Walter Nogueira Pizzo

**AVALIAÇÃO DA DISPONIBILIDADE DE SISTEMAS
COMPUTACIONAIS CRÍTICOS PARA O CONTROLE
DO ESPAÇO AÉREO POR MEIO DE MODELO
ANALÍTICO DA TEORIA DE FILAS**

São Paulo

2008

Walter Nogueira Pizzo

**AVALIAÇÃO DA DISPONIBILIDADE DE SISTEMAS
COMPUTACIONAIS CRÍTICOS PARA O CONTROLE
DO ESPAÇO AÉREO POR MEIO DE MODELO
ANALÍTICO DA TEORIA DE FILAS**

Dissertação apresentada à Escola Politécnica da
Universidade de São Paulo para obtenção do
título de Mestre em Engenharia

Área de Concentração:
Sistemas Digitais

Orientador:
Prof. Dr. Paulo Sérgio Cugnasca

São Paulo

2008

Este exemplar foi revisado e alterado em relação à versão original, sob responsabilidade única do autor e com anuência de seu orientador.

São Paulo, 21 de Julho de 2008.

Assinatura do autor _____

Assinatura do orientador _____

FICHA CATALOGRÁFICA

Pizzo, Walter Nogueira

Avaliação da disponibilidade de sistemas computacionais críticos para o controle do espaço aéreo por meio de modelo analítico da teoria de filas / W.N. Pizzo. -- ed.rev. -- São Paulo, 2008.

147 p.

Dissertação (Mestrado) - Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Computação e Sistemas Digitais.

1. Teoria da confiabilidade 2. Modelos analíticos 3. Teoria das filas 4. Espaço aéreo I. Universidade de São Paulo. Escola Politécnica. Departamento de Engenharia de Computação e Sistemas Digitais II. t.

*Dedico este trabalho à memória de meus pais:
Profs. Maria Alzira e Walter Guerino Pizzo*

“Para o sábio todas as terras são acessíveis, pois a pátria da alma virtuosa é o universo”.
(Demócrito, 460-370 a.C. *apud* CHAUÍ, 1994)

AGRADECIMENTOS

Agradeço ao Orientador deste trabalho, o Prof. Dr. Paulo Sérgio Cugnasca, pela clareza, objetividade e generosidade dedicada ao encaminhamento de todas as opções e dúvidas surgidas ao longo da pesquisa, assim como pelo espírito de acolhimento e colaboração encontrado junto aos professores e pesquisadores do Grupo de Análise de Segurança, do Departamento de Engenharia de Computação e Sistemas Digitais da Escola Politécnica.

O propósito de trabalhar sobre a confiabilidade de sistemas de controle do espaço aéreo teve respaldo inicial nos seminários do GAS, ainda no ano de 2003, contando também com apoio de colegas projetistas de sistemas de defesa aérea e controle de tráfego aéreo. Assim, destaco o valor das contribuições do especialista Eno Siewerdt, dos Engs. Fábio Eiras e Atsushi Fukumoto, da Fundação Atech, bem como do Ten.-Cel.-Eng. José Antônio da Motta Matinha, do CINDACTA III, que compartilharam seus conhecimentos técnicos e operacionais sobre centros de controle aéreo no Brasil.

Aos Profs. Benício José de Souza e Graça Bressan, que colaboraram com sugestões referentes ao emprego de ferramentas de simulação utilizadas neste trabalho.

Finalmente, fica a gratidão especial à minha querida Tatiana, que dedicou valioso tempo e muito amor na colaboração permanente à realização deste trabalho.

RESUMO

O transporte aéreo e a indústria de sistemas de defesa foram setores pioneiros na utilização de sistemas computacionais críticos, incrementando os níveis de automação nas atividades de controle do espaço aéreo. Com o crescimento desses setores, verificado pela expansão dos números de vôos, volumes de cargas e usuários, assim como pela ampliação e diversidade das operações militares, os sistemas de controle têm assumido maior complexidade técnica, introduzindo novos recursos de automação ou facilidades adicionais de apoio para funções exercidas manualmente. Essa situação tem ampliado a dependência dos serviços prestados, relativamente à disponibilidade dos sistemas computacionais. Diretrizes de projeto e procedimentos operacionais são estabelecidos para manter os níveis de segurança nos casos de falha, no entanto a disponibilidade torna-se parâmetro crítico, na medida em que algumas falhas podem afetar a eficiência nominal da prestação dos serviços. Nesse cenário, este trabalho propõe um modelo para avaliação da disponibilidade de sistemas de controle do espaço aéreo, a partir de recursos de análises da teoria de filas. Inicialmente é citado um modelo geral para análise de disponibilidade de *data centers*. Em seguida, é apresentada uma extensão do modelo geral para análise da disponibilidade em sistemas de controle do espaço aéreo. Para isso, considerou-se a intervenção humana existente nessa atividade, cujas decisões de controle são exercidas por operadores qualificados (controladores), tanto nas atividades inerentes ao serviço de controle, quanto nos casos de degradação, nos quais os operadores ou técnicos de manutenção assumem alguma tarefa de reparo, decorrente da eventual indisponibilidade de funções do sistema.

Palavras-chave: Confiabilidade de Sistemas Críticos, Tráfego Aéreo, Defesa Aérea, Simulação, Disponibilidade, Manutenibilidade e Segurança.

ABSTRACT

Due to the growth in airspace utilization, which can be verified both in terms of the expansions in aerial movements, airports and volumes of transported passengers and cargo, as well as in terms of the expansion of military operations demands and diversity, airspace control activities have been increasing their technical complexity, introducing new features into the existent automation systems or creating additional resources for the automation of some functions previously performed by human operators. This situation has increased the dependence on the availability of the computer systems involved in the services provided by control centers. Project directives and operational procedures are established in order to maintain the safety integrity levels of the systems, in case any failure occurs. However, the availability becomes a critical parameter, once failure events can force an undesirable state of degraded operation, jeopardizing the nominal capacity of the services being performed through any controlled airspace. In this scenario, this work presents an availability model for the computer systems used in airspace control centers, based on analysis from queuing theory. A general model is first presented, referencing a case study that describes the use of queuing models to access the availability of generic data centers. Further considerations are introduced to extend this general model in order to propose its application for the specific computer systems used in airspace control centers, where operational control relies on human activities. In this case, system operation involves intensive use of human-machine interfaces (HMI), for the regular control services provided, and additional technical or operational maintenance activities, occasionally imposed to repair a momentary loss of any function of the system.

Key words: Reliability of Critical Systems, Air Traffic Control, Air Defense Systems, Simulation, Availability, Maintainability and Safety Assessment.

SUMÁRIO

AGRADECIMENTOS	5
RESUMO.....	6
ABSTRACT	7
SUMÁRIO.....	8
LISTA DE FIGURAS.....	10
LISTA DE TABELAS	12
LISTA DE ABREVIATURAS E SIGLAS	13
1 Introdução.....	16
1.1 Objetivo.....	18
1.2 Motivação.....	19
1.3 Justificativa	20
1.4 Organização do Trabalho	21
2 Sistemas Computacionais Críticos no Controle do Espaço Aéreo.....	23
2.1 Atividades de Controle do Espaço Aéreo no Brasil.....	23
2.2 Visão Geral do Controle de Tráfego Aéreo	26
2.2.1 Serviços de Controle de Tráfego Aéreo	28
2.2.2 Características do Sistema de Controle de Tráfego Aéreo.....	30
2.2.3 Exemplo de Função no Sistema de Controle do Tráfego Aéreo	31
2.3 Visão Geral do Controle de Operações Militares (Defesa Aérea)	32
2.3.1 Exemplo de Atividade Militar para Policiamento do Espaço Aéreo	33
2.3.2 Exemplo de Função Computacional para Elaboração da Síntese Aérea	35
2.4 Considerações Finais deste Capítulo.....	38
3 Confiabilidade e Segurança de Sistemas Computacionais	39
3.1 Confiabilidade de Sistemas Computacionais	39
3.1.1 Conceitos Fundamentais sobre Confiabilidade e Segurança.....	40
3.1.2 Engenharia de Confiabilidade de Software (SRE).....	45
3.1.3 Segurança de Sistemas Computacionais Críticos.....	47
3.1.4 Confiabilidade no Segmento de Sistemas de Defesa	53
3.2 Testabilidade de Sistemas Computacionais	55
3.3 Considerações Finais deste Capítulo.....	57
4 Modelos de Filas na Avaliação de Disponibilidade	58
4.1 Teoria de Filas.....	58
4.1.1 Conceitos Fundamentais sobre Redes de Filas	58
4.1.2 Leis Operacionais dos Sistemas de Filas.....	59
4.1.3 Análise de Valor Médio (AVM)	61
4.2 Modelamento da Disponibilidade por meio da Teoria de Filas	62
4.2.1 Modelo Básico de Operação e Manutenção em um Data Center.....	63
4.2.2 Solução do Modelo de Rede de Filas	65
4.2.3 Exemplo de Cálculo do Modelo de Rede de Filas	67
4.3 Considerações Finais deste Capítulo.....	68
5 Avaliação de Disponibilidade de Sistemas de Controle do Espaço Aéreo....	69
5.1 Modelo de disponibilidade para Centros de Controle do Espaço Aéreo	70

5.1.1	Modos de Operação e Níveis do Serviço Prestado pelo Centro.....	72
5.1.2	Disponibilidade do Sistema Computacional – Estados Operacionais...	74
5.1.3	Exemplo de Modos de Operação de um Centro de Controle APP.....	78
5.1.4	Exemplo de Aplicação do Modelo Genérico para um APP	79
5.1.5	Proposta do Modelo Estendido para Análise de Disponibilidade de um Centro de Controle do Espaço Aéreo	81
5.1.6	Exemplo de Solução por Markov para um Centro APP.....	84
5.2	Solução do Modelo Estendido de Filas Aplicável aos Centros de Controle do Espaço Aéreo.....	85
5.3	Possibilidades Adicionais para Aplicação do Modelo na Avaliação de Desempenho dos Serviços de Controle	86
5.4	Considerações Finais deste Capítulo.....	87
6	Estudo de Caso – Aplicação do Modelo Proposto	88
6.1	Descrição do Ambiente de Simulação	89
6.1.1	Entradas e Saídas dos Cenários Simulados	89
6.1.2	Cenários Considerados para Simulação	91
6.1.3	Valores Considerados na Parametrização dos Cenários	93
6.1.4	Implementação do Modelo de Filas na Ferramenta Arena	95
6.2	Resultados Obtidos nas Simulações.....	99
6.2.1	Resultados de Disponibilidade dos Cenários de Pequeno Porte	101
6.2.2	Resultados de Disponibilidade dos Cenários de Médio Porte.....	104
6.2.3	Resultados de Disponibilidade dos Cenários de Grande Porte	105
6.3	Considerações Finais deste Capítulo.....	108
7	Conclusão	109
7.1	Trabalhos Futuros.....	110
7.2	Considerações Finais.....	111
8	Referências	112
	APÊNDICES	117
	APÊNDICE A	118
	APÊNDICE B.....	131
	APÊNDICE C	135
	ANEXOS	139
	ANEXO A.....	A-1
	ANEXO B.....	B-1
	ANEXO C.....	C-1

LISTA DE FIGURAS

Figura 1 – Sistemas com confiabilidade abaixo da especificada (DoD, 2005)	20
Figura 2 - Níveis hierárquicos dos órgãos de controle de tráfego aéreo	24
Figura 3 - Rotas Nacionais no Espaço Aéreo Brasileiro	24
Figura 4 - Níveis hierárquicos em sistemas militares de defesa aérea	26
Figura 5 – Regiões de Informação de Voo (FIR) no Espaço Aéreo Brasileiro	27
Figura 6 – Operação de um ACC (foto: Revista Força Aérea)	29
Figura 7 – Exemplo de Operação Militar de Reabastecimento em Voo (FAB, 2007).....	33
Figura 8 – Processo de detecção de uma aeronave e elaboração da síntese.....	37
Figura 9 – Decaimento exponencial da confiabilidade de sistemas eletrônicos.....	41
Figura 10 – Causas e efeitos das falhas e níveis de tratamento (JOHNSON, 1989).....	43
Figura 11 – Atividades de SRE no ciclo de vida do produto de software (LYU, 1996).....	47
Figura 12 – Fatores que definem a classificação de riscos.....	49
Figura 13 – Crescimento da parcela dos sistemas militares que não demonstram a confiabilidade especificada (DoD, 2005)	54
Figura 14 – Exemplo de Modelo de Desenvolvimento de Software (<i>Waterfall</i>)	56
Figura 15 – Variáveis associadas a um sistema de filas (JAIN, 1991).....	59
Figura 16 – Modelo de filas da disponibilidade de um centro computacional (MENASCÉ <i>et al</i> , 2004).....	64
Figura 17 – Modelo de Markov para um <i>data center</i> com M máquinas (MENASCÉ <i>et al</i> , 2004).....	65
Figura 18 – Probabilidades (P_j) de encontrar exatamente j máquinas em operação (MENASCÉ <i>et al</i> , 2004).....	68
Figura 19 – Níveis de degradação na prestação dos serviços de controle	74
Figura 20 – Estados das Posições Operacionais do Sistema Computacional.....	76
Figura 21 – Modelo de filas genérico aplicado a um centro APP	80
Figura 22 – Probabilidade (P_j) de encontrar pelo menos j máquinas em operação normal	81
Figura 23 – Modelo estendido para avaliação de disponibilidade de centros de controle do espaço aéreo (PIZZO; CUGNASCA, 2007).....	82
Figura 24 – Solução da fila com aplicação de um Modelo de Markov	84
Figura 25 – Efeito das interrupções do serviço na capacidade do NAS (HORROCKS <i>et al</i> , 2007a)	95
Figura 26 – Implementação do modelo de filas na ferramenta <i>Arena 10.0</i>	97
Figura 27 – Simulação da frequência de reparos com distribuição triangular (KELTON <i>et al</i> , 2007).....	98
Figura 28 – Melhoria da disponibilidade por aumento de operadores e técnicos	102
Figura 29 – Melhoria da disponibilidade por aumento da confiabilidade do sistema	103
Figura 30 – Melhoria da disponibilidade por aumento da redundância	104
Figura 31 – Melhoria da disponibilidade no cenário MBB com aumento de pessoal.....	105
Figura 32 – Melhoria da disponibilidade no cenário GBB com aumento de pessoal	106
Figura 33 – Crescimento da disponibilidade de cenário GBB por aumento da redundância de 6 para 8 posições operacionais	107
Figura 34 – Melhoria da disponibilidade por aumento da confiabilidade do sistema.....	108
Figura 35 – Arquitetura de sistema computacional de um APP	119
Figura 36 – Modelo de sucesso da operação do sistema computacional de um APP	120

Figura 37 – Blocos funcionais para sucesso de missão do sistema	121
Figura 38 – Exemplo de curva de confiabilidade de sistema com 3 estados.....	130
Figura 39 – Modelo de estimativa do crescimento de confiabilidade de software.....	132
Figura 40 – Modelo Log-Poisson (obtenção da taxa de falhas de software λ_0)	133

LISTA DE TABELAS

Tabela 1 – Classificação de aeronaves e procedimentos aplicáveis pela Defesa Aérea.....	35
Tabela 2 – Classificação de risco segundo DEF STAN 00-56 e IEC 61508.....	50
Tabela 3 – Aceitabilidade do risco: comparativo de interpretações.....	51
Tabela 4 – Níveis de Integridade de Segurança (SIL) (HERRMANN, 1999)	52
Tabela 5 – Algoritmo para análise de valor médio – AVM (MENASCÉ <i>et al</i> , 2004).....	62
Tabela 6 – Níveis de degradação do serviço x Estados do sistema computacional	77
Tabela 7 – Cenários de avaliação de disponibilidade de centros de controle aéreo.....	92
Tabela 8 – Confiabilidade dos Serviços e Reparabilidade de Sistemas de Controle em Área Terminal (FAA, 2006b)	94
Tabela 9 – Resultados dos cenários de pequeno porte “PXX”	101
Tabela 10 – Resultados dos cenários de médio porte “MXX”	104
Tabela 11 – Resultados dos cenários de grande porte “GXX”	106

LISTA DE ABREVIATURAS E SIGLAS

ACC	Centro de Controle de Área (<i>Area Control Center</i>)
ADCC	Centros de Comando de Defesa Aérea (<i>Air Defence Command Centers</i>)
ADS	Vigilância Dependente Automática (<i>Automatic Dependent Surveillance</i>)
AEW	Sistema de Alarme Aéreo Antecipado (<i>Airborne Early Warning</i>)
ANAC	Agência Nacional de Aviação Civil
APP	Controle de Aproximação em Área Terminal (<i>Approach Control</i>)
ASAS	Sistema embarcado de assistência à separação de aeronaves (<i>Airborne Separation Assistance Systems</i>)
ASDS	Sistema de visualização da situação aérea (<i>Air Situation Display System</i>)
AT&T	<i>American Telephone & Telegraph Corporation</i>
ATC	Controle de tráfego aéreo (<i>Air Traffic Control</i>)
ATCA	<i>Air Traffic Control Association, Inc.</i>
ATCo	Controlador de tráfego aéreo (<i>Air Traffic Controller</i>)
ATCS	Sistema de controle de tráfego aéreo (<i>Air Traffic Control System</i>)
ATFM	Gerenciamento do fluxo de tráfego aéreo (<i>Air Traffic Flow Management</i>)
ATM	Gerenciamento do tráfego aéreo (<i>Air Traffic Management</i>)
ATMS	Sistema de gerenciamento do tráfego aéreo (<i>Air Traffic Management System</i>)
ATS	Serviço de tráfego aéreo (<i>Air Traffic Service</i>)
AVM	Análise de valor médio de desempenho de um sistema de filas
CADCC	Comando Central de Defesa Aérea (<i>Central Air Defense Command Center</i>)
CAG	Circulação Aérea Geral
CDM	Sistemas colaborativos de apoio à decisão (<i>Collaborative Decision Making</i>)
CNS/ATM	Gerenciamento do tráfego aéreo / Comunicações, Navegação, Vigilância (<i>Communication, Navigation and Surveillance / Air Traffic Management</i>)
CGNA	Centro de Gerenciamento da Navegação Aérea
CINDACTA	Centro Integrado de Defesa Aérea e Controle de Tráfego Aéreo
COAM	Controlador de operações aéreas militares
CODA	Centro de Operações de Defesa Aérea
COM	Circulação operacional militar
COMAER	Comando da Aeronáutica do Ministério da Defesa

COMDABRA	Comando de Defesa Aeroespacial Brasileiro
CopM	Centro de Operações Militares
COTS	Item comercial (<i>Commercial Off The Shelf</i>)
CPDLC	Enlace de comunicações de dados entre controlador e piloto (<i>controller-pilot data link communication</i>)
CTA	Controle de tráfego aéreo
CTAM	Controlador de tráfego aéreo militar
DA	Defesa Aérea
DECEA	Departamento de Controle do Espaço Aéreo do COMAER
DEPV	Diretoria de Eletrônica e Proteção ao Vôo (atual DECEA)
DoD	Departamento de Defesa - EUA
EUA	Estados Unidos da América
EUROCONTROL	Organização Européia para Segurança da Navegação Aérea (<i>European Organization for the Safety of Air Navigation</i>)
FAA	Administração Federal de Aviação dos EUA (<i>Federal Aviation Administration</i>)
FAB	Força Aérea Brasileira
FIR	Região de informação de vôo (<i>Flight Information Region</i>)
FL	Nível de vôo (<i>Flight Level</i>)
GBD	Modelo de nascimento e morte (<i>Generalized Birth-Death</i>)
GCC	Grupo de Comunicações e Controle do DECEA
GPS	Sistema de posicionamento global (<i>Global Positioning System</i>)
HAZOP	<i>Hazard and Operability</i>
HMI	<i>Human-Machine Interface</i>
IAC	Instituto de Aviação Civil da ANAC
ICAO	<i>International Civil Aviation Organization</i> (OACI)
IEEE	<i>Institute of Electrical and Electronic Engineers</i>
IID	Variáveis aleatórias independentes e identicamente distribuídas
MOD	Ministério da Defesa do Reino Unido
MTBF	Tempo médio entre falhas (<i>Mean Time Between Failures</i>) ($MTBF = MTTF + MTTR$)
MTTF	Tempo médio para falhar (<i>Mean Time To Fail</i>)
MTTR	Tempo médio de reparo (<i>Mean Time To Repair</i>)
NAS	Espaço aéreo dos EUA (<i>National Airspace System</i>)
NASPAC	Análise de performance da capacidade do espaço aéreo dos EUA (<i>National Airspace System Performance Analysis Capability</i>)
NM	Milha náutica (<i>Nautical Mile</i>)

OACI	Organização da Aviação Civil Internacional (ICAO)
OCOAM	Órgão de controle de operações aéreas militares
OTAN	Organização do Tratado do Atlântico Norte
RAMS	Confiabilidade, disponibilidade, manutenibilidade e segurança (<i>Reliability, Availability, Maintainability and Safety</i>)
RDA	Região de defesa aeroespacial
RMA	Confiabilidade, manutenibilidade e disponibilidade (<i>Reliability, Maintainability, Availability</i>)
RPL	Plano de voo repetitivo
RVSM	Separação vertical mínima reduzida (<i>Reduced Vertical Separation Mínima</i>)
SBTA	Sociedade Brasileira de Pesquisa em Transporte Aéreo
SIL	Nível de integridade de segurança (<i>Safety Integrity Level</i>)
SRE	Engenharia de confiabilidade de software (<i>Software Reliability Engineering</i>)
STLSC	Categoria de severidade da perda de uma cadeia de serviço crítico (<i>Service Thread Loss Severity Category</i>)
STP	Servidor de tratamento de planos de voo
STR	Servidor de tratamento radar
TMA	Área controle terminal (<i>Terminal Movement Area</i>)
TWR	Torre de controle de aeródromo (<i>Tower</i>)
VHF	Faixa de rádio-frequência muito alto (<i>Very High Frequency</i>)
VOCOM	Plano de voo da circulação operacional militar

1 Introdução

O intuito deste capítulo é apresentar os objetivos deste trabalho de pesquisa, a motivação e as justificativas que levaram à escolha do tema da Dissertação, além da organização deste trabalho.

Os sistemas informatizados para automação dos processos de controle do espaço aéreo abrangem atuações tanto para os sistemas de controle do tráfego aéreo civil, quanto para os sistemas de controle das operações aéreas militares. Tais sistemas possuem arquiteturas funcionais e operacionais estabelecidas a partir de padrões e recomendações de entidades normativas nacionais e internacionais (ICAO, 1996).

No Brasil, devido à natureza integrada dos sistemas de controle civil e militar, as organizações normativas estão vinculadas ao Comando da Aeronáutica, no seu Departamento de Controle do Espaço Aéreo (DECEA), e no Ministério da Defesa, no que tange à Agência Nacional de Aviação Civil (ANAC).

Das entidades internacionais, destacam-se, no âmbito do tráfego aéreo civil: a Organização de Aviação Civil Internacional (ICAO), a Administração Federal de Aviação norte-americana (FAA) e a agência européia EUROCONTROL (*European Organization for the Safety of Air Navigation*). Já no âmbito do controle das operações militares: o Ministério da Defesa Britânico (MOD), a Organização do Tratado do Atlântico Norte (OTAN) e o Departamento de Defesa norte-americano (DoD).

No contexto das atividades de controle do espaço aéreo, os sistemas computacionais representam um elo de apoio à decisão, dentro de uma malha de controle comandada sob a responsabilidade de operadores humanos: os controladores de tráfego aéreo (ATCo), nas operações civis; e os controladores de tráfego aéreo militar (CTAM) ou os controladores de operações aéreas militares (COAM), nas funções de defesa aérea.

Uma vez que o controle humano das operações aéreas pode ser exercido de modo seguro, mesmo na indisponibilidade ou em condições degradadas dos sistemas computacionais (FAA, 2006a), a automação poderia ser considerada com um papel aparentemente secundário ao controle do espaço aéreo. No entanto, a disponibilidade da automação assume importância crítica à eficiência do controle, pois em face dos grandes volumes de operações, os serviços de controle não se tornam viáveis na eventualidade de uma falta prolongada dos sistemas computacionais.

A disponibilidade operacional dos sistemas computacionais torna-se cada vez mais relevante nas atividades de controle do espaço aéreo, em função do crescimento continuado da demanda global por operações aéreas (IAC, 1998). Esse mesmo crescimento também se verifica no Brasil, onde o relatório da demanda detalhada dos aeroportos brasileiros (IAC, 2005a) aponta uma expansão dos movimentos aéreos a taxas médias superiores de 4% ao ano (IAC, 2005b). Sendo assim, a eventual necessidade dos sistemas entrarem em operação degradada, com a adoção de procedimentos manuais (não-automatizados), resulta em maiores tempos de tomada de decisão pelos controladores, com conseqüente aumento no espaçamento entre aeronaves em vôo e imposição de atrasos devidos aos maiores intervalos para autorização de pousos e decolagens.

Um dos motivos que demandam altos índices de disponibilidade dos sistemas computacionais no controle do espaço aéreo é que as situações de atrasos mencionadas anteriormente podem propagar-se para uma grande área geográfica. Isso ocorre mesmo para casos de falha em uma área restrita, por exemplo, sobre um único centro de controle de área (ACC), ou sobre um centro de controle de aproximação (APP) de uma área terminal de grande movimento, cujos impactos nas operações aéreas podem afetar pontos remotos, ao longo de toda a rede de conexões envolvidas, atingindo inclusive regiões distantes de outros países.

Tais situações, apesar de ainda representarem uma condição segura de controle, afetam negativamente a eficiência da navegação aérea, reduzindo os fluxos e a capacidade de prestação de serviços naquele espaço aéreo, e cujo impacto pode alastrar-se por uma área muito mais abrangente e extrapolar também o período de tempo das ocorrências locais, onde teve origem a falha causadora da indisponibilidade inicial do sistema.

Assim, uma interrupção na oferta dos serviços de controle em seu nível nominal, com a conseqüente geração de atrasos nos movimentos aéreos, reduz a capacidade operacional do sistema (degradação da capacidade do espaço aéreo), eventualmente resultando em comprometimento econômico do transporte aéreo, no caso civil, ou comprometimento da eficácia de ações de vigilância e defesa, no caso de indisponibilidade de partes dos sistemas de controle das operações aéreas militares.

Em condições normais de operação, enquanto os sistemas computacionais permanecem disponíveis, os recursos automatizados representam um ganho adicional para a capacidade dos operadores desempenharem suas atividades de forma mais segura. Isso

ocorre, uma vez que suas decisões podem ser auxiliadas pelos algoritmos e processos automatizados que envolvem a avaliação de muitos parâmetros em pequenos intervalos de tempo, provendo informações de apoio relevantes que favorecem a correção, bem como a presteza e eficiência das ações dos controladores. Por isso, em condições degradadas pela eventual indisponibilidade dos sistemas automatizados de apoio, o processo de controle torna-se mais lento, devido às maiores separações entre aeronaves, resultando em comprometimento, muitas vezes severo, no nível de prestação de serviços desses centros.

Nesse contexto, este trabalho de pesquisa trata da avaliação da disponibilidade de sistemas computacionais em centros de controle do espaço aéreo, com interesse direto às questões de gerenciamento, dimensionamento de recursos e planejamento da manutenção operacional desses centros. Um modelo de avaliação de disponibilidade pode tornar-se recurso de apoio à gestão dos centros de controle do espaço aéreo, tanto para os centros de gerenciamento e controle de tráfego aéreo civil (ATM), quanto para os órgãos de controle das operações aéreas militares (OCOAM).

A principal contribuição esperada desta pesquisa é a apresentação de um modelo para avaliação de disponibilidade desses centros, com base nos conhecimentos científicos e técnicas de engenharia existentes na área de confiabilidade, que favoreçam a adoção prática de análises de disponibilidade no dimensionamento técnico-operacional dos sistemas empregados nos centros de controle do espaço aéreo.

Adicionalmente, espera-se que a prática dessas análises possa ainda contribuir para as atividades de concepção e projeto de sistemas computacionais críticos no controle aéreo, a partir do estabelecimento quantitativo de requisitos formais de confiabilidade, disponibilidade e segurança nessas aplicações.

1.1 Objetivo

O objetivo desta pesquisa é apresentar um modelo de avaliação de disponibilidade aplicável aos sistemas computacionais críticos dos centros de controle do espaço aéreo. Para isso, são empregados métodos analíticos da teoria de filas, ilustrando um exemplo de aplicação, com desenvolvimento de simulações, passíveis de reprodução em casos reais. Desta forma, pretende-se favorecer o uso do modelo apresentado para análise dos sistemas existentes de controle de tráfego aéreo e de defesa aérea.

A partir da aplicação de conhecimentos de engenharia já disponíveis na área de confiabilidade de sistemas computacionais, um objetivo complementar deste trabalho é apresentar contribuições teóricas que incentivem e favoreçam a prática de análises de confiabilidade, disponibilidade e segurança ao longo de todo o ciclo de vida do projeto de sistemas de controle do espaço aéreo.

1.2 Motivação

A motivação principal para realização deste trabalho decorre da expectativa de que os objetivos mencionados anteriormente pudessem ser úteis tanto para os projetistas, nos segmentos industriais aeronáuticos e de defesa, responsáveis pelas fases de projeto, desenvolvimento, implementação e testes dos sistemas computacionais críticos utilizados nos controles de tráfego aéreo e de operações de defesa aérea, quanto para as organizações operadoras desses sistemas, responsáveis pelas fases de concepção, especificação, certificação, operação e manutenção desses centros de controle.

A motivação inicial para execução desta pesquisa resultou de uma necessidade técnica verificada em projetos de sistemas na área de defesa (JACKSON *et al*, 2005), incluindo as aplicações de sistemas críticos do controle do espaço aéreo (FAA, 2006b), que recomenda a existência de um processo formal para especificar e verificar os requisitos não-funcionais ligados à confiabilidade, disponibilidade e segurança desses sistemas computacionais. Tais aplicações envolvem atividades de engenharia de sistemas de vigilância e defesa aérea, bem como o desenvolvimento de software utilizado para controle do espaço aéreo.

Adicionalmente, colaborou com a motivação mencionada o fato do Departamento de Defesa norte-americano (DoD) ter publicado, em 2005, novas diretrizes para assegurar a confiabilidade, disponibilidade e manutenibilidade (RAM - *Reliability, Availability and Maintainability*) das aquisições militares de sistemas de defesa (DoD, 2005). Esses estudos destacaram a necessidade de reformular a aplicação das ferramentas teóricas já disponíveis na área de confiabilidade, promovendo um aprimoramento da gestão das aquisições em projetos militares.

A Figura 1 ilustra o “Problema RAM”, mencionado pelo DoD, segundo o qual, no período de 1985 a 2000, houve um crescimento da parcela dos sistemas militares analisados que não demonstraram, nos testes operacionais, a confiabilidade especificada durante as fases de aquisição e projeto.

Figura 1 – Sistemas com confiabilidade abaixo da especificada (DoD, 2005)

Desse cenário, surgiu o interesse de colaborar com o processo de aquisições de sistemas de controle do espaço aéreo, de modo a evitar que o foco do projeto fique restrito aos requisitos de performance técnica e funcional no desenvolvimento, para considerar, em mesmo grau, os requisitos não-funcionais ligados à especificação e verificação de confiabilidade, disponibilidade e segurança desses sistemas computacionais.

Assim, o trabalho de pesquisa realizado pretende gerar benefícios diretos para as entidades governamentais, empresas e o meio científico, que de alguma forma estejam relacionados com atividades de definição, operação ou implantação de sistemas de controle do espaço aéreo. De forma indireta, os conceitos apresentados neste trabalho podem colaborar para o incremento da disponibilidade dos sistemas desenvolvidos para aplicações críticas do segmento aeronáutico.

