ASTROS 2020 - Um estudo de caso da análise multidisciplinar da segurança

Moisés da Silva Rodrigues[1] e Sidnei Barbieri[1]
[1]Instituto Tecnológico de Aeronáutica (ITA), São José dos Campos/SP – Brasil

***Resumo* – Sendo a segurança, caracterizada por suas dimensões *safety* e security, um requisito inerente a qualquer projeto de sistemas, verifica-se ser fundamental que a mesma seja sempre objeto de análise no gerenciamento de riscos, devendo estar presente desde as fases iniciais da concepção até um eventual descarte. Assim, o presente trabalho se propõe a apresentar algumas técnicas de análise de *safety*, com suas diferenças e similaridades, exemplificando sua aplicação, tendo, para isso, como objeto o Sistema de lançamento múltiplo de foguetes ASTROS 2020, atualmente em desenvolvimento no Brasil.**

Palavras-Chave* – safety, *ASTROS 2020, STPA

I. INTRODUÇÃO

Segurança, tanto *safety* quanto *security*, enquanto dimensão da qualidade, é algo que deve ser almejado em todos os sistemas. Entretanto, no caso de sistemas complexos, pode-se concluir que o esforço despendido na análise e definição de restrições de segurança pode ser muito elevado, sem que, contudo, haja quaisquer garantias quanto à sua completude. Obviamente, tal completude, se não impossível é algo improvável de ser alcançado; todavia a mesma deve, em todas as análises, ser um objetivo almejado.

Nesse contexto, é possível verificar que diversas técnicas de análise de *safety* e de security foram desenvolvidas, cada uma com seu próprio embasamento e visão, nenhuma, contudo, capaz de proporcionar a desejada completude da análise.

Tendo isto em mente, este artigo se propõe a apresentar uma análise baseada em múltiplas técnicas, na intenção de demonstrar a necessidade da aplicação de técnicas de *safety* diversas na busca da vislumbrada completude. Para tal, o objeto do presente estudo de caso será o Sistema lançador múltiplo de foguetes ASTROS 2020, em desenvolvimento pela empresa Avibrás.

Isto posto, a seção II apresenta conceitos básicos acerca de *safety* e suas metodologias para análise de *safety*. A seção III explica sobre o Projeto Estratégico do Exército (PEE) ASTROS 2020, enquanto que a seção IV apresenta uma visão geral de algumas técnicas de análise de *safety* que estão atualmente em voga no meio acadêmico. Já a seção V relata os resultados obtidos por meio da aplicação das técnicas descritas ao objeto de estudo. Por fim, a conclusão é apresentada n a seção VI.

II. SAFETY

"*Safety*" e "security" são termos que, ao serem traduzidas para o português, podem ser facilmente confundidos. A transcrição destas palavras para outros idiomas também gera este tipo de confusão como, por exemplo, na transcrição para o Norueguês, onde são recepcionadas pelo termo "*sikkerhet*".

Moisés da Silva Rodrigues, moises.s.rodrigues@gmail.com, +55-12-3947-6889, Sidnei Barbieri, sidneibarbieri@gmail.com,+55-12-3947-6889

Em consequência disto, a Norwegian University of Science and Technology – NTNU [1] propôs esclarecer os significados de ambos, a saber:

1) *Safety* é a proteção contra incidentes aleatórios. Incidentes aleatórios são incidentes indesejados que ocorrem como resultado de uma ou mais coincidências.

2) Security é a proteção contra incidentes pretendidos. Os incidentes de busca acontecem devido ao resultado de um ato deliberado e/ou planejado.

Security é uma condição onde se deseja proteção contra incidentes planejados, maliciosos e criminosos de uma ampla variedade de ameaças, onde o que está sendo protegido são todos os tipos de valores de uma organização ou indivíduo. Os incidentes acontecem em razão do desejo por um resultado, ou seja, como consequência das ações do atacante [1].

Por outro lado, *safety*, além de ser uma dimensão da qualidade, é um conceito relativo que corresponde a uma medida do grau de liberdade de "condições que podem causar morte, lesões, doenças ocupacionais, danos ou perdas em equipamentos ou propriedades" [2]. Assim, *safety* é considerada uma propriedade emergente que surge da interação dos componentes de um sistema.

A modelagem de acidentes, enquanto disciplina, tem por finalidade a busca da melhoria das condições de segurança e a redução de acidentes. Neste contexto, diversos modelos já foram apresentados, a maioria, contudo, baseada em relações causa-efeito e falhas de componentes individuais. Existem ainda outras abordagens como, por exemplo, o STAMP (*Systems-Theoretic Accident Model and Processes*), que tem como fundamento a teoria de sistemas. Por ela, os acidentes são considerados decorrentes das interações entre os seus componentes e, geralmente, não especificam variáveis ou fatores causais isolados. Portanto, também é possível considerar a teoria de sistemas como uma maneira útil de analisar acidentes, particularmente, em sistemas complexos [3].

Na concepção sistêmica de *safety*, os acidentes ocorrem quando perturbações externas, falhas de componentes ou interações incorretas entre eles não são adequadamente tratadas pelo sistema. Assim, podemos afirmar que acidentes são resultantes de descontroles ou controles insuficientes das restrições relacionadas com o desenvolvimento, projeto e operação de sistemas [3].

Uma vez estabelecidos quais são os acidentes possíveis e relevantes para um dado sistema, é possível identificar também quais são os *hazards*, ou seja, os eventos potencialmente perigosos que poderiam resultar nestes acidentes. Em sua obra, Levesson [4] assume que hazard é um estado do sistema ou conjunto específico de condições ambientais que podem conduzir a um ou mais acidentes, o que implica na associação direta entre *hazards* e acidentes.

