Considerações sobre Proteção e Segurança da Informação de Sistemas da Aeronave

Rafaela Patti Caillaux [1], Rodrigo Valério Magalhães [2]

1 Mestre em Segurança da Aviação e Aeronavegabilidade de Aeronaves
2 Mestre em Engenharia Aeronáutica

RESUMO: Atualmente as aeronaves operam num ambiente extremamente integrado e conectadas a diversas redes, permitindo comunicações em solo e em voo com o controle de tráfego aéreo, operadores aéreos e provedores de serviços de navegação aérea. O uso de novas tecnologias nos sistemas aeronáuticos permitiu que as aeronaves realizassem operações mais precisas e otimizadas aumentando também a eficiência na manutenção. Se por um lado isso aumentou o nível de segurança da aviação civil, a maior conectividade e o uso de equipamentos e padrões abertos não aeronáuticos criaram novas ameaças que podem representar oportunidades para ataques cibernéticos[1]. Essas novas ameaças precisam ser identificadas e devidamente tratadas. A Proteção e Segurança da Informação de Sistemas da Aeronave *(Aircraft Systems Information Security/Protection – ASISP)* versa sobre como a aeronave deve ser protegida contra ataques cibernéticos com potencial de resultar num evento de segurança *(safety event)*. Apesar de este assunto estar sendo discutido pelas autoridades de aviação civil em conjunto com a indústria há mais de uma década, ainda não há requisitos de aviação civil publicados. Há um bom alinhamento quanto às bases do processo a ser utilizado na análise de segurança da informação *(information security)*, porém ainda não há consenso com relação ao método a ser utilizado. Dessa forma, as autoridades têm tratado esse assunto caso a caso, estabelecendo requisitos mínimos de certificação para os requerentes através de Condições Especiais. Esse artigo tem por objetivo mostrar como a proteção da aeronave contra ataques cibernéticos está sendo tratada pelas principais autoridades de aviação civil e discutir as metodologias de análise de segurança da informação propostas pela organização europeia *European Organization for Civil Aviation*, EUROCAE e pela organização americana *Radio Technical Commission for Aeronautics*, RTCA. É de vital importância que as discussões avancem no sentido de se estabelecer requisitos mínimos de certificação, bem como desenvolver meios aceitáveis de cumprimento, harmonizados internacionalmente, que possam ser utilizados pela comunidade da aviação civil.

Palavras chave: Segurança da Informação, S*ecurity*, ASISP, Ataques Cibernéticos, Ameaças, Proteção de Sistemas.

Considerations on Protection and Security of Aircraft Information Systems

ABSTRACT: Nowadays, aircraft operate in an extremely integrated environment and are connected to various networks, air traffic control, air operators and air navigation service providers. The utilization of new technologies in the aeronautical systems allowed aircraft to perform more precise and optimized operations, and maintenance efficiency was also increased. While, on the one hand, this has increased the level of civil aviation safety, the higher level of connectivity and the use of non-aeronautical equipment and open standards have created new threats that may represent opportunities for cyberattacks1. These new threats need to be identified and treated accordingly. Aircraft Systems Information Security / Protection (ASISP) addresses the subject of how an aircraft should be protected against cyber-attacks with potential to result in a safety event. Although this subject has been discussed by civil aviation authorities in conjunction with the industry for more than a decade, no civil aviation requirements have been published yet. There is good alignment of thoughts regarding the bases of the process to be used in the analysis of information security, but no consensus has so far been achieved with regards to the method to be used. So, authorities have dealt with the matter on a case-by-case basis, establishing minimum certification requirements for applicants by means of Special Conditions. This article aims to show how the aircraft protection against cyber-attacks is being treated by the main civil aviation authorities, and to discuss the methodologies for analysis of information security proposed by the European Organization for Civil Aviation (EUROCAE) and by the American organization Radio Technical Commission for Aeronautics (RTCA). It is vitally important that the discussions move towards establishing minimum certification requirements and developing acceptable, internationally harmonized means of compliance that can be used by the civil aviation community.

Key words: Information Security, Security, ASISP, Cyber-Attacks, Threats, System Protection.

Citação: Caillaux, RP, Magalhães, RV. (2016) Considerações sobre Proteção e Segurança da Informação de Sistemas da Aeronave. *Revista Conexão Sipaer*, Vol. 7, No. 1, pp. 116-126.

1 BIOGRAFIA

Rafaela Patti Caillaux

Mestre em Segurança da Aviação e Aeronavegabilidade de Aeronaves pela *L'Ecole Nationale de l'Aviation Civile, ENAC* (2015), Mestre em Planejamento Energético, pelo Instituto Alberto Luiz Coimbra de Pós-Graduação e Pesquisa de Engenharia, COPPE (2003), Especializada em Engenharia Aeronáutica pela EMBRAER (2001) e graduada em Engenharia Civil pela Universidade Federal do Rio de Janeiro (1999). Atualmente é Especialista em Regulação de Aviação Civil na ANAC e trabalha na coordenação de projetos de

[1] Ataques cibernéticos são feitos através de uma ação eletrônica mal intencionada.

certificação de produtos aeronáuticos e no desenvolvimento de processo e regulação específicos para a Certificação de Organizações de Projeto no Brasil. Na iniciativa privada, trabalhou na Embraer com desenvolvimento de interiores e sistemas, em diferentes produtos da aviação executiva.

