQ/dt = 0.0 m/h
System.RepairAlarm = 0
Proximo evento ==> Failure (stuck off):SP1 em t= 2142.25 h.

SP1 = 2142.25 h ==> Falha tipo 0 ==> TimeToRepair = 6.72 h
SP2 = 5539.96 h ==> Falha tipo 0 ==> TimeToRepair = 18.97 h
SI = 41469.93 h ==> Falha tipo 0 ==> TimeToRepair = Inf h
SA = 421056.85 h ==> Falha tipo 0 ==> TimeToRepair = Inf h
TB = 491891.91 h ==> Falha tipo 0 ==> TimeToRepair = Inf h
VE = 4580379.86 h ==> Falha tipo 0 ==> TimeToRepair = Inf h
-----

***** Etapa = 2 *****
***** t = 2142.25 h *****
----- Estado dos componentes SP1 e SP2 -----
SP1 = 0 (0)Desligado (1)Ligado
SP2 = 0
-----

----- Condição dos componentes -----
SP1.Failure = 1 Falha desligado
SP2.Failure = 0
SI.Failure = 0
SA.Failure = 0
TB.Failure = 0
VE.Failure = 0
-----

t = 2142.25 h => Q = 1.00 dQ/dt = 0.0 m/h
System.RepairAlarm = 0
Proximo evento ==> Ajuste de ponto em t= 2142.25 h.

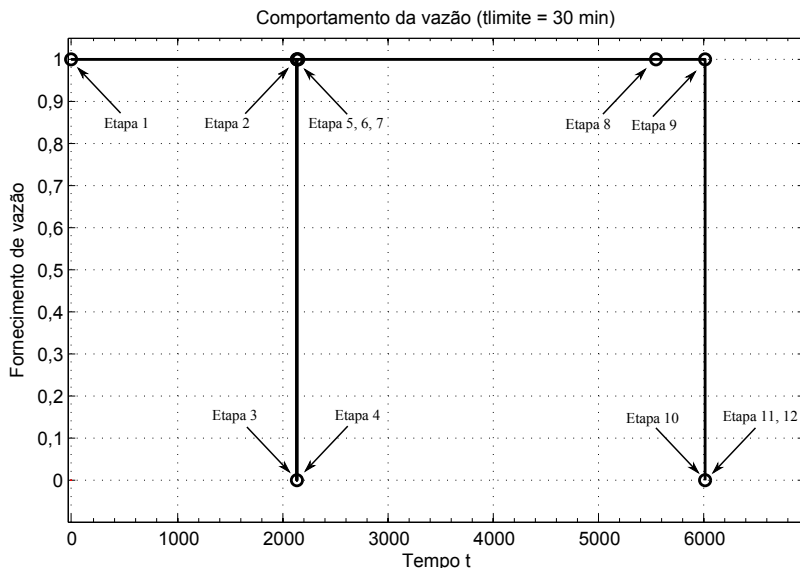
SP1 = 2142.25 h ==> Falha tipo 0 ==> TimeToRepair = 6.72 h
SP2 = 5539.96 h ==> Falha tipo 0 ==> TimeToRepair = 18.97 h
SI = 41469.93 h ==> Falha tipo 0 ==> TimeToRepair = Inf h
SA = 421056.85 h ==> Falha tipo 0 ==> TimeToRepair = Inf h
TB = 491891.91 h ==> Falha tipo 0 ==> TimeToRepair = Inf h
VE = 4580379.86 h ==> Falha tipo 0 ==> TimeToRepair = Inf h
-----

```

A Figura 6.11 apresenta um teste realizado para $t_{limite} = 30$ minutos onde estão identificados 12 pontos (etapas). Devido a escala do gráfico, não é possível identificar

alguns pontos, pois ficaram sobrepostos. As Figuras 6.12, 6.13 e 6.14 são ampliações de alguns pontos da Figura 6.11 que não estão visíveis. Assim, uma das características necessárias dos gráficos gerados é que permitam realizar ampliações para melhor visualizar os eventos que ocorrem em tempos muito próximos, que no gráfico geral acabam ficando sobrepostos.

Figura 6.11 – Comportamento dinâmico para simulação para $t_{Limite} = 30$ minutos



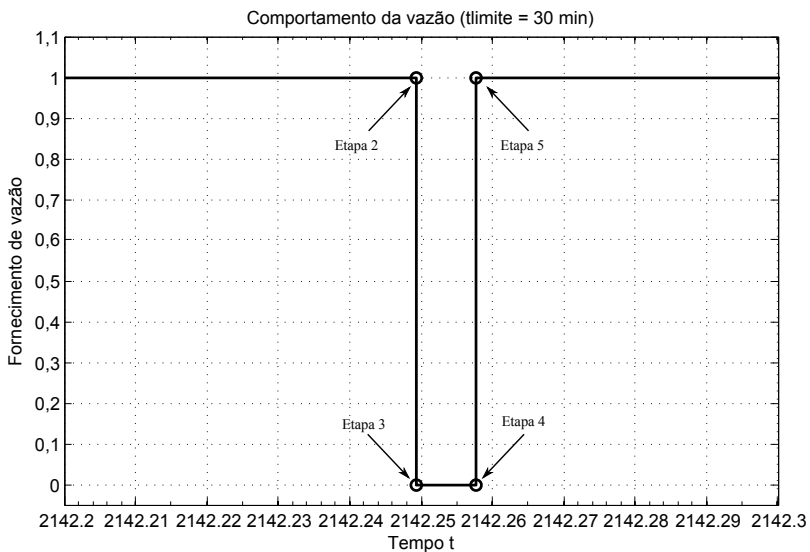
A etapa 1 da simulação ocorre no tempo $t = 0$ e representa o sistema nas condições iniciais de operação, quando não há nenhuma falha no sistema. Na Figura 6.12 é possível visualizar as etapas 2, 3, 4 e 5.

Na etapa 2 ($t = 2142,25$ h) ocorreu a falha de SP1. Como a função que descreve o comportamento é do tipo degrau, para um mesmo tempo t teremos dois valores de Q . Na etapa 2 $Q = 1$ e na etapa 3 ($t = 2142,25$ h) a vazão é nula, $Q = 0$. O tempo de manutenção de SP1 começa a ser contado a partir da falha. O valor calculado foi $t_{reparo} = 6,72$ h, desta forma SP1 estará sem falhas em $t = 2148,98$ h.

Dado que o sistema ficou sem vazão disponível, ocorre a comutação de SP1 para SP2. O tempo de comutação foi considerado fixo, $t_{comutacao} = 30$ s que é equivalente a aproximadamente $8,33 \cdot 10^{-3}$ h. Assim, na etapa 4 ocorre no tempo $t = 2142,26$ h e a vazão disponível ainda é nula. O tempo de comutação é muito pequeno quando comparado com os tempos de falha dos componentes, o que faz com que os pontos no gráfico fiquem sobrepostos.

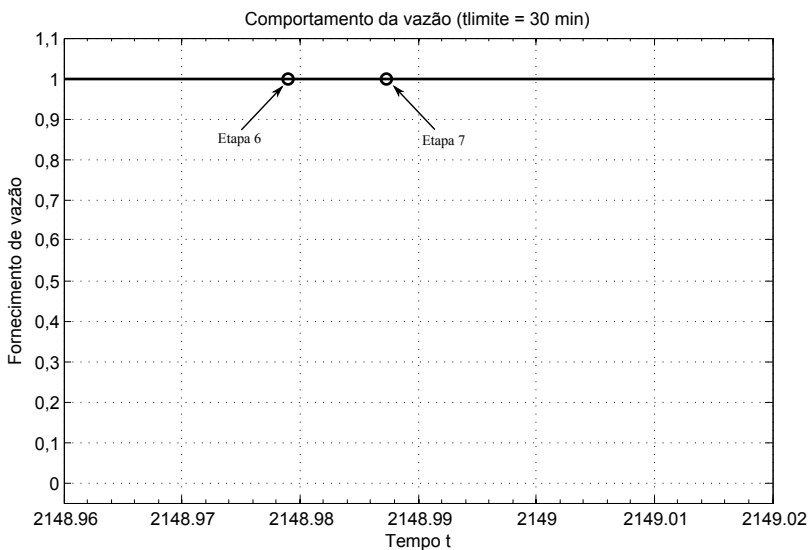
Na etapa 5 ($t = 2142,26$ h) ocorre a recuperação da vazão, ou seja, Q passa do valor 0 para 1. Esta é uma condição de emergência pois o sistema está operando

Figura 6.12 – Ampliação da Figura 6.11 nas etapas 2, 3, 4 e 5 da simulação



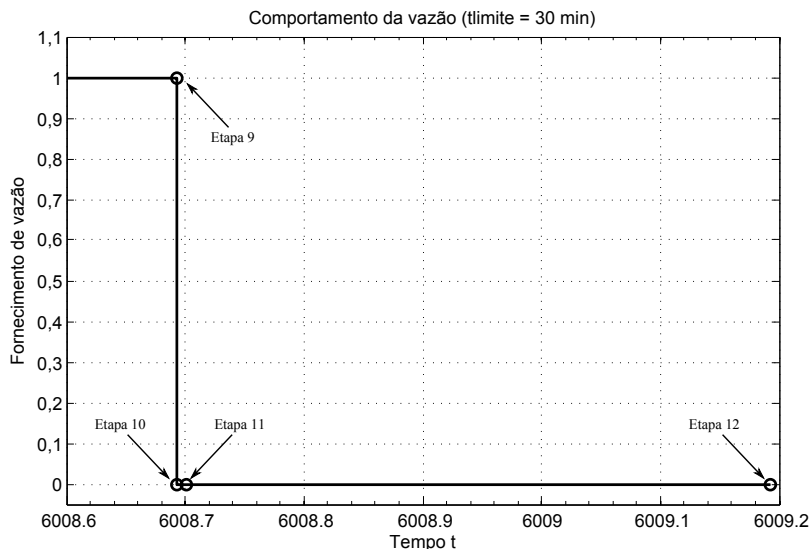
com o componente reserva (SP2) enquanto o componente principal (SP1) está em manutenção.

Figura 6.13 – Ampliação da Figura 6.11 nas etapas 6 e 7 da simulação



Na etapa 6 ($t = 2148,98$ h) é concluída a manutenção de SP1, mas SP2 ainda está ativado. Na etapa 7 (2148,99) h é realizada a comutação de SP2 para e SP1, sendo desativado o componente reserva e ativado o componente principal. As etapas 6 e 7 podem ser visualizadas na Figura 6.13.

Figura 6.14 – Ampliação da Figura 6.11 nas etapas 9, 10, 11 e 12 da simulação



Na etapa 8 ($t = 5539,96$ h), Figura 6.11, ocorre uma falha oculta de SP2. Como é uma falha oculta, a manutenção do componente não é iniciada.

Na etapa 9 ($t = 6008,69$ h), Figura 6.14, ocorre falha de SP1 novamente. Consequentemente, a etapa 10 representa o momento em que a vazão torna-se nula. O novo tempo de reparo de SP1 é igual a $t_{reparo} = 1,78$ h. Assim, dado que ocorreu a falha evidente de SP1, tem-se o início da manutenção, que será concluída no tempo $t = 6010,47$ h.

A etapa 11 ($t = 6008,70$ h) representa o momento em que ocorre a comutação de SP1 para SP2. No entanto, SP2 está com falha oculta que agora se torna uma falha evidente. O sistema de governo está com SP1 e SP2 em falha.

O tempo limite para recuperar um dos subsistemas de potência é em $t = 6009,19$ h. Como a manutenção de SP1 será concluída somente em $t = 6010,47$, fica caracterizada a falha do sistema de governo em $t = 6009,19$ h na etapa 12. Esse valor é armazenado para a construção de histogramas de falha.

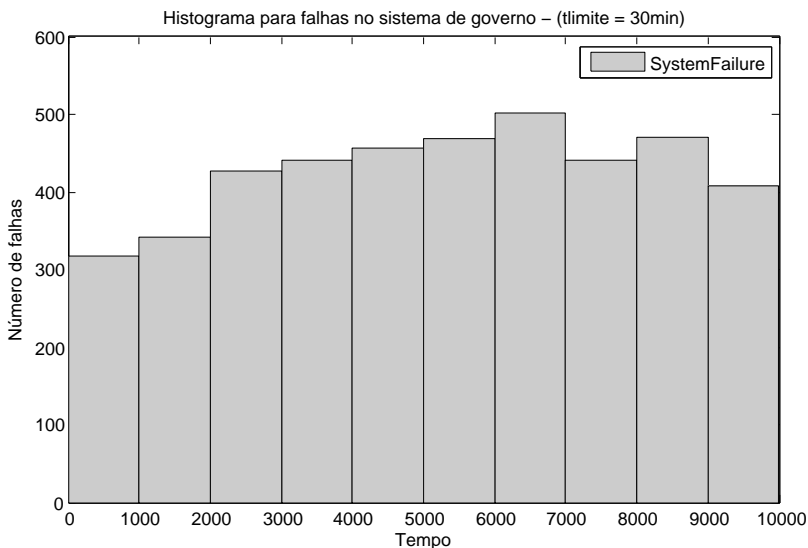
Esta seção apresentou a análise de um gráfico de cenário de falha. Durante a implementação computacional são gerados e analisados vários gráficos. Ao verificar que o comportamento do modelo está adequado e não há erros na simulação, a geração dos gráficos e relatórios ponto a ponto são desativadas. A próxima ação é a geração de histogramas para o cálculo da probabilidade de falha do sistema de governo.

6.8.2 Atividade 6.2: Cálculo da probabilidade de falha e confiabilidade do sistema técnico

A Figura 6.15 apresenta um histograma em que o tempo limite sem vazão utilizado foi de 30 minutos. O histograma apresenta a quantidade de falhas do sistema para cada intervalo de tempo. Para a construção de cada histograma são realizados 10 mil testes, cujo resultado de cada teste pode ser: sucesso da missão ou falha em determinado tempo.

Para cada t_{limite} (40, 30, 20, 10, 5 e 2 minutos) foram gerados 60 histogramas, obtendo assim conjuntos de curvas para análise de dispersão dos resultados. Significa que para cada tempo limite foram gerados 60 histogramas, sendo que cada um destes foi obtido com 10 mil testes.

Figura 6.15 – Histograma de falhas para sistema de governo do leme ($t_{Limite} = 30$ minutos)

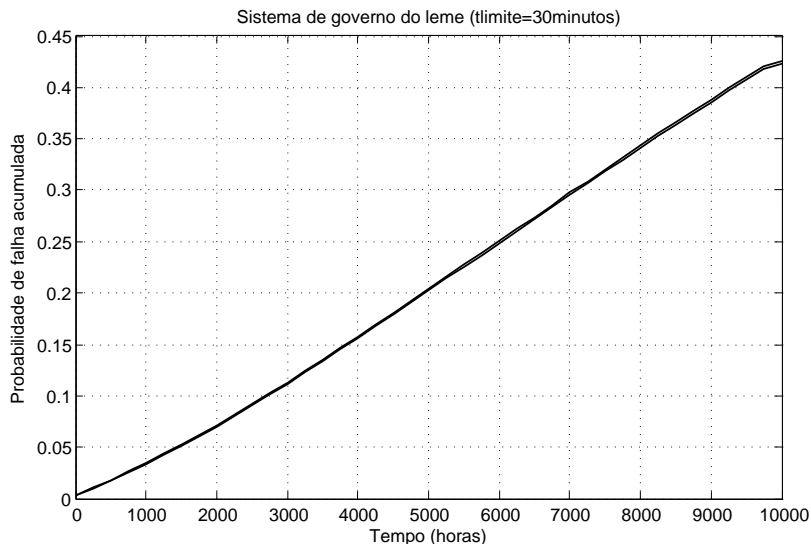


A Figura 6.16 apresenta a função distribuição acumulada de falhas para nível de confiança de 95%. A dispersão dos resultados é pequena, tendo em vista que os limites máximos e mínimos estão bastante próximos. Para o tempo de missão, $t_{missao} = 10000$ h, o intervalo (máximo; mínimo) de probabilidade de falha obtido foi:

$$IC_{95\%}(\mu) \approx (42,44\%; 42,67\%)$$

A Tabela 6.1 apresenta os valores de probabilidade de falha médios para três tempos de missão (t_{missao}). Para uma melhor apresentação dos dados no texto, foram

Figura 6.16 – Função distribuição acumulada de falhas ($t_{Limite} = 30$ minutos)



expostos somente os valores para tempo de missão igual a mil, 5 mil e 10 mil horas¹. Os valores da tabela foram gerados em simulações para os tempos limite, t_{Limite} : 40, 30, 20, 10, 5 e 2 minutos.

Tabela 6.1 – Valores de probabilidade de falha (ACoDi)

Tempo (horas)	1000	5000	10000
Simulação 40min	0,0333	0,2018	0,4205
Simulação 30 min	0,0345	0,2044	0,4255
Simulação 20min	0,0340	0,2057	0,4284
Simulação 10min	0,0344	0,2062	0,4322
Simulação 05min	0,0343	0,2076	0,4339
Simulação 02min	0,0354	0,2097	0,4373

6.8.3 Análise de confiabilidade estática

Nesta seção é apresentada uma análise de confiabilidade estática. Para isso, o cálculo realizado utiliza o diagrama de blocos apresentado na Figura 6.4 como base.

¹A simulação foi realizada para tempos de missão iniciando em zero até 10 mil, variando a cada mil horas.

Pelo diagrama observa-se que uma parte do sistema tem configuração em paralelo (SP1 e SP2) e o restante dos componentes ligados em série.

A comutação de SP1 para SP2 é considerada instantânea e não é considerada manutenção. Ou seja, dado que ocorreu uma falha em SP1, entra em operação SP2 que é o componente reserva, conseqüentemente, a falha neste componente acarreta a falha do sistema.

Também não há consideração de tempo limite sem vazão. Portanto, no instante que SP1 e SP2 estão em falha, automaticamente considera-se a falha do sistema.

Na Tabela 6.2 são apresentados as taxas de falhas dos componentes.

Quadro 6.2 – Taxas de falhas dos componentes

Componentes	Taxas de falha (Falhas/hora)
SP1	$93,9133.10^{-6}$
SP2	$93,9133.10^{-6}$
SI	$20,6187.10^{-6}$
SA	$4,3304.10^{-6}$
VE	$0,17366.10^{-6}$
TB	$1,0435.10^{-6}$

Por meio das Equações 3.2 e Equações 3.3 foram realizados os cálculos para confiabilidade em componentes ligados em série e paralelo, respectivamente. Os valores calculados estão apresentados na Tabela 6.2 em que estão apresentados apenas os valores para tempo de missão de 1 mil, 5 mil e 10 mil. No entanto, os cálculos foram desenvolvidos variando a cada mil horas, iniciando em 0 e terminando em 10 mil.