ISSN:1983 7402

III. PEE ASTROS 2020

O Exército Brasileiro (EB), por meio da Portaria nº 134-EME, de 10 de setembro de 2012, implantou o Escritório de Projetos do Exército (EPEx), com responsabilidade sobre a coordenação dos Projetos Estratégicos do Exército (PEE) [5]. Dentre eles, destaca-se o PEE ASTROS 2020 que, em conformidade com as Diretrizes da Estratégia Nacional de Defesa [6], visa atender a uma demanda específica em termos estratégicos, que consiste em prover a Força Terrestre com meios de apoio de fogo de longo alcance, com alta precisão e letalidade, o que eleva a capacidade de dissuasão extrarregional, ao mesmo tempo em que moderniza os meios militares de Artilharia [7].

O EPEx faz a seguinte relação entre a capacidade de dissuasão e o projeto em tela:

"No Processo de Transformação em desenvolvimento no Exército, foram elencadas onze novas capacidades, destacando-se a dissuasão extrarregional, que se define como sendo a capacidade que tem uma Força Armada de dissuadir a concentração de forças hostis junto à fronteira terrestre e às águas jurisdicionais e a intenção de invadir o espaço aéreo nacional, possuindo produtos de defesa e tropas capazes de contribuir para essa dissuasão e, se for o caso, de neutralizar qualquer possível agressão ou ameaça, antes mesmo que elas aconteçam." [7].

O Sistema ASTROS 2020 (*Artillery Saturation Rocket System* ou, em português, Sistema de Artilharia de Foguetes para Saturação de Área) foi concebido e elaborado em parceria com a empresa brasileira Avibrás Indústria Aeroespacial S/A, sediada em São José dos Campos (SP). A grandiosidade deste projeto torna-se evidente quando verificamos a geração de mais de 7.700 empregos e o envolvimento de mais de 60 empresas, dentre elas, Imbel, Alcoa, Polaris, Siemens, Carrier, Metrohm, Flight Technologies, Advantec, Aero Digital Tecnologia Aerodesportiva, Bridgestone e Ellan, entre outras [8].

Ainda segundo informações do Escritório de Projetos do Exército (EPEx), o custo total de investimento previsto no PEE ASTROS 2020 é de R$ 1,4 bilhões. Somente para o ano de 2017, as emendas da Comissão de Relações Exteriores e Defesa Nacional (CRE), aprovadas em 19 de outubro de 2016, destinaram à implantação do Sistema de Defesa Estratégico ASTROS 2020, o valor de R$ 355,4 milhões [9]. Por outro lado, o ASTROS 2020 também possui apelo no mercado internacional, o que reduz a dependência de recursos do Governo Federal. Recentemente, o faturamento anual da Avibrás foi multiplicado em consequência do crescente volume de negócios envolvendo a venda de Sistemas da família Astros. Neste panorama, destacam-se como principais clientes internacionais: Arábia Saudita, Malásia, Indonésia, Iraque, Angola, entre outros [10].

Partindo das plataformas da nova viatura lançadora múltipla universal (MK-6), o sistema ASTROS 2020 possibilitará a utilização dos tradicionais foguetes da Família ASTROS, mas também do Míssil Tático AV-TM, com alcance de 300 km, movido a turbina, o qual está em fase final de desenvolvimento e certificação. Além disso, o sistema permitirá fazer toda a preparação para a realização do tiro, desde o recebimento e análise da missão de tiro, passando pelo comando e controle, pela trajetória de voo e finalizando com o controle de danos [11].

Com o PEE ASTROS 2020, o Exército Brasileiro irá adquirir um total de 49 viaturas, divididas em três Baterias, sendo 18 Lançadoras Múltiplas Universais (AV-LMU), 18 viaturas Remuniciadoras (AV-RMD), 3 Unidades de Controle de Fogos (AV-UCF), 3 Estações Meteorológicas Móveis (AV-MET), 3 Oficinas Móveis Combinadas (AV-OFVE), 3 viaturas do tipo Posto de Comando e Controle (AV-PCC) em nível Bateria, e um último, integrado, de Comando & Controle em nível Grupo/Batalhão (AV-VCC) [11].

O sincronismo do sistema ASTROS 2020 é garantido pela comunicação, em tempo real, via datalink. Ele permite o compartilhamento de mensagens de texto, voz e, principalmente, informações referentes ao tiro a ser executado. Portanto, as mensagens podem ser trocadas entre todas as viaturas do sistema de forma instantânea, protegidas por meio de transmissões criptografadas que utilizam Salto de Frequência [12].

Corroborando para a valorização de todo o arcabouço tecnológico envolvido na concepção do Sistema ASTROS 2020, o Comandante do Exército Brasileiro, em demonstração realizada no dia 10 de dezembro de 2015, no 6º Grupo de Mísseis e Foguetes (GMF), ressaltou a importância destas aquisições:

"Essas viaturas têm um componente tecnológico muito intenso incorporado e elas vêm fortalecer um aspecto muito importante da estrutura de Defesa, que é a capacidade de dissuasão. Poucos países do mundo possuem essa capacidade e isso nos coloca num patamar elevado e em um grupo bastante restrito" [13].

