Abordagem STAMP aplicada à Análise de Acidentes na Operação Civil de Aeronaves no Brasil

Idoaldo José de Lima [1], Marcelo Santiago de Sousa [2], Ariosto Bretanha Jorge [2], Rogerio Frauendorf de Faria Coimbra [2], Carlos Henrique Netto Lahoz[3]

1 Instituto Tecnológico de Aeronáutica - ITA
2 Universidade Federal de Itajubá – UNIFEI
3 Instituto de Aeronáutica e Espaço - IAE

RESUMO: A metodologia tradicional promovida atualmente pela OACI é baseada no modelo de Reason, que considera o acidente como um resultado do encadeamento de eventos falhos, responsável pela perda do sistema. Uma nova metodologia, *Systems Theoretic Accident Model and Process* (STAMP), foi proposta pela Profª Nancy Leveson (MIT) e refuta as suposições utilizadas na aplicação do modelo de Reason. Baseado na teoria de engenharia de sistemas, esse novo modelo trata o acidente como o resultado de interações entre os componentes do sistema que violam as restrições do próprio sistema, e não mais o simples encadeamento de falhas nos componentes. Estudos publicados pela comunidade internacional avaliaram a abordagem STAMP como alternativa complementar à análise de ocorrências na aviação. Esse trabalho propõe uma aplicação direta da abordagem STAMP na análise de acidentes aéreos na operação civil brasileira de aeronaves. Aplicado à realidade nacional, esse estudo busca contribuir com a validação desse modelo no suporte à análise de acidentes aeronáuticos no Brasil. Para tanto, é utilizado como exemplo um acidente aéreo, cujas recomendações ocasionaram impacto no sistema de operação de aeronaves no país. As recomendações da análise produzida apontam resultados semelhantes aos do modelo tradicional, mas também resultados complementares diferenciados e mais abrangentes, diretivos de implementação para o aumento da segurança no sistema. Nesse contexto, o método constitui uma ferramenta eficaz na análise de falhas e na compreensão dos problemas nos diversos níveis do sistema em questão.

Palavras chave: Análise de Acidentes Aéreos; Engenharia de Sistemas; *Safety;* STAMP.

The STAMP Approach applied to the Analysis of Accidents in the Operation of Civil Aircraft in Brazil

ABSTRACT: The traditional methodology currently promoted by ICAO is based on the Reason model, which considers the accident as a result of the chaining of flawed events, responsible for the loss of the system. A new methodology (Systems Theoretic Accident Model and Process - STAMP) proposed by Prof. Nancy Leveson (MIT) refutes the assumptions utilized in the application of the Reason model. Based on the system engineering theory, this new model considers the accident as the result of interactions between system components that violate the constraints of the very system, and not the simple chaining of flaws in the components. Studies published by the international community have evaluated the STAMP approach as a complementary alternative to the analysis of aviation occurrences. This article proposes a direct application of the STAMP approach to the analysis of aircraft accidents in the operation of Brazilian civil aircraft. Applied to the national reality, this study seeks to contribute, with the validation of this model, to the support of the analysis of aeronautical accidents in Brazil. For this purpose, an aircraft accident is used as an example, the recommendations of which impacted the system of aircraft operation in the country. The recommendations derived from the analysis show results similar to those obtained by the traditional model, but they also present complementary, differentiated, and more comprehensive results, with directives of implementation aimed at increasing system safety. In this context, the method is an effective tool for the analysis of failures and the understanding of problems at the various levels of the system in question.

Key words: Analysis of Aircraft Accidents. System Engineering. Safety. STAMP.

Citação: Idoaldo, JL, Marcelo, SS, Ariosto, BJ, Rogerio, FFC, Carlos, HNL. (2016) Abordagem STAMP aplicada à Análise de Acidentes na Operação Civil de Aeronaves no Brasil. *Revista Conexão Sipaer*, Vol. 7, No. 1, pp. 127-142.

1 BIOGRAFIA

Idoaldo José de Lima

Engenheiro mecânico-aeronáutico formado pela Universidade Federal de Itajubá (UNIFEI- 2016). Atualmente é mestrando em transporte aéreo e aeroportos pelo Instituto Tecnológico de Aeronáutica (ITA). Tem experiência nas áreas de aeronaves não tripuladas, engenharia de sistemas, segurança operacional, instrumentação de voo e ensino de engenharia.

Marcelo Santiago de Sousa

Engenheiro aeronáutico formado pelo ITA (2001). Possui mestrado em mecatrônica e sistemas aeroespaciais pelo ITA (2005) e doutorado em mecânica e controle de voo pelo ITA (2013). Trabalhou como engenheiro de sistemas no grupo de mecânica de voo da Embraer e, desde 2011, tem atuado no

ensino e pesquisa de dinâmica de voo e sistemas aeronáuticos na UNIFEI.

Ariosto Bretanha Jorge

Engenheiro mecânico-aeronáutico formado pelo ITA (1987). Possui mestrado em tecnologias de helicópteros pela ENSICA (França-1992), doutorado em mecânica aplicada pelo *Vanderbilt University* (EUA-2002) e pós-doutorado em mecânica aplicada pelo *Vanderbilt University* (EUA-2010). Trabalhou como oficial-engenheiro da Marinha do Brasil e, desde 1995, tem atuado no ensino e pesquisa de detecção de danos em estruturas aeronáuticas e confiabilidade na Universidade Federal de Itajubá.

Rogerio Frauendorf de Faria Coimbra

Engenheiro mecânico formado pela Escola de Engenharia de Mauá (1992). Possui especialização em engenharia de ensaios em voo pela EPNER (França-2003), mestrado em aerodinâmica aplicada pela Universidade de São Paulo (USP-1997) e doutorado em aerodinâmica aplicada pela USP (2002). Trabalhou como engenheiro de ensaios em voo na Embraer, no CTA e na ANAC e, desde 2011, tem atuado no ensino e pesquisa de aerodinâmica aplicada e projeto de aeronaves na Universidade Federal de Itajubá.

Carlos Henrique Netto Lahoz

Tecnólogo em processamento de dados, formado pela Universidade de Taubaté (1983). Possui mestrado em computação aplicada pelo Instituto Nacional de Pesquisas Espaciais (INPE-2004), doutorado engenharia elétrica pela USP (2009) e é pós-doutorando em engenharia de sistemas pelo MIT (EUA). Trabalha atualmente como tecnologista sênior do Instituto de Aeronáutica e Espaço (IAE) e professor titular da Universidade Paulista.

2 INTRODUÇÃO

Abordagens de segurança baseadas na teoria dos sistemas consideram que acidentes são decorrentes das interações entre os componentes do sistema e geralmente não especificam fatores únicos de causa. Essa perspectiva trata a segurança como uma propriedade emergente que surge quando os componentes do sistema interagem dentro de um ambiente. A segurança, portanto, é controlada ou executada por um conjunto de restrições (leis de controle) relacionadas com o comportamento dos componentes do sistema. Acidentes resultam das interações entre componentes que violam essas restrições - em outras palavras, de restrições inadequadas sobre as interações. (LEVESON, 2011)

Segurança, então, pode ser vista como um problema de controle. Os acidentes ocorrem quando falhas nos componentes, perturbações externas, ou interações disfuncionais entre o sistema e os componentes não estão adequadamente controladas. Os eventos falhos refletem os efeitos de interações disfuncionais e aplicações inadequadas de restrições de segurança. A própria estrutura de controle deve ser examinada para determinar por que era inadequada para manter as restrições sobre comportamento seguro e por que os eventos ocorreram. A partir daí diversas perguntas precisam ser respondidas para entender por que o acidente ocorreu e obter as informações necessárias para prevenir acidentes futuros. (LEVESON, 2011)

Conforme Arnold (2009), o primeiro modelo de acidente aéreo promovido pela Organização Internacional de Aviação Civil (ICAO) foi o modelo de acidentes organizacionais de Reason, modelo baseado no encadeamento de falhas ordenadas no sistema de segurança, com todas as características descritas anteriormente. Em 2005, o Systemic Occurence Analysis Methodology (SOAM) passou a ser o novo modelo padrão utilizado pela comunidade internacional, para a investigação de acidentes aéreos. Esse novo modelo é uma adaptação baseada no mesmo modelo de Reason, apenas reduzindo a implicação de culpa por indivíduos ou organizações.

Com o advento dos fatores humanos e das novas tecnologias, pela virada do século, diversos pesquisadores começaram a desenvolver novos modelos que explicavam de maneira mais confiável e precisa os acidentes em sistemas cada vez mais complexos. Um desses modelos foi proposto pela Prof.ª Nancy Leveson (2004), o System Theoretic Accident Model and Processes (STAMP). Baseado em teoria de sistemas é inspirado nos conceitos de engenharia, matemática, psicologia cognitiva e social, política organizacional e ciências políticas e econômicas.

Nessa teoria, a ideia de acidentes como resultado de um evento causador inicial (raiz) em uma série de eventos que levam à perda do sistema, é contrariada. Acidentes passam a ser analisados como resultando de interações entre os componentes do sistema que levaram a uma violação das restrições do sistema (ARNOLD, 2009). Essa nova visão inclui todo o sistema técnico-social (e não apenas o lado técnico), as interações entre os componentes no acidente, além dos erros humanos e de desenvolvimento do próprio sistema.