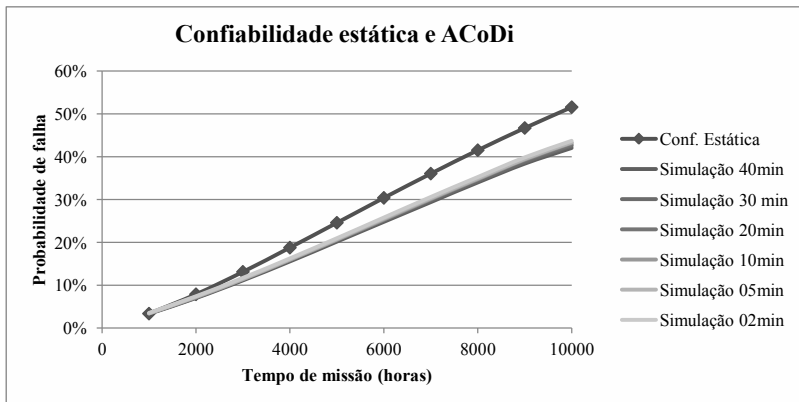
Tabela 6.2 – Valores de confiabilidade e probabilidade de falha (Confiabilidade estática)

Tempo (horas)	1000	5000	10000
R(t) sist.	0,9663	0,7542	0,4842
F(t) sist.	0,0337	0,2458	0,5158

6.8.4 Análise comparativa entre a confiabilidade estática e a metodologia ACoDi

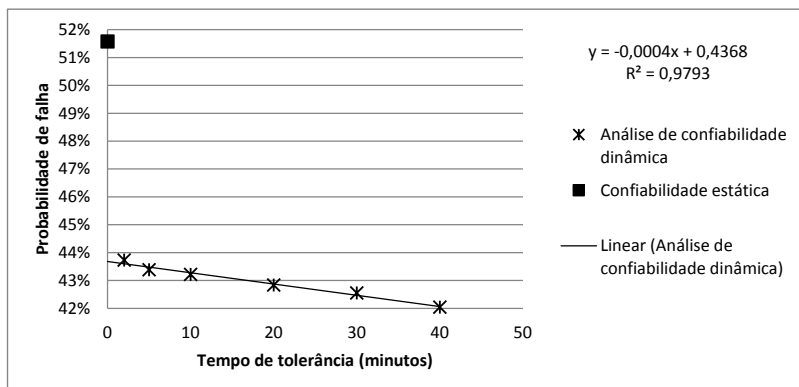
A Figura 6.17 apresenta os valores para análise de confiabilidade estática e a metodologia ACoDi para tempos de missão variando de 1 mil a 10 mil horas. Neste gráfico não é possível grande variação, da probabilidade de falha, em relação ao tempo limite sem vazão;

Figura 6.17 – Probabilidade de falha em função do tempo de missão



Como a análise de confiabilidade estática não considera a variação do tempo sem vazão, o valor da probabilidade de falha para este método foi relacionado com o tempo sem vazão nulo, $t_{sv} = 0$. Os dados obtidos com a metodologia ACoDi estão representados junto com a análise de confiabilidade estática na Figura 6.18.

Figura 6.18 – Probabilidade de falha em função do tempo limite sem vazão

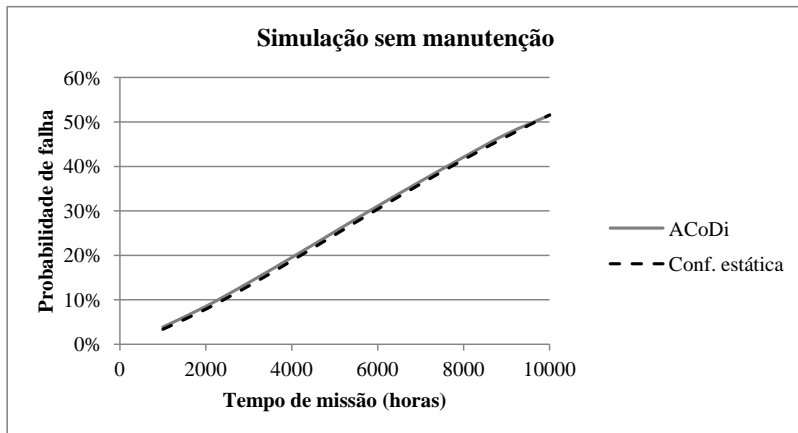


Na Figura 6.18 é possível verificar que existe uma influência em relação ao tempo limite sem vazão. A medida que há uma tolerância maior na indisponibilidade do sistema, há uma redução linear na probabilidade de falha do sistema.

A diferença entre as duas metodologias, observada na Figura 6.20, ocorrem basicamente devido a possibilidade de realizar reparos no sistema na metodologia ACoDi. Na Figura 6.19 foi obtida com uma simulação considerando que não há manutenção no sistema. Nessa modelagem foi utilizado o modelo com o tempo limite

sem vazão de 30 minutos. Verifica-se que a curva obtida analiticamente (confiabilidade estática), coincide com a curva obtida numericamente (metodologia ACoDi).

Figura 6.19 – Probabilidade de falha sem manutenção



A Tabela 6.3 apresenta os dados utilizados para a construção do gráfico apresentado na Figura 6.19.

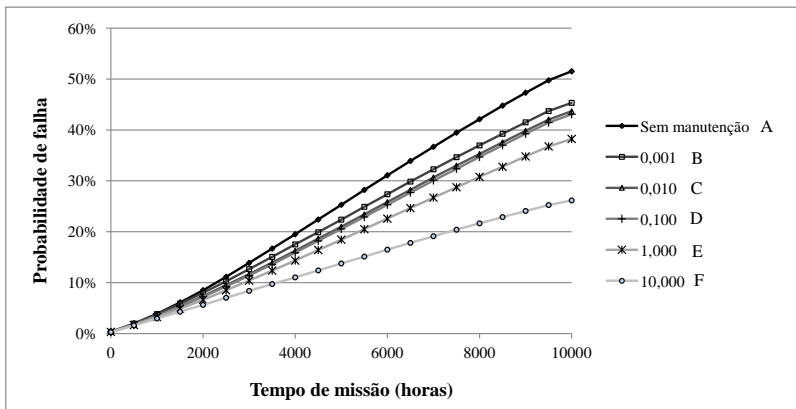
Tabela 6.3 – Valores de probabilidade de falha para análise sem manutenção

Tempo (horas)	ACoDi	Conf. estática
1000	0,0387	0,0337
2000	0,0853	0,0788
3000	0,1389	0,1312
4000	0,1952	0,1877
5000	0,2531	0,2458
6000	0,311	0,3039
7000	0,3668	0,3606
8000	0,421	0,4152
9000	0,4731	0,467
10000	0,5151	0,5158

A Figura 6.20 apresenta um gráfico no qual é analisado a probabilidade de falha em função da taxa de reparo de SP1 e SP2, para o tempo de missão de 0 a 10 mil horas. A probabilidade de falha sofre pouca influência da taxa de reparo para os tempos de missão abaixo de 2500 horas – para essa faixa de valores verifica-se a sobreposição das curvas. Esse comportamento ocorre porque quando o tempo de missão é curto, ocorrem poucos casos de falha e reparo. Por outro lado, se o tempo de missão é longo,

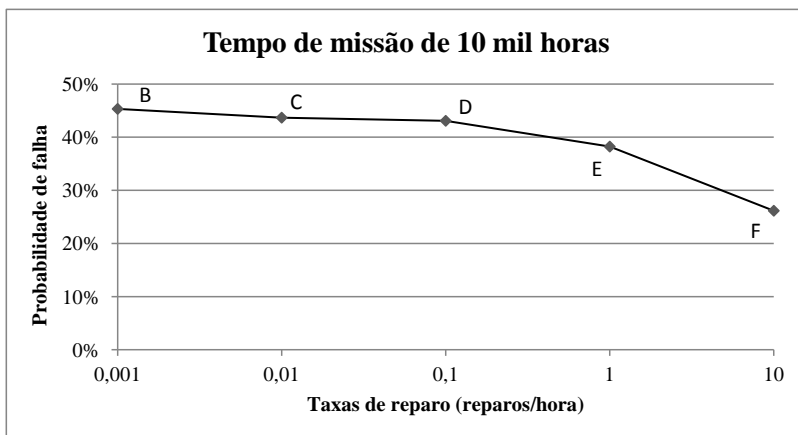
um componente pode passar por vários reparos, o que influencia com maior peso a probabilidade de falha e confiabilidade do sistema técnico.

Figura 6.20 – Probabilidade de falha em função das taxas de reparo



A Figura 6.21 é uma representação da variação da probabilidade de falha do sistema de governo em função da taxa de reparo, sendo considerada apenas para o tempo de missão de 10 mil horas. É possível verificar que para os valores abaixo de 0,100 reparos/hora a probabilidade de falha tem pouca variação. Significa que é preciso investir nos procedimentos e equipamentos de manutenção para que a taxa de reparo esteja acima deste valor.

Figura 6.21 – Probabilidade de falha em função das taxas de reparo (10mil horas)



Assim, a simulação permite visualizar a influência da manutenção na confiabilidade dinâmica do sistema. Para os sistemas com potencial catastrófico, a taxa de reparo não pode ser baixa. Isto vai exigir que se tenha componentes redundantes, peças sobressalentes à disposição, equipamentos e procedimentos de manutenção eficientes.

6.9 CONSIDERAÇÕES DO CAPÍTULO

O presente capítulo apresentou o uso da metodologia ACoDi para a análise do sistema de governo de um navio. A análise foi comparada com a análise de confiabilidade estática e os valores obtidos foram satisfatórios.

Foi possível verificar a influência da manutenção na probabilidade de falha e na confiabilidade do sistema. Para os sistemas com o tempo de missão curto, os resultados ficam próximos de uma análise de confiabilidade estática. Já, quando o tempo de missão é mais longo, ocorre uma maior quantidade de manutenções no sistema, o que faz com que a taxa de reparo tenha uma influência maior sobre os resultados.

As taxas de falha utilizadas dos componentes foram obtidas do relatório técnico de Biasotto (2008), onde o estudo foi realizado com *software* denominado Relx 2007, que usa o método de Monte Carlo para a realização das simulações. O estudo foi realizado para tempo de missão 720 horas, obtendo uma confiabilidade de aproximadamente 91,9%. Em comparação com a metodologia ACoDi, usando os dados da análise, também sem manutenção, houve uma diferença – obteve-se uma confiabilidade de aproximadamente 97%².

Com a geração dos diagramas que representam o comportamento dinâmico, pode-se perceber que a ocorrência de falha oculta no componente reserva (SP2) geralmente resulta na falha do sistema. A ocorrência da falha oculta no componente reserva, no momento de uma demanda – falha do componente principal (SP1) –, exige muito da capacidade de manutenção. Desta forma, o tempo que o sistema fica sem vazão disponível é muito elevado, ou seja, ultrapassa o tempo limite que caracteriza a falha do sistema. Foi possível perceber a necessidade de um estudo de impacto das falhas ocultas sobre a confiabilidade dinâmica do sistema.

Aqui, neste estudo de caso, ficou mais evidente que a metodologia ACoDi torna-se aderente à análise de sistemas já em operação, em que necessitem atualizações tecnológicas para adequarem-se às legislações em relação à segurança operacional, à continuidade do negócio e, principalmente, à segurança humana e ambiental.

Uma vez que se tenha as informações de manutenção e das tecnologias a serem implantadas é possível identificar de forma efetiva os sistemas, subsistemas e componentes de alta criticidade, que se ajustam às regiões R3 e R4, e para estas implementar esta metodologia e/ou mesmo outras técnicas para definir o grau de confiabilidade.

A capacidade de se gerar cenários de falhas traz como vantagem, a possibilidade de se poder implantar um supervisor para acompanhamento em tempo real o comportamento do sistema, na forma de um diagrama como da Figura 4.38, para que

²O valor foi obtido com base nos dados da Tabela 6.3.

os operadores em sala de comando ou em algum sistema eletrônico possam orientar as equipes de manutenção em situações de falhas em sistemas de alto risco operacional.

7 CONCLUSÕES E RECOMENDAÇÕES PARA TRABALHOS FUTUROS

A presente seção sintetiza os pontos considerados mais importantes do desenvolvimento do trabalho, apresenta as conclusões e recomendações para trabalhos futuros. Além disso, deseja-se neste momento da leitura do texto ter respostas para as seguintes questões:

- Por que este texto é um tema de tese?
- Onde está a tese nesta pesquisa?

A resposta para as duas questões será apresentada com base na utilidade da metodologia proposta, nos benefícios que a metodologia pode trazer, no seu campo de aplicação, e no atendimento aos objetivos gerais e específicos.

Como foi apresentado no Capítulo 1, a análise de confiabilidade dinâmica é pouco conhecida, e portanto, necessita de desenvolvimento e pesquisas relacionadas. A proposta de apresentar uma metodologia vem com o intuito de auxiliar na divulgação desta nova abordagem e facilitar o uso no meio acadêmico e industrial.

Para isso, a proposta da metodologia ACoDi apresenta uma estrutura para desenvolvimento de uma análise de confiabilidade dinâmica, onde estão organizadas as informações e técnicas de suporte necessárias para a realização da análise. Além da proposta da metodologia apresentada no Capítulo 4, os estudos de caso apresentados no Capítulo 5 (problema de controle de nível do reservatório) e no Capítulo 6 (problema da disponibilidade do leme do navio) exemplificam seu uso durante as **etapas** e **atividades** desenvolvidas na metodologia.

As sequências de etapas e atividades propostas permitem obter e organizar as informações, orientando o analista, durante a elaboração e execução de uma análise de confiabilidade dinâmica. Tal sistematização se reflete em um ganho de conhecimento sobre o sistema técnico do ponto de vista de projeto, de operação e de manutenção. Consequentemente, a metodologia dá suporte para os profissionais nas três áreas para a tomada de decisão que podem refletir em alterações de projeto, em procedimentos de operação e manutenção dos equipamentos.

A metodologia parte desde o princípio de se poder ou não executar a análise de confiabilidade dinâmica. Ou seja, a análise deste sistema é viável? Quando se deve realizar uma análise de confiabilidade estática ou clássica? Dado que se tenha concluído que a análise de confiabilidade dinâmica será realizada, os resultados obtidos são: cenários de falhas, confiabilidade ou probabilidade de falha, componentes críticos do sistema sob a ótica da operação e da manutenção, facilita a identificação dos itens a serem melhorados (taxa de falhas, taxa de reparo, sensores, componentes sobressalentes, capacitação, configurações do sistema, etc) e se os resultados são significativos por meio das simulações. A forma estruturada permite, atualizar as informações relacionadas com o sistema técnico e realizar novas análises a fim de verificar a efetividade das ações de melhoria.

A técnica se mostrou adequada para a análise de risco em sistemas, tendo em vista que faz uso de técnicas de suporte como FMECA e CNEA. Adicionalmente, a

obtenção de cenários de falhas e da confiabilidade dá subsídios para a proposição de barreiras, mudanças no projeto, alteração nos sistemas de controle, alarmes entre outros pontos que podem melhorar a confiabilidade dinâmica do sistemas. Conseqüentemente, pode-se reduzir a ocorrência de falhas ou mitigar os efeitos gerados.

Desta forma, a metodologia pode ser utilizada para a análise de confiabilidade de sistemas, suporte ao projeto de produto, suporte ao planejamento da manutenção de sistemas técnicos e na análise de risco.

7.1 QUANTO AOS OBJETIVOS

O objetivo geral proposto foi de apresentar uma metodologia para análise de confiabilidade dinâmica, contemplando o comportamento dinâmico de falhas e atualização do modelo de análise ao longo do tempo.

Para o cumprimento do objetivo geral deste trabalho, foi proposto os seguintes objetivos específicos:

1. Sistematizar o uso das técnicas para análise da confiabilidade dinâmica.
2. Sistematizar uma ferramenta computacional para auxiliar na implementação do modelo de análise.
3. Estruturar uma metodologia que permita o desenvolvimento da análise de confiabilidade dinâmica para identificar: início da análise, etapas de análise, informações requeridas e resultados.
4. Aplicar a metodologia para um problema clássico de confiabilidade dinâmica e comparar o resultado com as análises de outros pesquisadores.

No Capítulo 2 foi apresentado os aspectos que fazem uma análise de confiabilidade ser dinâmica e diferentes abordagens que podem ser feitas. A análise de confiabilidade deste trabalho está relacionada com as mudanças de configuração do sistema, acompanhamento das variáveis de controle e a atuação humana (por meio das taxas de reparo dos componentes).

Para realizar uma análise de confiabilidade dinâmica verificou-se que é preciso ter um conjunto de informações de projeto, operação e manutenção do sistema como: configurações de operação do sistema, limites que caracterizam operação normal ou falha do sistema, taxas de falha dos componentes, comportamento dinâmico da variável de estado do sistema, taxas de reparo e política de manutenção (se houver manutenção do sistema). As etapas e atividades sugeridas pela metodologia ACoDi visam capturar e organizar as informações para a implementação da análise de confiabilidade dinâmica.

O trabalho foi desenvolvido com base no método de Monte Carlo para a execução das simulações de falha, em que os sorteios dos tempos (de falha ou de reparo) foram obtidos de distribuições estatísticas. Neste trabalho foram utilizadas as distribuições exponencial e log-normal, no entanto, de acordo com a necessidade da modelagem pode-se utilizar outras como a normal e Weibull.

A metodologia ACoDi ficou aderente aos trabalhos desenvolvidos no NeDIP, visto que as técnicas de suporte – FMECA, CNEA, IDEFO, diagramas de blocos

para confiabilidade e MCC, – fazem parte do arcabouço de técnicas utilizadas pelos pesquisadores do laboratório.

A metodologia foi desenvolvida para produtos já existentes ou que já estejam na etapa do projeto detalhado, quando as configurações dos sistemas, lista de componentes entre outras informações necessárias para a modelagem, já estiverem sido definidas no projeto do produto. A relação entre a metodologia ACoDi e PRODIP foi apresentada na proposta da metodologia, no Capítulo 4.

Foi possível verificar com a aplicação da metodologia, no problema clássico de confiabilidade dinâmica (Capítulo 5) – que serviu de referência para comparação de resultados a serem obtidos nas análises de sistemas dinâmicos – e na análise do sistema de governo do navio (Capítulo 6), que as etapas e atividades descritas pela metodologia ACoDi facilitam o desenvolvimento da análise, direcionando a busca e geração de informações.

A metodologia foi desenvolvida com uma representação próxima do PRODIP, onde são definidas etapas e atividades, para facilitar a compreensão e aplicação da análise de confiabilidade dinâmica. Com isso, o desenvolvimento ficou sistematizado, sendo possível verificar em cada etapa, as atividades e técnicas de suporte que devem ser realizadas.

Foi apresentado um fluxograma geral do programa, Figura 4.32, os fluxogramas das principais rotinas e a representação do fluxo de informações dentro do *software*, Figura 4.31, para auxiliar na implementação computacional.

Diante dos resultados obtidos, conclui-se que os objetivos específicos apresentados foram contemplados. Quanto ao objetivo geral – desenvolver uma metodologia para análise de confiabilidade dinâmica, contemplando o comportamento dinâmico de falhas e atualização do modelo de análise ao longo do tempo – entende-se que este também foi cumprido.

Portanto, diante do que foi apresentado, pode-se concluir que o texto apresentado é uma tese, sendo que está localizada na metodologia para o desenvolvimento de análise de confiabilidade dinâmica.

7.2 RESULTADOS E CONTRIBUIÇÕES

O principal resultado e contribuição deste trabalho é a metodologia ACoDi, que por meio da estrutura representada com etapas e atividades, permite realizar a análise de confiabilidade dinâmica, que é a proposta desta tese. Em cada uma das etapas e atividades estão explicitadas as informações necessárias, bem como o uso de técnicas de suporte, que irão conduzir a equipe de analistas.

O uso da metodologia além de auxiliar no desenvolvimento da análise, serve como documentação para dar suporte ao projeto, manutenção e operação do sistema técnico. Adicionalmente, com o maior conhecimento adquirido com o uso da metodologia sobre o sistema (projeto, operação e manutenção), é possível realizar alterações que resultem na melhoria da confiabilidade do sistema.

O resultado das simulações com a metodologia ACoDi são explicitados na forma de gráficos com função densidade de probabilidade de falha, diagramas com

a representação do comportamento dinâmico das variáveis de controle e relatórios ponto a ponto ao longo do tempo de missão. Essas informações auxiliam no reprojeto de sistemas, análise do estado atual do sistema e dos controles (barreiras) de falhas e, principalmente, auxiliam o gestor de manutenção para organização dos planos de manutenção, capacitação de mão de obra, instalação de sensores e equipamentos de monitoramento/contenção de falhas.