O sistema ASTROS 2020 pode desencadear, em curto espaço de tempo, uma massa de fogos capaz de saturar uma determinada área, causando danos grandes e, possivelmente, dispersos naquele raio de atuação. Desta forma, para minimizar este efeito dispersivo e favorecer o emprego em áreas restritas, diminuindo os danos colaterais e preservando a capacidade de saturação de área, está em desenvolvimento o Foguete SS-40 G (guiado), que é uma evolução do Foguete SS-40 convencional. Com este artefato, será possível economizar munição e oferecer maior segurança às tropas amigas, haja vista que ele reduz em cerca de 75% o valor da área de dispersão do modelo atual. Isto tudo é possível por meio da utilização de tecnologias capazes de corrigir sua trajetória durante o deslocamento [14].

Isto posto, a complexidade do PEE ASTROS 2020, somada aos riscos inerentes aos produtos de aplicação militar, os vultosos recursos envolvidos e a grande preocupação para com segurança das tropas amigas, a preocupação com aspectos de *safety* é, notadamente, necessária e constante. Desta forma, elegemos o Sistema ASTROS 2020 como objeto de um estudo de caso acadêmico.

No início deste ano, o jornal O Globo [15] publicou a seguinte matéria: "A ONG Human Rights Watch denunciou que as forças da coalizão militar liderada pela Arábia Saudita no Iêmen dispararam foguetes de munição cluster (de fragmentação) de fabricação brasileira num ataque que feriu dois meninos. A ONG pró-direitos humanos relatou que os projéteis, que são banidos internacionalmente, atingiram uma fazenda no Norte do Iêmen no final de fevereiro.".

Além disso, em maio de 2015 a agência de notícias G1 [16] noticiou que a ignição acidental durante a manutenção de um foguete utilizado para artilharia de médio e longo alcance (Foguete SS-30) feriu funcionários da Avibrás: "Três homens ficaram feridos, um deles em estado grave, em um

ISSN:1983 7402

acidente na noite desta quarta-feira (14) na unidade da Avibrás em Jacareí (SP). Segundo o Sindicato dos Metalúrgicos, um foguete de artilharia produzido na unidade teria entrado em ignição e acabou ferindo os trabalhadores."

Outras reportagens, disponíveis em fontes abertas, são facilmente localizadas por meio de sites de busca como, por exemplo, Google, Yahoo, entre outros. Entretanto, essas duas matérias são suficientes para ilustrar alguns dos *hazards* relacionados ao desenvolvimento e à operação de Sistemas ASTROS 2020. Ainda que possa haver interesse na eliminação de uma tropa inimiga, é indiscutível que a preservação da vida de civis é prioritária. Neste sentido, devem ser utilizados modelos e técnicas de *safety* que consigam reduzir ao máximo eventuais *hazards*.

IV. TÉCNICAS DE ANÁLISE DE SAFETY

Segundo Ericson [17], as técnicas de análise de *hazards* no contexto de *safety* podem ser agrupadas em indutivas e dedutivas. Enquanto técnicas indutivas, como *Event Tree Analysis* (ETA) [18] e *Failure Modes and Effects Analysis* (FMEA) [19], partem de uma determinada falha para identificar as potenciais consequências para o sistema, técnicas dedutivas, como *Fault Tree Analysis* (FTA) [20], buscam identificar fatores causais para justificar a ocorrência de *hazards*. Outras como, por exemplo, o *Hazard and Operability* (HAZOP) [21] podem assumir, simultaneamente, características indutivas e dedutivas.

Em termos práticos, verifica-se que ambas as categorias são complementares no que concerne à sua aplicabilidade, senão, vejamos: enquanto técnicas indutivas tem como ponto de partida elementos individuais do sistema, o que possibilita uma análise detalhada de pontos considerados críticos, técnicas dedutivas favorecem uma visão sistêmica, na medida que possibilitam identificar de forma ampla potenciais fontes de *hazards* a partir de uma análise de alto nível. Nos parágrafos a seguir serão apresentadas as técnicas abordadas no presente trabalho, de maneira a favorecer a compreensão acerca da análise realizada.

O *Failure Modes And Effects Analysis* (FMEA) [19], técnica indutiva desenvolvida para aplicação em partes físicas, tem como proposta o estudo dos resultados da ocorrência de falhas individuais de componentes de um sistema. Para cada componente, são identificados diferentes modos de falha, a partir dos quais busca-se caracterizar as potenciais consequências para o sistema, classificando-se conforme a severidade, sendo os resultados apresentados na forma tabular.

Diametralmente oposto ao FMEA, considerando sua linha de raciocínio dedutiva, o *Fault Tree Analysis* (FTA) [20] provê um método lógico para apresentar de forma gráfica cadeias de eventos que poderiam conduzir a falhas do sistema. Tal metodologia se mostra particularmente útil na medida que propicia a determinação de probabilidades, o que pode ser obtido matematicamente.

Mantendo, ainda, o raciocínio comparativo entre técnicas indutivas e dedutivas cabe aqui apresentar o *Hazard and Operability* (HAZOP) [21], que reúne características dos dois grupos. De acordo com Brown [22], o HAZOP é uma das técnicas mais importantes utilizadas na identificação de *hazards*. Devido ao seu caráter bem estruturado e sistemático, ele é capaz de atuar com eficácia na detecção de consequências adversas associadas a riscos de processos. O método é tabular, à semelhança do FMEA, e utiliza palavras-guia combinadas com parâmetros de processos, buscando de forma indutiva e dedutiva encontrar possíveis desvios das intenções de projeto ou de operabilidade do sistema.