A ferramenta específica de análise de acidentes da abordagem STAMP é chamada Casual Analysis using Systems Theory (CAST) e busca principalmente determinar porque os componentes se comportaram da maneira que se comportaram e quais foram as interações da estrutura de controle de segurança que permitiram que o acidente viesse a ocorrer.

Essa é a abordagem proposta por esse trabalho, cujos resultados da análise de um acidente aéreo (estudo de caso) que aconteceu no país foram obtidos para a verificação da aplicabilidade dessa abordagem. Dessa forma, o objetivo geral do presente estudo é utilizar a abordagem STAMP para a análise de um acidente que aconteceu no Brasil.

3 ABORDAGEM STAMP

Nessa seção é apresentada a metodologia de análise de ocorrências baseada na teoria de sistemas (STAMP), bem como os procedimentos e resultados, que representam esse estudo de caso. Todas as informações apresentadas nesse capítulo são referências do livro da Profa. Nancy Leveson (2011), Engineering a Safer World: System Thinking Applied to Safety.

3.1 System-Theoretic Accident Model and Processes (STAMP)

A segurança, reformulada como um problema de controle, deixa de ser um problema de confiabilidade. Essa mudança leva a formas mais eficazes de projetar sistemas mais seguros, incluindo sistemas técnico-sociais complexos.

Generalizando a definição, um acidente é um evento não planejado e que ocasiona uma perda indesejada. Essa perda pode envolver não só a morte humana ou o prejuízo, mas também outras grandes perdas, que incluem a missão em si, o equipamento, o financiamento, e as perdas de informação. As perdas resultam de falhas de componentes, perturbações externas ao sistema, interações entre componentes do sistema, e o comportamento individual dos componentes do sistema que levam a estados de perigo do sistema.

Da teoria de sistemas, propriedades emergentes, tais como a segurança, surgem das interações entre os componentes do sistema. As propriedades emergentes são controladas impondo restrições sobre o comportamento e sobre as interações entre os componentes. Acidentes resultam, portanto, de um controle inadequado ou da violação de restrições de segurança sobre o desenvolvimento, projeto e operação do sistema.

Neste contexto, a prevenção de futuros acidentes requer a mudança de um foco na prevenção de falhas para um objetivo mais amplo de concepção e implementação de controles que impõem as restrições necessárias. A abordagem STAMP para a modelagem de acidentes é baseada nesses princípios e apresenta três bases: restrições de segurança, estruturas hierárquicas de controle de segurança e modelos de processos.

O conceito básico no modelo STAMP não é um evento, mas uma restrição. Eventos relacionados à perda ocorrem somente porque as restrições de segurança não foram aplicadas com êxito.

Na teoria de sistemas, os sistemas são vistos como estruturas hierárquicas, onde cada nível impõe restrições sobre a atividade do nível abaixo dela. Processos de controle operam entre os níveis para controlar os processos em níveis mais baixos na hierarquia. Esses processos de controle tem a função de impor as restrições de segurança para que o processo de controle seja seguro.

O terceiro conceito utilizado na abordagem STAMP, juntamente com as restrições de segurança e a estrutura hierárquica de controle de segurança, são os modelos de processos. Acidentes ocorrem quando as restrições de controle impostas nesses processos são inadequadas e então violadas no comportamento das componentes de nível inferior.

No modelo STAMP, o projeto do sistema, não só deve impor restrições adequadas sobre comportamento para garantir uma operação segura, mas o sistema deve continuar a aplicar as restrições de segurança conforme as alterações e adaptações ao projeto do sistema ocorrem ao longo do tempo.

A grande diferença de outros modelos de causalidade é que a abordagem STAMP vai além de simplesmente culpar o componente falho ao exigir que os motivos dos controles instituídos para prevenir essas falhas ou para minimizar o seu impacto sobre a segurança foram inadequados. Essa ideia geral do modelo STAMP é ilustrada na Figura 1.

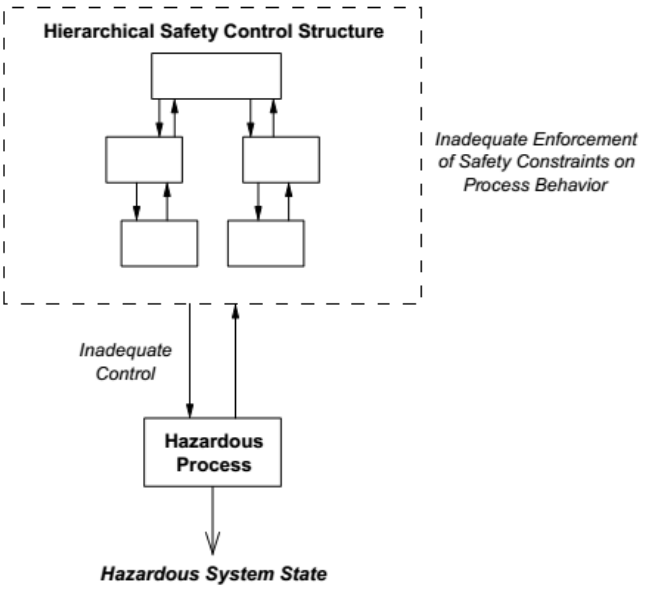

Figura 1 - Acidentes segundo a abordagem STAMP (LEVESON, 2011)

Os fatores de causa em acidentes podem ser divididos em três categorias gerais: a operação do controlador; o comportamento dos atuadores e processos controlados; e comunicação e coordenação entre controladores e tomadores de decisão. Além disso, quando humanos estão envolvidos na estrutura de controle de segurança, mecanismos de contexto e comportamento de conformação também desempenham um papel importante nos fatores de causa.

Vale ressaltar que o uso da modelagem STAMP contribui não só para identificar os fatores, mas também para compreender as relações entre eles. Esse modelo representa uma ferramenta muito útil na compreensão de acidentes, examinando cada parte do sistema para determinar sua contribuição para a perda, e possibilitando o desenvolvimento de sistemas mais seguros incluindo os aspectos técnicos, sociais, gerenciais, organizacionais e de regulação.

3.2 Causal Analysis using Systems Theory (CAST)

O modelo de análise de causalidade usado no acidente ou incidente determina o que deve ser procurado, como deve ser procurado, e o que é relevante para a compreensão do incidente. A maioria dos relatórios de acidentes são escritos a

partir da perspectiva de um modelo baseado em eventos encadeados. Eles costumam descrever claramente os acontecimentos e, geralmente, um ou vários destes eventos são escolhidos como causa-raiz. Em alguns casos, são identificadas causas contributivas, mas a análise do porquê esses eventos ocorreram geralmente é incompleta e a oportunidade de aprender mais profundamente com o acidente é perdida.

Uma técnica de análise de acidentes deve proporcionar um enquadramento ou processo para ajudar na compreensão de todo o processo acidente e identificar os mais importantes fatores de causa sistêmicos envolvidos. Esta subseção descreve a abordagem STAMP para análise de acidentes, intitulada CAST (Causal Analysis using Systems Theory). Essa análise pode ser utilizada para identificar as questões que precisam ser respondidas para compreender por que razão o acidente ocorreu.

O uso da análise CAST não leva à identificação de fatores de causa individuais ou variáveis. Em vez disso, ele fornece a capacidade de examinar o projeto do sistema técnico-social completo para identificar os pontos fracos existentes na estrutura de controle de segurança e para identificar mudanças que não vão simplesmente eliminar sintomas, mas potencialmente todos os fatores de causa, incluindo os sistêmicos.

A análise CAST implica a compreensão do processo dinâmico que levou à perda. A análise resulta em múltiplas visões do acidente, dependendo da perspectiva e nível a partir do qual a perda está sendo visualizada. Embora descrito na forma de passos, não há implicação de que o processo de análise é linear ou um passo que tem de ser completado antes que o próximo seja iniciado. São eles:

1. Identificar os sistemas e riscos envolvidos na perda.
2. Identificar as restrições de segurança do sistema e requisitos do sistema associados esses riscos;
3. Documentar a estrutura de controle de segurança no local para controlar o risco e fazer cumprir as restrições de segurança;
4. Determinar a cadeia de eventos próximos que levaram à perda;
5. Analisar a perda no nível do sistema físico;
6. Analisar a perda nos níveis superiores da estrutura de controle de segurança;
7. Examinar a coordenação e a comunicação contribuintes em geral para a perda;
8. Determinar a dinâmica, as mudanças no sistema e a estrutura de controle de segurança referentes à perda;
9. Gerar recomendações.

4 METODOLOGIA

Nessa seção é relatado o procedimento para a seleção e obtenção de informações sobre o acidente aeronáutico que representa o caso desse estudo. A descrição detalhada do acidente de interesse selecionado para tal não é apresentada nesse texto, dada a confidencialidade das informações. Dessa forma, o texto não é referenciado diretamente. Essa seção apresenta também uma descrição desidentificada do acidente.

4.1 Seleção e obtenção de dados

Uma vez ainda não definido o acidente de estudo, a primeira etapa tratou da seleção dos acidentes de interesse (aqueles enquadrados na proposta) e da obtenção dos dados (junto ao CENIPA). Nesse caso, para a seleção foram utilizados os relatórios anuais da ANAC (2015) sobre acidentes aéreos no Brasil e o banco de relatórios do CENIPA (2015).