Os relatórios ponto a ponto, ao longo do tempo de missão, junto com a representação do comportamento dinâmico das variáveis de controle auxiliam na visualização de cenários de falhas que podem ocorrer no sistema e não foram previstos pelos analistas. A partir destes relatórios, pode-se gerar cenários críticos de falha que devem comunicar-se com os operadores para auxiliar na tomada de decisões para conter o desvio de comportamento. Esses poderão ser representados de forma semelhante como na Figura 4.38.

Com os estudos de caso, verificou-se que a metodologia permite avaliar a confiabilidade dos sistemas em função das ações de manutenção. Se a manutenção dos componentes demanda um tempo muito grande¹, a confiabilidade do sistema pode ter valor muito baixo. Desta forma, se existe um dado valor limite de confiabilidade, o gestor de manutenção pode planejar a compra de equipamentos, programar a quantidade de componentes sobressalentes, preparar programas de capacitação da equipe, entre outras atividades com o objetivo de melhorar a confiabilidade.

Por exemplo, com a aplicação da metodologia no sistema de governo do navio foi possível perceber que, no caso de uma probabilidade de falha acima do desejado, pode-se elaborar simulações a fim de obter melhores resultados para o sistema. Pode-se sugerir, no caso de necessidade de melhoria da confiabilidade, as seguintes ações:

- Substituição de componentes que possuem menores taxas de falha. Pode-se buscar componentes de outras marcas ou, até mesmo, outros componentes na matriz morfológica do projeto que atendam a mesma função. Neste caso, estaria sendo feito um reprojeto do produto.
- Melhorar os procedimentos de manutenção, aquisição de peças sobressalentes que demandam maior tempo de manutenção, capacitação dos operadores, aquisição de equipamentos para manutenção, entre outras ações a fim de aumentar as taxas de reparo dos componentes.
- Propor alterações nos controles, sensores ou atuadores. Com isso, pode-se dificultar o avanço da variável de controle para região de falha. Em termos da análise de risco, essas ações correspondem ao estabelecimento de barreiras a fim impedir a propagação da falha ao longo da rede causal.
- Propor mudanças na configuração do sistema, como estabelecer redundâncias para os componentes com maior taxa de falha, ou maior tempo de reparo.

Portanto, o conhecimento inicial adquirido com as técnicas de suporte, apresentadas no Capítulo 3, é complementado com as informações obtidas com os resultados da implementação computacional. Estas informações complementares retornam para

¹Análise em sistemas que permitem a manutenção durante a operação.

o projeto (projeto informacional), para a operação e manutenção, buscando melhorar continuamente a confiabilidade dinâmica dos sistemas.

7.3 RECOMENDAÇÕES PARA TRABALHOS FUTUROS

Com a simulações foi possível perceber que grande parte das falhas do sistema acontecem devido à presença de falhas ocultas. Quando o controlador do sistema gera comando para alterar os estados dos componentes, percebe-se que estes estão em falha, que agora já passam a ser falhas evidentes. Assim, sugere-se a implementação de rotinas para obtenção de histogramas para falhas ocultas. Dessa forma, o gestor de manutenção pode ter uma probabilidade de falha oculta para cada componente. Com isso, são gerados planos de manutenção com testes para detecção de falhas ocultas.

Implementar estrutura para manutenção em paralelo e manutenção mista série/paralelo onde é feito manutenção em um grupo de componentes ao mesmo tempo, posteriormente, os grupos subsequentes são reparados. Desta forma, a manutenção em cada grupo é realizada em paralelo e a manutenção entre os grupos é realizada em série. Tendo esta flexibilidade o gestor de manutenção pode planejar melhor as manutenções nos equipamentos, ou seja, priorizar a manutenção nos equipamentos que tem maior impacto na confiabilidade do sistema.

Grande parte dos incidentes envolvem a falha humana, que ocorrem principalmente em situações de emergência onde o há grande pressão sobre o agente, devido às condições frente à uma falha catastrófica. A consideração da atuação humana no metodologia ACoDi ainda é deficiente e necessita de um maior aprimoramento. Deve-se implementar modos de falha humanos como erro de execução da tarefas, ou não execução das tarefas, ou execução de tarefa não exigida entre outras. Portanto, caracterizar as falhas humanas e implementá-las no modelo enriqueceria a análise de confiabilidade dinâmica.

Nas aplicações apresentadas no Capítulo 5, onde foi monitorado o nível do reservatório de fluido, e no Capítulo 6, onde foi monitorado o tempo de indisponibilidade do sistema de governo do leme do navio, os sistemas foram estudados apenas com uma variável de controle. Desta forma, sugere-se desenvolver uma estrutura para controlar várias variáveis de controle, para aumentar a possibilidade de uso do modelo proposto.

Desenvolver uma estrutura, como sistema especialista, para capturar as informações geradas pela metodologia ACoDi e fazer implementação em sistemas para monitoramento “*online*” em salas de controle. Assim, de acordo com os estados dos componentes e das variáveis de controle do sistema técnico, pode-se em um painel de informações, explicitar os cenários de falhas para os operadores de sistemas a fim de auxiliar na tomada de decisões que impeçam que o sistema entre em uma região de emergência ou de falha completa.

Implementar a estrutura de programação do ACoDi no Scilab, que é um ambiente utilizado para desenvolvimento de programas para resolver problemas numéricos. Tem a vantagem de ser gratuito e distribuído com o código fonte (*open source software*). Conseqüentemente, o uso da técnica com *software* livre pode ter maior divulgação, facilitando o compartilhamento do conhecimento sobre o assunto. O mesmo não foi

utilizado nesta tese, com receito de haver *bugs* e confundir o desenvolvimento das simulações.

REFERÊNCIAS

- ABNT (Associação Brasileira de Normas Técnicas). *NBR 5462: Confiabilidade e manutenibilidade – terminologia*. Rio de Janeiro, 1994. 37 p.
- ACOSTA, C.; SIU, N. Dynamic event trees in accident sequence analysis: application to steam generator tube rupture. *Reliability Engineering & System Safety*, v. 41, n. 2, p. 135 – 154, 1993. ISSN 0951-8320. <<http://www.sciencedirect.com/science/article/pii/095183209390027V>>.
- AL-DABBAGH, A. W.; LU, L. Reliability modeling of networked control systems using dynamic flowgraph methodology. *Reliability Engineering & System Safety*, v. 95, n. 11, p. 1202 – 1209, 2010. ISSN 0951-8320. <<http://www.sciencedirect.com/science/article/pii/S0951832010001262>>.
- ALVES, G. D. *Sistema especialista protótipo para diagnóstico de falha em um sistema hidráulico naval*. Dissertação (Mestrado) — Universidade Federal de Santa Catarina, Florianópolis, SC, 2001.
- ASSIS, R. Periodicidade ótima de inspeções na procura de falhas ocultas. *Risco, Segurança e Sustentabilidade*, p. 447–464, 2012.
- BACK, N.; OGLIARI, A.; DIAS, A.; SILVA, J. C. *Projeto Integrado de Produtos: planejamento, concepção e modelagem*. [S.l.]: Manole, 2008.
- BEGOSSO, L. C. *S.PERERE – Uma ferramenta apoiada por arquiteturas cognitivas para o estudo da confiabilidade humana*. Tese (Doutorado) — Universidade de São Paulo, São Paulo, SP, 2005. <<http://www.teses.usp.br/teses/disponiveis/3/3141/tde-09012006-093145/>>.
- BELAN, H. C. *Formalização da rede de petri canal/agência para projeto de equipamentos industriais*. Dissertação (Mestrado) — Universidade Federal de Santa Catarina, Florianópolis, SC, Abril 2007.
- BERTSCHE, B. *Reliability in automotive and mechanical engineering*. 1st. ed. Berlin: Springer, 2008.
- BIASOTTO, E. *Sistema de governo do navio Itabuna: Estudo de confiabilidade do sistema hidráulico de acionamento do leme*. [S.l.], 2008. Relatório final para Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq).
- BILLINTON, R.; ALLAN, R. *Reliability Evaluation of Engineering Systems: Concepts and Techniques*. 2nd. ed. New York: Plenum Pub Corp, 1992.
- BOTTA, R.; BAHILL, Z.; BAHILL, T. When are observable states necessary? *Systems Engineering*, John Wiley and Sons Ltd., Chichester, UK, v. 9, n. 3, p. 228–240, out. 2006. ISSN 1098-1241. <<http://dx.doi.org/10.1002/sys.v9:3>>.
- BOUDALI, H.; CROUZEN, P.; STOELINGA, M. Dynamic fault tree analysis using input/output interactive markov chains. In: *IEEE. Dependable Systems and Networks, 2007. DSN'07. 37th Annual IEEE/IFIP International Conference on*. [S.l.], 2007. p. 708–717.

- BUCCI, P.; KIRSCHENBAUM, J.; MANGAN, L. A.; ALDEMIR, T.; SMITH, C.; WOOD, T. Construction of event-tree/fault-tree models from a markov approach to dynamic system reliability. *Reliability Engineering and System Safety*, v. 93, n. 11, p. 1616 – 1627, 2008. ISSN 0951-8320. <<http://www.sciencedirect.com/science/article/pii/S0951832008000343>>.
- CALIL, L. F. P. *Metodologia de gerenciamento de risco: Foco na segurança e continuidade*. Tese (Doutorado) — Universidade Federal de Santa Catarina, Florianópolis, SC, Março 2009.
- CARDOSO, J.; VALETTE, R. *Redes de Petri*. Florianópolis, SC: Editora da UFSC, 1997. 212 p.
- CARVALHO, A. *Análise de Disponibilidade Utilizando Abordagem Nebulosa*. Dissertação (Mestrado) — Universidade Federal de Minas Gerais, 2008.
- CARVALHO, E. N. *Uma revisão crítica do emprego de bancos de dados de falhas em análises probabilísticas de segurança de plantas nucleares e químicas*. Dissertação (Mestrado) — Universidade Federal do Rio de Janeiro, 2007.
- CASSADY, C.; POHL, E. Introduction to repairable systems modeling. In: *Annual Reliability and Maintainability Symposium, 49^o*. Tampa, Florida, USA: [s.n.], 2003.
- CASSANDRAS, C.; LAFORTUNE, S. *Introduction to discrete event systems*. 2nd. ed. New York: Springer, 2008. 772 p.
- CHIACCHIO, F.; CACIOPPO, M.; D'URSO, D.; MANNO, G.; TRAPANI, N.; COMPAGNO, L. A weibull-based compositional approach for hierarchical dynamic fault trees. *Reliability Engineering & System Safety*, Elsevier, 2012.
- CODETTA-RAITERI, D.; BOBBIO, A. Stochastic petri nets supporting dynamic reliability evaluation. *International Journal of Materials & Structural Reliability*, v. 4, p. 65–77, March 2006.
- COLLAS, G. Dynamic reliability prediction: how to adjust modeling and reliability growth? In: *Proceedings of the IEEE Annual Reliability and Maintainability Symposium*. New York: Institute of Electrical and Electronics Engineers: [s.n.], 1991. p. 301–306.
- CURY, J. Teoria de controle supervisão de sistemas a eventos discretos. *V Simpósio Brasileiro de Automação Inteligente (Minicurso)*, Novembro 2001.
- DA ROSA, E. *Análise de resistência mecânica: Mecânica da fratura e fadiga*. Agosto 2002. Universidade Federal de Santa Catarina. <<http://www.grante.ufsc.br/download/FADIGA.pdf>>.
- DE NEGRI, V. J.; SANTOS, E. A. P. S. Projeto de sistemas de automação da manufatura. In: AGUIRRE, L. A. (Ed.). *Enciclopédia de automática: controle & automação*. 1. ed. São Paulo- SP: Blucher, 2007. v. 1, cap. 15, p. 382–417.
- DEVOOGHT, J. Dynamic reliability. In: LEWINS, M. B. J. (Ed.). *Advances in Nuclear Science and Technology*. New York: Springer, 1997. v. 25, p. 215–278.
- DEVOOGHT, J.; SMIDTS, C. Probabilistic reactor dynamics. I: The theory of continuous event trees. *Nuclear science and engineering*, American Nuclear Society, v. 111, n. 3, p. 229–240, 1992.

- _____. Probabilistic dynamics as a tool for dynamic PSA. *Reliability engineering & systems safety*, Elsevier, v. 52, n. 3, p. 185–196, 1996.
- DIAS, A. *Metodologia para Análise da Confiabilidade em Freios Pneumáticos Automotivos*. Tese (Doutorado) — Universidade Estadual de Campinas, Campinas, SP, Julho 1996.
- DIAS, A.; CALIL, L. F. P.; RIGONI, E.; OGLIARI, A.; SAKURADA, E. Y.; KAGUEIAMA, H. A. *Metodologia para análise de risco: Mitigação de perda de SF₆ em disjuntores*. 1. ed. Florianópolis, SC: Nova Letra Gráfica & Editora, 2011. 1304 p. ISBN: 978-85-98128-42-9.
- DISTEFANO, S.; PULIAFITO, A. Dynamic reliability block diagrams vs dynamic fault trees. *Proceedings of the 53rd Annual Reliability and Maintainability Symposium (RAMS07)*, IEEE, 2007.
- DISTEFANO, S.; XING, L. A new approach to modeling the system reliability: dynamic reliability block diagrams. *Reliability and Maintainability Symposium, 2006. RAMS'06. Annual*, p. 189–195, 2006.
- DOMÍNGUEZ-GARCÍA, A.; KASSAKIAN, J.; SCHINDALL, J.; ZINCHUK, J. An integrated methodology for the dynamic performance and reliability evaluation of fault-tolerant systems. *Reliability Engineering & System Safety*, Elsevier, v. 93, n. 11, p. 1628–1649, 2008.
- DROGUETT, E. L.; MOSLEH, A. Análise bayesiana da confiabilidade de produtos em desenvolvimento. *Gestão & Produção*, Scielo, v. 13, p. 57 – 69, 04 2006. ISSN 0104-530X.
- FRANKLIN, G.; POWELL, J.; EMAMI-NAEINI, A.; POWELL, J. *Feedback control of dynamic systems*. [S.l.]: Addison-Wesley Reading, MA, 1994.
- FUENTES, F. *Metodologia para inovação da gestão de manutenção industrial*. Tese (Doutorado) — Universidade Federal de Santa Catarina, Florianópolis, SC, 2006.
- GEORGES, M. R. R. *Metodologia para Modelagem e Simulação de Sistemas: Aplicação em Manufatura Discreta*. Tese (Doutorado) — Universidade Estadual de Campinas, 2005.
- GUIMARÃES, L. S. *Gerenciamento de Riscos e Segurança de Sistemas*. Rio de Janeiro, RJ: iEditora, 2003.
- HU, Y. *A guided simulation methodology for dynamic probabilistic risk assessment of complex systems*. Tese (Doutorado) — University of Maryland, 2005.
- HUBKA, V.; EDER, W. *Theory of technical systems*. [S.l.]: Springer-Verlag New York, 1988. 275 p.
- KAGUEIAMA, H. A. *Sistematização de técnicas de análise de falha e projeto para confiabilidade*. Dissertação (Mestrado) — Universidade Federal de Santa Catarina, Florianópolis, SC, 2012.
- LABEAU, P.; SMIDTS, C.; SWAMINATHAN, S. Dynamic reliability: towards an integrated platform for probabilistic risk assessment. *Reliability Engineering and System Safety*, Elsevier, v. 68, n. 3, p. 219–254, 2000.

LADDE, G.; SILJAK, D. Multiplex control systems: Stochastic stability and dynamic reliability. In: *Proc. 20th IEEE Conference on Decision and Control including the Symposium on Adaptive Processes*. [S.l.: s.n.], 1981. v. 20, p. 908–912.

LAW, A.; KELTON, W. et al. *Simulation modeling and analysis*. 3. ed. [S.l.]: McGraw-Hill, 2005.

LOBO, L. M. V. *Determinação de índices de fiabilidade em sistemas eléctricos utilizando o método de monte carlo*. Dissertação (Mestrado) — Faculdade de Engenharia da Universidade de Porto, Setembro 2000.

MANIAN, R.; DUGAN, J.; COPPIT, D.; SULLIVAN, K. Combining various solution techniques for dynamic fault tree analysis of computer systems. In: *Proceedings of 3rd IEEE International High-Assurance Systems Engineering Symposium*. [S.l.: s.n.], 1998. p. 21–28.

MANNO, G.; CHIACCHIO, F.; COMPAGNO, L.; D'URSO, D.; TRAPANI, N. Matcarlore: An integrated ft and monte carlo simulink tool for the reliability assessment of dynamic fault tree. *Expert Syst. Appl.*, v. 39, n. 12, p. 10334–10342, 2012.

MARRANGHELLO, N. *Redes de Petri: Conceitos e Aplicações*. São Paulo: DCCE/IBILCE/UNESP, p. 33, Março 2005.

MARSEGUERRA, M.; ZIO, E.; DEVOOGHT, J.; LABEAU, P. A concept paper on dynamic reliability via Monte Carlo simulation. *Mathematics and Computers in Simulation*, Elsevier Science, v. 47, n. 2, p. 371–382, 1998.

MATSUOKA, T.; KOBAYASHI, M. The go-flow reliability analysis methodology—analysis of common cause failures with uncertainty. *Nuclear Engineering and Design*, v. 175, n. 3, p. 205 – 214, 1997. ISSN 0029-5493. <<http://www.sciencedirect.com/science/article/pii/S0029549397000381>>.

MATURANA, M. *Aplicação de Redes Bayesianas na análise da contribuição do erro humano em acidentes de colisão*. Dissertação (Mestrado) — Universidade de São Paulo, 2011.

MENEZES, R. C. S.; DROGUETT, E. L. Análise da confiabilidade humana via redes Bayesianas: uma aplicação à manutenção de linhas de transmissão. *Produção*, Scielo, v. 17, p. 162 – 185, 04 2007. ISSN 0103-6513.

MERCURIO, D.; PODOFILLINI, L.; ZIO, E.; DANG, V. Identification and classification of dynamic event tree scenarios via possibilistic clustering: Application to a steam generator tube rupture event. *Accident Analysis and Prevention*, Elsevier, 2008.

MOLER, C. B. *Numerical computing with MATLAB*. [S.l.]: Society for Industrial and Applied Mathematics, 2004.

MORÉ, J. *Aplicação da lógica Fuzzy na avaliação da confiabilidade humana nos ensaios não destrutivos por ultra-som*. Tese (Doutorado) — Universidade Federal do Rio de Janeiro, Rio de Janeiro, RJ, Abril 2004.

- MOSLEH, A. et al. An integrated framework for identification, classification, and assessment of aviation systems hazards. In: INTERNATIONAL CONFERENCE ON PROBABILISTIC SAFETY ASSESSMENT AND MANAGEMENT (PSAM), 7 – ESREL '04: PROCEEDINGS OF THE 7TH INTERNATIONAL CONFERENCE ON PROBABILISTIC SAFETY ASSESSMENT AND MANAGEMENT. Berlin, Alemanha, 2004.
- MOUBRAY, J. *Reliability-centered Maintenance*. New York: Industrial Press, 1997.
- MOURA, M. J. C. *Processos semi markovianos e redes bayesianas para avaliação de indicadores de desempenho de confiabilidade de sistemas complexos tolerantes à falha*. Dissertação (Mestrado) — Universidade Federal de Pernambuco, Departamento de Engenharia de Produção, 2006.
- NASA (National Aeronautics and Space Administration). *Reliability Centered Maintenance Guide: For Facilities and Collateral Equipment*. Washington, 2008.
- NEJAD-HOSSEINIAN, S. H. *Automatic generation of generalized event sequence diagrams for guiding simulation based dynamic probabilistic risk assessment of complex systems*. Tese (Doutorado) — University of Maryland, College Park, MD, USA, 2007. AAI3297363.
- NETO, P. L. O. C. *Estatística*. São Paulo: Editora E. Blücher, 1977.
- NIST (National Institute of Standards and Technology). *FIPS PUBS 183: Integration definition for function modeling (IDEF0)*. Gaithersburg, MD, 1993. Draft Federal Information Processing Standards Publication.
