Yuri Maximilian Rottner Dirickson

Metodologia de Análise de Impacto em Segurança Crítica da Automação das Tarefas do Controlador de Tráfego Aéreo da Torre de Controle de Aeródromo

São Paulo
2016

Yuri Maximilian Rottner Dirickson

Metodologia de Análise de Impacto em Segurança Crítica da Automação das Tarefas do Controlador de Tráfego Aéreo da Torre de Controle de Aeródromo

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

Área de Concentração:
Engenharia de Computação

Orientador: Prof. Dr. João Batista Camargo Junior

São Paulo
2016

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

São Paulo, _____ de _____ de _____

Assinatura do autor: _____

Assinatura do orientador: _____

Catalogação-na-publicação

Dirickson, Yuri Maximilian Rottner
Metodologia de Análise de Impacto em Segurança Crítica da Automação das Tarefas do Controlador de Tráfego Aéreo da Torre de Controle de Aeródromo / Y. M. R. Dirickson -- versão corr. -- São Paulo, 2016.
98 p.

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

1.Tráfego Aéreo 2.Segurança de Tráfego 3.Sistemas de Controle de Tráfego I.Universidade de São Paulo. Escola Politécnica. Departamento de Engenharia de Computação e Sistemas Digitais II.t.

Este trabalho é dedicado a minha família e a minha esposa que sempre me apoiaram e nunca desistiram de mim.

AGRADECIMENTOS

Primeiro para a minha esposa, Karolyne, que me apoiou e ajudou nessa jornada que foi para nós dois, ambos estudantes de mestrado. Esse trabalho só foi possível ser terminado porque você estava ao meu lado, eu te amo!

Para a minha família, em especial meu pai Luiz e mãe Margarete, por serem um porto seguro nos fim de semanas estressados.

Para o meu professor e orientador, prof Dr. João Batista Camargo Jr, por ter me recebido tão respeitosa e alegremente em uma área que não tinha nada a ver com a minha, por ter me orientado e guiado nesses anos de mestrado e por ter depositado tanta confiança no meu trabalho. Ao Lúcio Vismari pela coorientação informal dada por tanto tempo, me ensinando como ser um pesquisador. Aos outros amigos e membros do GAS (Grupo de Análise de Segurança da Escola Politécnica da USP) que mesmo de longe me apoiaram nessa caminhada: prof. Dr. Paulo Cugnasca, prof. Dr. Jorge Rady, Daniel Baraldi, Débora Ribeiro, Laércio Quintanilha. Thiago Toshio, Wesley Medeiros, Antônio Vieira e Ricardo Gimenes.

Para os membros do Instituto de Controle do Espaço Aéreo, em especial ao Major J. Carlos, Ten. Cel. Barreto e Major Fernando, que sempre estiveram dispostos a colaborar com as pesquisas do GAS, seja com fornecimento de materiais, visitas e conversas esclarecedoras. Sem vocês a minha pesquisa não teria progredido.

Aos meus chefes de trabalho, Fernando Favato e Leandro Fregnani que sempre foram muito compreensivos em relação à importância do mestrado para mim.

"O universo é grande. É vasto e complicado e... ridículo e algumas vezes, bem raramente, coisas impossíveis simplesmente acontecem e nós as chamamos de milagres, e... essa é a teoria. Novecentos anos, ainda não vi nenhum, mas isso irá servir para mim."

(Doutor, The Pandorica Opens)

RESUMO

Com o crescimento contínuo na utilização da aviação como meio de transporte de pessoas e carga, o sistema de gerenciamento de tráfego aéreo (ATM) está no limite de sua capacidade. Para lidar com esse problema, a Organização de Aviação Civil Internacional (OACI), junto com diversos países membros, desenvolveu um novo conceito de ATM chamado CNS/ATM, composto de uma série de melhorias tecnológicas para melhorar a capacidade e desempenho do sistema, onde muitas dessas melhorias são automatizações de tarefas de operadores humanos, pilotos e controladores de tráfego aéreo (ATCo). Com o tempo percebeu-se que apenas avanços tecnológicos não seriam o suficiente, que era necessário uma integração maior entre todos os sistemas ATM, que garantisse uma interoperabilidade entre os sistemas. Portanto, o conceito CNS/ATM evoluiu para o conceito ATM Global, onde o planejamento de modernização se dará de forma integrada e global, incluindo muitas das melhorias previstas no conceito CNS/ATM. Essa mudança de paradigma faz surgir diversas questões de como essas mudanças impactarão no atual sistema, do ponto de vista econômico, ambiental, desempenho e segurança. Para entender os perigos envolvidos na execução dessas novas tarefas, utilizam-se diversas técnicas e modelos clássicas como a Análise de Árvores de Falhas (FTA) ou a Análise de Árvore de Erros (ETA). Essas técnicas tradicionais consideram que acidentes são causados por uma sequência de eventos de falha, todos com uma relação de causa e efeito. Essa suposição não é considerada mais suficiente para entender como acidentes acontecem nos sistemas mais atuais, onde cada vez mais eles se tornam mais complexos e mais dependentes da interação com softwares. Para lidar com essa dificuldade foram criados alguns modelos para entender acidentes utilizando a teoria de sistemas, como exemplo o Systems-Theoretic Accident Model and Proccesses (STAMP). Diversos estudo mostram que esses modelos ou métodos são capazes de representar problemas na estrutura de controle que as técnicas mais tradicionais não conseguem, inclusive incluindo fatores organizacionais na sua representação. Considerando todos esses fatos, este trabalho de investigação científica propõe uma metodologia de análise de impacto em segurança crítica da automação das tarefas dos ATCo de uma torre de comando de aeródromo (TWR). A metodologia consiste na modelagem dos perigos e acidentes envolvidas nas tarefas do ATCo da TWR utilizando o modelo sistêmico STAMP) depois na análise subsequente dos cenários antes da automação e depois da automação utilizando a técnica Systems-Theoretic Proccess Analysis (STPA), criada a partir do STAMP, para levantar os fatores causais de perigos e seus requisitos de segurança em cada cenário, de forma a ser possível obter uma comparação do que foi modificado com a automação proposta das tarefas. Para validar a metodologia, foi analisada uma tarefa do ATCo da TWR como exemplo. Espera-se obter com a metodologia proposta uma forma mais objetiva e sistêmica de obter o possível impacto em termos de segurança crítica da automação de uma tarefa específica, sendo possível então determinar qual a melhor forma

de se pensar essa automação no contexto do ATCo, podendo assim contribuir para a modernização segura do sistema ATM.

Palavras-chave: Segurança, ATC, TWR, Engenharia de Sistemas.

ABSTRACT

With the increasing growth of aviation as mode of transportation for people and cargo, the Air Traffic Management (ATM) system is on its limits. In order to cope with that, the International Civil Aviation Organization (ICAO), together with country members, developed a new ATM concept called CNS/ATM, bearing several technological improvements with the objective of enhancing capacity and performance of the system, where many of these improvements are automated tasks of human operators, pilots and air traffic controllers (ATCo). In time, it was seen that technological improvements were not enough it was necessary a greater integration between all ATM systems, which would guarantee an interoperability between them. Therefore, the CNS/ATM concept evolved to a Global ATM concept, in which the modernization plan would occur globally and integrated, including many of the improvements of the CNS/ATM concept. This paradigm shift raised several questions on how these changes would affect in the actual system from an economic, environmental, performance and safety points of view. To understand the hazards of the new tasks, several traditional techniques and models are used, like Fault Tree Analysis (FTA) and Error Tree Analysis (ETA). These traditional techniques see accidents because of a chain of failure events, all with an effect-cause relation. This assumption is no longer considered enough in order to understand how accidents occur in actual systems, which became more complexes and more software dependents. To cope with this difficulty, other models were created to understand accidents using systems theory, for example the Systems-Theoretic Accident Model and Processes (STAMP). Several studies show that these models or methods are capable of finding more problems in control structure that the traditional techniques, including organizational factors. Considering all the facts, this scientific investigation propose a methodology for analysis of the impact on safety for the automation of ATCo from Control Tower (TWR) tasks. This methodology consists in modeling the accidents and hazards of the TWR ATCo tasks using STAMP. Then the Systems-Theoretic Process Analysis (STPA) technique, created for STAMP, is used to gather all causal factors for hazards and its safety requirements in each scenario, in order to compare what changed with the automation of tasks. The objective of proposed methodology is to obtain a systemic and objective way of finding the possible impact on safety from the automation of a specific task, enabling the possibility of determining the best way of designing the automation in the context of ATCo, contributing to the safe modernization of ATM system.

Keywords: Safety, ATC, TWR, Systems Engineering.

LISTA DE ILUSTRAÇÕES

Figura 1 – Modelo Dominó 34
Figura 2 – Exemplo de Análise de Árvore de Falhas (FTA) 34
Figura 3 – Exemplo de Análise de Árvore de Eventos (ETA) 35
Figura 4 – Modelo Queijo Suíço (Swiss Chesse Model (SCM)) 36
Figura 5 – Diagrama do Functional Resonance Analysis Method (FRAM) 37
Figura 6 – Diagrama do Mapeamento de Acidentes (AcciMap) 39
Figura 7 – Visão de como acidentes acontecem segundo o Systems Theoretic Accident Model and Process (STAMP) 41
Figura 8 – Metodologia de Pesquisa 44
Figura 9 – Esquema de uma Zona de Tráfego de Aeródromo (ATZ) 51
Figura 10 – Esquema de uma Zona de Controle (CTR) 52
Figura 11 – Esquema de uma Área de Controle Terminal (TMA) 52
Figura 12 – Imagem da divisão das Regiões de Informação de Voos (FIRs) brasileiras 53
Figura 13 – Estrutura dos Componentes do Sistema ATM Global 56
Figura 14 – Diagrama de Blocos de Fluxo Funcional Melhorado (eFFBD) Controle de Aeródromo 59
Figura 15 – eFFBD Controle de Aeronaves que Deixam o Aeródromo 60
Figura 16 – eFFBD Autorização de Decolagem 61
Figura 17 – eFFBD Aeronaves chegando no Aeródromo 62
Figura 18 – eFFBD Controle de aeronaves no circuito de tráfego 63
Figura 19 – eFFBD Controle de aeronaves em Táxi 64
Figura 20 – eFFBD Seleção de Pistas em Uso 65
Figura 21 – eFFBD Escolher tipo de operação 66
Figura 22 – Fluxo de controle genérico. 68
Figura 23 – Fluxo de controle genérico com seus possíveis fatores causais. 71
Figura 24 – Esquema do Controlador 77
Figura 25 – Estrutura de Controle Manual e Possíveis Fatores Causais 84
Figura 26 – Estrutura de Controle Automatizado e Possíveis Fatores Causais 85

LISTA DE TABELAS

Tabela 1 – Causas de Acidentes Fatais em Porcentagem 26
Tabela 2 – Quadro Teórico 46
Tabela 3 – Exemplo de tabela do System Theoretic Proccess Analysis (STPA) . . 69
Tabela 4 – Exemplo de tabela de contexto da execução de ação 70
Tabela 5 – Exemplo de tabela de contexto de ausência de ação 70
Tabela 6 – Exemplo de falhas no modelo de processo 72
Tabela 7 – Perigos em Análise 80
Tabela 8 – Variáveis de Contexto 80
Tabela 9 – Ação: Autorizar Pouso 82
Tabela 10 – Ausência de Ação: Autorizar Pouso 82
Tabela 11 – Restrições de Segurança para a Ação Autorizar Pouso 83
Tabela 12 – Quantidades de Fatores Levantados por Cenário 89

SIGLAS

ACC Centro de Controle de Área.

AcciMap Mapeamento de Acidentes.

AIC Ação Insegura de Controle.

ANS Sistema de Navegação Aérea.

AO Operações de Aeródromos.

AOM Organização e Gerenciamento do Espaço Aéreo.

APP Centro de Controle de Aproximação.

ASBU Blocos de Atualização de Sistemas de Aviação.

ATC Controle de tráfego aéreo.

ATCo Controlador de Tráfego Aéreo.

ATM Gerenciamento de tráfego aéreo.

ATMSDM Gerenciamento de Prestação de Serviços.

ATS Serviços de Tráfego Aéreo.

ATZ Zona de Tráfego de Aeródromo.

AUO Operações dos Usuários do Espaço Aéreo.

CLR Autorização de Tráfego.

CM Gestão de Conflitos.

CNS-ATM Comunicações, Navegação e Vigilância - Gerenciamento de Tráfego Aéreo.

CSE Engenharia de Sistemas Cognitivos.

CTA Área de Controle.

CTR Zona de Controle.

DCB Balanceamento de Demanda e Capacidade.

DECEA Departamento de Controle do Espaço Aéreo.

e-FPV Ficha de Progressão de Voo Eletrônica.

eFFBD Diagrama de Blocos de Fluxo Funcional Melhorado.

ERC Cartas de Rota.

ETA Análise de Árvore de Eventos.

FANS Futuro dos Sistemas de Navegação Aérea.

FIR Regiões de Informação de Voo.

FIS Serviço de Informação de Voo.

FPV Ficha de Progressão de Voo.

FRAM Functional Resonance Analysis Method.

FTA Análise de Árvore de Falhas.

GANIS Global Air Navigation Industry Symposium.

GND Controle de Solo.

ICA Instrução do Comando da Aeronáutica.

ICEA Instituto de Controle do Espaço Aéreos.

IFR Regras de Voo por Instrumentos.

JCS Joint Cognitive Systems.

JPDO Joint Planning and Development Office.

KPA Áreas de Desempenho Chave.

NGATS Next Generation of Air Transportation System.

OACI Organização de Aviação Civil Internacional.

PHA Análise Preliminar de Perigos.

PIRG Grupo Regional de Planejamento e Implantação.

RS Restrição de Segurança.

SA Percepção Situacional - *Situation Awareness*.

SCM Swiss Chesse Model.

SESAR Single European Sky ATM Research.

SISCEAB Sistema de Controle do Espaço Aéreo Brasileiro.

STAMP Systems Theoretic Accident Model and Process.

STPA System Theoretic Proccess Analysis.

TMA Área de Controle Terminal.

TS Sincronização de Tráfego.

TWR Torre de controle de aeródromo.

VFR Regras de Voo Visual.

SUMÁRIO

1 INTRODUÇÃO . . . 25
1.1 MOTIVAÇÃO . . . 25
1.2 RELEVÂNCIA . . . 28
1.3 OBJETIVO . . . 28
1.4 ORGANIZAÇÃO DO TRABALHO . . . 29

2 PANORAMA ATUAL DA PESQUISA . . . 31
2.1 FATORES HUMANOS NO ATM . . . 31
2.1.1 Percepção Situacional e Carga de Trabalho . . . 32
2.1.2 Cognição . . . 32
2.2 MODELOS DE ACIDENTES E PERIGOS . . . 33
2.2.1 Modelos Sequenciais . . . 33
2.2.2 Modelos Epidemiológicos . . . 34
2.2.3 Modelos Sistêmicos . . . 36
2.2.3.1 Functional Resonance Analysis Method . . . 36
2.2.3.2 Accidents Mapping . . . 38
2.2.3.3 Systems Theoretic Accident Model and Process . . . 38

3 METODOLOGIA DE PESQUISA . . . 43
3.1 METODOLOGIA . . . 43
3.1.1 Revisão Bibliográfica . . . 43
3.1.2 Revisão da Documentação Oficial . . . 43
3.1.2.1 Modelagem das tarefas dos ATCo da TWR . . . 45
3.1.3 Proposição da Metodologia . . . 45
3.1.4 Validação da Metodologia Proposta . . . 45
3.2 QUADRO TEÓRICO . . . 45
3.2.1 Segurança Crítica . . . 46
3.2.2 Perigo . . . 46
3.2.3 Acidente . . . 46
3.2.4 Restrição de Segurança . . . 47
3.2.5 Fator Causal . . . 47
3.2.6 Requisito de Segurança . . . 47
3.2.7 Controlador . . . 47

4 CONTEXTO DO CONTROLADOR DE TRÁFEGO AÉREO . . . 49
4.1 CENÁRIOS DE CONTROLE DE TRÁFEGO AÉREO . . . 49

4.2 ESTRUTURA DO ESPAÇO AÉREO . . . 50
4.2.1 Espaço Aéreo Controlado . . . 50
4.2.2 Regiões de Informação de Voo . . . 53
4.2.3 Espaço Aéreo Condicionado . . . 53
4.3 ESTRUTURA DOS SERVIÇOS DE CONTROLE DE TRÁFEGO AÉREO . . . 54
4.3.1 Serviço de Controle de Área . . . 54
4.3.2 Serviço de Controle de Aproximação . . . 54
4.3.3 Serviço de Controle de Aeródromo . . . 54
4.4 PANORAMA PARA O ATM GLOBAL . . . 55
4.5 DEFINIÇÃO FUNCIONAL DO ATCO . . . 57
4.5.1 Controle de Aeródromo . . . 58
4.5.2 Controle das Aeronaves que Deixam o Aeródromo . . . 58
4.5.3 Autorização de Decolagem . . . 58
4.5.4 Controle de Aeronaves que Chegam ao Aeródromo . . . 58
4.5.5 Controle de Aeronaves no Circuito de Aeródromo . . . 58
4.5.6 Controle de Aeronaves em Táxi . . . 59
4.5.7 Seleção de Pistas em Uso . . . 60
4.5.8 Escolha do Tipo de Operação . . . 60

5 APRESENTAÇÃO DA METODOLOGIA DE ANÁLISE PROPOSTA 67
5.1 ANÁLISE DE PERIGOS . . . 67
5.1.1 Conceitos de Engenharia de Sistemas e Fluxo de Controle . . . 68
5.1.2 Identificar Possíveis Ações Inseguras de Controle . . . 68
5.1.3 Determinar as Causas de cada Ação Insegura . . . 71
5.1.3.1 Identificando como Ações não são executadas . . . 72
5.1.3.2 Identificando causas de uma AIC . . . 72
5.1.4 Análise dos Fatores Levantados . . . 74

6 APLICAÇÃO DA METODOLOGIA DE ANÁLISE . . . 77
6.1 DEFINIÇÃO DO ESCOPO E CONCEITOS UTILIZADOS . . . 77
6.2 CENÁRIOS ANALISADOS . . . 78
6.2.1 Cenário Manual . . . 78
6.2.2 Cenário Automático . . . 78
6.3 APLICAÇÃO DO STPA . . . 79
6.3.1 Conceitualização da Análise . . . 79
6.3.2 Identificando as Ações Inseguras de Controle . . . 81
6.3.3 Identificando as Possíveis Causas . . . 84
6.3.3.1 Causas para Ações Seguras não Executadas . . . 84
6.3.3.2 Causas de Ações Inseguras de Controle . . . 86

6.4 ANÁLISE DE IMPACTO EM REQUISITOS DE SEGURANÇA . . . 89

7 CONSIDERAÇÕES FINAIS 91
7.1 CONCLUSÕES 91
7.2 TRABALHOS FUTUROS 92

REFERÊNCIAS 93

1 INTRODUÇÃO

Este trabalho tem como objetivo propor uma metodologia de análise de impacto em segurança crítica da automação das tarefas dos Controladores de tráfego aéreo (ATCos) de uma Torre de controle de aeródromo (TWR) e validar sua eficácia.

Este capítulo mostrará a motivação do tema e desafios escolhidos, tratando da relevância de ambos e, ao fim, estabelecer-se-á o objetivo esperado do trabalho.

1.1 MOTIVAÇÃO

Segundo a Organização de Aviação Civil Internacional (OACI), espera-se um crescimento médio anual de 4,6% na taxa de passageiro-quilômetro para o período de 2005 a 2025 para voos comerciais internacionais (ICAO, 2007). Para o Brasil, entre os anos de 2010 e 2013 foi registrado um aumento de 6,6% a.a (DECEA, 2012). Tendo esse crescimento em vista, acentua-se a preocupação com a segurança do espaço aéreo como um todo, uma vez que não é aceitável que o aumento na demanda do sistema acarrete no aumento do risco em segurança, consequentemente aumentando o número de acidentes e a perda de vidas humanas. A OACI tem tomado medidas para lidar com esse crescimento (ICAO, 2005), conforme o descrito a seguir.

No início dos anos 1980, a OACI estabeleceu o comitê especial Futuro dos Sistemas de Navegação Aérea (FANS) com o objetivo de se criar recomendações para o planejamento do sistema de tráfego aéreo. No começo da década de 90, as recomendações feitas pelo comitê foram aceitas na décima quarta edição da conferência de navegação aérea e, com base nessa conferência, foi criado o conceito Comunicações, Navegação e Vigilância - Gerenciamento de Tráfego Aéreo (CNS-ATM).

Em 1996 a OACI determinou que o sistema já havia alcançado um nível de maturidade em que seria necessário um plano concreto que contivesse todos os desenvolvimentos tecnológicos planejados, focando também nas implantações regionais. A primeira revisão desse plano gerou o documento conhecido como *Global Air Navigation Plan to CNS-ATM Systems* (ICAO, 2013). Nos anos seguintes, vários membros da OACI começaram os seus próprios planos de implantação do CNS-ATM, como o Next Generation of Air Transportation System (NGATS) dos Estados Unidos (posteriormente recebendo o nome de *NextGen*) (FAA, 2012b) e o Single European Sky ATM Research (SESAR) da União Europeia (EUROCONTROL, 2012). Entretanto, reconheceu-se que não bastavam apenas avanços tecnológicos para que os sistemas Gerenciamento de tráfego aéreo (ATM) se modernizassem. Seria necessário um conceito de sistema global e integrado, baseado em

requisitos operacionais pré estabelecidos. Essa ideia foi concretizada e aprovada durante a décima primeira conferência de navegação aérea em 2003, onde foram delimitados os requisitos do Serviços de Tráfego Aéreo (ATS) e uma estratégia de transição para esse sistema de forma mais global e integrada, dando origem ao conceito ATM Global.

A partir da concepção do ATM Global, a OACI começou uma série de eventos de colaboração com os estados membros e indústrias, o principal sendo o Global Air Navigation Industry Symposium (GANIS) em 2011. Estes eventos permitiram um amadurecimento das estratégias de transição dos sistemas ATM, fazendo com que eles evoluíssem para a estratégia Blocos de Atualização de Sistemas de Aviação (ASBU). A OACI define essa estratégia da seguinte forma:

> *The Block Upgrades and their capacity Modules define a programmatic and flexible global systems engineering approach allowing all States to advance their Air Navigation capacities based on their specific operational requirements (ICAO, 2013, p10).*

Essa estratégia permitirá que todos os membros consigam implementar as melhorias previstas de forma harmoniosa e integrada, melhorando o desempenho do sistema em escala global. O ASBU representa a concretização dos planos propostos CNS-ATM, e posteriormente ao ATM Global, decorrido de três edições do plano global (ICAO, 2013).

Os planos de implementação do CNS-ATM e do ATM Global foram reformulados e revisados para se tornarem consistentes com o ASBU, no caso do *NextGen*, do SESAR, e do SIRIUS para o Brasil (DECEA, 2011).