Todo o procedimento de seleção dos acidentes de interesse foi realizado com base nos termos do projeto proposto por Lima (2016), onde o acidente selecionado deveria ter apresentado certo impacto no sistema de operação de aeronaves civis no país. Entretanto, dada a desidentificação necessária das partes envolvidas, parte do enfoque foi também concentrado na seleção de acidentes relativamente comuns à realidade brasileira.

No caso do presente estudo, a seleção do acidente de interesse foi realizada de maneira a não somente buscar uma maior representatividade do acidente como ocorrência comum ao meio em estudo, mas também lidar com a necessidade da maior quantidade de informações oficiais e imparciais disponíveis sobre a ocorrência. Os critérios de seleção foram os seguintes: tipo de ocorrência, tipo de informação disponível, natureza dos fatores contribuintes, impacto das recomendações de segurança, tipo de aeronave envolvida, fator contribuinte específico mais comum e quantidade de informações disponíveis.

4.2 Desidentificação e Confidencialidade

Conforme a metodologia de trabalho proposta por Arnold (2009) em sua dissertação, a desidentificação se deu de maneira que nenhuma das partes envolvidas no acidente de interesse selecionado como objeto de estudo fossem identificadas nos materiais relatados a terceiros ou publicados em quaisquer veículos acadêmico-científicos. O processo de desidentificação se motiva na isenção de consequências jurídicas que os resultados da pesquisa poderiam representar para as partes envolvidas tanto no acidente em si, no processo de investigação e análise, ou ainda no presente trabalho.

Desta forma, os dados foram desidentificados pela substituição da matrícula da aeronave envolvida pelo tipo de aeronave e retenção das identidades das pessoas encarregadas com a investigação, unidades de controle de tráfego aéreo e operadores envolvidos. O mapa do espaço aéreo apresentado na descrição a seguir é fictício e os nomes dos pontos de navegação e o formato geral do espaço aéreo foram alterados, mas as relações entre os envolvidos e posições relativas proporcionais das partes relevantes do espaço aéreo são precisos.

5 ACIDENTE EM ESTUDO

A informações apresentadas a seguir são uma transcrição resumida do texto original do Relatório Final emitida pelo CENIPA. O texto é desidentificado e não é referenciado dada a confidencialidade sobre as informações do acidente. O conteúdo completo do Relatório Final, não é apresentado neste texto dada a sua extensão. Contudo, as informações apresentadas a seguir são inteiramente coerentes com o Relatório Final do acidente selecionado.

5.1 Histórico da Ocorrência

A aeronave BIMOTOR decolou da pista 30 do Aeródromo ALFA com destino ao Aeródromo BRAVO, pelas 14h00min, com o piloto e o copiloto a bordo, com plano de voo VFR e posterior mudança para IFR.

De acordo com testemunhas, durante a decolagem, a aeronave correu normalmente sobre a pista. Após a rotação, assumiu uma atitude bastante cabrada (pitch up aparentemente excessivo), subindo até uma altura estimada de 1500 pés e nivelando as asas momentaneamente. Então, foi observado que a mesma começou a imprimir uma ligeira inclinação para a direita, aumentando progressivamente até alcançar 90º.

Em seguida, a aeronave iniciou uma descida com o nariz aproado com o solo (quase na vertical), vindo a atingir uma área residencial localizada a uma milha náutica à noroeste do Aeródromo ALFA.

Os dois tripulantes e seis pessoas que residiam nas casas atingidas faleceram no acidente. Três residências foram atingidas, sofrendo danos estruturais graves. A aeronave sofreu danos graves decorrentes do impacto e da ação do fogo.

A aeronave BIMOTOR, de asa baixa, equipada com dois motores turbofan e tanques de ponta de asa, foi fabricada pelo FABRICANTE, em 1981.

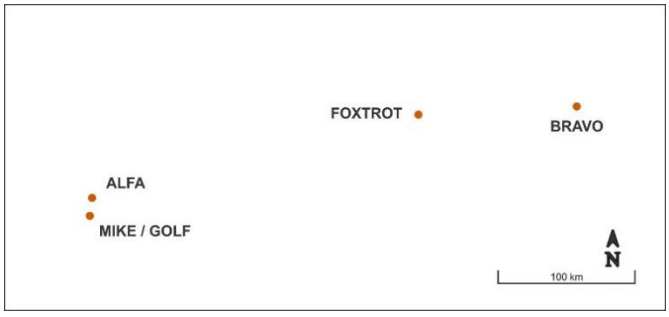

Figura 2 - Mapa esquemático desidentificado do acidente em estudo (Adaptado do Relatório Final do acidente em estudo)

6 ANÁLISE CAST

Nessa seção é apresentado o procedimento de desenvolvimento da análise do acidente em questão utilizando a ferramenta para análise de ocorrências (CAST) proposta segundo a abordagem STAMP.

Para facilitar a descrição da malha foi utilizada a plataforma XSTAMPP (Extensible STAMP Platform for Safety Engineering), desenvolvida por Asim Abdulkhaleq e Stefan Wagner (2014, 2015), com o objetivo de integrar a abordagem STAMP e todas as suas ferramentas em uma única plataforma de interface simplificada.

Nesse caso especificamente, bem como realizado por Nelson (2008) e por Arnold (2009), em seus respectivos trabalhos, o passo 4 é apresentado antes dos passos 1, 2 e 3. Dessa forma, as descrições desses primeiros passos são contextualizadas, facilitando a compreensão do leitor sobre o acidente e sobre a lógica da análise.

6.1 Passo 4 - Cadeia de Eventos Próximos

Enquanto que a cadeia de eventos falhos não fornece as informações mais importantes sobre a causalidade, os acontecimentos básicos relacionados com a perda precisam de ser identificados de modo que o processo físico envolvido na perda possa ser compreendido.

Para o acidente da aeronave BIMOTOR, os eventos de processos físicos são relativamente simples: A aeronave decolou da pista 30 do Aeródromo ALFA com destino ao Aeródromo BRAVO, com o piloto e o copiloto a bordo, com plano de voo VFR e posterior mudança para IFR. Após a decolagem, a aeronave desviou a trajetória para a direita e houve a perda de controle em voo, vindo a colidir contra o solo. Os dois tripulantes que estavam na aeronave e mais seis moradores das casas atingidas faleceram no local. A aeronave sofreu danos graves decorrentes do impacto e da ação do fogo.

Nesse caso, os eventos diretos que levaram ao impacto, aos danos e às mortes são:

1. O voo anterior ao acidente (FOXTROT-ALFA) é realizado com o Piloto a cargo da pilotagem sem qualquer pane ou anormalidade reportada;
2. Durante a preparação da cabine para o voo, que é realizada pelo Copiloto sem a presença do instrutor, um som similar à atuação da *standby pump* e da *cross flow valve* é emitido por um período aproximado de 3 minutos, segundo o CVR;
3. No reabastecimento, com o acompanhamento do Piloto, são colocadas 880 lb de combustível pelo bocal de abastecimento do *wing tip tank* esquerdo e, em seguida, 880 lb pelo bocal de abastecimento do *wing tip tank* direito;
4. O piloto entra na aeronave e procede o início do taxiamento;
5. O Copiloto inicia o taxiamento, enquanto o Piloto (instrutor) conversa, através do telefone celular, com o Piloto do helicóptero que está em FOXTROT;
6. O Piloto comanda a aeronave durante a decolagem;
7. O Copiloto reporta o escorregamento da aeronave durante a decolagem;
8. Após a rotação, a aeronave assume uma atitude bastante cabrada (*pitch up* aparentemente excessivo), segundo testemunhas;
9. O Piloto reporta um desbalanceamento no combustível e solicita que o Copiloto corrija a anormalidade;
10. A aeronave sobe até uma altura de 1500 pés, nivelando as asas momentaneamente;

11. A aeronave imprime uma ligeira curva para a direita, aumentando gradativamente a inclinação até aproximadamente 90°, segundo testemunhas;
12. A cerca de 1400 pés de altura ocorre a perda de controle em voo;
13. A aeronave inicia uma descida com o nariz aproado com o solo (quase na vertical);
14. Um som similar ao da atuação do "*shaker*" do manche da aeronave é emitido, segundo o CVR;
15. A aeronave sofre o impacto contra o solo, atingindo três casas da região residencial localizada a uma milha náutica à noroeste do Aeródromo ALFA;
16. Os dois tripulantes e seis pessoas que residiam nas casas atingidas falecem no acidente;
17. As três residências atingidas sofrem danos estruturais graves; e
18. A aeronave sofre danos graves decorrentes do impacto e da ação do fogo.

6.2 Passo 1 - Sistemas e Riscos envolvidos na Perda

O acidente de interesse está relacionado ao processo sistêmico de operação segura de uma aeronave civil.

Nesse caso, o Sistema Gerenciamento de Segurança Operacional (SGSO) é o sistema de mais alto nível responsável por controlar as operações e a segurança de todas as pessoas envolvidas na operação civil de aeronaves no país. Já o Sistema de Busca e Salvamento Aeronáutico é o sistema responsável, por controlar as atividades de assistência às pessoas envolvidas em ocorrências na aviação.

Em uma perspectiva completa do acidente, seriam abordados dois processos distintos: a operação segura da aeronave e também as operações de alerta à população, busca e salvamento das pessoas envolvidas no acidente. Contudo, uma vez que a análise original do acidente se ateve ao escopo do SGSO, o presente trabalho, se restringe às informações apresentadas no Relatório Final daquele acidente.