Rodrigo Valério Magalhães

Mestre em Engenharia Aeronáutica pelo Instituto Tecnológico de Aeronáutica (2010). Possui especialização em Projeto de Circuitos Integrados pela Universidade Federal de Minas Gerais (2008) e é graduado em Engenharia Elétrica também pela Universidade Federal de Minas Gerais (2006). Trabalhou na Embraer na área de estudos preliminares e atualmente é Especialista em Regulação de Aviação Civil na Agência Nacional de Aviação Civil (ANAC). Atua na certificação de produtos aeronáuticos com assuntos relacionados a plataformas aviônicas, avaliação de processos de desenvolvimento de software e hardware eletrônico embarcado e proteção/segurança da informação.

2 INTRODUÇÃO

Em 2013, a mídia divulgou uma apresentação do consultor em segurança da informação Hugo Teso, feita durante uma conferência em Amsterdam, mostrando uma técnica que possibilitaria controlar sistemas de aeronaves comerciais utilizando um smartphone com sistema operacional Android. Essa técnica possibilitaria inclusive derrubar uma aeronave remotamente (BLOOMBERG, 2013). Na época, as principais autoridades de aviação civil analisaram o caso e concluíram que a técnica descrita pelo consultor não seria realizável, considerando-se os equipamentos reais das aeronaves em questão. Isso porque o consultor utilizou como base de seu estudo, apenas versões não certificadas (de desenvolvimento) dos sistemas (BELLAMY III, 2013). Contudo, esse e outros casos mais recentes trazem à tona a seguinte questão: é possível um hacker derrubar um avião? Apenas a ideia de que isso possa acontecer tem um enorme potencial de causar danos à imagem da aviação perante a sociedade.

Segurança é um valor compartilhado por todos os stakeholders envolvidos na aviação civil e graças a isso, a aviação é considerada o meio de transporte mais seguro do mundo. A segurança relacionada com a proteção das informações dos sistemas da aeronave contra ataques eletrônicos é uma preocupação crescente da comunidade aeronáutica, que surgiu a partir do amplo uso de redes de dados (internas e externas) nas aeronaves.

A automação e o uso de novas tecnologias nos diferentes sistemas aviônicos trouxe para os operadores um ganho em eficiência e, para a aviação civil em geral, um ganho significativo de segurança, reduzindo o número de acidentes no transporte de passageiros. Por outro lado, o avanço tecnológico também introduziu novos perigos que precisam ser identificados e devidamente tratados. Dessa forma surgem diversos questionamentos, como por exemplo: quais são as ameaças e quais as vulnerabilidades do sistema? O que deve ser protegido? Como proteger a aeronave de forma eficiente? Como demonstrar para as autoridades que foi feita uma avaliação completa? Qual método utilizar?

Este artigo não tem a pretensão de responder a todas estas perguntas, mas, tem como objetivo, abordar estas questões de forma a dar uma visão geral para o leitor dos caminhos já trilhados e aceitos pela comunidade aeronáutica, apontar para as questões ainda em discussão e para os desafios futuros.

Para mostrar como ASISP está sendo tratado pelas principais autoridades de aviação civil e discutir as metodologias de análise de segurança da informação de sistemas aeronáuticos propostas pela EUROCAE e RTCA, serão mostradas as diferenças entre safety e security e como elas estão relacionadas com ASISP. Serão mostrados também, o que é considerado ameaça aos sistemas da aeronave, os principais elementos de um ataque eletrônico e como proteger a aeronave. Em seguida, será apresentada uma visão geral da conjuntura regulatória atual e algumas considerações adicionais.

3 SAFETY, SECURITY E PROTEÇÃO E SEGURANÇA DA INFORMAÇÃO DE SISTEMAS DA AERONAVE

Os termos *safety* e *security* podem ser traduzidos do Inglês como uma única palavra: segurança. No entanto, essas duas palavras têm significados bem diferentes. Enquanto *safety* está relacionado aos eventos fortuitos causados, por exemplo, por falhas mecânicas, condições climáticas e erros de software; *security* se refere aos eventos decorrentes de ataques deliberados e mal intencionados, que podem ser físicos ou eletrônicos. Dessa forma, neste artigo serão adotados os termos em Inglês para diferenciar o tipo de segurança em questão.

Em aviação o termo *security* é comumente utilizado para abordar os assuntos relativos à segurança física dos passageiros, tripulantes, pessoas ligadas à aviação civil e aeronaves. A preocupação com *security* na aviação civil intensificou-se com o ataque terrorista de 11 de Setembro de 2001 nos Estados Unidos, a partir do qual as operações aeroportuárias foram reformuladas para incluir métodos e procedimentos que atuassem como barreiras de proteção (i.e. medidas de *security*).

A questão em torno da segurança da informação dos sistemas das aeronaves é mais recente, e diferentes termos têm sido utilizados para se referir a este assunto, como por exemplo: *"cyber security", "Airworthiness Security" e "ASISP - Aircraft System Information Security/Protection".*

"Proteção e Segurança da Informação de Sistemas da Aeronave" (tradução da sigla ASISP) é o termo mais recente adotado pela autoridade de aviação civil americana, a *Federal Aviation Administration*, FAA. ASISP **não** está relacionado nem a ameaças físicas e nem a ameaças devidas a interferência eletromagnética. Para o propósito deste documento, ASISP

pode ser definido como: *a proteção de uma aeronave contra interações eletrônicas intencionais e não autorizadas (i.e. security) com o potencial de afetar safety.*

Essa definição de ASISP estabelece uma relação clara entre *security e safety*. Deve-se garantir a segurança de um recurso da aeronave, o qual, uma vez atacado, pode resultar em um evento de *safety*, isto é, *"security for safety"*. Este recurso da aeronave também é chamado de ativo (*asset*).