1.3 Justificativa

Para que os sistemas computacionais empregados nos centros de controle do espaço aéreo apresentem os parâmetros desejados de confiabilidade, segurança e disponibilidade operacional, faz-se necessária a adoção de determinadas práticas de engenharia que favoreçam o estabelecimento formal de requisitos, assim como a modelagem adequada que permita estabelecer métricas (DELONG *et al*, 2005) para análises realizadas nas fases de especificação, projeto, aceitação e, posteriormente, durante a vida operacional dos sistemas.

Em função das demandas e requisitos operacionais dos usuários finais desses sistemas, ou seja, as autoridades que operam, efetuam a manutenção, gerenciam as aquisições e a implantação dos sistemas de controle de tráfego aéreo e de defesa aérea, estima-se que a tecnologia de desenvolvimento dos sistemas nessas aplicações críticas deva suplantar o contexto restrito das metas de qualidade de engenharia de software – envolvendo o ciclo de vida, especificações, rastreabilidade de requisitos e testabilidade de sistemas críticos (LEVESON, 1995) – para a incorporar também as etapas previstas em padrões recentemente disponibilizados (DoD, 2003) (FAA, 2006b), concernentes aos requisitos de disponibilidade, confiabilidade e segurança do projeto, abrangendo toda a arquitetura do sistema, hardware, sensores, software utilizado e fatores humanos.

Assim, o interesse principal deste trabalho é contribuir com os segmentos brasileiros de desenvolvimento de sistemas de defesa - Indústria e Governo - com a identificação de vantagens da adoção de técnicas de análise de disponibilidade dos sistemas de controle do espaço aéreo, procurando ainda favorecer a disseminação no uso do estado da arte nesse segmento da engenharia, tanto no proveito dos benefícios dessas práticas no aspecto do desenvolvimento tecnológico, quanto no aspecto do gerenciamento de projetos e aquisições em aplicações críticas de controle do espaço aéreo.

1.4 Organização do Trabalho

Este trabalho está organizado com a seguinte estrutura:

O Capítulo 1 apresenta uma introdução geral, contendo o objetivo e a motivação da pesquisa na área de confiabilidade de sistemas de controle do espaço aéreo.

O Capítulo 2 apresenta uma visão geral sobre a atividade de controle do espaço aéreo, indicando a importância das características de confiabilidade, disponibilidade e manutenibilidade dos sistemas computacionais empregados nesses centros de controle para aplicações aeronáuticas civis e militares.

O Capítulo 3 apresenta uma introdução geral sobre a confiabilidade de sistemas computacionais, destacando os conceitos relevantes no enfoque das principais técnicas de modelamento de confiabilidade e disponibilidade de sistemas críticos, favorecendo um melhor embasamento da modelagem proposta no Capítulo 5.

O Capítulo 4 apresenta um modelo geral para avaliação de disponibilidade de sistemas computacionais com base em conceitos da teoria de filas.

O Capítulo 5 apresenta um modelo específico para avaliação da disponibilidade de sistemas de controle do espaço aéreo, a partir de uma extensão do modelo geral apresentado no Capítulo 4.

O Capítulo 6 detalha um caso de aplicação do modelo descrito no Capítulo 5, apresentando resultados da avaliação de disponibilidade simulados para alguns cenários característicos de centros de controle do espaço aéreo.

O Capítulo 7 apresenta as conclusões gerais deste trabalho, indicando interesses sobre futuros trabalhos decorrentes desta pesquisa na área de confiabilidade de sistemas computacionais críticos e aplicações de controle do espaço aéreo.

O Apêndice A contém um exemplo de cálculo de confiabilidade de sistemas, com base em modelos combinatórios, e uma planilha para análise de disponibilidade de sistemas com três estados de operação, com base em solução por diagrama de Markov.

O Apêndice B contém um resumo sobre modelos de crescimento de confiabilidade de software e técnicas de predição de confiabilidade de software.

O Apêndice C contém referências dos modelos implementados para simulações dos cenários apresentados no Capítulo 6 deste trabalho.

O Anexo A reproduz um exemplo teórico da aplicação de modelos de Markov, na solução geral de processos de nascimento e morte (GBD).

O Anexo B reproduz um conjunto das principais distribuições estatísticas disponíveis na ferramenta Arena, aplicáveis ao caso de interesse deste trabalho, na modelagem de tempos de execução de tarefas de reparo/manutenção de sistemas.

O Anexo C reproduz uma tabela comparativa dos recursos de diversas ferramentas de simulação, indicando algumas características que favoreceram o uso do software Arena.

2 Sistemas Computacionais Críticos no Controle do Espaço Aéreo

Este capítulo apresenta uma visão geral sobre a atividade de controle do espaço aéreo, destacando algumas características de confiabilidade, disponibilidade e manutenibilidade dos sistemas computacionais críticos empregados nesses centros de controle, para aplicações aeronáuticas civis e militares.

2.1 Atividades de Controle do Espaço Aéreo no Brasil

No Brasil, as atividades de controle do espaço aéreo são reguladas pelo Comando da Aeronáutica, por meio de seu Departamento de Controle do Espaço Aéreo (DECEA), respondendo, entre outras atribuições, pela gestão, implantação e manutenção de infraestrutura técnica e operacional das atividades relacionadas ao Controle do Tráfego Aéreo Civil e ao Controle das Operações Militares envolvidas na vigilância e defesa do espaço aéreo brasileiro.

Os serviços de controle de tráfego aéreo (ICAO, 1996) (DECEA, 2006) são prestados em estruturas operacionais cujas hierarquias estabelecem, basicamente, os quatro níveis de controle ilustrados pela Figura 2, descritos a seguir:

- a) Nível da Torre de Controle - TWR, onde ocorre a gestão de pousos e decolagens e demais operações internas a um aeródromo;
- b) Nível do Controle de Aproximação em Área Terminal - APP, onde se exerce o controle do tráfego em áreas terminais, que são estabelecidas no entorno de áreas de aproximação de grandes aeroportos, e que respondem pelo seqüenciamento de aeronaves, encaminhando-as para pouso ou direcionando seus trajetos desde a decolagem até a entrada em rota;
- c) Nível dos Centros de Controle de Área - ACC, onde se realiza o controle da evolução das aeronaves nas rotas nacionais e internacionais (aerovias). A Figura 3 contém um mapa de exemplo das rotas nacionais no Brasil;
- d) Nível da gestão estratégica de fluxos de aeronaves - ATFM, realizada nos Centros de Gerenciamento da Navegação Aérea (CGNA), onde são tratados os problemas da otimização dos fluxos operacionais, inclusive envolvendo as questões de médio e longo prazos, relativas às futuras demandas de vôos (DECEA, 2007).

Figura 2 - Níveis hierárquicos dos órgãos de controle de tráfego aéreo

A cada nível descrito corresponde uma escala temporal no controle de processos de tempo real: desde a escala de sensoriamento e tomada de decisões em segundos ou minutos, na Torre e no APP; até o controle de operações em rota, também em tempo real, envolvendo operações de até algumas horas, no ACC; sendo ainda, no nível estratégico do CGNA, considerados os dados históricos e as estatísticas para o planejamento e gestão de operações na escala de dias a até vários meses.

Figura 3 - Rotas Nacionais no Espaço Aéreo Brasileiro

Tais aplicações de sistemas de informação exigem um elevado grau de automação e capacidade computacional em todas as etapas, desde a coleta de dados em tempo real de sensores (radares), armazenamento e manutenção das bases de dados, passando pela análise das informações tratadas até a apresentação dessas informações para interação com os operadores, responsáveis pelo controle propriamente dito.

Analogamente à estrutura das aplicações do controle do tráfego aéreo civil, os sistemas voltados à defesa aérea organizam-se de forma hierarquicamente similar, respondendo desde o nível estratégico central de comando e controle das operações aéreas militares (FAA, 2004), até os sistemas remotos de vigilância local e geração de alarmes aéreos antecipados.

A Figura 4 ilustra uma hierarquia típica de comando nos sistemas de controle de operações militares de defesa aérea, conforme a seguinte descrição:

- a) No nível inferior, estão os sistemas de alerta ou controle de operações locais (AEW e ASDS), normalmente envolvendo a vigilância em localidades remotas, baterias de defesa antiaérea e radares transportáveis (em solo, embarcações ou aeronaves), cujas unidades respondem pela geração dos alarmes iniciais sobre as ameaças aéreas detectadas. Na FAB, por exemplo, tais atividades são realizadas pelos Grupos de Comunicações e Controle (GCC) e pelo 2º Esquadrão do 6º Grupo de Aviação, sediado em Anápolis, responsável pela condução de missões das aeronaves de controle e alarme aéreo antecipado R-99A;
- b) Nos centros de operações militares (ADCC), é realizada a vigilância sobre toda uma região de defesa aérea, de onde são acionadas e controladas operações militares de interceptação, busca e salvamento, etc., além do controle do tráfego aéreo militar. No Brasil, tais atividades são realizadas pelos Centros de Operações Militares (COPM), localizados em cada CINDACTA;
- c) No nível hierárquico mais elevado, o comando central das operações de defesa aérea (CADCC) coordena todas as operações militares, no nível estratégico, a partir da visualização da síntese da situação em todo o espaço aéreo nacional, sendo também o órgão responsável pelas ordens que demandem tomada de decisão pelas autoridades superiores. No Brasil, essas atividades são realizadas

pelo Centro de Operações de Defesa Aérea (CODA), sob responsabilidade do COMDABRA.

Figura 4 - Níveis hierárquicos em sistemas militares de defesa aérea

Sendo assim, com mais ênfase ao caso brasileiro, onde se estabeleceram os Centros Integrados de Defesa Aérea e Controle de Tráfego Aéreo (CINDACTA), o estudo de caso apresentado neste trabalho pode constituir também uma contribuição às aplicações de interesse dos sistemas militares de defesa, nos níveis correspondentes.

2.2 Visão Geral do Controle de Tráfego Aéreo

Em termos operacionais, o controle do tráfego aéreo é realizado basicamente por meio de comunicações via rádio em *very high frequency* (VHF), sendo que os sistemas de controle automatizados, envolvendo os sensores radar e os sistemas computacionais, servem como meios de apoio à decisão, para que controladores humanos efetuem corretamente as instruções para os pilotos em trânsito dentro de certas regiões do espaço aéreo controlado.

Quaisquer inoperâncias dos sensores ou dos sistemas computacionais repercutem na quantidade (capacidade) de aeronaves controladas em determinado espaço e tempo, e não na segurança delas, uma vez que tais situações devem levar a uma condição previamente estabelecida de operação degradada. Ou seja, nesses casos se estabelece uma operação mais limitada em relação à quantidade de aeronaves controladas, porém ainda segura e adequada aos tempos de decisão dos controladores, independentemente da indisponibilidade dos sistemas automatizados de apoio.

O controle das operações aéreas é executado segundo os níveis hierárquicos mencionados anteriormente. Inicia pela comunicação do piloto com o controle de solo, que autoriza a partida para taxiar, até que a torre de controle do aeródromo libere o acesso à pista e a decolagem da aeronave. Após a decolagem, o piloto é orientado a comunicar-se com o controle de aproximação (APP) correspondente, que controla a subida e evolução dentro da área terminal (TMA) até a entrada na rota planejada.

Uma vez em rota, o controle da aeronave passa a ser exercido pelos sucessivos centros de área (ACC), ao longo de todos os trechos subsequentes do plano de vôo, que pode envolver vários países. Segundo o apresentado em uma visão geral do sistema (OLIVEIRA, 2007), as Autoridades Aeronáuticas, em cada país, normalmente segmentam o espaço aéreo em Regiões de Informação de Vôo (FIR) que correspondem à abrangência do controle exercido por um Centro ACC de acordo com os padrões estabelecidos pela Organização da Aviação Civil Internacional (OACI). No Brasil, as regiões de espaço aéreo associadas a cada FIR estão ilustradas na Figura 5.

Figura 5 – Regiões de Informação de Vôo (FIR) no Espaço Aéreo Brasileiro

Posteriormente, com a chegada do vôo à região próxima do aeroporto de destino, a descida e aproximação passam a ser controladas pelo órgão responsável pelas operações na área terminal naquele destino. Esse centro de controle, então, encaminha a aeronave para aterrissagem, cuja etapa final é controlada pela torre do aeroporto.

A Instrução do Comando da Aeronáutica 100-12 (DECEA, 2006) estabelece as regras do ar e serviços de tráfego aéreo no Brasil. Essas regras descrevem os procedimentos que devem ser adotados em todas as etapas descritas anteriormente, envolvendo os diferentes níveis hierárquicos do controle, e se aplicam a todas as aeronaves que utilizem o espaço aéreo sob jurisdição brasileira.

Destacam-se, dessa norma, os seguintes tópicos:

- a) Antes de iniciar o voo, o piloto deve ter todas as informações necessárias ao planejamento de voo;
- b) O piloto é o responsável para que a operação se realize de acordo com as regras do ar, somente podendo delas se desviar quando absolutamente necessário ao atendimento de exigências de segurança;
- c) Todas as mudanças introduzidas em um plano de voo, definido conforme a IMA 100-11 (DEPV, 1985), devem ser comunicadas de imediato ao órgão ATS (órgão prestador do serviço de controle de tráfego aéreo) correspondente;
- d) Toda aeronave deverá ater-se ao plano de voo em vigor. Qualquer modificação no plano de voo deverá ser previamente solicitada ao órgão de controle do espaço aéreo e só pode ser realizada após autorização deste órgão.

2.2.1 Serviços de Controle de Tráfego Aéreo

A seguir são listados os principais serviços prestados pelos centros de Controle de Tráfego Aéreo, que operam em ambientes similares ao da Figura 6, que ilustra o ACC da região de Brasília. No caso do controle de aeronaves em rota, destacam-se especificamente os seguintes serviços (DECEA, 2006):

- a) Controle do tráfego aéreo em rota;
- b) Seqüenciamento de aeronaves em rota;
- c) Procedimentos de espera e emergência;
- d) Coordenação de transferências de controle entre setores e Centros adjacentes;

No caso do controle de aeronaves em áreas terminais, referentes aos procedimentos adotados após a decolagem ou na aproximação anterior ao pouso, destacam-se especialmente os seguintes serviços (DECEA, 2006) prestados pelo controle em área terminal (APP), conforme segue:

- a) Controle do tráfego aéreo na área terminal;
- b) Procedimentos de aproximação e partida;
- c) Seqüenciamento de aeronaves para pouso;
- d) Procedimentos de espera e emergência;
- e) Coordenação de transferências de controle entre setores e Centros adjacentes.

Figura 6 – Operação de um ACC (foto: Revista Força Aérea)

Relativamente aos serviços mencionados anteriormente, destacam-se as seguintes funções principais (DECEA, 2006):

- Tratamento de dados dos sensores (radares);
- Tratamento de dados dos Centros Adjacentes;
- Elaboração da síntese¹ da situação aérea em uma região de controle;
- Elaboração da síntese da situação aérea em uma área terminal;
- Tratamento de planos de voo da circulação aérea geral (vôos civis);
- Tratamento de conflitos para geração de alarmes de anti-colisão (ar-solo / ar-ar);
- Gravação e re-visualização de dados;
- Supervisão técnica e operacional.

¹ Apresentação visual integrada, com todos os vôos de interesse, sintetizando os dados (detecções) provenientes de vários radares.

2.2.2 Características do Sistema de Controle de Tráfego Aéreo

Ao longo de todas as fases do voo, a comunicação de áudio entre piloto e controlador é comumente estabelecida por rádios VHF, sendo as instruções passadas por comandos de voz, segundo uma fraseologia padronizada estabelecida pelas entidades normativas, por exemplo, pela instrução ICA-100-12 (DECEA, 2006), no espaço aéreo brasileiro.

Mais recentemente, novos sistemas passaram a ser introduzidos com o objetivo de permitir a comunicação de dados, entre controlador e piloto, por meio de equipamento instalado na cabine das aeronaves e nos órgãos de controle. Esse sistema, denominado CPDLC (*Controller-Pilot Data Link Communication*) possibilita a troca de mensagens digitais padronizadas entre o órgão de controle e o piloto, aumentando a precisão e eficiência das comunicações, e contribuindo para a segurança das operações de controle, na medida em que reduz riscos decorrentes das interpretações na comunicação por voz.

Durante o voo, a evolução da aeronave é rastreada por meio de sensores eletrônicos (radares) que permitem medir os parâmetros cinemáticos principais da aeronave, tais como posição, altitude (ou nível de voo), velocidade e sentido do deslocamento (proa). Essas informações normalmente são obtidas por uma rede de radares primários e secundários.

O radar primário é aquele que não depende de ação por parte do alvo que está sendo detectado, sendo que o sinal captado pela antena do radar é apenas a reflexão do pulso que ela mesma havia transmitido. A utilização de radares primários é essencial para as atividades de vigilância e defesa do espaço aéreo, uma vez que permite estabelecer a posição e comportamento dos alvos independentemente da ação destes.

O radar secundário é um sistema cooperativo, que recebe, em solo, um sinal ativamente transmitido pelo alvo toda vez que este responde a um sinal interrogador. Para tanto, a aeronave alvo deve estar equipada com um equipamento (*transponder*) capaz de receber e compreender o sinal interrogador, gerando a transmissão de uma mensagem de resposta, com informações de identificação, posicionamento e atitude² da aeronave. Por isso, o sistema secundário apresenta confiança e precisão superiores às obtidas pelo radar primário, uma vez que as informações transmitidas são geradas pelos próprios sistemas embarcados, GPS ou inercial, da aeronave. O uso desse equipamento

² Em alguns sistemas, a resposta pode incluir, além das informações básicas de posição e altitude, outras indicações adicionais sobre a atitude da aeronave, tais como: proa (rumo), razão de subida, descida, etc.

é mandatório para certas condições de voo por instrumentos, por exemplo, em regiões onde se navega sob condições de separação vertical mínima reduzida (RVSM).

A partir de definições mais recentes para a concepção de sistemas de vigilância (ICAO, 2003), geradas por conta da disponibilização de novas tecnologias de comunicação e posicionamento por satélite (GPS), os sistemas de controle de tráfego aéreo do futuro deverão adotar diversas facilidades adicionais (DONOHUE; ZELLWEGER, 2001), que incluem recursos de decisão colaborativa (CDM) e novos sistemas cooperativos, por exemplo, o sistema ASAS (OLIVEIRA, 2007), que provê auxílio de auto-separação entre aeronaves, no conceito *free flight*. O surgimento desses novos recursos cria ainda maior dependência das informações coletadas pelas próprias aeronaves em voo, dispensando em grande parte o sensoriamento efetuado pelos radares em solo.

Nesse contexto de evoluções dos sistemas de vigilância, foi estabelecido o conceito ADS - *Automatic Dependent Surveillance* (EUROCONTROL, 2002), no qual o espaçamento das aeronaves passa a ser realizado em função dos dados cinemáticos gerados e transmitidos autonomamente das aeronaves para os centros de controle, por meio de comunicações de dados por satélite ou de bases terrestres, podendo envolver também o mecanismo de comunicação automatizado entre piloto e controlador (CPDLC), mencionado anteriormente.

2.2.3 Exemplo de Função no Sistema de Controle do Tráfego Aéreo

Uma função de interesse para os sistemas computacionais no controle de tráfego aéreo é a extração de planos de voo de um sistema servidor, que contém todos os voos com planos autorizados para aquele centro. Essa função é responsável por manter atualizada uma fila de planos de voo que devem ser controlados em um determinado centro, durante um período de tempo. Assim, são apresentados na posição de controle os planos previstos, ativos e realizados, com todas as informações para acompanhamento e controle por parte do controlador.

Quando da ativação de um plano previamente autorizado para um certo período, o sistema computacional pode realizar a correlação com as aeronaves sendo rastreadas em tempo real. Quando do surgimento de uma aeronave, que entra na região de controle a partir de uma aerovia ou de um aeroporto, o sistema é capaz de comparar as informações reais do plano (código *transponder*, posição, altitude, etc.) associando as informações do plano com a aeronave rastreada.

Uma vez correlacionada a aeronave com seu plano de voo autorizado, o sistema pode então realizar outras funções automatizadas, como por exemplo, a verificação dos desvios da evolução real da aeronave rastreada no cenário, em relação a cada trecho do plano autorizado, no que diz respeito a eventuais variações de posição, rumo, velocidade ou altitude previstas ao longo da rota.

2.3 Visão Geral do Controle de Operações Militares (Defesa Aérea)

Para o exercício das atividades de controle das operações militares, o COMAER também estabelece, por meio da instrução IMA-100-13 (DEPV, 1989), as regras para o tráfego aéreo militar, além de outras normas - de acesso restrito - que regulamentam as operações aéreas militares de defesa aérea. De forma análoga, as entidades militares de cada país estabelecem seus procedimentos específicos para regulamentação das operações aéreas militares, sendo um exemplo a norma norte-americana FAA-7610.4 (FAA, 2004).

À semelhança do controle civil, as operações militares também são controladas segundo uma segmentação do espaço, em regiões de responsabilidade definidas pela Autoridade Aeronáutica que, no Brasil, denominam-se Regiões de Defesa Aeroespacial (RDA), correspondendo geograficamente às FIR mencionadas anteriormente.

A seguir estão listados os principais serviços prestados pelas organizações militares responsáveis pelas atividades de Defesa Aérea. Nesse contexto, destacam-se especialmente as seguintes atividades realizadas em um Centro de Controle de Operações Aéreas Militares (COPM), conforme segue (DEPV, 1989):

- a) Controle de tráfego aéreo militar, análogo ao controle do tráfego civil, porém específico para atender aos vôos da circulação operacional militar (COM);
- b) Controle de operações aéreas militares, incluindo: missões de patrulha e reconhecimento, vetoração³ de caças em missões de interceptação de aeronaves suspeitas, reabastecimento em voo (Figura 7), missões de busca e salvamento, recolhimento de aeronaves militares para as bases aéreas após suas missões, etc;
- c) Vigilância e apoio ao policiamento do espaço aéreo, por meio da identificação e classificação de aeronaves novas que surgem no cenário sob controle;

³ Orientação dos controladores aos pilotos na condução das aeronaves controladas.

- d) Autorização e monitoramento de aeronaves militares que sobrevoam o território brasileiro.

Figura 7 – Exemplo de Operação Militar de Reabastecimento em Vôo (FAB, 2007)

Relativamente aos serviços mencionados anteriormente, destacam-se as seguintes funções principais (DEPV, 1989):

- Tratamento dos dados dos sensores (radares fixos, transportáveis ou embarcados);
- Elaboração da síntese da situação aérea de interesse para a defesa aérea;
- Tratamento de dados dos Centros Adjacentes;
- Resolução de algoritmos de interceptação e recolhimento de aeronaves;
- Tratamento de planos de vôo da circulação aérea militar (VOCOM);
- Tratamento de conflitos e geração de alarmes de anti-colisão (ar-solo / ar-ar);
- Gravação e re-visualização de dados;
- Supervisão técnica e operacional.

2.3.1 Exemplo de Atividade Militar para Policiamento do Espaço Aéreo

Como exemplo das atividades prestadas pelo controle de operações militares, a página da FAB na Internet (FAB, 2007) apresenta uma descrição das atividades de

policciamento do espaço aéreo, com destaque para a recente regulamentação no Brasil, por meio de Lei de 2004, dos procedimentos de tiro de destruição, mais amplamente conhecida como “Lei do Abate”.

Os debates prévios à criação dessa Lei foram ampliados com o episódio das ações terroristas de 11 de setembro de 2001, nos EUA, e puderam levantar diversos aspectos referentes à política de defesa nacional (FLORES, 2002) e às dificuldades jurídicas e operacionais para a implantação efetiva de instrumentos de combate às atividades criminosas que utilizam o espaço aéreo como meio de ação. Tais debates têm abordado desde as alegações de vinculação jurídica ao conceito de pena de morte (ASSIS, 1998), até os procedimentos operacionais necessários aos militares que comandam e conduzem as ações correspondentes (QUÍRICO, 2002).

Finalmente, com a regulamentação da Lei do Tiro de Destruição, em 2004, foram criados os instrumentos de dissuasão adequados ao policiamento do espaço aéreo brasileiro, abrangendo apenas o caso de aeronaves suspeitas de envolvimento com o tráfico internacional de drogas.

Tal regulamentação define que, antes de ser classificada como hostil e, portanto, ficar sujeita à medida de destruição, a aeronave deve ser considerada suspeita, sendo submetida a procedimentos específicos, detalhados e seguros. São duas as situações em que uma aeronave pode ser considerada suspeita:

- a) A que entrar em território nacional, sem plano de voo aprovado, oriunda de regiões reconhecidamente fontes de produção ou distribuição de drogas ilícitas;
- b) A que omitir aos órgãos de controle informações necessárias à sua identificação, ou não cumprir determinações dessas mesmas autoridades, caso esteja trafegando em rota presumivelmente utilizada na distribuição de drogas ilícitas.

Caracterizada a aeronave como suspeita, ela fica sujeita a medidas coercitivas, aplicadas de forma progressiva, para somente então, se considerada hostil, ficar sujeita à medida de destruição. As aeronaves de interceptação da FAB, acionadas pelo Comando de Defesa Aeroespacial Brasileiro - COMDABRA, serão encarregadas da execução dessas medidas, conforme ilustra a Tabela 1 (FAB, 2007):

- Medidas de Averiguação – para determinar a identidade da aeronave, por meio dos seguintes procedimentos: reconhecimento à distância; confirmação da

matrícula da aeronave; interrogação na frequência internacional de emergência; e realização de sinais visuais, de acordo com as regras internacionais;

- Medidas de Intervenção – caso a aeronave suspeita não responda às medidas anteriores, a intervenção é realizada por meio de dois procedimentos: mudança de rota e pouso obrigatório, determinados pela aeronave interceptadora;
- Medidas de Persuasão – as medidas seguintes consistem na realização de tiros de advertência, com munição traçante, de forma visível e sem atingi-la;
- Medidas de Destruição – transgredidos todos os procedimentos anteriores, a aeronave será considerada hostil, ficando sujeita à medida de destruição pela interceptadora, com a finalidade de provocar danos e impedir o prosseguimento do voo hostil. Esse procedimento deve atender, obrigatoriamente, às exigências previstas no Decreto nº 5.144, de 16 de julho de 2004 (FAB, 2007), vinculadas à autorização da Presidência da República.

Tabela 1 – Classificação de aeronaves e procedimentos aplicáveis pela Defesa Aérea

Situação da Aeronave	Nível da Medida	Procedimentos
Normal	Situação de Normalidade	Verificação das condições de voo da aeronave.
Suspeita	Medidas de Averiguação	1) Reconhecimento à Distância; 2) Confirmação de Matrícula; 3) Contato por Rádio na Frequência de Emergência; 4) Sinais Visuais.
	Medidas de Intervenção	5) Mudança de Rota; 6) Pouso Obrigatório.
	Medidas de Persuasão	7) Tiros de Advertência.
Hostil	Medidas de Destruição	8) Tiro de Destruição

2.3.2 Exemplo de Função Computacional para Elaboração da Síntese Aérea

A seguir, apresenta-se um exemplo de função automática, desempenhada pelos sistemas computacionais no controle do espaço aéreo, fundamental tanto para os centros de Controle de Tráfego Aéreo, quanto para o Controle de Operações de Defesa Aérea.

Essa função corresponde à elaboração da síntese da situação aérea, em tempo real, responsável pela composição de uma visualização integrada (sintética) de toda a área de controle apresentada ao operador, a partir de sinais recebidos de forma redundante pelos diversos radares distribuídos na região de interesse.

Um aspecto importante do sensoriamento realizado pelos radares é a geração de múltiplas detecções para uma mesma aeronave rastreada. Esse processo ocorre de forma assíncrona, dado que cada radar possui período de rotação independente dos demais, podendo variar, normalmente de 4 a 15 segundos, em função do tipo do radar.

A Figura 8 ilustra o processo de detecção⁴ de uma aeronave, em uma área de controle na qual se requer elaborar a síntese da situação aérea. Essa área é dividida em quadrículas, compondo um mosaico com a resolução desejada do modelo digital de elevação do terreno (relevo). Comparando as situações indicadas em t_1 e t_2 , verifica-se que em cada quadrícula pode ser estabelecida uma lista de prioridades dos radares capazes de efetuar a detecção. O critério de definição considera a distância dos radares até a quadrícula e demais parâmetros geográficos que afetam a qualidade do sinal, em função das feições do relevo e a possibilidade de visada relativamente a cada radar naquela região.

No exemplo da Figura 8, uma aeronave que trafega pela quadrícula Q_n , no instante inicial $t_1 = t$, situação em que pode ser detectada pelos radares A, B, C, D e E. Seguindo sua trajetória, essa mesma aeronave sobrevoa outras quadrículas, onde passa a ser detectada pelos radares A, D, E e F. Posteriormente, no instante $t_2 = t + \Delta t$, a aeronave atinge a quadrícula Q_m , na qual pode ser detectada apenas pelos radares A, E e F.

Assim, observa-se uma situação inicial com cinco componentes da detecção ($C1_n$ a $C5_n$), geradas na quadrícula Q_n . Cada componente da detecção corresponde a uma mensagem-pista, contendo informações de velocidade, posição, altitude, etc., geradas a cada ciclo de rotação dos radares D, A, E, B e C, respectivamente.

Para a quadrícula Q_n , a ordem de prioridades indica que, nessa região, as "mensagens-pista" geradas pelo radar D possuem a maior precisão, enquanto que as mensagens do radar C possuem a menor confiança a ser considerada.

⁴ Cada detecção realizada pelos radares gera informações denominadas "pistas radar", que contêm dados cinemáticos e de identificação referentes ao instante da detecção da aeronave. Cada "mensagem-pista" gerada é encaminhada aos Centros de Controle para processamento e composição de uma síntese da situação aérea, para apresentação aos controladores.

Ao ser atingida a quadrícula Q_m , as três componentes geradas a cada ciclo ($C1_m$ a $C3_m$) correspondem apenas às mensagens com informações obtidas pelos radares F, E e A.

Figura 8 – Processo de detecção de uma aeronave e elaboração da síntese

Nesse contexto, e considerando o assincronismo dos instantes de envio de cada uma das cinco componentes geradas próximas ao instante t_1 , a função de elaboração da síntese consiste em estabelecer uma única posição de visualização para a aeronave.

Esse mesmo processo de síntese é realizado ciclicamente e, após o intervalo Δt , pode ser estabelecida uma nova posição de síntese para a aeronave, a partir das três componentes geradas em torno do instante t_2 .

A vantagem do estabelecimento do tratamento por quadrículas, por exemplo, com dimensão de uma milha náutica⁵ quadrada, é a redução da carga total de processamento do sistema. Assim, em face das grandes velocidades envolvidas na navegação aérea, que podem resultar em deslocamentos de algumas milhas náuticas em poucos ciclos de detecção radar, torna-se conveniente estabelecer parâmetros uniformes (altura máxima do terreno, distância até os radares, etc.) válidos para toda a área de cada quadrícula.

⁵ Cerca de 1,6 Km.

2.4 Considerações Finais deste Capítulo

Este capítulo apresentou uma visão geral sobre a atividade de controle do espaço aéreo, exemplificando algumas funções tipicamente realizadas e serviços prestados pelos Centros de Controle de Tráfego Aéreo (civil), bem como pelos Centros de Operações Militares, responsáveis pelas atividades de defesa aérea e vigilância do espaço aéreo.

A partir dessa visão geral, pode-se verificar a natureza crítica dos sistemas computacionais envolvidos, o que remete à preocupação fundamental do ponto de vista do projeto, para a necessidade de adoção de processos definidos no desenvolvimento e das melhores práticas de engenharia de confiabilidade no ciclo de vida desses sistemas.

3 Confiabilidade e Segurança de Sistemas Computacionais

O intuito deste capítulo é apresentar conceitos gerais sobre a confiabilidade de sistemas computacionais, enfocando os aspectos relevantes das técnicas de modelamento de confiabilidade, disponibilidade e características de testabilidade no projeto de sistemas críticos.