Dessa forma, os perigos sistêmicos principais relacionados ao acidente em estudo são:

- Perigo 1: Aeronave preparada sozinha por membro da tripulação sem o devido treinamento;
- Perigo 2: Decolagem da aeronave sem realizar o procedimento do checklist completo;

6.3 Passo 2 - Restrições e Requisitos de Segurança do Sistema

Dados os perigos associados à perda, as restrições de segurança do sistema são as seguintes:

- Restrição 1: A aeronave não deve ser preparada sozinha por membro da tripulação sem o devido treinamento;
- Restrição 2: A decolagem da aeronave deve ser realizada somente após a realização completa dos procedimentos do checklist;

6.4 Passo 3 - Estrutura Hierárquica de Controle de Segurança (EHCS)

Uma estrutura de controle de segurança de altos níveis é criada para facilitar a visualização dos controladores primários, ações de controle e linhas de retorno. Para facilitar a visualização, a Estrutura Hierárquica de Controle de Segurança (EHCS) do sistema em questão é apresentada no Anexo A, ao fim deste texto. A EHCS retratada é simplificada e idealizada de maneira a capturar um cenário mais generalista do SGSO.

De um modo geral, a descrição de cada componente na estrutura de controle inclui as seguintes informações:

- Requisitos e restrições de segurança;
- Ações de controle inseguras;
- Falhas no modelo mental;
- Contexto no qual as decisões são tomadas.

No caso, o detalhamento dessas informações será apresentado nos tópicos a seguir.

6.5 Passo 5 - Perda no Nível do Sistema Físico

Nessa etapa do processo CAST, o sistema físico (isto é, a aeronave BIMOTOR) é analisado no intuito de identificar os controles físicos e operacionais e qualquer falha física, interação disfuncional ou perturbação, externa ao sistema, que de alguma forma contribuíram para a ocorrência. O objetivo, portanto, é determinar porque os controles físicos atuantes durante o acidente não foram efetivos em prevenir o risco.

De um modo geral, a análise do nível físico do sistema busca determinar a contribuição de cada um dos itens a seguir: requisitos e restrições de segurança violados; falhas e ações de controle inadequadas; e contexto do sistema físico.

Além disso, nas descrições a seguir são apresentadas referências numéricas à figura

No caso, os detalhamentos são apresentados a seguir.

Equipamentos de Segurança e Emergência

- Equipamentos de proteção para a tripulação;
- *Checklists* da aeronave BIMOTOR;
- Manual de Voo da aeronave BIMOTOR (MV); e
- Manual Geral de Operações da empresa ECHO (MGO);

Requisitos e Restrições de Segurança Violados

- O procedimento de preparação da aeronave deve sempre ser orientado pelo checklist;
- As bombas de fluxo cruzado não devem funcionar de maneira inadvertida para a tripulação;
- As bombas de fluxo cruzado devem funcionar apenas sob comando da tripulação;
- A aeronave não deve decolar com desbalanceamento de combustível excessivo, conforme MV;
- A aeronave não deve decolar com atitude excessivamente cabrada, conforme MV;
- A aeronave não deve apresentar tendência de rolamento expressiva devido a desbalanceamento de combustível;

- Deve ser fornecida a informação de atitude insegura para a tripulação durante as operações da aeronave;
- Deve ser fornecida a informação de distúrbios externos ao sistema para a tripulação;
- Não deve ocorrer impacto da aeronave contra o solo; e
- Caso ocorra impacto da aeronave contra o solo, o impacto não deve ser catastrófico.

Falhas e Ações de Controle Inadequadas

- Procedimento de preparação da cabine inadequado;
- Funcionamento inadvertido das bombas de fluxo cruzado;
- Funcionamento não-comandado das bombas de fluxo cruzado;
- Decolagem inadequada da aeronave, com desbalanceamento de combustível excessivo, conforme o MV;
- Decolagem inadequada da aeronave, com atitude excessivamente cabrada, conforme o MV;
- Indicações inadequadas sobre as situações inseguras da aeronave:
    - Funcionamento inadvertido da bomba de fluxo cruzado;
    - Atitude excessivamente cabrada da aeronave; e
    - Desbalanceamento de combustível excessivo; e
- Controle inadequado da tripulação sobre os comandos da aeronave.

Contexto do Sistema Físico

- O voo anterior ao voo do acidente (FOXTROT-ALFA) é realizado com o Piloto a cargo da pilotagem sem qualquer pane ou anormalidade reportada;
- Funcionamento inadvertido das bombas de fluxo cruzado (no voo do acidente);
- Diretiva de Aeronavegabilidade (DA) sobre o funcionamento inadvertido das bombas de combustível (*Standby Fuel Pump Annunciators*).

6.6 Passo 6 - Perda nos Níveis Hierárquicos Superiores da EHCS

Para analisar quais restrições de segurança foram violadas no nível do sistema físico e por que elas não foram controladas nesse nível, os níveis mais elevados da EHCS devem ser examinados para explorar as possíveis contribuições para aqueles controles inadequados.

Quaisquer decisões humanas ou ações de controle de falhas devem ser entendidas, segundo Leveson (2011), em termos de quais são as informações disponíveis para os controladores, bem como qualquer informação exigida que não estava disponível; o contexto e o ambiente em que a decisão está sendo tomada; as estruturas de valores subjacentes à decisão; quaisquer falhas no processo ou modelos mentais de quem toma as decisões e por que essas falhas existiram.

Dessa forma, restringindo as análises às informações fornecidas pelo Relatório Final do acidente em questão, a seguir são apresentadas as considerações sobre os componentes da EHCS. De um modo geral, a descrição de cada componente na estrutura de controle inclui as seguintes informações:

- Requisitos e restrições de segurança;
- Ações de controle inseguras;
- Falhas no modelo mental; e
- Contexto no qual as decisões são tomadas.

Os controladores da EHCS serão apresentados em grupos, conforme a divisão apresentada no Anexo A:

- Tripulação (Piloto e Copiloto);
- Torre de Controle (Controlador de Tráfego);
- Empresa (Diretor Executivo, Diretor de Operações, Equipe de Apoio, Diretor de Manutenção e Intermediário);
- Fabricante (Diretor Executivo, Diretor de Serviços e Suporte ao Cliente); e

Agência Reguladora (Regulador)

6.6.1 Tripulação: Piloto

Requisitos e Restrições de Segurança

- Operar a aeronave segundo os procedimentos e normas da Empresa ECHO, as orientações do Controle de Tráfego Aéreo e as regulações da Agência Reguladora;
- Preparar a cabine para voo conforme os manuais de operação da aeronave;
- Decolar a aeronave com atitude em conformidade com os manuais de operação da aeronave;
- Manter a aeronave sob controle em conformidade com os manuais de operação da aeronave; e
- Supervisionar o treinamento do Copiloto.

Ações de Controle Inseguras

- Estava ausente durante todo o procedimento de preparação da cabine para o voo;
- Estava ausente durante o procedimento de partida dos motores;
- Falava ao celular durante o taxi da aeronave na pista;
- Até a decolagem, não atuava sobre o sistema físico (aeronave);
- Comando de preparação da cabine, partida do motor e taxi da aeronave para o Copiloto (em treinamento, sem acompanhamento)
- Não realizou o *briefing* de decolagem;
- Não utilizava o *checklist*;
- Não cobrava o uso do *checklist* pelo Copiloto;
- Não apresentava o Diário de Bordo para o Setor de Operações;
- Não reportava ao Setor de Operações sobre a situação do treinamento do Copiloto;
- Acumulo de funções do sistema operacional;
- Comandou a decolagem para o Copiloto (em treinamento, com acompanhamento, sob pressão);

- Comandou o balanceamento do combustível em voo para o Copiloto (em treinamento, com acompanhamento, sob pressão);
- Imprimiu um comando de atitude extremante cabrada para a decolagem da aeronave;
- Coordenar as atividades de operação da aeronave diretamente com a Diretoria Executiva da empresa; e
- Interferia nas atividades de manutenção da aeronave.

Falhas no Modelo Mental

- Acreditava que o Copiloto poderia realizar os procedimentos de preparação da cabine, partida do motor e taxi da aeronave, sem acompanhamento;
- Acreditava que a aeronave suportava a atitude insegura imposta e que não haveriam consequências para a segurança do voo;
- Pensava que devido à experiência, não seria necessária a leitura do checklist ou do briefing de decolagem;
- Acreditava que o Copiloto poderia realizar os procedimentos de decolagem, ainda que em fase de treinamento e sob grande pressão; e
- Acreditava que, dada a sua experiência, deveria/poderia interferir na programação das atividades de manutenção.

Contexto das decisões

- Pressa para chegar ao destino;
- Condições climáticas desfavoráveis iminentes;
- Acumulo de funções;
- Dispersão na execução das operações;
- Costume de pilotar a mesma aeronave;
- Distanciamento da empresa;
- Aeronave com tendência de rolamento; e
- Excesso de confiança.

6.6.2 Tripulação: Copiloto

Requisitos e Restrições de Segurança

- Operar a aeronave segundo os procedimentos e normas da Empresa, as orientações do Controle de Tráfego Aéreo e as regulações da Agência Reguladora;
- Realizar as tarefas orientadas pelo supervisor de treinamento (Piloto); e
- Realizar os treinamentos necessários à imersão de pilotagem da aeronave em questão.