Um dos vários conceitos presentes em todos esses projetos é a da implantação crescente de automação das tarefas realizadas por operadores humanos, desde os ATCos até os pilotos (BROOKER, 2008; ICAO, 2013) tentando aumentar, assim, o desempenho e diminuir os erros cometidos por esses operadores. Erros humanos corresponderam com a maior parcela dos fatores contribuintes dos acidentes aéreos ocorridos nas últimas décadas, como mostra a Tabela 1 (adaptada de PlaneCrashInfo.com (2015)).

Tabela 1 – Causas de Acidentes Fatais em Porcentagem

Causa	**1950**	**1960**	**1970**	**1980**	**1990**	**2000**	**Todas**
Erro piloto	41	34	24	26	27	30	29
Erro piloto (rel. clima)	10	17	14	18	19	19	16
Erro piloto (rel. falha mecânica)	6	5	5	2	5	5	5
Total erro piloto	57	56	43	46	51	54	50
Outro erro humano	2	9	9	6	9	5	7
Clima	16	9	14	14	10	8	12
Falha mecânica	21	19	20	20	18	24	22
Sabotagem	5	5	13	13	11	9	9
Outras causas	0	2	1	1	1	0	1

Nessa tabela o erro do piloto dividido em três tipos: erro do piloto relacionado com condições climáticas extremas, erro do piloto relacionado a falhas mecânicas da aeronave e erro do piloto em outras situações. Além destas categorias, ainda existe uma para outro erro humano, que compreende erros de controladores e outro pessoal.

Seguindo o conceito ATM Global, torna-se necessária a investigação do impacto que essas novas tecnologias podem causar nos atuais níveis de segurança, principalmente nas áreas em que elas serão utilizadas em parceria com operadores humanos. A Joint Planning and Development Office (JPDO), agência criada pelo governo norte-americano para coordenar o desenvolvimento do *NextGen*, em seu plano de pesquisa para fatores humanos afirma que:

> *... the human is the most important element in the air transportation system and must be considered first and foremost in the design of improvements to it...(PREVOT et al., 2012).*

Isso mostra a importância do desenvolvimento e testes baseados nos operadores humanos (*human centered development*) (PARASURAMAN; SHERIDAN; WICKENS, 2000).

Parasuraman, Sheridan e Wickens (2000) observa que ferramentas mais automatizadas não simplesmente substituem os operadores em suas tarefas, mas acabam por modificar a operação humana, muitas vezes de maneiras indevidas e não antecipáveis, e como resultado acabam criando novas demandas dos operadores que as utilizam, e são essas novas maneiras que mais podem gerar situações perigosas na operação do tráfego aéreo.

Para esse deslocamento tecnológico de tarefas manuais para mais automatizadas, faz-se necessária uma avaliação de como serão afetadas as tarefas desempenhadas pelo controlador, procurando todas as características planejadas, latentes e emergentes que essa integração traz consigo, de forma a avaliar como elas podem impactar na segurança do sistema. Para tanto, ao longo do tempo foram desenvolvidas técnicas de avaliação de segurança crítica para sistemas, novos ou existentes.

As técnicas mais tradicionais utilizadas modelam acidentes como uma sequência de eventos causais, onde muitas vezes esses eventos são representados por falhas nos componentes dos sistemas (FLEMMING, 2004). Cada evento leva a uma próxima falha em uma corrente de eventos, onde existe uma relação direta entre ambos.

Entretanto, conforme a complexidade dos sistemas tem crescido, muitos acidentes não conseguem ser explicados como uma simples sequência de eventos a partir de um evento raiz, mas sim como um fenômeno emergente da variação na operação normal de um sistema (DE CARVALHO, 2011).

Essas técnicas também acabam por considerar o operador humano como mais um componente independente do sistema, descrevendo eventuais erros do operador de maneira similar aos erros de um hardware, ignorando aspectos cognitivos e sociotécnicos da operação.

Para lidar com o problema da complexidade, do acoplamento dos componentes do sistema, dos fatores sociotécnicos e organizacionais, modelos que utilizam a teoria de sistemas como a sua base começaram a surgir, como o FRAM, o AcciMap e o STAMP, que serão discutidos com mais detalhes no decorrer do texto. Esses modelos surgem para tentar representar a complexidade em que os sistemas mais atuais atuam, com uso cada vez mais de ferramentas automáticas baseadas em software.

1.2 RELEVÂNCIA

Por se tratar da preservação de vidas humanas, o estudo de segurança de sistemas críticos já justifica a sua própria relevância. Mesmo sendo um meio de transporte confiável, acidentes relacionados à aviação costumam gerar grande comoção devido à gravidade deles, em geral não havendo sobreviventes.

Como visto anteriormente, com essa necessidade de aumentar a capacidade do sistema sem comprometer a sua segurança, são imperativos novos estudos que assegurem que essas novas viagens vão acontecer de modo seguro, frente à mudança de paradigmas tecnológicos e procedimentos que o ATM vai enfrentar.

Uma visão global do impacto na segurança da automação de tarefas dos controladores ajudará nas análises mais específicas dos pontos frágeis levantados, em específico da TWR. Além disso, a utilização de análises preliminares permite que o sistema seja modificado ainda na fase de projeto, reduzindo os riscos e os custos envolvidos no desenvolvimento.

Como as técnicas mais tradicionais não conseguem representar toda essa crescente complexidade dos sistemas, novas surgem para preencher esse requisito. Faz-se necessária, então, uma avaliação de como essas técnicas se comportam nos mais diferentes cenários, e como elas podem avaliar o impacto nas mudanças que os sistemas estão passando.

1.3 OBJETIVO

Este trabalho de pesquisa científica possui como objetivo principal propor uma metodologia de análise, do ponto de vista sistêmico, o impacto da automação de tarefas do Controlador de Tráfego Aéreo (ATCo) de uma Torre de controle de aeródromo em relação à segurança crítica (*safety*). Entende-se por automação qualquer emprego de tecnologia que auxilie o operador humano em suas tarefas, desde uma simples ferramente de auxílio

em tomada de decisão (telas com informações extra) até um sistema completamente automatizado.

Como objetivo secundário, é feita uma aplicação da metodologia proposta utilizando-a em um cenário de exemplo da automação da comunicação entre o ATCo e a tripulação da aeronave durante a autorização de aterrissagem da aeronave.

A metodologia proposta analisa o impacto em termos de fatores causais de perigos e dos seus respectivos requisitos de segurança das operações com e sem ferramentas automatizadas, determinando dessa forma a maneira que a automação impacta na segurança da operação. Como modelo de análise de acidentes, foi adotado o Systems Theoretic Accident Model and Process (STAMP), que possui embutido o conceito de engenharia de sistemas para a análise de acidentes. Será utilizado a técnica System Theoretic Proccess Analysis (STPA), associada ao modelo, de modo a levantar todas as restrições de segurança associadas aos processos do sistema avaliado.

1.4 ORGANIZAÇÃO DO TRABALHO

O restante do trabalho está dividido da seguinte forma:

- Capítulo 2 (Panorama de Pesquisa): Revisão bibliográfica da pesquisa dentro da área de segurança no controle de tráfego aéreo, traçando o atual estado da arte nessas áreas.
- Capítulo 3 (Metodologia de Pesquisa): Definição do quadro teórico utilizado na pesquisa, modelos e técnicas utilizadas.
- Capítulo 4 (Contexto ATC): Apresentação do contexto atual ao qual o ATCo se encaixa.
- Capítulo 5 (Apresentação da Metodologia Proposta): Apresentação do modelo STAMP e da técnica STPA e a forma com que serão utilizados.
- Capítulo 6 (Validação da Metodologia): Descrição do cenário delimitado para a análise, bem como a execução da metodologia proposta.
- Capítulo 7 (Considerações Finais): Considerações finais e trabalhos futuros.

2 PANORAMA ATUAL DA PESQUISA

Neste capítulo será discutido o atual panorama do conceito ATM Global, bem como está o estado da arte em pesquisas relacionadas ao ATM e às áreas de estudo contidas nesse trabalho.

2.1 FATORES HUMANOS NO ATM

Para o assunto de fatores humanos, as pesquisas tentam entender como alguns aspectos da operação do sistema feita pelo operador humano será modificado. Prevot et al. (2012) cita a importância da pesquisa nas operações homem-máquina nas novas tecnologias, para que essa possa permitir que o operador se dedique a outras tarefas que exijam mais de sua atenção. Uma mudança que os autores parecem concordar é o fato de que os operadores estão migrando de um estado de *controladores ativos* para *monitores passivos* (METZGER; PARASURAMAN, 2001).

Conforme as tecnologias vão melhorando e vão aparecendo para o operador, a necessidade de interação ativa com o sistema vai diminuindo, fazendo com que o operador apenas monitore o estado do sistema e só atue em casos que a operação se desvie do seu curso normal (entre em um estado perigoso).

Metzger e Parasuraman (2005) mostra como essa troca de papéis do controlador, do ativo para monitor passivo, acaba por reduzir em muito a capacidade cognitiva do ATCo em um cenário com alto tráfego e taxa de automação (como o *Free-Flight*).

Corver e Aneziris (2014) analisa a operação de dois Centro de Controle de Área (ACC)'s na Europa, um com a operação chamada *stripless*, ou seja, sem o recurso de *strips* eletrônicas, e outra *strip*, contando com o recurso de *strips* eletrônicas[1].

Nesse estudo foi observado que ao se adotar a operação *strip*, a carga de trabalho dos ATCo's diminui consideravelmente, devido ao fato de todas as informações estarem disponíveis na tela do radar. Devido a este fato, as conversas entre operadores diminuíram, ou cessaram de vez, o que levantou uma possibilidade de diminuição de Percepção Situacional - *Situation Awareness* (SA) entre eles, uma vez que a conversa entre os operadores para passar as informações na operação *stripless* era uma das formas de os mesmos saberem do que está acontecendo com os outros controladores.

Parasuraman, Sheridan e Wickens (2000) aponta que uma ferramenta automatizada não simplesmente substitui a operação de um humano, mas acaba por transformar essa

[1] *Strip* é o nome genérico para Ficha de Progressão de Voo (FPV) e *strip eletrônica* a Ficha de Progressão de Voo Eletrônica (e-FPV)

operação, muitas vezes de maneiras inesperadas.

2.1.1 Percepção Situacional e Carga de Trabalho

A pesquisa a respeito dos valores de carga de trabalho (*workload*) e Percepção Situacional - *Situation Awareness* (SA) tornou-se valiosa para se determinar o quão efetiva está sendo a integração entre o operador e a automação (VU et al., 2012), uma vez que o impacto que automações mal projetadas e falhas podem causar no operador pode ser danosa (ROVIRA; PARASURAMAN, 2010).

Necessita-se, então, descobrir como essas tecnologias vão afetar o treinamento de novos operadores (CAMP et al., 2001). Vu et al. (2012) detecta que ATCos treinados extensivamente em operações automatizadas tem grande dificuldade de lidar em situações em que suas ferramentas automatizadas falham, ao passo que ATCos experientes em situações manuais conseguem detectar o erro da automação mais facilmente e assim conduzir a operação de forma manual e segura.

Gil et al. (2012) mostra que a carga de trabalho do piloto aumenta consideravelmente quando a sua ferramenta de rota para aeródromos calcula rotas erradas, diminuindo o seu desempenho no processo de pouso.

Langan-Fox, Sankey e Canty (2009) cita que o foco em estudos de carga de trabalho e SA acabaram por deixar outros conceitos como vigilância, monotonia e estresse sem ser avaliados, fazendo com que exista poucas pesquisas relacionadas com esses fatores, causando um alerta, pois são áreas impactadas diretamente ao se desenvolver novas tecnologias para o ATCo.

2.1.2 Cognição

Uma maneira de analisar o comportamento dos operadores frente a essas mudanças é entender como ele consegue estruturar todas as informações é o estudo dos *mapas cognitivos*, ou imagem mental (MALAKIS; KONTOGIANNIS, 2013). Os mapas cognitivos são estruturas de busca de informação dentro de um ciclo cognitivo do pensamento humano, composto pela percepção e sensação (NEISSER, 1976; WEICK, 1995).

Desse conceito de cognição e mapas mentais, Hollnagel e Woods (2005) criaram o conceito de Engenharia de Sistemas Cognitivos (Engenharia de Sistemas Cognitivos (CSE)), onde o sistema não é visto mais como formado por um operador e uma tecnologia separadamente, mas como um sistema cognitivo conjunto (Joint Cognitive Systems (JCS)), permitindo entender como esse sistema pode aprender com ele mesmo (HOLLNAGEL, 2007). Esse novo conceito permitiu pesquisas tentarem entender como a tecnologia e os operadores podem ser considerados membros de uma mesma equipe (LANGAN-FOX; CANTY; SANKEY, 2009).

2.2 MODELOS DE ACIDENTES E PERIGOS

Todo tipo de esforço de análise ou projeto baseado em segurança crítica começa por como modelar os acidentes referentes ao sistema, modelo este que representa o embasamento teórico da análise do sistema (LEVESON; STEPHANOPOULOS, 2014).

Hollnagel (2004) define que os atuais modelos de acidentes fazem parte de três grandes categorias:

- Modelos Sequenciais: acidentes definidos por uma sequência de eventos lineares, com o último evento sendo o acidentes de fato.
- Epidemiológicos: acidentes definidos como uma combinação de condições latentes do sistema (ex: ambiente, operacional, desgaste, etc.) que resultam no acidente.
- Sistêmicos: acidentes definidos como um problema de controle no sistema, desrespeitando alguma restrição previamente estabelecida (ou estabelecida de maneira incorreta) .

2.2.1 Modelos Sequenciais

Estes modelos admitem que acidentes são causados por uma sequência de eventos catastróficos, iniciado por um evento raiz (UNDERWOOD; WATERSON; BRAITHWAITE, 2016). Esse primeiro evento pode ser considerado como sendo uma falha de equipamento ou um erro humano durante a operação do sistema.

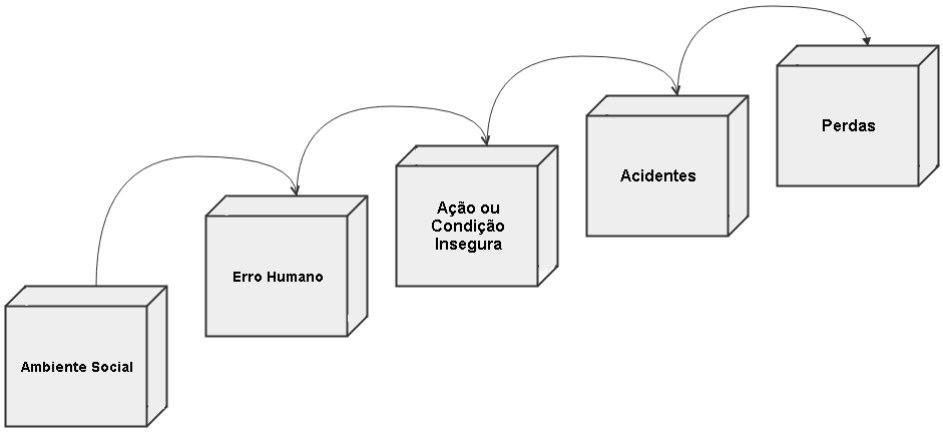
Este tipo de modelo foi inciado pelo modelo dominó (HEINRICH, 1931), ainda na década de 30. Nele, a sequência de eventos é considerada como uma fila de dominós, ao acontecer um evento, este cai e começa a derrubar todos os outros (figura 1).

A Análise de Árvore de Falhas (FTA) é outro destes modelos. Envolve representar uma falha como uma árvore de eventos, tentando determinar as possíveis causas deste com base em combinações de diferentes causas possíveis, ligados por operadores lógicos (e/ou) (NETJASOV; JANIC, 2008).

Esta técnica leva em conta a teoria de confiabilidade, definindo que a probabilidade de ocorrência deste evento é a multiplicação das probabilidades de cada evento que leva ao acidente. A figura 2 mostra um exemplo de FTA.

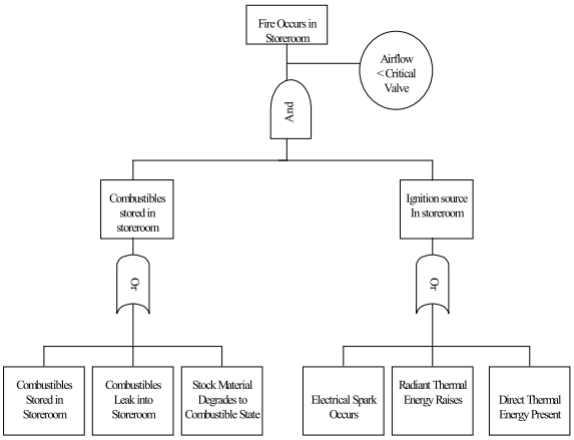
A Análise de Árvore de Eventos (ETA) é utilizada para modelar a sequência de eventos possíveis que acontecem a partir de um determinado perigo, com o objetivo de descrever as consequências da ocorrência do evento perigoso (NETJASOV; JANIC, 2008). A figura 3 mostra uma exemplo de uma ETA.

Figura 1 – Modelo Dominó



Fonte: Adaptado de Leveson e Thomas (2013)

Figura 2 – Exemplo de FTA



Fonte: SAP (2007)

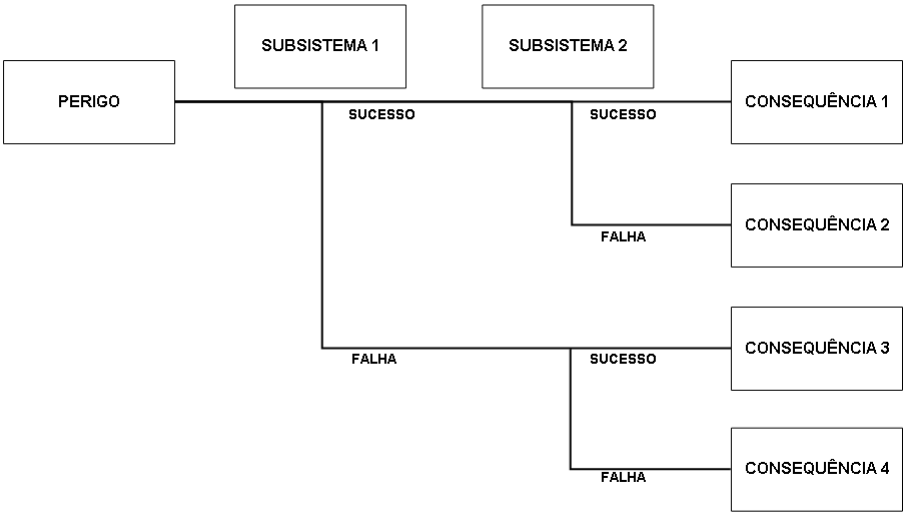
2.2.2 Modelos Epidemiológicos

Descrevem acidentes pela combinação, não necessariamente ordenada, de fatores causais, como desvios de desempenho, condições de ambiente e problemas em barreiras (STROEVE; BLOM; BAKKER, 2009). O maior representante deste tipo é o Swiss Chesse Model (SCM) (UNDERWOOD; WATERSON, 2014).

O SCM modela a causa de um acidente como uma sequência de falhas em quatro níveis (REASON, 1990):

1. Influências organizacionais.

Figura 3 – Exemplo de ETA



Fonte: Adaptado de SAP (2007)

2. Supervisão insegura.

3. Pré-condições para ações inseguras.

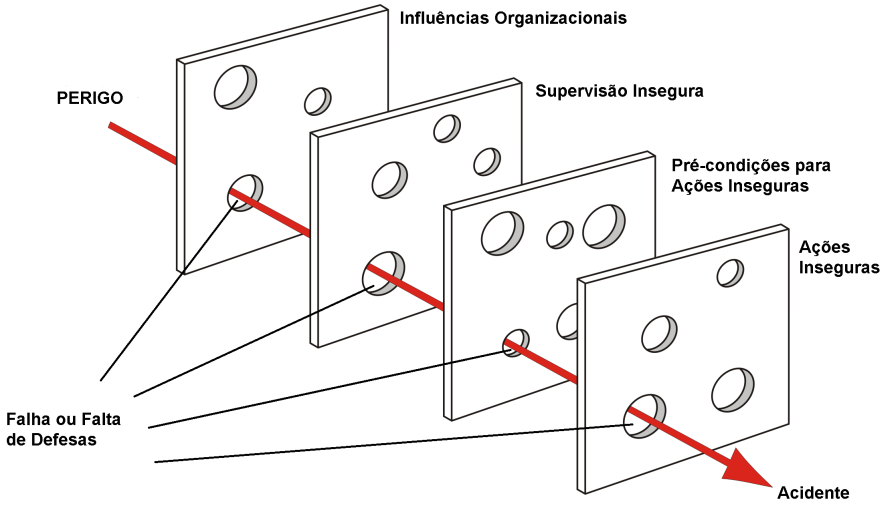
4. Ações inseguras.

A figura 4 representa esse modelo. Os buracos na figura representam os problemas e fragilidades em cada aspecto, distribuídos aleatoriamente em tamanho e localização. Assume-se que eventualmente esses buracos se alinham, de uma maneira a criar um caminho através de cada nível, representando a combinação de falhas que leva a um acidente, atravessando até mesmo as barreiras existentes.

O SCM assume não só uma relação linear entre os eventos, mas também um comportamento aleatório entre os componentes e a independência entre cada um dos eventos catastróficos (FLEMMING, 2004).

Muitos críticos argumentam que as hipóteses de linearidade e independência de eventos não são comprovadas na prática, principalmente em sistemas críticos que dependam fortemente de software e operação humana para funcionar (DEKKER, 2006). Isso acaba gerando uma simplificação muito grande da complexidade de interações entre os componentes do sistema, o que torna esse modelo ineficaz em representar as causas de um acidente no mundo moderno (HOLLNAGEL, 2012).