- OGATA, K. *System Dynamics*. Prentice Hall, 2004. (cram 101). ISBN 9780131424623. <<http://books.google.co.uk/books?id=5OanQgAACAAJ>>.
- OGATA, K.; MAYA, P.; LEONARDI, F. *Engenharia de controle moderno*. São Paulo: Prentice Hall, 2003.
- OUHBI, B.; LIMNIOS, N. Nonparametric reliability estimation of semi-markov processes. *Journal of Statistical Planning and Inference*, v. 109, n. 1–2, p. 155 – 165, 2003. ISSN 0378-3758. <ce:title>C.R. Rao 80th Birthday Felicitacion Volume, Part III</ce:title>. <<http://www.sciencedirect.com/science/article/pii/S0378375802003087>>.
- PALLEROSI, C.; MAZZOLINI, L.; MAZZOLINI, B. *Confiabilidade humana: Conceitos, Análises, Avaliação e Desafios*. ALL PRINT, 2011. ISBN 9788577189830. <<http://books.google.com.br/books?id=eFicpwAACAAJ>>.
- PAPOULIS, A. *Probability, Random Variables, and Stochastic Processes*. 3rd. ed. New York: McGraw-Hill, 1991.
- PETERSON, J. *Petri Net Theory and the Modeling of Systems*. [S.l.]: Prentice Hall PTR Upper Saddle River, NJ, USA, 1981.
- PORCIÚNCULA, G. S. *Sistematização do processo da análise de falha em sistemas automáticos*. Tese (Doutorado) — Universidade Federal de Santa Catarina, Florianópolis, SC, 2009.

PRESLEY, A. R. *A representation method to support enterprise engineering*. Tese (Doctor of Philosophy) — Faculty of the Graduate School of University of Texas at Arlington, Arlington, 1997.

REASON, J. *Managing the risk of organizational accidents*. England: Ashgate Publishing Limited, 1997.

RIGONI, E. *Metodologia para Implantação da Manutenção Centrada na Confiabilidade: uma abordagem fundamentada em Sistemas Baseados em Conhecimento e Lógica Fuzzy*. Tese (Doutorado) — Universidade Federal de Santa Catarina (UFSC), Florianópolis, SC, 2009.

RODRIGUEZ, C. P. *Análise de risco em operações de “offloading” – Um modelo de avaliação probabilística dinâmica para a tomada de decisão*. Tese (Doutorado) — Universidade de São Paulo, 2012.

SAE (Society of Automotive Engineers). *JA1011: Evaluation criteria for reliability-centered maintenance (RCM) processes*. Warrendale, PA, 1999.

_____. *J1739: Potential Failure Mode and Effects Analysis in Design (Design FMEA) and Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA) Reference Manual*. [S.l.], 2000.

SAKURADA, E. Y. *As técnicas de análise dos modos de falhas e seus efeitos e análise da árvore de falhas no desenvolvimento e na avaliação de produtos*. Dissertação (Mestrado) — Universidade Federal de Santa Catarina, Florianópolis, SC, 2001.

SAKURADA, E. Y.; ANDRADE, B. L. R. *Implantação de Laboratório para Análise e Avaliação de Risco: Estudo de confiabilidade da máquina do leme – Itabuna*. São Paulo, 2007. Relatório técnico CNPQ.

SANABRIA, J. A. *Metodologia para análise de confiabilidade em robôs com aplicação em robô paralelo*. Dissertação (Mestrado) — Universidade Federal de Santa Catarina, Florianópolis, SC, Maio 2012.

SIDDIQUI A. W.; BEN-DAYA, M. *Handbook of Maintenance Management and Engineering*. 1. ed. Springer-Verlag London Ltd: Springer, 2009. 397-415 p.

SILJAK, D. *Large-Scale Dynamic Systems: Stability and Structure*. 1. ed. New York: Elsevier Science Ltd, 1978. 432 p.

SIU, N. Risk assessment for dynamic systems: an overview. *Reliability engineering & systems safety*, Elsevier, v. 43, n. 1, p. 43–73, 1994.
<<http://www.sciencedirect.com/science/article/pii/0951832094900957>>.

SMITH, A. M. *Reliability-centered maintenance*. Boston, MA: Mc Graw Hill, 2001.

SOBOL, I. *O método de Monte Carlo*. Tradução de M. DOMBROVSKY. Moscou: Editora Mir, 1983. 64 p.

SOUZA, F. S.; FIRMINO, P. R.; DROGUETT, E. A. L. A análise de confiabilidade humana: Uma revisão comentada da literatura. In: *XLII SBPO – Sociedade Brasileira de Pesquisa Operacional*. Bento Gonçalves, RS: Anais do XLII SBPO, 2010.

- STAMATELATOS, M.; APOSTOLAKIS, G.; DEZFULI, H.; EVERLINE, C.; GUARRO, S.; MOIENI, P.; MOSLEH, A.; PAULOS, T.; YOUNGBLOOD, R. Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners. *Office of Safety and Mission Assurance NASA Headquarters, Washington, DC. March*, v. 31, 2002.
- STAMATIS, D. H. *Failure mode and effects analysis: FMEA from theory to execution*. 7. ed. Milwaukee: ASQC Quality Press, 1995.
- SWAMINATHAN, S.; SMIDTS, C. Identification of missing scenarios in esds using probabilistic dynamics. *Reliability Engineering and System Safety*, v. 66, n. 3, p. 275 – 279, 1999. ISSN 0951-8320. <<http://www.sciencedirect.com/science/article/pii/S0951832099000241>>.
- _____. The mathematical formulation for the event sequence diagram framework. *Reliability Engineering and System Safety*, Elsevier, v. 65, n. 2, p. 103 – 118, 1999. ISSN 0951-8320. <<http://www.sciencedirect.com/science/article/pii/S0951832098000921>>.
- _____. The Event Sequence Diagram framework for dynamic Probabilistic Risk Assessment. *Reliability Engineering and System Safety*, Elsevier, v. 63, n. 1, p. 73–90, 1999.
- TANAKA, T.; KUMAMOTO, H.; INOUE, K. Evaluation of a dynamic reliability problem based on order of component failure. *Reliability, IEEE Transactions on*, v. 38, n. 5, p. 573–576, 1989.
- UFSC (Universidade Federal de Santa Catarina). NEDIP (Núcleo de Desenvolvimento Integrado de Produtos). *MT-PR-RT-NE-01: IDEF0 dos processos relacionados à manipulação do SF₆*. Revisão 4. Florianópolis, 2008. Relatório do projeto MitiSF6.
- USA (United States of America). DOD (Department of Defense). *MIL-STD-1629A: Procedures for performing a failure mode, effects and criticality analysis*. Washington, 1980.
- VARGAS, E. High availability fundamentals. *Sun Blueprints series*, Novembro 2000.
- VINADÉ, C. *Sistematização do Processo de projeto para Confiabilidade e Manutenibilidade aplicado a sistemas Hidráulicos e Implementação de um Sistema Especialista*. Tese (Doutorado) — Universidade Federal de Santa Catarina, Florianópolis, SC, 2003.
- WANG, Y.; ENACHESCU, M.; COTOFANA, S.; FANG, L. Variation tolerant on-chip degradation sensors for dynamic reliability management systems. *Microelectronics Reliability*, 2012. ISSN 0026-2714. <<http://www.sciencedirect.com/science/article/pii/S0026271412002351>>.
- WERNER, L. *Modelagem dos tempos de falhas ao longo do calendário*. Dissertação (Mestrado) — Programa de Pós-Graduação em Engenharia de Produção. Universidade Federal do Rio Grande do Sul, Porto Alegre, 1996.
- XU, H.; XING, L.; ROBIDOUX, R. Drbd-dynamic reliability block diagrams for system reliability modelling. *International journal of computers applications*, Acta Press, v. 31, n. 2, p. 132–141, 2008.

XUE, J.; YANG, K. Dynamic reliability analysis of coherent multistate systems. *Reliability, IEEE Transactions on*, v. 44, n. 4, p. 683–688, Dec. 1995.

ZHU, D. *Integrating software behavior into dynamic probabilistic risk assessment*. Tese (Doutorado) — University of Maryland, 2005.

ZÜRN, H. H. *Processos Estocásticos em Engenharia Elétrica*. 2009. Notas de aula, Universidade Federal de Santa Catarina.

APÊNDICE A – Conceitos e definições

Neste capítulo são apresentadas as definições relacionadas com a confiabilidade em sistemas.

A análise de confiabilidade realizada usualmente é a análise de confiabilidade estática. Tanto neste tipo de análise, quanto na análise de confiabilidade dinâmica existem termos, parâmetros e abordagens que, antes de tudo, devem estar definidos da forma mais objetiva possível.

A.1 SISTEMA

No cotidiano, depara-se frequentemente com o termo **sistema**. Pode-se citar como exemplos: sistemas de controle, sistemas de segurança, sistema de áudio/vídeo, sistema de monitoramento, etc. O termo é utilizado em diversas áreas e, para a área tecnológica, pode-se utilizar a definição apresentada por Hubka e Eder (1988):

Conjunto finito de elementos reunidos para formar um todo sob certas regras bem definidas, por meio das quais existem determinadas relações precisas definidas entre os elementos e para com seu ambiente [...].

Sistema, subsistema e componente são termos que estão associados à conjuntos de elementos (sejam mecanismos ou processos) e a distinção entre eles é relativa, ou seja, variam de acordo com cada caso em estudo e também do ponto de vista do analista. Por exemplo, em uma análise uma bomba de engrenagens pode ser tratada como um sistema e seus elementos internos como componentes e, em uma outra análise a mesma bomba pode ser tratada com um componente inserido em um subsistema de potência, que por sua vez faz parte de um sistema hidráulico. Dependendo do problema que está sendo estudado, da extensão atingida pela falha, da formação da equipe, entre outros fatores, será definido como sistema, subsistema ou componente.

Na área tecnológica comumente utiliza-se o termo **sistema técnico** quando se refere à máquinas, equipamentos e *softwares*. Segundo Calil (2009), o termo pode ser definido como “um conjunto de equipamentos e instalações que têm uma (ou mais) função para ser desempenhada e, a todo o momento, está interagindo como o ambiente, o homem e outros sistemas técnicos, influenciando e sendo influenciado”. Assim, os sistemas utilizados no âmbito da engenharia são sistemas técnicos.

Segundo De Negri e Santos (2007) os sistemas podem ser representados por modelos a fim de facilitar a análise e o projeto, sendo realizadas descrições simplificadas que enfatizam certos detalhes ou propriedades enquanto outros são suprimidos. Essa atividade de representar por modelos é denominada de modelagem e pode ser desenvolvida segundo as **perspectivas funcional, estrutural e comportamental**.

De forma resumida, pode-se descrever os modelos da seguinte maneira (DE NEGRI; SANTOS, 2007):

- O **modelo funcional** apresenta a função de cada item do sistema e a inter-relação entre eles. A realização das funções de cada um dos itens reflete na função global do sistema. Pode-se citar exemplos como os circuitos elétricos, pneumáticos e hidráulicos. O modelo funcional responde a pergunta “**O que** o

sistema faz?”.

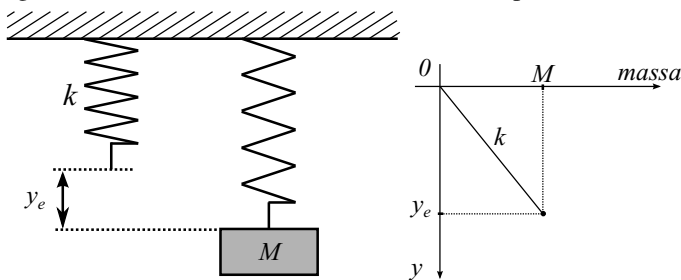
- O **modelo estrutural** representa como os itens do sistema estão relacionados entre si, por meio de conexões físicas, ou de comunicação ou relações hierárquicas. Pode-se citar como exemplos os desenhos mecânicos e maquetes do sistema. O modelo estrutural responde a pergunta “**Onde** as funções estão implementadas?”.
- O **modelo comportamental** responde a pergunta “**Como** ou **quando** uma função é executada?”. Como exemplo de modelo comportamental pode-se citar uma equação matemática, uma implementação comutacional onde se observa as variáveis de controle do sistema ao longo do tempo, etc.

Assim, no texto desta tese, quando um sistema for designado como estático, significa que a modelagem adotada para o sistema é um modelo comportamental que o descreve de forma estática, ou seja, as suas características ou variáveis não variam com o tempo. Esse mesmo sistema pode ter um modelo comportamental que o representa dinamicamente. Dessa forma, as suas características que variam no tempo descritas e analisadas no modelo.

Segundo Ogata (2004), Botta et al. (2006) e Georges (2005) quando se descreve um sistema por meio de um modelo comportamental estático, as variáveis de saída dependem apenas dos valores de entrada do presente. Assim, se não houver alteração no valor de entrada, o resultado na saída permanece constante.

Para ilustrar a modelagem de um sistema como estático e dinâmico, considere a Figura A.1. Inicialmente, analisa-se o sistema massa-mola sob o ponto de vista estático. O deslocamento y_e da extremidade da mola depende da massa M e da constante elástica k – considerada constante. Desta forma, se for adicionado um valor extra de massa (entrada do sistema), o deslocamento y_e (saída do sistema) sofrerá um acréscimo proporcional. Não importa o tempo que a massa esteja acoplada na mola, o deslocamento será sempre o mesmo.

Figura A.1 – Sistema massa-mola – modelo comportamental estático



O modelo matemático que descreve o deslocamento da extremidade da mola, y_e , é representado pela Equação A.1, sendo g a aceleração da gravidade.

$$y_e = \frac{M \cdot g}{k} \quad (\text{A.1})$$

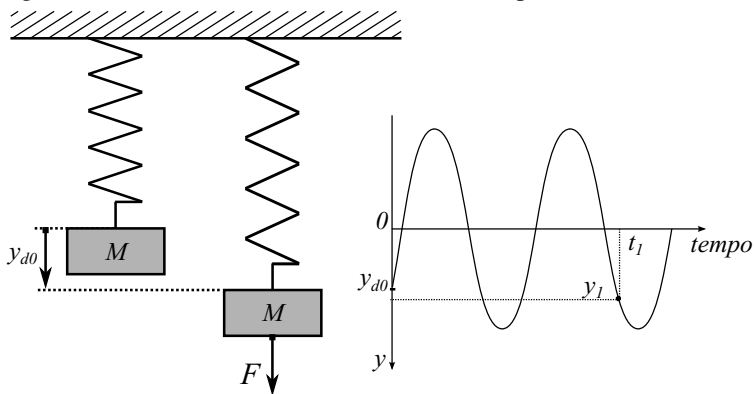
O termo **sistema dinâmico** é frequentemente encontrado nos textos relacionados com a análise de confiabilidade dinâmica. O termo refere-se a sistemas que utilizam **modelos comportamentais que levam em consideração características dinâmicas**, ou seja, possuem variáveis que sofrem alterações ao longo do tempo.

Segundo Ogata (2004, p. 2), as variáveis de saída dos modelos comportamentais dinâmicos no tempo presente, dependem dos valores de entrada do passado e do presente. Neste caso, se o sistema não estiver em equilíbrio, os valores de saída variam com o tempo.

A Figura A.2 apresenta um sistema massa-mola no qual foi considerado um modelo comportamental dinâmico. Inicialmente é imposto um deslocamento y_{d0} , por meio da força F , na massa M acoplada na extremidade da mola – entrada do sistema. Ao liberar a massa, a extremidade da mola desenvolve um movimento oscilatório conforme uma onda senoidal.

Para determinar a posição y_1 , ou suas derivadas, no tempo t_1 é preciso saber, além do valor da massa M e da constante elástica k , o valor da força F ou o deslocamento inicial imposto y_{d0} . Assim, seguindo a definição de Ogata (2004), os valores de saída (y e suas derivadas) do presente, no tempo t_1 , dependem dos valores de entrada do passado ($M(t=0)$, $k(t=0)$, F ou y_{d0}) e do presente ($M(t=t_1)$, $k(t=t_1)$).

Figura A.2 – Sistema massa-mola – modelo comportamental dinâmico



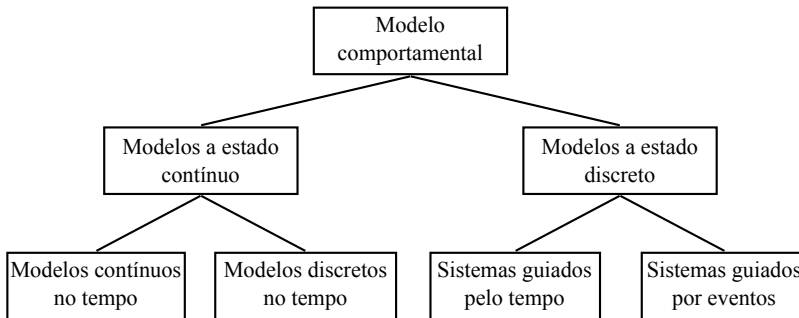
O modelo matemático que descreve o comportamento da variável y ao longo do tempo é obtido da Equação A.2.

$$M \cdot \frac{d^2 y}{dt^2} + k \cdot y - F = 0 \quad (\text{A.2})$$

A parcela dinâmica do modelo está incorporada na variável d^2y/dt^2 , que representa a aceleração. Portanto, para o mesmo sistema massa-mola é possível analisá-lo sob a ótica de uma modelagem estática e também dinâmica.

De Negri e Santos (2007) apresenta uma classificação de modelos comportamentais em função dos tipos de sinais¹ processados pelo sistema, que podem ser organizados de acordo com a Figura A.3.

Figura A.3 – Classificação dos modelos comportamentais



Fonte: De Negri e Santos (2007)

Assim, os modelos comportamentais podem ser inicialmente classificados em modelos a **estado contínuo** ou a **estado discreto**. No primeiro caso, são modelos que descrevem o sistema utilizando variáveis de estado, entradas e saídas com amplitude contínua. No segundo, as variáveis de estado, entradas e saídas possuem amplitude discreta, ou seja, assumem valores determinados dentro de um intervalo de existência. A mudança de um estado do sistema para outro é denominada de transição de estado.

O modelo a estado contínuo ainda pode ter uma subdivisão em dois grupos: modelos contínuos no tempo e modelos discretos no tempo. Quando o modelo é contínuo no tempo tanto a amplitude dos sinais quanto a variável independente são contínuas, isto é, o sistema opera sobre entradas analógicas e produz saídas e estados analógicos. Sistemas modelados desta forma são denominados **sistemas contínuos no tempo**.

Os modelos discretos no tempo possuem a amplitude dos sinais contínua, mas a variável independente é discreta, ou seja, as variáveis de saída e de estados são modificadas somente em instantes discretos. Os sistemas modelados desta forma são denominados de **sistemas discretos no tempo** e, normalmente, são expressos por meio de equações de diferenças.

Os modelos a estado discreto podem ser **guiados pelo tempo** ou **guiados por eventos**. Para o caso dos sistemas guiados pelo tempo, as mudanças são sincronizadas

¹Os sinais podem ser variáveis físicas observáveis, cujo estado ou parâmetros associados com o tempo portam a informação. Ou variáveis de uma função matemática associadas com as entradas, saídas ou processamento do sistema (DE NEGRI; SANTOS, 2007).

com o tempo, pois, a cada instante marcado por um relógio interno², um evento (ou nenhum) é selecionado provocando uma transição de estado. O relógio é responsável por qualquer possível mudança de estado. Por outro lado, para o caso dos modelos a estado discreto guiados por eventos, a ocorrência dos eventos independe dos instantes marcados pelo relógio.

Os sistemas ainda podem apresentar uma característica determinística ou aleatória. Um sistema é determinístico se, dado um vetor de variáveis de entrada para um determinado tempo $t \geq t_0$, então o estado do sistema $x(t)$ poderá ser calculado. Já nos sistemas estocásticos o estado $x(t)$ é um vetor de variáveis aleatórias e somente a distribuição de probabilidades poderá ser calculada e não o estado do sistema.