3.1 Confiabilidade de Sistemas Computacionais

Uma premissa de enfoque deste trabalho de pesquisa, decorrente do objetivo exposto no Capítulo 1, é a apresentação de um modelo de análise de disponibilidade aplicável aos sistemas computacionais empregados no controle do espaço aéreo. Por isso, a pesquisa realizada não teve o objetivo de estabelecer a avaliação de nenhuma instalação específica, de algum sistema real existente, nem tampouco se procurou explicitar o desenvolvimento detalhado dos cálculos de confiabilidade para uma arquitetura particular de algum sistema.

Dessa forma, os capítulos subseqüentes apresentam um modelo de avaliação de disponibilidade, com exemplos de aplicação que partem do conhecimento prévio das taxas de falhas, MTBF (*mean time between failures*) teórico e taxas de reparo aplicáveis ao sistema integrado que se deseja avaliar, eventualmente referenciando cálculos apresentados nos Apêndices.

Em decorrência do enfoque mencionado anteriormente, esta seção descreve conceitos básicos sobre a engenharia de confiabilidade de sistemas computacionais, procurando, assim, prover uma revisão útil à compreensão dos capítulos seguintes, e também servir de referência e orientação quanto às técnicas de engenharia e conhecimentos disponíveis para cálculo de confiabilidade de sistemas complexos (SHOOMAN, 2002), incluindo seus aspectos de hardware e software (MUSA *et al*, 1987).

Para isso, são feitas algumas considerações sobre o cálculo de confiabilidade global de um sistema computacional, abordando suas características de redundância e tolerância a falhas, bem como aspectos da confiabilidade de software, sendo referenciadas algumas técnicas de cálculo e normas aplicáveis. São ainda introduzidos os conceitos gerais pertinentes à análise de segurança de sistemas computacionais, apresentando algumas definições sobre risco, classificação de níveis de integridade de segurança e normas aplicáveis aos principais segmentos industriais, inclusive em defesa aérea e aviação.

O objetivo da descrição desses conceitos gerais é indicar como se pode estabelecer teoricamente os principais parâmetros de confiabilidade (MTBF e taxas de falhas) para sistemas complexos, envolvendo os seus diversos aspectos de arquitetura, hardware, software e fatores humanos.

Apresentam-se também os resultados do estudo (JACKSON *et al*, 2005) sobre as aquisições militares no segmento de Defesa, onde se constatou um problema de não-conformidade dos índices observados de confiabilidade em relação aos parâmetros especificados em aquisições de sistemas militares.

3.1.1 Conceitos Fundamentais sobre Confiabilidade e Segurança

Segundo as definições consolidadas na literatura (JOHNSON, 1989), apresentam-se a seguir alguns conceitos fundamentais sobre a confiabilidade de sistemas.

O conceito de confiabilidade (*reliability*) refere-se ao nível de confiança de um sistema permanecer em funcionamento ao longo do tempo. A confiabilidade pode ser definida como a probabilidade condicional de um sistema permanecer em funcionamento correto, durante o intervalo de tempo $[t_0, t]$, dado que funcionava corretamente no instante t_0 . Tal probabilidade é expressa como uma função no tempo: $R(t)$.

Para sistemas eletrônicos, cujas taxas de falhas apresentam valores constantes ao longo da vida útil do sistema, a função densidade de probabilidade de falha é modelada como uma constante e costuma ser representada pela taxa λ . Nesse caso, para sistemas sem reparos, o tempo médio entre falhas (MTBF) equivale ao inverso da taxa de falhas $1/\lambda$, com a função de confiabilidade apresentando decaimento exponencial, $R(t) = e^{-\lambda t}$.

A Figura 9 indica a função de confiabilidade de um sistema eletrônico permanecer em funcionamento em um instante t , dado que funcionava em $t = 0$. No instante $t = 0$ a probabilidade do sistema permanecer em funcionamento é 100%, enquanto que para intervalos de observação muito grandes a probabilidade de encontrar o sistema em funcionamento tende a zero. Neste tipo de distribuição, para $t = 1/\lambda$, ou seja, no instante $t = \text{MTBF}$, a confiabilidade do sistema $R(t) = e^{-1}$, ou cerca de 37%, que representa a probabilidade do sistema encontrar-se funcionando após decorrido um período igual ao tempo médio entre falhas.

Figura 9 – Decaimento exponencial da confiabilidade de sistemas eletrônicos

Esse tipo de análise é de grande valor para sistemas e componentes eletrônicos, no entanto, não se aplica para sistemas que apresentam taxas de falhas variáveis no tempo, como é o caso do software – abordado como exemplo no Apêndice B deste trabalho – cujas falhas resultam de defeitos de projeto, sendo passíveis de detecção e correção durante as fases de teste e ao longo de toda a vida operacional. Por isso, dada a possibilidade de redução das taxas de falhas do software, em decorrência da correção de defeitos de projeto, sua confiabilidade pode crescer com o tempo. Para predição da confiabilidade de software, adotam-se modelos de crescimento de confiabilidade, sendo empregadas funções de taxas de falhas variáveis no tempo, com base em distribuições Weibull ou Log-Poisson, entre outras (MUSA *et al*, 1987).

Analogamente à confiabilidade, o conceito de segurança (*safety*) refere-se à probabilidade de um sistema permanecer em funcionamento seguro, durante um intervalo de tempo, dado que funcionava de forma segura no instante inicial. O que caracteriza o funcionamento inseguro, diz respeito à potencial consequência de uma *falha insegura*, que é definida como uma ocorrência cujos efeitos implicariam risco de exposição do sistema, seus usuários ou o meio-ambiente a perigo de acidente.

A disponibilidade (*availability*) de um sistema refere-se à probabilidade do mesmo encontrar-se disponível em um instante qualquer de observação.

Assim, define-se disponibilidade como a probabilidade de se encontrar o sistema em funcionamento correto, para um dado instante qualquer t . Essa função no tempo é

expressa como $A(t)$. Nesse aspecto destaca-se a diferença entre os dois conceitos, uma vez que a confiabilidade é dependente de um intervalo de tempo, enquanto a disponibilidade é determinada para um dado instante qualquer de observação.

O conceito de manutenibilidade (*maintainability*), às vezes também definido como reparabilidade ou “mantenabilidade”, refere-se à possibilidade do sistema admitir manutenção, ou seja, à capacidade que um sistema apresenta para receber um reparo e retornar à condição operacional, após ter sofrido um evento de falha.

A métrica fundamental associada à manutenibilidade de um sistema é o tempo médio de reparo (MTTR). O *RMA Handbook* (FAA, 2006b) também especifica o conceito de MTTRS (*mean time to restore service*) como métrica para avaliação de sistemas complexos, nos quais se contabiliza, adicionalmente ao MTTR, toda necessidade de tempo requerido para intervenções manuais (procedimentos de instalação, ativações de software, tempos para início de operação de funções essenciais, etc.), que sejam consideradas essenciais para retorno à operação regular de um sistema após um evento não programado de indisponibilidade do serviço.

Considerando essa capacidade de reparo presente na maioria dos sistemas, a disponibilidade caracteriza uma métrica importante para determinar a parcela do tempo em que um sistema encontra-se disponível, em relação ao tempo total de operação.

Costuma-se encontrar diferentes definições para os diversos conceitos relacionados à engenharia de confiabilidade, muitas vezes gerando imprecisão a respeito dos termos: falha, falta, erro, disfunção e defeito. A literatura ainda utiliza esses termos de maneira variada, porém este trabalho procurou seguir a terminologia adotada pelo IEEE, conforme algumas referências específicas da área da confiabilidade de sistemas digitais (JOHNSON, 1989) e de software (MUSA *et al*, 1987).

As falhas (*fault*), derivadas de problemas de projeto ou implementação, caracterizam um estado de defeito interno dos sistemas, não necessariamente manifestado externamente ao usuário. Tais defeitos podem ocasionar erro (*error*), manifestado internamente ao sistema, módulo ou unidade, na forma de valores de variáveis (dados ou parâmetros de controle) diferentes do esperado para um determinado estado conhecido, cuja consequência eventual é a verificação de disfunções ou falhas refletidas externamente ao sistema, na forma de um mal funcionamento, incompatível ao comportamento especificado nos requisitos formais. Essas ocorrências externas são

chamadas falhas (*failures*) do sistema, às vezes sendo também denominadas defeitos, segundo autores (WEBER, 2006) que assim caracterizam o mal funcionamento do sistema, quando manifestado ao universo do usuário.

As falhas manifestadas externamente ao sistema podem eventualmente desencadear eventos inseguros, ou estados perigosos, o que as caracteriza como falhas inseguras (*unsafe failures*).

A Figura 10 apresenta um diagrama representativo das causas de falhas de um sistema computacional, originadas no hardware ou no software, bem como dos efeitos, na forma de erros no universo interno dos dados do sistema, sem manifestação ao usuário, até a ocorrência externa de um defeito, manifestado externamente ao sistema.

Figura 10 – Causas e efeitos das falhas e níveis de tratamento (JOHNSON, 1989)

Nesse diagrama, são também expostas as possíveis barreiras que se podem construir, nas etapas de projeto, visando: a) evitar a ocorrência de falhas (prevenção); ou b) adotar técnicas de mascaramento, para contornar a ocorrência de um erro, evitando que se manifeste externamente; ou ainda c) implementar tolerância a falhas, de modo que mesmo manifestando-se externamente, uma falha não impeça a continuidade do serviço.

Como exemplos de técnicas relacionadas a cada um dos níveis de tratamento de falhas indicados na Figura 10, podem-se citar: a) adoção de processos definidos de qualidade e

métodos formais de projeto (LYU, 1996) como recursos para evitar a ocorrência de falhas; b) no nível de mascaramento de erros, técnicas de codificação para gerar redundância das informações, por exemplo, a paridade de dados, que pode evitar que uma falha, causadora de um erro, chegue a manifestar-se externamente; e c) como técnica de tolerância a falha costuma-se usar redundâncias dos sistemas.

Segundo a padronização específica para as aplicações da área aeronáutica (FAA, 2006b), apresentam-se a seguir algumas definições referentes aos conceitos de disponibilidade e segurança nas aplicações de controle do espaço aéreo, as quais serão úteis para distinção de alguns conceitos de interesse deste trabalho.

As atividades desempenhadas pelos sistemas de controle do espaço aéreo são discriminadas em linhas de serviço específicas (*Service Threads*) correspondendo à cadeia de componentes técnicos ou operacionais, equipamentos ou subsistemas de hardware, software e a ação humana, necessários à prestação do serviço pelo centro de controle. Essas linhas de serviço (STLSC⁶) são classificadas em categorias de severidade de uma eventual perda para a capacidade do espaço aéreo, conforme segue:

- Críticas em segurança (*Safety-critical*): devem operar durante 0.99999 do tempo e correspondem aos serviços cujas indisponibilidades aumentam o risco para um nível inaceitável associado à segurança e eficiência das operações;
- Críticas em eficiência (*Efficient-critical*): devem operar durante 0,999 do tempo e correspondem aos serviços cuja indisponibilidade gera degradação na eficiência global do sistema, reduzindo a capacidade operacional no espaço aéreo, ou gerando atrasos, porém preservando a segurança das operações;
- Essenciais/Rotina (*Essential/Routine*) – devem operar durante 0,99 do tempo e correspondem aos serviços de rotina cuja indisponibilidade gera degradação local na eficiência do sistema, reduzindo a capacidade operacional no centro de controle, porém preservando a segurança das operações.

Como exemplo de técnicas de análise de confiabilidade, o Apêndice A apresenta um resumo da aplicação de modelos combinatórios – série-paralelo – e modelos de Markov na solução de sistemas tolerantes a falhas, a partir do conhecimento da confiabilidade dos componentes.

⁶ *Service Thread Loss Severity Category* (FAA, 2006b).

3.1.2 Engenharia de Confiabilidade de Software (SRE)

Com relação ao software de sistemas críticos, uma definição (HERRMANN, 1999) estabelece que a confiabilidade de software é uma medida de confiança em que um software produza resultados precisos e consistentes, de forma reprodutível, independentemente da carga de uso, dentro do ambiente operacional especificado. A literatura descreve o desenvolvimento de um conjunto de práticas de engenharia de confiabilidade de software – SRE – a partir de um caso de destaque (LYU, 1996) obtido na experiência da empresa AT&T, em que puderam ser organizados seis passos da prática de engenharia da confiabilidade de software, conforme segue:

- a) Quantificar o uso do produto, especificando frequências de uso das diversas facilidades pelos usuários;
- b) Estabelecer uma definição de objetivos da qualidade esperada com os clientes, definindo o que representa falhas e respectivas severidades, além de definir objetivos de confiabilidade;
- c) Empregar o perfil de uso do produto e objetivos de qualidade como guias do desenvolvimento do projeto;
- d) Medir a confiabilidade de software reutilizado ou adquirido de fornecedores, de forma a adotar essa prática como critério de aceitação;
- e) Rastrear a confiabilidade e adotar essa prática como critério de liberação do produto ao cliente;
- f) Monitorar a confiabilidade do sistema em campo, como referência a considerar em eventuais evoluções de produto ou para melhoria do processo de desenvolvimento.

A contribuição principal do caso estudado para software crítico na indústria de telecomunicações é auxiliar a avaliação de benefícios e impactos de custos nas organizações que implantam uma prática de engenharia de confiabilidade de software.

A teoria da engenharia de confiabilidade de software (LYU, 1996) indica que o principal fator de custo na aplicação das melhores práticas de SRE é a obtenção ou levantamento do perfil operacional do produto. O esforço envolvido em SRE pode variar de uma semana a um ano de uma pessoa, porém o esforço médio observado, para um projeto com equipe de 10 pessoas, admitindo o produto da ordem de 100 mil linhas

de código e prazo de 18 meses, seria da ordem de 2 pessoas-mês, ou seja, cerca de 1% do esforço de um projeto de 180 pessoas-mês. Para projetos muito grandes (acima de 1000 pessoas envolvidas) esse esforço em SRE pode ficar abaixo de 1% do custo total da engenharia do desenvolvimento.

A teoria da confiabilidade de software, segundo a mesma referência (LYU, 1996), recomenda abordagem incremental para a implantação de SRE nas organizações. Assim, sugere-se implantar somente as etapas iniciais, referentes à alocação e rastreabilidade da confiabilidade no processo de desenvolvimento, porém com a etapa de monitoração de confiabilidade real dos produtos entregues sendo suprimida nos primeiros projetos, por se tratar de tarefa custosa (MUSA *et al*, 1987), ficando essa etapa para uma implantação posterior, a partir do momento em que houver massa de dados suficiente para efetivar o monitoramento em campo.

A implantação em projetos existentes não diferencia muito da aplicação em projetos iniciais, no entanto poderá ser observada grande redução de esforço ao se replicar o processo para novas instâncias (versões) de produto a partir de um processo estabelecido anteriormente na organização.

A Figura 11, a seguir, ilustra esse processo de implantação das atividades de SRE no ciclo de vida do produto.

Resumidamente, a prática da SRE no ciclo de vida gerencial das atividades de desenvolvimento de software, pode ser descrita da seguinte forma:

- Durante a fase de análises de viabilidade e requisitos, são levantados o perfil funcional e os objetivos da confiabilidade de software, estabelecidos em conjunto com o cliente;
- Durante as fases de projeto e implementação, são estabelecidas as alocações dos objetivos de confiabilidade entre os itens de software e hardware, levando em conta o perfil operacional (uso do sistema) e aspectos dos componentes adquiridos ou reusados;
- Na fase de testes, são refinados os perfis operacional e funcional, sendo estabelecida a data de liberação do produto em função de metas de compromisso entre prazos de entrega e custos totais do SRE;

- Durante as fases de pós-entrega e manutenção, são realizados o registro e monitoração da confiabilidade do sistema em campo, com objetivos vinculados ao planejamento de futuras evoluções funcionais ou de processo de engenharia.

Figura 11 – Atividades de SRE no ciclo de vida do produto de software (LYU, 1996)

Como informação complementar, o Apêndice B apresenta alguns conceitos sobre a modelagem do crescimento de confiabilidade de software (MUSA et al, 1987), com um exemplo de cálculo baseado na utilização da ferramenta CASRE (SHOOMAN, 2002).

3.1.3 Segurança de Sistemas Computacionais Críticos

Podem ser citados, como exemplos importantes de aplicações computacionais críticas, os sistemas de transporte automotivo, metro-ferroviário, naval e de aviação, a indústria aeroespacial e de defesa, os equipamentos e sistemas de saúde, nas áreas hospitalares, médicas ou biomédicas, e a indústria nuclear (LEVESON, 1995).

Na área de defesa, os projetos de engenharia de sistemas, equipamentos e software de emprego militar envolvem uma preocupação inerente com os riscos de manifestação descontrolada do poder destrutivo vinculado a esses sistemas (HERRMANN, 1999). A presença desses riscos fomentou a formação de conhecimentos de engenharia de segurança nos projetos militares, onde puderam ser desenvolvidos métodos formais de definição e validação de requisitos, técnicas de implementação e operação dos sistemas, envolvendo práticas específicas para mitigação dos riscos e controle dos efeitos decorrentes das eventuais falhas. Isso levou ao aprimoramento dos projetos para incorporação das condições de degradação com tolerância a falhas, e de operação segura mesmo em condições de falha (operação “*failsafe*”).

Além do setor de defesa, um contexto análogo é também verificado em diversos outros setores, nos quais algum mal funcionamento tecnológico possui relação direta com a probabilidade de ocorrência de acidentes, implicando na perda de vidas, danos ou prejuízos aos usuários, ao público ou ao meio ambiente.

Em todas essas aplicações críticas, requer-se uma atividade importante da engenharia de projeto, voltada à análise e classificação de riscos envolvidos, ou seja, dos riscos vinculados ao funcionamento dos sistemas e equipamentos em questão, tendo sido, por esse motivo, geradas e aperfeiçoadas diversas normas e recomendações técnicas de padronização dos critérios e mecanismos de segurança adotados internacionalmente.

Na área de defesa, destaca-se o desenvolvimento das normas do Ministério de Defesa Britânico, das séries DEF STAN 00-55 *Safety Related Software* (MOD, 1997) e DEF STAN 00-56 *Safety Management Requirements for Defence Systems* (MOD, 2007), bem como a IEC 61508 *Functional safety of electrical/ electronic/ programmable electronic safety-related systems* (STOREY, 1996), que estabelecem definições de segurança (*safety*) e recomendações gerais para as atividades de análise de risco de sistemas computacionais, ou sistemas com eletrônica programável.

Os fundamentos envolvidos na análise de risco dependem do estabelecimento de uma conceituação básica para os seguintes termos: acidente (*accident / mishap*), risco (*risk*) e perigo (*hazard*), conforme as seguintes definições (STOREY, 1996):

- a) Acidente: é a sequência de eventos, cujos resultados são traduzidos em danos às pessoas, prejuízos às propriedades ou ao meio ambiente;

- b) Risco: é uma combinação da frequência, ou probabilidade, específica da ocorrência de um dado evento perigoso e de suas consequências;
- c) Perigo: é uma exposição à fonte em potencial, sempre existente, que pode induzir à ocorrência de algum acidente.

A análise de risco busca estabelecer as probabilidades de ocorrência destas seqüências que levam aos acidentes. Trata-se, portanto de uma análise quantitativa. De forma sucinta, a análise de risco depende da análise de perigo.

A classificação de risco é um processo qualitativo que leva em consideração o cruzamento das categorias de severidade e da frequência (ou probabilidade) de ocorrência dos eventos perigosos, conforme ilustra a Figura 12.

Figura 12 – Fatores que definem a classificação de riscos

Quatro categorias de severidade foram estabelecidas em função dos danos potencialmente presentes na ocorrência dos eventos, conforme segue (STOREY, 1996):

- Catastrófica: muitas mortes;
- Crítica: uma morte ou sérias lesões;
- Marginal: apenas lesões;
- Negligenciável: escoriações e machucaduras.

Seis categorias de probabilidade ou de frequência esperada dos eventos foram estabelecidas nas normas anteriormente citadas, em função da vida útil do equipamento ou sistema, sendo também indicada uma grandeza para as taxas de ocorrências por tempo de operação (por exemplo: horas de voo), conforme segue (STOREY, 1996):

- Frequente: Ocorrências continuamente esperadas (10^{-2} eventos/hora ou maior);

- Provável: Frequentemente esperadas (10^{-2} a 10^{-4} eventos/hora);
- Ocasional: Muitas ocorrências esperadas (10^{-4} a 10^{-5} eventos/hora);
- Remota: Esperadas algumas ocorrências (10^{-5} a 10^{-7} eventos/hora);
- Improvável: Não esperadas. Ocorrências excepcionais (10^{-7} a 10^{-9} eventos/hora);
- Incrível (extremamente improvável): Não esperadas durante toda a vida operacional (10^{-9} eventos/hora ou menor);

A composição das categorias de severidade com as categorias de frequência resulta na classificação de riscos, conforme indica a Tabela 2, na qual estão apresentadas as terminologias adotadas pelas duas normas IEC 61508 e DEF STAN 00-56 *System Safety Management* (STOREY, 1996). Essa classificação estabelece a definição de quatro níveis de aceitabilidade de riscos, cujo quadro comparativo, para as duas normas citadas, está apresentado pela Tabela 3.

Tabela 2 – Classificação de risco segundo DEF STAN 00-56 e IEC 61508

Frequências	Consequências			
	Catastrófica	Fatal / Crítica	Severa / Marginal	Menor / Negligenciável
Frequente	A / I	A / I	A / I	B / II
Provável	A / I	A / I	B / II	C / III
Ocasional	A / I	B / II	C / III	C / III
Remota	B / II	C / III	C / III	D / IV
Improvável	C / III	C / III	D / IV	D / IV
Incrível	D / IV	D / IV	D / IV	D / IV

Tabela 3 – Aceitabilidade do risco: comparativo de interpretações das normas DEF STAN 00-56 e IEC 61508 (STOREY, 1996)

DEF STAN 00-56		IEC - 61508	
Classes de Risco	Interpretação	Interpretação	Classes de Risco
A	<i>Intolerável.</i>	<i>Risco Intolerável.</i>	I
B	<i>Não desejável. Aceitável apenas se a redução de risco for impraticável.</i>	<i>Risco não desejável. Aceitável apenas se a redução de risco for impraticável ou o custo for brutalmente desproporcional ao ganho obtido.</i>	II
C	<i>Tolerável apenas com o aval do Comitê de Revisão de Segurança do Projeto.</i>	<i>Tolerável se o custo da redução exceder o ganho obtido.</i>	III
D	<i>Tolerável com o aval das Revisões Normais de Projeto.</i>	<i>Risco negligenciável.</i>	IV

Para o caso específico do software, a classificação de riscos estabelecida pela norma MIL-STD-882 (DoD, 1998) (HERRMANN, 1999) leva em conta um conjunto de seis categorias, incluindo as classes I a IV mencionadas anteriormente, e adicionando um detalhamento intermediário para os níveis IIa, IIb, IIIa e IIIb, em função do nível de controle exercido pelo software sobre hardware potencialmente perigoso:

- I - O software controla autonomamente sistemas ou componentes de hardware potencialmente perigosos;*
- IIa - O software exerce controle sobre hardware perigoso, porém com tempo para intervenção de sistemas de segurança redundantes e independentes;*
- IIb - O software gera informação que requer ação imediata do operador para mitigar o perigo. Falhas do software dificultariam a prevenção ou permitiriam a ocorrência do evento perigoso;*
- IIIa - O software comanda hardware potencialmente perigoso, porém a ação humana completa a função de controle (há medidas de segurança independentes e redundantes para cada evento de perigo);*
- IIIb - O software gera informação de natureza crítica, utilizada para tomada de decisão crítica (há medidas de segurança independentes e redundantes para cada evento de perigo);*
- IV - O software não controla sistemas/hardware críticos e não provê informação de segurança crítica.*

A partir das análises de risco mencionadas anteriormente, pode-se estabelecer o nível de integridade de segurança para um sistema, ou *safety integrity level* (SIL), o qual se define como a probabilidade de um sistema desempenhar a segurança requerida, segundo as condições estabelecidas, dentro de um dado intervalo de tempo.

Os níveis de integridade SIL 4 (muito alto) e 3 (alto) indicam sistemas implementados com maior rigor nas atividades e técnicas de verificação e medição de segurança, enquanto os níveis 2 (médio) e 1 (baixo) indicam sistemas implementados com menor rigor nas atividades de segurança. O nível SIL 0 indica sistemas não relacionados a requisitos de segurança. As faixas de ocorrências de falhas inseguras, que correspondem a cada nível de integridade, são estabelecidas pela norma DEF STAN 00-55 (MOD, 1997) (HERRMANN, 1999), conforme ilustra a Tabela 4.

Tabela 4 – Níveis de Integridade de Segurança (SIL) (HERRMANN, 1999)

SIL	Taxas de falhas inseguras por ano (λ_u) (ou por solicitação)
4	Melhor que 10^{-4} , até 10^{-5} ($10^{-4} > \lambda_u \geq 10^{-5}$)
3	Melhor que 10^{-3} , até 10^{-4} ($10^{-3} > \lambda_u \geq 10^{-4}$)
2	Melhor que 10^{-2} , até 10^{-3} ($10^{-2} > \lambda_u \geq 10^{-3}$)
1	Melhor que 10^{-1} , até 10^{-2} ($10^{-1} > \lambda_u \geq 10^{-2}$)
0	Igual ou pior que 10^{-1} ($\lambda_u \geq 10^{-1}$)

Assim como as demais aplicações críticas citadas anteriormente, nos setores de transportes, indústria aeroespacial, os sistemas médicos e a indústria nuclear, os sistemas de apoio ao controle do espaço aéreo demandam atenção em diversos fatores que afetam a confiabilidade e segurança final dos sistemas.

Dessa forma, podem ser destacados os seguintes fatores principais envolvidos na análise de segurança: processo de engenharia de projeto e implementação; definição das arquiteturas de hardware e software do sistema; tratamento de incertezas dos dados sensorizados (NEAPOLITAN, 2004); uso de produtos COTS em módulos de software crítico; interfaces de operação; e fatores humanos DEF STAN 00-25 (MOD, 2004).

3.1.4 Confiabilidade no Segmento de Sistemas de Defesa

No âmbito internacional, os segmentos da indústria de desenvolvimento dos sistemas espaciais, aeronáuticos e dos sistemas de controle do espaço aéreo tiveram origem e permanecem atrelados à indústria de defesa, sendo por esse motivo alvo de políticas de incentivo local ou mesmo de medidas protecionistas (FLORES, 2002), voltadas ao desenvolvimento e geração de autonomia tecnológica nesses setores críticos, por serem considerados política e economicamente estratégicos.

Esses segmentos industriais críticos, vinculados ao desenvolvimento tecnológico da área de defesa, possuem uma longa história de aplicações da engenharia de confiabilidade e segurança (HERRMANN, 1999). Após a Segunda Grande Guerra, um rápido crescimento do segmento de defesa ocorreu devido à introdução de novas tecnologias nos sistemas de armas existentes, com destaque para o aprimoramento das aeronaves e o desenvolvimento de novas classes de sistemas associados às armas nucleares, mísseis balísticos, veículos pilotados remotamente, armas guiadas a laser, sistemas de navegação avançados, sistemas de comunicação por satélite, entre outros. A partir desse aumento de complexidade operacional e funcional, as concepções dos sistemas de controle de operações aéreas passaram a se tornar fortemente dependentes (TRIBBLE; MILLER, 2004) dos sistemas computacionais e, conseqüentemente, do software.

Justamente pelo poder destrutivo inerente dos sistemas de defesa, a operação confiável e segura é uma preocupação primária de projeto. Por esses motivos, o setor de defesa foi um dos primeiros segmentos industriais a desenvolver processos de engenharia da confiabilidade e segurança de sistemas que, mais recentemente, incluíram também os conceitos de confiabilidade e segurança de software (*software safety*), os quais hoje são largamente empregados na indústria de sistemas aeronáuticos (sistemas embarcados), sendo também importante ao desenvolvimento e operação dos sistemas de controle do espaço aéreo.

Um trabalho publicado pelo DoD - Departamento de Defesa dos EUA (JACKSON *et al*, 2005), no qual foram compilados resultados de estudos efetuados no final das décadas de 1980 e 1990, constatou que apesar da evolução tecnológica e do incremento das características de confiabilidade de componentes básicos - por exemplo, no segmento de microeletrônica - os mesmos graus de evolução não haviam sido observados na

confiabilidade conjunta dos equipamentos ou dos sistemas integrados, adquiridos na indústria de defesa.

Conforme foi apresentado anteriormente, na motivação deste trabalho, a Figura 13 reproduz o resultado detalhado da publicação do DoD (DoD, 2005), na qual se observou crescimento na parcela dos sistemas militares adquiridos que não demonstraram, durante testes operacionais, a confiabilidade especificada nas fases de aquisição. No período de 1985 a 1990, de um conjunto de 34 aquisições analisadas, 20 projetos (ou cerca de 59%) não apresentaram a confiabilidade especificada. Posteriormente, no período de 1996 e 2000, um segundo conjunto mais amplo de projetos foi analisado, indicando que apenas 20% dos sistemas adquiridos demonstraram confiabilidade igual ou superior à especificada originalmente na aquisição.

Figura 13 – Crescimento da parcela dos sistemas militares que não demonstram a confiabilidade especificada (DoD, 2005)

A despeito de várias técnicas aplicáveis estarem disponíveis para uso na implementação e avaliação dos requisitos de confiabilidade nos sistemas de defesa, esses estudos verificaram que tais técnicas não estavam sendo adequadamente empregadas durante as aquisições desses sistemas. As causas sugeridas pelo DoD para o agravamento do quadro verificado no segundo período analisado são, basicamente, as seguintes: a) as análises de requisitos dos sistemas de defesa tendem a focar aspectos técnicos funcionais e de performance, com menor atenção às questões dos custos operacionais e de suporte, em especial nos estágios iniciais de especificação; b) a utilização de

tecnologias de ponta (imaturas), no intuito de atingir as metas de performance técnica, enfraquecem a habilidade para projetar sistemas robustos e de alta confiabilidade; c) a integração e a colaboração entre as organizações envolvidas mostraram-se limitadas, sendo que várias organizações distintas ficam encarregadas, isoladamente, por diferentes etapas de definições de requisitos, desenvolvimento, implementação e manutenção dos sistemas.

Uma conclusão importante desses estudos foi o reconhecimento da necessidade de comunicar melhor, à comunidade DoD, as técnicas desenvolvidas nos últimos vinte anos. Tais técnicas mostraram-se adequadas para a avaliação de confiabilidade de sistemas de defesa, porém geralmente não têm sido consideradas, em toda sua abrangência, nas aquisições de sistemas de defesa. Uma recomendação importante foi a atualização ou substituição da norma DoD 3235.1-H - *Test and Evaluation of System Reliability Availability and Maintainability: a Primer* (DoD, 1982), conhecida como *RAM Primer*, por publicação que venha a prover cobertura mais adequada às necessidades atuais dos projetos militares.

Nesse contexto, tem sido privilegiado também o uso de componentes ou módulos disponíveis comercialmente no mercado - produtos COTS - em função das demandas pelo incremento de produtividade nos projetos, dado que a complexidade crescente dos sistemas, em termos funcionais e tecnológicos, acaba por somar-se às pressões para redução orçamentária e de prazos, exigindo rápida disponibilização de funções complexas a custo reduzido (YE; KELLY, 2004). Isso acaba gerando a adoção de soluções comercialmente consagradas, uma vez que, em princípio, sua escala de utilização favorece as condições para redução de custos, associada à confiabilidade e robustez de uma ampla base instalada.

Por isso, a Organização do Tratado do Atlântico Norte – OTAN – gerou um conjunto de recomendações específicas (NATO, 1996) para disciplinar o uso de software COTS nos projetos militares.