Figura 4 – Modelo Queijo Suíço (SCM)



Fonte: Adaptado de Reason (1990)

2.2.3 Modelos Sistêmicos

A grande mudança de paradigma dos novos métodos que começam a surgir é o fato de que eles exploram mais afundo a teoria de sistemas, em específico de complexidade, do que apenas de se contentar com a redução de sequência de eventos ou mesmo a teoria de confiabilidade. Dentro deste conceito surgem modelos novos que incorporam esse pensamento sistêmico, onde os mais famosos são (UNDERWOOD; WATERSON, 2014):

1. Systems Theoretic Accident Model and Process (STAMP)
2. Functional Resonance Analysis Method (FRAM)
3. Mapeamento de Acidentes (AcciMap)

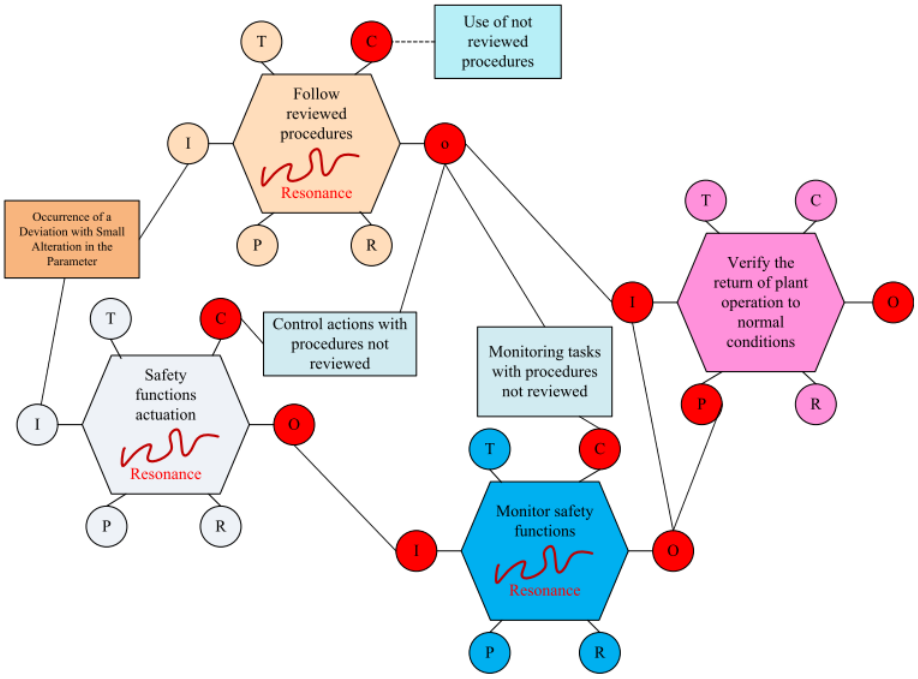
Esses novos modelos incorporam também o conceito de engenharia de resiliência, onde ao invés de procurar por causas de acidentes puramente, eles procuram entender como projetar sistemas que conseguem lidar com a variabilidade de eventos perigosos, que fazem com que o sistema entre em um estado de perigo, e assim possam utilizar de respostas projetadas para mover o sistema para um estado mais seguro (DE CARVALHO, 2011).

2.2.3.1 Functional Resonance Analysis Method

O FRAM (HOLLNAGEL, 2012) utiliza um modelo não-linear para representar acidentes como uma combinação, ou ressonância, da variabilidade do desempenho normal

do sistema (DE CARVALHO, 2011). Ele caracteriza os sistemas complexos pelas funções que eles possuem ao invés de sua estrutura. As restrições do sistema são definidas através da descrição de suas funções em acordo com o princípio do JCS. A figura 5 mostra como é o diagrama do FRAM.

Figura 5 – Diagrama do FRAM



Fonte: Alvarenga, Melo e Fonseca (2014)

É executado em quatro partes (ALVARENGA; MELO; FONSECA, 2014):

- Identificar as funções essenciais através de seis parâmetros básicos.
- Caracterizar o potencial de variabilidade de cada função em função do contexto aplicado.
- Definir a ressonância funcional baseada nas possíveis dependências ou acoplamentos entre as funções.
- Identificar barreiras ou mitigações que absorvam essa variabilidade.

Os seis parâmetros básicos são:

- Entrada: o que é utilizado para produzir a saída da função.
- Saída: o que é produzido após a função.

- Controle: o que supervisiona ou ajusta a função.
- Recurso: o que é necessário pela função para processar a entrada.
- Pré-condição: condições do sistema para que a função execute.
- Tempo disponível: tipo de recurso ou uma restrição da função.

2.2.3.2 Accidents Mapping

O AcciMap (RASMUSSEN, 1997) foi projetado para utilizar a teoria de controle juntamente com o pensamento sistêmico para a análise de acidentes, consequentemente considerando que acidentes são causados pela perda de controle de um processo (UNDERWOOD; WATERSON, 2014). Rasmussen (1997) cita que todos os níveis hierárquicos afetam o controle dos perigos, portanto uma visão verticalizada do comportamento do sistema é necessária.

O modelo analista a série de interações, eventos e processos de decisão que ocorreram no sistema e resultaram na perda do controle do processo. Para isso, utiliza-se uma mistura de um fluxograma de causa e consequência com o arcabouço de gerenciamento de risco (RASMUSSEN, 1997), descrevendo então o sistema sociotécnico através de seis níveis organizacionais (a figura 6 mostra um exemplo).

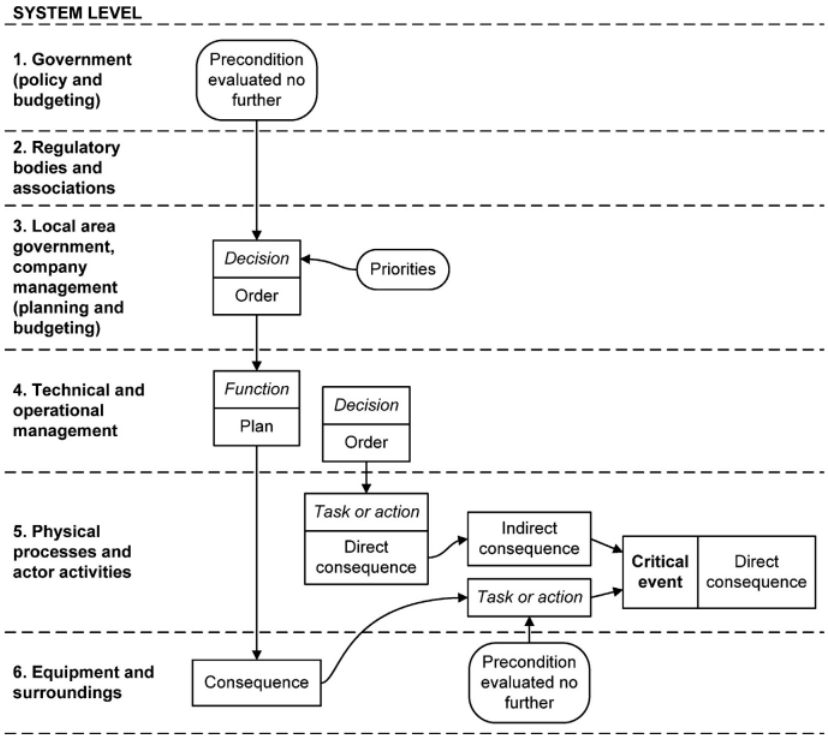
2.2.3.3 Systems Theoretic Accident Model and Process

O STAMP foca em segurança crítica como um problema de controle, similar ao AcciMap (UNDERWOOD; WATERSON, 2014). Leveson e Thomas (2013) definem segurança crítica como uma propriedade emergente do sistema, que aparece quando os componentes interagem entre si dentro de um ambiente mais amplo. Existem um conjunto de restrições relacionado à operação do sistema que, quando todos respeitados, asseguram a propriedade de segurança. Essas restrições podem ser: físicas, humanas e sociais. Acidentes ocorrem, então, quando as interações entre componentes do sistema violam alguma dessas restrições, ou seja, essas restrições não foram devidamente aplicadas no projeto do sistema.

O STAMP se estrutura em três conceitos básicos: restrições de segurança, estruturas de controle hierárquicas e modelos de processos. Esses três conceitos que possibilitam o modelo a ter um poder de representação e de análise superior do que as técnicas baseadas em sequência de eventos.

O mais básico conceito do STAMP dos três apresentados, inclusive, não é evento, mas sim a restrição. Para o STAMP, eventos que produzem acidentes apenas acontecem quando uma restrição de segurança não foi satisfeita, ou inexiste. A dificuldade em se determinar essas restrições vem da própria complexidade que os sistemas estão adquirindo. Cook (1996) cita que quando os sistemas possuíam controles mais mecânicos, o operador

Figura 6 – Diagrama do AcciMap



Fonte: Underwood e Waterson (2014)

ficava mais próximo do sistema, no sentido físico e lógico, o que permitia que ele tivesse uma gama de informações do processo muito maiores, por estar tão próximo. Agora os controles eletromecânicos introduziram uma camada de interação entre o operador e o processo que impede que ele tenha acesso ao mesmo número de informações, sendo essas apenas as que os projetistas julgaram que ele deveria saber para qualquer momento, ou seja, caso aconteça algum evento que o projetista não presumiu como possível, o operador ficaria sem informações para agir.

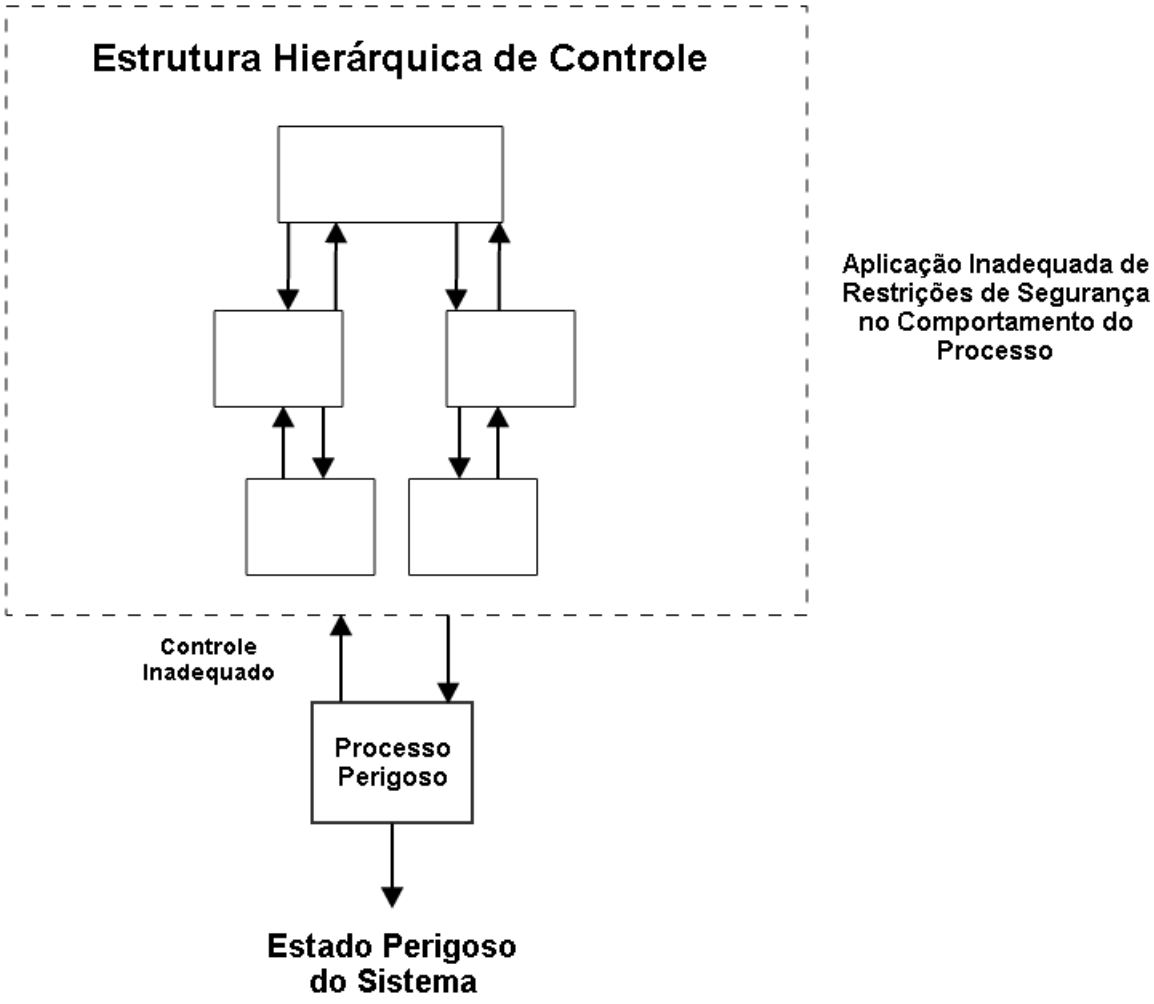
A cada nível hierárquico dentro do sistema, algum tipo de ação inadequada pode acontecer devido a restrições não obedecidas ou não existentes em qualquer nível de sistema, ou ainda que não houve resposta (*feedback*) correta de níveis mais baixos. Por exemplo, se um gestor faz uma série de instruções de maneira a garantir a segurança durante a operação, pode acontecer que as instruções não tenham chegado aos operadores de maneira correta, ou já estavam incorretas desde o começo, ou ainda que estivessem corretas, os operadores podem ter as ignorado. Em qualquer hipótese, o gestor pode não ter um canal de *feedback* adequado para saber se as instruções estão sendo seguidas ou não. Nesse caso temos um problema hierárquico de uma não interação entre os níveis do sistema. Canais de comunicação são necessários entre todos os níveis hierárquicos de um sistema para levar a informação necessária para que se garanta as restrições de segurança

são críticos.

O terceiro conceito do STAMP são os modelos de processo. Os modelos podem ser dos mais simples, com apenas duas ou três variáveis até os mais complexos, com transições de estados e variáveis numerosas. Não importa se o controle vai estar em um sistema automatizado ou em uma lógica de processos controlados por humanos, todos os modelos de processos devem conter: a relação entre as variáveis de sistema, acesso ao estado atual e uma maneira de controlar como o processo muda de estado. Acidentes que envolvem interações errôneas de componentes em geral são explicadas pelos modelos de processo (em geral errados). Esse modelos são importantes principalmente por auxiliar a descoberta de como os acidentes ocorrem e como os operadores podem controlar de maneira inadequada sistemas críticos.

O STAMP então é construído com base nesses três conceitos, juntamente com a teoria de sistemas. Nesse cenário, sistemas são definidos como um conjunto de componentes inter-relacionados em um estado de equilíbrio dinâmico, mantido por controles de *feedback*. Como definido anteriormente, segurança é vista como uma propriedade emergente do sistema que aparece quando as restrições certas são satisfeitas durante a operação do sistema. Então defini-se, neste caso, gerenciamento de segurança (*safety management*) como o projeto e criação de uma estrutura de controle que consegue aplicar as restrições de segurança e que continue garantindo essas restrições conforme as mudanças nos estados do sistema vão acontecendo. Desta forma, acidentes são entendidos ao identificar quais restrições de segurança não foram obedecidas e quais controles foram inadequados ao aplicá-las. A figura 7 sumariza os conceitos citados, nela podemos ver que dentro de uma estrutura hierárquica segura, um controle inadequado pode, através de um processo perigoso e de uma restrição não obedecida, colocar o sistema em um estado perigoso.

Figura 7 – Visão de como acidentes acontecem segundo o STAMP



Fonte: Adaptado de Leveson (2012)

3 METODOLOGIA DE PESQUISA

Neste capítulo será mostrada a metodologia proposta para esse trabalho de investigação científica, mostrando os caminhos percorridos do estabelecimento do objetivo até a avaliação final.

3.1 METODOLOGIA

A metodologia está dividida em cinco grande partes, cada uma dividida em uma série de tarefas. A figura 8 resume o processo proposto. As quatro grande partes são:

1. Revisão Bibliográfica.
2. Revisão da Documentação Oficial.
3. Proposição da Metodologia de Análise.
4. Aplicação da Metodologia de Análise.
5. Considerações Finais.

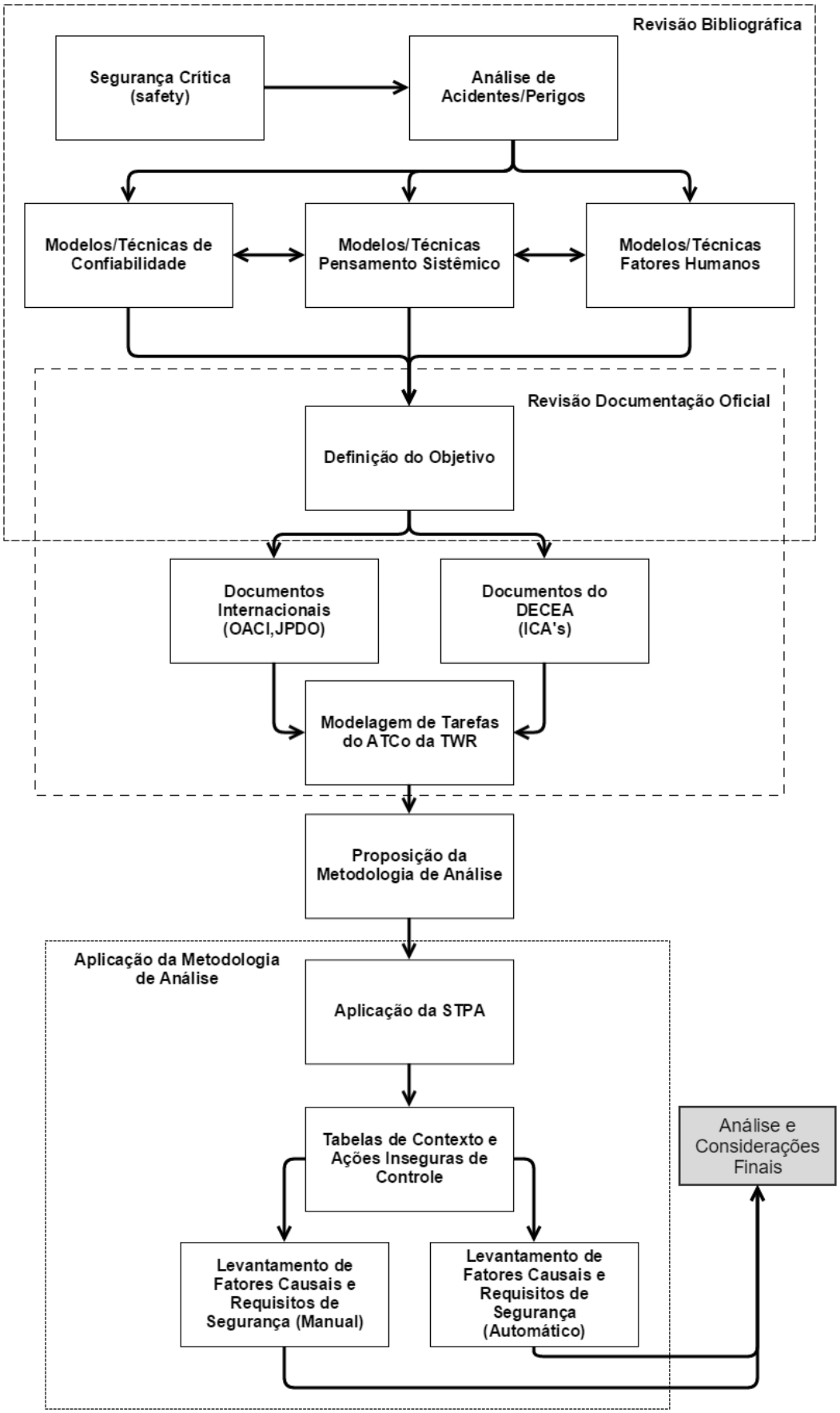
3.1.1 Revisão Bibliográfica

A revisão da literatura foi feita para contextualizar a atual situação de pesquisa nas áreas correlatas com essa pesquisa, mostrado no capítulo 2. Primeiro foi feito um levantamento sobre o conceito básico desta pesquisa, segurança crítica (*safety*). Com isso foram pesquisadas as técnicas, modelos e metodologias associadas à análise de perigos e acidentes, tanto das mais tradicionais (teoria de confiabilidade), quanto as mais modernas (teoria sistêmica e fatores humanos). Com base nessas informações, foi possível formalizar o objetivo desta pesquisa, apresentado na introdução.

3.1.2 Revisão da Documentação Oficial

Foram utilizados principalmente documentos do Departamento de Controle do Espaço Aéreo (DECEA), órgão oficial responsável pelo Gerenciamento de tráfego aéreo (ATM) no Brasil. Para entender o escopo global de mudanças no ATM, foram utilizados os documentos da Organização de Aviação Civil Internacional (OACI). Os documentos do Departamento de Controle do Espaço Aéreo (DECEA), principalmente os chamados Instruções do Comando da Aeronáutica (ICAs), serviram como base para que se pudesse

Figura 8 – Metodologia de Pesquisa



entender o papel do ATCo dentro da TWR no cenário brasileiro e permitiram a criação dos modelos de tarefas.

3.1.2.1 Modelagem das tarefas dos ATCo da TWR

A partir do panorama construído, foram criados os modelos das tarefas realizadas pelos ATCos dentro da TWR, utilizando o método formal de engenharia de sistemas Diagrama de Blocos de Fluxo Funcional Melhorado (eFFBD) para representar a sequência lógica das tarefas e de suas interdependências, traduzindo as tarefas descritas apenas em linguagem formal para uma linguagem mais visual. Maiores detalhes sobre a eFFBD se encontram no capítulo 4.

3.1.3 Proposição da Metodologia

Com base nos levantamentos do estado da arte na pesquisa e com o levantamento do contexto atual do ATCo, foi proposta a metodologia de análise do impacto de automação de tarefas dos ATCo da TWR. A metodologia segue basicamente os passos definidos pela aplicação do STPA, mas com o diferencial de analisar dois cenários simultaneamente, para poder levantar as diferenças em termos de fatores causais e requisitos de segurança entre os cenários manual e automático.

Os passos da metodologia estão descritos no capítulo 5. Na figura 8, eles estão representados no bloco *Validação da Metodologia*

3.1.4 Validação da Metodologia Proposta

Para poder validar a metodologia proposta, ela foi aplicada em um cenário exemplo apresentado no capítulo 6. A tarefa analisada será a autorização de aterrissagem para aeronaves no aeródromo e a tecnologia avaliada será o link de dados digital (Datalink), que substitui a comunicação por rádio transmissão, utilizando mensagens pré-formatadas, evitando assim o problema de pronuncias e esquecimento dos termos adequados.

Ao final da execução do STPA, teremos os conjuntos de fatores causais e dos requisitos de segurança referentes aos controles sendo analisados.

3.2 QUADRO TEÓRICO

Para ajudar na condução da pesquisa, foi delimitado um quadro teórico para determinar todas as definições dos parâmetros, métricas e conceitos utilizados (ver tabela 2).

Tabela 2 – Quadro Teórico

Conceito	**Definição**
Segurança Crítica (*safety*)	Não-existência de acidentes.
Acidente	Evento indesejado que resulta na perda de vidas humanas.
Perigo (*hazard*)	Estado do sistema que pode levar a um acidente dado uma combinação de condições específicas.
Restrição de Segurança	Limitações do sistema para que não haja perigos/acidentes.
Fator Causal	Algum fator que não obedece a uma restrição de segurança, podendo levar o sistema a um perigo.
Requisito de Segurança	Comportamento necessário para que o sistema evite os fatores causais de um perigo/acidente.
Controlador	Dispositivo que é capaz de alterar e monitorar o estado de um sistema dinâmico

3.2.1 Segurança Crítica

Segurança crítica, ou *safety* em inglês, tem a sua definição mais usual como "não existência de acidentes" (LEVESON, 2012), ou seja, algo (sistema) é considerado seguro quando não há acidentes. Para o restante do texto, trataremos de segurança crítica, ou *safety*, apenas por segurança, excluindo assim a parte de segurança de dados (*security*).

A engenharia de sistemas define ainda que segurança é uma propriedade emergente do sistema, que surge quando seus componentes em todos os níveis hierárquicos se inter-relacionam respeitando as restrições de segurança estabelecidas (LEVESON, 2004; FLEMMING, 2004; THOMAS, 2013).