Portanto, a partir da análise das várias definições de sistemas, foi possível estabelecer uma definição para sistema dinâmico, sendo esta apresentada no Quadro A.1.

Quadro A.1 – Sistema dinâmico

Conjunto de elementos organizados que possuem uma (ou mais) função para ser desempenhada, cuja modelagem comportamental considera alterações na configuração, nas variáveis de estado do sistema ou em alguma característica de seus componentes ao longo do tempo.

Desta forma, de acordo com a análise feita sobre o sistema e o modelo comportamental adotado, uma ponte – por exemplo – pode ser um sistema dinâmico; basta que tenha carregamentos dinâmicos ou corrosão da estrutura metálica – elementos que afetam as características dos componentes ao longo do tempo, e conseqüentemente, o sistema.

As alterações da configuração de um sistema são mudanças que podem ocorrer causadas por eventos, tais como: falha de componentes, atuação de um controlador, intervenção humana, entre outros fatores. Pode-se citar alguns exemplos:

- Um reservatório cuja variável de saída seja o nível do fluido. Altera-se os estados dos componentes (ligando/desligando bombas e válvulas) em função do nível do fluido no reservatório.
- Uma máquina de lavar roupas cuja variável de saída seja o grau de limpeza das roupas. Para determinados estágios do processo de lavagem a máquina passa por diferentes estados, acionando/desacionando componentes.
- Um ambiente em que a temperatura deva permanecer em determinada faixa. Para determinados níveis de temperatura, altera-se os estados dos aquecedores ou dos trocadores de calor.

Nos exemplos apresentados ocorrem mudanças na configuração do sistema ao longo do tempo, isto é, alguns componentes ora participam, ora ficam desativados. Desta forma, as configurações dos sistemas podem mudar em função dos valores das

²Por exemplo, relógio interno dos microcomputadores.

variáveis de saída (nível, limpeza, temperatura), atuação humana ou de controlador, condição dos componentes, tempo de operação entre outros fatores.

A.2 MANTENABILIDADE

Formalmente, o termo *manutenibilidade* é definido pela norma NBR 5462 (ABNT, 1994) como:

Capacidade de um item ser mantido ou recolocado em condições de executar suas funções requeridas, sob condições de uso especificadas, quando a manutenção é executada sob condições determinadas e mediante procedimentos e meios prescritos.

A *manutenibilidade* é um parâmetro de desempenho que indica a capacidade de recolocar o equipamento em operação. Tal parâmetro está associado com a capacitação da equipe, programas de manutenção e recursos disponíveis como equipamento, mão de obra e instalação.

Este parâmetro irá influenciar diretamente na disponibilidade do sistema e está associado com o tempo médio de reparo – *Mean time to repair* (MTTR).

A.3 CONFIABILIDADE E PROBABILIDADE DE FALHA

A *confiabilidade* e a *probabilidade de falha* são eventos complementares, e portanto, serão abordadas juntas nesta seção. Inicialmente serão tratados os conceitos relacionados à *confiabilidade*.

A norma NBR 5462 (ABNT, 1994) define *confiabilidade* como: a “**capacidade** de um item desempenhar uma função requerida sob condições especificadas, durante um dado intervalo de tempo”. Geralmente, a *confiabilidade* está associada a um valor de **probabilidade**, possibilitando dessa forma quantificar essa capacidade. Esta definição de *confiabilidade* é a estática. Mais adiante será apresentada a definição de *confiabilidade* dinâmica.

No trabalho escrito por Dias (1996, p. 24) várias definições de *confiabilidade* são apresentadas, nas quais o autor identificou quatro estruturas fundamentais: “**probabilidade, comportamento adequado, período de uso (ou de vida) e condições de uso**”.

Ainda que a definição descrita na NBR 5462 (ABNT, 1994) pareça menos restritiva, ela contempla todos os elementos identificados por Dias (1996). O termos empregados na definição da norma estão relacionados com as estruturas fundamentais no Quadro A.2.

Assim, a *confiabilidade* é um parâmetro de desempenho do sistema em relação à capacidade de operar e realizar funções, para um dado período de tempo sob condições específicas em projeto. Este parâmetro pode ser interpretado como uma qualidade do produto em relação ao projeto e à fabricação.

Quadro A.2 – Elementos da definição da norma NBR 5462

NBR 5462 (ABNT, 1994)	Elementos identificados por Dias (1996)
Capacidade	Probabilidade
Função	Comportamento adequado
Intervalo de tempo	Período de uso (ou de vida)
Condições especificadas	Condições de uso

A confiabilidade de um componente pode ser obtida por meio de ensaios experimentais ou de uso. A Equação A.3 é usada para o cálculo da confiabilidade $R(x)$.

$$R(x) = \frac{N_s(x)}{N_0(0)} \quad (\text{A.3})$$

onde

x = vida do componente, geralmente expressa em tempo, mas pode ser utilizado o número de ciclos, número de rotações, etc;

$N_s(x)$ = quantidade de componentes em bom funcionamento para a vida x ;

$N_0(0)$ = quantidade de componentes, em bom funcionamento, no início do ensaio;

Comumente, é realizada a contagem da quantidade de componentes que falharam, $N_f(x)$, ao invés dos componentes que estão em bom funcionamento. Desta forma, sabendo que $N_0(0) = N_s(x) + N_f(x)$, pode-se reescrever a Equação A.3 com base na quantidade de componentes que falharam,

$$\begin{aligned} R(x) &= \frac{N_s(x)}{N_0(0)} \\ &= \frac{N_0(x) - N_f(x)}{N_0(0)} \\ &= 1 - \frac{N_f(x)}{N_0(0)} \end{aligned} \quad (\text{A.4})$$

O termo $N_f(x)/N_0(0)$ presente na Equação A.4 representa a probabilidade de falha, razão entre os componentes que falharam – para um período de vida x – e a quantidade de componentes no início do ensaio.

Segundo Dias (1996) a **probabilidade de falha**, $Q(x)$, ou não-confiabilidade, pode ser definida como a probabilidade de um item não desempenhar a função requerida, ou seja, não estar em falha para um determinado período de uso, sob determinadas condições de operação previamente estabelecidas.

Assim, pode-se reescrever a Equação A.4 em função de $Q(x)$,

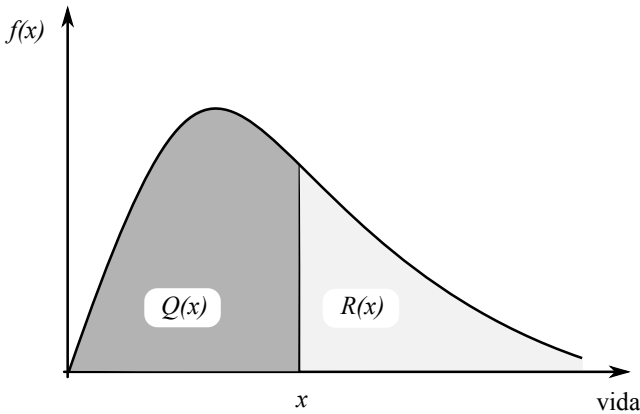
$$R(x) = 1 - Q(x) \quad (\text{A.5})$$

A Equação A.5 demonstra que a confiabilidade e a probabilidade de falha são eventos complementares. Esta equação, quando derivada, fornece a função densidade de probabilidade de falha, $f(x)$, apresentada na Equação A.6.

$$f(x) = \frac{dF(x)}{dx} = -\frac{dR(x)}{dx} = \frac{1}{N_0} \frac{dN_f(x)}{dx} \quad (\text{A.6})$$

Graficamente, a função densidade de falha $f(x)$, confiabilidade $R(x)$ e probabilidade de falha $Q(x)$ podem ser representados de acordo com a Figura A.4.

Figura A.4 – Função densidade de probabilidade de falha hipotética $f(x)$ em função da vida x



Fonte: Billinton e Allan (1992)

Assim, os valores da probabilidade de falha $Q(x)$ e da confiabilidade $R(x)$ ficam definidas pela área sob a curva da função densidade de falha, conforme a Figura A.4. Matematicamente, pode ser escrita como apresentado nas Equações A.7 e A.8:

$$Q(x) = \int_0^x f(x) dx \quad (\text{A.7})$$

$$R(x) = 1 - \int_0^x f(x) dx = \int_x^{\infty} f(x) dx \quad (\text{A.8})$$

A maior dificuldade de se obter a confiabilidade por meio de ensaios experimentais é o custo e o tempo demandado para a realização dos ensaios, pois além do tempo de preparação, realização e tratamento dos dados é preciso ter um tamanho de amostra significativo.

Assim, o que é feito na maioria dos casos é recorrer à banco de dados de falhas. Geralmente, as informações obtidas de banco de dados são valores de taxa de falha, λ , que obedecem uma distribuição exponencial.

A taxa de falhas, é a relação entre o número de componentes que falharam em um dado intervalo de uso x (tempo, ciclos, rotações, etc) e o número total de componentes expostos à falha, Equação A.9, (DIAS, 1996):

$$\lambda(x) = \frac{n^{\circ} \text{ de falhas por unidade de uso}}{n^{\circ} \text{ de componentes expostos à falha}} \quad (\text{A.9})$$

No entanto, vale ressaltar que as taxas de falhas contidas nos banco de dados, muitas vezes, são valores pessimistas o que resulta em um valor de confiabilidade muito baixo. Desta forma, é preciso cautela no uso desses valores para que o modelo calculado seja realmente uma representação próxima do sistema real.

Uma das funções densidades de probabilidade, $f(x)$, mais utilizadas é a distribuição exponencial, Equação A.10.

$$f(x) = \lambda e^{-\lambda x} \quad (\text{A.10})$$

Para esta distribuição, o cálculo da confiabilidade é realizado com a Equação A.11, tendo como entrada de dados a vida, x , e a taxa de falhas, λ .

$$R(x) = e^{-\lambda x} \quad (\text{A.11})$$

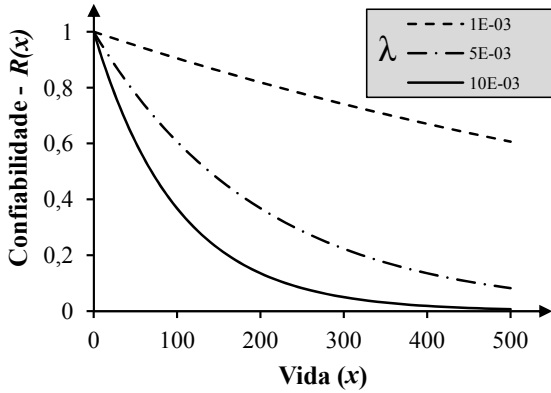
Paralelamente, a probabilidade de falha é calculada com o complemento da confiabilidade, Equação A.12.

$$Q(x) = 1 - e^{-\lambda x} \quad (\text{A.12})$$

A Figura A.5 é uma representação gráfica da Equação A.11 para três valores distintos de taxa de falha: $1 \cdot 10^{-3}$, $5 \cdot 10^{-3}$ e $10 \cdot 10^{-3}$ falhas/hora. É possível constatar que, visualizando o comportamento das três curvas apresentadas no gráfico, o aumento da taxa de falhas resulta em uma queda mais acentuada da confiabilidade, $R(x)$, ao longo da vida x . Isto significa que, para um mesmo x , um sistema com maior taxa de falha possui uma menor confiabilidade, conseqüentemente uma maior probabilidade de falha.

Carvalho (2007) disserta de forma detalhada sobre os banco de dados de falhas existentes, suas origens e características. Para o uso das taxas de falhas em componentes, deve-se atentar às características e aplicações para os quais foram desenvolvidos os bancos de dados – buscando dessa maneira aproximar o modelo com o sistema real que está sendo analisado.

Figura A.5 – Confiabilidade em função do tempo para distribuição exponencial



Além da distribuição exponencial, podem ser utilizadas outras distribuições, tais como: log-normal, Weibull e gamma. Entre essas, destaca-se a distribuição Weibull, que pode assumir a forma de uma distribuição exponencial, ou aproximadamente de uma distribuição de Rayleigh ou de uma distribuição Gaussiana, dependendo dos valores do seu parâmetro de forma.

Maiores detalhes, com a descrição da manipulação matemática das equações relacionadas com confiabilidade podem ser encontrados em Dias (1996), Bertsche (2008) e Billinton e Allan (1992).

A.4 DISPONIBILIDADE

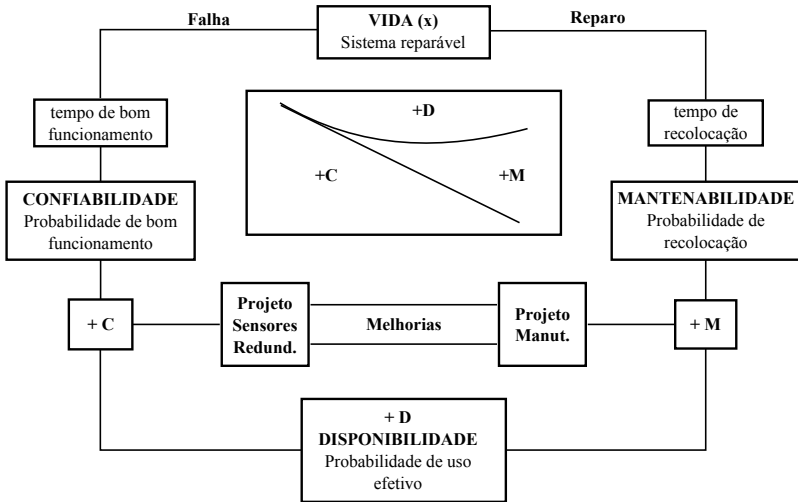
De acordo com a norma NBR 5462 (ABNT, 1994) o termo disponibilidade é definido como:

Capacidade de um item estar em condições de executar uma certa função em um dado instante ou durante um intervalo de tempo determinado, levando-se em conta os aspectos combinados de sua confiabilidade, manutenibilidade e suporte de manutenção, supondo que os recursos externos requeridos estejam assegurados.

A Figura A.6, apresenta a relação entre confiabilidade (C), manutenibilidade (M) e disponibilidade (D). A disponibilidade de um sistema está diretamente relacionada com a manutenibilidade e a confiabilidade. Um item que possui uma manutenibilidade elevada significa, em poucas palavras, que caso ocorra uma falha, esta será eliminada rapidamente, colocando o sistema novamente em funcionamento. Já uma confiabilidade elevada no sistema irá indicar que o sistema é pouco suscetível às falhas ao longo de

sua vida. Esses dois parâmetros irão garantir que o sistema terá poucas “paradas”, o que garante tempo de operação, ou seja, disponibilidade.

Figura A.6 – Correlação entre confiabilidade, manutenibilidade e disponibilidade para produtos reparáveis



Fonte: Dias (1996)

Portanto, o aumento na confiabilidade do sistema (+C) – por meio de ações no projeto –, bem como o aumento da manutenibilidade (+M) – por meio das ações na manutenção – resultam no aumento da disponibilidade (+D) do sistema.

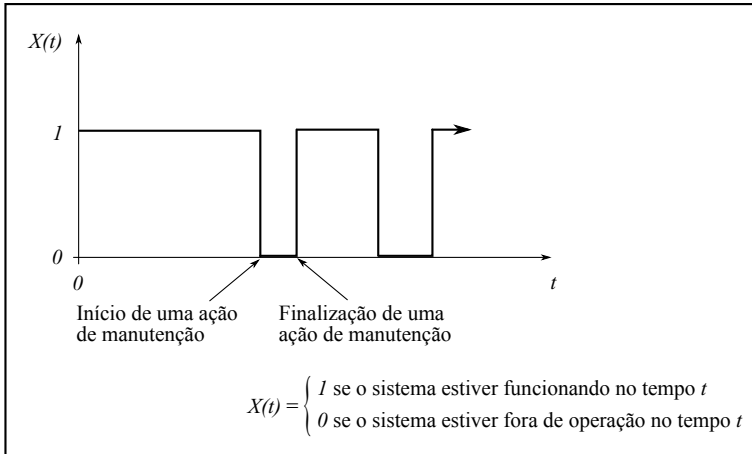
A Figura A.7 apresenta um sistema técnico em que estão representados os estados do sistema técnico em funcionamento e fora de operação. A figura será utilizada para demonstrar o conceito de disponibilidade.

Assim, a partir do comportamento $X(t)$ do sistema técnico, pode-se definir a disponibilidade instantânea $D(t)$ como a probabilidade do sistema estar em funcionamento no instante t , Equação A.13.

$$D(t) = P[X(t) = 1] \quad (\text{A.13})$$

A disponibilidade instantânea $D(t)$ é um valor difícil de se obter e é pouco utilizada na prática. Segundo Cassady e Pohl (2003), ao invés de se trabalhar com a disponibilidade instantânea, costuma-se fazer uso da variável denominada disponibilidade estacionária D – recebe esta denominação porque seu valor é constante quando t tende a infinito –, apresentada na Equação A.14.

$$D = \lim_{t \rightarrow \infty} D(t) = \frac{\mu}{\lambda + \mu} \quad (\text{A.14})$$

Figura A.7 – Comportamento da variável $X(t)$ ao longo do tempo

Fonte: Cassady e Pohl (2003)

Em muitas aplicações, as taxas de falha e de reparo, são consideradas constantes ao longo do seu período de uso. Nesses casos, o MTBF (tempo médio entre falhas) é o inverso da taxa de falhas λ e o MTTR (tempo médio de reparo) é o inverso da taxa de reparo μ (CARVALHO, 2008). Assim, por meio da Equação A.15, calcula-se a disponibilidade estacionária, D .

$$D = \frac{\mu}{\lambda + \mu} = \frac{MTBF}{MTBF + MTTR} \quad (\text{A.15})$$

O valor do MTBF está relacionado com a confiabilidade, já que quanto maior for o tempo médio entre as falhas, maior será o período de tempo que o sistema cumpre a sua função e, conseqüentemente, maior será sua confiabilidade. Enquanto que o MTTR está relacionado com a manutenibilidade, visto que quanto menor for o tempo de reparo, maior será a manutenibilidade do sistema.

Desta forma, ao analisar a Equação A.15, percebe-se que mesmo que o sistema tenha uma confiabilidade baixa, ou seja, tempo médio entre falhas baixo este ainda pode ter uma disponibilidade (D) elevada – basta que tenha um valor de MTTR pequeno comparado ao MTBF.

Assim, para os sistemas que possuem valores de confiabilidade baixos, é fundamental que se tenha elevada manutenibilidade para garantir que se tenha disponibilidade. No artigo escrito por Vargas (2000) o autor descreve aspectos básicos de confiabilidade e disponibilidade em *hardwares*, onde garantir a disponibilidade de sistemas é muito

importante não só do ponto de vista do custo monetário, mas também para reputação da empresa.

Maiores detalhes sobre a função disponibilidade podem ser encontrados em Carvalho (2008), Billinton e Allan (1992) e Cassady e Pohl (2003).

A.5 RISCO

A análise de confiabilidade tem uma relação muito próxima com a gestão de risco. Antes de tratar da gestão do risco, o termo “risco” foi analisado por Calil (2009), onde após analisar vários trabalhos, apresentou a seguinte definição:

Risco é a chance de ocorrência de um estado futuro “ x ”, dada a ocorrência de um estado inicial – que pode ser expressa pela probabilidade condicional $P(\text{Estado futuro “}x\text{”}|\text{Estado inicial})$ –, sendo necessário para sua completa caracterização o delineamento dos dois estados, além dos cenários que possibilitem esta transição (que compõem o perfil do risco).