Os documentos ED-202A (EUROCAE, 2014a) e DO-326A (RTCA, 2014a) trazem uma definição para *Airworthiness Security* que relaciona *security* com a aeronavegabilidade da aeronave. De acordo com a SAE (2010), um item é considerado aeronavegável quando ele é capaz de cumprir sua função pretendida de forma segura. Portanto, a definição de aeronavegabilidade é mais abrangente, não sendo precisa em relação ao alvo da análise, que é *safety*.

Existe certa controvérsia na comunidade de aviação civil também sobre os termos "intencional" e "não autorizado". De fato, as proteções relacionadas a ASISP devem também tratar de casos onde, por exemplo, pessoas autorizadas (ex: pilotos ou mecânicos) executam uma atualização de software com vírus, intencionalmente desenvolvido por outra pessoa que não tem autorização de acesso.

4 AMEAÇAS AO SAFETY DA AERONAVE

O sistema de comunicação da aviação é um sistema complexo e integrado que permite a troca de informações entre diferentes *stakeholders*. A Figura 1 mostra um exemplo do ambiente de comunicação de informações da aviação civil.

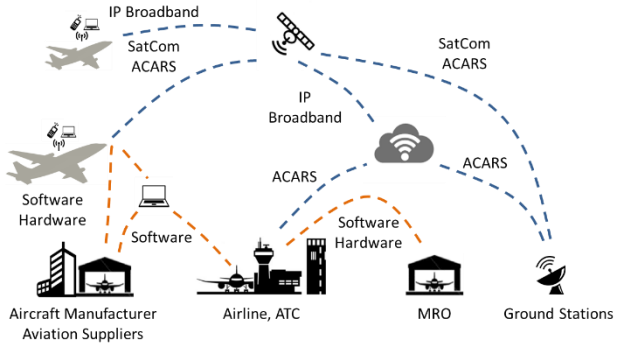

Figura 1 - Ambiente de Comunicação da Aviação Civil

As aeronaves mais modernas operam conectadas a diversas redes permitindo comunicações em voo com o controle de tráfego aéreo, provedores de serviços de navegação aérea e operadores aéreos. Essa conectividade possibilita que os operadores melhorem os seus processos, podendo por exemplo, planejar manutenções com antecedência, reduzindo os custos de operação e o *turn-around-time*[2].

Os sistemas embarcados nas aeronaves, que antes eram desenvolvidos exclusivamente para uso aeronáutico, hoje utilizam partes e padrões abertos comuns a outras indústrias, (i.e. utilizam tecnologias COTS (*Commercial Off The Shelf*)). As interfaces específicas das aeronaves são projetadas para que o sistema tenha uma conexão simples e direta com tecnologias COTS (AIAA, 2013).

Os operadores aéreos têm interesse em disponibilizar novos serviços aos passageiros, que envolvem a adoção de tecnologias como redes Wi-Fi para acesso à Internet ou conteúdo de entretenimento e conexões via USB para leitura de informações de áudio/vídeo dos usuários. Tais tecnologias, voltadas à conectividade dos passageiros, têm o potencial de introduzir novas ameaças ao *safety* da aeronave.

Esse ambiente de troca de informações, através das diversas redes de comunicação, e o uso de tecnologias COTS criaram novas ameaças na aviação que podem representar oportunidades para ataques cibernéticos. Essas novas ameaças se dão devido às vulnerabilidades da segurança da informação (*information security*) que podem ser exploradas por uma pessoa mal intencionada (i.e. atacante ou *attacker*) para corromper ou inibir a transmissão de dados da aeronave, podendo ter consequências em *safety* (*safety effects*).

4.1 Interações Eletrônicas Intencionais não Autorizadas

Para compreender melhor o que são interações eletrônicas intencionais e não autorizadas em uma aeronave será utilizado o exemplo de um cenário de ameaça (*threat scenario)* mostrado na Figura 2, extraída do documento da EUROCAE ED-203.

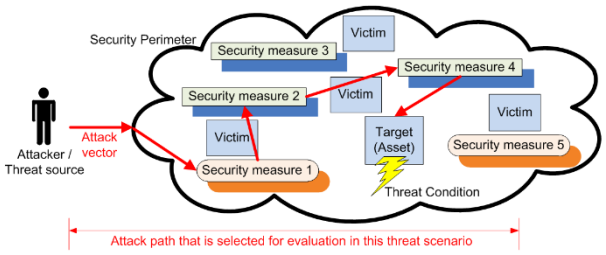

Figura 2 - Exemplo de Cenário de Ameaça (EUROCAE, 2015a)

Um ataque eletrônico ocorre quando uma pessoa mal intencionada (i.e. atacante ou *attacker*) utiliza um meio (i.e. vetor de ataque ou *attack vector*) para penetrar no perímetro de *security* (*security perimeter*). Perímetro de *security* é a noção de fronteira entre o contexto interno de *security* e o ambiente externo da aeronave/sistema. Ele registra os elementos da aeronave/sistema que têm interface com sistemas externos ou pessoas.

A fonte da ameaça *(threat source*) é a intenção e o método almejado, (i.e. o atacante e o vetor de ataque). A condição de ameaça (*threat condition*) é uma condição que tem um efeito na aeronave e/ou nos seus ocupantes, desencadeada por um cenário de ameaça.