3.2 Testabilidade de Sistemas Computacionais

Esta seção descreve alguns conceitos básicos de testabilidade de sistemas computacionais, uma vez que a realização de testes formais é fator fundamental de garantia da qualidade e confiabilidade do produto entregue, de modo a assegurar o

recebimento de um sistema em conformidade aos requisitos do projeto, estabelecidos nas fases de aquisição.

A validação funcional de um sistema (SHOOMAN, 2002) constitui um processo de natureza complexa, realizado no interesse de assegurar que as características esperadas de um projeto venham a ser reproduzidas de modo confiável na vida operacional do produto entregue.

O processo depende da metodologia de desenvolvimento adotada. Por exemplo, quando se considera uma abordagem para projeto de sistema computacional, segundo o modelo *waterfall*⁷ e desenvolvimento de software estruturado, o processo de validação e teste ocorre como ilustra o diagrama da Figura 14.

Figura 14 – Exemplo de Modelo de Desenvolvimento de Software (*Waterfall*)

No modelo ilustrado anteriormente, o primeiro estágio de teste corresponde à execução de testes de módulo ou testes de unidade, com objetivo de assegurar que cada unidade apresente funcionamento correto, quando em operação isolada.

⁷ Processo de desenvolvimento em cascata, no qual as etapas do projeto se sucedem de forma linear, cada uma gerando insumos à etapa imediatamente subsequente.

O segundo estágio corresponde aos testes de integração, nos quais são executados testes da operação de cada módulo implementado, verificando se o mesmo funciona corretamente dentro do ambiente real de interfaces em que irá operar. Geralmente os testes de integração são concebidos com base nas especificações teóricas de cada módulo, a partir do exame do código desenvolvido e dos requisitos daquele módulo específico. Por isso, tais testes costumam ser chamados de testes caixa branca.

O próximo estágio corresponde aos testes de sistema, para validação final do produto liberado, considerando os requisitos de alto nível, visando aceitação interna (do fornecedor) antes da liberação do sistema para a aceitação junto ao cliente. Como esses testes de sistema são escritos com base nos requisitos e especificações gerados nas fases iniciais do projeto, costumam receber a denominação de testes caixa preta.

O último estágio de teste corresponde à aceitação pelo cliente, que costuma incluir testes em fábrica, mais voltados à verificação lógica do sistema, e testes de aceitação em campo, para verificação do comportamento do sistema no ambiente definitivo de operação real em campo, nos quais podem ser validadas as características esperadas contratualmente para o sistema.

Como exemplo de processo formal pode-se citar a norma IEEE-829 (IEEE, 1998), que descreve um conjunto de documentos para as atividades de teste de um produto de software, separando as atividades de teste em três etapas: preparação do teste (planejamento e elaboração de casos e procedimentos), execução do teste (diário de execução dos procedimentos) e registro do teste (emissão de relatórios de resultados e itens de ação a tratar derivados dos testes).

3.3 Considerações Finais deste Capítulo

Este capítulo apresentou uma revisão de conceitos gerais sobre a confiabilidade de sistemas computacionais, de modo a favorecer a compreensão do modelo proposto a seguir, referente à análise de disponibilidade em centros computacionais críticos no Controle do Espaço Aéreo.

4 Modelos de Filas na Avaliação de Disponibilidade

Este capítulo introduz o conceito básico para aplicação de uma rede de filas na avaliação de disponibilidade de sistemas computacionais genéricos. Inicialmente, são apresentados conceitos gerais sobre a teoria de filas. Em seguida, destaca-se um exemplo de avaliação de disponibilidade de data centers a partir de modelos analíticos da teoria de filas.

4.1 Teoria de Filas

Esta seção descreve alguns conceitos básicos da teoria de filas, úteis à compreensão dos modelos apresentados nos Capítulos seguintes. A análise de desempenho de sistemas por meio de modelos de redes de filas é especialmente útil às questões de dimensionamento operacional na prestação de diferentes tipos de serviços. Por exemplo, pode-se citar uma aplicação estudada sobre o dimensionamento de equipes de projeto de software (ANTONIOL *et al*, 2004). No caso de interesse desta pesquisa, realizou-se uma investigação sobre a disponibilidade de sistemas críticos de controle do espaço aéreo com vistas ao dimensionamento de equipes de operação (controladores de tráfego aéreo ou de operações militares de defesa aérea) e equipes de manutenção de hardware e software, nas aplicações desses centros computacionais (PIZZO; CUGNASCA, 2006).

Para isso, resumem-se a seguir algumas considerações sobre modelos de redes de filas, com introdução de conceitos básicos pertinentes às análises de sistemas de fila, cujos desenvolvimentos mais detalhados podem ser obtidos nas referências (JAIN, 1991) e (MENASCÉ *et al*, 2004).

4.1.1 Conceitos Fundamentais sobre Redes de Filas

Segundo as definições para um sistema de fila (RUGGIERO, 1997), o processo de chegada, no qual os usuários se apresentam nos instantes $t_1, t_2, \dots, t_n$, as variáveis aleatórias $\tau = t_j - t_{j-1}$ são chamadas de intervalos entre chegadas. O processo mais comum de chegada é o processo de Poisson, caso em que os intervalos entre chegadas são distribuídos exponencialmente (IID - independentes e identicamente distribuídos).

O tempo que cada usuário de um sistema de fila passa em serviço define seu tempo de serviço. Também nesse caso é usual considerar que esses tempos são variáveis aleatórias (IID) com distribuição exponencial.

O número de servidores (m) define o número de estações de serviço disponíveis no sistema de fila, sendo a capacidade o número máximo de usuários que o sistema de fila pode apresentar, considerando tanto aqueles que estão em espera, na fila, quanto os que estão sendo atendidos nos servidores associados à fila.

A seguir são definidas algumas variáveis de um sistema de fila, conforme ilustra a Figura 15:

- τ – intervalo entre chegadas sucessivas;
- λ – taxa média de chegadas;
- s – tempo médio de serviço de um usuário;
- μ – taxa média de serviço por servidor, sendo a taxa total de serviço igual a $m\mu$.
- n - número de usuários no sistema (tamanho da fila), incluindo os que estão em serviço;
- nq – número de usuários na fila, sempre menor que n , pois não inclui os usuários em serviço, limitando-se apenas aos que estão esperando para receber serviço;
- ns - número de usuários em serviço ($n = nq + ns$);
- w – tempo médio de espera na fila.
- r – tempo médio de resposta: soma dos tempos de serviço e de espera ($r = s + w$);

Figura 15 – Variáveis associadas a um sistema de filas (JAIN, 1991)

4.1.2 Leis Operacionais dos Sistemas de Filas

Define-se uma rede de filas como um conjunto de sistemas de filas interconectados, onde um usuário necessita de serviços em um ou mais nós da rede. Após terminar um

serviço na estação i , o usuário procura serviço em uma outra estação ou abandona a rede, caso seu serviço total esteja completado.

Para uma rede de filas, com K elementos (ou estações), algumas grandezas básicas listadas a seguir podem ser diretamente mensuráveis:

- T – tempo de observação;
- A_i – número total de chegadas no elemento i , observadas no período T ;
- A_0 – número total de chegadas no sistema no intervalo de observação;
- B_i – tempo total de ocupação da estação i no período T ;
- C_i – número de partidas na estação i no período T ;
- C_0 – número total de partidas do sistema no intervalo de observação.

Dessas quantidades mensuráveis, podem ser obtidas as seguintes *variáveis operacionais*:

- λ_i – taxa média de chegadas na estação i ($\lambda_i = A_i / T$);
- U_i – utilização, ou fator de utilização, da estação i , onde $U_i = B_i / T$;
- S_i – tempo médio de serviço na estação i , onde $S_i = B_i / C_i$;
- X_i – vazão (*throughput*) na estação i no período T , onde $X_i = C_i / T$;
- X_0 – vazão (*throughput*) total da rede no período T , onde $X_0 = C_0 / T$;
- V_i – número de visitas à estação i , por chegada na rede, onde $V_i = C_i / C_0$.

Derivadas das relações existentes entre essas variáveis operacionais, podem ser descritas as chamadas Leis Operacionais de Redes de Filas (RUGGIERO, 1997), conforme segue:

- Lei da Utilização: que estabelece a utilização $U_i = S_i * X_i$;
- Lei do Fluxo: que correlaciona a vazão global do sistema com as vazões das estações, em função do número de visitas em cada estação, onde $X_i = V_i * X_0$. Para uma rede aberta, o número de partidas da rede estabelece a vazão, enquanto que, para uma rede fechada, a taxa com que se circula na rede define sua vazão;

- Lei de Little: que estabelece que o número de usuários em cada estação é igual à vazão da estação multiplicada pelo tempo gasto naquela estação $N_i = X_i * R_i$. O mesmo é válido para o sistema como um todo, onde $N_0 = X_0 * R_0$;
- Lei do Tempo de Resposta: estabelece que para todo sistema com fluxo balanceado, vale a relação $Q = X_0 * R$;
- Lei do Tempo de Resposta Interativo: para um sistema interativo, o tempo que o usuário gasta pensando antes de fornecer uma nova requisição para o sistema é Z . Se o tempo de resposta do sistema é R , então o tempo do ciclo completo é $(R + Z)$. Como cada usuário produz $T/(R+Z)$ requisições no intervalo T , então um sistema com N usuários a vazão será dada por: $X = N / (R + Z)$, ou $R = (N/X) - Z$.

4.1.3 Análise de Valor Médio (AVM)

Um recurso importante para resolução de modelos de redes de filas é a análise de valor médio ou AVM (MENASCÉ *et al*, 2004). Esse método permite obter a solução para uma rede de filas com N usuários e K estações servidoras, por meio de um processo interativo, de forma a estabelecer os parâmetros de desempenho dessa rede.

Para sistemas de filas de classe única - ou seja, filas em que as estações servidoras e as demandas são idênticas para todos os usuários - o algoritmo de solução por AVM está apresentado na Tabela 5, a seguir.

O tempo médio de serviço para um usuário na estação i é S_i . O número médio de visitas que um usuário faz à estação i é V_i e, portanto, $D_i = S_i.V_i$, representa a demanda média colocada sobre a estação i . Assim, para todas as n populações de usuários ($N \geq n \geq 1$), o algoritmo permite obter os seguintes parâmetros de desempenho: o tempo médio de resposta em cada estação, o tempo de resposta e a vazão total do sistema, as vazões individuais em cada estação, suas respectivas utilizações e os números médios de usuários em cada estação.

Tabela 5 – Algoritmo para análise de valor médio – AVM (MENASCÉ *et al*, 2004).

<p>Inicie o número médio de usuários em cada estação i:</p> $n_i(0) = 0$
<p>Para cada população de usuários: $n = 1, 2, \dots, N$,</p> <ul style="list-style-type: none"> - calcule o tempo médio de resposta para cada estação i: $R'_i(n) = V_i S_i [1 + n_i(n-1)] = D_i [1 + n_i(n-1)]$ - calcule o tempo total de resposta do sistema: $R_0(n) = \sum_{i=1}^K [V_i \cdot R_i(n)] = \sum_{i=1}^K R'_i(n)$ - calcule a vazão (<i>throughput</i>) total do sistema: $X_0(n) = n/R_0(n)$ - calcule a vazão para cada dispositivo i: $X_i(n) = V_i \cdot X_0(n)$ - calcule a utilização para cada dispositivo i: $U_i(n) = S_i \cdot X_i(n)$ - calcule o número médio de usuários para cada dispositivo i: $n_i(n) = X_0(n) \cdot R'_i(n)$

4.2 Modelamento da Disponibilidade por meio da Teoria de Filas

A seguir, apresenta-se de forma resumida a abordagem de modelamento da disponibilidade na operação de um *data center*, conforme ilustra um estudo de caso (MENASCÉ *et al*, 2004), no qual os autores propõem uma utilização de modelos de filas para dimensionamento operacional e estabelecimento de parâmetros de disponibilidade de um centro computacional genérico.

4.2.1 Modelo Básico de Operação e Manutenção em um Data Center

Na abordagem apresentada pelos autores do estudo de caso citado (MENASCÉ *et al*, 2004), propõe-se a adoção do seguinte modelo: um *data center* hipotético opera com M máquinas e uma equipe de N pessoas dedicadas ao atendimento das ocorrências e manutenção, efetuando os reparos dos equipamentos que entram em falha. Admite-se que um processo ou sistema de diagnóstico seja utilizado para desempenhar as seguintes funções:

- Detectar falhas em qualquer uma das M máquinas;
- Manter uma fila de máquinas aguardando por reparo;
- Registrar o instante em que uma máquina falhou;
- Registrar os instantes em que um técnico inicia e termina o reparo de cada máquina.

Nesse tipo de configuração de centros computacionais, interessa ao gerenciamento manter elevados índices de disponibilidade, por meio da manutenção de alta confiabilidade (reduzidas taxas de falhas), bem como otimizar o processo de manutenção das máquinas, com sistemas de diagnóstico automático, equipes especializadas e processos bem definidos de identificação das falhas, execução eficiente dos reparos e retorno à operação, quando do término do atendimento aos equipamentos submetidos à manutenção.

O problema fundamental da gestão de um centro desse tipo é o dimensionamento necessário à operação, ou seja, estabelecer o número de máquinas necessário para garantir certa confiança na operação, dentro da faixa nominal de oferta dos serviços, e até um limite mínimo estabelecido contratualmente para o caso degradado. Esses parâmetros estão relacionados ao número de pessoas envolvidas na manutenção (tamanho da equipe) e ao nível de habilidade ou conhecimento dessa equipe. Esses parâmetros refletem-se no tempo médio de reparo das máquinas (MTTR), de modo a garantir o grau desejável de disponibilidade.

Algumas considerações são feitas sobre o processo de operação desse centro, conforme ilustra a Figura 16:

- a) Todas as máquinas são idênticas, operando em rede e acessando sistemas de arquivos comuns, também disponibilizados em rede, de modo que todas as

máquinas apresentam taxas de falhas idênticas λ , sendo $\lambda = 1/\text{MTTF}$ (tempo médio entre falhas);

- b) Cada uma das M máquinas apresenta apenas dois estados possíveis (“em operação” ou “em falha”);
- c) Um mecanismo de diagnóstico executa verificações periódicas em todas as máquinas em operação e, uma vez verificada uma anomalia, sinaliza automaticamente à equipe de manutenção, indicando que aquela máquina deve entrar em uma fila para aguardar reparo;
- d) Uma vez na fila, a máquina aguarda por um dos N integrantes da equipe de reparo;
- e) Uma vez reparada, a máquina retorna imediatamente ao “*pool*” de máquinas operacionais.

Figura 16 – Modelo de filas da disponibilidade de um centro computacional
(MENASCÉ *et al*, 2004)

Conforme exemplos mencionados no mesmo estudo de caso, ao gerenciamento desse tipo de centro interessa resolver os seguintes problemas:

- Questão 1: Dados a taxa λ com que as máquinas falham, o número M de máquinas, o número N de pessoas na equipe de reparo e o tempo médio de reparo MTTR , qual é a probabilidade de que *exatamente* j máquinas estejam operacionais?

- Questão 2: Dados os mesmos parâmetros anteriores, qual é a probabilidade de que *pelo menos* j máquinas estejam operacionais?
- Questão 3: Dados a taxa de falhas λ , o número M de máquinas e a taxa de reparo μ ($\mu = 1/\text{MTTR}$), qual é o tamanho N da equipe de reparo necessário para garantir que *pelo menos* j máquinas estejam operacionais com uma certa probabilidade?

No caso citado, admite-se que as falhas de todas as máquinas ocorram independentemente, com a mesma taxa de falhas λ . Considera-se também que a taxa de reparos μ , equivalente ao inverso do tempo médio de reparo ($1/\text{MTTR}$), seja idêntica para todos os tipos de reparo e independente do técnico que executa o serviço.

Caso sejam observadas diferentes taxas de falhas para cada máquina ou subconjunto relevante de máquinas e funções, um modelo de filas mais complexo poderia ser elaborado, considerando múltiplas classes de demandas de serviços. Caso haja necessidade de diferenciar os tempos de reparo para cada técnico, um modelo de múltiplos servidores poderia ser elaborado, para representar cada taxa de reparo individual.

4.2.2 Solução do Modelo de Rede de Filas

Conforme ilustra o caso citado (MENASCÉ *et al*, 2004), a solução para a rede fechada com duas filas, apresentada na Figura 17, pode ser modelada por meio de uma cadeia de Markov (SHOOMAN 2002), na qual cada estado corresponde à situação na qual existem k máquinas em falha, de um total de M máquinas, e com um máximo de N máquinas em manutenção.

Figura 17 – Modelo de Markov para um *data center* com M máquinas (MENASCÉ *et al*, 2004)

A transição do estado k para o estado $k+1$ ocorre quando uma máquina falha, evento que ocorre na taxa λ , multiplicada pelo número de máquinas em operação $M-k$. Do mesmo modo, uma transição do estado k para o estado $k-1$ é realizada sempre que uma máquina é reparada, processo esse que ocorre a uma taxa de reparos μ , multiplicada pelo número de máquinas sendo reparadas k , porém limitada a um máximo de $N \cdot \mu$, uma vez que o número máximo de máquinas em manutenção é igual ao tamanho N da equipe de técnicos de manutenção.

Sendo os eventos de falha independentes, a taxa de falhas agregada é $M \cdot \lambda$, quando as M máquinas estão operacionais. Essa taxa decresce até λ , quando restar apenas 1 máquina em operação. Dessa forma, no estado k , tem-se a seguinte taxa de falhas:

$$\lambda_k = (M-K) \cdot \lambda, \text{ para } K = 0, 1, 2, \dots, M-1 \quad (1)$$

A taxa agregada de reparo pode ser expressa como segue, uma vez que é dependente do número total de técnicos disponíveis, cuja limitação máxima é de N técnicos:

$$\begin{aligned} \mu_k &= K\mu, \text{ enquanto há técnico disponível, quando } K = 0, 1, 2, \dots, N \\ \text{ou,} \\ \mu_k &= N\mu, \text{ quando todos os técnicos ficam ocupados, para } k = N+1, \dots, M \end{aligned} \quad (2)$$

A solução desse modelo é feita a partir do teorema geral dos processos de nascimento e morte – conforme Anexo A: GBD (MENASCÉ *et al*, 2004) – resultando no estabelecimento, em regime, da seguinte probabilidade P_k do sistema encontrar-se no estado k , o que equivale à probabilidade de encontrar-se k máquinas em falha:

$$P_K = P_0 \cdot \prod_{i=0}^{K-1} \lambda_i / \mu_{i+1}, \quad \text{para } K = 0, 1, 2, 3, \dots \quad (3)$$

O que resulta em:

$$\begin{aligned} p_k &= p_0 \cdot [M\lambda/\mu \cdot (M-1)\lambda/2\mu \cdot (M-2)\lambda/3\mu \dots (M-k+1)\lambda/k\mu], \text{ para } k = 1, 2, \dots, N \\ \text{ou,} \\ p_k &= p_0 \cdot [M\lambda/\mu \cdot (M-1)\lambda/2\mu \dots (M-N+1)\lambda/N\mu] \cdot \\ &\quad [(M-N)\lambda/N\mu \cdot (M-N-1)\lambda/N\mu \dots (M-k+1)\lambda/N\mu], \text{ para } k = N+1, \dots, M \end{aligned} \quad (4)$$

Considerando que a soma das probabilidades do sistema encontrar-se em algum dos estados é igual a 1 (com $k = 0$ até $k=M$ máquinas em falha), então:

$$\sum_{k=0}^M p_k = 1 \quad (5)$$

Logo, pode-se obter o valor de p_0 a partir dos parâmetros conhecidos do modelo, como segue:

$$p_0 = 1 / \left[\sum_{k=0}^N \left(\frac{\lambda}{\mu} \right)^k \cdot \binom{M}{k} + \sum_{k=N+1}^M \left(\frac{\lambda}{\mu} \right)^k \cdot \binom{M}{k} \cdot \frac{N^{N-k} \cdot k!}{N!} \right] \quad (6)$$

Uma vez estabelecido o valor de p_0 , na Equação 6, pode-se calcular qualquer valor p_k , por meio da Equação 4. Dessa forma, essa solução formal permite a realização de um processo iterativo de cálculo, por exemplo, com o uso de uma planilha, na qual são obtidas todas as probabilidades p_k .

4.2.3 Exemplo de Cálculo do Modelo de Rede de Filas

Conhecidos os parâmetros básicos de confiabilidade de um sistema, que podem ser obtidos por levantamentos teóricos ou coleta de dados em campo, as três questões mencionadas no item 4.2.1 podem ser resolvidas a partir do uso do modelo descrito em 4.2.2. Por exemplo, no estudo de caso citado (MENASCÉ *et al*, 2004) foi considerado um *data center* com 120 máquinas ($M=120$), com tempo médio entre falhas de 500 minutos ($MTTF=500$ minutos, ou seja: $\lambda=0,002$ falhas por minuto) e o tempo médio de reparo de 20 minutos ($MTTR=20$ minutos, ou $\mu=0,05$ reparos por minuto), de forma que se pode obter a solução da rede de filas, respondendo a *Questão 1*, mencionada anteriormente, como segue:

Solução da Questão 1: Para conhecer a probabilidade de que *exatamente* j máquinas estejam operacionais, calculam-se os valores p_k por meio da Equação (4), resultando no exemplo gráfico ilustrado na Figura 18.

Uma vez que na Figura 18 estão plotadas as probabilidades individuais p_k , correspondentes a cada situação em que *exatamente* j máquinas estejam em operação, destaca-se que o somatório de todas as probabilidades individuais é sempre igual a 1, pois o sistema tem, necessariamente, um número entre 0 e 120 posições operacionais em um dado momento. Pode-se observar a formação de picos em torno da probabilidade de se encontrar um determinado número específico de posições em operação, para cada uma das três situações exemplificadas, para $N = 2, 5$ ou 10 técnicos de manutenção.

Nesse caso, observa-se o seguinte:

- Para $N = 2$, P_j é desprezível para $j < 34$ ou $j > 67$ e o pico ocorre em 50 máquinas, com $P_{50} = 5,6\%$;
- Para $N = 5$, P_j relevantes se concentram entre 92 e 120, com pico em 116 máquinas, com $P_{116} = 10\%$;
- Para $N = 10$, P_j relevantes se concentram entre 108 e 120, com pico em 116 máquinas, com $P_{116} = 19\%$.

Figura 18 – Probabilidades (P_j) de encontrar exatamente j máquinas em operação
(MENASCÉ *et al*, 2004)

Mais adiante neste trabalho, ilustra-se também o exemplo de uma situação cumulativa, referente à probabilidade de se encontrar *pelo menos* j máquinas em operação, o que equivale a somar as probabilidades individuais de se encontrar desde j até 120 máquinas em operação, que é o caso de interesse para responder à *Questão 2*.

4.3 Considerações Finais deste Capítulo

Este capítulo apresentou uma revisão de conceitos gerais sobre a teoria de filas, ilustrando ainda a aplicação de uma rede de filas na avaliação de disponibilidade de um centro computacional genérico. Procurou-se, dessa forma, favorecer a compreensão do modelo estendido, proposto a seguir no Capítulo 5, referente à análise de disponibilidade para centros computacionais mais específicos, utilizados nos sistemas de controle do espaço aéreo.

5 Avaliação de Disponibilidade de Sistemas de Controle do Espaço Aéreo

A partir do conceito geral para aplicação de uma rede de filas na avaliação de disponibilidade de sistemas computacionais – conforme o exemplo apresentado no Capítulo 4 – este capítulo apresenta o foco principal deste trabalho de pesquisa, descrevendo um modelo estendido de rede de filas, visando aplicação mais específica à avaliação de disponibilidade de sistemas computacionais dos centros de controle do espaço aéreo.

Este capítulo apresenta um modelo para análise da disponibilidade de sistemas computacionais em centros de controle do espaço aéreo, nos quais são realizadas atividades de controle do tráfego aéreo civil ou das operações aéreas militares, com interesse direto para questões de gerenciamento, dimensionamento de recursos e planejamento da manutenção operacional desses centros.

O capítulo anterior apresentou uma abordagem geral, baseada na modelagem da operação e manutenção de um centro computacional genérico (*data center*), a partir de um sistema de filas fechado. Os conceitos e métodos analíticos descritos auxiliam a solucionar problemas normalmente endereçados à gestão e dimensionamento de recursos utilizados nesses tipos de *data centers*, os quais se caracterizam pelo uso intensivo de processamento de informações, com funcionamento autônomo – ou seja, não assistido por operadores – e que costumam atender a uma ampla variedade de serviços, tais como: servidores de aplicações transacionais, em comércio eletrônico ou automação bancária; e centros de controle automatizado de processos, nos quais se realiza o controle de malha fechada integralmente efetuado pelo computador, como ocorre em alguns sistemas industriais ou nos sistemas de controle metro-ferroviários.

A partir desse conceito geral, neste capítulo são feitas considerações adicionais sobre as características operacionais encontradas nos centros de controle do espaço aéreo, com o objetivo de estender o modelo geral e torná-lo mais adequado para os casos de interesse deste trabalho. Isso porque, nos processos aeronáuticos em questão, o controle das operações não é integralmente fechado pelos sistemas computacionais (intensivo em processamento), sendo dependente de intervenções efetuadas por operadores humanos.

Nesse aspecto, destaca-se que o modelo passe a considerar a existência de estados de operação não completamente automatizada, seja pela necessidade inerente de algum

tipo de ação humana, por questões de confiabilidade ou de segurança, seja pela existência de falhas ou outras condições de operação degradada, ou ainda pela definição de diferentes classes de máquinas e demandas de serviço.

Com base no modelo apresentado, o próximo capítulo ilustra alguns casos de avaliação de disponibilidade de sistemas, simulando o uso da solução do modelo de filas na abordagem de questões práticas de dimensionamento e disponibilidade, comumente verificadas nesses centros, nos quais os aspectos vinculados à necessidade de operação humana, tolerância a falhas, operação degradada e demanda de serviços de manutenção são preocupações fundamentais.

5.1 Modelo de disponibilidade para Centros de Controle do Espaço Aéreo

Este item apresenta um modelo para análise de disponibilidade em sistemas computacionais utilizados no Controle do Espaço Aéreo, a partir de uma extensão do modelo genérico descrito no capítulo anterior.

Assim, para maior adequação às aplicações de interesse do Controle do Espaço Aéreo, introduz-se uma extensão do modelo geral apresentado anteriormente, a partir da consideração das possibilidades de intervenção humana inerentes dessa atividade. Nas aplicações do controle aéreo, diferentemente de outras aplicações de sistemas de automação - tais como: Metrô, automação industrial, etc. - apesar do alto índice de recursos automatizados, as decisões finais de controle são exercidas por operadores humanos, que são os responsáveis, portanto, pelo fechamento da malha de controle no processo de orientação dos pilotos em uma determinada área.

Da mesma forma, esses controladores são também responsáveis pela atuação eventual no processo, por meio de procedimentos manuais adicionais, para os casos de indisponibilidade momentânea de quaisquer das funções automatizadas.

Nesse tipo de ambiente de controle, onde as decisões finais são fechadas por operadores humanos, estão listados, a seguir, alguns exemplos de funções exercidas pelos controladores que estão suportadas por algoritmos e sistemas de apoio à decisão, tanto nos centros de controle de tráfego aéreo, quanto nos centros de controle de operações militares de defesa aérea:

a) Controle de tráfego aéreo (ACC e APP):

- Separação de aeronaves em rota e resolução de conflitos;
- Processamento de planos de voo;
- Seqüenciamento de aeronaves para pouso;
- Reconhecimento de alarmes e resolução de conflitos.

b) Defesa Aérea (COPM):

- Seleção de bases aéreas para recolhimento de aeronaves após realizadas as missões, em função de critérios de configuração das aeronaves controladas, consumo de combustível e condições ambientais diversas;
- Cálculos de combustível e vetoração de aeronaves para reabastecimento em voo;
- Identificação de novas aeronaves que entram no cenário de controle para classificação das mesmas em termos de ameaça (aeronaves amigas, irregulares, suspeitas, hostis, etc).

Todos os processos relacionados acima representam exemplos de funções de responsabilidade operacional de um ou mais controladores habilitados nos centros de controle correspondentes (civis ou militares). Portanto, uma indisponibilidade de algum automatismo de apoio, no caso de uma falha não crítica dos sistemas computacionais, gera uma demanda adicional pela realização de procedimentos manuais (operação degradada), o que pode acarretar uma sobrecarga à capacidade do sistema, em função do número de operadores disponíveis, e também em função da infra-estrutura necessária para a efetivação desses procedimentos manuais (rádios, aerovias disponíveis, etc.).

Na avaliação de disponibilidade para um centro de controle de tráfego aéreo, por exemplo, em um centro de controle de aproximação em área terminal (APP), pode-se considerar o caso de uma situação real de degradação prevista na operação desse tipo de centro. Essa é a condição referente ao tratamento de extração de planos de voo⁸, processo que normalmente é automatizado, mas que pode passar a ser realizado manualmente em certas situações de perda de comunicação entre esse APP e o centro de controle de área (ACC) correspondente.

⁸ Os vôos com frequências regulares (diárias, semanais, etc.), previstos para uma região de controle, ficam armazenados em um arquivo compartilhado de planos de vôos repetitivos (RPL). A partir desse arquivo, o sistema executa um processo automático de extração de informações, de forma a apresentar ao controlador, em tempo real, uma lista de vôos que demandarão serviço naquela região de controle.

Destaca-se que, devido à similaridade operacional existente entre os centros de controle do espaço aéreo, o modelo de avaliação de disponibilidade apresentado neste trabalho pode ser aplicado de forma análoga tanto na avaliação dos sistemas usados no controle da circulação aérea civil, em um APP ou ACC, quanto para os centros de controle das operações de defesa aérea, em um COpM.

5.1.1 Modos de Operação e Níveis do Serviço Prestado pelo Centro

Uma vez que o serviço de um centro de controle do espaço aéreo não é prestado de maneira totalmente automatizada, sendo intrinsecamente dependente da atuação humana, além dos aspectos físicos e tecnológicos, uma condição fundamental que define o nível da prestação dos serviços é a situação de disponibilidade dos operadores (controladores) e dos técnicos de manutenção desses centros.

Normalmente, tais recursos humanos são organizados em equipes operacionais e técnicas. As equipes operacionais abrangem os supervisores operacionais e os controladores, responsáveis pelas comunicações com os pilotos e pelo controle propriamente dito. As equipes técnicas, por sua vez, abrangem os técnicos e respectivos supervisores técnicos encarregados da adequada configuração e da manutenção dos sistemas, software, equipamentos e toda a infra-estrutura técnica.

Nesse cenário de organização técnico-operacional, pode-se então caracterizar a operação dos centros de controle do espaço aéreo (DECEA,2006), de forma resumida, em quatro níveis de prestação dos serviços de controle:

- 1- Serviço normal: caracterizado pela prestação dos serviços em condição normal, em sua capacidade nominal de operação, com disponibilidade da infra-estrutura técnica e operacional, quando os sistemas computacionais operam com toda a automação disponível;
- 2- Serviço em modo degradado: caracterizado pela prestação dos serviços em nível abaixo do desempenho operacional nominal, por limitação em relação às quantidades de aeronaves controladas ou alongamento dos tempos de resposta no controle. Tipicamente, essa situação deriva de uma indisponibilidade temporária da infra-estrutura, resultando na necessidade de atuação humana adicional (controladores ou supervisores), decorrente de uma eventual degradação no nível de automatismo no apoio à decisão dos controladores, ou derivada de problemas ou erros operacionais;

- 3- Serviço convencional (ou não-radar): caracterizado pela perda temporária das funções básicas do sistema computacional, quando a posição operacional⁹ passa a ser utilizada pelo controlador apenas para manter a comunicação por voz com os pilotos, efetivando o modo de controle convencional, realizado exclusivamente por ação humana, denominado modo de controle não-radar;
- 4- Serviço indisponível: caracterizado pela ausência ou perda total da prestação de serviço de controle do espaço aéreo, seja por indisponibilidade completa das redundâncias dos sistemas de comunicação entre o controlador e o piloto, ou de qualquer outra infra-estrutura crítica, por exemplo, energia, ou outros motivos operacionais de indisponibilidade eventual dos recursos humanos de operação.