3.2.2 Perigo

Os perigos, ou do inglês *hazards*, são considerados estados do sistema que, em combinação com condições de ambiente e sistêmicas específicas, podem gerar um acidente (LEVESON; THOMAS, 2013).

3.2.3 Acidente

Leveson (2012) define acidente como um evento indesejado que resulta em algum tipo de perda, seja vidas humanas, danos a propriedades, poluição ambiental ou a perda da missão do sistema. Como no caso do Controle de tráfego aéreo (ATC) a missão é o transporte seguro de pessoas, acidentes aqui serão tratados apenas como eventos inesperados ou não planejados que geram perda de vidas humanas.

3.2.4 Restrição de Segurança

Restrição de Segurança (RS) (*safety constraint*) é definida como uma limitação da operação de controle para que não haja perigos (LEVESON; THOMAS, 2013). Neste sentido uma Restrição de Segurança (RS) determina aquilo que o controlador não deve fazer para que o sistema opere de maneira segura.

3.2.5 Fator Causal

No STAMP as causas não são vistas como uma sequência de eventos ou um conjunto de eventos com relação de causa e efeito que levam a um acidente, e sim fatores que violam as RS por algum motivo. Esses fatores são chamados de fatores causais (THOMAS, 2013).

3.2.6 Requisito de Segurança

Diferentemente da restrição, um requisito mostra aquilo que o controlador deve fazer para o sistema alcançar o seu objetivo (LEVESON; THOMAS, 2013), neste caso de requisitos de segurança, o objetivo é ter uma operação segura. Trata-se então requisitos de segurança como aquilo que deve ser feito pelo sistema para se evitar os fatores causais levantados.

3.2.7 Controlador

A palavra controlador será utilizada como referência ao conceito de engenharia de sistemas, onde ele é visto como um dispositivo, seja mecânico, hidráulico ou eletrônico, que é capaz de alterar e monitorar o estado de um sistema dinâmico (BENNETT, 1993)

4 CONTEXTO DO CONTROLADOR DE TRÁFEGO AÉREO

Nesse capítulo será discutido e explicado o contexto em que o controlador de tráfego aéreo (ATCo) está inserido atualmente dentro do Sistema de Controle do Espaço Aéreo Brasileiro (SISCEAB). Salvo quando especificado o contrário, as definições encontradas nesse capítulo foram adaptadas dos textos DECEA (2013a), DECEA (2013b), DECEA (2013c).

4.1 CENÁRIOS DE CONTROLE DE TRÁFEGO AÉREO

O principal objetivo do ATM, segundo a OACI, é garantir voos regulares e eficazes, respeitando as condições meteorológicas e as limitações das aeronaves. Para garantir a segurança e eficiência desses voos, os conhecimentos básicos são:

- A demanda de tráfego atual e futura.
- A topografia e infraestrutura instalada.

Analisando essas informações, foram estabelecidas ações adequadas para cada segmento específico do espaço aéreo, as estruturas de uso do espaço aéreo (as aerovias), necessidades operacionais para cada órgão que compõe o sistema ATC, e os espaços que os controladores proverão a separação entre todas as aeronaves. A esse conjunto de decisões é dado o nome de ATM, que foi ramificado em três partes:

1. **Gerenciamento do Espaço Aéreo:** Controla as divisões dos espaços aéreos controlados, não controlados e condicionados. Através dessa divisão são determinados os conjuntos de responsabilidades e deveres dos pilotos e controladores.
2. **Gerenciamento de Fluxo de Tráfego Aéreo:** Consiste em adotar ações necessárias, levando-se em conta três fases de planejamento: a estratégica (operações coordenadas com os prestadores de serviço), a pré tática (baseia-se nas mudanças meteorológicas e de demandas) e a de operações táticas (ações diante situações imprevisíveis).
3. **Serviços de Tráfego Aéreo:** Relação entre os pilotos das aeronaves e os operadores de algum órgão de tráfego aéreo, por meio da comunicação para que os objetivos de ambos sejam entendidos e atendidos.

4.2 ESTRUTURA DO ESPAÇO AÉREO

Para um gerenciamento efetivo, o espaço aéreo do Brasil foi divido em:

- Superior, com limite inferior no nível de voo 245 (FL 245 - 24.500 pés ou cerca de 7.500 metros de altitude) e superior ilimitado.
- Inferior, com limite superior no FL 245 inclusive e inferior no nível do solo ou água.

Os limites laterais de cada um estão determinados nas Cartas de Rota (ERC). Essa divisão tem por finalidade estabelecer as partes do espaço aéreo onde aeronaves de porte e desempenhos semelhantes podem voar, assim é possível tornar compatível os tipos de aeronaves em trânsito nas vias com o espaçamento exigido para elas pelas normas, além do tipo de topografia do caminho e outros fatores que dependam de sua categoria (BAUM, 2007).

Dentro dessa divisão física do espaço aéreo, existem as três categorizações citadas anteriormente, que são os espaços controlados, não controlados e condicionados.

4.2.1 Espaço Aéreo Controlado

Um espaço aéreo é dito controlado se for possível manter uma comunicação bilateral contínua entre o órgão de controle do espaço e as aeronaves transitando nele. Internamente todos os movimentos das aeronaves são controlados por algum órgão de tráfego aéreo mantendo os pilotos em rotas conhecidas e executando manobras pré estabelecidas, de forma a garantir a segurança de todas as aeronaves nesse espaço. Para melhor caracterizá-lo e decidir qual serviço é mais adequado para determinado lugar ou momento, esse espaço é dividido nas seguintes cinco partes, de menor para a maior em tamanho físico.

Cada uma dessas áreas é controlada por algum órgão de controle de tráfego aéreo (ACC, APP ou TWR), sendo oferecidos certos tipos de ATS para elas. Esses órgãos e serviços serão descritos detalhadamente mais adiante. As regiões deste espaço aéreo ainda são categorizadas em classes (A, B, C, D, E e F) de acordo com algumas características dos voos neles permitidos.

- **Classe A:** Permitidos apenas voos IFR[1]. Todos os voos recebem serviços de controle de tráfego aéreo e são separados entre si.
- **Classe B:** Permitidos voos IFR e VFR[2]. Todos os voos recebem serviços de controle de tráfego aéreo e são separados entre si.

[1] Regras de voo por instrumentos: conjuntos de regras das quais o piloto se utiliza para pilotar a aeronave utilizando apenas os instrumentos de bordo (FAA, 2012a)

[2] Regras de voo visual: conjunto de regras que ajudam na operação da aeronave quando as condições atmosféricas permitem o controle visual de altitude e separação (FAA, 2014)

- **Classe C:** Permitidos voos IFR e VFR. Todos os voos recebem serviços de controle de tráfego aéreo. Os voos IFR são separados de outros voos IFR e VFR. Os voos VFR são separados apenas dos voos IFR e recebem informações de tráfego em relação aos outros voos VFR e aviso para evitar tráfego, quando solicitado pelo piloto.

- **Classe D:** Permitidos voos IFR e VFR. Todos os voos recebem serviços de controle de tráfego aéreo. Os voos IFR são separados de outros voos IFR e recebem informação de tráfego em relação aos voos VFR e aviso para evitar tráfego, quando solicitado pelo piloto. Os voos VFR recebem apenas informação de tráfego em relação a todos os outros voos e aviso para evitar tráfego, quando solicitado pelo piloto.

- **Classe E:** Permitidos voos IFR e VFR. Somente os voos IFR tem acesos ao serviço de controle de tráfego aéreo e estes são separados dos outros voos IFR. Todos os voos recebem informação de tráfego sempre que for factível.

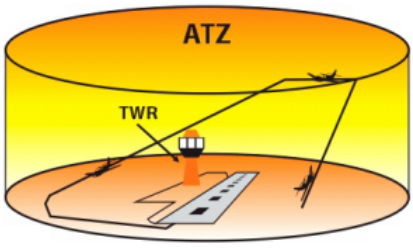
- **Classe F:** Permitidos voos IFR e VFR. Somente os voos IFR tem acesso ao assessoramento de tráfego aéreo. Todos os voos recebem serviço de informação de voo, quando solicitado pelo piloto.

- **Classe G:** Permitidos voos IFR e VFR, recebendo somente serviço de informação de voo, sempre que for factível.

Zona de Tráfego de Aeródromo

Espaço aéreo estabelecido em torno de um aeródromo, envolvendo o circuito de tráfego e o espaço de manobras das aeronaves. O circuito de tráfego é um conjunto de trajetórias especificadas que devem ser seguidas pelas aeronaves que estejam nas imediações de um aeródromo, em geral formada por espirais de curvas em ângulos retos à esquerda, como mostra a Figura 9.

Figura 9 – Esquema de uma ATZ

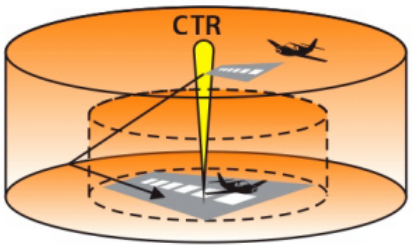


Fonte: Baum (2007, p. 24)

Zona de Controle

Espaço aéreo que envolve um ou mais aeródromos próximos, capaz de conter as trajetórias dos procedimentos de aproximação e saída por instrumentos (Figura 10).

Figura 10 – Esquema de uma CTR

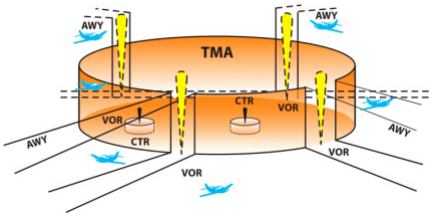


Fonte: Baum (2007, p. 24)

Área de Controle Terminal

É formada pela junção de todas as rotas que possuem serviços de tráfego aéreo associadas, envolvendo os procedimentos de chegada ou saída de um ou mais aeródromos. Pode conter mais de uma CTR e forma um espaço aéreo controlado adicional para aproximações e saídas dos aeródromos dessas CTR (Figura 11).

Figura 11 – Esquema de uma TMA



Fonte: Baum (2007, p. 24)

Área de Controle

Compreende as aerovias (AWY) inferiores, uma ou mais áreas de controle terminais e outras áreas do espaço aéreo inferior. Aerovias são áreas do espaço estabelecidas em forma de corredor, ligando em geral o aeroporto de saída com o de chegada das aeronaves.

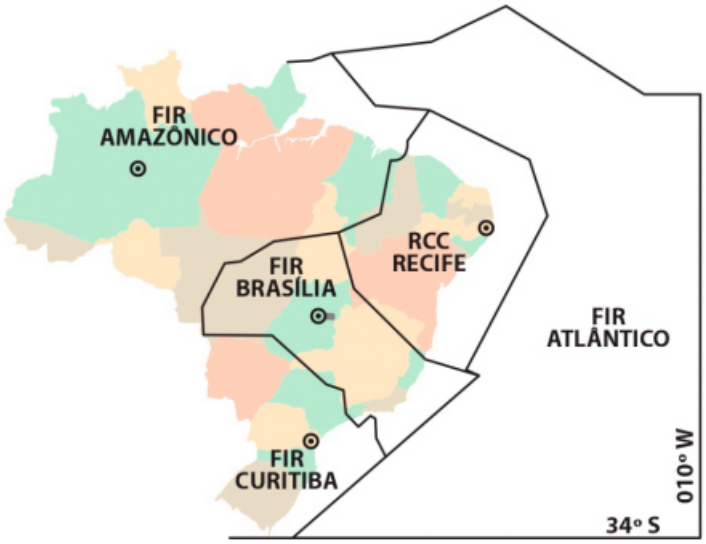
Área Superior de Controle

Compreende basicamente uma parte do espaço aéreo superior e as aerovias superiores.

4.2.2 Regiões de Informação de Voo

Espaços aéreos onde são prestados os serviços de informação de voo e de alerta. Existem cinco FIR no Brasil: Amazônica, Recife, Brasília, Curitiba e Atlântico como mostra a Figura 12.

Figura 12 – Imagem da divisão das FIRs brasileiras



Fonte: Baum (2007, p. 24)

O Serviço de Informação de Voo (FIS) fornece uma série de dados atmosféricos, climáticos e quaisquer outros que sejam importantes para a segurança da aeronave. Já o serviço de alerta emite alertas às aeronaves que tenham apresentado um plano de voo VFR e não tenham chegado ao aeródromo de destino.

4.2.3 Espaço Aéreo Condicionado

Os espaços aéreos condicionados são espaços aéreos com restrição à circulação aérea geral, de dimensões definidas, dividindo-se em três partes de limites indicados nas cartas aeronáuticas e manuais (AIP-BR, ASIL, SID, IAC) do DECEA. Os três segmentos são identificados da seguinte forma:

- Área Proibida (P): Voo não é permitido sob nenhuma circunstância.

- Área Restrita (R): Voo só é autorizado sob condições pré estabelecidas.
- Área Perigosa (D): Espaço aéreo com riscos potenciais ou reais de navegação.

4.3 ESTRUTURA DOS SERVIÇOS DE CONTROLE DE TRÁFEGO AÉREO

Para um gerenciamento e controle de tráfego aéreo mais eficiente, foram definidos três órgãos para dividir as responsabilidades do sistema de controle, baseados nas regiões e tipos de espaços e fases de voo da aeronave. Para tal, esses três órgãos oferecem os serviços adequados para cada necessidade das aeronaves e do sistema.

4.3.1 Serviço de Controle de Área

O órgão responsável é o ACC, cujas jurisdições englobam as FIR, Área de Controle (CTA) e áreas de manobra e ajuda das FIR. Os outros dois órgãos (APP e TWR) são sempre subordinados ao ACC responsável pela FIR em que estão inseridos.

No Brasil, existem cinco desses centros, localizados em Brasília, Curitiba, Manaus e Recife, sendo que a capital pernambucana abriga dois deles: um responsável pelo espaço aéreo continental do Nordeste e outro de todo o espaço aéreo oceânico sob a responsabilidade brasileira.

4.3.2 Serviço de Controle de Aproximação

O serviço de controle de aproximação tem como função emitir autorizações de tráfego às aeronaves que estiverem voando ou que queira voar dentro das TMA ou CTR, com os objetivos de manter as separações mínimas entre elas, acelerar e manter ordenado o fluxo de tráfego aéreo e instituir as aeronaves nos procedimentos de espera, chegada e saída estabelecidos pelo DECEA.

O órgão responsável por este serviço é o Centro de Controle de Aproximação (APP), que está subordinado ao ACC e mantém as torres dos aeródromos sobre a sua juridição. Atualmente existem 47 unidades de APP no Brasil.

4.3.3 Serviço de Controle de Aeródromo

O serviço de controle de aeródromo é prestado por uma TWR. Ela controla todas as aeronaves voando nos circuitos de tráfego do aeródromo, operando em áreas de manobras, pousando, decolando e veículos operando em áreas de manobra. A TWR está em constante comunicação com o ACC e APP sobre possíveis falhas em equipamentos, luzes ou outros dispositivos do aeroporto. Devem informar aos outros dois órgãos a respeito das aeronaves

que deixarem de se comunicar com a TWR, por qualquer motivo. Ela é responsável também pelo horário de saída e chegada das aeronaves e de encaminhas essas informações ao ACC responsável.

Para conseguir desempenhar todas essas atividades, os ATCos da TWR podem se dividir em três posições dentro da torre:

- Autorização de Tráfego (CLR): Responsável em emitir as autorizações de decolagem às aeronaves segundo os seus planos de voo autorizados.
- Controle de Solo (GND): Responsável por coordenar todo o tráfego nas pistas e *taxiways*, seja das aeronaves, veículos ou pessoal autorizado.
- Torre de controle de aeródromo (TWR): Responsável pelo sequenciamento das aeronaves que chegam e saem do aeródromo, comunicação com as aeronaves próximas e com o ACC sobre as aeronaves entrando e saindo dos entornos do aeródromo.

Caso o tráfego dentro do aeródromo não demande muito dos controladores, cada função de uma posição pode ser agrupada pela outra, da primeira para a última, ou seja, o serviço de controle de solo pode ser responsável pela autorização de tráfego caso a demanda seja pequena e a posição da torre pode agrupar os outros dois caso seja menor ainda a demanda.

4.4 PANORAMA PARA O ATM GLOBAL

Como discutido na introdução, o conceito do ATM evoluiu para o CNS-ATM e depois para o ATM Global. Esta última foi consolidada em 2003 definindo que a OACI, os Estados membros e os Grupo Regional de Planejamento e Implantação (PIRG) devem considerar o ATM Global como um marco mundial comum como forma de guia de implantação nos sistemas ATM. Todos deverão proceder conjuntamente na implementação do conceito, de acordo com os preceitos e componentes do mesmo, descritos no documento 9854 NA/458 da OACI (ICAO, 2005). Os três componentes anteriores de ATS (serviços de alerta, informação de voo e de controle de tráfego aéreo)(ICAO, 1998) foram reformulados em novos sete:

1. Organização e Gerenciamento do Espaço Aéreo (AOM)
2. Operações de Aeródromos (AO)
3. Balanceamento de Demanda e Capacidade (DCB)
4. Sincronização de Tráfego (TS)

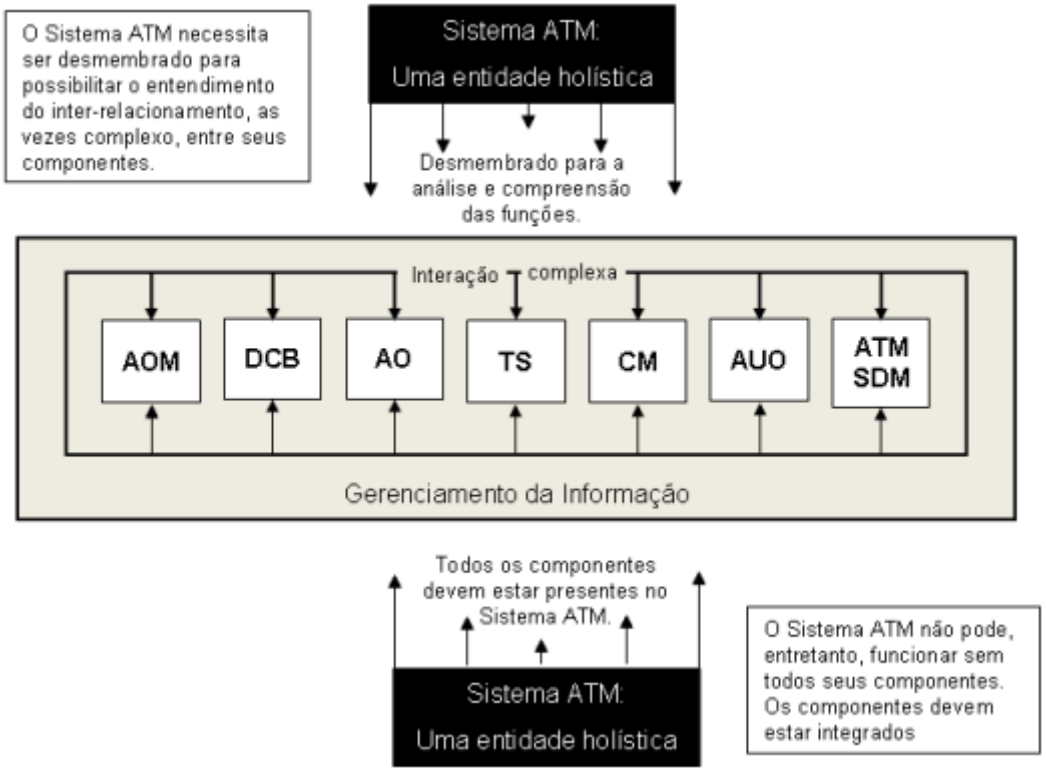
5. Gestão de Conflitos (CM)

6. Operações dos Usuários do Espaço Aéreo (AUO)

7. Gerenciamento de Prestação de Serviços (ATMSDM)

A visão do ATM Global descreve como o Sistema de Navegação Aérea (ANS) deve operar de forma integrada e global; a base dos novos serviços e como eles vão interagir de forma integrada, utilizando uma estratégia colaborativa para resolver a maioria dos problemas de forma estratégica (SILVA, 2010). A Figura 13 sintetiza os componentes presentes nessa concepção.

Figura 13 – Estrutura dos Componentes do Sistema ATM Global



Fonte: DECEA (2011)

Além desses sete componentes, a OACI definiu onze Áreas de Desempenho Chave (KPA), que são as expectativas da comunidade ATM em relação ao ATM Global, sendo elas:

1. Acesso

2. Equidade.

3. Capacidade.
4. Eficiência.
5. Ambiente.
6. Flexibilidade.
7. Interoperabilidade global.
8. Participação pela comunidade ATM.
9. Previsibilidade.
10. Segurança Crítica (*Safety*).
11. Segurança da Informação (*Security*).

Essas KPA's definem os objetivos gerais que a implantação do ATM Global deve seguir, não necessariamente na ordem apresentada.

A maioria das pesquisas agora visa entender os novos conceitos, tecnologias e técnicas que serão a base nessa evolução para o ATM Global. Como os interesses envolvidos abrangem aspectos econômicos, políticos, desempenho e segurança (ICAO, 2013), as pesquisas relacionadas a esse assunto são diversificadas.

4.5 DEFINIÇÃO FUNCIONAL DO ATCO

Através das revisões bibliográfica e da documentação oficial do DECEA foi possível realizar um levantamento dos requisitos operacionais das tarefas dos ATCo's de uma TWR no Brasil. Através disso, foram criados os modelos operacionais das tarefas realizadas pelo ATCo (independente da sua posição) dentro da TWR - Etapa 3.1.2.1 (DIRICKSON; VISMARI; CAMARGO, 2013).

Os modelos foram desenvolvidos utilizando o método eFFBD[3], método formal de comportamento utilizado na formalização de projetos de engenharia de sistemas, utilizado pela Airbus, NASA e Boeing (LETCHWORTH; SCHLIERF, 2012; SEIDNER; ROUX, 2008).

Os elementos principais da eFFBD são os blocos, representadas por caixas de borda arrendondada, um título e um número. Cada bloco representa uma tarefa no tempo de execução do sistema. A ligação lógica entre os blocos é feita utilizando setas. Utiliza-se portas lógicas (E/& e OU) e de iteração (IT e LOOP) para controlar a lógica do fluxo de

[3] Mais detalhes sobre as eFFBD podem ser encontrados em Letchworth e Schlierf (2012), Seidner e Roux (2008), Yoon et al. (2008)

atividades. Os balões representam o fluxo de dados das atividades, podendo ser utilizado como dados disparadores ou não de novas atividades. representando a sequência de tarefas necessárias para que a primeira se realize, podendo ser quebrado em quantos níveis se desejam.

É apresentado a seguir de maneira resumida cada um dos diagramas produzidos[4]:

4.5.1 Controle de Aeródromo

Esse é o modelo inicial (Figura 14), mostrando as cinco tarefas paralelas que os controladores devem executar. Cada uma delas vai ser quebrada num nível para melhor descrevê-las.