Neste mesmo contexto, destaca-se o *System-Theoretic Process Analysis* (STPA), técnica dedutiva para análise de *hazards* derivada do *Systems-Theoretic Accident Model and Processes* (STAMP). O STAMP [4] é um modelo de acidentes baseado na teoria dos sistemas que é construído sobre três conceitos básicos: restrições de segurança, estruturas hierárquicas de controle de *safety* e modelos de processos. Ao contrário da visão apresentada por diversos outros modelos de acidentes, segundo Leveson [4], no STAMP, *safety* é uma propriedade emergente dos sistemas, alcançada como consequência de restrições adequadas aplicadas sobre o comportamento do sistema e de seus componentes. Assim, o gerenciamento de *safety* não é realizado na forma de prevenção de falhas de componentes, mas como a criação de uma estrutura de fortalecimento de restrições de *safety*, de forma contínua e efetiva.

O STAMP, assim como outros modelos de acidentes baseados em sistemas, se contrapõe aos modelos baseados em falhas. Em modelos de acidentes baseados em falhas, conforme afirmado por Leveson [23], *hazards* são sempre decorrentes de alguma falha, seja de um componente, seja de erro humano ou, ainda, de um evento relacionado a liberação de energia, visão que proporciona uma noção limitada de causalidade, dificultando a incorporação de relações não lineares, como, por exemplo, o *feedback*. O STAMP, por outro lado, proporciona uma visão mais ampla, considerando em sua análise outros fatores, como fatores organizacionais e sociais, interações entre componentes, as quais podem inserir problemas inexistentes quando considerado cada componente de forma individual e outras propriedades emergentes. Desse modo, verifica-se que o STAMP é capaz de identificar *hazards* de todas as categorias apresentadas por Ericson [17]: funcionais, sistêmicos, operacionais, relacionados à saúde do sistema, relacionados a testes, relacionados ao software e relacionados ao operador.

Enquanto o STAMP é um modelo de acidentes que suporta a visão sistêmica de *safety*, a técnica STPA, segundo Thomas [24], aplica essa visão por meio de um processo de duas etapas, denominadas *steps*: o *step* 1, que consiste em identificar, para o sistema sob análise, as potenciais ações de controle inseguras; e o *step* 2, que consiste em examinar o loop de controle de *safety*, visando identificar potenciais fatores causais que possam originar ações de controle inseguras ou, ainda, a violação de restrições de segurança.

Além do STPA, outras técnicas, como o STPA-Sec [25] e o STPA-SafeSec [26], apresentam aplicações do STAMP para sistemas complexos, essas últimas estendendo a funcionalidade daquela para além da finalidade primeira de *safety*, incluindo a análise de security, o que possibilita sua aplicação até em contextos de possíveis guerras cibernéticas, o que é especialmente útil em se tratando de projetos de armas militares

Apesar da grande amplitude da análise de *hazards* proporcionada pelo STPA ou suas afins, verifica-se, contudo, que a completude não pode ser garantida mediante a aplicação de uma única técnica, conforme afirmado por Ericson [17]. Assim a recomendação é que sejam aplicadas diversas técnicas em conjunto, visando à complementaridade entre elas, o que proporcionará uma análise mais ampla e completa.

V. RELATO DA ANÁLISE ACADÊMICA DE SAFETY DO SISTEMA ASTROS 2020

No intuito de ilustrar a necessidade da adoção de técnicas diversas na busca da completude, foi realizada uma análise acadêmica de *safety* do Sistema ASTROS 2020, baseada principalmente na técnica STPA, corroborada por outras técnicas de análise de *hazards*.

Na aplicação do STPA, seguindo as etapas apresentadas por Thomas [24], inicialmente foi realizada a modelagem do sistema, composta pela definição dos objetivos dos sistema, de acidentes, de *hazards* a nível de sistema, da estrutura de controle funcional e do loop de controle de *safety*. Nesse contexto, foram identificados os seguintes objetivos primários do sistema: G-1: executar tiros precisos; G-2: lançar múltiplas munições de forma orquestrada; G-3: controlar os níveis de destruição; e G-4: preservar a segurança da tropa.

Segundo Thomas [24], acidentes em geral envolvem perdas de vidas humanas ou danos, podendo, todavia, incluir quaisquer perda inaceitável que possa ser prevenida. Com base nessa definição, bem como nos objetivos apresentados, foram identificados os seguintes acidentes relacionados ao sistema ASTROS 2020: A-1: os fogos lançados não alcançam o objetivo previsto (alvos/áreas); e A-3: explosão de ogiva dentro ou próxima à LMU.

Tendo os acidentes definidos, a tarefa seguinte foi a realização de uma exercício mental para a dedução de *hazards* que levassem a tais acidentes, tendo sido obtidos os seguintes resultados: H-1: emissão de fogos sem orientação; H-2: alteração da trajetória após o lançamento dos fogos; H-3: comunicação dessincronizada entre o PCC e os diversos LMUs; H-4: lançamento com munições inadequadas; H-5: execução de tiros com LMUs descalibrados; H-6: LMUs não obedecem às ordens do PCC; e H-7: identificação (pelo foguete) de ordem para autodestruição antes do lançamento.

A definição dos supramencionados *hazard*s possibilitou, de imediato, identificar restrições de *safety* a nível de sistema, a fim de impedir que, em algum momento, se caracterizassem os referidos *hazard*s, a saber: SSC-1: a emissão de fogos antes que seja garantida a devida orientação; SSC-2: deve ser garantida a manutenção da trajetória prevista após o lançamento dos fogos; SSC-3: deve ser garantido o sincronismo da comunicação entre o PCC e as diversos LMUs; SSC-4: deve ser garantido o lançamento de munições compatíveis com a missão; SSC-5: deve ser garantida a calibragem das LMUs antes da execução do tiro; SSC-6: deve ser garantida a estrita obediência das LMUs às ordens do PCC; e SSC-7: deve ser garantida que a capacidade de identificação (pelo foguete) de ordens para autodestruição esteja disponível somente após seu lançamento.