Nesses centros, a prestação de serviços de controle apóia-se na disponibilidade da infra-estrutura dos sistemas de sensores (radar), equipamentos e redes de comunicações de dados e de voz (áudio entre controladores e pilotos), dos sistemas computacionais, suas respectivas posições operacionais de controle e, principalmente, na disponibilidade de recursos humanos específicos: controladores e técnicos de manutenção.

A Figura 19 ilustra cada uma das situações descritas, caracterizando os quatro níveis de degradação previstos na prestação dos serviços pelos centros de controle do espaço aéreo.

Convém observar que são previstas as transições do estado normal (1) para: a) o estado degradado (2), quando o sistema passa a requerer algum atendimento operacional adicional; b) para o estado de falha ou operação não-radar (3), quando ocorre alguma falha que requer atendimento da equipe técnica de manutenção; e c) para o estado de interrupção do serviço (4), quando são perdidas as condições mínimas de continuidade do serviço, decorrente de indisponibilidade completa de operadores ou por perda de todas as redundâncias dos sistemas de comunicação entre os controladores e os pilotos.

⁹ Console ou estação de trabalho, normalmente composta por um ou dois computadores e demais periféricos, nos quais o controlador desempenha suas atividades (posição de controle).

Figura 19 – Níveis de degradação na prestação dos serviços de controle

Admitem-se todas as possibilidades de retorno de quaisquer dos estados de falha para condições mais próximas à normalidade (1), com exceção do caso de manutenção pela equipe operacional (3), pois quando é finalizado um atendimento técnico, o sistema retorna à sua condição normal, não havendo necessidade de transitar previamente pelo estado de degradação operacional (2).

Por outro lado, admite-se a possibilidade de transição do estado de interrupção do serviço (4) para o estado de operação degradada (2), pois se considera possível o caso em que uma interrupção do serviço tenha sido motivada por indisponibilidade de operadores, sendo viável retornar para qualquer dos estados mais favoráveis (3), (2) ou (1), quando se restabelece a disponibilidade dos operadores.

5.1.2 Disponibilidade do Sistema Computacional – Estados Operacionais

Para definição de um modelo de disponibilidade, sob o ponto de vista do sistema computacional, interessa estabelecer os estados das posições operacionais e cada posição de controle, ou seja, prever os possíveis estados de atuação ou de perda

funcional do sistema em seu ponto de interface com os operadores, onde se dá a interação dos controladores.

Neste trabalho, para efeito da elaboração do modelo de disponibilidade aplicável aos sistemas computacionais dos centros de controle do espaço aéreo, foram estabelecidos três estados de disponibilidade para cada posição operacional, em correspondência aos três primeiros níveis de prestação de serviço mencionados anteriormente (1), (2) e (3), descartando, portanto, o estado de interrupção na prestação de serviços de controle (4), uma vez que essa última situação não decorre da inoperância do sistema computacional:

- a) Estado Normal (N): caracterizada pela disponibilidade plena de uma dada posição operacional, indicando que os sistemas, infra-estrutura técnica e recursos operacionais encontram-se em sua capacidade plena para a prestação dos serviços de controle no nível nominal;
- b) Estado Degradado (D): caracteriza a situação em que uma posição operacional passa a requerer serviço operacional adicional, decorrente de *falha não-crítica*, que não inviabiliza a operação radar, seja por erro de operação, adoção circunstancial de procedimentos inadequados, indisponibilidade momentânea de comunicações de dados (p.ex: entre centros adjacentes), perda de funções automatizadas do software ou por qualquer outra necessidade de recursos humanos adicionais na operação, supervisores, etc. A recuperação desse estado para retorno à condição normal se dá apenas após serviço desempenhado pela equipe operacional (supervisores, outros controladores, ou tarefas adicionais impostas ao próprio controlador), responsável pela correção do erro, re-configuração do sistema, ou efetivação de operações manuais adicionais;
- c) Estado de Falha (F): caracteriza a situação decorrente de *falha crítica* nos sistemas computacionais, inabilitando suas funcionalidades básicas principais e inviabilizando o desempenho da operação radar. Neste estado, os sistemas computacionais entram em estado de manutenção e os controladores continuam prestando os serviços de controle em modo convencional. A recuperação desse estado para retorno à condição normal se dá apenas após serviço desempenhado pela equipe de técnicos ou supervisores de manutenção de hardware ou software.

O diagrama de estados da Figura 20 representa as transições de cada posição operacional do sistema computacional, que pode então assumir as condições de normalidade, degradação ou falha.

Figura 20 – Estados das Posições Operacionais do Sistema Computacional

Quando no seu estado de normalidade (N), uma posição de controle mantém o nível de serviço nominal, com os recursos operacionais em capacidade nominal, contando com funcionamento adequado da infra-estrutura e dos automatismos de apoio à decisão, exigindo a carga normal de atuação do controlador.

Uma vez em condição degradada (D), a posição operacional demandará serviço operacional adicional, durante um certo intervalo de tempo, de modo que os controladores ou supervisores da operação resolvam uma situação de erro operacional (falha humana) ou venham a suprir quaisquer demandas extras de atuação de operadores humanos, derivadas, por exemplo, da indisponibilidade circunstancial de uma função automatizada, seja por falha de software, seja por falha de qualquer infra-estrutura não crítica que implique em atividade complementar operacional ou procedimento manual para suprir o serviço demandado.

Uma vez em falha (F), a posição operacional demandará serviços técnicos para manutenção, reconfiguração ou reinicialização de software etc, ou demais atividades da equipe técnica ou de supervisão técnica do centro.

A Tabela 6 indica a correspondência dos quatro níveis de degradação para os serviços prestados em um centro de controle do espaço aéreo (operação 1-Normal, 2-Degradada, 3-Convencional e 4-Indisponível), em relação aos três estados considerados para as posições operacionais dos sistemas computacionais, estabelecidos para definição do modelo de disponibilidade de interesse neste trabalho: posição em operação Normal(N), Degradada(D) ou em Manutenção/Falha(F).

Tabela 6 – Níveis de degradação do serviço x Estados do sistema computacional

Nível do serviço prestado pelo centro (Figura 19)	Estado inicial dos sistemas computacionais (Figura 20)	Condições para degradação (situações que levam a um nível inferior de serviço, passando para um estado de maior degradação)	Condições para recuperação (que levam a um nível superior de serviço)
1 - Normal	(N) Operação Normal (disponível)	Erro operacional, falha não-crítica de hardware ou de software dos sistemas computacionais, incluindo meios de transmissão de dados e sensores.	-
		Falha crítica de infra-estrutura (energia, comunicações com os pilotos, etc).	-
		Indisponibilidade crítica de operadores	-
2 - Degradado	(D) Operação Degradada	Serviço operacional não resolve a degradação, sendo gerada demanda de manutenção.	Serviço da equipe operacional
		Falha crítica de infra-estrutura (energia, comunicações com os pilotos, etc).	-
		Indisponibilidade crítica de operadores.	-
3 - Convencional	(F) Falha (Manutenção)	Falha crítica de infra-estrutura (energia, comunicações com os pilotos, etc).	Serviço da equipe técnica de manutenção
		Indisponibilidade crítica de operadores.	-
4 - Indisponível	-	-	Serviço da equipe técnica de manutenção da infra-estrutura crítica
		-	Disponibilidade mínima de operadores

5.1.3 Exemplo de Modos de Operação de um Centro de Controle APP

Os serviços de Controle de Tráfego Aéreo (ICAO, 1996) são prestados em estruturas operacionais que adotam as hierarquias mencionadas anteriormente, no Capítulo 2 deste trabalho, desde a gestão estratégica no CGNA até o controle de aeródromo, no âmbito da aviação civil e, analogamente, desde o nível do comando geral de operações de defesa aérea até o nível dos grupamentos de controle de ações táticas no nível local, para as operações militares.

As entidades normativas internacionais estabelecem os procedimentos para a prestação de serviços de controle de tráfego aéreo (ICAO, 1996) e para coordenação de operações especiais militares (FAA, 2004), de modo a garantir a segurança e continuidade de funcionamento desses serviços, mesmo que de forma degradada, durante eventuais paralisações ou indisponibilidade de serviços de apoio diversos (DEPV, 1999).

Como exemplo das situações de degradação operacionais previstas, pode-se mencionar a eventual indisponibilidade das ligações de dados entre um ACC e um APP, situação em que o APP passaria a operar em modo autônomo, ou degradado. O caso contrário, com as comunicações disponíveis, caracteriza a operação normal de um APP. Tais modos estão relacionados à forma de entrada de dados de planos de voo no sistema, a fim de assegurar continuidade operacional, na ocorrência da indisponibilidade mencionada. Em **modo normal**, a forma usual de entrada de alguns tipos de planos de voo no sistema é automática. Em **modo autônomo (degradado)**, não há criação automática de planos, e essa função passa a ser realizada manualmente. A passagem ao modo autônomo exige a adoção de algumas medidas operacionais para assegurar a continuidade de prestação dos serviços:

- Introdução manual dos planos de voo no sistema, pelo operador de planos de voo;
- Extração automática de planos de voo repetitivos – RPL – a partir de um arquivo (ICAO, 1996). O supervisor operacional verifica a conveniência da utilização completa ou parcial desse arquivo RPL e faz as ativações correspondentes;
- As coordenações com o ACC passam a ser feitas por outro meio de comunicação (telefone, etc.).

Um terceiro caso, denominado *modo convencional (não-radar)*, caracteriza-se pela indisponibilidade completa da visualização em uma posição operacional de APP, que poderia ocorrer: a) por falha crítica do sistema computacional, envolvendo falhas nos recursos de visualização (monitores) ou de processamento, redes locais de computadores ou demais recursos informáticos redundantes; ou b) por falha crítica na obtenção dos dados sensorizados, envolvendo as falhas em todas as redundâncias existentes nas comunicações e nos radares.

Mesmo nesse caso, os serviços de controle continuam a ser prestados de forma segura, conforme os procedimentos manuais “não-radar”, nos quais os controladores efetuam as comunicações de voz e as diversas atividades mencionadas anteriormente, de separação dos vôos, seqüenciamento de aeronaves, execução de esperas, etc., sem a visualização radar, apenas seguindo os procedimentos de controle e separações no espaço e tempo adequados a cada situação operacional.

As informações descritas anteriormente, especificamente para o caso de operação degradada, ou *modo autônomo* de operação de um APP, exemplificam um tipo de função normalmente automatizada pelo sistema computacional, quando em seu modo normal de operação, e que passaria a exigir alguma intervenção humana adicional, por parte dos controladores, quando da entrada em modo de operação degradada.

A Figura 20, apresentada anteriormente, ilustra os casos de operação normal, degradada ou em falha (operação não-radar) para esses mesmos exemplos, que podem ser verificados na rotina de um APP.

Dessa forma, partindo do modelo de filas genérico, citado anteriormente e aplicável a um *data center*, no qual se considerava simplesmente a disponibilidade ou não de uma máquina, que entrando em falha passaria a demandar um serviço de manutenção, pode-se considerar um modelo equivalente, com as máquinas desempenhando alguma função automática que, ao entrarem em estado degradado, passam a demandar intervenção humana por parte de um operador habilitado naquela função.

5.1.4 Exemplo de Aplicação do Modelo Genérico para um APP

A partir do mesmo modelo usado no exemplo de um *data center*, mencionado anteriormente, pode-se estabelecer um sistema de filas equivalente, conforme ilustra a Figura 21, no qual se considera um total de M máquinas em operação normal, ou automática, sendo que um subconjunto dessas máquinas, ao entrar em um estado de

operação degradada, requer a intervenção de até D operadores extras que passam a realizar algum tipo de ação manual adicional, tal como no caso ilustrado, referente à necessidade de introdução manual de planos de voo.

Figura 21 – Modelo de filas genérico aplicado a um centro APP

Nesse caso, continuando com a mesma dimensão do exemplo anterior (*Questão 1* no item 4.2.3), considerou-se um centro de controle com 120 máquinas ($M=120$), que representaria um sistema com 60 posições de operacionais.

Como exemplo, foram admitidos: um tempo médio entre falhas de 80 horas ($\lambda=0,0125$ falhas/hora) para caracterizar a taxa de perda de qualquer função não-crítica; e um tempo médio total de retorno à operação normal de 4 horas (onde se aplica o conceito de MTTRS mencionado anteriormente), ou seja, o tempo médio de espera mais a duração de uma operação manual, e que seria equivalente ao período de ocupação adicional de um operador ($\mu=0,25$: taxa horária de recuperação da operação degradada).

Então, da mesma forma que a solução apresentada no item 4.2.2, pode-se obter a solução da rede de filas, respondendo às *Questões 2 e 3*, mencionadas anteriormente na seção 4.2.1, como segue:

Solução da Questão 2: A probabilidade de que *pelo menos* j máquinas estejam em operação normal (automática) pode ser obtida dos valores acumulados da resposta análoga à da *Questão 1*, conforme ilustra a Figura 22;

Solução da Questão 3: O tamanho D da equipe de operadores extras, necessários para garantir que as operações manuais sejam finalizadas, resultando em pelo menos j máquinas de volta à operação normal (automática), também pode ser verificado com base nos dados acumulados de probabilidades, conforme ilustra a Figura 22, onde se destacam os seguintes aspectos:

- Para $D = 2$, a probabilidade de ter pelo menos 30 máquinas operacionais é de 96%, enquanto que para ter pelo menos 40 máquinas essa probabilidade cai para 53%;
- Desejando-se uma confiança de 90% sobre o número de máquinas em operação normal (automática), a partir de equipe extra de 4 operadores, só se poderia garantir 69 máquinas; ou 88, para $D=5$; ou ainda 112, para uma equipe de 10 operadores.

Figura 22 – Probabilidade (P_j) de encontrar pelo menos j máquinas em operação normal

5.1.5 Proposta do Modelo Estendido para Análise de Disponibilidade de um Centro de Controle do Espaço Aéreo

Em face da possibilidade de operação degradada existente em um sistema de controle do espaço aéreo real, pode-se então estabelecer um modelo estendido (PIZZO; CUGNASCA, 2007), integrando as duas situações mencionadas anteriormente em uma rede fechada com três filas, de forma a representar simultaneamente as transições entre os três estados de operação: normal, degradada e falha.

A extensão do modelo se justifica pela importância em considerar também a operação degradada nesse tipo de sistema. Durante um estado de operação degradada, aumenta-se a dependência do serviço prestado relativamente aos tempos de resposta e decisões tomadas autonomamente pelo operador.

Dessa forma, o modelo de filas pode ser estendido para a configuração ilustrada na Figura 23. Dado um centro de controle com um conjunto (P) de posições operacionais, o modelo estendido passa a considerar não somente o efeito do tamanho da equipe de técnicos (T) alocados para a manutenção do sistema, mas também o efeito do tamanho da equipe de operadores extras disponíveis (D), eventualmente alocados para atender a um estado de degradação.

Ou seja, o modelo estendido considera também a situação da operação degradada, na qual a recuperação para retorno à condição normal resulta dos serviços de uma equipe operacional, com (D) supervisores ou controladores extras, capacitados e disponíveis, para desempenhar, quando solicitados, aqueles procedimentos manuais necessários para correção de algum erro, ou mesmo para substituir os processos automatizados que atendiam regularmente à operação normal.

Figura 23 – Modelo estendido para avaliação de disponibilidade de centros de controle do espaço aéreo (PIZZO; CUGNASCA, 2007)

Nesse modelo, a taxa λ representa o fluxo de posições operacionais cujos serviços críticos, equipamentos, ou funções entram em falha, saindo da operação normal e requerendo uma atuação extra de controlador/supervisor disponível, ou ainda requerendo uma ação técnica de manutenção de hardware ou software.

O estabelecimento prático desse fluxo pode ser realizado, em sistemas existentes, por meio de observação e registro de ocorrências de indisponibilidade operacional. No entanto, ressalta-se que também é possível estimar valores teóricos desse fluxo λ , considerando que o mesmo corresponde à taxa combinada de falhas (sistêmica) referente a uma determinada cadeia de serviço crítico.

O cálculo da taxa λ pode ser elaborado a partir de modelos combinatórios série-paralelo, que leve em conta os componentes de hardware, software e os fatores humanos associados. Adicionalmente, para levar em conta ainda os demais aspectos de redundância previstos na arquitetura do sistema, bem como os eventuais mecanismos de tolerância a falhas previstos no projeto, pode-se também considerar a utilização de cadeias de Markov, conforme exemplificado nos Apêndices A e B.

No modelo apresentado pela Figura 23, a taxa λ representa o fluxo de posições operacionais que falham, saindo da operação normal, e corresponde à soma dos fluxos $\lambda.p1$ e $\lambda.p2$, os quais se referem, respectivamente: a) à passagem do estado normal para a situação de falha (operação convencional), com probabilidade $p1$, quando se exige um acionamento da equipe de manutenção técnica; e b) à passagem do estado normal para a operação degradada, com probabilidade $p2$, situação em que se exige um acionamento de equipe operacional para recuperação da situação de degradação.

O retorno do estado de manutenção para a operação normal ocorre com taxa de reparos $\mu1$ (determinada pelo tempo de serviço da equipe técnica), enquanto $\mu2$ representa a taxa das posições que saem da operação degradada por meio de serviço da equipe operacional, retornando à condição normal ou ainda passando ao estado de falha, com probabilidades $p4$ e $p3$, respectivamente, compondo assim os fluxos $\mu2.p4$ e $\mu2.p3$.

Com base nesse novo modelo, resolvido de forma análoga ao apresentado no item 4.1 deste trabalho, pode-se realizar uma análise do valor médio (MENASCÉ *et al*, 2004) dos parâmetros de filas, estabelecendo as influências da equipe de manutenção e de operação sobre a disponibilidade sistêmica, neste caso considerando mais de um estado de degradação.

5.1.6 Exemplo de Solução por Markov para um Centro APP

Para a situação de um APP, considerando então sua possibilidade de operação degradada com os três estados previstos no modelo estendido, uma solução pode ser implementada por meio de um diagrama de Markov, conforme ilustra a Figura 24. Nesse diagrama, cada estado corresponde ao modo de operação de uma única posição operacional, ou de uma linha de serviço crítico (*service thread*), referente, por exemplo, ao processamento de planos de voo: Estado 1 - operação normal, com automatismo; Estado 2 - operação degradada, envolvendo procedimentos manuais adicionais; Estado 3 - operação convencional, em caso de falha (não-radar).

O Apêndice A apresenta uma planilha elaborada para análise baseada na solução do modelo de Markov apresentado na Figura 24.

Figura 24 – Solução da fila com aplicação de um Modelo de Markov

No entanto, essa solução por modelos de Markov fica limitada à análise de apenas um único elemento (estação) por vez, servindo apenas para as análises individuais, por exemplo, da disponibilidade de uma única posição operacional, ou para verificação de alocação/ocupação de um único controlador específico, ou ainda para analisar a disponibilidade de uma única funcionalidade ou serviço crítico, como o caso mencionado de tratamento dos planos de voo.

Para analisar a mesma situação, porém considerando simultaneamente duas posições operacionais, ou duas funcionalidades críticas por vez, o diagrama da Figura 24 passaria a ter 6 estados. Para análise de um centro com 20 posições e 3 situações de degradação, seria necessária uma cadeia de Markov com 231 estados. Genericamente, para N

usuários e K estações, a cadeia de Markov teria o número de estados definido pela seguinte expressão binomial:

$$\binom{N + K - 1}{K - 1}$$

Destaca-se, assim, a limitação descrita (MENASCÉ *et al*, 2004) para a solução por meio de modelos de Markov, que é sua característica de explosão do universo de estados, tornando inviável a implementação de algoritmos de resolução, mesmo para sistemas de tamanho moderado.

Nesses casos, sugere-se a adoção de uma análise de valor médio (AVM) do modelo de filas estendido, proposto na Figura 23, de forma que, a partir do desempenho de uma rede de filas na presença de $N-1$ usuários, pode-se calcular o desempenho da rede de filas para a presença de N usuários. Assim, a adoção de uma análise de valor médio pode estabelecer a solução geral do modelo estendido, segundo o algoritmo de AVM apresentado anteriormente no Capítulo 4.

Adicionalmente, as referências mencionadas apresentam abordagens alternativas de cálculo, com base no algoritmo de convolução (JAIN, 1991) (MENASCÉ *et al*, 2004), que também pode favorecer a elaboração de planilhas ou outras ferramentas para a solução interativa do modelo, no caso de envolver múltiplos estados.

5.2 Solução do Modelo Estendido de Filas Aplicável aos Centros de Controle do Espaço Aéreo

Para o caso de interesse deste trabalho de pesquisa, que é a solução do modelo de filas estendido apresentado na Figura 23, e considerando a situação geral que pode envolver algumas dezenas de posições operacionais (P), dezenas de controladores envolvidos na operação degradada (D) e diversos técnicos de manutenção (T) a analisar simultaneamente, foi adotada uma abordagem de simulação numérica do modelo de filas, por meio do uso de uma ferramenta específica: o software Arena (KELTON *et al*, 2007), em sua versão 10.0.

A seleção da ferramenta Arena foi realizada em decorrência da disponibilidade comercial do software, dos recursos embutidos para análise estatística dos resultados e também pelas suas facilidades de edição e animação gráfica, em função dos mesmos

critérios de seleção verificados em um trabalho de análise operacional de sistemas aeronáuticos (RIBEIRO, 2003), conforme reproduz o Anexo C.

Os cenários analisados, as descrições da parametrização das simulações e os resultados obtidos estão apresentados no Capítulo 6, a seguir.

5.3 Possibilidades Adicionais para Aplicação do Modelo na Avaliação de Desempenho dos Serviços de Controle

Este trabalho tem o objetivo focado na apresentação de um modelo para avaliação de disponibilidade de sistemas computacionais dos centros de controle do espaço aéreo e, por isso, foram considerados apenas os três estados afetos a esses sistemas, envolvendo a operação normal, degradada e não-radar. No entanto, é interessante destacar que, adotando os mesmos conceitos descritos anteriormente, torna-se possível, de forma análoga, estabelecer um modelo mais amplo, incluindo o quarto estado - serviço interrompido - quando se pretende avaliar a disponibilidade do serviço de controle prestado pelo centro como um todo, e não apenas dos sistemas computacionais. Essa seria a perspectiva do cliente do serviço, por exemplo, das companhias aéreas que utilizam os serviços de controle prestados nesses centros.

Essa extensão pode ser útil quando for de interesse considerar o caso (4), mencionado anteriormente na Figura 19, referente à indisponibilidade ou interrupção completa dos serviços de controle, ou seja, quando são levados em conta também aqueles fatores exógenos aos sistemas computacionais, que estão além dos aspectos técnicos de confiabilidade e manutenibilidade impostas apenas pelos sensores, equipamentos de transmissão de dados, redes, computadores e periféricos.

Nesse caso, o modelo de avaliação de disponibilidade estaria incluindo os demais efeitos externos que levam à interrupção completa do serviço, derivados de problemas em infra-estrutura crítica (sistemas de energia, sistemas de comunicação por voz, etc) ou decorrentes de episódios eventuais de indisponibilidade crítica de recursos humanos (controladores).

5.4 Considerações Finais deste Capítulo

A partir do modelo genérico de aplicação de redes de filas para avaliação de disponibilidade de sistemas computacionais, apresentado no Capítulo 4, este capítulo descreveu um modelo estendido, mais adequado à avaliação de disponibilidade de operação de sistemas computacionais nos sistemas de controle do espaço aéreo, onde se considera a degradação do automatismo, e que demanda atividade extra dos operadores.

Nesses casos, quando se requer operação humana adicional, passam a ser considerados então os três possíveis estados de operação: normal, degradada ou em falha, no ponto de vista da disponibilidade dos sistemas computacionais.

A partir do modelo estendido, apresentado neste capítulo, algumas possibilidades teóricas de solução foram referenciadas, permitindo a seguir ilustrar-se um exemplo prático de avaliação de disponibilidade de sistemas de controle do espaço aéreo, baseado em simulação numérica, e demonstrando a potencialidade do uso dessa mesma ferramenta na avaliação de disponibilidade de centros reais de interesse.

6 Estudo de Caso – Aplicação do Modelo Proposto

Este capítulo detalha a aplicação do modelo de avaliação de disponibilidade apresentado no Capítulo 5, por meio de simulações efetuadas com a ferramenta Arena. A partir dos cenários simulados neste capítulo, e com as devidas parametrizações particularizadas para casos reais de interesse, esses mesmos exemplos poderão ser configurados e aplicados em avaliações de disponibilidade em Centros de Controle do Espaço Aéreo existentes.

A partir do modelo de filas estendido, para avaliação de disponibilidade de sistemas de controle do espaço aéreo (PIZZO; CUGNASCA, 2007), conforme a Figura 23, este capítulo apresenta um exemplo de aplicação desse modelo para algumas configurações típicas desses centros de controle, envolvendo desde cenários menores, característicos das arquiteturas de sistemas de controle de tráfego em área terminal (APP), até os cenários de grande capacidade, característicos dos centros de controle de área (ACC).

Ressalta-se que os estudos aqui apresentados têm por objetivo principal demonstrar o uso e aplicação do modelo de avaliação de disponibilidade descrito neste trabalho. Assim, não é objetivo desses exemplos fazer uma avaliação da disponibilidade de nenhum centro específico, mas sim validar o modelo, explicitando benefícios e facilidades de sua aplicação na obtenção de indicadores de interesse ao dimensionamento do efetivo de controladores e técnicos nos centros, ou mesmo para analisar as influências de arquiteturas e redundâncias técnicas dos sistemas que, ao melhorar seus parâmetros de confiabilidade e reparabilidade, possam resultar em vantagens mensuráveis na disponibilidade do sistema.

Com os exemplos desenvolvidos neste capítulo, pretende-se facilitar o emprego do mesmo tipo de análise para avaliação de disponibilidade de casos reais específicos de algum centro de controle do espaço aéreo. Para isso, será necessário empregar um cenário adequado de dimensão do sistema em questão, bem como considerar os parâmetros reais de confiabilidade e reparabilidade específicos do caso de interesse, o que pode ser feito por meio do cálculo teórico das taxas de falhas e de levantamentos de dados de operação e manutenção do centro que se deseja analisar.

Dessa forma, este trabalho de pesquisa procurou consolidar um exemplo prático de aplicação do modelo de avaliação da disponibilidade apresentado anteriormente, com

valores hipotéticos para parâmetros de confiabilidade, dimensões de equipes técnicas e operacionais aplicáveis em casos reais de sistemas de controle de tráfego aéreo.

Conforme mencionado anteriormente, em função do grande número de estados envolvidos no modelo com dezenas de posições operacionais, controladores e técnicos de manutenção a analisar simultaneamente, tais quantidades tornariam impeditiva uma solução genérica por cadeias de Markov. Assim, nos cenários exemplificados neste capítulo, foi considerada uma abordagem de solução envolvendo simulação numérica do modelo de filas proposto, por meio da ferramenta Arena 10.0 (KELTON *et al*, 2007).

6.1 Descrição do Ambiente de Simulação

Para elaboração do estudo de caso, este tópico exemplifica a aplicação do modelo de avaliação de disponibilidade apresentado no Capítulo 5, por meio de simulação numérica do comportamento da rede de filas ilustrada pela Figura 23.

6.1.1 Entradas e Saídas dos Cenários Simulados

Para cada um dos cenários simulados, foram consideradas as seguintes variáveis de entrada e saída para avaliação do modelo de filas:

Entradas dos cenários simulados:

- **Dimensão do sistema**, em termos do número (P) de posições operacionais;
- **Confiabilidade do sistema**, representada pela taxa de falhas λ , referente a cada posição operacional;
- **Capacidade máxima de atendimento operacional simultâneo**, representada pelo tamanho (D) da equipe operacional de reserva, composta pelos controladores ou supervisores responsáveis pelo atendimento em qualquer eventual degradação;
- **Capacidade máxima de atendimento técnico simultâneo**, representada pelo tamanho (T) da equipe de manutenção, composta pelos técnicos de manutenção responsáveis pelo reparo de falhas no sistema computacional;

- **Taxas de reparo** correspondentes aos tempos médios de atendimentos prestados pelas equipes técnica e operacional, representados pelas taxas μ_1 e μ_2 , respectivamente;
- **Percentual p_1 de falhas críticas**, do total de ocorrências λ , que levam a posição à condição de manutenção (operação convencional). Derivado de p_1 , o **percentual p_2 representa a parcela de falhas não críticas** encaminhadas para atendimento pela equipe operacional, sendo definida como: $p_2 = 1 - p_1$;
- **Percentual p_3 de falhas críticas** ocorridas durante o atendimento operacional, que levam o sistema de uma condição degradada para a condição de falha. Derivado de p_3 , o **percentual p_4 representa o sucesso de atendimento da equipe operacional**, definido como: $p_4 = 1 - p_3$, que indica a parcela das ocorrências não críticas resolvidas apenas no âmbito da equipe operacional.

Saídas dos cenários simulados:

- **Disponibilidade global do sistema**, representada pelo percentual médio de posições operacionais disponíveis, durante todo o intervalo de simulação, em relação ao número total de posições instaladas (P). Quando a disponibilidade global é menor que 1, significa que há posições operacionais fora do seu estado normal. Não significa, no entanto, que necessariamente tenha sido afetada a prestação do serviço do centro, pois a perda pode estar dentro da margem de folga prevista no nível de redundância instalada do sistema;
- **Disponibilidade nominal do sistema**, representada pelo percentual médio de posições operacionais disponíveis, durante o intervalo de simulação, em relação ao número mínimo (P_n) de posições necessárias à prestação do serviço, em sua capacidade nominal. Esse número (P_n) foi inicialmente estabelecido em 80% da dimensão do sistema (P): $P_n = 0,8.P$, resultando em um nível de redundância inicial de 25% das posições. Quando a disponibilidade nominal fica abaixo de 1, significa que o sistema está operando abaixo da sua capacidade nominal, e que, portanto, pode haver degradação da prestação do serviço em sua carga nominal;
- **Tamanho médio da fila operacional**, que representa a média de posições que ficam na espera de controladores extras (atendimento operacional) durante uma demanda por operação degradada;

- ***Tamanho médio da fila de manutenção***, que representa a média de posições que ficam na espera de técnicos de manutenção (atendimento técnico) durante uma ocorrência de falha com demanda por manutenção;
- ***Tamanho máximo da fila operacional***, que representa a média dos valores máximos assumidos na fila de espera por controladores, durante os episódios de operação degradada;
- ***Tamanho máximo da fila de manutenção***, que representa a média dos valores máximos assumidos na fila de espera por técnicos, durante os episódios de falha com demanda por manutenção.

6.1.2 *Cenários Considerados para Simulação*

Para efeito da ilustração dos casos de emprego do modelo de avaliação de disponibilidade, este item descreve algumas configurações típicas encontradas em centros de controle de tráfego aéreo, considerando tanto casos de instalações de pequeno porte, típicas de alguns sistemas de controle de área terminal (APP), até configurações de grande porte, encontradas em centros de controle de área (ACC) das regiões de grande volume de tráfego.

Nos cenários simulados, foram consideradas três situações básicas:

- a) Uma arquitetura de pequeno porte, dimensionada com 5 posições operacionais, típica de um APP de pequeno porte;
- b) Uma arquitetura de médio porte, típica de sistemas com cerca de 15 posições operacionais, por exemplo, em um APP de grande capacidade instalada (p.ex: TMA São Paulo), que atenda cerca de 100 movimentos¹⁰ por hora;
- c) Uma arquitetura de grande porte, equivalendo a um sistema com 30 posições operacionais, típico de uma situação utilizada, por exemplo, nos principais centros de controle em rota (ACC) com grande capacidade instalada.