4.5.2 Controle das Aeronaves que Deixam o Aeródromo

Esse primeiro modelo representa as ações necessárias para autorizar uma aeronave sair do aeródromo, desde o acionamento dos motores até a sua decolagem (Figura 15). Esse grupo de tarefas ainda depende do diagrama 3.0 (Controle de aeronaves em solo). A tarefa 1.5 (Autorizar Decolagem) será quebrada mais um nível, dado a sua complexidade.

4.5.3 Autorização de Decolagem

Essa eFFBD (Figura 16) mostra a sequência necessária para a tarefa 1.5 do modelo anterior. Esse modelo é um intermediário entre tarefas do modelo 1.0, não depende diretamente de nenhum outro.

4.5.4 Controle de Aeronaves que Chegam ao Aeródromo

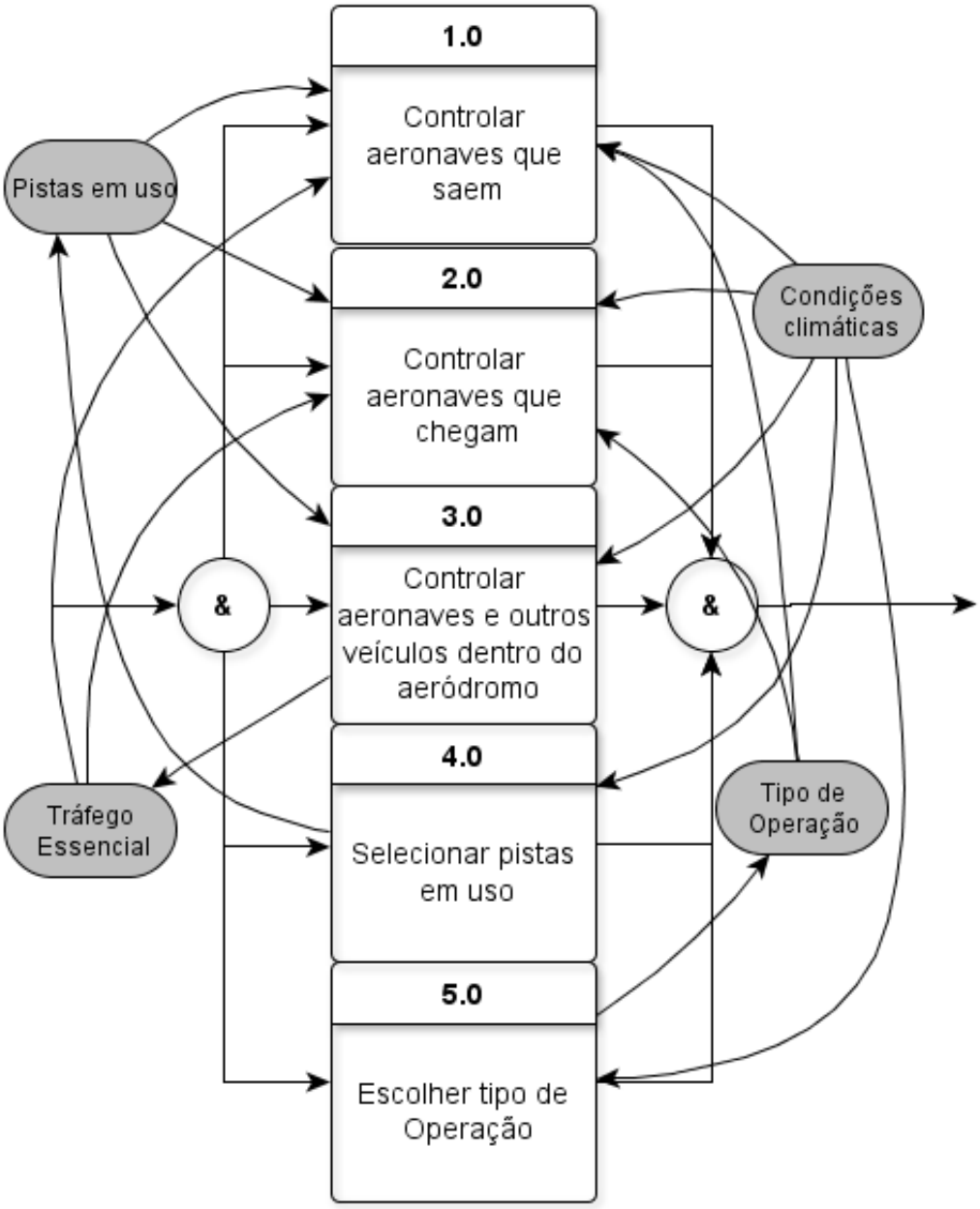
Esse modelo representado na figura 17, mesmo aparentando ser simples, é um dos mais complexos, necessitando que a atividade 2.2 seja quebrada em outro diagrama maior e mais detalhado do controle de aeronaves no circuito de tráfego.

4.5.5 Controle de Aeronaves no Circuito de Aeródromo

Nesse modelo da figura 18 é o conjunto de tarefas em que o ATCo e o piloto mais se conversam, pois a todo momento o controlador necessita saber a posição exata do piloto para que ele possa manter a separação mínima entre as outras aeronaves.

[4] Mais detalhes Dirickson, Vismari e Camargo (2013)

Figura 14 – eFFBD Controle de Aeródromo

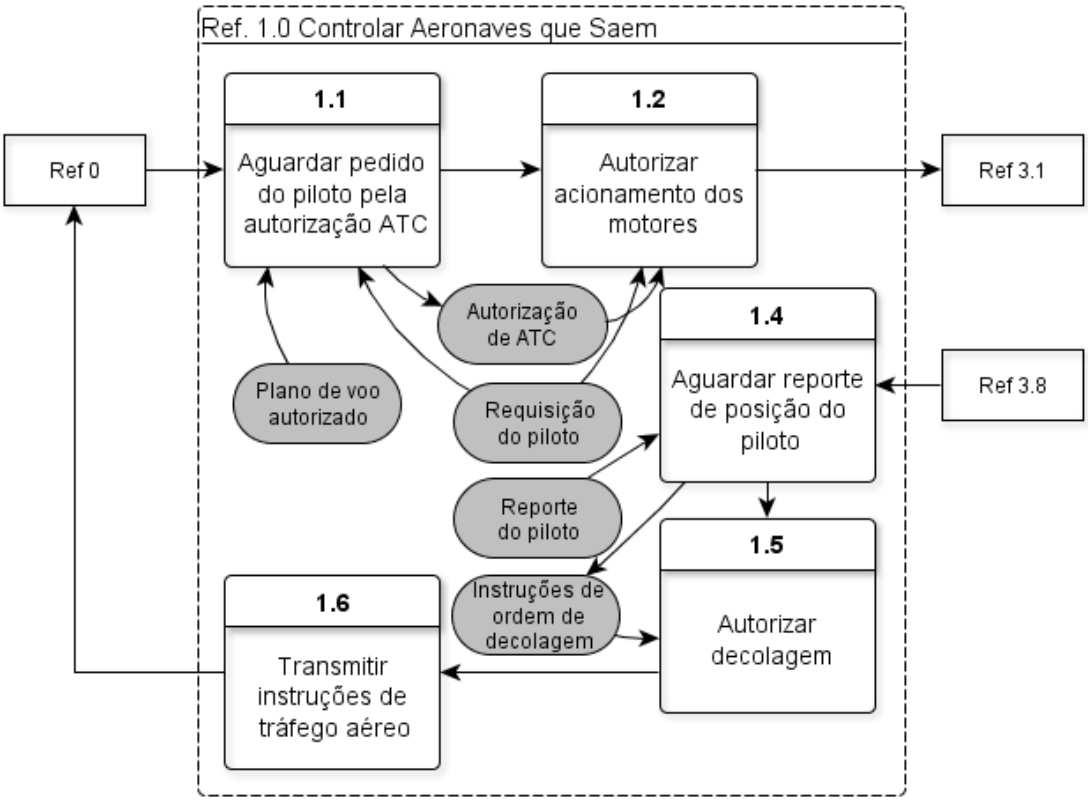


Fonte: Dirickson, Vismari e Camargo (2013)

4.5.6 Controle de Aeronaves em Táxi

O modelo da Figura 19 é o maior em número de tarefas, pois o controlador está observando tanto as aeronaves que estão chegando, quanto as que estão saindo, que podem estar utilizando as mesmas vias e pistas, praticamente de maneira simultânea.

Figura 15 – eFFBD Controle de Aeronaves que Deixam o Aeródromo



Fonte: Dirickson, Vismari e Camargo (2013)

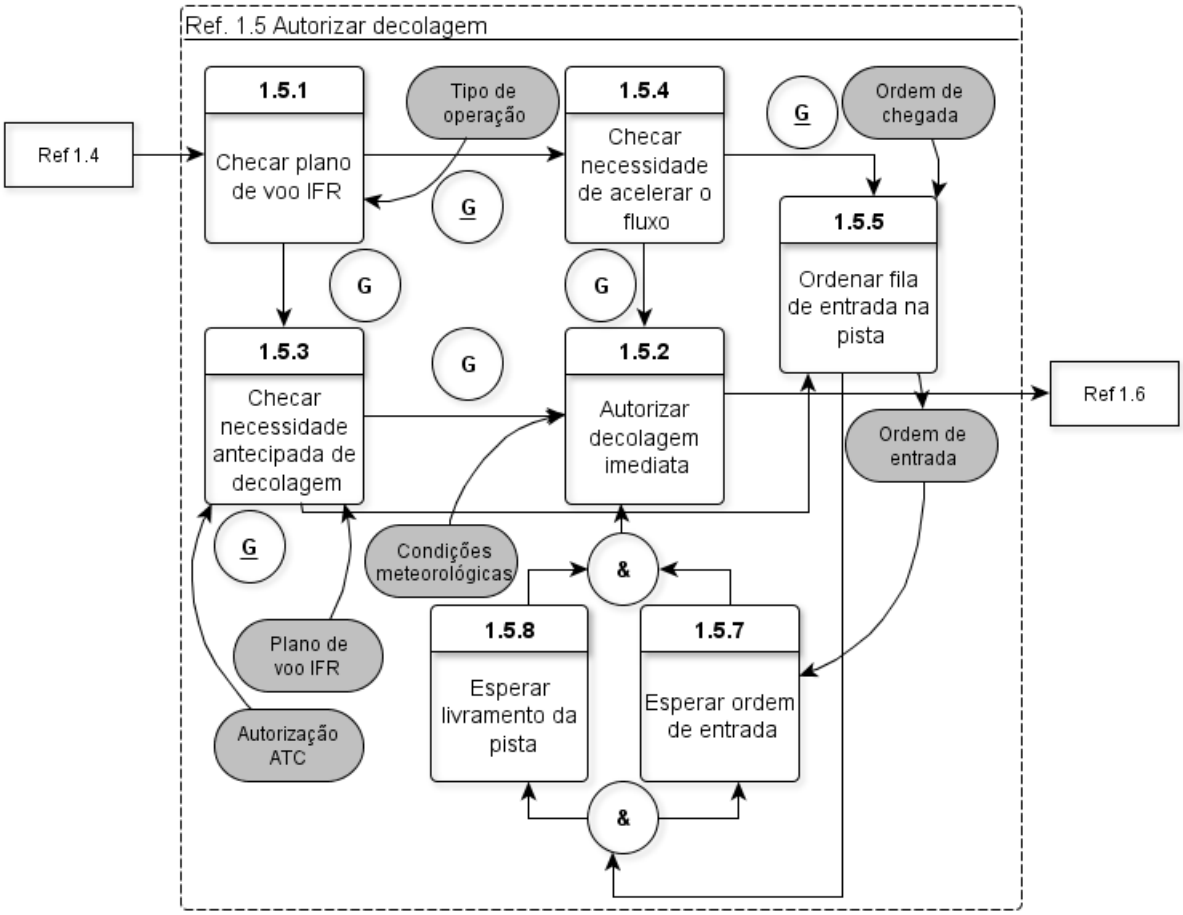
4.5.7 Seleção de Pistas em Uso

A Figura 20 representa a sequência lógica que o ATCo utiliza para escolher quais pistas do aeródromo (quando existe mais do que uma possível) são mais adequadas para os pousos e decolagens. Preferencialmente as aeronaves devem decolar e pousar na direção oposta ao vento.

4.5.8 Escolha do Tipo de Operação

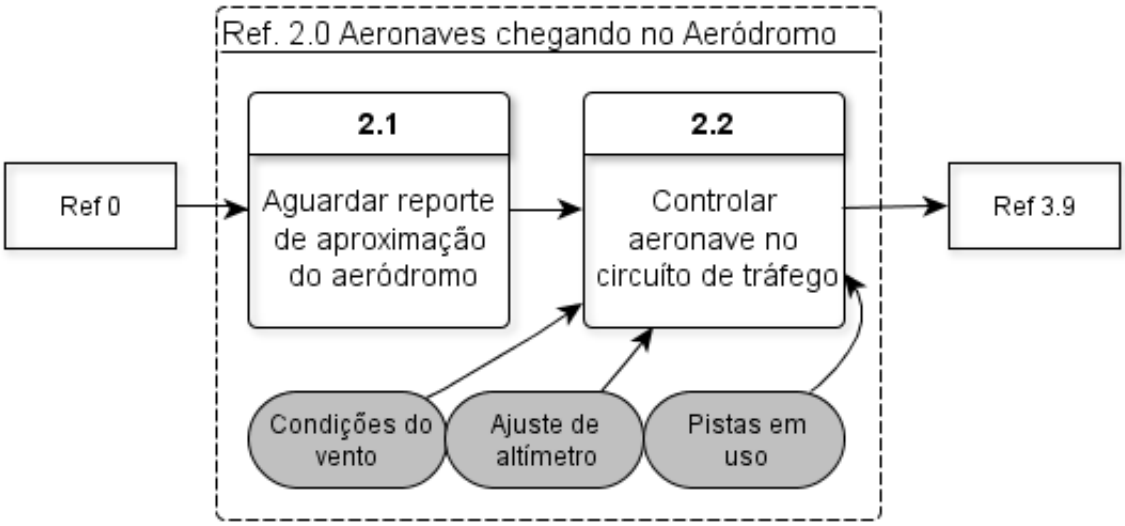
Dentro da região do aeródromo, o ATCo da TWR tem a incumbência de decidir, baseando-se nas condições meteorológicas e de visibilidade do aeródromo, se as aeronaves devem seguir em VFR, IFR ou a suspensão das operações do aeródromo, conforme mostra a figura 21.

Figura 16 – eFFBD Autorização de Decolagem



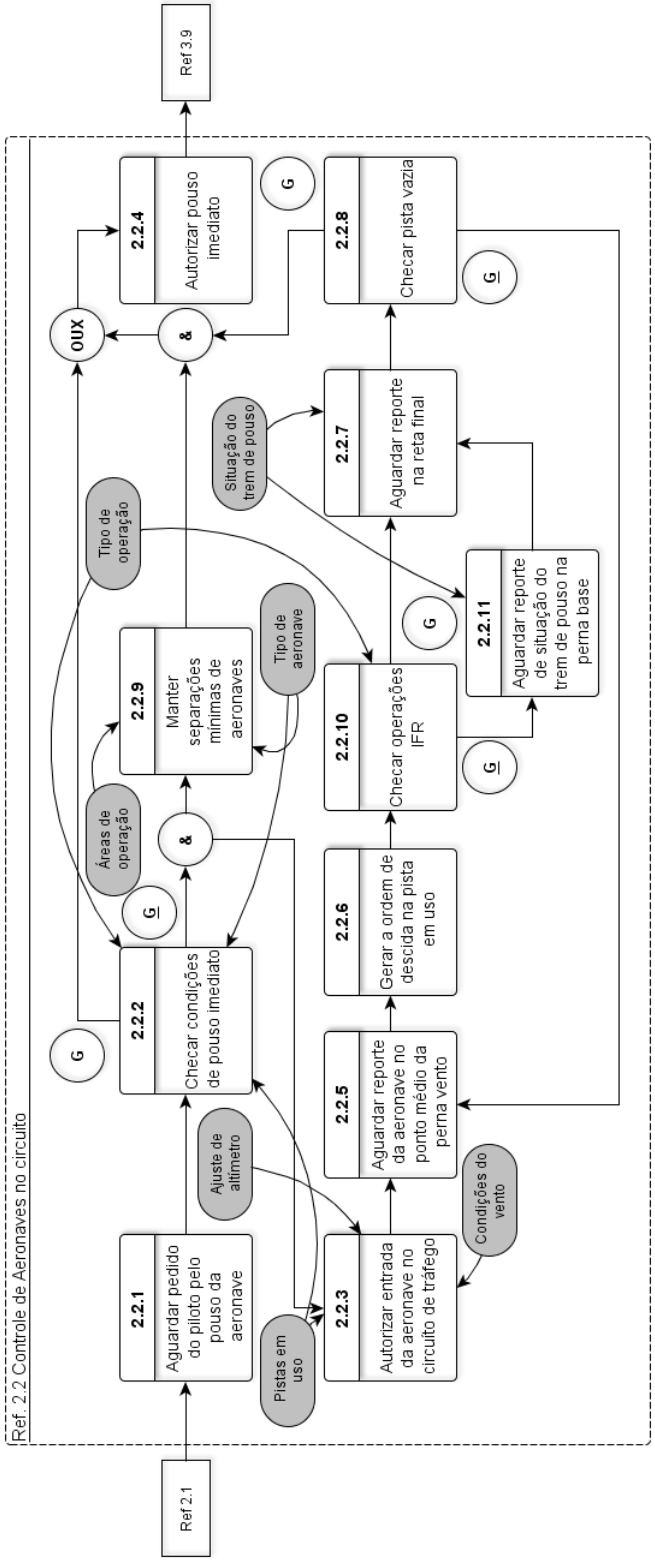
Fonte: Dirickson, Vismari e Camargo (2013)

Figura 17 – eFFBD Aeronaves chegando no Aeródromo



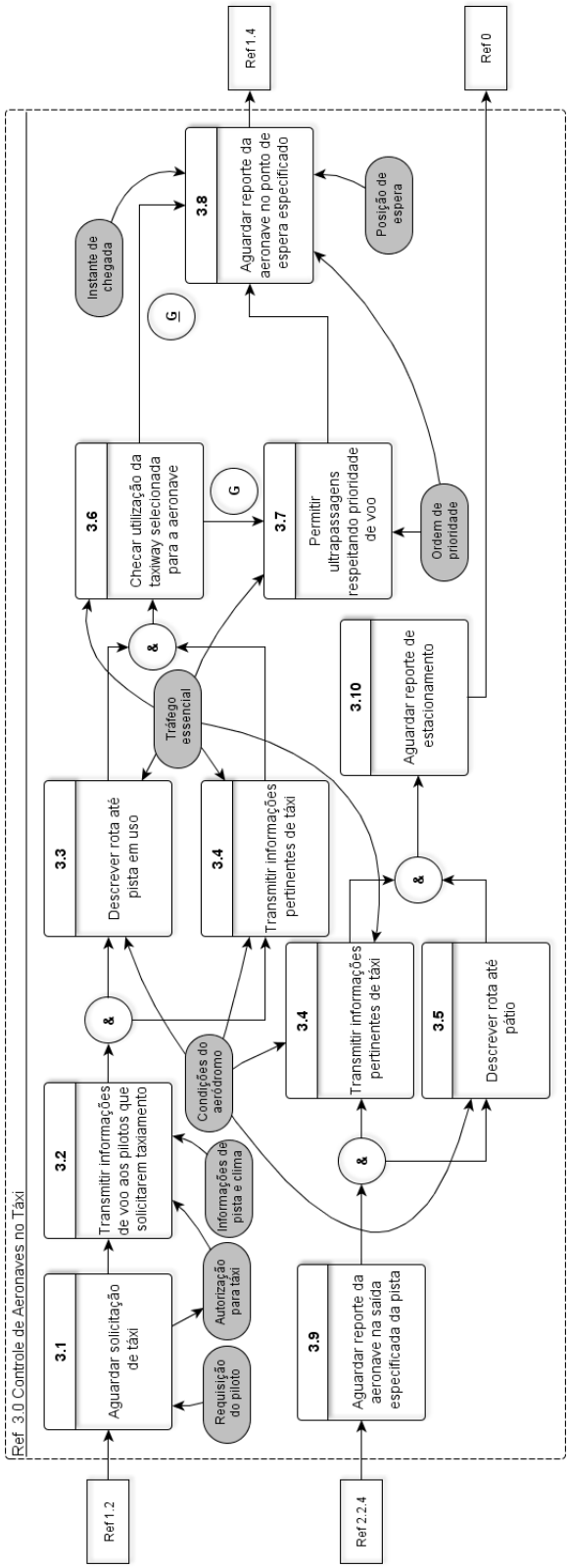
Fonte: Dirickson, Vismari e Camargo (2013)

Figura 18 – eFFBD Controle de aeronaves no circuito de tráfego



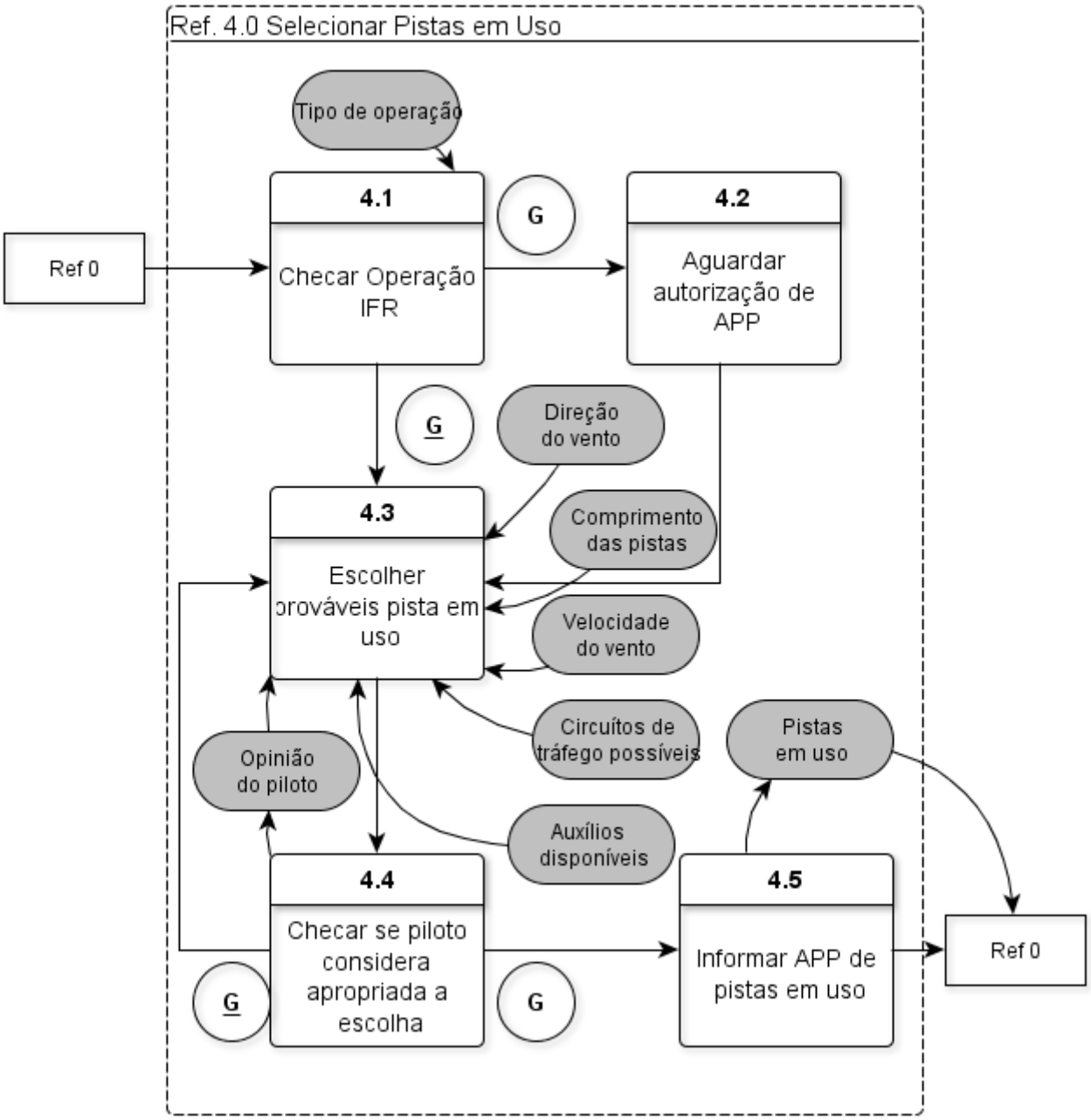
Fonte: Dirickson, Vismari e Camargo (2013)