A tarefa que se seguiu à definição das restrições de segurança a nível de sistema foi a caracterização da estrutura de controle do sistema, a qual é apresentada a seguir em dois níveis: estrutura hierárquica de controle, conforme a Fig. 1, a qual denota a estrutura de controle em alto nível, tanto do ponto de vista do desenvolvimento quanto da operação, e estrutura de controle funcional, conforme a Fig. 2, que apresenta a interação, em alto nível de abstração, entre os componentes internos do sistema: Viatura AV-PCC (Comando e Controle do sistema ASTROS 2020), Viatura AV-UCF (Diretora de Tiros), Viatura AV-LMU (Lançadoras Múltipla Universal), Viatura AV-RMD (Remuniciadora) e Viatura AV-MET (Meteorológica).

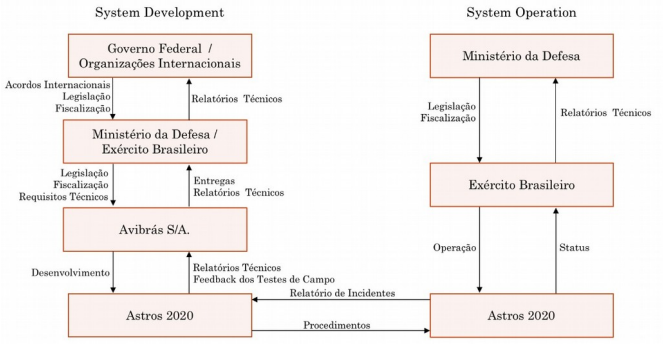

Fig. 1: Estrutura hierárquica de controle do sistema ASTROS 2020.

Ambas as estruturas de controle apresentadas são de grande relevância para a análise, não se podendo prescindir de uma ou de outra. Através da estrutura hierárquica, entre outros aspectos, foi possível identificar as responsabilidades relativas à regulamentação e às decisões de projeto ou decisões relativas à aplicação do sistema. Já na estrutura de controle funcional foi possível identificar as ações de controle entre os diversos componentes, o que, em última análise, permitiu realizar a verificação do loop de controle de *safety*, o que, além do referido loop, se valeu das variáveis de controle, identificáveis somente mediante a definição da estrutura de controle funcional.

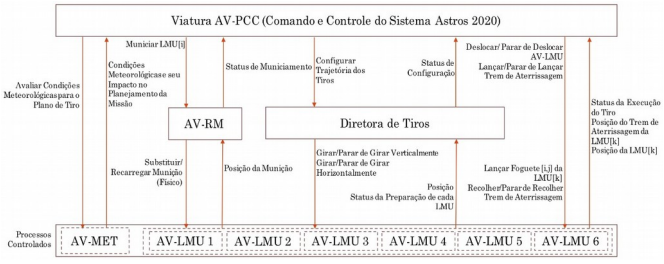

Fig. 2: Estrutura funcional de controle do sistema ASTROS 2020.

Uma vez concluída a modelagem do sistema, foi realizado o *step* 1 da análise STPA, a saber, a identificação de ações de controle inseguras, mediante a análise de cada uma das ações de controle definidas na estrutura de controle funcional. Para cada uma das ações de controle, verificou-se em quais contextos elas poderiam levar a ações de controle inseguras caso: não fossem providas quando se fizessem necessárias; fossem providas em situações inadequadas; fossem providas na ordem errada ou em momento inoportuno; ou fossem providas por mais ou menos tempo que o necessário, em se tratando de ações de controle não discretas no domínio do tempo. Exemplificando os resultados obtidos, a Tabela I apresenta algumas ações de controle que poderiam conduzir ao hazard “H-1: emissão de fogos sem orientação”.

TABELA I: ANÁLISE DE AÇÕES DE CONTROLE RELACIONADAS AO HAZARD H-1

Control Action	Controller / Actuator	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing / Order of Causes Hazard	Stopped Too Soon or Applied Too Long
Parar de Deslocar AV-LMU	AV-PCC	NA	NA	NA	NA
Lançar Trem de Aterrissagem	AV-PCC	AV-PCC Não Provê Lançar Trem de Aterrissagem quando em posição de tiro	NA	AV-PCC Provê Lançar Trem de Aterrissagem antes da LMU estar na posição	AV-PCC para de prover Lançar Trem de Aterrissagem antes da LMU alcançar estabilidade
Parar de Lançar Trem de Aterrissagem	AV-PCC	AV-PCC Não Provê Parar de Lançar Trem de Aterrissagem após a LMU alcançar estabilidade	NA	AV-PCC Provê Parar de Lançar Trem de Aterrissagem antes da LMU alcançar estabilidade	NA
Lançar Foguete [i,j] da LMU[k]	AV-PCC	NA	NA	NA	NA
Recolher Trem de Aterrissagem	AV-PCC	NA	AV-PCC Provê Recolher Trem de Aterrissagem durante o tiro	AV-PCC Provê Recolher Trem de Aterrissagem antes da execução do tiro	NA

Os resultados da tarefa de identificação de ações de controle inseguras, além de servirem de argumento para a etapa seguinte, possibilitaram a definição de novas restrições de *safety*, algumas delas apresentadas na Tabela II, concluindo as tarefas atinentes ao *step* 1.