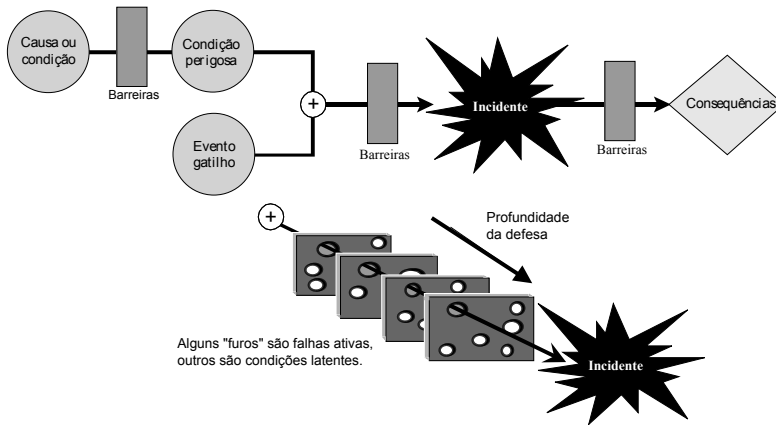
Em outras palavras, analisa-se a chance de ocorrer um estado futuro, geralmente um evento indesejado, um incidente. Para isso, parte-se da hipótese de ocorrência de um evento inicial e considera-se os possíveis cenários que poderiam conduzir àquele estado futuro.

A Figura A.8 é um modelo, adaptado de Mosleh et al. (2004) e Reason (1997), que pode ser utilizado para representar o desencadeamento de um incidente. O processo tem início com um evento inicial, representado por um círculo contendo a expressão “causa ou condição” que, ao atravessar as barreiras, conduz a uma “condição perigosa”. Esta, quando associada a um “evento gatilho”, pode levar à um incidente, se as barreiras de proteção falharem.

A relação entre a análise de confiabilidade e de risco é que o foco principal da primeira análise, geralmente, está sobre a função equipamento. Assim, tomando como referência a Figura A.8, a análise de confiabilidade estaria associada com os eventos que poderiam conduzir ao incidente, ou seja, “causa ou condição”, “condição perigosa” e as “barreiras”. O “evento gatilho” é um evento que se busca antecipar nas análises de confiabilidade, mas muitas vezes ocorrem de forma imprevista.

A análise de risco corresponde à Figura A.8 por completo. Desta forma, este tipo de análise tem um foco mais abrangente e busca avaliar as consequências que uma falha no sistema poderia gerar para os operadores do sistema, para a população, para o meio ambiente, etc. Assim, uma análise de confiabilidade é extremamente importante para a análise de risco, principalmente, como uma etapa inicial de entrada de dados.

Figura A.8 – Desencadeamento de um incidente



Fonte: Dias et al. (2011)

A.6 PROCESSO ESTOCÁSTICO

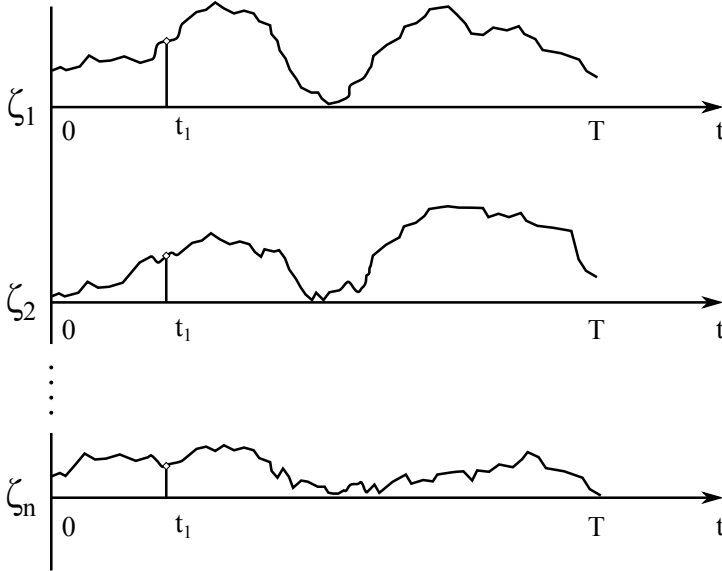
Segundo Moura (2006) processo estocástico é uma família de variáveis aleatórias indexadas no tempo que descreve o comportamento dinâmico de algum processo – sendo este físico, químico, biológico, etc.

Papoulis (1991) descreve o processo estocástico matematicamente como $X(t, \zeta)$, onde $X(t_i, \zeta)$ é uma variável aleatória para um dado instante determinado i e $X(t, \zeta_j)$ é a função temporal, ou função amostra, correspondente ao resultado de um experimento ζ_j . Portanto, quando as variáveis (t ou ζ) são escritas acompanhadas dos índices (i ou j), significa que são casos particulares das variáveis, ou seja, t_i é um instante de tempo determinado i para várias amostragens ou observações. Em contrapartida, ζ_j é uma amostragem específica j , acompanhada ao longo do tempo.

A Figura A.9 é uma representação gráfica de n resultados, ζ , com comportamento estocástico entre $0 \leq t < T$. Por exemplo, ζ_1 poderia ser o monitoramento, em uma dada região, da quantidade de chuva ao longo do ano 1990, ζ_2 do ano 1991 e assim por diante. Cada acompanhamento anual da quantidade de chuva corresponde à uma função amostra, ζ_j . Ao se fazer a leitura da quantidade de chuva para uma data específica t_1 de vários anos, obtém-se valores de variável aleatória $X(t_1, \zeta)$. Com esses valores, pode-se realizar análises estatísticas para o obter o valor médio da quantidade de chuva e assim, tomar ações preventivas para os períodos críticos onde ocorrem chuvas em excesso ou períodos de seca.

Desta forma, os processos estocásticos são importantes não pelos valores da variável aleatória, mas pelos tipos de distribuição de probabilidade (normal, log-normal, exponencial, Weibull, etc) obtidos, valores característicos da variável de

Figura A.9 – Funções amostra ou realizações do processo



Fonte: Zürn (2009)

aleatória – médias, máximos, mínimos, dispersão, etc. Com essas informações, pode-se realizar simulações cujos resultados serão utilizados nas etapas de projeto, operação, manutenção e uso dos sistemas técnicos.

A.7 ESTADO DE UM COMPONENTE

O estado do componente traz duas informações importantes: uma com relação à condição funcional (sem falha, com falha evidente ou com falha oculta) e outra com relação à condição operacional (ligado ou desligado).

Assim, os estados dos componentes são definidos com base nas possíveis combinações das condições funcionais e operacionais, conforme apresentado no Quadro A.3.

Na Figura A.10 estão representados todos os estados dos componentes, bem como as transições. Cada estado do componente está representado por um círculo; os arcos representam as transições de um estado para outro; e os retângulos com linhas tracejadas representam as condições funcionais.

Em condições normais de operação – ou seja, sem falha –, um componente pode mudar de “ligado” para “desligado” (transição a) e de “desligado” para “ligado”

Quadro A.3 – Condição funcional e operacional dos componentes

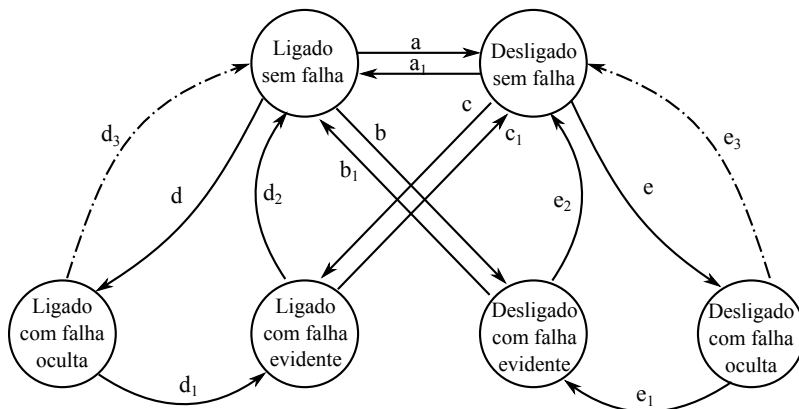
Condição		Estados dos componentes
Funcional	Operacional	
Sem falha	Ligado	Sem falha ligado
	Desligado	Sem falha desligado
Com falha evidente	Ligado	Com falha evidente ligado
	Desligado	Com falha evidente desligado
Com falha oculta	Ligado	Com falha oculta ligado
	Desligado	Com falha oculta desligado

(transição a_1).

A falha evidente é caracterizada pela mudança da condição do componente. Na transição b , o componente está operando ligado e com a falha passa para a condição operacional desligado. O restabelecimento da condição funcional e operacional, para este caso está representado pela transição b_1 . O outro caso de falha evidente, representada pela transição c , é menos comum. Ocorre quando o componente está desligado, e a falha o leva para a condição operacional ligado. A manutenção do componente, que é o retorno para a condição sem falha e desligado está representada pela transição c_1 .

A ocorrência de falhas ocultas estão representadas pelas transições d e e . Pela Figura A.10 é possível visualizar que este tipo de falha somente ocorre quando o componente está ligado e o componente fica “travado ligado” e também na condição contrária a esta, quando o componente está desligado e fica “travado desligado”. Ou seja, neste caso a condição operacional se mantém e o ocorre mudança da condição funcional do componente (sem falha \rightarrow falha oculta).

Figura A.10 – Possíveis estados de um componente



Destaca-se que na metodologia que será apresentada, uma falha oculta não pode

mudar de estado diretamente para uma condição sem falha – caminhos representados pelas transições d_3 e e_3 – antes é preciso passar para a condição de falha evidente – caminho d_1 e e_1 . Seria possível corrigir falhas ocultas com inspeções periódicas, enquanto o sistema está aparentemente em condições normais, sem falha. Assim, nessa ação as falhas ocultas passam a ser evidentes e então pode-se, desta forma, alterar o estado do componente para as condições sem falha representados pelas transições d_2 e e_2 . Vale destacar que mesmo assim, foi preciso passar para o estado de falha evidente, ou seja, as falhas foram detectadas na inspeção.

A análise dos estados dos componentes, bem como suas transições, é fundamental para o presente trabalho, dado que esta dinâmica³ se mostra determinante para a análise de confiabilidade estática e dinâmica. Quando ocorre a mudança de estado (componente sem falha → componente com falha), não implica a perda da função do sistema, mas simplesmente, demandas por ação de manutenção para recuperar o estado inicial do sistema a uma condição “tão bom quanto novo”.

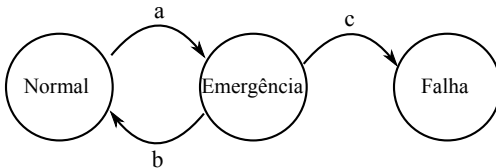
A.8 VARIÁVEIS DE ESTADO DE UM SISTEMA

É o conjunto de variáveis que determina completamente o sistema em um dado instante de tempo t (LAW et al., 2005). Em um sistema dinâmico haverá pelo menos duas variáveis de estado. Uma para caracterizar o estado do sistema – por exemplo indicar que o sistema está em falha – e outra para indicar o tempo.

A.9 ESTADO DE UM SISTEMA

Os estados dos sistemas abordados neste trabalho são discretos. A Figura A.11 apresenta os possíveis estados do sistema: condição de operação normal, condição de emergência ou em falha.

Figura A.11 – Possíveis estados do sistema



Os estados do sistema dependem das variáveis de estado y (variável de controle) e t (tempo). Assim, conhecendo o valor destas variáveis é possível identificar qual o estado do sistema.

Dado que o sistema tenha entrado em uma condição de emergência – transição

³Transições de um estado para outro.

$a -$, deve-se tomar ações para trazer o sistema para a condição normal – transição b e impedir a falha do sistema, indicada pela transição c .

A.10 EVENTO

Esta definição é utilizada nos sistemas a eventos discretos (SED), onde a ocorrência do evento é uma ação instantânea e confere, para o sistema, o caráter discreto no tempo (CURY, 2001). Podem ser considerados como eventos: a falha ou reparo de um componente, acionamento de um sensor, disparo de um alarme, intervenção humana.

A.11 PROCESSO MARKOVIANO

Segundo Papoulis (1991), processo Markoviano é um processo estocástico cujos valores do passado não tem influência no futuro se os valores presente estiverem definidos, sendo representado pela Equação A.16. A expressão está escrita para $t_1 < t_2 < \dots < t_{n-2} < t_{n-1} < t_n$.

$$P\{x(t_n) \leq x_n | x(t_{n-1}), \dots, x(t_1)\} = P\{x(t_n) \leq x_n | x(t_{n-1})\} \quad (\text{A.16})$$

Ou seja, a probabilidade condicional para o instante de tempo t_n é determinada em função do valor x no tempo t_{n-1} , independente do valor assumido nos tempos anteriores $t_1, t_2 \dots t_{n-2}$.

O conceito de processo Markoviano se torna importante na metodologia para racionalizar o processamento das informações. Assim, não são armazenados os estados antigos do sistema, pois para saber o estado futuro basta saber o estado atual. Desta forma, não há necessidade de armazenar todos os estados que foram assumidos para o sistema, resultando em uma quantidade menor de variáveis para ser gerenciada na simulação numérica.

A.12 PROCESSO SEMI MARKOVIANO

Da mesma forma que o processo Markoviano, o semi Markoviano não necessita das informações dos estados do sistema no tempo passado para calcular a probabilidade de um estado futuro – interessa somente as informações do estado atual.

Quanto às transições, no processo semi Markoviano ocorrem da mesma maneira que nos processos Markovianos. A diferença é que no processo Markoviano o tempo de permanência nos estados obedecem uma distribuição exponencial. Ou seja, segundo Moura (2006), no processo semi Markoviano esse tempo pode ter uma distribuição arbitrária, isto é, pode não ser uma exponencial – o que torna o processo semi Markoviano menos restritivo – podendo ser aplicado em uma gama maior de

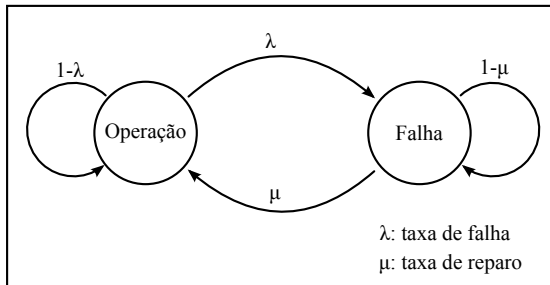
problemas.

A.13 DIAGRAMAS DE TRANSIÇÃO DE ESTADOS

Os diagramas de transição de estados serão utilizados para representar os possíveis estados dos componentes. Algumas mudanças de estados serão determinísticas, como ligar e desligar componentes. No entanto, as mudanças de estado relacionadas com a condição do componente (operação \leftrightarrow falha) serão estocásticas. Para esses casos, será considerado que o comportamento é Markoviano – a mudança do estado em operação para falha estará associado à uma taxa de falha, λ , e a manutenção do componente estará associada a uma taxa de reparo, μ .

A Figura A.12 apresenta um exemplo de cadeia de Markov com dois estados (operação e falha). A probabilidade de um componente em operação passar para o estado em falha está relacionado com a taxa de falhas λ . De maneira análoga, a probabilidade de um componente em falha passar para o estado de operação está relacionado com a taxa de reparos μ .

Figura A.12 – Mudanças de estados de um componente



Cada combinação de estados dos componentes representará uma configuração do sistema, que terá um dado comportamento dinâmico. Portanto, o comportamento dinâmico do sistema está fortemente relacionado com os parâmetros λ e μ dos componentes.

Assim, para a modelagem do sistema técnico deve-se ter uma representação do diagrama de transição de estados dos componentes, as taxas de transição – para os eventos estocásticos – e as regras para mudança de estados para os eventos com comportamento determinístico.

A.14 CONSIDERAÇÕES DO CAPÍTULO

O presente capítulo apresentou alguns conceitos básicos relacionados com confiabilidade estática. As equações apresentadas para cálculo de confiabilidade de sistemas em série e paralelo, com o uso de diagramas de bloco é bastante simples, sendo

um dos motivos que seja uma forma amplamente utilizada. Existem outros aspectos que não foram abordados como análise funcional, redução de sistemas, redundância passiva, etc, mas podem ser encontrados de forma detalhada nos trabalhos de Billinton e Allan (1992), Dias (1996) e Moubray (1997).

A definição de sistema é bastante subjetiva, mas a classificação apresentada por Cassandras e Lafortune (2008) permite delimitar o amplo conjunto de definições que podem ser encontrados, facilitando as discussões sobre o assunto. Um conjunto de elementos pode ser tratado como um sistema, subsistema ou componente. A aplicação dos conceitos irá depender da equipe que realiza o estudo, do problema que está sendo tratado, da complexidade dos elementos, entre outras variáveis.

O objetivo principal na seção de sistemas foi de esclarecer o termo “sistemas dinâmicos”, visto que na definição de confiabilidade dinâmica o termo é citado. Outros conceitos relacionados com análise de confiabilidade dinâmica, como processos estocásticos, estado de um sistema e componente, evento, processos Markovianos e semi Markovianos foram tratados.

O estado do sistema não pode ser definido somente pelos estados dos componentes, pois além disso é necessário saber o valor da variável de controle e o tempo. O Capítulo 2 irá tratar especificamente da análise de confiabilidade dinâmica. Na seção será possível compreender melhor sobre os estados de um sistema.

APÊNDICE B – Valores obtidos na simulação do problema clássico

Os gráficos das Figuras 5.15 e 5.16 representam a função distribuição acumulada de falhas, $F(t)$, para o problema do reservatório de líquido. A geração dos gráficos foi a partir dos valores contidos nas Tabelas B.1 e B.2. Esses valores foram obtidos por meio da aplicação da metodologia para análise de confiabilidade dinâmica proposta neste trabalho. A simulação realizada considera que os componentes do sistema não reparáveis.

Tabela B.1 – Dados para transbordamento (Metodologia ACoDi)

Tempo t (horas)	Probabilidade de falha (máx)	Probabilidade de falha (mín)
0	0,000000000	0,000000000
100	0,123925239	0,122304761
200	0,261320386	0,259103614
300	0,355972677	0,353689323
400	0,414377133	0,411956867
500	0,449766336	0,447179664
600	0,470523893	0,468086107
700	0,482859897	0,480438103
800	0,490350448	0,487947552
900	0,494765522	0,492340478
1000	0,497368700	0,494967300

Tabela B.2 – Dados para esvaziamento (Metodologia ACoDi)

Tempo (horas)	Probabilidade de falha (máx)	Probabilidade de falha (mín)
0	0,000000000	0,000000000
100	0,010632667	0,010115333
200	0,037664070	0,036679930
300	0,065436334	0,064161666
400	0,086567370	0,085124630
500	0,101231918	0,099616082
600	0,110621894	0,108952106
700	0,116518776	0,114803224
800	0,120112003	0,118397997
900	0,122327930	0,120592070
1000	0,123520799	0,121781201

Os dados dos gráficos de probabilidade de falha acumulada, gerados na aplicação das redes de petri estocásticas (GSPN) e redes de petri fluidas estocásticas (FSPN), Figuras 5.19 e 5.20, foram obtidos das Tabelas B.3 e B.4.

Tabela B.3 – Dados para transbordamento (Redes de Petri)

Tempo	GSPN	FSPN (máx)	FSPN(mín)
0	0,000000	0,000000	0,000000
100	0,074208	0,079228	0,068572
200	0,195182	0,209277	0,191723
300	0,292146	0,306257	0,284943
400	0,359876	0,373996	0,350404
500	0,405374	0,422347	0,397253
600	0,435689	0,454625	0,428575
700	0,455953	0,475018	0,448382
800	0,469595	0,489827	0,462773
900	0,478857	0,498549	0,471251
1000	0,485200	0,504734	0,477266

Tabela B.4 – Dados para esvaziamento (Redes de Petri)

Tempo	GSPN	FSPN (máx)	FSPN(mín)
0	0,000000	0,000000	0,000000
100	0,004463	0,005355	0,002845
200	0,022077	0,027037	0,020963
300	0,044846	0,049890	0,041510
400	0,065827	0,072385	0,062215
500	0,082568	0,087613	0,076387
600	0,095014	0,099597	0,087603
700	0,103939	0,108157	0,095643
800	0,110227	0,114853	0,101947
900	0,114622	0,119074	0,105926
1000	0,117689	0,123190	0,109810

APÊNDICE C – Simulação do problema clássico com componentes reparáveis em série

Nessa seção estão apresentadas duas simulações. A primeira considera que os componentes em falha deverão ser reparados na seguinte ordem: bomba P1, bomba P2 e por último a válvula V. Na segunda simulação, a ordem de reparo estipulada foi: válvula V, bomba P1 e por último a bomba P2.