Figura 19 – eFFBD Controle de aeronaves em Táxi



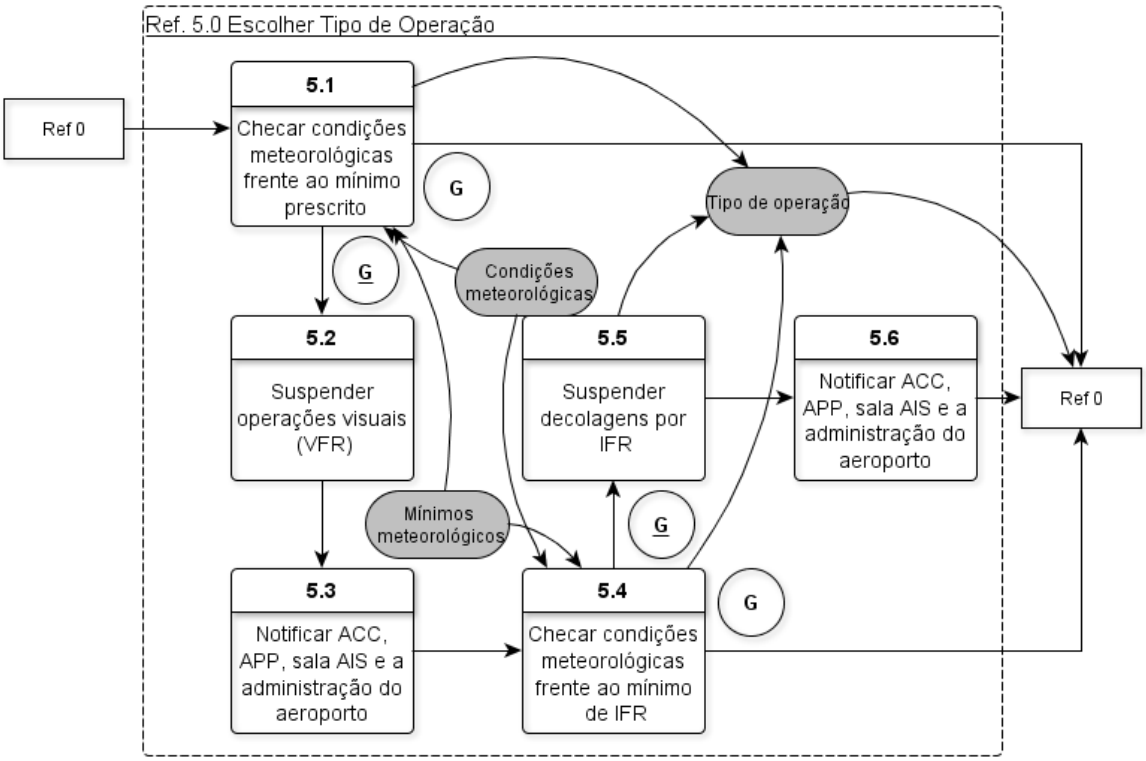
Fonte: Dirickson, Vismari e Camargo (2013)

Figura 20 – eFFBD Seleção de Pistas em Uso



Fonte: Dirickson, Vismari e Camargo (2013)

Figura 21 – eFFBD Escolher tipo de operação



Fonte: Dirickson, Vismari e Camargo (2013)

5 APRESENTAÇÃO DA METODOLOGIA DE ANÁLISE PROPOSTA

Nesse capítulo será apresentado a metodologia proposta para a análise de impacto, que utiliza a técnica STPA, derivada do modelo STAMP, em ambos cenários automático e manual. Os passos descritos neste capítulo foram retirados basicamente de Leveson (2012) e Thomas (2013), onde este último desenvolveu uma metodologia sistemática de aplicação do STPA, e adicionados um passo adicional de análise dos fatores causais levantados.

5.1 ANÁLISE DE PERIGOS

Para a análise de perigo foi utilizada uma técnica derivada do modelo STAMP, o System Theoretic Proccess Analysis (STPA). Ela é uma técnica de análise de perigos (*hazard*) com o objetivo de coletar informações de como os perigos podem aparecer, e em quais cenários, da mesma forma que todas as outras técnicas tradicionais, com a diferença de que: (1) o STPA utiliza a teoria de sistemas para a análise, ao invés da de confiabilidade, não tratando erros como falhas de componentes e sim um problema de controle, o STPA consegue determinar um número maior de perigos, principalmente aqueles referentes a questões organizacionais e (2) o STPA não gera nenhum número de probabilidade para os perigos, uma vez que isso só seria possível se fosse omitido uma série de fatores da análise que não são de natureza estocástica ou que não possuem informação probabilística disponível.

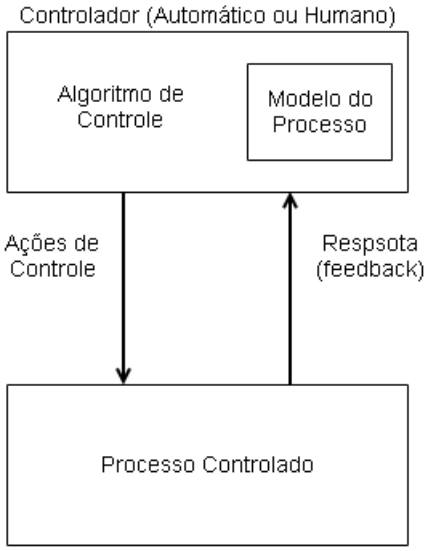
O STPA é dividido em quatro grande partes, onde a primeira é tratada como uma preparação (fundamentação) da técnica em si, as duas seguintes a aplicação da técnica e a quarta seria a recomendação feita com base nos dados levantados. As quatro parte são:

- Definir os conceitos de engenharia de sistemas utilizados para a análise, incluindo como é o fluxo de controle da estrutura do sistema.
- Identificar as ações de controle potencialmente inseguras.
- Criar restrições de segurança em cima das ações levantadas.
- Determinar como cada uma das ações poderia acontecer.

5.1.1 Conceitos de Engenharia de Sistemas e Fluxo de Controle

A primeiro parte do STPA é estabelecer o embasamento teórico que será utilizado durante a aplicação da técnica. Primeiro deve-se estabelecer os conceitos básicos de engenharia de sistemas utilizados como o que se considera como acidentes, perigos e segurança e também um modelo da estrutura de controle sendo analisada, em geral representada por um fluxograma (como na figura 22).

Figura 22 – Fluxo de controle genérico.



Fonte: Adaptado de Leveson e Thomas (2013)

Em seguida, os tipos de acidentes que vão ser considerados na análise devem ser levantados, identificando todos os perigos relacionados a estes acidentes. Desta forma é delimitado o escopo da análise feita pelo STPA e se evita que gaste-se tempo com a busca de ações e causas que não estejam ligados com o que está sendo analisado (FLEMING et al., 2013).

5.1.2 Identificar Possíveis Ações Inseguras de Controle

De maneira geral, o STPA define os seguintes tipos de Ação Insegura de Controle (AIC):

1. Ação insegura que coloca o sistema em um estado de perigo.
2. Uma ação necessária para evitar um perigo não é feita.
3. Um controle possivelmente seguro ocorre de maneira tardia, muito antecipada ou fora da sequência com o evento de perigo.

4. O controle seguro acaba muito cedo ou é aplicado por mais tempo do que deveria.

A maneira mais conveniente de escrever os resultados é em tabela como a tabela 3. A primeira coluna marca o tipo de ação sendo considerada, que deve estar presente no levantamento anterior. Cada uma das outras colunas indica as condições em que a ação pode gerar um perigo (se existir), juntamente com o tipo de perigo em questão.

Tabela 3 – Exemplo de tabela do STPA

	Causa perigo se			
Ação de Controle	**Não executar**	**Executar**	**Executar muito cedo, muito tarde ou fora de ordem**	**Acabar antes ou aplicar por muito tempo**
Ação	Condição	Condição	Condição	Condição

Thomas (2013) define uma maneira sistemática de encontrar as possíveis AIC, dividindo esta tarefa em duas subcategorias: ações executadas que podem levar a um perigo e ações que *não executadas* podem levar a um perigo.

Para cada ação que o controle analisado pode executar, será construída uma tabela de contexto, como a tabela 4, para tentar determinar se a ação em questão é uma possível AIC. Na tabela, a primeira coluna marca qual ação está em análise (suprimida por simplicidade).

As próximas n colunas são as n variáveis de contexto para esta ação, bem como as possíveis combinações das mesmas. Variáveis de contexto são parâmetros que os controladores utilizam ao desempenhar suas funções, elas podem ser respostas (*feedback*) do processo controlado (ex: um alarme avisando que há emergência em um trem de pouso) ou um parâmetro que seja coletado por fora, como um sensor que não faz parte do controle (ex: dados climáticos para o ATCo). Para cada combinação possível é dado o nome de **contexto**.

As últimas três colunas da tabela de contexto guardam informações referentes à ocorrência de perigos no contexto em específico da linha. A primeira das três colunas marca se a ação leva a um perigo (e qual), a segunda se a execução adiantada da ação leva a um perigo (e qual) e por último se execução tardia leva a um perigo (e qual).

A segunda parte leva consideração que por algum motivo a ação *não foi executada*. Neste caso apenas precisa se determinar se a ausência de ação em um determinado contexto pode causar algum tipo de perigo, como mostra a tabela 5.

Para cada AIC encontrada, é possível derivar uma RS correspondente. Thomas (2013) define que para cada AIC que executada pode causar perigos, uma RS foi violada,

Tabela 4 – Exemplo de tabela de contexto da execução de ação

Var 1	**Var 2**	**Var 3**	**...**	**Var n**	**Executada?**	**Causa perigo se Executada muito cedo?**	**Executada muito tarde?**
v_1	v_2	v_3	...	v_n	Sim/Não	Sim/Não	Sim/Não

Tabela 5 – Exemplo de tabela de contexto de ausência de ação

Var 1	**Var 2**	**Var 3**	**...**	**Var n**	**Não executada gera perigo?**
v_1	v_2	v_3	...	v_n	Sim/Não

portanto, uma RS seria a negativa da AIC encontrada. Um exemplo:

- **AIC**: Comando de abrir a porta do trem executado enquanto o trem está em movimento.
- **RS**: Comando de abrir a porta não pode ser executado enquanto o trem estiver em movimento.

Da mesma forma para uma AIC que quando não executada pode levar a um perigo:

- **AIC**: Comando de abrir a porta do trem não executado enquanto o trem está parado na plataforma e uma pessoa está presa na porta.
- **RS**: Comando de abrir a porta do trem deve ser executado enquanto o trem está parado na plataforma e uma pessoa está presa na porta.

Em alguns casos podem existir conflitos de restrições, como por exemplo:

- RS_1: Comando de abrir portas deve ser acionado quando pessoa está presa na porta.
- RS_2: Comando de abrir portas não deve ser acionado quando trem está se movendo.

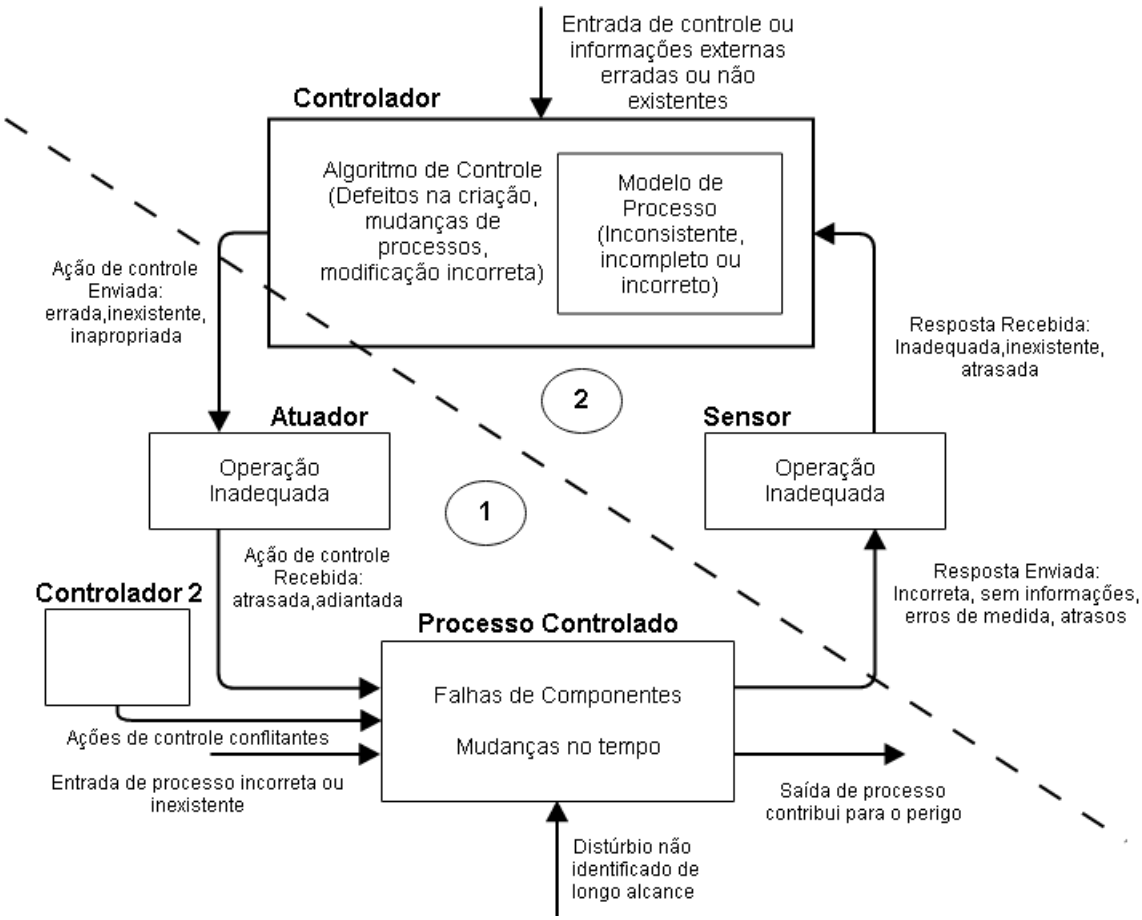
Nesse caso, se o trem estiver se movendo e existir uma pessoa presa na porta, existe um conflito de restrições. Pode-se resolver adotando um procedimento padrão, por exemplo, que neste caso é mais seguro manter a porta fechada até que o trem pare e alguém possa ajudar a pessoa presa, mas nem sempre é possível resolver desta maneira. Quando não for possível, deve-se analisar esses casos fora da questão de controle do sistema, tentando impedir esses acontecimentos a nível de projeto ainda (LEVESON; THOMAS, 2013).

5.1.3 Determinar as Causas de cada Ação Insegura

Além de se determinar as AICs, é importante também determinar as causas possíveis para elas e levantar como elas aconteceram e poderiam ser evitadas. Como foi apresentado, apenas estudar as AICs não é suficiente, pois mesmo uma ação segura pode levar a um perigo, dado que os componentes envolvidos podem falhar em algum momento, portanto a esta fase do STPA é feita com base nas restrições de segurança. Para tanto, o levantamento das possíveis causas é dividido em duas frentes: (1) Como as restrições de segurança podem não ser obedecidas e (2) Identificação de como as AICs acontecem. A parte (1) é vista como uma análise do porque uma ação segura foi tomada mas não executada pelo controle.

A figura 23 resume de forma genérica os possíveis fatores causais que podem ser encontrados em um fluxo de controle.

Figura 23 – Fluxo de controle genérico com seus possíveis fatores causais.



Fonte: Adaptado de Thomas (2013)

5.1.3.1 Identificando como Ações não são executadas

Ao se analisar comando que não foram executados corretamente, é possível coletar possíveis cenários de ações não executadas diretamente das AICs geradas anteriormente. Seja C_n o cenário número n da AIC em questão, analisa-se então da seguinte forma:

- **AIC**: Comando de abrir porta de trem não executado quando o trem está parado na plataforma e existe uma pessoa presa na porta.
- **Ação/Comando**: Abrir porta do Vagão.
- **Função Esperada**: Porta abrir quando o comandada.
- **Contextos Críticos**: Porta fechando em uma pessoa, durante uma emergência, trem parado em uma plataforma.
- C_1: Comando de porta executado, mas porta não abre.

Para cada cenário levantado desta maneira, utiliza-se então a região (1) do fluxo de controle analisada (figura 23) para levantar os fatores causais relacionados ao cenário. Normalmente nesse estágio os fatores encontrados são os que estão descritos na figura 23:

- Ação de controle enviada, mas não recebida ou recebida com atraso.
- Ação de controle não enviada, mas recebida.

5.1.3.2 Identificando causas de uma AIC

Assim como determinar cenários em que ações seguras não são executadas, Thomas (2013) cita a importância em determinar cenários que possibilita a ocorrência das AIC, e suas possíveis causas. Para isso, utiliza-se a região (2) do fluxo de controle (figura 23), a região de resposta. A busca tenta encontrar possíveis falhas no modelo de processo diretamente das tabelas de contexto, por exemplo a tabela 6 mostra algumas dessas falhas.

Tabela 6 – Exemplo de falhas no modelo de processo

AIC	**Falhas no modelo de processo**
Comando de abrir a porta não é acionado enquanto o trem está parado na plataforma e uma pessoa está presa na porta.	Controlador acredita incorretamente que o trem está se movendo Controlador acredita incorretamente que não há pessoas na porta. Controlador acredita incorretamente que o trem não está alinhado na plataforma
Comando de abrir a porta é acionado enquanto o trem está se movendo	Controlador acredita incorretamente que o trem está parado.

Essas falhas estão diretamente ligadas à região de resposta do fluxo de controle. Nota-se que existe uma simetria entre a região de controle e a região de resposta da figura 23, portanto é possível construir os cenários de maneira similar às AICs, ou seja, com quatro tipo de problemas:

1. Parâmetro de resposta obrigatório para a segurança não é retornado.
2. Parâmetro de resposta é retornado com valor errado e isso leva a um perigo.
3. Parâmetro de resposta retorna com valor correto, mas muito tarde, cedo ou fora da melhor sequência, levando um perigo.
4. Resposta contínua é interrompida muito cedo ou aplicada por muito tempo, levando a um acidente.

Com base nos quatro tipos, é possível gerar cenários inseguros da mesma maneira que as AICs. Um exemplo destes cenários seria:

- **Problema**: Controlador acredita que não há emergência.
- C_1: Existe emergência, mas sinal não foi recebido.
- C_2: Sinal de não emergência foi recebido, mesmo havendo uma emergência.
- C_3: Existe emergência, mas o controlador só é notificado após X segundos da ocorrência.

Esses cenários já são considerados fatores causais de alto nível. Como o STPA é uma técnica *top-down* (THOMAS, 2013), se os analistas possuírem maiores detalhes da aplicação, é possível determinar quantas níveis de fatores causais desejáveis, por exemplo para o cenário de Sinal de emergência não emitido quando há emergência, uma análise no sensor poderia detectar que isso pode acontecer pois este não resiste a altos índices de fumaça e acaba desativando antes de emitir a emergência. O nível necessário para cada análise fica a julgamento do analista.

É possível também fazer o levantamento de requisitos de segurança referentes a aplicação específica sendo analisada, por exemplo um requisito importante seria que o sinal de emergência fosse projetado para aguentar doses altas de fumaça. Esses requisitos podem ser levantados a partir do detalhamento da aplicação analisada e também podem conter os níveis de profundidade que o analista necessitar.

5.1.4 Análise dos Fatores Levantados

Se o último passo foi executado para os cenários automático e manual, existirão agora três conjuntos de fatores causais. Define-se esses conjuntos básicos da seguinte forma:

- M: Conjunto de fatores causais referentes ao cenário manual.
- A: Conjunto de fatores causais referentes ao cenário automático.
- I: Conjunto de fatores causais que são encontrados em ambos os cenários, ou seja, $I = M \cap A$.

A partir desses conjuntos é possível fazer uma análise do impacto da automação. Neste caso não há uma sequência de tarefas a serem feitas, mas algumas comparações possíveis trazem muitas informações. As comparações mais óbvias são as de tamanhos de conjuntos, ou seja, se o número de fatores causais aumentou com a implantação da automação ou não.

Mas mais importante é a análise do conjunto I em relação ao $\overline{I}$ (complementar de I). Neste caso pode ser observado aquilo que não foi modificado em relação a automação e as diferenças entre os cenários. Um tratamento importante deve ser feito, algumas mudanças de fatores podem ocorrer mas estes serem ainda equivalentes.

Por exemplo, sejam os seguintes fatores causais para um cenário manual: *Válvula da tubulação emperra e operador não consegue fechá-la* e para um cenário automatizado: *Válvula da tubulação emperra e controle não consegue fechá-la.* Ambos são o mesmo tipo de problema (válvula não consegue ser fechada por estarem emperradas), só mudou o atuador (controlador mecânico ou operados humano). Esses casos devem ser analisados separadamente em um subconjunto de $\overline{I}$, definido como E.

Ao fim da análise, existirão então os seguintes conjuntos:

- M: Conjunto de fatores causais referentes ao cenário manual.
- A: Conjunto de fatores causais referentes ao cenário automático.
- I: Conjunto de fatores causais que são encontrados em ambos os cenários, ou seja, $I = M \cap A$.
- $\overline{I}$: Conjunto de fatores causais que são diferentes entre os cenários, ou seja, $\overline{I} = \overline{M} \cup \overline{A}$. Este conjunto é subdividido em mais dois:
  - E: Conjunto de fatores causais que são equivalentes entre si, mas não estão em I.

- $\overline{E}$: Conjunto de fatores causais que são diferente em cada cenário e não possuem equivalência.