O ataque percorre um caminho (i.e. caminho do ataque ou *attack path*, representado pelas setas vermelhas na Figura 2) dentro do perímetro de *security*, interagindo com diferentes sistemas e redes até atingir o alvo do ataque (*target*). Durante

[2] Tempo que a aeronave fica no solo entre um voo e outro, necessário para o desembarque, a preparação da aeronave (verificação, abastecimento e manutenção) e o embarque de passageiros e cargas para o próximo voo.

o ataque são executadas ações para contornar ou adulterar sistemas e medidas de *security* que estão no caminho do ataque. Uma medida de *security* (*security measure*) pode ser qualquer elemento capaz de mitigar ou evitar o ataque em cada fase do caminho do ataque.

Os ativos (*assets)* são recursos físicos e lógicos da aeronave que contribuem para o *safety* da aeronave. Os sistemas/itens que, por acaso estejam no caminho do ataque, mas que não forneçam proteção, são chamados de vítimas (*victims*).

Um sistema pode ser mais ou menos suscetível aos ataques eletrônicos. Para se avaliar o nível de ameaça (*level of threat*) de um sistema, devem ser levados em consideração, por exemplo: o tempo necessário para preparar e executar o ataque; os conhecimentos necessários para preparar e executar o ataque; o conhecimento do alvo e do caminho do ataque; a janela de oportunidade e o equipamento necessário para preparar e executar o ataque.

A análise de *security* também deve levar em consideração ataques considerados multiestágios (*multi-stage attacks*). Por exemplo, um ataque composto por duas etapas: (1) uma mídia de carregamento é adulterada e (2) o mecânico instala os arquivos adulterados no avião sem tomar conhecimento da adulteração realizada previamente, por uma pessoa não autorizada e mal intencionada.

Com os principais elementos de um cenário de ameaça definidos, será discutido no próximo tópico, uma maneira de se prover *security* à aeronave de forma eficiente.

5 PROTEGENDO A AERONAVE

Toda medida de *security* adicionada para proteger um determinado elemento ou sistema, representa um custo adicional de implementação, manutenção e monitoramento. Além disso, uma medida de *security* pode, ela mesma, conter vulnerabilidades que resultem em novas ameaças. Dessa forma, não é viável proteger todos os sistemas de todas as ameaças e, uma discussão interessante é: *o quê* exatamente deve ser protegido na aeronave e *como*.

Como visto anteriormente, ativos são os recursos da aeronave que, uma vez atacados, podem resultar em um evento de *safety* e são eles que devem ser protegidos. Agora a questão é: como proteger a aeronave de forma eficiente?

Uma possível solução poderia ser: agrupar os ativos num domínio específico e proteger as fronteiras deste domínio. Onde domínio é um conjunto de entidades arquiteturais controladas, de forma que as comunicações entre domínios estão sujeitas à especificações e requisitos de interface (para controlar fluxo de dados entre domínios), (RTCA, 2014c).

De acordo com o documento DO-356 (RTCA, 2014c), o uso de domínios simplifica a tarefa de avaliar os requisitos de garantias (*assurance requirements*) provendo propriedades de separação e isolamento.

O documento da *Aeronautical Radio, Incorporated*, ARINC 811 (ARINC, 2005), sugere alocar os sistemas e redes em domínios definidos por funcionalidade e propõe a utilização de 4 domínios, como ilustrados na Figura 3.

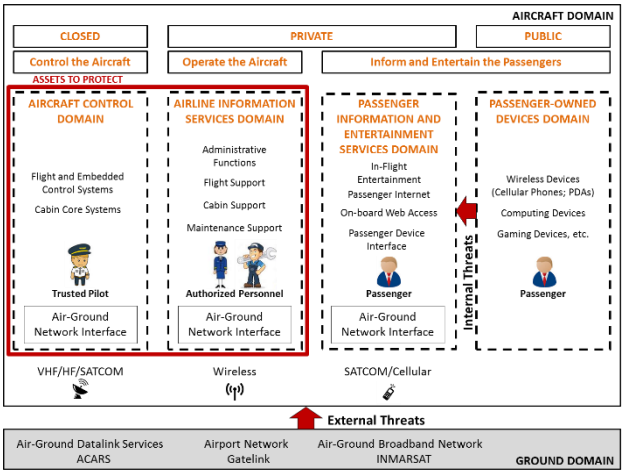

Figura 3 - Domínios Operacionais de Segurança da Informação da Aeronave

1. *Aircraft Control Domain* (ACD): o Domínio de Controle da Aeronave é um domínio fechado, formado pelos sistemas responsáveis pela operação segura da aeronave, suas redes associadas e sistemas de interface (*boundary systems*).

2. *Aircraft Information Services Domain* (AISD): o Domínio de Serviços de Informação da Aeronave é um domínio privado, formado pelos sistemas não essenciais relativos ao suporte em voo, incluindo, suporte às companhias aéreas e às operações da tripulação, rede externa, rede associada e os dispositivos de interface.

3. *Passenger Information and Entertainment Systems Domain* (PIESD): o Domínio de Informações de Passageiros e Sistemas de Entretenimento é um domínio privado, que consiste nos sistemas que dão suporte aos serviços de passageiros, redes associadas e sistemas de interface.

4. *Passenger Owned Devices Domain* (PODD): o Domínio dos Dispositivos de Propriedade dos Passageiros é um domínio público, formado pelos equipamentos eletrônicos do público externo.