Para estabelecimento de uma taxa de falhas típica de cada um dos centros desse tipo, pode-se abordar a relação completa das cadeias de serviço consideradas (*safety-critical*, *efficiency-critical* e *essential service threads*) nas atividades operacionais do sistema,

¹⁰ Vãos controlados.

incluindo seus aspectos de arquitetura de hardware e software, conforme ilustra o exemplo de cálculo do Apêndice A.

Nessas simulações, foram considerados os cenários de pequeno (P), médio (M) e grande (G) porte, mencionados anteriormente, com variações dos perfis de alta (A) e baixa (B) confiabilidade, bem como das estruturas operativas e de manutenção, com alta (A) e baixa (B) reparabilidade, caracterizando o universo de cenários apresentados na Tabela 7. Os valores de referência para confiabilidade e reparabilidade estabelecidos na tabela estão detalhados mais adiante no item 6.1.3.

A ordem dos cenários representa uma progressão do cenário mais favorável (PAA), para um sistema de pequeno porte, com altas taxas de confiabilidade e reparabilidade, respectivamente, até o cenário menos favorável, para um centro de grande porte (GBB) caracterizado com baixas taxas de confiabilidade e reparabilidade, respectivamente.

Tabela 7 – Cenários de avaliação de disponibilidade de centros de controle aéreo

CENÁRIOS		Dimensão do Centro (N° posições operacionais)			Confiabilidade (MTTF (h) por posição)		Reparabilidade (MTTR (h) por posição)	
		(P)	(M)	(G)	(A)	(B)	(A)	(B)
		5	15	30	200	50	0,5	24
1	PAA	x			x		x	
2	PAB	x			x			x
3	PBA	x				x	x	
4	PBB	x				x		x
5	MAA		x		x		x	
6	MAB		x		x			x
7	MBA		x			x	x	
8	MBB		x			x		x
9	GAA			x	x		x	
10	GAB			x	x			x
11	GBA			x		x	x	
12	GBB			x		x		x

6.1.3 Valores Considerados na Parametrização dos Cenários

Para efeito de se estabelecer uma confiabilidade típica, tomou-se por base o cálculo teórico de uma posição operacional contendo dois computadores, dois monitores e demais periféricos, conforme cálculos detalhados no Apêndice A. Para essa posição operacional, a confiabilidade teórica calculada é **MTTF = 11187 horas**, considerada como uma confiabilidade típica, de forma que podem então ser estabelecidos os cenários de alta e de baixa confiabilidade (A: MTTF = 20000 horas e B: MTTF = 5000 horas) para *falha crítica* em cada posição (vide item 5.1.2 e Apêndice A – item 2).

Considerando também as falhas operacionais não críticas, da ordem de 1 evento a cada 50h ou 200h (ou $p_1 = 1\%$ das falhas críticas), respectivamente, têm-se então os valores a simular para o MTTF total de cada posição nos cenários A e B. As probabilidades de transição de estados, consideradas para balizar as classes de alta e baixa reparabilidade, tiveram por base a planilha do Apêndice C, na qual podem ser configurados os valores de p_1 , p_2 , p_3 e p_4 para cada um dos fluxos de interesse do modelo. Destaca-se que, no interesse de aplicação para um caso real, de um centro existente, esses fluxos poderiam ser livremente calibrados em função de observações práticas da operação e manutenção do sistema, gerando medidas precisas para ajuste do modelo.

Para o efetivo operacional, em face da redundância de 25% mencionada anteriormente, foram consideradas equipes de 1, 3 e 6 controladores disponíveis para atendimento operacional, respectivamente para os cenários (P), (M) e (G). Da mesma forma, foram também consideradas equipes técnicas de manutenção com 1, 2 e 3 técnicos para cada um dos cenários (P), (M) e (G), conforme ilustra a planilha auxiliar no Apêndice C.

Além disso, foram consideradas, ainda, as referências de reparabilidade e confiabilidade apresentadas no *RMA Handbook* (FAA, 2006b) e em artigo que trata da especificação de requisitos de confiabilidade, disponibilidade e manutenibilidade de sistemas computacionais para controle de tráfego aéreo (HORROCKS *et al*, 2007b). Essas fontes apresentam parâmetros de confiabilidade, por atividade ou funcionalidade crítica do sistema (com MTTF típico de 50000h), não afetando significativamente, portanto, as faixas de 5000h a 20000h dos cenários A e B utilizados nas simulações deste trabalho. No interesse do estabelecimento mais preciso da confiabilidade teórica do sistema, destacam-se as considerações sobre a cobertura de falhas e confiabilidade de software, mencionadas no *RMA Handbook* (FAA, 2006b) e no Apêndice B deste trabalho.

Assim, ressalta-se que os valores adotados nesse estudo, apesar de hipotéticos, por não corresponderem a medições reais de sistemas existentes, são valores representativos das condições típicas admissíveis para os sistemas em questão.

Alguns valores mencionados do *RMA Handbook* foram reproduzidos na Tabela 8, que ilustra casos de indisponibilidade de funções automatizadas em um controle de área terminal, para os quais pode haver necessidade de intervenção humana em condições de degradação da capacidade nominal de operação dos sistemas. Essa tabela apresenta requisitos de confiabilidade e reparabilidade do sistema, indicando, por exemplo, que pode haver falhas críticas (referentes aos sistemas STR e STP) com MTTF de 300 horas, desde que o tempo de recuperação automática seja de 10 segundos (por exemplo, por chaveamento e acionamento de sistemas redundantes), considerando ainda uma taxa de reparo MTTR de 0,5 hora.

Conforme mencionado anteriormente, para composição de um MTTF típico para simulação, a Tabela 8 destaca um tempo médio entre falhas de 50000 horas para falhas críticas (não cobertas pelos mecanismos de redundância) e, portanto, reparáveis apenas após o tempo de recuperação automática.

Tabela 8 – Confiabilidade dos Serviços e Reparabilidade de Sistemas de Controle em Área Terminal (FAA, 2006b)

Sistema /Serviço	Manutenibilidade (MTTR em horas)	Tempo de recuperação automática (segundos)	Confiabilidade MTTF (horas)	
			Para falhas reparáveis dentro do tempo de recuperação automática.	Para falhas reparáveis depois do tempo de recuperação automática.
Tratamento de dados radar (STR)	0,5	10	300	50000
Tratamento de planos de voo (STP)	0,5	10	300	50000
Sistema de Gerenciamento de Tráfego	0,5	N/A	5000	5000
Sistema de supervisão técnica (processador de manutenção)	0,5	N/A	5000	5000

Como ilustração adicional, além do caso da disponibilidade tratado neste trabalho de pesquisa, estudos nos quais se deseje avaliar os aspectos de segurança do sistema devem considerar, também, os modos de falha possíveis de ocorrer durante a parcela do tempo em que o sistema fica no estado de transição, ilustrado pela Figura 25. Nesse intervalo, quando o sistema apresenta-se migrando da situação normal para o estado de degradação, identifica-se um tipo de situação potencialmente perigosa.

Uma vez atingida a situação de degradação, os serviços continuam sendo prestados de forma segura, porém exigindo maior intervenção dos controladores e, portanto, promovendo redução na capacidade nominal do espaço aéreo (NAS), eventualmente reduzindo a eficiência e o desempenho nominal do sistema (operação degradada).

Figura 25 – Efeito das interrupções do serviço na capacidade do NAS
(HORROCKS *et al*, 2007a)

6.1.4 Implementação do Modelo de Filas na Ferramenta Arena

No simulador Arena, a representação do modelo estendido de filas apresentada no Capítulo 5 (Figura 23) pode ser implementada conforme ilustra a Figura 26, contando com os seguintes componentes:

- Objeto de inicialização (“**Início**”): a rede de filas fechada requer um objeto de inicialização, responsável pela ativação de novas posições operacionais no início da simulação, com número total de posições limitado ao tamanho P de cada cenário estudado (pequeno, médio ou grande porte);

- Processo de “**Operação Normal**”: é o módulo que descreve o processo de geração aleatória de ocorrências de falha, para o conjunto de todas as posições que estão operando normalmente, e cujos eventos de falha crítica ou não crítica encaminham as posições retiradas da operação normal para os estados de degradação operacional (ocorrências resolvidas pela equipe operacional) ou de manutenção (ocorrências tratadas pela equipe de manutenção de hardware ou software). Conforme modelo consagrado (taxa de falhas constante) para sistemas eletrônicos, mencionado no Capítulo 3, este módulo caracteriza-se por uma distribuição exponencial de ocorrências por posição operacional, com a taxa $\lambda = 1/\text{MTTF}$, conforme está representado no modelo de filas;
- Módulo de decisão “**Falha Crítica**”: responsável por encaminhar cada posição acometida de uma ocorrência, para os estados D ou F, em função das probabilidades p_1 e p_2 , conforme descreve o modelo de filas da Figura 23;
- Processo de “**Operação Degradada**” (Estado D): caracterizado por uma fila de atendimento operacional, cuja taxa de reparos é μ_2 ;
- Módulo de decisão “**Recupera ou Falha**”: responsável por encaminhar cada posição que passou pelo atendimento operacional de volta ao estado Normal, no caso da ocorrência ter sido resolvida pela equipe operacional, ou ainda encaminhada para manutenção, conforme as probabilidades p_4 e p_3 , indicadas no modelo de filas;
- Processo de “**Manutenção**” (Estado F): caracterizado por uma fila do atendimento técnico para manutenção de hardware ou software, cuja taxa de reparos é μ_1 ;

Figura 26 – Implementação do modelo de filas na ferramenta *Arena 10.0*

O modelo adotado para representação das ocorrências de reparo foi uma *distribuição Triangular*, tanto para representação dos tempos médios do atendimento operacional ($MTTR_{op} = 1/\mu_2$), quanto para representação dos tempos médios de reparo no atendimento de manutenção técnica ($MTTR_{tec} = 1/\mu_1$).

A adoção de uma distribuição triangular permite considerar que os tratamentos das equipes operacional e técnica apresentam um valor mínimo observável para atendimento, assim como um valor de pico (máxima frequência observável para os tempos de reparo), podendo ainda, em casos menos frequentes, prolongar-se o tempo de reparo até um valor máximo, conforme ilustra a Figura 27.

Nos 12 cenários mencionados na Tabela 7, os tempos de reparo ($MTTR_{op}$ e $MTTR_{tec}$) foram simulados considerando uma distribuição triangular simétrica, com valor mínimo $a = 0$ e valor máximo $b = 2 * MTTR$, portanto, com valor de pico igual ao tempo médio de reparo, ou seja $m = MTTR$.

Figura 27 – Simulação da frequência de reparos com distribuição triangular
(KELTON *et al*, 2007)

No modelo geral indicado no item 4.2.1 (Figura 16), apesar de poder ser adotada uma distribuição exponencial, visando simplificação, para caracterizar a aleatoriedade dos processos de atendimento técnico e operacional, tal distribuição não é a mais indicada para representar os processos de reparo, cujos tempos, dependendo do caso específico, podem ser melhor modelados com uma distribuição Normal, ou por uma distribuição Uniforme (com taxas de reparo igualmente distribuídas ao longo de um intervalo mínimo/máximo de tempos observados), ou até mesmo por uma distribuição Constante, em casos em que há um despacho cíclico (com horários bem definidos de remessas e retorno de material para conserto), garantindo um período exato determinístico do MTTR observado, independentemente do tempo real de reparo efetuado no centro de manutenção.

Para maior realismo, os processos de manutenção costumam ser modelados (KELTON *et al*, 2007) por distribuições que indicam um tempo mínimo típico de trabalho, com um pico na frequência mais provável de término do serviço e com um decaimento assintótico a zero, à direita da distribuição, indicando que eventos extraordinários podem demandar um grande atraso ou um tempo de tratamento muito acima da média.

Para esse tipo de situação, a **distribuição Erlang** mostra-se mais adequada, conforme mencionam os manuais de usuário da própria ferramenta Arena (ROCKWELL, 2005), cujos principais modelos de distribuição disponíveis estão reproduzidos no Anexo B.

Esses mesmos manuais indicam que, na ausência de uma curva precisa de distribuição levantada em campo, a adoção de uma distribuição Triangular, como a apresentada na Figura 27, pode estabelecer uma boa aproximação teórica para uma distribuição de tempos de manutenção de sistema, uma vez que considera tempos mínimos e máximos para o reparo. Assim, torna-se mais representativa da realidade dos processos de manutenção, em relação à adoção de outros modelos mencionados anteriormente, dados que as limitações práticas impõem tempos mínimos para acionamento das equipes, diagnóstico e tratamento do problema.

O Anexo B apresenta algumas distribuições alternativas que poderiam ser adotadas na simulação dos tempos de reparo. Caso um levantamento de dados em campo seja conduzido, pode-se promover, de forma bastante simples, a alteração da distribuição triangular, adotada neste trabalho, para outra distribuição cuja curva demonstre maior compatibilidade aos dados reais, extraídos do comportamento observado na manutenção efetuada no ambiente dos centros de controle do espaço aéreo.

6.2 Resultados Obtidos nas Simulações

Conforme as recomendações de uso da ferramenta Arena (KELTON *et al*, 2007), visando o objetivo de obter valores significativos, com 95% de confiança para as médias dos parâmetros analisados, os resultados apresentados a seguir foram obtidos a partir da execução de diversas repetições da simulação de cada cenário. Assim, um cenário é inicializado e simulado a partir de valores independentes na base de geração de números aleatórios do modelo. Tais repetições são também denominadas “replicações” ou “corridas” independentes para cada cenário.

A determinação de um número ótimo de replicações para obtenção de valores apropriados à análise depende da dispersão dos resultados de saída, e, por isso, não pode ser conhecido *a priori* no processo de simulação.

A execução de um número muito reduzido de simulações poderia gerar resultados distorcidos pela aleatoriedade do processo (em função de uma sequência específica de

eventos ocorrida naquela simulação em particular), prejudicando assim as comparações entre cenários distintos, pois as diferentes respostas poderiam estar sendo geradas pela dispersão aleatória e não pela influência direta de um parâmetro de entrada (controle).

Por exemplo, uma análise comparativa entre dois cenários, com o objetivo de avaliar o benefício do aumento no número de técnicos de manutenção para o aumento da disponibilidade do sistema, poderia indicar resultados imprecisos, caso os parâmetros de interesse de saída (disponibilidade, tamanho de filas, etc) estivessem apresentando variações dentro da margem de erro aleatória de uma única simulação. Assim, poderia se chegar a uma conclusão favorável, ou desfavorável, ao incremento do número de técnicos em decorrência da margem de erro da simulação, e não pela variação realmente provocada pelo aumento no número de técnicos.

Por outro lado, a execução de um número extremamente elevado de simulações pode comprometer o tempo de análise, sem conhecimento do número a partir do qual o grau de confiança sobre as médias deixa de ser incrementado.

Para isso, são indicados (KELTON *et al*, 2007) alguns recursos especiais incluídos na própria ferramenta Arena, destinados especificamente para análise estatística dos resultados simulados (*Process Analyser*). As facilidades dessa ferramenta fornecem, por exemplo, os valores médios de cada parâmetro de saída com suas respectivas margens de erro (“*half width*”), considerando confiança estatística de 95%.

A definição do número de replicações na simulação seguiu critério similar ao adotado em (RIBEIRO, 2003), estabelecendo como mínimo o número que gerasse convergência nas médias de disponibilidade de saída, com margens de erro menores que 0,0001. Dessa forma, os resultados apresentados neste capítulo foram obtidos a partir da execução mínima de 50 replicações dos cenários de grande porte (GXX)¹¹, 60 replicações para os cenários de médio porte (MXX) e 100 replicações para os cenários de pequeno porte (PXX).

¹¹ Conjunto dos 4 cenários: GAA, GAB, GBA e GBB.

6.2.1 Resultados de Disponibilidade dos Cenários de Pequeno Porte

A Tabela 9 apresenta os resultados da simulação dos cenários de pequeno porte (PXX), com 5 posições operacionais, onde podem ser verificadas inicialmente as quatro combinações para alta ou baixa confiabilidade/manutenibilidade: PAA, PBA, PAB, PBB, nas linhas 1 a 4 da tabela. Essa tabela apresenta uma linha para cada cenário simulado, indicando na coluna “REPS” o total de replicações para os 5 anos de simulação considerados. Conforme as definições apresentadas no item 6.1.1, as entradas (“**Controls**”) estão representadas nas colunas em que são variados os parâmetros de interesse, por exemplo o número de controladores, técnicos, assim como os tempos médios de falhas e reparo. As saídas do modelo estão representadas na coluna da direita (“**Responses**”), no qual se destaca o principal parâmetro de interesse que é a disponibilidade nominal, que ilustra a possibilidade do sistema operar abaixo de sua capacidade nominal, conforme define o item 6.1.1.

Para os cenários de pequeno porte foram executadas 100 replicações de um mesmo intervalo de simulação, com 5 anos de operação ininterrupta, ou 2.628.000 minutos.

Nesses cenários, pode-se verificar que, mesmo na presença de apenas um técnico e um operador (controlador extra disponível para operação degradada), os cenários de alta manutenibilidade geram disponibilidade melhor que 0,9999, sendo que as médias dos tamanhos das filas são desprezíveis.

Tabela 9 – Resultados dos cenários de pequeno porte “PXX”

	Scenario Properties				Controls					Responses					
	S	Name	Program File	Reps	MTTF pos	MTTR op	MTTR tec	Controlador	Técnico	Média da fila op.	Média da fila téc.	Máx. da fila op.	Máx. da fila téc.	Disponibilidade global	Disponibilidade nominal
1		PAA_1D_1T	28 : Cenários_1	100	200	6	30	1	1	0.000	0.000	0.920	0.010	0.9995	1.0000
2		PBA_1D_1T	28 : Cenários_1	100	50	6	30	1	1	0.000	0.000	1.110	0.420	0.9980	1.0000
3		PAB_1D_1T	28 : Cenários_1	100	200	120	1440	1	1	0.001	0.001	1.530	0.820	0.9862	0.9995
4		PBB_1D_1T	28 : Cenários_1	100	50	120	1440	1	1	0.018	0.009	2.780	1.750	0.9456	0.9929
5		PBB_1D_2T	28 : Cenários_1	100	50	120	1440	1	2	0.018	0.000	2.760	0.610	0.9464	0.9932
6		PBB_2D_2T	28 : Cenários_1	100	50	120	1440	2	2	0.001	0.000	1.600	0.610	0.9486	0.9941
7		PBB_4D_2T	28 : Cenários_1	100	50	120	1440	4	2	0.000	0.000	0.000	0.610	0.9487	0.9941
8		PBBB_1D1T	3 : Cenário_4_P	100	50	120	1440	1	1	0.028	0.014	3.090	1.950	0.9419	0.9990
9		PMB_1D_1T	28 : Cenários_1	100	100	120	1440	1	1	0.005	0.002	2.100	1.170	0.9725	0.9981

Em seguida, podem ser observados também alguns cenários adicionais para ilustração dos efeitos do aumento do número de recursos. Os cenários das linhas 5, 6 e 7, indicam o incremento da disponibilidade do sistema a partir da alocação de mais operadores e técnicos em relação ao cenário PBB de referência, no qual existem 5 posições

operacionais (para uma capacidade nominal de 4, ou seja, redundância de 25%), com 1 operador e 1 técnico.

Nesse caso, o gráfico da Figura 28 evidencia que não há melhoria de disponibilidade do sistema a partir da alocação de mais que 2 operadores ou 2 técnicos. Isso ocorre porque a partir de 2 recursos de atendimento técnico / operacional, as filas deixam de ser formadas, ficando o tempo de indisponibilidade restrito à relação de parâmetros de confiabilidade e reparabilidade do cenário.

Figura 28 – Melhoria da disponibilidade por aumento de operadores e técnicos

Nessa situação, pode-se então ilustrar a análise de alternativas para incremento da disponibilidade do sistema, por meio do aumento da confiabilidade e redução nos tempos de reparo, ou por meio do aumento das redundâncias operacionais.

No cenário da linha 9 da Tabela 9, fica evidenciado o efeito da melhoria da confiabilidade (cenário PMB - onde foi duplicado o valor do MTTF global para 100h), equivalente a uma taxa típica mencionada anteriormente no item 6.1.3. Nesse caso, verifica-se aumento da disponibilidade nominal para 0,9981, conforme a Figura 29.

**Incremento da disponibilidade de um cenário de pequeno porte
(PBB)
com o aumento da Confiabilidade
(para demanda nominal de 4 posições operacionais)**

Figura 29 – Melhoria da disponibilidade por aumento da confiabilidade do sistema

No entanto, há situações – após a aquisição e instalação dos sistemas – em que pode se tornar bastante complexo, ou custoso, um processo de melhoria de confiabilidade dos sistemas já implantados. Da mesma forma, pode haver limitação para redução de taxas de reparo, caso essas tenham atingido um valor ótimo.

Assim, finalmente, pode-se verificar também a alternativa de incremento de disponibilidade por meio do aumento do nível de redundância das posições operacionais. No caso ilustrado, para atender à mesma demanda nominal de 4 posições em operação normal, o cenário “P6BB” considera um sistema com o total de 6 posições, ou seja, com redundância de 50%.

Dessa forma, a linha 8 da Tabela 9 indica crescimento da disponibilidade para o nível de 0,9990, conforme ilustra a Figura 30 demonstrando assim que o aumento de redundância seria uma alternativa mais eficaz para melhoria da disponibilidade, comparativamente ao aumento de confiabilidade ou ao aumento do efetivo de operadores ou técnicos.

O Apêndice C apresenta os resultados gráficos obtidos nas simulações desse modelo, referente às comparações desses dois cenários.

**Incremento da disponibilidade de um cenário de pequeno porte (PBB)
com o aumento da Redundância
(para demanda nominal de 4 posições operacionais)**

Figura 30 – Melhoria da disponibilidade por aumento da redundância

6.2.2 Resultados de Disponibilidade dos Cenários de Médio Porte

A Tabela 10, a seguir, apresenta os resultados da simulação dos cenários de médio porte (MXX), com 15 posições operacionais. Para esse cenários de médio porte foram executadas 60 replicações de um intervalo de simulação de 5 anos de operação, ou 2.628.000 minutos.

Nesses cenários, pode-se verificar que, mesmo na presença de apenas um técnico e um operador (controlador/supervisor disponível para operação degradada), os cenários de alta confiabilidade ou alta manutenibilidade geram disponibilidade melhor que 0,9999.

Tabela 10 – Resultados dos cenários de médio porte “MXX”

Scenario Properties				Controls					Responses					
S	Name	Program File	Reps	MTTF pos	MTTR op	MTTR tec	Controlad or	Tecnico	Média da fila op.	Média da fila téc.	Máx. da fila op.	Máx. da fila téc.	Disponibilidade global	Disponibilidade nominal
1	MAA_3D_2T	6 : Cenários_5a	60	200	6	30	3	2	0.000	0.000	0.000	0.000	0.9994	1.0000
2	MBA_3D_2T	6 : Cenários_5a	60	50	6	30	3	2	0.000	0.000	0.000	0.017	0.9976	1.0000
3	MAB_3D_2T	6 : Cenários_5a	60	200	120	1440	3	2	0.000	0.000	0.733	0.650	0.9844	1.0000
4	MBB_1D_1T	6 : Cenários_5a	60	50	120	1440	1	1	0.302	0.127	6.433	3.850	0.9167	0.9951
5	MBB_2D_1T	6 : Cenários_5a	60	50	120	1440	2	1	0.023	0.136	4.083	4.000	0.9313	0.9979
6	MBB_2D_2T	6 : Cenários_5a	60	50	120	1440	2	2	0.024	0.009	4.117	2.383	0.9386	0.9988
7	MBB_3D_2T	6 : Cenários_5a	60	50	120	1440	3	2	0.002	0.008	2.850	2.167	0.9400	0.9990
8	MBB_3D_3T	6 : Cenários_5a	60	50	120	1440	3	3	0.002	0.000	2.967	1.150	0.9402	0.9990
9	MBB_4D_3T	6 : Cenários_5a	60	50	120	1440	4	3	0.000	0.001	1.917	1.150	0.9403	0.9990
10	MBB_6D_5T	6 : Cenários_5a	60	50	120	1440	6	5	0.000	0.000	0.083	0.017	0.9404	0.9991
11	MBB_12D_12	6 : Cenários_5a	60	50	120	1440	12	12	0.000	0.000	0.000	0.000	0.9404	0.9991

Os cenários das linhas 4 a 11 da Tabela 10 indicam o incremento da disponibilidade do sistema a partir da alocação de mais operadores e técnicos, em relação ao cenário MBB de referência, no qual existem 15 posições operacionais (para uma capacidade nominal de 12 posições em operação normal, ou seja, com redundância de 25%).

Para esses casos, o gráfico da Figura 31 evidencia que não há melhoria de disponibilidade do sistema a partir da alocação de mais que 3 operadores e 2 técnicos, e que valida o dimensionamento das equipes, conforme foi estabelecido *a priori* para o cenário de médio porte, no item 6.1.3.

Isso ocorre pelo mesmo motivo indicado no caso de pequeno porte, quando as filas deixam de ser formadas, ficando o tempo de indisponibilidade restrito à relação de parâmetros de confiabilidade e reparabilidade do cenário.

Figura 31 – Melhoria da disponibilidade no cenário MBB com aumento de pessoal

6.2.3 Resultados de Disponibilidade dos Cenários de Grande Porte

A Tabela 11 apresenta os resultados da simulação dos cenários de grande porte (“GXX”), para as quais foram executadas 50 replicações do mesmo intervalo de simulação, com 5 anos de operação, ou 2.628.000 minutos.

Tabela 11 – Resultados dos cenários de grande porte “GXX”

	Scenario Properties				Controls					Responses					
	S	Name	Program File	Reps	MTTF pos	MTTR op	MTTR tec	Controlador	Tecnico	Média da fila op.	Média da fila téc.	Máx. da fila op.	Máx. da fila téc.	Disponibilidade global	Disponibilidade nominal
1		GAA_6D_3T	7 : Cenários_9a	50	200	6	30	6	3	0.000	0.000	0.000	0.000	0.9994	1.0000
2		GBA_6D_3T	7 : Cenários_9a	50	50	6	30	6	3	0.000	0.000	0.000	0.000	0.9975	1.0000
3		GAB_6D_3T	7 : Cenários_9a	50	200	120	1440	6	3	0.000	0.000	0.040	0.400	0.9838	1.0000
4		GBB_1D_1T	7 : Cenários_9a	50	50	120	1440	1	1	3.752	0.742	16.860	7.860	0.8091	0.9559
5		GBB_2D_1T	7 : Cenários_9a	50	50	120	1440	2	1	0.218	1.158	7.300	9.140	0.8986	0.9957
6		GBB_2D_2T	7 : Cenários_9a	50	50	120	1440	2	2	0.249	0.080	8.020	4.220	0.9288	0.9995
7		GBB_3D_2T	7 : Cenários_9a	50	50	120	1440	3	2	0.038	0.084	5.320	4.300	0.9349	0.9998
8		GBB_3D_3T	7 : Cenários_9a	50	50	120	1440	3	3	0.038	0.011	5.400	2.900	0.9367	0.9998
9		GBB_4D_3T	7 : Cenários_9a	50	50	120	1440	4	3	0.006	0.011	3.960	2.880	0.9378	0.9999
10		GBB_6D_3T	7 : Cenários_9a	50	50	120	1440	6	3	0.000	0.011	2.100	2.940	0.9379	0.9999
11		GBB_6D_5T	7 : Cenários_9a	50	50	120	1440	6	5	0.000	0.000	2.040	0.800	0.9383	0.9999
12		GBB_8D_5T	7 : Cenários_9a	50	50	120	1440	8	7	0.000	0.000	0.120	0.020	0.9382	0.9999
13		GBB_14D_10	7 : Cenários_9a	50	50	120	1440	16	14	0.000	0.000	0.000	0.000	0.9382	0.9999
14		GMB_1D_1T	7 : Cenários_9a	50	100	120	1440	1	1	0.377	0.150	7.680	4.420	0.9523	0.9999
15		G32BB_1D1T	1 : Cenário_12_	50	50	120	1440	1	1	4.995	0.838	18.500	8.080	0.7799	0.9626

Nos cenários básicos propostos para simulação (linhas 1 a 3, e 10, da Tabela 11), foram considerados 6 operadores e 3 técnicos.

Nessa situação, pode-se verificar, na Figura 32, que o limite de disponibilidade derivado do acréscimo de equipes fica estabilizado, a partir de 4 operadores e 3 técnicos, quando se atinge a disponibilidade nominal de 0,9999 (linha 9 da Tabela 11).

Esse resultado, verificado nas linhas 4 a 13 da Tabela 11, permite efetuar uma revisão, para menor, sobre o dimensionamento de equipe definido *a priori* para o cenário de grande porte, no item 6.1.3, reduzindo, portanto, de 6 para 4, o número de operadores disponíveis para atendimento às eventualidades de operação degradada.

Figura 32 – Melhoria da disponibilidade no cenário GBB com aumento de pessoal

Voltando, nesse caso GBB, a considerar as alternativas de incremento da disponibilidade por meio do aumento da confiabilidade ou por aumento de redundância, a Figura 33 indica a alternativa de incremento de disponibilidade por meio do aumento do nível de redundância de posições operacionais.

Pode-se verificar esses benefícios, relativamente ao cenário na linha 4, pois mantendo apenas 1 operador e 1 técnico, o sistema passa a ter a disponibilidade elevada de 0,9559 para 0,9626, em decorrência da elevação da redundância de 6 para 8 posições excedentes. Assim, para atender à mesma demanda nominal por 24 posições em operação normal, o cenário G32BB considera um sistema com o total de 32 posições, significando redundância de cerca de 33%.

**Incremento da disponibilidade de um cenário de grande porte (GBB)
com o aumento da Redundância
(para demanda nominal de 24 posições operacionais)**

Figura 33 – Crescimento da disponibilidade de cenário GBB por aumento da redundância de 6 para 8 posições operacionais

No cenário da linha 14 da Tabela 11, pode-se também verificar o efeito da melhoria da confiabilidade (cenário GMB - onde foi duplicado o valor do MTTF global para 100h). Nesse caso, a disponibilidade nominal pode ser elevada de 0,9981 para 0,9999, conforme indica a Figura 34. Este é o caso de exemplo aplicável a sistemas em fase de especificação ou projeto, onde se constata que um aumento de confiabilidade traria efeitos melhores à operação, relativamente à alternativa analisada de ampliação da redundância.

**Incremento da disponibilidade de um cenário de pequeno porte (GBB)
com o aumento da Confiabilidade
(para demanda nominal de 24 posições operacionais)**

Figura 34 – Melhoria da disponibilidade por aumento da confiabilidade do sistema

6.3 Considerações Finais deste Capítulo

Este capítulo apresentou alguns exemplos de emprego do modelo descrito no Capítulo 5, ilustrando a análise de disponibilidade para centros de pequeno, médio e grande porte. Nos casos apresentados, foi possível indicar alguns tipos de resultados derivados da análise, por exemplo, permitindo visualizar as alternativas de dimensionamento de equipes, bem como as possibilidades de incremento da disponibilidade dos sistemas a partir do aumento do nível de redundâncias previstas.

7 Conclusão

Este capítulo apresenta os resultados do trabalho desenvolvido nesta pesquisa, mencionando o modelo proposto e o método para o cálculo de disponibilidade de sistemas computacionais dos centros de controle do espaço aéreo, com potenciais benefícios ao ciclo de vida do projeto desses sistemas.

Esse trabalho de pesquisa apresenta uma conceituação geral de temas de interesse ao estudo da confiabilidade de sistemas críticos da área de Controle do Espaço Aéreo, apresentando referências sobre análises de risco, confiabilidade e disponibilidade nos processos de especificação e aquisição de sistemas empregados nos centros de controle do espaço aéreo, tanto em aplicações civis quanto em aplicações militares.