TABELA II: RESTRIÇÕES DE SAFETY DECORRENTES DE AÇÕES DE CONTROLE INSEGURAS

Unsafe Control Actions	Safety Constraints
AV-PCC Não Provê Configurar Trajetória dos Tiros quando há tiro a ser executado	Not Provided: Quando há tiro a ser executado AV-PCC deve prover Configurar Trajetória dos Tiros
AV-PCC Provê Configurar Trajetória dos Tiros somente depois de Executar o tiro	Wrong Timing or Order: O Tiro somente deve ser executado após AV-PCC Prover Configurar Trajetória dos Tiros
AV-PCC para de prover Configurar Trajetória dos Tiros antes que a LMU esteja na posição prevista para o tiro	Stopped Too Soon or Applied Too Long: enquanto a LMU não estiver na posição prevista para o tiro AV-PCC não deve parar de prover Configurar Trajetória dos Tiros
AV-PCC Não Provê Lançar Trem de Aterrissagem quando a LMU está na posição de tiro	Not Provided: Quando a LMU alcançar a posição de tiro AV-PCC Não Prover lançar Trem de Aterrisagem
AV-PCC Provê Lançar Trem de Aterrissagem antes da LMU estar na posição	Wrong Timing or Order: Antes da LMU alcançar a posição de tiro AV-PCC não Prover Lançar Trem de Aterrisagem

Uma vez concluída a identificação de ações de controle inseguras, teve início o *step* 2 da análise STPA, ou seja, a identificação dos fatores causais que poderiam conduzir às referidas ações de controle inseguras. Para tanto, fez-se uso de questões e palavras guia, visando classificar tais ações segundo 3 tipos de cenário: 1) quando uma ação de controle para *safety* é provida porém não é seguida ou não é executada adequadamente; 2) quando uma ação de controle insegura é provida; ou 3) quando uma ação de controle para *safety* não é provida, ainda que requerida, ou é provida de forma inadequada (cedo ou tarde demais ou em ordem errada). Neste momento verificou-se na prática a utilidade do loop de controle de *safety*, conforme apresentado de forma genérica na Fig. 3, podendo, todavia, ser adaptado conforme o contexto específico.

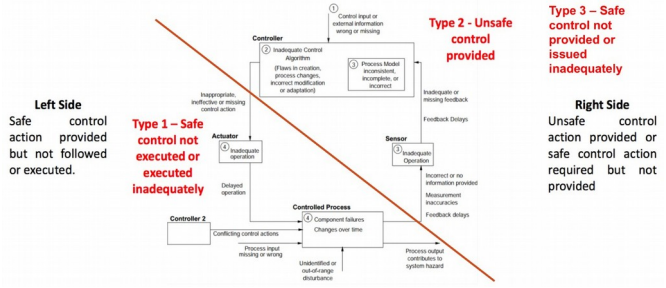

Fig. 3: Loop de controle de *safety* genérico, para *step* 2 do STPA.

A execução do *step* 2 proporcionou a identificação de diversos cenários, como os apresentados na III, que respondem à Pergunta guia "Quais fatores causais levam a LMU a não seguir a ação de controle Rotacionar provida pela Diretora de Tiros quando há lançamento a ser executado?".

Desse modo, verificou-se que potenciais fontes de *hazards*, mediante a adequada aplicação do STPA, poderiam ser caracterizadas ainda nas fases iniciais do projeto, garantindo que o desenvolvimento do projeto fosse, concomitantemente, baseado em *safety* e *security*.

Conforme já apresentado na seção Tabela III, Ericson [17] afirma que a completude da análise de *hazards* não pode ser garantida mediante a aplicação de uma única técnica. Em consequência, outras técnicas foram selecionadas para aplicação neste estudo de caso acadêmico, na intenção de buscar possíveis *hazards* não identificados durante a realização da análise STPA.

TABELA III: CENÁRIOS DECORRENTES DO STEP 2 DA ANÁLISE STPA

Scenario	Associated Causal factor	Requirement	Allocated to	Rationale
[Control Action perdida] Control Action provida pela Diretora de Tiros não chega à LMU	Problemas no canal de comunicação (DATALINK)	Deve-se garantir a disponibilidade do DATALINK durante a operação	Engenheiros	Podem ser desenvolvidos canais redundantes para o tráfego de dados
[Control Actions Conflitantes] LMU recebe control action para não rotacionar	Control Action decorrente de Ataque cibernético	Deve-se garantir a integridade da comunicação entre a Diretora de Tiro e a LMU	Engenheiros	Recomenda-se utilização de criptografia do canal

A primeira técnica complementar selecionada foi o FMEA [19]. Considerando que uma das características do FMEA é sua capacidade de gerar grandes quantidades de dados de saída, o que poderia dificultar a análise, optou-se por aplicá-lo apenas à algumas partes do sistema, a exemplo do sensor de elevação da LMU, cujos resultados parciais são apresentados na Tabela IV.

TABELA IV: RESULTADOS DA ANÁLISE FMEA

Função	Modo de falha e efeito a) perda da funcionalidade b) função provida quando não requerida c) Função incorreta	Severidade	Justificativas / comentários
Lançamento eletrônico do Trem de Aterrisagem	a) sem lançamento	Minor	O lançamento pode ser realizado de forma manual
	b) Lançamento quando a LMU está pronta para o tiro	Catastrophic	Poderá ocorrer um disparo sem direção
	c) Lançamento continua mesmo após a LMU atingir a estabilidade	Hazardous	A instabilidade, se percebida, poderá ser corrigida
Identificação de alvos pelo Radar da Diretora de Tiros	a) radar incapaz de identificar alvos	Minor	A direção de tiro pode se basear em um plano oriundo do escalão superior
	b) Busca de alvos sem requisição	Negligible	
	c) identificação de alvo em posição errada	Catastrophic	

Em seguida, optou-se pela aplicação de uma técnica dedutiva para complementação da visão apresentada pelo FMEA, a saber, o FTA. Aplicada ao *hazard* "A LMU não atende ordem emitida pelo PCC para direcionamento, também abordada na análise STPA, verificou-se que, ainda que por outros caminhos, foram identificadas fontes semelhantes para o *hazard* considerado, conforme apresentado na Fig. 4.