As setas vermelhas na Figura 3 representam os ataques aos ativos da aeronave. Eles podem se originar de fontes externas (i.e. ameaças externas), como por exemplo: acesso e transmissão eletrônica de bases de dados e aplicações de software atualizáveis em campo (*field-loadable*), como também podem vir de fontes internas, no domínio de passageiros (i.e. ameaças internas).

O ACD e o AISD são os domínios que devem ser protegidos contra ameaças de *security* com potencial de afetar *safety*. As Condições Especiais, emitidas pelas autoridades, geralmente, impõem aos requerentes que os ativos presentes nesses domínios (ACD e AISD) devam ser protegidos de ameaças à integridade e disponibilidade que comprometam

safety e de acessos eletrônicos não autorizados, de forma automática[3] e em diferentes camadas (FAA, 2008).

No entanto, como há dificuldades associadas com a proteção destes domínios contra todos os potenciais riscos, as autoridades têm aceitado que os requerentes protejam as fronteiras destes domínios, por meio da proteção de suas interfaces externas (inclusive utilizando produtos de *security* comerciais, desde que eles sejam validados por uma autoridade reconhecida) sob determinadas condições previstas.

6 DEMONSTRANDO QUE A AERONAVE ESTÁ PROTEGIDA

Toda a atividade humana implica em um risco e na aviação civil não é diferente. Para as aeronaves certificadas há requisitos que definem critérios de aceitação dos riscos. Estes critérios baseiam-se na severidade de uma condição de falha e na possibilidade desta falha ocorrer.

A metodologia que avalia os riscos de *safety* de uma aeronave é conhecida como *Safety Assessment* (SAE, 1996). O *Safety Assessement* é uma metodologia consagrada, largamente utilizada em projeto aeronáutico e devidamente regulada pelas autoridades de aviação civil. Todavia, ASISP é um assunto ainda em discussão, onde ainda não há requisitos de certificação publicados e nem uma metodologia de *Security Assessment* que seja amplamente aceita. Atualmente, cada fabricante desenvolve sua própria metodologia para demonstrar para as autoridades que o projeto é seguro.

Apesar da falta de requisito específico de *security*, as autoridades de aviação civil, em conjunto com a indústria, vêm debatendo sobre segurança da informação para definir a melhor maneira de proteger a aviação civil de ataques eletrônicos. Para entender melhor o que já foi feito, serão mostrados os documentos já publicados pelos principais organismos de padronização que trabalham com a aviação civil, a *European Organization for Civil Aviation*, EUROCAE e a *Radio Technical Commission for Aeronautics*, RTCA.

Em 2007, a RTCA estabeleceu o *Special Commitee* SC-216 intitulado *Aeronautical Systems Security* e a EUROCAE por sua vez, criou o *Working Group* WG-72, chamado *Aeronautical Information Systems Security*, ambos com o objetivo de desenvolver material de apoio e recomendações nesta área do conhecimento.

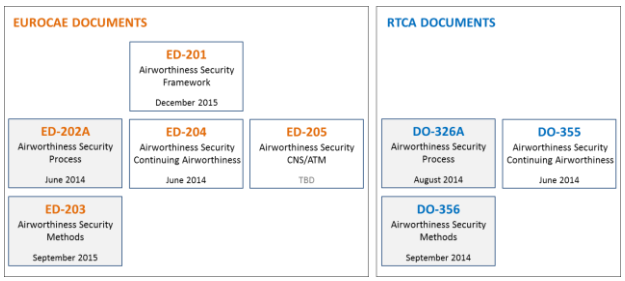

Figura 4 – Documentos EUROCAE e RTCA

Desde a sua formação em 2007, os grupos de trabalho vêm discutindo esse assunto e publicaram uma série de documentos, como ilustrado na Figura 4. Em 2014 foram publicados os documentos ED-202A e DO-326A, intitulados *Airworthiness Security Process*, sobre o processo de *security*. O conteúdo técnico desses documentos é equivalente e traz recomendações sobre *o quê* deve ser feito em termos de gerenciamento de *security* no nível do processo.

O objetivo dos documentos ED-203 (EUROCAE, 2015a) e DO-356 (RTCA, 2014c) é detalhar como o gerenciamento de *security* deve ser feito, estabelecendo as metodologias de análise de segurança da informação de sistemas das aeronaves. Esses documentos foram publicados com 1 (um) ano de diferença entre eles e, diferentemente dos documentos anteriores, não houve consenso quanto ao seu conteúdo.

O tópico seguinte mostra uma visão geral dos processos de Gerenciamento do Risco de *Security* e de *Security Risk Assessement* propostos pelos documentos DO-326A e ED-202A para, a seguir, expor as diferenças entre as metodologias propostas pelos documentos subsequentes, as DO-356 e ED-203.

6.1 Gerenciamento do Risco de Security - Security Risk Management

O objetivo do processo de *Airworthiness Security* é assegurar que um equipamento (i.e. aeronave, sistema ou item) esteja protegido de ataques a dados ou interfaces. Para se fazer isso, gerencia-se o risco de *security* avaliando e identificando lacunas no projeto, corrigindo e melhorando o projeto, aumentando a confiança sobre como o equipamento será implementado, verificando sua efetividade após a implementação e estabelecendo critérios de aceitação do risco de *security* para o equipamento desenvolvido (RTCA, 2014a).