De posse desses conjuntos o analista será capaz de determinar o impacto em relação a segurança da automação da tarefa analisada.

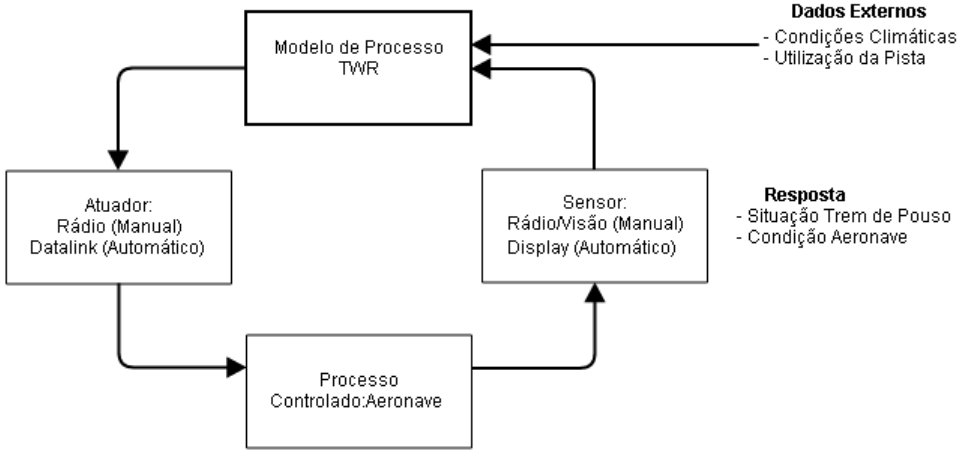
6 APLICAÇÃO DA METODOLOGIA DE ANÁLISE

Apresenta-se neste capítulo o cenário delimitado para a aplicação da metodologia proposta no capítulo 3 e a aplicação do STPA no cenário. Mostra-se a construção das tabelas de contexto, como descrito no capítulo 5, a determinação das restrições de segurança e o levantamento dos requisitos de segurança frente às restrições feitas e fatores levantados.

6.1 DEFINIÇÃO DO ESCOPO E CONCEITOS UTILIZADOS

Como forma de mostrar a eficácia da metodologia proposta, foi determinada uma tarefa de uma posição específica da TWR. A tarefa analisada é autorização de pouso de uma aeronave, executado pela posição TWR, simbolizado pelo bloco 2.2.4 do diagrama da figura 18. Como o STAMP considera acidentes como um problema de controle, desenvolveu-se um fluxo sintetizado de controle para autorização do pouso (figura 24).

Figura 24 – Esquema do Controlador



Nesse fluxo definiu-se a aeronave e sua tripulação como o processo controlado pelo ATCo. Foram considerados dois cenários para a análise, um com o canal de comunicação tradicional via rádio frequência e outro via um *link* digital de dados (*DataLink*). Ambos os cenários serão melhor apresentados na seção 6.2.

6.2 CENÁRIOS ANALISADOS

Para análise do impacto da automação de tarefas do controle de tráfego aéreo, dividiu-se o cenário em duas possibilidades: uma manual e outra automatizada.

6.2.1 Cenário Manual

O cenário manual é similar ao encontrado em grande parte do mundo (BBC, 2013). Os ATCo contam apenas com os seus recursos cognitivos, as Ficha de Progressão de Voo (FPV) em papel e um rádio para comunicação. Cada informação referente ao voo da aeronave (ex: tipo de operação, altitude, vias aéreas, etc.) deve estar devidamente anotada na FPV da aeronave e qualquer modificação nestas informações deve ser atualizada na FPV.

A comunicação em rádio é utilizada tanto com as aeronaves, quanto com outros órgãos. Neste caso o rádio será tratado como o atuador do controle sendo analisado, conforme a figura 24 mostra. Do outro lado, ele também vai ser tratado como sensor de resposta do processo controlado (aeronave). A cada controle feito pelo ATCo, o piloto da aeronave deve reportar uma confirmação. É através do rádio que o piloto informa suas posições e, caso haja, declara uma emergência, que são considerados parte das repostas do processo controlado.

Outros recursos importantes são os cognitivos do ATCo, como memória, e sensoriais, como visão. O ATCo deve, sempre que possível, confirmar com a visão todo o andamento do processo ou, quando a visão está prejudicada, contar com as FPVs e sua memória para tomar uma decisão.

6.2.2 Cenário Automático

Para este modelo, em substituição ao rádio na parte de atuação considerou-se um Datalink, que é um canal de comunicação digital com mensagens pré-formatadas com base na fraseologia utilizada entre piloto e ATCo[1]. Da mesma forma que o rádio foi utilizado como sensor, o Datalink ocupou a mesma responsabilidade para emitir as confirmações da aeronave, bem como as informações necessárias (trem de pouso, situação, posições relativas, etc.).

Por fim, o ATCo terá acesso ao Datalink através de uma interface de computador, que conta também com as informações externas, como condições climáticas e estado atual das pistas.

[1] Para mais informações em Datalink e CPDLC, ver ICAO (2013)

6.3 APLICAÇÃO DO STPA

Segue no restante do capítulo a aplicação do STPA para o cenário proposto. Retomando o capítulo 5, a análise feita pelo STPA não leva em conta o tipo de controle proposto (automático ou não) para encontrar os tipos de AIC e suas restrições, mas a partir da análise de causas de como os tipos de controle específicos foram utilizados.

6.3.1 Conceitualização da Análise

Como primeiro passo do STPA, deve-se estabelecer toda a fundação teórica do objeto em análise. A estrutura de controle já foi apresentada no capítulo 4 e sintetizada nas seções anteriores, inclusive com o seu fluxo de controle apresentado, faltando a apresentação dos perigos que foram considerados e as variáveis de contexto utilizadas. Todas as informações referentes a este contexto foram levantadas com apoio de especialistas do Instituto de Controle do Espaço Aéreos (ICEA).

Os acidentes considerados ao se determinar o pouso da aeronave foram:

- A_1: Colisão entre duas aeronaves, com uma delas na pista.
- A_2: Colisão de uma aeronave com pessoal ou veículos no aeródromo.
- A_3: Colisão de uma aeronave com um obstáculo inerte (prédios, montanhas, etc.).
- A_4: Colisão de uma aeronave com o solo.
- A_5: Morte ou ferimentos graves de pessoas dentro de uma aeronave.

Com base nesses acidentes, foram levantados os seguintes perigos:

- P_1: Aeronave inicia processo de aterrissagem com a pista ainda ocupada (referente aos acidentes A_1 e A_2).
- P_2: Aeronave opera abaixo dos mínimos estabelecidos para a sua operação (referente aos acidentes A_3 e A_4).
- P_3: Aeronave em emergência não consegue pousar imediatamente para receber o socorro necessário (referente ao acidente A_5).
- P_4: Aeronave entra em estado não-controlável (referente aos acidentes A_3 e A_4).

A tabela 7 resume o que cada um destes perigos significa.

Tabela 7 – Perigos em Análise

	Perigo	**Descrição**
P_1	Aterrissagem com pista ocupada	Aeronave inicia aterrissagem/decolagem enquanto a pista está ocupada, podendo haver uma colisão com obstáculo na pista (ex: veículos, aeronaves).
P_2	Operação abaixo dos mínimos estabelecidos	Aeronave voa em condições não recomendadas para as suas capacidades (VFR ou IFR), possibilitando a colisão da aeronave com quaisquer obstáculos, até um pouso perigoso por não haver confirmações visuais da pista.
P_3	Aeronave em emergência não consegue pousar imediatamente para receber o socorro necessário	Algo impede que uma aeronave em estado de emergência (ex: combustível, emergência interna) consiga autorização imediata de pouso (ex: outra aeronave parada na pista por algum motivo).
P_4	Estado não-controlável	Piloto perde controle da aeronave, em geral após algum tipo de manobra arriscada mal executada (ex: arremetida) ou de fatores climáticos adversos, possibilitando a queda da aeronave.

Em cada célula das últimas colunas das tabelas de contexto foi utilizada a notação P_n para identificar qual perigo é potencialmente causado na combinação específica de variáveis, sendo esses P_n referências aos perigos supracitados.

A tabela 8 resume as variáveis utilizadas, retiradas dos diagramas do capítulo 4, bem como seus possíveis valores. Os valores que estão entre parênteses nas linhas da tabela 8 são os valores utilizados nas tabelas de contexto, de modo a facilitar a apresentação dessas tabelas.

Tabela 8 – Variáveis de Contexto

Variável	**Estados Possíveis**
Condições climáticas	Normais (Bom), Desfavoráveis para VFR (Ruim VFR) ou Desfavoráveis para IFR (Ruim IFR).
Aeronave em Emergência	Sim ou Não
Trem de Pouso Abaixado	Sim ou Não
Tipo de Operação	IFR ou VFR
Utilização da Pista	Vazia ou Ocupada

Da lista de perigos percebeu-se alguns possíveis conflitos de procedimentos como por exemplo autorizar o pouso de uma aeronave em emergência com a pista ocupada é perigoso (P_1), mas não autorizar o pouso de uma aeronave em emergência também é

perigoso (P_4). Como Thomas (2013) cita, a melhor maneira de se prevenir esses conflitos seria criar saídas no projeto do sistema que os evitassem, mas caso não seja possível, uma das maneiras é ordenar os perigos em importância e escolher o perigo que causa o menor impacto possível.

De forma a resolver os possíveis conflitos, definiu-se uma prioridade para os perigos considerados, do mais importante para o menos, na ordem que foi apresentada anteriormente, ou seja:

- P_1: Aeronave inicia processo de aterrissagem/decolagem com a pista ainda ocupada.
- P_2: Aeronave opera abaixo dos mínimos estabelecidos para a sua operação.
- P_3: Aeronave em emergência não consegue pousar imediatamente para receber o socorro necessário.
- P_4: Aeronave entra em estado não-controlável.

Estabeleceu-se como perigo de maior prioridade o P_1, pouso em pista ocupada, uma vez que a velocidade que a aeronave em procedimento de aterrissagem está quando toca a pista é tão alta, que qualquer colisão na pista se torna desastrosa, principalmente se houver outra aeronave tripulada ocupando a pista por algum motivo.

Autorizar pouso de aeronaves operando fora dos limites climáticos e visuais estabelecidos para a sua operação (VFR ou IFR) foi considerada a segunda prioridade. Navegar em condições climáticas desfavoráveis às capacidades da aeronave dificulta qualquer tipo de manobra necessária já que não é possível obter nenhum tipo de confirmação visual, mesmo para voos IFR.

Em terceiro ficou P_3, pois aeronaves em emergência que não sejam prontamente atendidas podem acabar colocando as outras aeronaves próximas em estado de perigo e emergência também. Por último P_4 com a menor prioridade.

6.3.2 Identificando as Ações Inseguras de Controle

A tabela 9 mostra a tabela de contexto para a ação *Autorizar Pouso* e a tabela 10 a tabela de contexto para a *Ausência de Autorização de Pouso*. Em ambas as tabelas as colunas foram abreviadas para melhorar a apresentação das mesmas. As abreviações foram as seguintes:

- **Clima**: Condições climáticas.
- **Pista**: Utilização da pista.

- **Operação**: Tipo de operação da aeronave.
- **Emergência**: Aeronave em situação de emergência.
- **Trem**: Trem de Pouso abaixado.
- **ECP**: Execução Causa Perigo.
- **ETCP**: Execução Tardia Causa Perigo.
- **EACP**: Execução Adiantada Causa Perigo.
- **NECP**: Não Execução Causa Perigo.

Foi utilizada também a técnica de simplificação discutida no capítulo 5 para tornar as tabelas mais enxutas, sem perder informações necessárias. Nesta técnica, é utilizada a notação N/I, que significa que *não importa*, marcando que o valor do campo não é importante para o restante do contexto.

Tabela 9 – Ação: Autorizar Pouso

Clima	**Pista**	**Operação**	**Emergência**	**Trem**	**ECP**	**ETCP**	**EACP**
N/I	Ocupada	N/I	N/I	N/I	P1	P1	P1
Bom	Liberada	N/I	Não	Sim	Não	Não	Não
Bom	Liberada	N/I	Não	Não	P4	P4	P4
Bom	Liberada	N/I	Sim	N/I	Não	P3	Não
Ruim VFR	Liberada	VFR	N/I	N/I	P2	P2	P2
Ruim VFR	Liberada	IFR	Não	Sim	Não	Não	Não
Ruim VFR	Liberada	IFR	Não	Não	P4	P4	P4
Ruim VFR	Liberada	IFR	Sim	N/I	Não	P3	Não
Ruim IFR	Liberada	N/I	N/I	N/I	P2	P2	P2

Tabela 10 – Ausência de Ação: Autorizar Pouso

Clima	**Pista**	**Operação**	**Emergência**	**Trem**	**NECP**
N/I	Ocupada	N/I	N/I	N/I	Não
Bom	Liberada	N/I	Não	Sim	Não
Bom	Liberada	N/I	Não	Não	Não
Bom	Liberada	N/I	Sim	N/I	P3
Ruim VFR	Liberada	VFR	N/I	N/I	Não
Ruim VFR	Liberada	IFR	Não	Sim	Não
Ruim VFR	Liberada	IFR	Não	Não	Não
Ruim VFR	Liberada	IFR	Sim	N/I	P3
Ruim IFR	Liberada	N/I	N/I	N/I	Não

Com bases nas tabelas de contexto geradas, é possível levantar as Ação Insegura de Controle (AIC) da tarefa analisada e, por consequência, as Restrição de Segurança (RS)

do controle (tabela 11). Algumas simplificações nas AICs foram feitas, uma vez que essas AICs acabaram sendo equivalentes. São elas:

- Autorizar pouso de uma aeronave em VFR em condições desfavoráveis para VFR e autorizar pouso de uma aeronave em IFR em condições desfavoráveis para IFR ⇒ autorizar pouso de uma aeronave em condições climáticas desfavoráveis para o seu tipo de operação.

- Autorizar pouso de uma aeronave em condições climáticas boas, o trem de pouso não abaixado e sem emergência e autorizar pouso de uma aeronave IFR em condições climáticas desfavoráveis para VFR, com o trem de pouso não abaixado e sem emergência ⇒ autorizar pouso de uma aeronave com o trem de pouso não abaixado e sem emergência.

Um caso especial de simplificação foi para as AICs relacionadas ao pouso de aeronaves em emergência. Quando a pista está desocupada e as condições climáticas estão condizentes com o seu tipo de operação, os casos em que é possível levar a um perigo são se a autorização demorar para ser emitida ou se ela não é emitida. Em ambos estes casos a consequência (perigo) é o mesma: como a autorização de pouso não saiu, ou demorou muito, a aeronave dá mais uma volta no circuito de tráfego (ou arremete no caso de aeronaves em IFR) para esperar a autorização, com isso a emergência em que se encontra pode piorar, levando a perdas piores ainda. Por isso ambos os casos foram tratados da mesma forma.

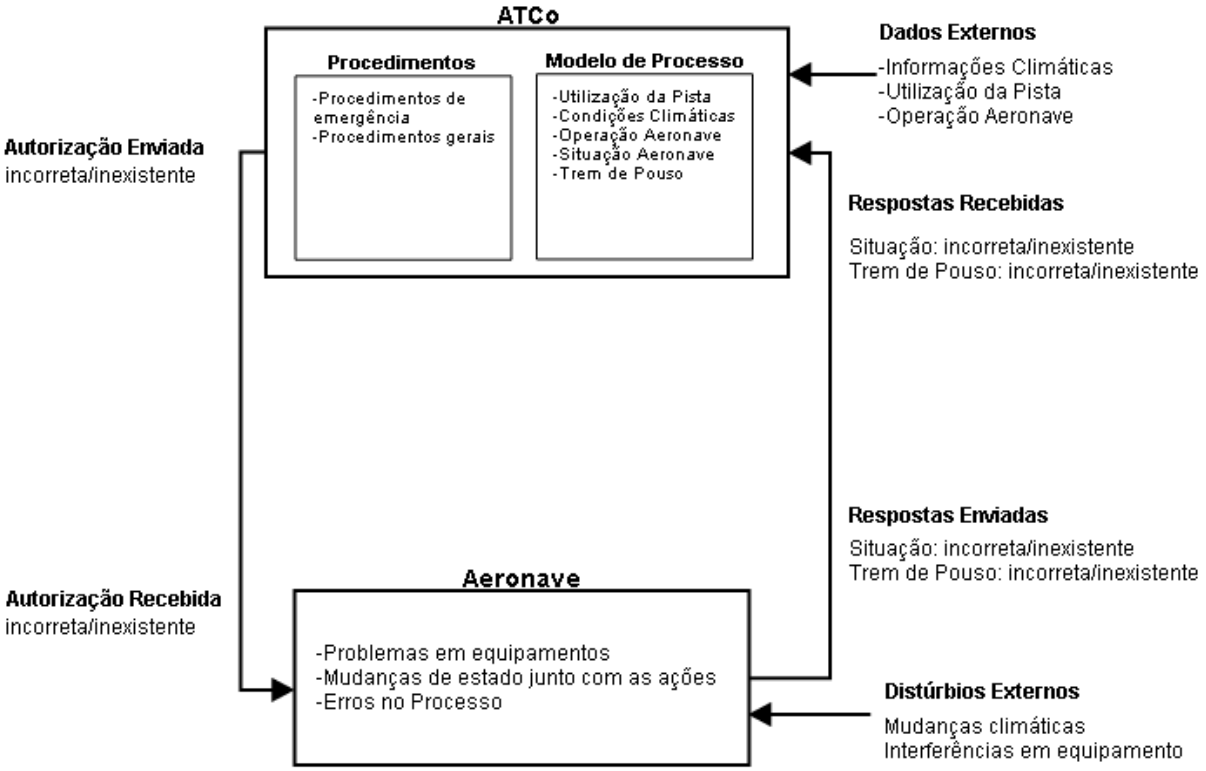
Tabela 11 – Restrições de Segurança para a Ação Autorizar Pouso

Ação Insegura de Controle (AIC)	**Restrição de Segurança (RS)**
AIC_1: Autorizar pouso de uma aeronave com a pista em uso ocupada por outra aeronave ou veículos/pessoal	RS_1: Não autorizar pouso de aeronaves enquanto a pista em uso estiver ocupada por outra aeronave ou veículos/pessoal
AIC_2: Autorizar pouso de uma aeronave sem emergência com o trem de pouso não abaixado	RS_2: Não autorizar pouso de uma aeronave sem emergência enquanto o trem de pouso da mesma não esteja abaixado.
AIC_3: Autorizar pouso de uma aeronave com condições climáticas desfavoráveis para voos do seu tipo	RS_3: Não autorizar pouso de uma aeronave quando as condições climáticas forem desfavoráveis para o seu tipo de voo
AIC_4: Autorizar tardiamente ou não autorizar o pouso de uma aeronave em emergência com condições climáticas condizentes com o seu tipo de operação	RS_4: Autorizar imediatamente o pouso de uma aeronave em emergência com condições climáticas condizentes com o seu tipo de operação

6.3.3 Identificando as Possíveis Causas

Como explicado no capítulo 5, esse passo se divide em duas partes: levantamento de causas para AIC e levantamento de causas para ações seguras não ocorrerem. Nesse momento, é necessário o detalhamento de como o controle opera, havendo agora a distinção de como é a operação do sistema. As figuras 25 e 26 mostram, respectivamente, as estruturas de fluxo de controle das operações manual e automatizada, juntamente com os possíveis fatores causais destes controles.

Figura 25 – Estrutura de Controle Manual e Possíveis Fatores Causais



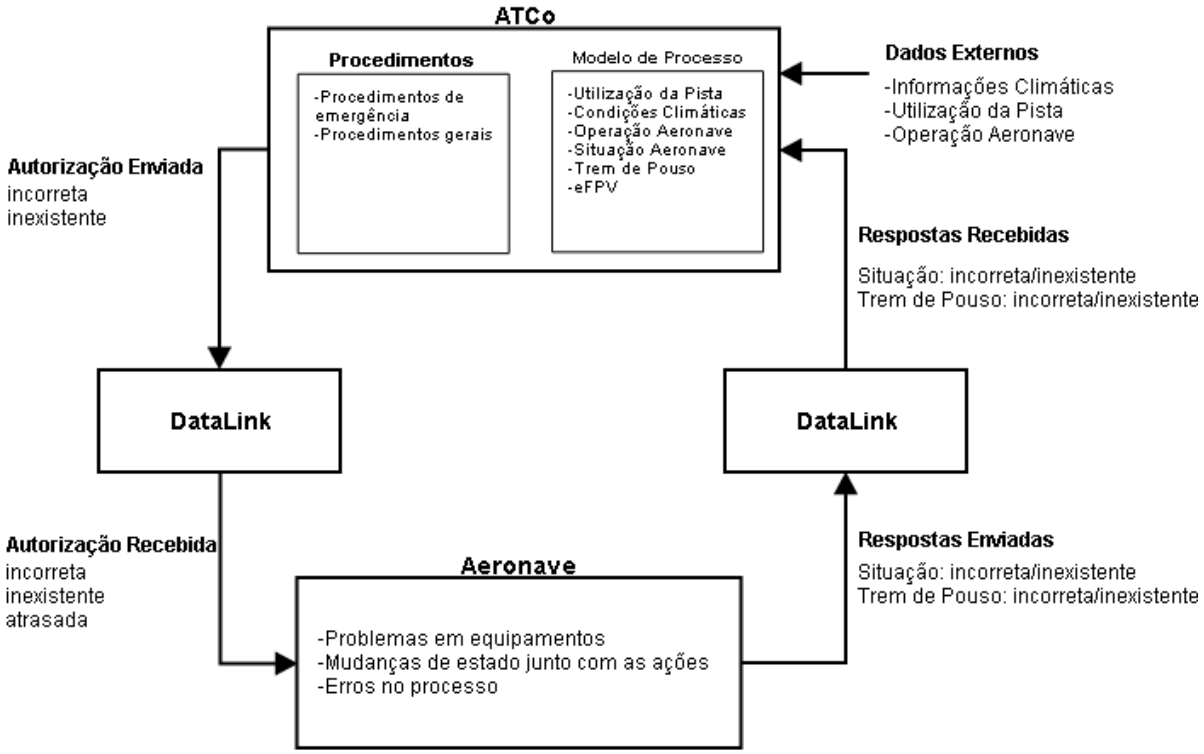
Todas as causas citadas podem ser localizadas nas figuras 25 e 26. Para cada causa listada, adicionou-se os marcadores **MANUAL** quando ela estiver associada ao cenário manual e **AUTO** para o cenário automático, podendo haver os dois marcadores em uma mesma causa.

6.3.3.1 Causas para Ações Seguras não Executadas

Analisando a região de controle das figuras 25 e 26, é possível notar os seguintes cenários que podem ocorrer:

- Autorização foi emitida para a aeronave, mas esta não a recebeu ou recebeu muito tarde.

Figura 26 – Estrutura de Controle Automatizado e Possíveis Fatores Causais



- Autorização não foi emitida para a aeronave, mas esta a recebeu.