Ações de Controle Inseguras

- Realizou os procedimentos de preparação da cabine, partida do motor e taxi da aeronave, sem qualquer supervisão;
- Não gerou feedback com a frequência adequada ao Piloto sobre a situação dos procedimentos do qual foi encarregado;
- Até a decolagem, era o único controlador atuante sobre o sistema físico (aeronave);
- Não realizou o briefing de decolagem;
- Não utilizou o checklist;
- Não completou as horas de treinamento em simulador de voo da Empresa ECHO;
- Não reportou diretamente ao Setor de Operações;
- Iniciou os procedimentos de decolagem, com supervisão, mas em fase e treinamento e sob pressão; e
- Realizou o procedimento de balanceamento de combustível, mesmo em situação de treinamento.

Falhas no Modelo Mental

- Não possuía a habilitação, nem, possivelmente, o conhecimento para realizar os procedimentos que realizava;
- Apresentava comportamento incoerente com a formação e os manuais da empresa ECHO e da aeronave; e
- Não questionava os comandos do Piloto e confiava na experiência e no treinamento dele como Piloto e supervisor.

Contexto das decisões

- Pressão para apresentar um bom desempenho;
- Em fase de treinamento sob supervisão do Piloto;
- Condições Climáticas desfavoráveis iminentes;
- Distanciamento da empresa; e
- Contratado em período de experiência e treinamento.

6.6.3 Torre de Controle: Controlador de Tráfego

Requisitos e Restrições de Segurança

- Controlar o tráfego aéreo segundo os procedimentos e normas internacionais, as informações fornecidas pelas empresas de operação de aeronaves e pelos tripulantes das aeronaves controladas;
- Verificar a execução do plano de voo informado pela tripulação; e
- Reportar anormalidades nas operações e NOTAMs à tripulação.

Contexto das decisões

- Atitude da aeronave incoerente com o plano de voo submetido anteriormente.

6.6.4 Empresa ECHO: Diretor Executivo

Requisitos e Restrições de Segurança

- Gerenciar, de maneira sustentável, a empresa de taxi aéreo ECHO, com a operação da aeronave segundo os procedimentos e normas da Empresa, e as regulações da Agência Reguladora;
- Manter a unidade da empresa para garantir a segurança das operações.

Ações de Controle Inseguras

- Permitiu a operação da aeronave sem coordenação ou suporte em uma base diferente da sede;
- Controlou diretamente as operações da aeronave, com o Piloto, sem o intermédio do setor de operações;
- Permitiu que a tripulação deixasse de reportar ao setor de operações da empresa; e

- Não instalou um setor de Recursos Humanos para a empresa.

Falhas no Modelo Mental

- Acreditava que essa situação não prejudicaria a segurança operacional;
- Situação incoerente com as normas e padrões de certificação da empresa pela agência reguladora; e
- Modelo de processo adaptado pela confiança no Piloto.

Contexto das decisões

- Aeronave não fazia parte do escopo operacional da empresa;
- A certificação da aeronave no escopo operacional da empresa estava em andamento; e
- Confiança na competência e experiência do Piloto para coordenar as operações.

6.6.5 Empresa ECHO: Diretor de Operações

Requisitos e Restrições de Segurança

- Gerenciar as atividades de operação de aeronaves da empresa de taxi aéreo ECHO, segundo os procedimentos e normas da Empresa, e as regulações da Agência Reguladora;

Ações de Controle Inseguras

- Permitiu a operação da aeronave em uma base diferente da sede;
- Permitiu a coordenação de atividades de operação da aeronave diretamente entre o Piloto e a Diretoria Executiva da empresa ECHO;
- Não cobrou o preenchimento dos diários de bordo do Piloto;
- Não controlou o processo de treinamento do Copiloto; e
- Não cobrou do Copiloto a realização dos treinamentos em simulador de voo da aeronave.

Falhas no Modelo Mental

- Permitia que o Piloto operasse a aeronave sem qualquer suporte operacional, apenas coordenando as missões com a Diretoria executiva.

Contexto das decisões

- Distanciamento entre a tripulação e a base principal da empresa ECHO;
- Setor de operações inoperante quando relacionado às operações dessa aeronave; e
- Aeronave não fazia parte oficialmente do escopo operacional da empresa

6.6.6 Empresa ECHO: Equipe de Apoio

Requisitos e Restrições de Segurança

- Suportar/Apoiar as atividades de operação de aeronaves da empresa de taxi aéreo ECHO, segundo os procedimentos e normas da Empresa, e as regulações da Agência Reguladora.

Ações de Controle Inseguras

- Ausente durante a operação da aeronave;

Contexto das decisões

- Todo o setor de operações era inoperante; e
- Não havia sido informada sobre a operação da aeronave naquele dia e hora.

6.6.7 Empresa ECHO: Diretor de Manutenção

Requisitos e Restrições de Segurança

- Gerenciar as atividades de manutenção da empresa de taxi aéreo ECHO, segundo os procedimentos e normas da Empresa, e as regulações da Agência Reguladora.

Ações de Controle Inseguras

- Permitir a interferência do Piloto nas atividades de manutenção;
- Não se comunicar diretamente com o Piloto; e
- Não reportar, ao Fabricante, problemas nos manuais relacionados à falta de informações específicas sobre o desbalanceamento de combustível dessa aeronave.

Falhas no Modelo Mental

- Acreditava que essa alteração na estrutura de controle de segurança não prejudicaria a situação.

Contexto das decisões

- Desentendimento com o Piloto; e
- Ausência de um setor de Recursos Humanos.

6.6.8 Empresa ECHO: Intermediário de Manutenção

Requisitos e Restrições de Segurança

- Transmitir, de maneira integral, a comunicação entre as atividades de manutenção da empresa e o piloto;

Falhas no Modelo Mental

- Acreditava que essa alteração na estrutura de controle de segurança não prejudicaria a situação.

6.6.9 Fabricante: Diretoria Executiva

Requisitos e Restrições de Segurança

- Gerenciar as atividades de fabricação de aeronaves do Fabricante, segundo as regulações da Agência Reguladora.

Ações de Controle Inseguras

- Certificação antiga, sem proposta de atualização por parte do Fabricante; e
- Publicações técnicas sem orientações efetivas sobre o problema de desbalanceamento de combustível, que já era conhecido pelo Fabricante.

6.6.10 Fabricante: Suporte ao Cliente

Requisitos e Restrições de Segurança

- Gerenciar as atividades de suporte às aeronaves produzidas pelo Fabricante, segundo as regulações da Agência Reguladora, bem como a atualização da documentação de manutenção do sistema.

Ações de Controle Inseguras

- Lançamento tardio de recomendação sobre o funcionamento inadvertido das bombas de combustível.

6.6.11 Agência Reguladora: Regulador

Requisitos e Restrições de Segurança

- Gerenciar as atividades de regulação da operação de aeronaves, segundo os procedimentos e normas da OACI.

Ações de Controle Inseguras

- Fiscalização ineficiente, uma vez que:
  - Permitiu a empresa operar a aeronave em questão;
  - Permitiu o Copiloto atuar na aeronave, mesmo sem o devido treinamento; e
  - Permitiu publicações técnicas incompletas pelo Fabricante (sem as informações específicas sobre desbalanceamento); e
- Certificação antiga, sem proposta de atualização.

Falhas no Modelo Mental

- Acredita que a renovação da certificação é suficiente para a manutenção dos níveis de segurança.

6.7 Passo 7 - Coordenação e Comunicação Contribuintes

Revisando o Passo 6 do método CAST, é evidente que os maiores problemas desse acidente não estão somente nos componentes que falharam isoladamente, mas na interação entre cada um deles. Uma vez que já apresentada essa discussão anteriormente no passo 6º, do ponto de vista de cada um dos componentes, a seguir é apresentada uma perspectiva sistêmica. Dessa forma, todos os canais de comunicação e coordenação são examinados para identificar cenários onde a comunicação e a coordenação entre controladores resultou em uma fonte de perigos para o sistema ou contribuiu de alguma forma para a ocorrência do acidente.

Seguindo a mesma lógica do Passo 6, serão apresentados os meios de comunicação falhos entre os componentes, seguindo a EHCS de baixo (tripulação) para cima (agência reguladora).

Primeiramente, na relação entre o Piloto e o Copiloto é marcada por uma comunicação falha, seja pela ausência do Piloto durante a preparação da cabine, seja pela falta de feedback frequente do Copiloto para o Piloto. Esta situação muda apenas quando iniciada a decolagem da aeronave pelo Piloto. Neste caso, esse canal de comunicação passa a apresentar comandos inseguros por parte do Piloto. Essas interações inseguras acabaram levando o sistema como um todo a um estado de elevado perigo associado.

Outra falha na comunicação evidente é daquela realizada entre a Tripulação e o Controlador de Tráfego. Nesse cenário, o Controlador, ao perceber a incoerência da atitude da aeronave com o plano de voo submetido, tentou contatar a Tripulação por duas vezes sem obter resposta. Existem muitas possibilidades diferentes, nesse caso: o sistema de comunicação pode ter falhado e uma das partes não estava recebendo a mensagem; ou a Tripulação pode não ter respondido para se concentrar em controlar a aeronave; ou ainda a mensagem pode ter chegado atrasada de alguma forma. Em ambos os casos, a comunicação entre esses componentes do sistema foi incoerente.