O Gerenciamento do Risco de *Security* é um processo necessário para demonstrar que as ameaças de *security* à aeronave foram identificadas, avaliadas e que foram implementadas estratégias de mitigação do risco. O documento ED-202A define Gerenciamento do Risco de *Security* como um processo contínuo que estabelece o contexto, avalia o risco e atribui objetivos para que o plano de tratamento de risco possa implementar recomendações e decisões (EUROCAE, 2014a).

O Gerenciamento do Risco de *Security* deve levar em conta ameaças possivelmente causadas por atividades de manutenção ou pela conexão de qualquer equipamento, dentro ou fora da aeronave. Além disso, essas ameaças devem ser gerenciadas durante todo o ciclo de vida da aeronave.

Segundo os documentos DO-326A e ED-202A, o processo de gerenciamento do risco de *security* possui 7 etapas

[3] A função de *security* requerida é obtida utilizando-se funcionalidades características do equipamento, sem a necessidade de intervenção humana (nem da tripulação nem do pessoal de manutenção).

como mostra a **Erro! A origem da referência não foi encontrada.**.

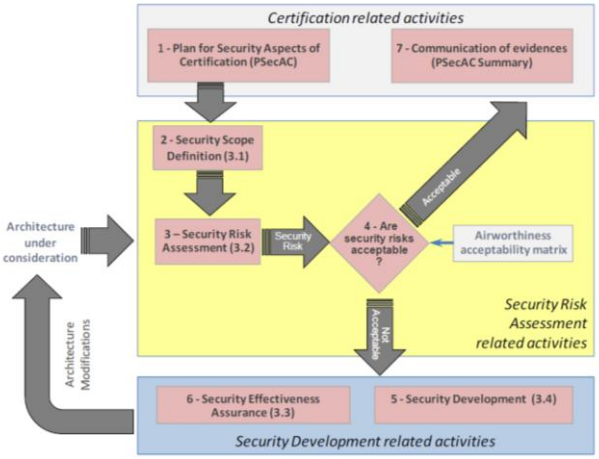

Figura 5 - Processo de Gerenciamento do Risco (EUROCAE, 2014a) (RTCA, 2014a)

- **Passo 1: Plano para Aspectos de *Security* na Certificação:** o plano é definido pelo requerente e acordado pelas autoridades de aviação civil. Ele seve de entrada para todas as demais atividades.
- **Passo 2: Definição do Escopo de *Security*:** estabelece o escopo de *security* como entrada da Avaliação dos Riscos de *Security*.
- **Passo 3: *Security Risk Assessment*:** identifica e avalia riscos de *security*.
- **Passo 4: "Os Riscos de Security são aceitáveis?":** O risco de *security* é aceitável ou não de acordo com uma matriz de aceitação. A matriz de aceitação do risco define uma combinação aceitável de nível de ameaça e efeito em *security* (*security effect*)[4] e deve ser definida pelo requerente juntamente com as autoridades de aviação civil.
- **Passo 5: Desenvolvimento de *Security*:** são ações de mitigação do risco que resultem no projeto de elementos arquiteturais de *security* para tratar o conjunto de cenários de ameaças envolvidos no risco a ser mitigado. Novos elementos arquiteturais de *security* devem ser levados em conta como entrada para reavaliar os riscos de *security* (Passo 3).
- **Passo 6: *Security Effectiveness Assurance*:** esta etapa representa as atividades que devem ser feitas para assegurar que os riscos de *security* sejam aceitáveis, como uma forma de garantir a efetividade das medidas de *security* (*security measures*) introduzidas.
- **Passo 7: Comunicação das Evidências:** quando os riscos são aceitáveis, os resultados das atividades de *security* devem ser registrados no documento *Plan for Security Aspects Certification Summary*.

Como se pode observar, o *Security Risk Assessment* é parte do processo de Gerenciamento do Risco de *Security* e a metodologia de *Security Risk Assessment* é uma ferramenta utilizada para analisar e avaliar o risco de *security.*

6.2 Security Risk Assessment

O *Security Risk Assessment* identifica e avalia os riscos de *security*. Ele consiste na identificação de quais ameaças podem ocorrer, suas possíveis consequências e qual o impacto deste evento, antes de decidir o que deve ser feito para reduzir o risco para níveis aceitáveis.

O risco de *security* de um cenário de ameaça é definido por:

- Nível de Ameaça (*Level of Threat*) deste cenário de ameaça e,
- Severidade do Efeito *(Severity of Effect)* da condição de ameaça causado ou contribuído por este cenário de ameaça.

O nível de ameaça (*level of threat*) pode ser descrito como a possibilidade que uma condição de ameaça ocorra ou como a dificuldade de um ataque ocorrer. A avaliação do nível de ameaça está relacionada com a efetividade da medida de *security* (*security measure effectiveness*) em um cenário de ameaça específico. Ou seja, quanto maior a efetividade de uma medida de *security*, maior será a sua capacidade de proteger o sistema e menor será a chance de um ataque ser bem sucedido. Em contrapartida, a severidade do efeito (*severity of effect)* avalia as consequências do ataque.

A Figura 6 ilustra o *Security Risk Assessment* proposto pela DO-326A/ED-202A.