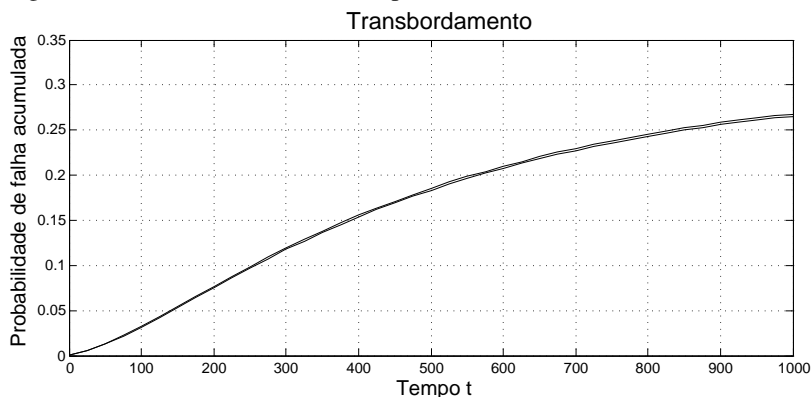
Cada histograma foi obtido com 10 mil ensaios. A dispersão dos resultados foi obtida um conjunto de 100 histogramas.

O objetivo aqui é verificar se a confiabilidade do sistema é influenciada pela ordem de manutenção dos componentes. Destaca-se que não foram realizadas manutenções dos componentes com falha oculta.

C.1 ORDEM: BOMBA P1, BOMBA P2, VÁLVULA V

A Figura C.1 apresenta os valores máximos e mínimos da probabilidade de falha acumulada, considerando o intervalo de confiança de 99 %, para o caso de transbordamento do reservatório.

Figura C.1 – Probabilidade de falha por transbordamento – P1P2V



A Figura C.2 apresenta os valores máximos e mínimos da probabilidade de falha acumulada, considerando o intervalo de confiança de 99 % considerando a falha por esvaziamento do reservatório.

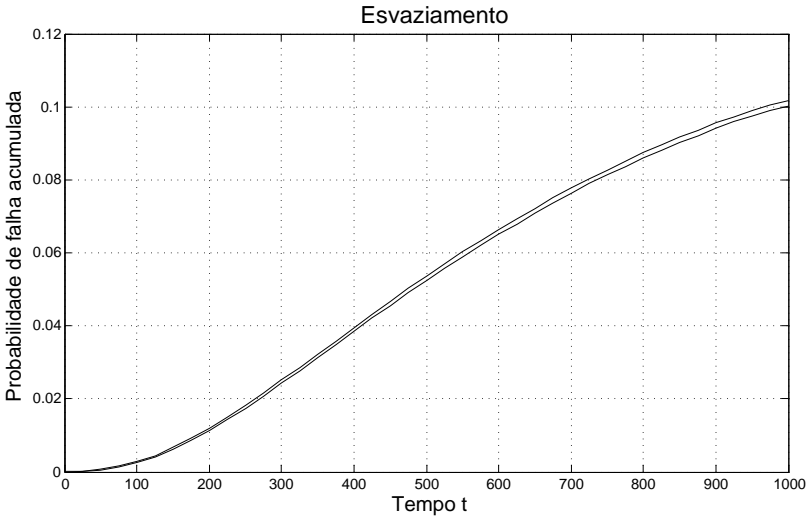
Assim, os intervalos de confiança para as falhas, no tempo $t = 1000h$, resultam em:

$$\text{Transbordamento: } IC_{99\%}(\mu) \approx (0,2653; 0,2677)$$

$$\text{Esvaziamento: } IC_{99\%}(\mu) \approx (0,1001; 0,1017)$$

Em relação à simulação sem manutenção, a probabilidade de falha por transbordamento reduziu quase a metade. Ou seja, reduziu do valor em torno de 49 % para 26 %. Por outro lado, a probabilidade de falha por esvaziamento não teve mudanças tão significativas. Reduziu de valores em torno de 12 % para aproximadamente 10 %.

Figura C.2 – Probabilidade de falha por esvaziamento – P1P2V

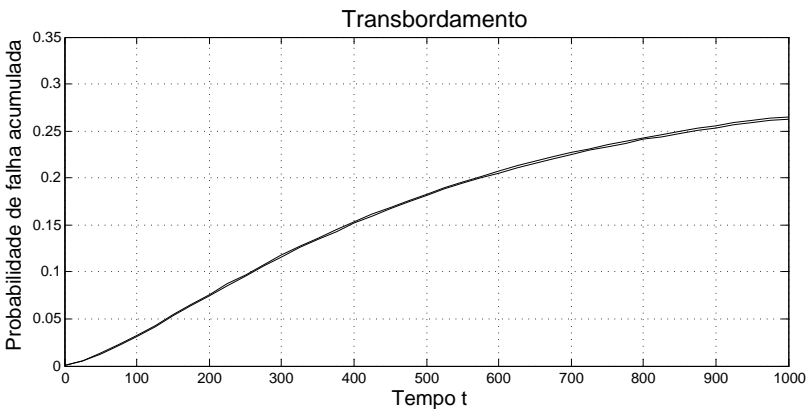


C.2 ORDEM: VÁLVULA V, BOMBA P1, BOMBA P2

Nesta seção estão apresentados os resultados para simulação considerando que a ordem com que os componentes foram reparados foi inicialmente a válvula V, depois a bomba P1 e por último a bomba P2.

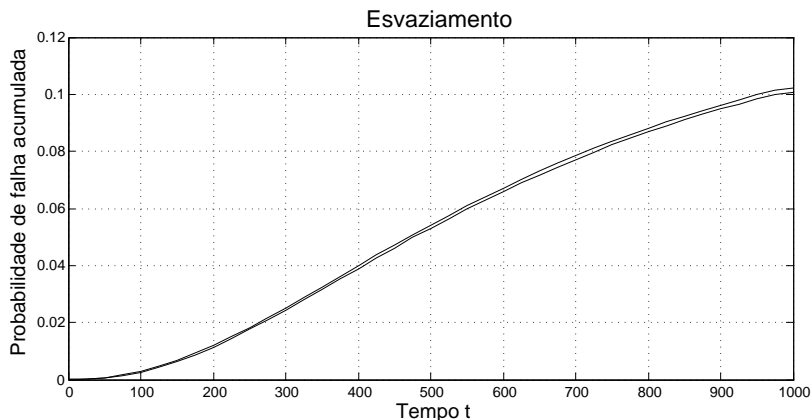
A Figura C.3 apresenta os valores máximos e mínimos, para um intervalo de confiança de 99 %, da probabilidade de falha acumulada para transbordamento.

Figura C.3 – Probabilidade de falha por transbordamento – VP1P2



A Figura C.4 apresenta os valores máximos e mínimos, para um intervalo de confiança de 99 %, da probabilidade de falha acumulada para esvaziamento.

Figura C.4 – Probabilidade de falha por esvaziamento – VP1P2



Assim, os intervalos de confiança para as falhas, no tempo $t = 1000h$, resultam em:

Transbordamento: $IC_{99\%}(\mu) \approx (0,2628; 0,2651)$

Esvaziamento: $IC_{99\%}(\mu) \approx (0,1009; 0,1024)$

Em relação à simulação anterior, em que a manutenção inicialmente é realizada na bomba P1, os valores são muito próximos, tanto para a falha por transbordamento quanto para o esvaziamento.

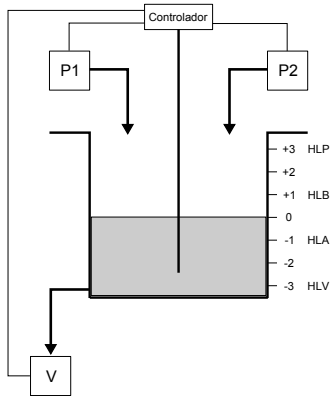
Assim, para o gestor da manutenção pode-se definir tanto uma como outra sequência de manutenção. Pois a probabilidade de falha do sistema, praticamente não sofre diferença para as sequências de manutenção apresentadas.

APÊNDICE D – Análise do reservatório: confiabilidade clássica

Para esclarecer as diferenças da metodologia estática e dinâmica, considere o exemplo a seguir.

A Figura D.1 apresenta um reservatório no qual existe um líquido e este deve se manter no nível 0. Para isso, existem duas bombas para fazer o enchimento do reservatório e uma válvula para o esvaziamento. No entanto, em condições normais de operação, somente a bomba P1 e a válvula V ficam ligadas, de forma que a vazão que entra no reservatório é a mesma que sai, consequentemente, o nível se mantém em zero.

Figura D.1 – Problema exemplo



Dados:

Tempo de missão (t): 1000 h

Taxa de falha de P1: 0,004566 falhas/h

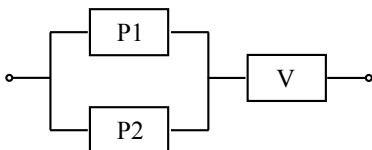
Taxa de falha de P2: 0,005714 falhas/h

Taxa de falha de V: 0,003125 falhas/h

D.1 DIAGRAMA DE BLOCOS PARA CONFIABILIDADE

Na análise tradicional não é considerada a presença de um controlador. Fazendo uso de diagrama de blocos para confiabilidade, o sistema pode ser representado de acordo com a Figura D.2.

Figura D.2 – Diagrama de blocos para confiabilidade



Por meio da equação $R(t) = e^{-\lambda \cdot t}$, para um tempo $t = 1000h$, calcula-se a confiabilidade de cada componente.

$$R_{P1}(1000) \cong 0,0104 \text{ (1,04 \%)}$$

$$R_{P2}(1000) \cong 0,0033 \text{ (0,33 \%)}$$

$$R_V(1000) \cong 0,0439 \text{ (4,39 \%)}$$

Nas seções seguintes são apresentadas duas análises do sistema. Inicialmente, trata-se a análise do sistema sem considerar as diferenças entre falha evidente e oculta. Posteriormente, utiliza-se para o cálculo da confiabilidade do sistema somente a probabilidade de falha evidente.

D.2 ANÁLISE DO SISTEMA SEM CONSIDERAR AS FALHAS OCULTAS

Na análise de confiabilidade estática dos sistemas técnicos, geralmente, não são consideradas as falhas ocultas dos componentes. Ou seja, no valor da taxa de falha do componente estão incorporados as falhas que são evidentes, que causam mudança de estado do componente, e as ocultas, que travam o componente no estado que coincide com a demanda do sistema.

O que se deseja com essa análise é destacar que, na maior parte dos casos, considera-se que o sistema está em falha independentemente se a falha de seu componente é evidente ou oculta. No entanto, o que ocorre na prática é que se o componente está com falha oculta, isto não é percebido pelo sistema, ou seja, o sistema não está em falha, visto que continua a executar sua função.

A confiabilidade do sistema, $R_{sistema}$, foi calculada por meio das associações de série e paralelo, sendo obtido o seguinte valor:

$$R_{sistema}(1000) \cong 0,0006 \text{ (0,06 \%)}$$

De forma complementar, a probabilidade falha do sistema, $Q_{sistema}$, é igual a:

$$Q_{sistema}(1000) \cong 0,9994 \text{ (99,94 \%)}$$

O valor da probabilidade de falha obtida para 1000 h indica que o sistema tem pouca chance de cumprir sua função para este tempo de missão.

Nessa análise não é possível identificar se o sistema irá falhar por transbordamento ou esvaziamento. Além disso, nos cálculos estão incluídos os casos em que ocorreram falhas ocultas nos componentes, mas o sistema não entrou em falha.

Por exemplo, considere uma falha oculta na válvula V. O sistema continua a operar, pois ela ainda continua a dar vazão de fluido, cumprindo sua função. No entanto, nesta análise é considerada falha do sistema, visto que o componente V não tem redundância. Assim, a ocorrência de falha neste componente leva à falha do sistema, embora o nível de fluido permaneça em zero.

D.3 ANÁLISE DO SISTEMA COM DISTINÇÃO DAS FALHAS EVIDENTES E OCULTAS

A análise a seguir considera que a probabilidade de falha oculta e evidentes são iguais. No entanto, as falhas ocultas dos componentes não causam a falha do sistema, já que este continua a operar com se estivesse sem falhas.

Desta forma, a confiabilidade é obtida com sendo uma composição da probabilidade de não-falha do componente junto com a probabilidade de falha oculta. Ou seja, a falha do sistema será considerada somente com as falhas evidentes, pois estas mudam alteram os estados dos componentes para uma condição indesejada para o sistema.

As probabilidade de falha (evidente) e confiabilidade de cada componente estão apresentadas na Tabela D.1

Tabela D.1 – Probabilidades de falha e confiabilidade de cada componente

Componente	Probabilidade de falha evidente	Confiabilidade
P1	0,494800263	0,505199737
P2	0,498350276	0,501649724
V	0,478031533	0,521968467

O resultado para a confiabilidade do sistema, $R_{sistema}$, nesta segunda análise de confiabilidade estática foi:

$$R_{sistema}(1000) \cong 0,3932 \text{ (39,32 \%)}$$

De forma complementar, a probabilidade falha do sistema, $Q_{sistema}$, é igual a:

$$Q_{sistema}(1000) \cong 0,6067 \text{ (60,67 \%)}$$

Na análise de confiabilidade estática não é possível saber probabilidade de falha por transbordamento e esvaziamento. Para isso seria preciso conhecer a ordem cronológica com que os eventos ocorrem e o estado do componente estipulado pelo sistema. Desta forma, só é possível verificar, por meio do diagrama de blocos, se o sistema vai falhar ou não. A análise é construída sobre as funções dos componentes. Então, dado que o componente está em falha e ele não tem redundância, considera-se a falha do sistema.

Considere o Quadro D.1. Nele estão representados as possíveis configurações que podem ocorrer no sistema. Um componente em bom estado está representado por “0” e com falha evidente por “1”. As possíveis configurações são obtidas por meio da análise por árvore de eventos, onde para cada nó da árvore existem duas possibilidades: sucesso ou falha do componente.

Portanto, neste exemplo o sistema consegue operar para as configurações “1”, “3” e “5”. Na configuração “1” todos os componentes estão bons. Na configuração “3”

Quadro D.1 – Possíveis configurações no sistema reservatório baseado em árvore de eventos

Configuração	P1	P2	V	Condição do sistema
1	0	0	0	Operação
2	0	0	1	Falha
3	0	1	0	Operação
4	0	1	1	Falha
5	1	0	0	Operação
6	1	0	1	Falha
7	1	1	0	Falha
8	1	1	1	Falha

e “5” apenas uma das bombas P1 ou P2 estão em falha, sendo garantida o fornecimento de vazão por pelo menos por uma das bombas.

D.4 PRINCIPAIS DIFERENÇAS

Na validação da metodologia, Capítulo 5, foram feitas simulações que identificaram duas falhas no sistema: falha por transbordamento e falha por esvaziamento no reservatório.

A probabilidade de falha para esvaziamento, no tempo de 1000 h, é em torno de 12% e transbordamento de 50%.

A probabilidade de falha por transbordamento é bem maior do que a secagem, como era de se esperar. A existência de duas bombas para alimentar o reservatório e apenas uma válvula para a drenagem conduz o sistema para esta tendência.

No início da análise é possível perceber que a quantidade das informações que devem ser fornecidas para a análise de confiabilidade dinâmica é bem maior do que na estática. Isto porque para poder avaliar o sistema dinamicamente, faz-se necessário esse conjunto de dados.

Com a soma da probabilidade de falha por transbordamento com a de secagem tem-se um valor em torno de 62%. Esse valor, comparado com a primeira análise de confiabilidade estática é significativamente inferior que os 99,94%. No entanto, se comparado com a segunda análise, onde se considera apenas as falhas evidentes o valor fica bastante próximo, pois o valor obtido na segunda análise foi de 60,67%.

A probabilidade de falha na análise de confiabilidade dinâmica (62%) foi um pouco maior que os 60,67% obtidos com a análise estática para as falhas evidentes. Essa diferença pode ser ocasionada pelas falhas ocultas, que na análise dinâmica estão sendo consideradas. Observou-se ao longo das simulações que, muita das falhas do sistema são consequências de falhas ocultas associadas à falha de outros componentes. Nesses casos as falhas ocultas passam a ser evidentes pois o sistema demanda mudanças de estados nos componentes a fim de impedir o transbordamento ou esvaziamento do reservatório.

A presença do controlador, responsável em mudar a configuração do sistema quando o valor da variável de controle está fora da faixa normal de operação, torna o sistema um pouco mais tolerante às falhas. Por exemplo, em uma análise de confiabilidade estática, considera-se a falha do sistema quando ocorre a falha na válvula V. No sistema dinâmico é preciso que outros componentes falhem, além da válvula, para que ocorra a falha do sistema.

Desta forma, o controlador atua não somente na bomba sobressalente, que entra em funcionamento quando o nível do reservatório está baixando, mas também na válvula V que é fechada para evitar o esvaziamento. Portanto, mesmo que as duas bombas P1 e P2 parem de fornecer vazão, ainda é preciso que a válvula V tenha uma falha aberta para que haja esvaziamento. Na análise estática, quando ocorre a falha na bomba principal, é considerada apenas a ação de substituir a bomba em falha.

Grande parte dos sistemas dinâmicos funcionam como no exemplo apresentado. Tais sistemas devem ser modelados com uso da metodologia de confiabilidade dinâmica.

Outra característica que pode ser observada com o exemplo é que os valores de confiabilidade podem se tornar mais próximos da realidade. Ou seja, muitos cálculos propostos pelas normas são pessimistas, resultam em uma confiabilidade bem mais baixa do que ocorre nos sistemas reais.

Por fim, a modelagem permite acompanhar a variável de controle nas simulações. Com isso é possível obter vários cenários de falha do sistema que irão ajudar a equipe a desenvolver controles para evitar a ocorrência de uma falha do sistema.

APÊNDICE E – Técnicas e ferramentas adicionais

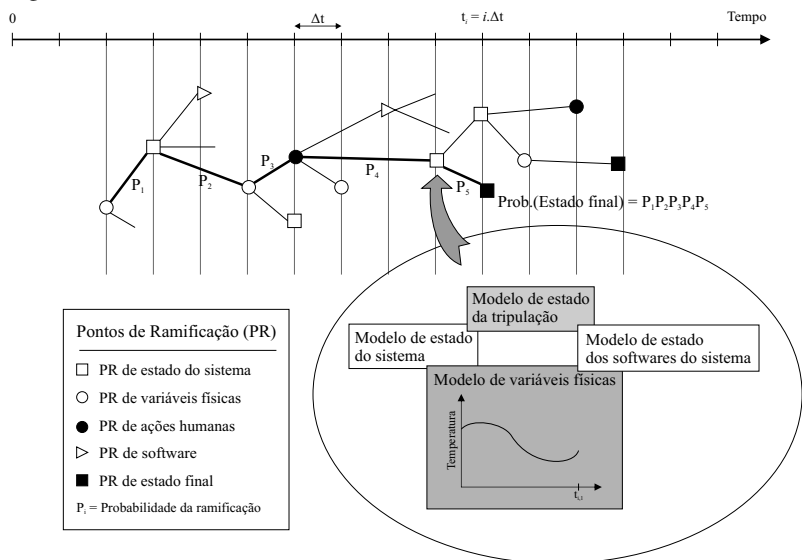
O presente capítulo apresenta, de forma resumida, as principais técnicas e ferramentas utilizadas para análise de confiabilidade dinâmica. O objetivo desta seção é dar uma visão geral das possíveis técnicas que podem ser utilizadas atualmente.