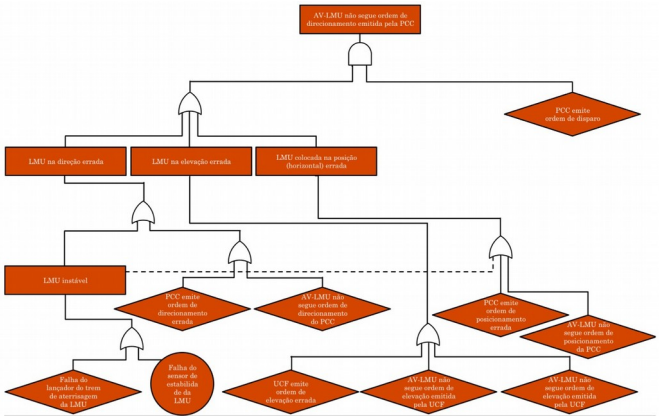

Fig. 4: Resultado da Análise FTA parcial.

Por fim, foi aplicada a técnica HAZOP, a qual, por seu raciocínio ao mesmo tempo indutivo e dedutivo, possibilitou identificar tanto causas quanto consequências de potenciais desvios de design, tendo como objeto principal de análise o datalink. Os resultados da referida análise são apresentados na Tabela V.

TABELA V: RESULTADO DA ANÁLISE HAZOP

Guide Word	Deviation	Possible Causes	Consequences	Action Required
NO or NONE	Mensagem não chega ao destino	1) Falha no equipamento 2) Interferência intencional (Guerra Eletrônica)	Perda da comunicação entre subsistemas fracamente acoplados	1) Reparar equipamento 2) Remover a fonte de interferência
MORE	Não há confirmação do recebimento da mensagem	Falha no equipamento receptor	Perda da comunicação entre subsistemas fracamente acoplados	Reparar equipamento
LESS	A comunicação não é efetiva	1) Falha no equipamento transmissor 2) Equipamento fora do alcance útil	Perda do controle sobre subsistemas fracamente acoplados Controle parcial sobre subsistemas fracamente	1) Reparar equipamento 2) Reposicionar viaturas
PART OF	Mensagens não são inteligíveis para os equipamentos	Problemas no protocolo de comunicação	Perda de capacidade de configuração de recursos	Corrigir protocolo
OTHER THAN	Informações redundantes divergentes	Falha de sensores	Interrupção ou execução parcial da missão	Gerar alerta para operador
EARLY	NA	NA	NA	NA
LATE	Atraso no recebimento da mensagem	Baixa Prioridade ou Interferências diversas	Execução tardia de comandos	Calcular ajuste de tempo para sincronização dos recursos

Conforme previsto, a aplicação de diferentes técnicas, quer pela abrangência, quer por sua abrangência, produziu resultados em grande parte diversos, contudo complementares. Desse modo, verificou-se a importância de se considerar técnicas variadas desde as fases preliminares de um projeto, de maneira a identificar *hazards* o mais cedo possível, reduzindo riscos e custos.

VI. CONCLUSÃO

Mais que simplesmente apresentar diferentes técnicas de análise de *safety*, o presente trabalho procurou ressaltar a importância de sua aplicação em contextos variados, desde as fases preliminares de um projeto, como parte do gerenciamento de riscos, tanto os relacionados a *safety* quanto a *security*.

Nesse contexto, o sistema ASTROS 2020, objeto deste estudo de caso, possui importância estratégica e elevado investimento financeiro. A severidade dos riscos associados, demonstrou a necessidade de uma análise multidisciplinar e sistêmica, percorrendo diferentes métodos, técnicas e ferramentas em prol da análise de riscos mais completa para as diversas perspectivas.

Com efeito, pudemos constatar que a completude sob a ótica da *safety* e da security, não pode ser alcançada senão pela aplicação de um diversificado conjunto metodológico, o que deve ser realizado de forma cíclica e incremental, conforme a evolução do projeto.

REFERÊNCIAS

[1] E. Albrechtsen. 2002. A generic comparison of industrial *safety* and information security. Term paper in the PhD course "Risk an Vulnerability", NTNU. December 2002.

[2] Department of Defense. Standard MIL-STD-882B – System Safety Program Requirements. 1984.

[3] J. Leplat. Occupational accident research and systems approach in Rasmussen, J., Duncan, K. & Jacques Leplat, J. (Eds.), New Technology and Human Error, p.181-191, New York: John Wiley & Sons, 1987.

[4] N. G. Leveson. “Engineering a safer world: systems thinking applied to *safety*”, Massachusetts Institute of Technology, 2011, p. 76.

[5] T. S. Ramalho. Processo de Inovação no Setor de Defesa: Um Estudo no Exército Brasileiro. Dissertação apresentada ao curso de mestrado profissional, na área de Gestão de Negócios, do programa de pós-graduação stricto sensu em administração de empresas da Faculdade Instituto de Administração. São Paulo, 2017.

[6] Brasil. Decreto nº 6.703, de 18 de dezembro de 2008. Aprova a Estratégia Nacional de Defesa, e dá outras providências. Ministério da Defesa - MD; Secretaria de Assuntos Estratégicos da Presidência da República - SAE-PR. D.O.U. DE 19/12/2008, P. 4.