Os fatores associados a cada um destes cenários são os seguintes:

Autorização foi emitida para a aeronave, mas esta não a recebeu ou recebeu muito tarde

1. Problemas na transmissão fazem com que a aeronave errada receba a mensagem de autorização (**MANUAL** e **AUTO**).
2. Problemas no Datalink fazem com que a mensagem demore muito tempo para ser recebida (**AUTO**).
3. Problemas no Datalink fazem com que a mensagem se perca e não seja recebida (**AUTO**).

Autorização não foi emitida para a aeronave, mas esta a recebeu

1. Problemas na transmissão fazem com que a aeronave errada receba a mensagem de autorização (**MANUAL** e **AUTO**).
2. Erro no Datalink interpreta outra mensagem como autorização de pouso (**AUTO**).

3. Problemas na transmissão de voz faz com que o piloto entenda uma outra mensagem como permissão de pouso (**MANUAL**).

6.3.3.2 Causas de Ações Inseguras de Controle

Para facilitar a apresentação dos fatores causais, estes foram divididos nos seguintes grupos em que estão associados:

- Controlador de Tráfego Aéreo (ATCo).
- Aeronave.
- Informações externas.
- Resposta.

Cada grupo será seguidos dos fatores encontrados que são associados com eles, ou por um *não se aplica* quando o grupo não estiver diretamente envolvido com as causas encontradas.

AIC_1 - Autorizar pouso de uma aeronave com a pista em uso ocupada por outra aeronave ou veículos/pessoal

- **ATCo**:
    1. ATCo acredita que a pista está vazia, quando não está (**MANUAL** e **AUTO**).
    2. Informações nas FPVs (ou e-FPV) erradas, inexistentes ou defasadas (**MANUAL** e **AUTO**).
    3. Informações nas FPVs (ou e-FPV) conflitantes com o que o ATCo lembra (**MANUAL** e **AUTO**).
    4. Pista está ocupada sem a permissão do ATCo (**MANUAL** e **AUTO**).
    5. ATCo confunde o procedimento a ser utilizado (**MANUAL** e **AUTO**).
    6. Falha em equipamentos causa defasagem de informações (ex: tela congelada)(**AUTO**).
- **Aeronave**: Não se aplica.
- **Informações externas**:
    1. Informação sobre ocupação da pista errada ou inexistente (**MANUAL** e **AUTO**).
- **Resposta**: Não se aplica.

AIC_2 - Autorizar pouso de uma aeronave sem emergência com o trem de pouso não abaixado

- **ATCo**:
  1. ATCo acredita que o trem de pouso está abaixado, quando não está (**MANUAL** e **AUTO**).
  2. ATCo confunde o procedimento a ser utilizado (**MANUAL** e **AUTO**).
  3. Falha em equipamentos causa defasagem de informações (ex: tela congelada) (**AUTO**).
- **Aeronave**:
  1. Erro de processo interno ou problemas em equipamento faz aeronave responder com situação errada de trem de pouso, ou não responder, ou demorar para responder (**MANUAL** e **AUTO**).
  2. Trem de pouso volta a subir após a aeronave responder com a situação abaixada (**MANUAL** e **AUTO**).
- **Informações externas**: Não se aplica
- **Resposta**:
  1. Situação do trem de pouso recebida/enviada incorreta por problemas na transmissão de rádio como interferência ou pronuncia (**MANUAL**).
  2. Situação do trem de pouso recebida/enviada incorreta por problemas na transmissão digital como interferência (**AUTO**).
  3. Situação do trem de pouso não enviada/recebida devido a problemas na transmissão como interferência (**MANUAL** e **AUTO**).
  4. Atraso no recebimento da situação do trem de pouso por problemas na transmissão (**AUTO**).

AIC_3 - Autorizar pouso de uma aeronave com condições climáticas desfavoráveis para voos do seu tipo

- **ATCo**:
  1. ATCo acredita que as condições climáticas estão favoráveis em relação ao tipo de operação da aeronave, quando não está (**MANUAL** e **AUTO**).
  2. ATCo acredita que o tipo de operação da aeronave está de acordo com as condições climáticas, quando não está (**MANUAL** e **AUTO**).

3. Informações nas FPVs (ou e-FPV) erradas, inexistentes ou defasadas (**MANUAL** e **AUTO**).
4. Informações nas FPVs (ou e-FPV) conflitantes com o que o ATCo lembra (**MANUAL** e **AUTO**).
5. ATCo confunde o procedimento a ser utilizado (**MANUAL** e **AUTO**).
6. Falha em equipamentos causa defasagem de informações (ex: tela congelada) (**AUTO**).

- **Aeronave**: Não se aplica.
- **Informações externas**:
  1. Informações sobre operação da aeronave incorretas ou inexistentes (**MANUAL** e **AUTO**).
  2. Informações meteorológicas incorretas ou inexistentes (**MANUAL** e **AUTO**).
- **Resposta**: Não se aplica.

AIC_4 - Autorizar tardiamente ou não autorizar o pouso de uma aeronave em emergência com condições climáticas condizentes com o seu tipo de operação

- **ATCo**:
  1. ATCo acredita que a aeronave não está em emergência, quando está (**MANUAL** e **AUTO**).
  2. ATCo confunde o procedimento a ser utilizado (**MANUAL** e **AUTO**).
  3. Falha em equipamentos causa defasagem de informações (ex: tela congelada) (**AUTO**).
- **Aeronave**:
  1. Erro de processo interno ou problemas em equipamento faz aeronave responder com situação de emergência incorreta, ou não responder, ou demorar para responder (**MANUAL** e **AUTO**).
  2. A emergência acontece após envio de resposta ao ATCo (**MANUAL** e **AUTO**).
- **Informações externas**: Não se aplica.
- **Resposta**:
  1. Sinal de emergência recebido/enviado incorreto por problemas na transmissão de rádio, como interferência ou pronuncia errada (**MANUAL**).

2. Sinal de emergência recebido/enviado incorreto por problemas na transmissão digital, como interferência (**AUTO**).
3. Sinal de emergência não enviado/recebido devido a problemas na transmissão, como interferência (**MANUAL** e **AUTO**).
4. Atraso no recebimento do sinal de emergência por problemas na transmissão (**AUTO**).

6.4 ANÁLISE DE IMPACTO EM REQUISITOS DE SEGURANÇA

Com base nos fatores causais levantados é possível fazer uma análise do impacto da automação proposta (Datalink) na segurança do sistema. Com base na notação definida no capítulo 5, defini-se os conjuntos de fatores causais. A tabela 12 mostra os tamanhos de cada conjunto básico.

Tabela 12 – Quantidades de Fatores Levantados por Cenário

Conjunto	**Quantidade**
M	23
A	28
I	20
TOTAL	31

Embora os números mostrem que existem mais fatores associados ao cenário automático, essa informação ainda não é suficiente para uma avaliação precisa do impacto. Nota-se pela tabela 12 que apenas três fatores de M ficaram de fora de I. Voltando no levantamento vemos que os fatores foram os seguintes:

- Problemas na transmissão de voz faz com que o piloto entenda uma outra mensagem como permissão de pouso.
- Situação do trem de pouso recebida/enviada incorreta por problemas na transmissão de rádio como interferência ou pronuncia errada.
- Sinal de emergência recebido/enviado incorreto por problemas na transmissão de rádio, como interferência ou pronuncia errada.

Destes fatores pode-se ver que eles estão relacionados ao equipamento utilizado (rádio transmissão) e todos tem em comum o problema que a pronuncia pode causar na transmissão das mensagens, algo que o Datalink não teria problemas uma vez que ele utiliza mensagens de texto pré-formatadas. Os três fatores são acompanhados por um par equivalente no conjunto A, portanto fazem parte do conjunto E:

- Erro no Datalink interpreta outra mensagem como autorização de pouso.
- Situação do trem de pouso recebida/enviada incorreta por problemas na transmissão digital, como interferência.
- Sinal de emergência recebido/enviado incorreto por problemas na transmissão digital, como interferência.

Aqui nota-se que o problema de interferência aparece em ambos os cenários e afetam da mesma maneira os controles envolvido. O conjunto A possui 8 fatores levantados a mais do que aparecem em I, mas desses, três possuem equivalência em M. Os cinco restantes são os seguintes:

- Problemas no Datalink fazem com que a mensagem demore muito tempo para ser recebida.
- Problemas no Datalink fazem com que a mensagem se perca e não seja recebida.
- Falha em equipamentos causa defasagem de informações (ex: congelamento de tela).
- Atraso no recebimento da situação do trem de pouso por problemas na transmissão.
- Atraso no recebimento do sinal de emergência por problemas na transmissão.

O que todos esses fatores tem em comum é estarem associados a falhas do equipamento envolvido na nova automação. Pode-se resumir o impacto analisado em dois importantes pontos:

1. A introdução de novos equipamentos também introduz uma maior quantidade de fatores causais relacionados às falhas de seus componentes, aumentando por consequência o número de restrições de segurança do sistema.
2. Nenhum dos possíveis fatores causais do cenário manual foi resolvido pela automação diretamente, ou permaneceram os mesmos ou foram modificados para algo equivalente.
3. Importante salientar que mesmo que exista uma maior quantidade de fatores causais no cenário automático, é esperado que eles tenham uma probabilidade menor de acontecer, então ainda não é possível afirmar que é mais ou menos seguro a automação da tarefa.

7 CONSIDERAÇÕES FINAIS

7.1 CONCLUSÕES

Este trabalho de pesquisa científica propôs uma metodologia para analisar o impacto da automação das tarefas do Controlador de Tráfego Aéreo (ATCo) de uma Torre de controle de aeródromo (TWR), utilizando o modelo sistêmico do STAMP. A metodologia proposta utiliza a aplicação do STPA em dois cenários: antes da automação e depois da automação. Dessa forma foi possível avaliar os fatores causais de ambos os cenários e, com base nas diferenças encontradas, determinar como a automação impacta sobre os requisitos de segurança.

O exemplo utilizado mostrou que a metodologia proposta permite analisar com uma boa riqueza de detalhes como os fatores causais são modificados com a inclusão de uma determinada ferramenta automatizada, inclusive conseguindo mostrar aquilo que permaneceu mesmo com a automação da tarefa. A metodologia proposta se mostra muito eficaz para uma Análise Preliminar de Perigos (PHA).

Notou-se que grande parte dos fatores se manteve e, aqueles que modificaram de alguma forma, ainda possuem alguma equivalência no cenário manual, fortalecendo a afirmação de que a tecnologia não cria problemas novos, apenas muda a maneira em que os problemas acontecem (LEVESON, 2012).

Percebeu-se que os fatores do cenário automático que não possuíam equivalência no conjunto de fatores manuais eram de origem basicamente tecnológicas, como problemas em transmissão ou robustez de execução, mostrando a importância de se produzir tecnologias com boa confiabilidade.

Em específico para o sistema Controle de tráfego aéreo (ATC), o operador humano ainda tem uma participação fundamental na segurança da operação. Os fatores causais com relação às decisões do ATCo e dos pilotos foram tratadas de maneira muito simples, para apenas validar a metodologia proposta, mas o melhor caso seria se eles pudessem ser analisados do ponto de vista de cognição humana, buscando os reais motivos do fator ter acontecido. Thornberry (2014) estendeu o STPA para incluir essa proposta.

Thomas (2013) cita que dependendo do nível de detalhe desejado na análise do STPA, as tabelas de contexto podem ficar enormes e o levantamento de fatores causais pode levantar uma quantidade muito grande de fatores. Um possível foco de estudo seria em ferramentas automatizadas na análise de grande tabelas de contexto e de levantamento de fatores causais.

Em termos gerais, o objetivo geral da pesquisa em propor uma metodologia que seja capaz de analisar o impacto em segurança da automação de tarefas de operadores humanos, nesse caso os ATCos, foi alcançada. Mesmo que faltando o formalismo em sua validação, foi possível ver que ela consegue levantar diferenças significativas dos dois cenários.

7.2 TRABALHOS FUTUROS

O cenário exemplo utilizado apenas exemplifica a metodologia proposta, seria necessário uma validação matemática para formalizar a metodologia, além de uma análise junto com especialistas do Instituto de Controle do Espaço Aéreos (ICEA).

Como dito anteriormente, o ATCo tem um papel fundamental na operação do sistema, então é necessário uma análise mais profunda na parte cognitiva do controlador.

O desenvolvimento de ferramentas automáticas que auxiliem na criação das tabelas de contexto e no levantamento inicial de fatores causais ajudaria na análise detalhada de uma ação de controle, onde haverá muitas variáveis de contexto envolvidas no controle, que é o caso da maioria dos sistemas atuais.

A introdução de cálculo de probabilidades de fatores causais permitiria uma avaliação precisa do impacto em segurança da implantação da automação, a partir dos fatores causais levantados durante a análise.

REFERÊNCIAS

ALVARENGA, M. A. B.; MELO, P. F. Frutuoso e; FONSECA, R. A. A critical review of methods and models for evaluating organizational factors in Human Reliability Analysis. *Progress in Nuclear Energy*, v. 75, p. 25–41, ago. 2014.

BAUM, D. *Apostila do Espaço Aéreo*. [S.l.]: Associação Brasileira de Parapente, 2007.

BBC. Man v machine at 30,000ft. *BBC*, fev. 2013.

BENNETT, S. *A History of Control Engineering, 1930-1955*. [S.l.]: IET, 1993.

BROOKER, P. SESAR and NextGen: Investing in new paradigms. *The Journal of Navigation*, v. 61, n. 02, p. 195–208, 2008.

CAMP, G. et al. Dynamic problem selection in air traffic control training: a comparison between performance, mental effort and mental efficiency. *Computers in Human Behavior*, v. 17, n. 5–6, p. 575–595, 2001. ISSN 0747-5632. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0747563201000280>.

COOK, R. I. Verite, abstraction, and ordinateur systems in the evolution of complex process control. In: *Third Annual Symposium on Human Interaction with Complex Systems, 1996. HICS '96. Proceedings*. [S.l.: s.n.], 1996. p. 38–42.

CORVER, S. C.; ANEZIRIS, O. N. The impact of controller support tools in enroute air traffic control on cognitive error modes: A comparative analysis in two operational environments. *Safety Science*, 2014.

DE CARVALHO, P. V. R. The use of Functional Resonance Analysis Method (FRAM) in a mid-air collision to understand some characteristics of the air traffic management system resilience. *Reliability Engineering & System Safety*, v. 96, n. 11, p. 1482–1498, nov. 2011.

DECEA. *DCA 351-2 Concepção Operacional ATM Nacional*. [S.l.], 2011.

DECEA. *Anuário Estatístico de Tráfego Aéreo*. [S.l.], 2012.

DECEA. *ICA 100-12 Regras do Ar*. [S.l.], 2013.

DECEA. *ICA 100-31 Requisitos dos Serviços de Tráfego Aéreo*. [S.l.], 2013.

DECEA. *ICA 100-37 Serviços de Tráfego Aéreo*. [S.l.], 2013.

DEKKER, S. *The Field Guide to Understanding Human Error*. 1 edition. ed. Aldershot, England ; Burlington, VT: Ashgate Publishing Company, 2006.

DIRICKSON, Y.; VISMARI, L.; CAMARGO, J. Elicitation of Operational Requirements in ATC Activities Automation Process: The TWR Case. In: *2013 III Brazilian Symposium on Computing Systems Engineering (SBESC)*. [S.l.: s.n.], 2013. p. 149–154.

EUROCONTROL. *European ATM Master Plan*. [S.l.], 2012. Disponível em: <https://www.atmmasterplan.eu/download/25>.

FAA. *Instrument Flying Handbook*. [S.l.], 2012.

FAA. *NextGen Implementation Plan*. [S.l.], 2012. Disponível em: <http://www.faa.gov/nextgen/implementation/media/NextGen_Implementation_Plan_2012.pdf>.

FAA. *Glossary of Terms*. 2014. Disponível em: <http://www.fly.faa.gov/Products/Glossary_of_Terms/glossary_of_terms.html>.

FLEMING, C. H. et al. Safety assurance in NextGen and complex transportation systems. *Safety Science*, v. 55, p. 173–187, jun. 2013.

FLEMMING, C. H. *Safety-driven Early Concept Analysis and Development*. Tese (Doutorado) — Massachusetts Institute of Technology, EUA, 2004.

GIL, G.-H. et al. Effects of modes of cockpit automation on pilot performance and workload in a next generation flight concept of operation. *Human Factors and Ergonomics in Manufacturing & Service Industries*, v. 22, n. 5, p. 395—406, 2012.

HEINRICH, H. W. *Industrial Accident Prevention: A Scientific Approach*. [S.l.]: McGraw-Hill book Company, Incorporated, 1931.

HOLLNAGEL, E. *Barriers and Accident Prevention*. [S.l.]: Ashgate, 2004.

HOLLNAGEL, E. Flight decks and free flight: Where are the system boundaries? *Applied Ergonomics*, v. 38, n. 4, p. 409–416, jul. 2007. ISSN 0003-6870.

HOLLNAGEL, E. *FRAM: the functional resonance analysis method : modelling complex socio-technical systems*. Surrey: Ashgate, 2012.

HOLLNAGEL, E.; WOODS, D. D. *Joint Cognitive Systems: Foundations of Cognitive Systems Engineering*. [S.l.]: CRC Press, 2005.

ICAO. *Air Traffic Services Planning Manual*. [S.l.], 1998.

ICAO. *Global Air Traffic Management Operational Concept*. [S.l.], 2005.

ICAO. *Outlook for Air Transport to the Year 2025*. [S.l.], 2007.

ICAO. *2013-2028 Global Air Navigation Plan*. [S.l.], 2013.

ICAO. *Global Operational Data Link Document (GOLD)*. [S.l.], 2013.

LANGAN-FOX, J.; CANTY, J. M.; SANKEY, M. J. Human–automation teams and adaptable control for future air traffic management. *International Journal of Industrial Ergonomics*, v. 39, n. 5, p. 894–903, set. 2009.

LANGAN-FOX, J.; SANKEY, M. J.; CANTY, J. M. Human Factors Measurement for Future Air Traffic Control Systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, v. 51, n. 5, p. 595–637, jan. 2009.

LETCHWORTH, G.; SCHLIERF, R. NASA planning for Orion Multi-Purpose Crew Vehicle ground operations. In: *2012 IEEE Aerospace Conference*. [S.l.: s.n.], 2012. p. 1–11.

LEVESON, N. A new accident model for engineering safer systems. *Safety Science*, v. 42, n. 4, p. 237–270, abr. 2004. ISSN 0925-7535.

LEVESON, N. G. *Engineering a Safer World: Systems Thinking Applied to Safety*. Cambridge, Mass.: The MIT Press, 2012.

LEVESON, N. G.; STEPHANOPOULOS, G. A system-theoretic, control-inspired view and approach to process safety. *AIChE Journal*, v. 60, n. 1, p. 2–14, jan. 2014.

LEVESON, N. G.; THOMAS, J. *STPA Primer*. USA, 2013.

MALAKIS, S.; KONTOGIANNIS, T. A sensemaking perspective on framing the mental picture of air traffic controllers. *Applied Ergonomics*, v. 44, n. 2, p. 327–339, mar. 2013.

METZGER, U.; PARASURAMAN, R. The Role of the Air Traffic Controller in Future Air Traffic Management: An Empirical Study of Active Control versus Passive Monitoring. *The Journal of the Human Factors and Ergonomics Society*, v. 43, n. 4, p. 519–528, jan. 2001.

METZGER, U.; PARASURAMAN, R. Automation in Future Air Traffic Management: Effects of Decision Aid Reliability on Controller Performance and Mental Workload. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, v. 47, n. 1, p. 35–49, jan. 2005.

NEISSER, U. *Cognition and Reality: Principles and Implications of Cognitive Psychology*. San Francisco: W. H. Freeman and Company, 1976.

NETJASOV, F.; JANIC, M. A review of research on risk and safety modelling in civil aviation. *Journal of Air Transport Management*, v. 14, n. 4, p. 213–220, jul. 2008.

PARASURAMAN, R.; SHERIDAN, T.; WICKENS, C. D. A model for types and levels of human interaction with automation. *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, v. 30, n. 3, p. 286–297, maio 2000.

PLANECRASHINFO.COM. *Accidents Statistics*. 2015. Disponível em: <http://planecrashinfo.com/cause.htm>.

PREVOT, T. et al. Toward automated air traffic control—investigating a fundamental paradigm shift in human/systems interaction. *International Journal of Human-Computer Interaction*, v. 28, n. 2, p. 77–98, 2012.

RASMUSSEN, J. Risk management in a dynamic society: a modelling problem. *Safety Science*, v. 27, n. 2–3, p. 183–213, nov. 1997.

REASON, J. *Human Error*. [S.l.]: Cambridge University Press, 1990. ISBN 978-0-521-31419-0.

ROVIRA, E.; PARASURAMAN, R. Transitioning to future air traffic management: Effects of imperfect automation on controller attention and performance. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, v. 52, n. 3, p. 411–425, jun. 2010.

SAP. *FAA/EUROCONTROL ATM Safety Techniques and Toolbox*. 2007.

SEIDNER, C.; ROUX, O. Formal Methods for Systems Engineering Behavior Models. *IEEE Transactions on Industrial Informatics*, v. 4, n. 4, p. 280–291, 2008.

SILVA, S. da. *Global ATM Operational Concept*. Nairobi: [s.n.], 2010.

STROEVE, S. H.; BLOM, H. A.; BAKKER, G. Systemic accident risk assessment in air traffic by Monte Carlo simulation. *Safety Science*, v. 47, n. 2, p. 238–249, fev. 2009.

THOMAS, J. *Extending and Automating a System-Theoretic Hazard Analysis for Requirements Generation and Analysis*. Tese (Doutorado) — Massachusetts Institute of Technology, EUA, jun. 2013.

Thornberry, C. L. *Extending the Human-Controller Methodology in Systems- Theoretic Process Analysis (STPA)*. Dissertação (Dissertação de Mestrado) — MIT, EUA, jun. 2014.

UNDERWOOD, P.; WATERSON, P. Systems thinking, the Swiss Cheese Model and accident analysis: A comparative systemic analysis of the Grayrigg train derailment using the ATSB, AcciMap and STAMP models. *Accident Analysis & Prevention*, v. 68, p. 75–94, jul. 2014.

UNDERWOOD, P.; WATERSON, P.; BRAITHWAITE, G. 'Accident investigation in the wild' – A small-scale, field-based evaluation of the STAMP method for accident analysis. *Safety Science*, v. 82, p. 129–143, fev. 2016.

VU, K.-P. L. et al. How does reliance on automated tools during learning influence students air traffic management skills when the tools fail? In: *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*. Boston, Massachusets USA: [s.n.], 2012. v. 56, p. 16–20.

WEICK, K. E. *Sensemaking in Organizations*. Thousand Oaks: SAGE Publications, Inc, 1995.

YOON, J. H. et al. An Integrated Process Model for the Systems Development Requiring Simultaneous Consideration of the SE Process and Safety Requirements. In: *2008 2nd Annual IEEE Systems Conference*. [S.l.: s.n.], 2008. p. 1–8.