No âmbito da empresa ECHO Taxi Aéreo Ltda., a Tripulação se comunicava diretamente com a Diretoria da empresa e dessa forma, acabava tornando não efetivo a atuação, não só o Setor de Operações, mas todo o sistema de comunicação desse setor da empresa. Além disso, a Tripulação não providenciava o reporte ao então controlador, Diretor Executivo da empresa, tornando falho esse canal de comunicação adaptado. Uma vez que havia uma interação entre os comandos da Diretoria da empresa e os comandos do Setor de Operações, também existe aqui um problema de coordenação de comandos, a qual, se implementada de maneira correta, poderia evitar a maioria dos problemas relacionados ao relacionamento entre a Tripulação e o Setor de Operações (Diretor de Operações e Equipe de Apoio).

Um outro problema de comunicação se evidencia na relação entre o Piloto e o Setor de Manutenção da empresa. O Diretor de Manutenção não tinha uma linha de contato direto com o Piloto da aeronave. Ainda que o Setor de Operações fosse operante ou que as atividades de manutenção fossem coordenadas entre o Setor de Operações e o Setor de Manutenção, o contato entre O Setor de Manutenção e a Tripulação ainda seria necessário para garantir o reporte rápido de problemas com a aeronave. Essa comunicação, nesse caso, foi adaptada, passando a ser feita por meio de um interlocutor (Interlocutor de Manutenção). Não é possível afirmar se essa comunicação era efetiva ou não, mas era ineficiente se comparada àquela realizada diretamente.

Além disso, os problemas de relacionamento e coordenação entre os controladores acabaram sendo resultado de uma ação de controle inadequada da Diretoria da empresa ECHO sobre as atividades da empresa. A implementação de um setor de gerenciamento de pessoas (recursos humanos) provavelmente traria melhorias nesse sentido. Gerenciando o relacionamento e a coordenação entre os controladores, a empresa ECHO, como um todo, apresentaria comunicações mais coerentes e eficazes.

No caso do relacionamento entre a empresa e o Fabricante, o Suporte ao Cliente passava os padrões e as documentações ao Setor de Manutenção da empresa ECHO, mas não há informações sobre o reporte de problemas no sentido contrário deste canal de comunicação. Da mesma forma, a comunicação entre a Diretoria de Serviços do Fabricante e a Diretoria da empresa ECHO era realizada de maneira ineficiente, possivelmente sem o reporte de problemas operacionais por parte a empresa ECHO.

Por fim, são considerados os canais de comunicação entre a Agencia Reguladora (Regulador) e todas as entidades atuantes na EHCS. Tanto para a tripulação, quanto para a empresa ECHO, ou para o Fabricante, não havia um canal de comunicação direto para o reporte de problemas ao Regulador. Além disso, não havia uma fiscalização efetiva para garantir a segurança nas atividades dos controladores do sistema. Outro problema estava relacionado à certificação da aeronave, que tinha uma certificação de tipo antiga e não havia sido revisada, evidenciando um problema na coordenação entre o Fabricante e o Regulador. Relacionado a empresa ECHO, o Regulador também não apresentava uma coordenação eficiente, dada a situação não regulada da aeronave na empresa ECHO.

6.8 Passo 8 - Dinâmica e Migração do Sistema

Na abordagem CAST/STAMP, os acidentes resultam da migração do sistema, ao longo do tempo, em direção às

restrições de segurança enfraquecidas. Nesse contexto, a análise da dinâmica do sistema mostra como o sistema foi enfraquecido ao longo do tempo e se tornou inseguro. O objetivo em se compreender a dinâmica é adaptar a EHCS para que sejam adequados à manutenção da segurança operacional do sistema.

Nesse texto não são apresentadas todas as possibilidades de dinâmica e migração do sistema e da EHCS, mas apresentada uma perspectiva geral desse efeito. As recomendações de Segurança, se bem trabalhadas, cobrem, de maneira sistêmica a maioria das possibilidades de ocorrência.

Observando o problema de um nível superior, é possível perceber que as necessidades da empresa ECHO apresentam grande influência na dinâmica do sistema e, consequentemente, na segurança do sistema operacional ao longo do tempo. As necessidades empresariais de lucro e custo-efetividade provavelmente geram pressões sobre as atividades operacionais para que apresentem uma melhor relação custo-benefício para a empresa. Esta pressão, quando no contexto das atividades da Tripulação, pode ocasionar um controle ineficiente sobre a aeronave. Desta forma, a aeronave passaria a operar em um estado de segurança operacional enfraquecida e o cenário de um acidente se torna iminente.

De uma perspectiva menos abrangente, outros problemas de dinâmica do sistema podem ser analisados. Um exemplo bastante evidente é a organização da estrutura da empresa sem um setor de recursos humanos. No caso, a empresa ECHO foi organizada de maneira à diretoria da empresa absorver as funções desse setor. É possível supor que com o passar do tempo e o acumulo de atividades, a empresa acumulou problemas de relacionamentos.

O fato de o Piloto apresentar problemas de relacionamento com o Setor de Manutenção, por exemplo, ocasionou de fato uma alteração na EHCS que incluiu um Intermediário nesse canal de comunicação (tornando-o indireto). Um canal de comunicação indireto pode ser ineficiente, uma vez que estará sempre sujeito à perspectiva de uma terceira pessoa, o Intermediário, que apresenta um viés, um contexto e um modelo de processo pessoal, o que pode ocasionar em interferências no canal de comunicação. Se o canal de comunicação sofre interferências, os comandos podem não ser interpretados da maneira como deveriam e podem se tornar inseguros. Este controle inadequado, pode levar o sistema a um estado de risco mais elevado em direção à ocorrência de um incidente.

Um cenário, nesse caso, poderia ser o funcionamento inadvertido da bomba de fluxo cruzado de combustível devido a uma ordem de manutenção interpretada de maneira incoerente devido à comunicação indireta entre o Piloto e o Setor de Manutenção da empresa ECHO.

6.9 Passo 9 - Recomendações de Segurança

O objetivo da análise CAST é a determinação de como as adaptações da EHCS devem ser feitas de maneira que sejam as mais práticas e econômicas para evitar acidentes semelhantes no futuro. Essas adaptações são geradas a partir de recomendações de segurança que podem ser físicas, organizacionais ou operacionais.

Muitas das recomendações são simplesmente práticas de bom manejo de segurança, mas é importante que todas sejam clarificadas. Além disso, os canais de feedback devem ser estabelecidos para determinar se as recomendações e alterações foram bem-sucedidas na redução do perigo.

Desta forma, cada um dos comportamentos falhos identificados nos Passos 5 a 8 da análise CAST, devem ser endereçados com recomendações de segurança coerentes para satisfazer os requisitos de segurança em cada um dos níveis hierárquicos do sistema.

As recomendações de segurança apresentadas a seguir são geradas para fornecer as restrições de segurança necessárias. Elas foram elaboradas buscando a mínima alteração no projeto da aeronave (e na certificação de tipo). Para facilitar a organização, elas estão divididas nos seguintes níveis:

1. Sistema Físico;
2. Tripulação;
3. Torre de Controle;
4. Empresa ECHO;
5. Fabricante; e
6. Agência Reguladora.

6.9.1 Recomendações sobre o Sistema Físico

1. As bombas de fluxo cruzado de combustível não devem funcionar de maneira inadvertida para a tripulação;
   a. Deve haver um sistema de sinalização sobre o funcionamento das bombas de fluxo cruzado de combustível;
   b. Deve haver um sistema de controle retroativo que garanta o funcionamento dessa sinalização;
   c. O sistema sinalização das bombas de fluxo cruzado de combustível não deve falhar;
   d. Em caso de falha, deve haver uma maneira alternativa de sinalização (e.g., sons característicos)
2. As bombas de fluxo cruzado de combustível devem funcionar apenas sob comando da tripulação;
   a. Deve haver um sistema de controle retroativo que possibilite a tripulação controlar, de maneira integral, o funcionamento das bombas de fluxo cruzado de combustível;
   b. O sistema de controle do funcionamento das bombas de fluxo cruzado de combustível deve responder, em condições normais de operação, apenas ao comando da tripulação;
   c. O sistema de controle de funcionamento das bombas de fluxo cruzado não deve responder a perturbações externas;
3. A aeronave não deve decolar com o combustível desbalanceado;
   a. A aeronave não deve decolar com o desbalanceamento de combustível acima do limite permitido em projeto;

b. Deve haver uma maneira de detectar, integralmente, a situação de desbalanceamento de combustível;
c. Deve haver um sistema de sinalização sobre o desbalanceamento de combustível próximo aos limites operacionais de desbalanceamento estabelecidos;
d. O sistema de sinalização de desbalanceamento excessivo de combustível, não deve falhar;
e. Em caso de falha do sistema de sinalização de desbalanceamento de combustível, deve haver um sistema de sinalização alternativo (e.g. indicadores de combustível em cada um dos tanques);