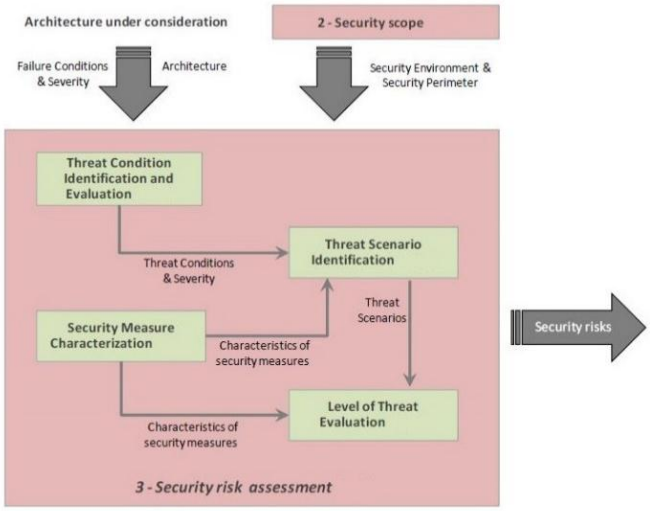

Figura 6 - Security Risk Assessment (EUROCAE, 2014a) (RTCA, 2014a)

O *Security Risk Assessment* consiste nas seguintes atividades:

- **Identificação e avaliação da Condição de Ameaça:** identifica as condições de ameaça, que surgem através da existência de vulnerabilidades[5], identifica os efeitos em *safety* das condições de ameaça e classifica a severidade

[4] Também chamado de *severity of threat condition effects.*

[5] Vulnerabilidade é uma falha ou fraqueza nos procedimentos de *security* do sistema, design, implementação ou controles internos que poderiam ser exercidos (desencadeados involuntariamente ou explorados intencionalmente) e resultar em uma violação de *security* ou em uma violação das políticas de *security* do sistema (EUROCAE, 2014a).

de cada condição de ameaça (i.e., *Catastrophic, Hazardous, Major, Minor,* ou *No Safety Effect*).

- **Identificação dos Cenários de Ameaça:** identifica todos os elementos num cenário de ameaça (veja Figura 2).
- **Caracterização das Medidas de *Security*:** caracteriza as medidas de *security* de acordo com o tipo do seu efeito (i.e. preventiva, dissuasiva, *detective*, corretiva, ou reparadora), efetividade e vulnerabilidades. Neste momento, são consideradas as medidas de *security* atualmente presentes no sistema.
- **Avaliação do Nível de Ameaça:** avaliação qualitativa da possibilidade dos cenários de ameaça causarem uma condição de ameaça.

Uma vez apresentado o processo de gerenciamento do risco de *security*, o tópico seguinte faz uma análise das metodologias propostas pelos documentos DO-356 e ED-203.

6.3 Metodologias para Airworthiness Security

Os documentos RTCA DO-356 e EUROCAE ED-203 apresentam diferenças significativas entre as metodologias propostas para *Airworthiness Security.* Também apresentam algumas semelhanças. Os principais pontos a constar são descritos abaixo, assim como considerações a respeito das interfaces com os processos de desenvolvimento já existentes.

O documento emitido pela RTCA trata do nível de ameaça em termos de probabilidade (por meio do termo *likelihood),* o que levaria em consideração o número de vezes que uma determinada condição de ameaça poderia acontecer durante o ciclo de vida da aeronave, inspirando-se nos preceitos qualitativos do requisito RBAC 25.1309 aplicável a *safety*. O conceito de probabilidade na DO-356 também leva em consideração o chamado nível de confiabilidade (*trustworthiness),* que trata das questões organizacionais, por meio de um julgamento qualitativo sobre as fontes de ameaça em relação ao ativo sendo analisado, considerando-se um determinado ambiente. Por exemplo, se a ameaça depende de acesso ao *cockpit*, deve-se considerar o nível de confiabilidade deste ambiente, que é regido pelas normas operacionais aplicáveis. Embora pareça uma estratégia razoável, a análise pode se tornar impraticável.

Enquanto isso, o documento da EUROCAE propõe uma análise mais criteriosa, baseada na dificuldade do ataque, o que considera critérios mais técnicos em relação às ameaças de *security*, tais como o tempo para se preparar um ataque e a janela de oportunidade, mas que com certeza também precisa de mais maturidade por parte da indústria aeronáutica a fim de tecer considerações precisas. A severidade de cada condição de ameaça é bem semelhante em ambos os documentos, considerando a classificação em relação ao *safety effect* (i.e., *Catastrophic*, *Hazardous*, *Major*, *Minor*, ou *No Safety Effect*).

Os dois documentos (DO-356 e ED-203) traçam estratégias distintas em relação ao nível de garantia das proteções (i.e. medidas de *security*) que precisam ser implementadas devido à identificação de riscos considerados inaceitáveis (a partir da análise de nível de ameaça *versus* severidade da condição de ameaça). No entanto, ambos reconhecem que, conforme os preceitos da DO-326A e ED-202A, as proteções devem ser garantidas (*Security Assurance*) tanto pela efetividade (*Security Effectiveness Assurance*) quanto pela garantia do desenvolvimento (*Security Development Assurance*), que visa a minimizar os erros de desenvolvimento.

A efetividade da proteção trata da capacidade da medida de *security* em impedir o ataque e proteger contra as vulnerabilidades do sistema. Já a garantia do desenvolvimento seria dada por uma metodologia sistemática de desenvolvimento equivalente a ED-79A/ARP 4754A (SAE, 2010) para sistemas, a ED-12C/DO-178C (RTCA, 2011) para software ou a ED-80/DO-254 (RTCA, 2000) para hardware eletrônico embarcado, com as adaptações necessárias. É neste ponto que a maioria das diferenças entre as normas aparece, sendo que atualmente ainda não existe um consenso na metodologia para atribuição de níveis de garantia (*assurance levels*) de *security*, considerando tanto a efetividade como a garantia do desenvolvimento, e muito menos sobre as ações necessárias decorrentes dos níveis de garantia estabelecidos.