O principal resultado desse trabalho é a proposição de um modelo de análise de disponibilidade para Centros de Controle do Espaço Aéreo, a partir de recursos analíticos de uma rede fechada de filas. Esse modelo, apresentado no Capítulo 5, visa gerar contribuições diretas para o dimensionamento dos sistemas computacionais desses Centros, em função dos efetivos de operação e manutenção. O modelo pode ser adotado para análises de disponibilidade, com utilidade tanto para os projetistas (Indústria), responsáveis pelas fases de especificação, projeto e implantação dos sistemas, quanto para os operadores (Autoridades Aeronáuticas), responsáveis pelas fases de concepção, certificação, operação e manutenção dos Centros de Controle.

Uma vez compreendida a aplicação prática do modelo, detalhada no Capítulo 6, o mesmo processo pode ser reproduzido para análise de outras arquiteturas similares de sistemas de controle do espaço aéreo, visando estabelecer um dimensionamento adequado de equipes, compatível com os parâmetros de confiabilidade e o nível de degradação eventual dos serviços resultante da indisponibilidade do sistema. As simulações desenvolvidas na ferramenta Arena permitem comparar cenários de interesse, explorando suas facilidades de análise estatística para obtenção de resultados sobre o comportamento da disponibilidade operacional desses centros.

Nos cenários apresentados, foram admitidos parâmetros de confiabilidade típicos de especificações formais, porém as mesmas simulações podem ser conduzidas para outros valores específicos de confiabilidade que venham a ser levantados em sistemas reais, em quaisquer centros de controle do espaço aéreo de interesse.

Dessa forma, a utilização do modelo apresentada no Capítulo 6 deste trabalho serve de exemplo prático, que pode auxiliar o emprego do modelo proposto nesta pesquisa para instalações reais, existentes ou em fase de projeto.

Assim, este trabalho visa favorecer o uso do modelo apresentado como ferramenta de avaliação no dimensionamento de equipes, definição de parâmetros de projeto para a confiabilidade e níveis de redundâncias desejados, em função da disponibilidade exigida na aquisição dos sistemas de controle do espaço aéreo.

7.1 Trabalhos Futuros

Este trabalho torna-se uma proposição inicial para desenvolvimento de estudos de dimensionamento de equipes operacionais e de manutenção dos órgãos de Controle do Espaço Aéreo, cujos parâmetros de alocação ou de restrição de equipes podem ser fatores determinantes à imposição das características de disponibilidade e confiabilidade esperadas para os sistemas em cada tipo de centro (APP, ACC, COpM, etc.).

Podem ser incluídas, nesses estudos futuros, as devidas considerações de detalhamento sobre os sistemas de apoio específicos (servidores, aplicações, infra-estrutura COTS utilizada, etc.), assim como sobre as facilidades inerentes aos serviços automatizados desempenhados nas posições de controle (equipamentos e software aplicativo dos consoles de operação). Esse sentido de aplicação do modelo se justifica quando, a partir das limitações nos efetivos de pessoal, deseja-se estabelecer os níveis de redundância técnica para que o sistema atinja a disponibilidade especificada.

De forma análoga, outras análises também poderão ser consideradas, visando o emprego do modelo no sentido oposto, onde eventuais limitações de engenharia, relativas à dificuldade técnica ou restrições de custos para incremento dos índices de confiabilidade, podem ser fatores determinantes para o dimensionamento de equipes operacionais e de manutenção nesses tipos de centros computacionais, de forma a garantir a continuidade operacional dos sistemas computacionais, garantindo os níveis de prestação dos serviços dentro dos níveis de segurança, qualidade e capacidade nominal especificada para os serviços de tráfego aéreo ou defesa aérea.

Assim, alguns temas vislumbrados de pesquisas futuras, com interesses complementares ou derivados deste trabalho, são:

- Realização de análises de disponibilidade de centros de controle existentes, com vistas ao dimensionamento de equipes técnicas e operacionais ou para adequação dos níveis de redundâncias existentes;
- Aplicação do modelo, de forma mais restrita, na avaliação de desempenho de funções automatizadas do sistema (disponibilidade de itens críticos de software);
- Extensão do modelo de filas mencionado no item 5.3, de forma a permitir avaliação de desempenho operacional dos centros (não limitada aos sistemas computacionais) , bem como estudos de qualidade dos serviços (QoS) prestados pelos centros de controle do espaço aéreo.

7.2 Considerações Finais

Destaca-se que o foco deste trabalho não foi desenvolvimento de um estudo específico, voltado à avaliação numérica de nenhum centro real existente. No entanto, os exemplos aqui elaborados permitem que projetistas e as Autoridades Aeronáuticas desenvolvam estudos específicos, com base no modelo apresentado, no interesse de quaisquer centros de controle do espaço aéreo, visando o aperfeiçoamento continuado dessas instalações, nos pontos de vista gerencial, funcional e técnico.

A contribuição esperada dos exemplos de aplicação apresentados no Capítulo 6 deste trabalho é incentivar a reprodução e uso desse modelo em sistemas reais, possibilitando a adoção de um método formal de análise de disponibilidade, com uma ferramenta de simulação que permite realizar comparações quantitativas entre estratégias de melhoria de confiabilidade, adequação do efetivo de pessoal técnico e operacional, ou de condições de redundância projetadas.

A partir da coleta de dados reais de taxas de falhas e de reparos em campo, nos centros de controle existentes, civis e militares, tais comparações e resultados obtidos podem integrar-se às etapas de engenharia de requisitos de confiabilidade inerentes ao ciclo de projeto e aquisição desses sistemas computacionais do segmento aeronáutico.

8 Referências

- ANTONIOL, G.; CIMITILE, A.; DI LUCCA, G.; DI PENTA, M. **Assessing Staffing Needs for a Software Maintenance Project through Queuing Simulation**. IEEE Transactions on Software Engineering, Vol. 30, No. 1, January 2004.
- ASSIS, J. C. **Interceptação e Abate de Aeronave: Considerações sobre a Lei nº 9.614, de 05.03.1998**. Acesso à página da CESDIM da Internet em julho de 2007: <http://www.cesdim.org.br/temp1.aspx?PaginaID=82>
- CHAUÍ, M. **Introdução à História da Filosofia: dos Pré-Socráticos a Aristóteles**. Volume 1, pg 104. Brasiliense, São Paulo, 1994.
- DECEA. **ICA 100-12 Tráfego Aéreo: Regras do Ar e Serviços de Tráfego Aéreo**. Instrução do Comando da Aeronáutica, Departamento de Controle do Espaço Aéreo, Rio de Janeiro, 2006.
- DECEA. **ICA 100-22 Tráfego Aéreo: Serviço de Gerenciamento de Fluxo de Tráfego Aéreo**. Instrução do Comando da Aeronáutica, Departamento de Controle do Espaço Aéreo, Rio de Janeiro, 2007.
- DELONG, T. A.; SMITH, D. T.; JOHNSON, B.W. **Dependability Metrics to Assess Safety-Critical Systems**. IEEE Transactions on Reliability, Vol. 54, No. 3, September, 2005.
- DEPV. **IMA 100-11 Plano de Voo**. Instrução do Ministério da Aeronáutica, Diretoria de Eletrônica e Proteção ao Voo, 1985.
- DEPV. **IMA 100-13 Regras de Tráfego Aéreo para Aeronaves Militares Brasileiras**. Instrução do Ministério da Aeronáutica, Diretoria de Eletrônica e Proteção ao Voo, 1989.
- DEPV. **DMA 63-1 Telecomunicações Aeronáuticas e Controle do Tráfego Aéreo: Diretrizes Básicas para Situações de Degradação**. Diretriz do Ministério da Aeronáutica, Diretoria de Eletrônica e Proteção ao Voo, Rio de Janeiro, 1999.
- DoD. **DOD-3235.1H Test and Evaluation of System Reliability Availability and Maintainability: a Primer**. U.S. Department of Defense, Washington, DC, USA, 1982.
- DoD. **MIL-STD-882D Mishap Risk Management (System Safety)**. U.S. Department of Defense Standard Practice, Washington, DC, USA, 1998.

- DoD. **MIL-STD-961E Defense and Program-Unique Specifications Format and Content**. U.S. Department of Defense Standard Practice, Washington, DC, USA, 2003.
- DoD. **Guide for Achieving Reliability, Availability and Maintainability** U.S. Department of Defense, Washington, DC, USA, 2005.
- DONOHUE, G.; ZELLWEGER, A. (Ed.). **Air Transportation Systems Engineering – Progress in Astronautics and Aeronautics**. American Institute of Aeronautics and Astronautics, Inc. AIAA Press, 2001.
- EUROCONTROL. **Automatic Dependent Surveillance Requirements**. European Organization for the Safety of Air Navigation. August, 2002.
- FAA. **Order 7610.4K Special Military Operations**. U.S Department of Transportation, Federal Aviation Administration, Washington, DC, USA, 2004.
- FAA. **Order 7210.3U Facility Operation And Administration**. U.S Department of Transportation, Federal Aviation Administration, Washington, DC, USA, 2006a.
- FAA. **Reliability, Maintainability and Availability (RMA) HANDBOOK**. U.S Department of Transportation, Federal Aviation Administration, Washington, DC, USA, 2006b. <http://ato-p.se-apps.faa.gov/faastandards/#Recent>
- FAB. **Entenda a Lei do Tiro de Destruição**. Sítio da FAB na Internet – Decreto n° 5.144, de 19/07/2004, acessado em julho/2007. <http://www.fab.mil.br/imprensa>
- FLORES, M. C. **Reflexões Estratégicas: repensando a defesa nacional**. Cap.1 – Conservadorismo Militar e Orientação Política; Cap.4 – Desdobramentos para o Brasil. É Realizações, São Paulo, 2002.
- HERRMANN, D. Defense Industry: IEC-61508, MIL-STD-882D, DEF STAN 00-55. In: HERRMANN, D. **Software Safety and Reliability**. IEEE Computer Society Press, Los Alamitos, CA, USA, 1999.
- HORROCKS, J.; McVEIGH, M.; SNOW, J.; BALL, D.; SCHMIDT, N. **Availability Alone is Inadequate – Part 2 – A New Approach to RMA Requirements Derivation – The Journal of Air Traffic Control Association – Vol. 49 No.2**, pg. 50-56 – ATCA – Alexandria, VA, USA, 2007a.
- HORROCKS, J.; McVEIGH, M.; SNOW, J.; BALL, D.; SCHMIDT, N. **Availability Alone is Inadequate – Part 3 – Specifying RMA Requirements – The Journal of Air Traffic Control Association – Vol. 49 No.2**, pg. 57-64 – ATCA – Alexandria, VA, USA, 2007b.

- IAC. **Demanda Global** – Relatório da Subdivisão de Estudos de Demanda por Transporte Aéreo do Instituto de Aviação Civil - Departamento de Aviação Civil do Ministério da Aeronáutica. Rio de Janeiro, 1998.
- IAC. **Demanda Detalhada dos Aeroportos Brasileiros – 2005 – Vol. 1** - Relatório da Subdivisão de Estudos de Demanda por Transporte Aéreo do Instituto de Aviação Civil do Departamento de Aviação Civil. COMAER. Rio de Janeiro, 2005a.
- IAC. **Demanda Detalhada dos Aeroportos Brasileiros – 2005 – Vol. 2** - Relatório da Subdivisão de Estudos de Demanda por Transporte Aéreo do Instituto de Aviação Civil do Departamento de Aviação Civil. COMAER. Rio de Janeiro, 2005b. (Publicações da ANAC na página <http://www.anac.gov.br/biblioteca/publicacoes.asp>)
- ICAO. **Doc 4444-RAC/501 – Rules Of The Air And Air Traffic Service. Procedures For Air Navigation Services**. International Civil Aviation Organization, Montreal, 1996.
- ICAO. **Automatic Dependent Surveillance – Broadcast (ADS-B) Concept of Use**. International Civil Aviation Organization, Montreal, 2003.
- IEEE. **IEEE 829 - Standard for Software Test Documentation**. The Institute of Electrical and Electronic Engineers. IEEE Computer Society, New York, 1998.
- JACKSON, Y.; TABBAGH, P.; GIBSON, P.; SEGLIE, E. **The New Department of Defense (DoD) Guide for Achieving and Assessing RAM**. In Annual Reliability and Maintainability Symposium - RAMS 2005 Tutorial Notes. IEEE, 2005.
- JAIN, R. **The Art of Computer Systems Performance Analysis: Techniques for Experimental Design, Measurement, Simulation and Modeling**. John Wiley & Sons, Inc. 1991
- JOHNSON, B. W. **Design and Analysis of Fault-Tolerant Digital Systems**. Massachusetts. Addison-Wesley Publishing Company, Inc. 1989
- KELTON, W. D.; SADOWSKI, R.; STURROCK, D. **Simulation with Arena**. McGraw-Hill Series in Industrial Engineering and Management Science, Fourth Edition, New York, 2007
- LEVESON, N. G. **Safeware – System Safety and Computers. A Guide to Prevent Accidents and Losses Caused by Technology**. (System Safety; Accident and Human Error Models) Addison-Wesley Publishing, Company, Inc. 1995.
- LYU, M. Best Current Practice of SRE. In: LYU, M. **Handbook of Software Reliability Engineering** - McGraw Hill, 1996.

- MENASCÉ, D., ALMEIDA, V., DOWDY, L. **Performance by Design – Computer Capacity Planning by Example** (Case Study III: A Data Center; Markov Models; Generalized Birth-Death Models). Prentice Hall PTR, NJ, USA, 2004.
- MOD, **Defence Standard 00-55 – Requirements for Safety Related Software in Defence Equipment (Part 1) – Issue 2 – 01 August 1997**. Ministry of Defence, UK, 1997
- MOD, **Defence Standard 00-25 – Human Factors for Designers of Systems**. Ministry of Defence, UK, 2004
- MOD, **Defence Standard 00-56 – Safety Management Requirements for Defence Systems – Issue 4 – 01 June 2007**. Ministry of Defence, UK, 2007
- MUSA, J. D., IANNINO, A., OKUMOTO, K. **Software Reliability - Measurement, Prediction, Application** (Failures and Faults; Software Reliability Modeling). McGraw-Hill, 1987.
- NATO. **Commercial off-the-shelf (COTS) Software Acquisition Guidelines and COTS Policy Issues**. Communication and Information Systems Agency – NATO – 1st revision, 10 January 1996.
- NEAPOLITAN, R. E. **Learning Bayesian Networks** – Inference; Probabilities Relationships pg. 69-180 – Prentice Hall. New Jersey, USA – 2004
- OLIVEIRA, I. R. **Análise de Risco do Espaçamento Temporal Aerotransportado por meio de um Modelo em Rede de Petri Estocástica e Dinamicamente Colorida**. Tese (Doutorado) - Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Computação e Sistemas Digitais, 2007
- PIZZO, W. N.; CUGNASCA, P. S. **Aplicação da Teoria das Filas para a Avaliação de Disponibilidade em Sistemas de Controle do Espaço Aéreo**. In: V Simpósio de Transporte Aéreo (SITRAER), 2006, Brasília - DF. Trabalhos apresentados no V Simpósio de Transporte Aéreo (SITRAER), v. 1. p. 305-314, São Paulo – SP, ed. por L. Weigang e E. Santana, 2006.
- PIZZO, W. N.; CUGNASCA, P. S. **Application of Queuing Theory for Availability Assessment in Airspace Control Systems**. Journal of the Brazilian Air Transportation Research Society, v. 3, p. 53-65, ISBN: 1808331, São Paulo, 2007.
- QUÍRICO, T. F. **Lei do Abate: Problema ou Solução?** Documento de 27/10/2002, colocado no sítio da FAB em Nov/2002 e acessado na página de notícias do sítio Defesa@Net na Internet (defesanet.com.Br) em julho de 2007, no seguinte endereço: <http://defesanet.web.terra.com.br/noticia/leidoabate/>

- RIBEIRO, F. R. **Modelo de Simulação para Análise Operacional de Pátio de Aeroportos**. Dissertação (Mestrado) - Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia Naval e Oceânica, São Paulo, 2003.
- ROCKWELL Software, **Arena User's Guide**, Online book: Publication ARENA-UM001B-EN-P, October, 2005 – In: KELTON, W. D.; SADOWSKI, R.; STURROCK, D. **Simulation with Arena**. McGraw-Hill Series in Industrial Engineering and Management Science, Fourth Edition, New York, 2007
- RUGGIERO, W. V. **Teoria das Filas e Avaliação de Desempenho de Sistemas Computacionais**. Apostilas do Programa de Pós-Graduação em Engenharia Elétrica (PCS-5804). Laboratório de Arquitetura de Redes de Computadores (LARC). Escola Politécnica da USP, 1997.
- SHOOMAN, M. L. **Reliability of Computer Systems and Networks** (Software Development Life Cycle; Modelos de Markov de Confiabilidade e Disponibilidade). John Wiley and Sons Inc., New York, USA, 2002.
- STOREY, N. **Safety Critical Computer Systems**. (Risk Analysis – DEF STAN 00-56 / IEC 61508) Prentice Hall, 1996
- TRIBBLE, A. C., MILLER, S. P. **Software Intensive Systems Safety Analysis**. IEEE A&E Systems Magazine, October 2004.
- WEBER, T. S. **Tolerância a Falhas: Conceitos e Exemplos**. Programa de Pós-Graduação em Computação – Instituto de Informática. UFRGS, 2006.
- YE, F.; KELLY, T. **COTS Product Selection for Safety-Critical Systems**. In: 3rd International Conference on COTS-Based Software Systems, ICCBSS 2004, CA. USA. Lecture Notes in Computer Sciences. v. 2959 p. 53-62, Springer Berlin/Heidelberg, 2004. <http://www.springerlink.com/content/0pawkx4ypdy1h1yc/>

APÊNDICES

APÊNDICE A – Cálculo de Confiabilidade para Sistemas de Controle Aéreo

APÊNDICE B – Confiabilidade de Software (Aplicação de modelagem Log-Poisson)

APÊNDICE C – Implementação dos Cenários de Simulação na Ferramenta Arena

APÊNDICE A

Cálculo de Confiabilidade para Sistemas de Controle Aéreo

1- Exemplo de Modelo Combinatório (Sistemas Série-Paralelo)

A partir dos conceitos de análise combinatória no cálculo de confiabilidade de sistemas (SHOOMAN, 2002), apresenta-se a seguir um exemplo de cálculo de disponibilidade para sistemas computacionais empregados no controle de tráfego aéreo de uma área terminal, conforme arquitetura padronizada indicada na Figura 35, que considera as redundâncias recomendadas (FAA, 2006a) para os módulos servidores, posições operacionais, redes locais e de longa distância (LAN e WAN) para acesso aos radares, acesso direto a radar (ADR) e acesso aos centros adjacentes, sendo composta pelos subsistemas descritos a seguir:

- a) Subsistema de Tratamento de Dados Radar (STR): responsável por manter atualizada a situação aérea de síntese, a partir dos dados recebidos dos radares componentes do conjunto de sensores de vigilância do APP;
- b) Subsistema de Tratamento de Planos de Vôo (STP): responsável pelo processamento dos dados de planos de vôo, esse subsistema fornece informações de suporte à decisão dos controladores, relativas aos tráfegos sob controle, realizando os cálculos necessários para atualização e difusão das informações dos planos de vôo, com os aeródromos de origem e destino, tempos estimados de partida, chegada e de sobrevôo de cada elemento fixo da trajetória planejada, etc.;
- c) Subsistema de Supervisão (SUP): fornece recursos de apoio às atividades de *supervisão técnica*, responsável pelo monitoramento e registro de dados técnicos do sistema (envolvendo tarefas de inicialização, monitoramento e reconfiguração dos recursos físicos e apresentação do estado das conexões externas e das condições de funcionamento das aplicações e subsistemas), bem como apoio às atividades de *supervisão operacional* (envolvendo as configurações do ambiente operacional, alocação do pessoal a cada posição de controle, gerenciamento das condições de controle, situações de emergência, etc.);

- d) Subsistema de Visualização e Comando (CTR/ASC): responsável pela apresentação da situação aérea de síntese, respectivamente para o controlador e para o controlador assistente, com as informações de pistas, dados de radar bruto e contornos de nuvens (NUV). Responde também pelo tratamento de ordens dos operadores (*controlador/assistente*) e gestão das imagens associadas aos diversos postos operacionais;
- e) Subsistema de Gravação de Dados (SGD): responsável pela gravação dos dados e ações efetuadas no ambiente operacional, possibilitando posterior reprodução, para análise de eventos operacionais de interesse, tais como ocorrências significativas no tráfego aéreo ou monitoramento da qualidade dos serviços prestados;
- f) Subsistema de Planejamento (PLJ): responsável pelas tarefas de edição, manutenção e atualização dos aplicativos, mapas, cenários operacionais e bancos de dados do sistema;
- g) Subsistema de Tratamento de Informações Aeronáuticas (AIS): este subsistema responde pela criação, manutenção e consulta de telas apresentadas em vídeo, contendo informações aeronáuticas, meteorológicas e outras de interesse operacional para o APP, disponibilizando, aos operadores, o acesso a informações complementares de auxílio às tarefas executadas pelos mesmos.

Figura 35 – Arquitetura de sistema computacional de um APP

A análise realizada sobre a arquitetura computacional apresentada, permite identificar os caminhos críticos envolvidos na probabilidade de sucesso para completar a missão operacional do sistema de tratamento e visualização de dados (STVD) de um APP. Assim, pode-se elaborar o diagrama da Figura 36, onde se apresenta um modelo série-paralelo representativo do funcionamento bem sucedido do sistema, assim como o conjunto das relações de dependência entre componentes envolvidos na operação normal ou degradada. Não foram considerados como elemento crítico o módulo NUV.

Figura 36 – Modelo de sucesso da operação do sistema computacional de um APP

A partir desse diagrama série-paralelo, é possível identificar grandes blocos funcionais, em termos da confiabilidade do sistema, com o objetivo de se estabelecer uma taxa de falhas global, ou da função de probabilidade de cumprimento da missão operacional do sistema.

A análise e demarcação dos caminhos críticos ao funcionamento do sistema, por meio da identificação dos conjuntos de componentes necessários à operação normal do sistema (*tie-sets*), bem como daqueles conjuntos cujas falhas inviabilizam operação normal (*cut-sets*), permitem estabelecer probabilidades de sucesso da operação,

conseqüentemente estabelecendo os parâmetros de confiabilidade do sistema, conforme ilustra a Figura 37.

Figura 37 – Blocos funcionais para sucesso de missão do sistema

Para o modo de operação normal do sistema (com capacidade nominal), tem-se:

$$\lambda_{\text{Sistema}} = \lambda_{\text{RAD}} + \lambda_{\text{COM}} + \lambda_{\text{OP}} + \lambda_{\text{CTR}}$$

Onde:

RAD – refere-se ao funcionamento dos radares redundantes

COM – refere-se ao funcionamento das comunicações WAN e LAN redundantes

OP – refere-se ao funcionamento da infra-estrutura de servidores redundantes

CTR – refere-se ao funcionamento das posições de controle redundantes

Para o modo de operação local ou autônomo do APP, ou seja, em estado degradado devido à falha de comunicação com os Centros (WAN) ou falha das redes locais (LAN), servidores ou demais elementos da infra-estrutura operacional, tem-se:

$$\lambda_{\text{Modo Local}} = \lambda_{\text{RAD}} + \lambda_{\text{ADR}} + \lambda_{\text{CTR}}$$

Onde:

RAD – Refere-se ao funcionamento dos radares redundantes

ADR – Refere-se ao funcionamento do sistema sobressalente para acesso direto ao radares

CTR – Refere-se ao funcionamento das posições de controle redundantes

Esse tipo de modelo permite verificar o real benefício das redundâncias implementadas no projeto de arquitetura, assim como identificar as influências de falhas de software, de erro humano, ou das interfaces homem-máquina alocados a cada item de hardware do modelo. A influência desses itens críticos, relativos ao software e à operação humana alocados a cada item de hardware, permite estabelecer, em nível ainda mais detalhado, as correspondentes determinações quantitativas de taxas mais específicas, associando os valores numéricos na composição das taxas de falhas apresentadas anteriormente, como parte dos itens de hardware aos quais estejam alocados.

2- Confiabilidade de Posições Operacionais para um Sistema APP

A tabela seguinte contém valores de confiabilidade especificada pelos fabricantes de equipamentos típicos utilizados em instalações de sistemas de controle de área terminal (APP), servindo de base para os exemplos de cálculo de confiabilidade de uma posição operacional e da disponibilidade dos diversos componentes do sistema.

Tabela de MTTF e MTTR dos principais equipamentos utilizados:

Equipamento	MTTF (h)	λ (10^{-6} h)	MTTR (h)	Disponib.
CPU (Ex: Workstation SUN Ultra 20)	61320	16,31	0,50	0,999992
HD 80GB - 7200RPM SATA	500000	2,00	0,50	0,999999
Unidade de DVD-CD R/W	100000	10,00	0,50	0,999995
Controlador de Vídeo Nvidia NVS285	250000	4,00	0,50	0,999998
Monitor 21 " Flat-Panel LCD	55000	18,18	0,20	0,999996
Acelerador Gráfico 2Kx2K (Ex: PVS6600)	200000	5,00	0,50	0,999997
Monitor 28" (Ex: ISIS - DP471-LCD, 28")	33790	29,59	1,00	0,999970
Thermal printer, strip FPV	8000	125,00	0,20	0,999975
Dual-Port Async/Sync Serial WIC	280000	3,57	0,30	0,999998
Impressora (Ex: HP Laserjet 1320)	60000	16,67	0,20	0,999996
10/100 Ethernet Router	514526	1,94	0,60	0,999998
Switch (EX: Cisco Catalyst 500-24TT)	308482	3,24	0,50	0,999998
MODEM Banda Base DT256 MI-DX/GB	44928	22,26	0,50	0,999988
8 Port PCI-Bus serial controller (Saturn)	70800	14,12	0,50	0,999992
XP7-R PCI Expansion Chassis	70800	14,12	1,00	0,999985
Breakout box with 8 DB25M	131400	7,61	1,00	0,999992
Sub-bastidor 19" p/12 Placas UDD 4x1	100000	10,00	1,20	0,999988
Placa UDD 4x1	96360	10,38	0,10	0,999998
Master Clock - GPS Sync. 4860net	50000	20,00	0,40	0,999992
GPS satellite receiver time sync. 488B	50000	20,00	1,20	0,999976
AutoView 2015 KVM Switch,	72786	13,74	0,50	0,999993
AutoView 2015 KVM Switch module	333153	3,00	0,20	0,999999

2.1- Taxa de falhas de uma posição operacional (Assistente + Controlador)

Considerando uma posição de controle completa composta por duas estações de trabalho, com monitores de 28" (2Kx2K) para o controlador e 21" para o assistente, tem-se um modelo em série dos seis componentes principais:

$$\lambda_{\text{Posição-operacional}} = \lambda_{\text{Workstation}} + \lambda_{\text{NVIDIA}} + \lambda_{\text{monitor 21}} + \lambda_{\text{Workstation}} + \lambda_{\text{PVS}} + \lambda_{\text{monitor 28}}$$

$$\lambda_{\text{Posição-operacional}} = (16,31 + 4,00 + 18,18 + 16,31 + 5,00 + 29,59) \times 10^{-6} \text{ h}$$

$$\lambda_{\text{Posição-operacional}} = 89,39 \times 10^{-6} \text{ h}$$

$$MTTF_{\text{Posição-operacional}} = 11187 \text{ h}$$

2.2- Disponibilidade da Posição de Controle

Posição Controlador (CTR)

$$D_{\text{CTR}} = D_{\text{Wkst}} * D_{\text{pl. Gráfica}} * D_{\text{monitor}}$$

$$D_{\text{CTR}} = 0,999959$$

Posição Controlador Assistente (ASC):

$$D_{\text{ASC}} = D_{\text{Wkst}} * D_{\text{pl. Gráfica}} * D_{\text{monitor}}$$

$$D_{\text{ASC}} = 0,999986$$

Posição de Controle Operacional (CTR e ASC):

$$D_{\text{PCTA}} = D_{\text{CTR}} * D_{\text{ASC}}$$

$$D_{\text{PCTA}} = 0,999945$$

2.3- Disponibilidade das Posições de Supervisão

Posição Supervisão

$$D_{SUP} = D_{Wkst} * D_{pl. \text{ Gráfica}} * D_{monitor}$$

$$D_{SUP} = 0,999986$$

Disponibilidade das Posições Duais de Supervisão (Operacional e Técnica)

$$D_{2xSUP} = D_{SOP} + D_{STEC} - D_{SOP} * D_{STEC}$$

$$D_{2xSUP} = 0,999999$$

2.4- Disponibilidade das Posições Planejamento (PLJ)

$$D_{PLAN} = D_{Wkst} * D_{pl. \text{ Gráfica}} * D_{monitor} * D_{DVD}$$

$$D_{PLAN} = 0,999981$$

2.5- Disponibilidade dos Servidores

Disponibilidade de cada estação servidora

$$D_{RDP} = D_{Wkst} * D_{Xp7} * D_{8\text{ port}}$$

$$D_{RDP} = 0,999969$$

Disponibilidade dos servidores duais (RDP)

$$D_{2xRDP} = (D_{RDP\ 1} + D_{RDP\ 2} - D_{RDP\ 1} * D_{RDP\ 2}) * D_{Sub\ UDD} * D_{UDD}$$

$$D_{2xRDP} = 0,999985$$

Disponibilidade dos servidores de ADR

$$D_{ADR} = D_{Wkst} * D_{Xp7} * D_{8\text{ port}} * D_{Sub\ UDD} * D_{UDD}$$

$$D_{ADR} = 0,999955$$

Disponibilidade dos servidores de tratamento de planos de vôo (STP)

$$D_{FDP} = D_{Wkst} * D_{8\text{ port}}$$

$$D_{FDP} = 0,999984$$

Disponibilidade dos Servidores Duais (FDP):

$$D_{2xFDP} = (D_{FDP\ 1} + D_{FDP\ 2} - D_{FDP\ 1} * D_{FDP\ 2}) * D_{Sub\ UDD} * D_{UDD}$$

$$D_{2xFDP} = 0,999985$$

Disponibilidade de cada Servidor de Gravação de Dados (GRD):

$$D_{GRD} = D_{Wkst} * D_{HD} * D_{DVD}$$

$$D_{DARD} = 0,999986$$

Disponibilidade dos Servidores Duais de Gravação de Dados (GRD):

$$D_{2xGRD} = D_{GRD 1} + D_{GRD 2} - D_{GRD 1} * D_{GRD 2}$$

$$D_{2xGRD} = 0,999999$$

2.6- Disponibilidade das Redes de Dados

$$D_{rede} = D_{Rede 1} + D_{Rede 2} - D_{Rede 1} * D_{Rede 2}$$

$$D_{rede} = 0,999999$$

3- Planilha para Análise de Disponibilidade por Modelo de Markov

A planilha seguinte foi utilizada como solução de um modelo triplicado (3 estados) de Markov, a partir da solução da matriz A, da qual se obtêm os valores de probabilidade do sistema encontrar-se nos estados (1), (2) ou (3), para até 2000 instantes de simulação.