4. A aeronave não deve decolar com atitude excessivamente cabrada;
   a. Deve haver um sistema de sinalização sobre a atitude insegura da aeronave e dos comandos;
   b. Deve haver um sistema de controle retroativo que garanta o funcionamento dessa sinalização;
   c. O sistema sinalização de atitude insegura da aeronave não deve falhar;
   d. Em caso de falha, deve haver uma maneira alternativa de sinalização (e.g. *diretional gyro*)
5. A aeronave não deve apresentar tendência de rolamento expressiva devido a desbalanceamento de combustível;
   a. A aeronave não deve apresentar tendência de rolamento excessiva devido a desbalanceamento de combustível quando dentro dos limites operacionais de desbalanceamento;
   b. A aeronave deve apresentar maneiras de compensar a tendência de rolamento excessivo (e.g., empenagens);
6. Não deve haver perda de controle da aeronave por distúrbios externos ao sistema;
   a. A aeronave deve apresentar controlabilidade segura em todas as fases de voo;
   b. A controlabilidade da aeronave não deve ser prejudicada por perturbações externas;
   c. Em casos onde a aeronave apresentar falta de controlabilidade, devem haver dispositivos ou procedimentos para a recuperação das características operacionais da aeronave;
   d. Deve haver um sistema de fornecimento de informação à tripulação sobre distúrbios nos sistemas da aeronave;
   e. O sistema de fornecimento de informação à tripulação sobre distúrbios nos sistemas da aeronave não deve falhar;
   f. Em caso de falha, deve haver uma maneira alternativa de informação (e.g., medidores de pressão, técnicas de troubleshooting)
7. Não deve ocorrer impacto da aeronave contra o solo;
   a. Em caso de falha, a aeronave não deve se chocar contra o solo;
      i. Em caso de falha, a aeronave deve ser capaz de manter o voo até que possa pousar em segurança em um aeródromo próximo.
   b. Em caso de falha, devem haver dispositivos ou procedimentos que impeçam o impacto contra o solo;
   c. Caso não seja possível impedir o impacto, devem haver dispositivos ou procedimentos que minimizem as consequências do impacto tanto para a aeronave, quanto para todas as outras entidades envolvidas;
      ii. Caso ocorra impacto da aeronave contra o solo, o impacto não deve ser catastrófico;
      iii. Caso o impacto seja catastrófico, o número de vítimas deve ser minimizado;
      iv. Caso o impacto seja catastrófico, devem ser coordenadas missões de busca e salvamento para minimizar o número de vítimas;

6.9.2 Recomendações sobre a Tripulação

1. Operar a aeronave segundo:
   a. os procedimentos e normas da Empresa;
   b. as orientações do Controle de Tráfego Aéreo; e
   c. as regulações da Agência Reguladora;
2. A preparação da cabine para voo deve ser realizada de maneira coerente;
3. A aeronave deve ser decolada de maneira segura;
4. A aeronave deve ser mantida sob controle da tripulação durante todo o percurso do voo;
5. Os tripulantes em treinamento devem estar sob constante supervisão, de maneira coerente, controlada e segura;
6. Os tripulantes em treinamento devem ser auto reguladores, de maneira a executar as operações de forma coerente, controlada e segura;
7. A tripulação deve reportar todas as atividades de operação da aeronave ao Setor de Operações da empresa;
8. Os tripulantes não devem acumular funções dentro da organização da empresa;
9. Melhorar os dispositivos e procedimentos de adequação dos modelos mentais de processos (e.g. treinamentos, cursos).

6.9.3 Recomendações sobre a Torre de Controle

1. Controlar o tráfego aéreo segundo os procedimentos e normas internacionais, as informações fornecidas pelas empresas de operação de aeronaves e pelos tripulantes das aeronaves controladas;
2. A execução do plano de voo informado pela tripulação deve ser constantemente verificada;
3. Anormalidades nas operações e NOTAMs, devem ser reportadas e atualizadas à tripulação em operação.

6.9.4 Recomendações à Empresa ECHO

1. A empresa de operação das aeronaves ECHO Taxi Aéreo Ltda. deve ser gerenciada, de maneira sustentável, segundo os procedimentos e normas da Empresa, e as regulações da Agência Reguladora;
2. A unidade da empresa deve ser mantida para garantir a segurança das operações.
3. As atividades de operação de aeronaves da empresa ECHO devem ser gerenciadas segundo os procedimentos e normas da própria empresa (e.g. MGO), e as regulações da Agência Reguladora (e.g. RBACs);
4. As atividades de operação de aeronaves da empresa ECHO devem apresentar o devido suporte/apoio segundo os procedimentos e normas da empresa, e as regulações da Agência Reguladora;

5. As atividades de manutenção das aeronaves operadas pela empresa ECHO devem ser coordenadas segundo os procedimentos e normas da empresa (e.g. MGM), e as regulações da Agência Reguladora;
6. Todas as informações e canais de comunicação da empresa ECHO devem ser realizados por meios formais, transmitidos de maneira integral, para com a Tripulação ou entidades externas.

6.9.5 Recomendações ao Fabricante da aeronave

1. As atividades de fabricação de aeronaves do Fabricante devem ser gerenciadas e suportadas segundo as regulações da Agência Reguladora (e.g. RBACs);
2. As atividades de suporte às aeronaves produzidas pelo Fabricante devem ser realizadas e acompanhadas segundo as regulações da Agência Reguladora
3. A documentação de manutenção das aeronaves produzidas pelo fabricante deve ser atualizada de prontidão e com coerência, segundo as regulações da agência Reguladora.

6.9.6 Recomendações à Agência Reguladora

1. As atividades de regulação da operação de aeronaves, da fabricação de aeronaves, e da manutenção de aeronaves devem ser realizadas e gerenciadas segundo os procedimentos e normas da OACI (e.g. RBACs).
2. A atividades de fiscalização devem ser eficientes, de modo a impedir as irregularidades que aconteceram no acidente em estudo, segundo as regulações da Agência Reguladora;
3. As certificações de tipo muito antigas, com grandes alterações no projeto de fabricação devem ser atualizadas.

Segundo a própria filosofia SIPAER, o objetivo da investigação e análise de acidentes aeronáuticos objetiva, exclusivamente, o aumento da segurança operacional na aviação. (CENIPA, 2012)

Desta forma, são considerados os resultados desta análise, não os fatores contribuintes para a perda, mas sim as recomendações de segurança que são geradas a partir da análise. Portanto, os resultados desse estudo estão apresentados na descrição do desenvolvimento desse Passo 9.

7 DISCUSSÃO

Na seção anterior foi apresentado o desenvolvimento da análise CAST e as recomendações de segurança geradas deste processo, que são os resultados desse estudo.

Para efeitos de comparação, são apresentadas a seguir, um resumo das recomendações de segurança emitidas no Relatório Final do acidente em estudo.

7.1 Recomendações de Segurança

7.1.1 À Empresa ECHO Táxi Aéreo, recomenda-se:

1. Inserir em seu programa de treinamento instrução aos pilotos sobre limitações operacionais e performance de qualquer tipo de aeronave pertencente a sua frota, as quais estão previstas no manual do fabricante, considerando a influência de diversos tipos de situações adversas, tais como: desbalanceamento de combustível nas fases de decolagem, cruzeiro e pouso, limites de desempenho da aeronave em pistas contaminadas, influência de condições meteorológicas adversas, temperatura elevada, baixa pressão atmosférica e voo em ar turbulento.
2. Inserir no programa de treinamento dos instrutores um controle adequado de proficiência na realização dos procedimentos normais e de emergências, permitindo uma melhor difusão da doutrina de Segurança de Voo, no que concerne à obediência aos limites da aeronave e à realização dos procedimentos preconizados no Manual de Operação do fabricante.
3. Aprimorar o Programa de Gerenciamento de Recursos de Tripulação (CRM) da empresa, tornando obrigatória a participação de todos os tripulantes, levando-se em consideração as características de operação dos voos da empresa, em especial, a realização de voos de instrução.
4. Estabelecer uma sistemática de acompanhamento e de supervisão da instrução de voo realizada por tripulantes da empresa, determinando aos instrutores a confecção de fichas de avaliação de pilotos, nas quais devam conter comentários do desempenho dos alunos em cada voo ou etapa de voo.
5. Programar o treinamento inicial de simulador a todos os tripulantes em fase inicial de treinamento, conforme o previsto no RBHA 135, de forma a autorizar o voo de instrução na aeronave somente após o treinamento inicial de simulador.
6. Estabelecer uma política solidificada de operação de suas aeronaves fora da base sede, de forma a permitir uma correta supervisão das atividades, bem como a melhor assistir os tripulantes e a aeronave, fornecendo-lhes um padrão mínimo de apoio necessário às atividades de solo, nos casos de abastecimento, pré-voo, limpeza, partida de motores e outros serviços de rampa.
7. Programar aulas e palestras a todos os tripulantes e funcionários da empresa a respeito da participação do fator humano na prevenção de acidentes aeronáuticos, abordando os conceitos como cultura organizacional, ambiente organizacional, condições latentes, falhas ativas e acidente organizacional.
8. Estabelecer uma estratégia de recrutamento de tripulantes adequada à sua política de operação, de forma a diminuir desvios de conduta de procedimentos previstos no MGO e a melhor padronizar os procedimentos determinados pelo setor de operações.

7.1.2 À Agência Reguladora, recomenda-se:

1. Estabelecer uma política de segurança, de forma a impedir a emissão de concessões de "desvios" de procedimentos e de regras estabelecidas em regulamentações da Aviação Civil, mormente, àqueles relacionados à treinamento inicial de

simulador e voos em aeronaves à reação operadas por empresas de táxi aéreo.