[7] Escritório de Projetos do Exército (EPEx). “ASTROS 2020: Alcance - Precisão – Poder”. Disponível em: < http://www.epex.eb.mil.br/index.php/astros-2020>. 2014. Acesso em 10 de julho de 2017.

[8] W. M. Ramos; L. R. F. Goldoni. "Os Projetos do Exército Brasileiro e o alinhamento com as diretrizes da Estratégia Nacional de Defesa." Revista Política Hoje-ISSN: 0104-7094 25.1 (2016): 153-175.

[9] R. Godoy. Avibrás planeja faturar R$ 1,3 bilhão neste ano. [26 de janeiro, 2016]. Matéria publicada na Revista EXAME.com. São Paulo, 2016. Disponível em: http://exame.abril.com.br/ciencia/com-mercado-externo-forte-avibras-planeja-faturar-r-1-3-bilhao-neste-ano/.

[10] Senado Notícias. CRE e CDH aprovam emendas ao Orçamento 2017. Disponível em: < http://www12.senado.leg.br/noticias/materias/2016/10/19/cre-e-cdh-aprovam-emendas-ao-orcamento-2017>. 2016. Acesso em 10 de julho de 2017.

[11] M. F. G. Viana. Os Projetos Estratégicos do Exército Brasileiro e suas contribuições para a implementação da Política Nacional de Defesa. Trabalho de Conclusão do Curso apresentado à Escola de Comando e Estado-Maior do Exército, como requisito parcial para a obtenção do título de Especialista em Ciências Militares. Escola de Comando e Estado Maior do Exército/ Escola Marechal Castello Branco. Rio de Janeiro, 2014.

[12] Portal Defesa. As novas garras dos Fuzileiros Navais – UPDATE. Matéria publicada na agência de notícias Portal Defesa, em 3 de outubro de 2014. Disponível em: <http://portaldefesa.com/3459-as-novas-garras-dos-fuzileiros-navais-update/>. 2016. Acesso em 10 de julho de 2017.

[13] L. Barreto. Ministério da Defesa. Exército Brasileiro recebe nove viaturas lança mísseis ASTROS. Disponível em: <http://www.defesa.gov.br/noticias/17732-exercito-brasileiro-recebe-nove-viaturas-antimisseis-astros>. Acesso em 10 de julho de 2017.

[14] Departamento de Ciência e Tecnologia (DCT). Astros 2020 - Projeto Estratégico do Exército. Disponível em: <http://www.dct.eb.mil.br/index.php/component/content/article?id=136:astros-2020>. Acesso em 10 de julho de 2017.

[15] O Globo. Banidas mundialmente, munições brasileiras ferem crianças no Iêmen, denuncia HRW. Matéria publicada na agência de notícias O Globo, em 17 de março de 2017. Disponível em: < https://oglobo.globo.com/mundo/banidas-mundialmente-municoes-brasileiras-ferem-criancas-no-iemen-denuncia-hrw-21073048>. Acesso em 10 de julho de 2017.

[16] G1. Acidente com foguete deixa três feridos na Avibras em Jacareí, SP. Matéria publicada na agência de notícias G1, em 14 de maio de 2015. Disponível em: <http://g1.globo.com/sp/vale-do-paraiba-regiao/noticia/2015/05/acidente-com-foguete-deixa-tres-feridos-na-avibras-em-jacarei-sp.html>. Acesso em 10 de julho de 2017.

[17] C. A. Ericson, “Hazard analysis techniques for system *safety*”, 2ed., Jonh Wiley & Sons, Inc., New Jersey, 2016, p. 63-65, 82-83, 383-386.

[18] Hong E.-S., Lee I.-M., Shin H.-S., Nam S.-W., Kong J.-S. , “Quantitative risk evaluation based on event tree analysis technique: Application to the design of shield TBM”, Tunnelling and Underground Space Technology 24, 2009, pp. 269-277.

[19] United States Department of Defense, MIL-STD-1629A - Procedures for performing a failure mode effect and criticality analysis, 24 November 1980.

[20] W. F. Larsen, “Technical Report 4556 - Fault Tree Analysis”, U.S. Army Picatinny Arsenal, Dover, New Jersey, 1974.

[21] J. Dunjó et al, “Hazard and operability (HAZOP) analysis. A literature review.” Journal of Hazardous Materials, n. 173, 2010”

[22] A. Brown, “Análise de Risco. Boletim Técnico da GSI”, Grupo de Pesquisa em Segurança contra Incêndio do Núcleo de Pesquisa em Tecnologia da Arquitetura e do Urbanismo da Universidade de São Paulo – GSI/NUTAU/USP. Ano III, no1, janeiro- fevereiro/1998. Disponível em: <http://www.lmc.ep.usp.br/grupos/gsi/wp-content/boletim/3-1.pdf>, Acessado em 10 de julho de 2017.

[23] N. Leveson, “A new accident model for engineering safer systems”, Safety Science, Vol. 42, No. 4, April 2004, pp. 237-270.

[24] J. Thomas, “Extending and automating a systems-theoretic hazard analysis for requirements generation and analysis”, Doctorate Thesis, Massachusetts Institute of Technology, 2013, p. 64-69.

[25] W. Young, N. G. Leveson, “An integrated approach to *safety* and security based on systems theory”, Communications of the ACM Journal, 2014, p. 31-35.

[26] I. Friedberg, K. Mclaughlin, P. Smith, D. Laverty, S. Sezer, “STPA-SafeSec: *safety* and security analysis for cyber-physical systems”, Journal of Information Security and Applications, 2017.