Disponibilidade Assintótica para Sistema com 2 Estágios de Degradação

Simulação de confiabilidade de sistema com 3 estados utilizando modelo de Markov

variáveis			
taxa de falhas	λ	0,020000	falhas por hora
taxa de reparos	μ_1	0,500000	reparos / hora (manutenção)
taxa de reparos	μ_2	0,041667	reparos / hora (op. degradada)
prob. transição	p_1	0,010000	sair de operação normal para falha
prob. transição	p_2	0,990000	sair de operação normal para degradada
prob. transição	p_3	0,050000	sair de degradada para falha
prob. transição	p_4	0,950000	sair de degradada para normal
intervalo	Δt	1,000000	horas

$P(t+\Delta t) = A \cdot P(t)$																											
$A = \begin{bmatrix} 1-\lambda.\Delta t & \mu_1.\Delta t & \mu_2.p_4.\Delta t & 0 \\ p_1.\lambda.\Delta t & 1-\mu_1.\Delta t & \mu_2.p_3.\Delta t & 0 \\ p_2.\lambda.\Delta t & 0 & 1-\mu_2.\Delta t & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$																											
$A = \begin{bmatrix} 0,980000 & 0,500000 & 0,039583 & 0,041667 \\ 0,000200 & 0,500000 & 0,002083 & 0,000000 \\ 0,019800 & 0,000000 & 0,958333 & 0,000000 \\ 0,000000 & 0,000000 & 0,000000 & 1,000000 \end{bmatrix}$																											
<table> <tr> <th>Estados</th><th>1</th><th>2</th><th>3</th><th>4</th><th colspan="2"></th></tr> <tr> <td></td><td>$P_{normal}(t)$</td><td>$P_{falha}(t)$</td><td>$P_{manual}(t)$</td><td>$P_F(t)$</td><td>$P_{disponivel}(t)$</td><td>$P_{OK}(t)+P_F(t)$</td></tr> <tr> <td>MTTF</td><td>1359,49</td><td>3,20</td><td>638,31</td><td></td><td>1997,80</td><td></td></tr> </table>							Estados	1	2	3	4				$P_{normal}(t)$	$P_{falha}(t)$	$P_{manual}(t)$	$P_F(t)$	$P_{disponivel}(t)$	$P_{OK}(t)+P_F(t)$	MTTF	1359,49	3,20	638,31		1997,80	
Estados	1	2	3	4																							
	$P_{normal}(t)$	$P_{falha}(t)$	$P_{manual}(t)$	$P_F(t)$	$P_{disponivel}(t)$	$P_{OK}(t)+P_F(t)$																					
MTTF	1359,49	3,20	638,31		1997,80																						
t_0	0,00	1,000000	0,000000	0,000000	0,000000	1,000000	1,000000																				
$t_0+\Delta t$	1,00	0,980000	0,000200	0,019800	0,000000	0,99980	0,99980																				
	2,00	0,961284	0,000337	0,038379	0,000000	0,99966	0,99966																				
	3,00	0,943746	0,000441	0,055813	0,000000	0,99956	0,99956																				
	4,00	0,927301	0,000525	0,072174	0,000000	0,99947	0,99947																				
	5,00	0,911874	0,000599	0,087527	0,000000	0,99940	0,99940																				
	6,00	0,897401	0,000664	0,101935	0,000000	0,99934	0,99934																				
	7,00	0,883820	0,000724	0,115457	0,000000	0,99928	0,99928																				
	8,00	0,871075	0,000779	0,128146	0,000000	0,99922	0,99922																				
	9,00	0,859116	0,000831	0,140053	0,000000	0,99917	0,99917																				
	10,00	0,847893	0,000879	0,151228	0,000000	0,99912	0,99912																				
	11,00	0,837360	0,000924	0,161715	0,000000	0,99908	0,99908																				
...																											
	1995,00	0,676782	0,001611	0,321607	0,000000	0,99839	0,99839																				
	1996,00	0,676782	0,001611	0,321607	0,000000	0,99839	0,99839																				
	1997,00	0,676782	0,001611	0,321607	0,000000	0,99839	0,99839																				
	1998,00	0,676782	0,001611	0,321607	0,000000	0,99839	0,99839																				
	1999,00	0,676782	0,001611	0,321607	0,000000	0,99839	0,99839																				
	2000,00	0,676782	0,001611	0,321607	0,000000	0,99839	0,99839																				

Curva de Confiabilidade com Modelo de Markov

Figura 38 – Exemplo de curva de confiabilidade de sistema com 3 estados

APÊNDICE B

Confiabilidade de Software (Aplicação de modelagem Log-Poisson)

1- Crescimento de Confiabilidade de Software

A obtenção de parâmetros de confiabilidade de software pode ser realizada por meio de processos de testes nas fases de verificação funcional de um sistema perante seus requisitos especificados. As falhas de software decorrem de defeitos pré-existentes ocorridos nas fases de especificação, projeto e implementação. É possível, em determinados casos, a adoção de um modelo básico de crescimento contínuo da confiabilidade, com número finito de ocorrência de falhas, considerando que a taxa de falhas do software decresce até tornar-se nula, significando eliminação de todos os defeitos latentes.

No entanto, para o caso mais geral das aplicações apresentadas neste trabalho, recomenda-se adoção do modelo Logaritmo-Poisson, descrito por (MUSA, 1987), no qual ocorre um crescimento assintótico da confiabilidade do software. Nesse modelo, a redução da taxa de falhas decai exponencialmente, tendendo a zero, porém sem jamais atingir a taxa nula. Fisicamente, esse modelo equivale a considerar que, mesmo promovendo a correção do defeito a cada falha manifestada, sempre haverá um número residual de defeitos não detectáveis em projetos complexos, que envolvem um universo de dados de entrada muito amplo e com perfis operacionais muito variados.

Nesse modelo, após a medição de um dado número de falhas durante o período inicial de testes, consegue-se estabelecer uma estimativa da taxa de falhas λ_p e curva de crescimento θ , para o instante de liberação do software após os testes. Essa taxa inicial pode ser utilizada para obter uma nova taxa (desejada) de falhas λ_F , após um período calculado de tempo Δt , e que equivale à necessidade de observação de um conjunto adicional de falhas $\Delta \mu$ durante esse mesmo período. Esse processo é útil para a definição do tempo de testes necessário para se atingir uma dada confiabilidade especificada para um sistema, sendo também útil, no sentido inverso, para o estabelecimento de medidas de incremento de confiabilidade após um dado período de testes. Dessa forma, uma vez conhecidos os parâmetros da curva de crescimento do

modelo Log-Poisson (θ e λ_P), podem ser relacionados: λ_F e o período adicional de tempo Δt , ou λ_F e o número adicional de falhas $\Delta\mu$, conforme segue:

$$\Delta\mu = 1/\theta \cdot \ln(\lambda_P / \lambda_F) \quad \text{e} \quad \Delta t = 1/\theta \cdot (1/\lambda_F - 1/\lambda_P)$$

A Figura 39 ilustra o modelo a partir do qual poderia ser obtido o intervalo de tempo necessário (ou o número de falhas adicionais a observar) para se atingir a taxa de falhas especificada. Inversamente, tendo o número de falhas observadas em testes adicionais, pode-se estimar um valor de λ_F , que representaria o ganho de confiabilidade decorrente da aplicação dos testes adicionais.

Figura 39 – Modelo de estimativa do crescimento de confiabilidade de software

Assim, uma vez conhecida a curva de crescimento da confiabilidade do software inicialmente testado, pode-se então calcular uma estimativa para o eventual ganho de confiabilidade. O resultado obtido é um número adicional de falhas que devem ser observadas (ou um tempo de execução) em um novo período de testes, de forma a se atingir a meta para a taxa de falhas λ_F , desejada para o software em questão.

2- Uso do Software CASRE na Estimativa de Confiabilidade de Software

A tabela a seguir ilustra um exemplo real de análise de dados, conforme apresentado na literatura (GOEL, 1979), no qual foram realizados testes de um software durante 849 dias, sendo registrados os instantes de 34 falhas:

Número da falha	Instantes de falha (dias)	Número da falha	Instantes de falha (dias)	Número da falha	Instantes de falha (dias)
1	9	13	78	25	249
2	21	14	87	26	250
3	32	15	91	27	337
4	36	16	92	28	384
5	43	17	95	29	396
6	45	18	98	30	405
7	50	19	104	31	540
8	58	20	105	32	798
9	63	21	116	33	814
10	70	22	149	34	849
11	71	23	156		
12	77	24	247		

Utilizando o software CASRE (SHOUMAN, 2002), são obtidas as estimativas de taxas de falhas do software (λ_0) e do parâmetro Θ do modelo Log-Poisson, efetuando-se o ajuste à curva, conforme ilustra a Figura 40. Nessa ferramenta, ajusta-se a curva para as 34 falhas acumuladas no tempo, conforme observado no período de testes de 849 dias.

- $\Theta = 0,148$
- $\lambda_0 = 1,141$

Figura 40 – Modelo Log-Poisson (obtenção da taxa de falhas de software λ_0)

Com o modelo de crescimento de confiabilidade ajustado à curva do modelo Log-Poisson, pode-se então estabelecer o tempo adicional de testes necessário para que, por exemplo, obtenha-se uma taxa de falhas final do software igual à metade da taxa λ_0 , observada no dia 849.

No dia 849, a taxa de falhas λ_P se obtém com o $t = 849$ dias e $\mu = 34$ falhas, como segue:

- $\lambda(t=849) = \lambda(\mu=34) = \lambda_0 \cdot e^{-\theta\mu}$
- $\lambda(34) = 1,148 \cdot e^{-0,148 \cdot 34} = 0,00745$
- $\lambda_P = 0,00745$

A taxa final que se deseja obter, neste exemplo, é metade da taxa obtida das medições efetuadas até o dia 849, ou seja:

- $\lambda_F = 1/2 \cdot \lambda_P = 0,00373$

Assim, o intervalo de tempo adicional e o número de falhas adicionais para se atingir a taxa de falhas desejada (λ_F) podem ser obtidos como segue:

- $\Delta\mu = 1/\theta \cdot \ln \lambda_P/\lambda_F \Rightarrow \Delta\mu = 6,76 \cdot \ln 2 = 6,76 \cdot 0,693 = 4,68$ falhas

Este resultado indica que, para continuar percorrendo a curva de crescimento de confiabilidade do software deste exemplo – com a meta de reduzir sua taxa de falhas à metade daquela verificada após 849 dias – **seria necessário continuar realizando os testes até que fossem encontradas 5 falhas adicionais.**

- $\Delta t = 1/\theta \cdot [1/\lambda_F - 1/\lambda_P] \Rightarrow \Delta t = 6,76 \cdot [268,46 - 134,23] = 907$ dias

Este resultado indica também que, do ponto de vista do tempo adicional para se conseguir detectar essas cerca de 5 falhas adicionais, para atingir a meta de redução da taxa de falhas do software à metade, **seria necessário continuar realizando os testes durante 907 dias adicionais.**

APÊNDICE C

Implementação dos Cenários de Simulação na Ferramenta Arena

Este apêndice apresenta alguns exemplos dos modelos implementados na ferramenta Arena 10.0 para simulação de cenários mencionados no capítulo 6 deste trabalho, bem como a planilha de apoio utilizada para registro prévio dos parâmetros de entrada que seriam simulados no ambiente Arena.

1- Cenários de Pequeno Porte (arquivo: Cenários_1a4_PXX.p)

Modelo PBB Inicial com 25% de redundância (5 posições totais)

Modelo PBB com 50% de redundância (6 posições totais)

Detalhe de cálculo da disponibilidade nominal

(Submodel interno ao processo “Operação Normal”)

2- Cenários de Grande Porte (arquivo: Cenários_9a12_PXX.p)

Modelo GBB Inicial com 25% de redundância (30 posições totais)

Modelo GBB com 33% de redundância (32 posições totais)

3- Planilha de Apoio para Definição de Parâmetros no Software Arena

A planilha seguinte foi utilizada como meio de apoio pra definição de parâmetros de entrada na ferramenta Arena. A partir de valores de dimensão do cenário de interesse, bem como dos parâmetros de confiabilidade de falhas críticas (manutenção) e não críticas (degradação) de um sistema, podem-se ajustar os percentuais p1 a p4, obtendo os valores de MTTF*, por posição a considerar na ferramenta Arena.

Cenários

Considerando reserva operacional de 25% no número de posições

Nota: editar apenas os campos escuros em verde/azul/amarelo

	total de posições operac.	escala de operadores (24hx7d)	escala de reserva (24hx7d)	escala de técnicos (24hx7d)	MTTF global(horas) Arena	
					MTTF _{sis} (alta confiab.)	MTTF _{sis} (baixa confiab.)
* Pequeno porte (4+1 posições)	5	4	1	1	40,00	10,00
total do efetivo 24x7	= 30	20	5	5		
* Médio porte (12+3 posições)	15	12	3	2	13,33	3,33
total do efetivo 24x7	= 85	60	15	10		
* Grande porte (24+6 posições)	30	24	6	3	6,67	1,67
total do efetivo 24x7	= 165	120	30	15		

Indicadores por posição

MTTF_{falha} (horas)

Ocorrências de manutenção λ.p1

MTTF_{op.} (horas)

Ocorrências operacionais λ.p2

λ da posição (ocorrências/h)

Por posição (Arena)

MTTF_{posição} (horas)

A) Alta confiabilidade

20000

0,00005

202,02

0,00495

0,005

200,00

B) Baixa confiabilidade

5000

0,0002

50,51

0,0198

0,02

50,00

p1

0,01

obs:

1,0% das ocorrências são falhas críticas que demandam a equipe de manutenção

p2

0,99

99,0% das ocorrências são falhas não-críticas atendidas pela equipe operacional

Serviço Operacional

Distribuição triangular

MTTR₁ (minutos)

μ1 (reparos/h)

MTTR₁ min (min.)

MTTR₁ máx (min.)

A) Alta manutenibilidade

6

10

3

24

B) Média manutenibilidade

30

2

15

120

C) Baixa manutenibilidade

120

0,5

60

480

Serviço Técnico

Distribuição triangular

MTTR₂ (minutos)

μ2 (reparos/h)

MTTR₂ min (min.)

MTTR₂ máx (min.)

A) Alta manutenibilidade

30

2

15

120

B) Média manutenibilidade

360

0,1666667

180

1440

C) Baixa manutenibilidade

1440

0,0416667

720

5760

p3

0,05

obs:

5,0% das ocorrências operacionais evoluem para falha e demandam manutenção

p4

0,95

95,0% das ocorrências operacionais são solucionadas e retornam à condição normal

* Nota sobre o modelo de taxa de falhas das posições operacionais:

Para as posições operacionais, o modelo de confiabilidade adotado é o de taxa de falhas constante (λ), normalmente utilizado para sistemas eletrônicos, e no qual a confiabilidade de cada posição operacional apresenta uma curva de decaimento exponencial, com tempo médio para falhar (MTTF) correspondente a $1/\lambda$.

Dessa forma, pode-se configurar a ferramenta Arena de modo a simular os eventos aleatórios de falha de cada posição operacional com a distribuição exponencial (EXPO), descrita no Anexo B. Essa distribuição é capaz de reproduzir o comportamento aleatório dessas falhas, com média MTTF (= MTBF – MTTR), conforme ilustra a Figura 9, apresentada no Capítulo 3.

ANEXOS

ANEXO A – Modelo de Nascimento e Morte - GBD. (MENASCÉ *et al*, 2004)

ANEXO B – Distribuições Disponíveis no Arena 10.0 (KELTON *et al*, 2007)

ANEXO C – Resumo Comparativo de Ferramentas de Simulação (RIBEIRO, 2003)

ANEXO A

Modelos de Nascimento e Morte (GBD)

(MENASCÉ *et al*, 2004)

Alguns modelos de Markov, chamados modelos de nascimento e morte, são muito úteis por exibirem uma solução geral. Para um sistema no estado k , que significa a presença de k usuários, apenas dois eventos podem ocorrer para que se deixe esse estado k : um “nascimento” ocorre, indicando a chegada de um novo usuário, e o sistema passa ao estado $k + 1$; ou ocorre uma “morte”, indicando a saída de um usuário, fazendo então que o sistema passe ao estado $k - 1$.

Assim, para o estado corrente k , assume-se uma taxa de chegada de novos usuários (nascimento) como λ_k e uma taxa de saída de usuários (morte) como μ_k . As taxas de nascimento e morte são, portanto, dependentes do estado no qual o sistema se encontra, conforme ilustra o diagrama de transição de estados na Figura 1A.

Dessa forma, as equações de balanço do fluxo do sistema ficam como segue:

$$\text{Vazão de entrada} = \text{Vazão de saída}$$

$$\mu_1 P_1 = \lambda_0 P_0$$

$$\lambda_0 P_0 + \mu_2 P_2 = \lambda_1 P_1 + \mu_1 P_1$$

.

$$\lambda_{k-1} P_{k-1} + \mu_{k+1} P_{k+1} = \lambda_k P_k + \mu_k P_k$$

Figura 1A – Diagrama de estados do modelo generalizado nascimento-morte
(MENASCÉ *et al*, 2004)

Após algumas manipulações algébricas, e usando a conservação de probabilidade total, $P_0 + P_1 + P_2 + \dots = 1$, a solução é obtida como segue:

$$P_0 = \left[\sum_{k=1}^{\infty} \prod_{i=0}^{k-1} \lambda_i / \mu_{i+1} \right]^{-1} \quad (1)$$

Onde o primeiro termo de somatório é definido como sendo 1. Portanto, a solução generalizada, na situação em regime, para qualquer sistema de nascimento e morte, quando no estado particular k , é:

$$P_K = P_0 = \left[\sum_{k=1}^{\infty} \prod_{i=0}^{k-1} \lambda_i / \mu_{i+1} \right]^{-1} \cdot \prod_{i=0}^{k-1} \lambda_i / \mu_{i+1} \quad , \quad \text{para } k = 1, 2, 3, \dots \quad (2)$$

Desta solução generalizada, em regime, são diretamente obtidas as expressões para outras medidas de performance indicadas a seguir:

$$\text{Utilização} = P_1 + P_2 + \dots = 1 - P_0 \quad (3)$$

$$\text{Vazão (throughput)} = \mu_1 P_1 + \mu_2 P_2 + \dots = \sum_{k=1}^{\infty} \mu_k P_k \quad (4)$$

$$\text{Tamanho da fila} = 0P_0 + 1P_1 + 2P_2 + \dots = \sum_{k=1}^{\infty} k \cdot P_k \quad (5)$$

$$\text{Tempo de resposta} = \text{tamanho da fila} / \text{vazão} = \frac{\sum_{k=1}^{\infty} k P_k}{\sum_{k=1}^{\infty} \mu_k P_k} \quad (6)$$

ANEXO B

Modelos de Distribuição Disponíveis no Software Arena 10.0

(KELTON *et al*, 2007)

A tabela a seguir, extraída da referência (KELTON *et al*, 2007), por meio do manual de usuário do software Arena - *User's Guide* (ROCKWELL, 2005), reproduz a lista das distribuições disponíveis para simulação de eventos aleatórios por meio da ferramenta Arena 10.0.

Summary of Arena's Probability Distributions

	Distribution	Parameter Values
Beta	BETA	Beta, Alpha
Continuous	CONT	CumP ₁ , Val ₁ , . . . CumP _n , Val _n
Discrete	DISC	CumP ₁ , Val ₁ , . . . CumP _n , Val _n
Erlang	ERLA	ExpoMean, k
Exponential	EXPO	Mean
Gamma	GAMM	Beta, Alpha
Johnson	JOHN	Gamma, Delta, Lambda, Xi
Lognormal	LOGN	LogMean, LogStd
Normal	NORM	Mean, StdDev
Poisson	POIS	Mean
Triangular	TRIA	Min, Mode, Max
Uniform	UNIF	Min, Max
Weibull	WEIB	Beta, Alpha

A seguir, foram também extraídas do manual de usuário do Arena - *User's Guide* (ROCKWELL, 2005), as descrições das principais distribuições disponíveis, para o caso de interesse desta pesquisa, referente ao modelamento de distribuições de tempos de reparo técnico e operacional dos sistemas de controle do espaço aéreo.

Conforme foi destacado no capítulo 6, as simulações desenvolvidas neste trabalho adotaram um modelo de distribuição Triangular, porém os levantamentos em campo poderiam registrar comportamentos, para as taxas μ_1 e μ_2 , compatíveis, por exemplo, com as distribuições Uniforme, Normal, Erlang ou Weibull, cujos modelos podem ser

facilmente alterados na ferramenta, para produção de resultados simulados com maior precisão e aderência ao caso de interesse específico.

Distribuição Uniforme:

Uniform(*a, b*) UNIFORM(Min, Max) or UNIF(Min, Max)

<i>Probability Density Function</i>
<i>Parameters</i>	The minimum (<i>a</i>) and maximum (<i>b</i>) values for the distribution specified as real numbers with $a < b$.
<i>Range</i>	$[a, b]$
<i>Applications</i>	The uniform distribution is used when all values over a finite range are considered to be equally likely. It is sometimes used when no information other than the range is available. The uniform distribution has a larger variance than other distributions that are used when information is lacking (e.g., the triangular distribution).

Distribuição Exponencial:

Exponential(β) EXPONENTIAL(Mean) or EXPO(Mean)

<i>Probability Density Function</i>
<i>Parameters</i>	The mean (β) specified as a positive real number.
<i>Range</i>	$[0, +\infty)$
<i>Applications</i>	This distribution is often used to model inter-event times in random arrival and breakdown processes, but it is generally inappropriate for modeling process delay times. In Arena's Create module, the Schedule option automatically samples from an exponential distribution with a mean that changes according to the defined schedule. This is particularly useful in service applications, such as retail business or call centers, where the volume of customers changes throughout the day.

Distribuição Normal:

Normal(μ, σ) NORMAL(Mean, StdDev) or NORM(Mean, StdDev)

**Probability
Density
Function**

Parameters The mean (μ) specified as a real number and standard deviation (σ) specified as a positive real number.

Range $(-\infty, +\infty)$

Applications The normal distribution is used in situations in which the central limit theorem applies; i.e., quantities that are sums of other quantities. It is also used empirically for many processes that appear to have a symmetric distribution. Because the theoretical range is from $-\infty$ to $+\infty$, the distribution should only be used for positive quantities like processing times when the mean is at least three or four standard deviations above 0.

Distribuição Erlang:

Erlang(β, k) ERLANG(ExpMean, k) or ERLA(ExpMean, k)

**Probability
Density
Function**

Parameters If $X_1, X_2, \dots, X_k$ are independent, identically distributed exponential random variables, then the sum of these k samples has an Erlang- k distribution. The mean (β) of each of the component exponential distributions and the number of exponential random variables (k) are the parameters of the distribution. The exponential mean is specified as a positive real number, and k is specified as a positive integer.

Range $[0, +\infty)$

Applications The Erlang distribution is used in situations in which an activity occurs in successive phases and each phase has an exponential distribution. For large k , the Erlang approaches the normal distribution. The Erlang distribution is often used to represent the time required to complete a task. The Erlang distribution is a special case of the gamma distribution in which the shape parameter, α , is an integer (k).

Distribuição Weibull:

Weibull(β , α) WEIBULL(Beta, Alpha) or WEIB(Beta, Alpha)

*Probability
Density
Function*

Parameters Shape parameter (α) and scale parameter (β) specified as positive real numbers.

Range $[0, +\infty)$

Applications The Weibull distribution is widely used in reliability models to represent the lifetime of a device. If a system consists of a large number of parts that fail independently, and if the system fails when any single part fails, then the time between successive failures can be approximated by the Weibull distribution. This distribution is also used to represent non-negative task times that are skewed to the left.

ANEXO C

Resumo Comparativo de Ferramentas de Simulação (RIBEIRO, 2003)

As tabelas a seguir reproduzem uma comparação dos recursos de diversas ferramentas de simulação, indicando algumas características que favoreceram o uso do software Arena neste trabalho.

Programas ou linguagens	Desenvolvido por	Linguagem que utiliza	Tipo simulação	Animação	Observação
<i>Bibliotecas de Programas</i>					
C++SIM, SSS, CSIM18 [73]	?	C	discreta	?	Bibliotecas em C++ para simulação de eventos discretos.
SIMJAVA [75]	?	JAVA	discreta	?	Bibliotecas em Java para simulação de eventos discretos.
<i>Ferramentas de simulação</i>					
Taylor ED [44]	F&H Simulations Inc.	4D-script	discreta ou continua	sim	Ferramenta da com arquitetura orientada a objetos para modelagem e simulação de processos de controle de negócios e aplicações industriais.
SIMUL8 [75]	Visual Thinking Intl.	?	discreta	sim	Com objetos de simulação pré-definidos e distribuições estatísticas embutidas. Também permite modelagem hierárquica.
Extend [50]	ImagineThat Inc.	ModL (parecida com C)	discreta ou continua	sim	Ambiente de simulação gráfico, com capacidade de animação, contendo bibliotecas de modelos e hierarquia para os modelos. Módulos personalizados podem ser criados com a linguagem ModL.
VisSim [81]	Visual Solutions Inc. / Mesquite Software Inc.	CSIM18	discreta ou continua	sim (gráficos das tarefas)	Linguagem visual de diagrama de blocos (orientada a processos) para simulação de dinâmica não linear e para simulação de eventos discretos. Mostra gráficos das tarefas conforme a simulação é executada.
AweSim [72]	Pritsker Corporation / Symix Systems Inc.	Visual SLAM/Visual C++	discreta ou continua	sim	Presta-se a modelos de redes, simulação de eventos discretos ou contínuos, sua arquitetura é orientada a objetos, com blocos pré-definidos. Funciona em ambiente Windows, podendo ser integrado a aplicações em outras linguagens visuais (V Basic ou Visual C).
MicroSaint [8]	Micro Analysis and Design Inc.	?	discreta ou continua	sim	Programa de simulação genérico e bastante flexível com interface gráfica do tipo diagrama de fluxo, ou rede de tarefas. Aplicações em diversas áreas (desde industrial até hospitalar).
Simprocess [97]	CACI Products Company	MODSIM III	discreta ou continua	sim	SIMPROCESS (Business Process Simulator), arquitetura hierárquica, orientada a objetos, combinando a simplicidade dos diagramas de fluxo com simulação, análise estatística, custos baseados em atividades e animação.

Programas ou linguagens	Desenvolvido por	Linguagem que utiliza	Tipo simulação	Animação	Observação
WITNESS [59]	Lanner Group	?	discreta	sim	Ambiente gráfico para elaboração de simulações voltadas para fluxo de materiais/veículos no sistema. É capaz de gerar animações em 3D ("Virtual Realit Models")
ARENA [85]	Systems Modeling Corp	SIMAN	discreta ou continua	sim	Ambiente gráfico de programação, arquitetura orientada a objetos com aplicações em virtualmente qualquer área em que se necessite da simulação. Seus objetos permitem a modelagem de sistemas nos mais variados graus de complexidade e com abordagem "top to bottom", tornando o modelo mais detalhado ou "bottom to top", agregando-se modelos menores. Arquitetura aberta (integrável a outros aplicativos via VBA). Baseado na linguagem SIMAN, criada por pessoas que participaram nas criações do SLAM e GPSS, incorporando assim as vantagens dessas linguagens. Pode ser usado para otimização em conjunto com simulação (módulo OptQuest).
Promodel [35]	Promodel Corporation	C, Pascal ou Basic (para rotinas externas)	discreta ou continua	sim	ProModel Optimization Suite é um programa de simulação orientado a objetos para avaliação, projeto ou reengenharia de sistemas logísticos, indústrias ou armazéns.
AutoMod [77]	AutoSimulations Inc.	?	discreta ou continua	sim	Permite a simulação de instalações industriais ou de armazenagem em 3 dimensões, permitindo a avaliação do funcionamento da instalação industrial e de parâmetros estatísticos de desempenho. O módulo AutoMod é o responsável pelo ambiente de modelagem e simulação, o módulo AutoStat é usado para análises estatísticas e otimização e o módulo AutoView permite a navegação na animação.
Proof [39]	Wolverine Software Corporation	n/a	discreta ou continua	sim	É um poderoso programa de animação de simulações a partir de arquivo de texto criado por programas de simulação. As simulações a serem animadas podem ser feitas com SLX, GPSS/H Extend SLAM, SIMAN, Simscript II.5, C, JAVA etc. Tem interfaces com programas de CAD ("Computer Aided Design").
Quest[9]	Deneb Robotics,	SCL (Simulation	discreta	sim	Modelo para simulação industrial com capacidade de simulações

Programas ou linguagens	Desenvolvido por	Linguagem que utiliza	Tipo simulação	Animação	Observação
	Inc.	Control Language), pode comunicar-se com programas em C			em 3D considerando as geometrias dos objetos. Integrado com ferramentas de CAD.
Alpha/Sim[21]	AlphaTech Inc.	?	discreta	sim	Baseado em redes de Petri, permite a modelagem hierárquica, em ambiente totalmente visual. Pode ser conectado a outros programas, coletando dados de filas e outros dados estatísticos automaticamente.
VSE[7]	Orca Computer Inc.	?	discreta	sim	Desenvolvido no escopo do SDME ("Simulation Model Development Environment") projeto iniciado em 1983 na Virginia Tech com financiamento da Marinha dos EUA. Totalmente orientado a objetos (e classes de objetos).
<i>Linguagens de Simulação</i>					
SLAM II [72]	?	Visual SLAM	discreta ou continua	n/a	Ver AweSim
GPSS/H [23]	Wolverine Software Corporation	GPSS	discreta	n/a	General Purpose Simulation System (GPSS). Modelos são desenvolvidos em código em formato texto, que são compilados e carregados diretamente na memória para execução, o que permite alta performance. A modelagem é baseada na interação entre processos, ou seja, o modelo descreve o fluxo de um objeto, o que garante uma leitura do código como um fluxograma do sistema modelado. Esses objetos são controlados e estatísticas são geradas como resultado da simulação. É uma linguagem amplamente difundida e tem sido usada nas mais diversas áreas.
MODSIM III [97]	CACI Products Company	MODSIM III	discreta ou continua	n/a	Linguagem para simulação tanto em arquitetura orientada a objetos como a processos. Desenvolvida para modelagem de sistemas complexos. Contém bibliotecas específicas de simulações e animação. Tem interface para o HLA ("High Level Architecture"), padrão do Departamento de Defesa dos EUA de simulação distribuída. É melhor que linguagens como JAVA ou C++ pois além de oferecer as mesmas vantagens em termos de polimorfismo, herança e encapsulamento é uma linguagem voltada para simulação.

Programas ou linguagens	Desenvolvido por	Linguagem que utiliza	Tipo simulação	Animação	Observação
Simscrip II.5 [75]	?	Simscrip II.5	discreta ou continua	n/a	Linguagem de forma livre (em inglês). Usada em diversas aplicações. O SIMMOD foi construído nessa linguagem.
SIMAN [69]	Pedgen / Systems Modeling Corporation	SIMAN	discreta e/ou continua	n/a	Desenvolvido por participantes do projeto que desenvolveu a linguagem SLAM. Seu desenvolvimento contém heranças desde o GPSS e GASP. É a linguagem base do ARENA.
<i>Programas e linguagens de simulação "web based" e distribuída</i>					
SILK[37]	ThreadTech Inc	JAVA	discreta e/ou continua	n/a	Silk é uma ferramenta de modelagem que une as características de modelagem por descrição de processos com uma linguagem orientada a objetos, com todas as vantagens que isso pode trazer (herança, encapsulamento, polimorfismo etc.). Sua grande vantagem é a possibilidade de reutilização de sub-modelos e componentes criados por outros usuários. Assim essas bibliotecas descrevendo o comportamento de determinados objetos poderiam ser coletadas na "Internet" e integradas compondo um modelo de simulação, poupando muito esforço de desenvolvimento.
SLX[38]	Wolverine Software Corporation	C	discreta e/ou continua		SLX é construído sobre os avanços dados pelo GPSS/H. Sua estrutura em diversas camadas, desde o código parecido com C até um nível médio baseado no GPSS/H até uma linguagem totalmente visual, voltada à aplicações. É compatível com o HLA ("High Level Architecture"), e possui ilimitada expansibilidade, em quaisquer dos níveis em que se deseje tal expansão, podendo assim servir de ferramenta para virtualmente qualquer tipo de modelo de simulação.
JSIM [75]		JAVA	discreta e/ou continua		Ambiente de simulação e animação baseado em JAVA . Modelos podem ser construídos graficamente com orientação a eventos ("Event-Scheduling Paradigm") ou a processos ("Process-Interaction Paradigm"). Pode acessar bases de dados para entradas ou saídas da simulação.