2. Implantar uma política de acompanhamento dos processos de treinamento de tripulantes de empresas de táxi aéreo, de forma a melhor supervisionar o setor de operações da empresa, quanto à instrução de voo dos tripulantes (inicial ou periódica).
3. Avaliar, em conjunto com o órgão de certificação primária da aeronave BIMOTOR, a viabilidade de determinar ao fabricante da aeronave que estabeleça os limites máximos de desbalanceamento de combustível da aeronave BIMOTOR para as fases de decolagem e de cruzeiro, divulgando-os a todos os operadores em documentação pertinente.
4. Avaliar, em conjunto com o órgão de certificação primária da aeronave BIMOTOR, a viabilidade de serem implantadas melhorias no painel de controle de combustível, de forma que o mesmo apresente simultaneamente a quantidade existente em cada tanque, visando prover segurança na leitura e na interpretação feita pela tripulação.

7.1.3 O SERIPA-X deverá, no prazo de seis meses:

1. Realizar reuniões, aulas e palestras sobre padronização de instrução de voo para todos os instrutores de voo de empresas de táxi aéreo de seu âmbito de atuação, enfatizando não só os aspectos do papel do instrutor de voo na prevenção de acidentes, como a necessidade estabelecer uma sistemática de acompanhamento do desempenho do aluno, do instrutor e dos processos de instrução na formação de pilotos em geral.

7.2 Análise Comparativa

O Princípio da Incerteza de Heisenberg afirma que: "A mensuração da posição das partículas perturba, necessariamente, a dinâmica dessas partículas, e vice-versa". Dessa forma, o princípio da incerteza é uma manifestação do efeito do observador. Um problema semelhante surge nas abordagens de análise comparativa. A comparação direta requer uma análise separada do mesmo evento usando diferentes técnicas, mas a análise de um evento envolve, inevitavelmente, o viés individual (ainda que inconscientemente). Assim, a primeira análise pode afetar a segunda análise, quando realizada pela mesma pessoa. Por outro lado, uma análise do mesmo evento realizada por diferentes indivíduos que usam abordagens diferentes (como é o caso da comparação apresentada nessa tabela) envolverá preconceitos individuais. Dessa forma, comparações diretas absolutamente imparciais figuram um cenário praticamente impossível. (ARNOLD, 2009)

Claramente, as recomendações de segurança emitidas pelo CENIPA são escritas de maneira distinta daquelas geradas na análise CAST. Dessa forma, as comparações propostas são baseadas na semântica dos textos em questão.

Conforme pode ser observado, todos os pontos apresentados pelo Relatório Final do acidente em estudo foram adereçados de alguma maneira pelas recomendações de segurança geradas pela analise CAST. Esse cenário representa um forte indício de que a ferramenta CAST, baseada na abordagem STAMP, pode, de fato, ser utilizada como ferramenta complementar na análise de ocorrências em sistemas complexos, como é o caso do sistema de operação civil de aeronaves no Brasil e no mundo.

É notável também o fato de apenas uma pequena parcela das recomendações de segurança geradas pela análise CAST foram adereçadas. As recomendações de segurança do Relatório Final do acidente em estudo foram distribuídas entre 11 das 53 subdivisões de recomendações de segurança geradas pela análise CAST. Contudo, não é possível afirmar que esses números tenham um significado quantitativo expressivo, uma vez que os contextos das análises são diferentes e seus resultados são requisitos de níveis diferentes.

A grande maioria dessas recomendações não é pareada provavelmente por representarem culturas de boas práticas, comuns à indústria. Porém, essas recomendações de segurança não têm menor valor por isso, já que são derivadas das falhas e incoerências evidenciadas nas análises dos componentes da EHCS. Portanto, ainda que classificadas como boas práticas, são necessárias à manutenção dos níveis de segurança do sistema.

Nesse contexto, a diferença principal entre os resultados, é o nível das recomendações de segurança (requisitos para o sistema). Enquanto que a análise do Relatório Final do acidente em estudo recomenda requisitos de baixo nível, isto é, como as implementações devem ser realizadas no sistema, a análise CAST gerou recomendações de requisitos de alto nível. Esse segundo caso representa o que deve ser alcançado pelo sistema, sem indicar de que maneira deve ser realizada a implementação.

É possível que, o desdobramento das recomendações de segurança da análise CAST resulte em recomendações de baixo nível semelhantes às indicadas pela análise do Relatório Final do acidente em estudo. Nesse caso, a afirmação demanda do desenvolvimento dessas recomendações para a verificação dessa hipótese.

Contudo, existe uma evidência de que seria esse o caso. São indicados diversos pontos em que as recomendações de segurança da análise apresentada no Relatório Final do acidente em estudo são representadas. Um exemplo dessa ocorrência são os canais de controle entre a Agência Reguladora e os outros componentes da EHCS. Nesse caso, é representada recomendação à Agência Reguladora sobre novas políticas de segurança, de forma a impedir "desvios" de procedimentos e de regras estabelecidas em regulamentações da aviação civil.

Dessa forma, é possível afirmar que a análise CAST, conforme esperado, gerou requisitos de segurança diretivos de implementação no sistema, que podem ser aplicadas não

somente ao contexto da empresa ECHO, mas no sistema de aviação civil como um todo.

Assim, com a análise CAST gera recomendações que tratam não apenas as causas diretas do acidente em estudo, mas também aquelas indiretas e outras sistêmicas. Esse nível de análise não é suportado pela abordagem tradicional de encadeamento de eventos falhos.

8 CONCLUSÃO

A proposta do presente trabalho é utilizar a abordagem STAMP para a análise de um acidente na aviação civil brasileira, em estudo de caso. Nesse sentido, este trabalho apresentou todo o desenvolvimento realizado, conforme o cronograma proposto.

A abordagem STAMP trata a falha de maneira sistêmica e complexa, como acontece na realidade, mas que em poucos casos é estudada. Neste contexto, o método CAST se apresenta como uma ferramenta eficaz na análise de falhas e na compreensão dos problemas nos diversos níveis do sistema em questão; características verificadas ao longo desse trabalho.

Os resultados obtidos apontaram grandes pontos de análise não explorados inicialmente pelo Relatório Final do Acidente em estudo. Este cenário indica que a análise CAST, baseada na abordagem STAMP, se apresenta como uma ferramenta eficaz na geração de recomendações de segurança na análise de acidentes. Além disso, esta abordagem pode ser utilizada como alternativa de complementação à análise de acidentes aeronáuticos já implementada pelos órgãos responsáveis no país.

Contudo, existem limitações quanto à generalização dos resultados encontrados. Realizar um maior número de estudos CAST com diferentes tipos e cenários de acidentes seria mais coerente com a ideia de generalização dos resultados, ao mesmo passo que seria impraticável por recursos de tempo e disponibilidade. Portanto, apesar da grande aplicabilidade evidenciada sobre a abordagem STAMP e a ferramenta CAST, o estudo apresenta a limitação de ser um estudo de caso.

AGRADECIMENTOS

Os autores agradecem à Fundação de Amparo à Pesquisa de Minas Gerais – FAPEMIG pelo suporte financeiro durante o desenvolvimento do trabalho.

Os autores agradecem também a Fernando Volkmer, Investigador de Acidentes Aeronáuticos do CENIPA e Consultor em Segurança Operacional, e também a João S. D. Garcia, Gerente de Normas Operacionais e Suporte da Superintendência de Padrões Operacionais da ANAC, pela grande contribuição durante a revisão do trabalho.

REFERÊNCIAS

ABDULKHALEQ, A; WAGNER, S. Open Tool Support for System-Theoretic Process Analysis. , 2014.

ABDULKHALEQ, A. XSTAMPP (An eXtensible STAMP Platform). 2015. Disponível em: <http://www.iste.uni-stuttgart.de/se/forschung/werkzeuge/xstampp.html>. Acesso em: 6 mar. 2016.

ANAC, A. N. DE A. C. Dados e Estatísticas - Acidentes. 2015. Disponível em: <http://www.anac.gov.br/Conteudo.aspx?slCD_ORIGEM=26&ttCD_CHAVE=178>. Acesso em: 1 aug. 2015.

ARNOLD, R. A qualitative comparative analysis of SOAM and STAMP in ATM occurrence investigation. 2009.MIT, 2009.

CENIPA, C. DE I. E P. DE A. A. MCA 3-3 - MANUAL DE PREVENÇÃO DO SIPAER. Brasília: MANUAL DE PREVENÇÃO DO SIPAER, 2012.

CENIPA, C. DE I. E P. DE A. A. RELATÓRIOS FINAIS / SUMAS - CENIPA. 2015. Disponível em: <http://www.cenipa.aer.mil.br/cenipa/paginas/relatorios/relatorios>. Acesso em: 2 aug. 2015. LEVESON, N. G. A new accident model for engineering safer systems. Safety Science, v. 42, n. 4, p. 237–270, Apr. 2004.

LEVESON, N. G. Engineering a safer world: Systems thinking applied to safety. Massachusetts: The MIT Press, 2011.

LIMA, I. J. Comparação Qualitativa entre as Metodologias SOAM e STAMP para a Análise de Acidentes Aeronáuticos na Operação Civil de Aeronaves no Brasil - Relatório Final. 2016.Universidade Federal de Itajubá - UNIFEI, Itajubá, 2016.

NELSON, P. A STAMP analysis of the LEX COMAIR 5191 accident. 2008.Lund University, Sweden, 2008.

ANEXO A

Figura 3 - EHCS Idealizada do Acidente de Interesse. (Fonte: o autor)