E.1 ANÁLISE POR ÁRVORE DE EVENTOS DINÂMICA

As árvores de eventos dinâmicas, *Dynamic event tree analysis* (DETA), são geradas por *softwares* que levam em consideração o comportamento dinâmico das variáveis de controle da planta. Essa capacidade é devido a implementação de modelos matemáticos que simulam o comportamento dinâmico do sistema (MERCURIO et al., 2008).

A Figura E.1 é um exemplo de árvore eventos dinâmica onde é possível observar o cálculo da probabilidade de um cenário, que é realizado por meio do produto entre todos os nós participantes da ramificação.

Figura E.1 – Árvore de eventos discreta dinâmica



Fonte: Hu (2005)

Para gerar as árvores de eventos dinâmicas é preciso identificar os pontos de ramificação ao longo do tempo, onde ocorrem os eventos estocásticos e também quando são gerados algumas ações do sistema, do componente ou de um operador. Posteriormente, armazena-se os estados do sistema para cada ponto ramificação, que recebem a denominação de “nós”.

Assim, são geradas várias ramificações, sendo que cada uma representa um possível cenário de falha. No trabalho desenvolvido por Bucci et al. (2008) é possível verificar um exemplo de aplicação. Nele, é possível observar que a árvore de eventos dinâmica tem a vantagem de apresentar a probabilidade de ocorrência de cada ramificação, além de fornecer a probabilidade de falha do sistema.

A árvore de eventos permite visualizar os cenários que poderiam ocorrer em função dos vários eventos (ação humana, software etc). No entanto, segundo Siu (1994), todas as possíveis combinações dos estados do sistema devem ser consideradas. Consequentemente, o número de sequências de eventos pode crescer e dificultar o tratamento das informações, o que obriga o uso de estratégias para limitar este problema.

Um dos *softwares* mais conhecidos para árvore de eventos dinâmica é conhecido como *Dynamic event tree analysis method* (DETAM), desenvolvido a partir de uma generalização de um *software* utilizado para análise e avaliação probabilística do risco PRA, denominado DYLAM (ACOSTA; SIU, 1993).

E.2 ANÁLISE POR ÁRVORE DE FALHAS DINÂMICA

A Análise por árvore de falhas dinâmica, *Dynamic fault tree analysis* (DFTA), é uma extensão da análise por árvore de falhas (FTA). Desta forma, possui algumas portas lógicas e elementos adicionais que permitem modelar o comportamento e a interação de componentes em sistemas complexos (BOUDALI et al., 2007).

Além das portas lógicas utilizadas nas árvores de falhas estáticas (E, OU, K/M) e eventos básicos, as árvores de falhas dinâmicas utilizam as portas apresentadas no Quadro E.1.

Para solucionar os problemas relacionados com os sistemas dinâmicos é necessário fazer uso de uma representação que acompanhe a história do sistema, na forma de um “estado”. Por esta razão as DFTA utilizam as cadeias de Markov, que contém toda informação a respeito das falhas dos componentes, a sequência de falhas e informação sobre alocações de componentes sobressalentes (MANIAN et al., 1998, p.2, tradução nossa).

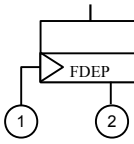
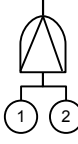
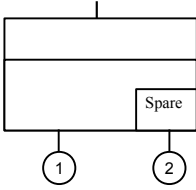
Os modelos de Markov são transformados em equações diferenciais e resolvidos numericamente. Mas também é possível utilizar, como alternativa aos modelos de Markov: redes de Petri, inferências bayesianas e simulações de Monte Carlo (DISTEFANO; PULIAFITO, 2007).

E.3 REDES DE PETRI ESTOCÁSTICAS

É uma rede na qual para cada transição tem-se associada uma variável aleatória com distribuição exponencial, que expressa a frequência de disparo da transição (CARDOSO; VALETTE, 1997). A Figura E.2 é um pequeno exemplo onde a variável T1 representa uma condição de transição para a ficha avançar da posição P1 para P2.

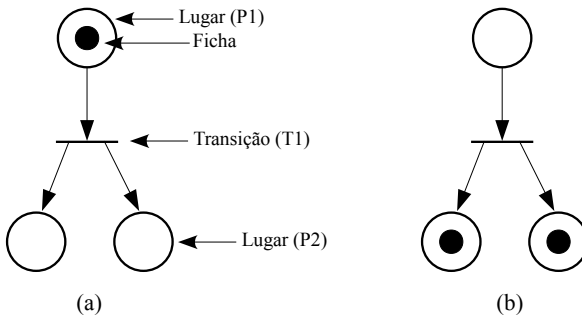
As representações gráficas permitem a modelagem comportamental de sistemas discretos, possuindo três elementos básicos de representação: lugar, transição e ficha.

Quadro E.1 – Portas lógicas dinâmicas

Símbolo	Porta lógica	Relação causal
	Dependência funcional FDEP	Propaga o evento da entrada do gatilho (1) para os eventos básicos dependentes (2).
	E prioridade PAND	A falha na saída ocorre se as falhas na entrada ocorrerem em uma dada ordem. Ex. ocorre a falha (1) e depois a falha (2).
	Reserva	Quando a entrada primária falha (1), as entradas reservas disponíveis (2) são usadas em ordem até não sobrar nenhuma.

Fonte: Boudali et al. (2007)

Figura E.2 – (a) Uma simples rede de Petri (b) Depois do disparo de T1



Fonte: Labeau et al. (2000, p.223, tradução nossa)

A movimentação da rede é feita por meio dos disparos das transições, fazendo com que as fichas se movimentem pelos lugares (círculos). A Figura E.2 apresenta dois estados de uma rede: antes e depois de disparar a transição T1. Assim, não basta que a

ficha esteja no lugar (P1) para ocorrer a mudança de estado, a condição (representada pela transição T1) tem que ser atendida.

A redes de Petri são amplamente utilizadas na modelagem de *hardware* e *software* de computadores (LABEAU et al., 2000 apud PETERSON, 1981). Seu potencial está na habilidade de levar em conta a sincronização e o paralelismo.

Associar regras com o disparo das transições é um fenômeno recente. Ao longo dos anos, o conceito de transição dependente do tempo foi sendo introduzido. Inicialmente, ou utilizavam tempo determinístico ou tempo derivado de uma taxa de transição. Essa característica permitiu um mapeamento entre redes de Petri e as cadeias de Markov (LABEAU et al., 2000).

As redes de Petri temporizadas são extensões que buscam acrescentar às redes de Petri a possibilidade de análise no domínio de tempo. Nestas extensões o tempo pode estar associado às marcas, aos arcos, aos lugares ou às transições.

As extensões estocásticas [...] permitem considerar incertezas nos instantes de execução de eventos do sistema, associando a eles funções de probabilidade para a determinação de sua execução (MARRANGHELLO, 2005).

A Figura E.3 apresenta uma classificação de redes de Petri temporizadas, que podem ser determinísticas ou estocásticas.

Segundo Labeau et al. (2000) as redes de Petri estocásticas podem ser utilizadas para representar os sistemas dinâmicos qualitativamente, e se os modelos das variáveis do processo forem incorporados na rede, torna-se possível realizar uma análise de confiabilidade quantitativa por meio da simulação de Monte Carlo.

Uma desvantagem desta técnica é que ela também pode conduzir a uma explosão de estados, mas isso pode ser mitigado com o uso da simulação de Monte Carlo guiada (*biasing*).

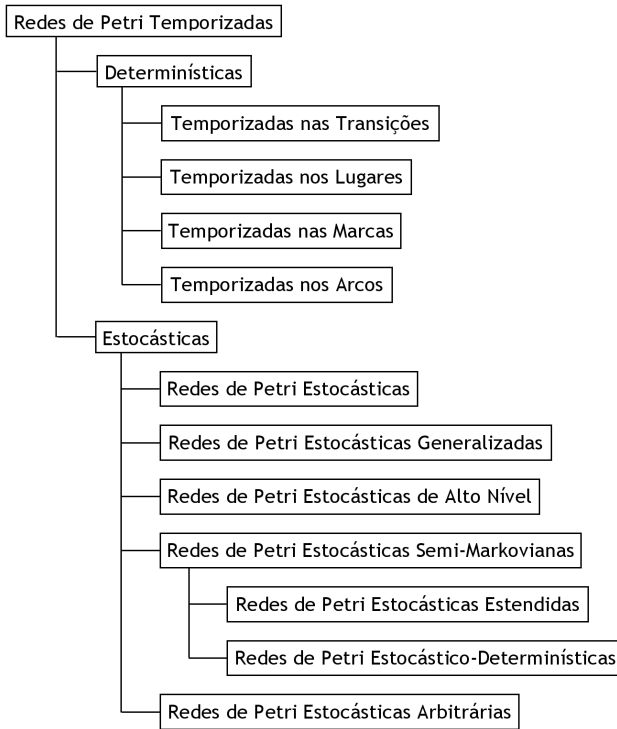
E.4 DIAGRAMA SEQUENCIAL DE EVENTOS

Um diagrama sequencial de eventos (*Event sequence diagram* (ESD)) é uma representação orientada para explicitar a sequência de eventos que chegam a diferentes estados finais. Cada caminho desse fluxo é um cenário no qual eventos pivotais são estabelecidos como: ocorreu ou não (STAMATELATOS et al., 2002).

A possibilidade de construir cenários constitui-se na grande aplicação desta técnica. Ela permite visualizar o inter-relacionamento entre sistemas técnicos, ambientais e humanos, o que se constitui numa particularidade da técnica. Por sua vez, o nível de complexidade torna-se muito grande, para o caso de sistemas complexos.

A estrutura para uma análise qualitativa é apresentada por Swaminathan e Smidts (1999c). Sua construção consiste em capturar as informações dos cenários dinâmicos com base no conhecimento de um especialista. As estruturas consistem de eventos, condições, portas, regras de dependência, restrições e variáveis de processo. Os símbolos utilizados nos diagramas estão apresentados no Quadro E.2.

Figura E.3 – Redes de Petri temporizadas



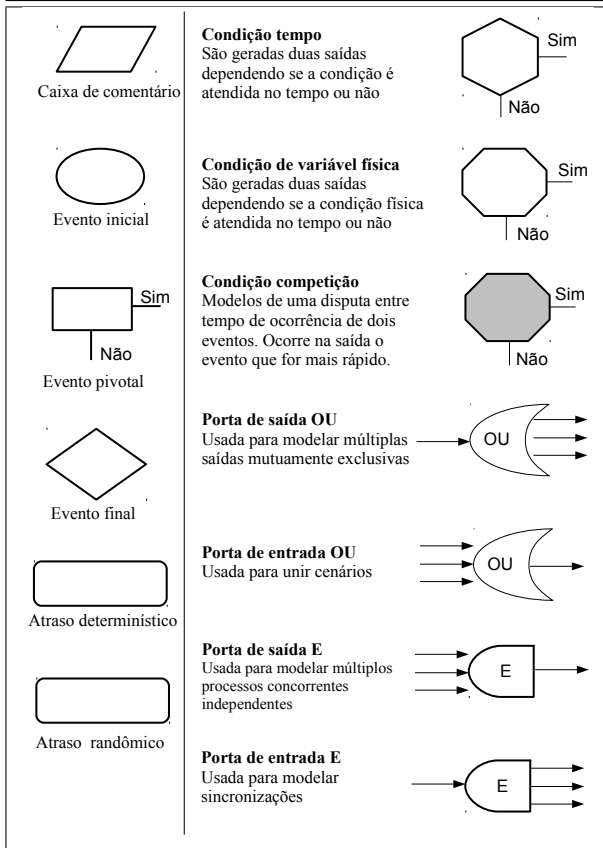
Fonte: Marranghello (2005, p.25)

O formalismo matemático para a utilização dos componentes do ESD estão presentes na obra seguinte de Swaminathan e Smidts (1999b). Esse formalismo pode ser usado com equações de transições de estado Markoviana e semi-Markoviana (SWAMINATHAN; SMIDTS, 1999c; LABEAU et al., 2000).

A técnica tem sido utilizada na indústria nuclear como forma de documentação, para que os operadores possam entender melhor os cenários de acidentes. O diagrama nesse caso é denominado de “diagrama sequencial de eventos funcionais” – *Functional event sequence diagram* (FESD) (SWAMINATHAN; SMIDTS, 1999c; LABEAU et al., 2000).

Os diagramas atuais possuem estruturas que permitem analisar o comportamento dinâmico dos sistemas por meio das variáveis de processo. Assim, é possível identificar e construir sequências de eventos ordenados no tempo.

Quadro E.2 – Eventos, condições e portas da estrutura ESD



Fonte: Labeau et al. (2000, p.224, tradução nossa)

E.5 DIAGRAMAS DE BLOCOS PARA CONFIABILIDADE DINÂMICA

Cada bloco no diagrama de blocos para confiabilidade, RBD, representa um componente físico funcionando e a falha desse componente representa a interrupção da ramificação onde está instalado. Se uma quantidade suficiente de blocos estiver em falha, de forma que não haja nenhuma comunicação entre a entrada e a saída, significa a falha do sistema. Em outras palavras, se existir pelo menos uma caminho comunicando a entrada com a saída, o sistema irá funcionar (DISTEFANO; PULIAFITO, 2007).

O RBD tradicionalmente tem sido usado com sistemas não reparáveis, nos quais é possível obter a função confiabilidade do sistema, $R(t)$, analiticamente (DISTEFANO;

PULIAFITO, 2007).

Da mesma forma que se observou a necessidade de modelar fatores dinâmicos na FTA, no RBD foi feita uma extensão da técnica, adicionando novos elementos, criando assim o diagrama de blocos de confiabilidade dinâmica – DRBD. Nessa versão, surgiram elementos adicionais em relação aos diagramas de blocos (RBD) tradicionais. Segundo Xu et al. (2008) com o uso desses elementos adicionais é possível representar blocos dependentes do estado do sistema – possibilitando representar configurações alternativas –; blocos para representação de peças sobressalentes e divisão de carga (*load sharing*).

O RBD garante as características de interesse na modelagem de confiabilidade como simplicidade, versatilidade e poder expressivo. Tais características foram herdadas nos modelos DRBD, que além disso permitem levar em consideração as dinâmicas do sistema. Um sistema é considerado variante no tempo se os estados de seus componentes desenvolvem-se quando uma sequência de eventos ocorre. É possível definir relações de confiabilidade (dependências) entre componentes associando tais relações a eventos (DISTEFANO; PULIAFITO, 2007).

Em um modelo DRBD a condição de cada componente é caracterizada por uma variável de estado que identifica a condição operacional do componente em um dado tempo. A evolução de um estado do componente (dinâmica do componente) é caracterizada por eventos que ocorrem com ele (DISTEFANO; PULIAFITO, 2007).

De acordo com Distefano e Puliafito (2007) um componente genérico pode assumir os seguintes estados:

- **Ativo** se o componente funciona sem qualquer problema.
- **Falha** se o componente não está funcionando, acompanhamento de sua falha.
- **Standby** se o componente está funcionando (sem falhas), mas está indisponível.

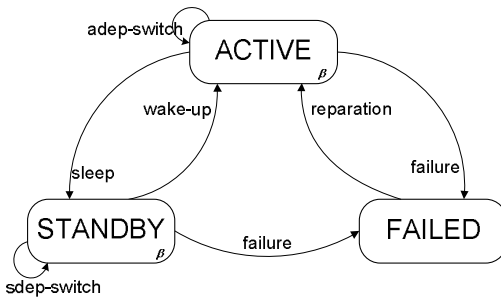
Um evento representa a transição de um estado do componente para outro. A seguir, uma breve descrição das transições (eventos) que podem ser assumidas por um componente:

- O evento **failure** modela a mudança de estado de **ativo**, ou **standby**, para **falha**.
- O evento **wake-up** muda o estado de **standby** para **ativo**.
- O evento **sleep** muda o estado de **ativo** para **standby**.
- O evento **reparation** muda o estado de **falha** para **ativo**.
- O evento **adep-switch** representa a transição entre dois estado **ativos**.
- O evento **sdep-switch** representa a transição entre dois estado **standby**.

A Figura E.4 resume os estados e as transições (eventos) de um DRBD.

A análise dos diagramas de blocos facilita muito a obtenção dos grupos de corte e grupos de ligação. Desta forma, a principal contribuição do DRBD é a capacidade de modelar dependência entre subsistemas, ou componentes, a respeito do comportamento de suas confiabilidades. A Figura E.4 é uma forma de modelar que lembra bastante o modelo de Markov, indicando que as duas técnicas possuem grande interação.

Figura E.4 – Estados e eventos de um DRBD



Fonte: Distefano e Puliafito (2007, p.73)

E.6 CONSIDERAÇÕES DO CAPÍTULO

Neste capítulo foram apresentadas algumas técnicas para análise de dinâmica nos sistemas. Vale citar que ainda existem outras técnicas como *Go-flow*, *Dynamic flowgraph methodology* (DFM), cujas descrições podem ser encontradas em Matsuoka e Kobayashi (1997) e Al-Dabbagh e Lu (2010) respectivamente.

Muitas técnicas acabam trabalhando junto com as cadeias de Markov. Nelas ocorrem os a explosão de estados. Para essa questão Zhu (2005) cita três formas de tratamento: A primeira consiste em unir alguns estados ou estados finais, com isso reduzir a quantidade de ramificações desenvolvidas. A segunda seria a simulação paralela em vários computadores, distribuindo dessa maneira a carga computacional. A terceira forma é por meio da simulação de Monte Carlo guiada para os estados ou eventos de interesse.

Durante a pesquisa foi possível perceber que embora os estudos sobre confiabilidade dinâmica tenham começado na década de oitenta, ainda tem muito a ser desenvolvido. Embora existam alguns *softwares* como FTA dinâmico, ETA dinâmico, redes de petri estocásticas, entre outras, a aplicação da confiabilidade dinâmica ainda é muito dependente de um especialista, visto que devem ser desenvolvidos modelos específicos para cada sistema que está sendo estudado. Existem algumas instituições que estão se destacando neste contexto como a Universidade de Maryland e a Universidade Duke – nos Estados Unidos – e a Universidade de Messina na Itália.

No Brasil o tema ainda é muito recente e até o presente momento, muito pouco foi encontrado. O trabalho de Moura (2006) faz uso de processos semi markovianos e redes bayesianas para avaliação de indicadores de desempenho (disponibilidade, confiabilidade, manutenibilidade) de sistemas complexos tolerante à falhas. Tais sistemas podem ser considerados como sistemas dinâmicos, no entanto, o autor não trata como uma análise de confiabilidade dinâmica de forma evidente.

No trabalho de Porciúncula (2009) o autor desenvolveu uma metodologia para análise de confiabilidade no projeto de sistemas automáticos. Embora os sistemas automáticos apresentados tenham várias configurações de operação, a abordagem é feita com os conceitos de confiabilidade estática. Ou seja, não foi levada em consideração o comportamento dinâmico das diferentes configurações do sistema. O problema foi analisado por um ponto de vista mais externo, em que foi considerado o tempo médio de ocupação de cada configuração. Com as informações levantadas com a metodologia apresentada pelo autor, a compreensão do sistema torna-se facilitada, principalmente, pelo uso da metodologia Grafcet, onde é explicitado a representação comportamental do modelo.

Em face dessa carência de trabalhos relacionados com o tema, percebeu-se a necessidade de investir pesquisa neste campo de conhecimento e desenvolver uma metodologia para facilitar a análise e o desenvolvimento de modelos.