Na prática, é fundamental que o processo de desenvolvimento voltado à *security* tenha mapeado as interfaces necessárias com os processos de desenvolvimento de sistemas e de *Safety Assessment* existentes, muitas vezes utilizando os documentos ED-79A/ARP-4754A (SAE, 2010) e ED-135/ARP-4761 (SAE, 1996), respectivamente. As interfaces permeiam todo o ciclo de desenvolvimento.

Ao realizar as atividades relativas ao *Security Assessment*, deve-se quebrar a análise em níveis (aeronave/sistemas) e fases (preliminar/final), assim como realizado para o *Safety Assessment*. A Figura 7, extraída da DO-326A, ilustra os conceitos de *Security Assessment*.

Dessa forma, verificamos as seguintes interfaces:

- Após a definição do escopo da avaliação no nível aeronave, um *Aircraft Security Risk Assessment* preliminar é gerado e se relaciona com o *Aircraft Functional Hazard Assessment* (AFHA) e o *Preliminary Aircraft Safety Assessment* (PASA). O AFHA e o PASA fornecem as funções nível aeronave e as condições de falha da aeronave para o processo de *Security*.

- Após a definição do escopo da avaliação no nível de sistema, um *System Security Risk Assessment* preliminar é relacionado aos seus correspondentes do *Safety Assessment*, os *System Functional Hazard Assessments* (SFHAs) e os *Preliminary System Safety Assessments* (PSSAs). Os SFHAs e PSSAs fornecem as funções nível sistema e as condições de falha dos sistemas para suportar o processo de *Security*. O *System Security Risk Assessment* preliminar gera, por sua vez, os requisitos de *security* que podem ser implementados utilizando o próprio processo de desenvolvimento de sistemas da aeronave, tal como prescrito pela ED-79A/ARP-4754A, com as devidas considerações relativas ao processo específico de *security*.

- Ao final, um *System Security Risk Assessment* é gerado, confirmando que os resultados do desenvolvimento relativo à *security* trazem os riscos a níveis aceitáveis, conforme critério pré-estabelecido e requisitos estabelecidos de acordo com o *assessment* preliminar. Tal atividade relaciona-se aos *System Safety Assessments* (SSAs).
- Da mesma forma, um *Aircraft Security Risk Assessment* final é gerado, relacionando-se com o *Aircraft Safety Assessment* (ASA).

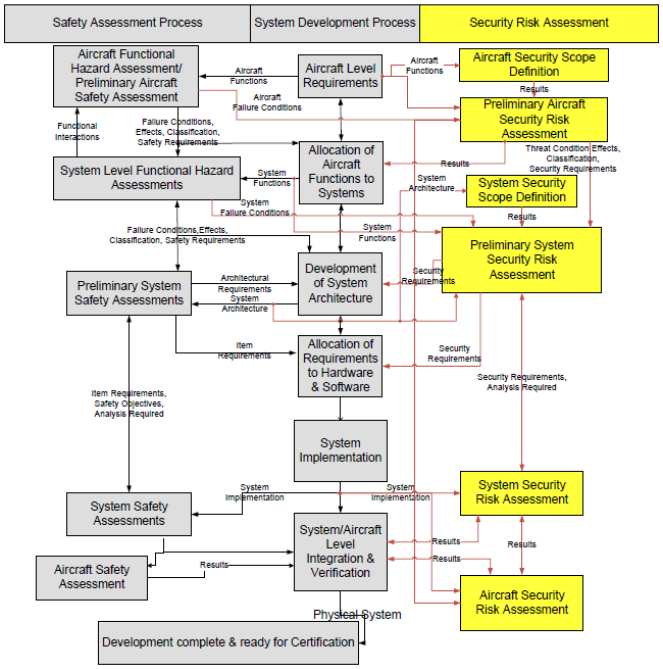

Figura 7 - Conceitos do Security Assessment (RTCA, 2014a)

7 CONJUNTURA REGULATÓRIA ATUAL

Conforme mencionado anteriormente, não existem ainda requisitos de certificação que abordem as questões relativas à ASISP. Portanto, as autoridades de aviação civil precisam atualmente estabelecer Condições Especiais para os projetos vigentes assim que identificados possíveis riscos.

Para estabelecer os critérios de aplicação das Condições Especiais, a ANAC utiliza como base o *Policy Statement* PS-AIR-21.16-02 de 06 de março de 2014 (FAA, 2014), desenvolvido pela autoridade de aviação norte-americana, a FAA (*Federal Aviation Administration*). Esta *policy* está atualmente em processo de revisão e, portanto, não convém tratar dos seus critérios neste artigo. É importante, porém, ressaltar que o foco tem sido a avaliação de riscos relativos à ASISP que afetem sistemas com condições de falha de *safety* que sejam classificadas como *major* ou mais severo. Para tanto, é necessário avaliar a propagação de um possível ataque, podendo, inclusive, ter como elemento de entrada, um equipamento com classificação de condição de falha *minor* ou *no safety effect*.

A primeira condição especial sobre o assunto foi emitida pela FAA para o modelo 787-8 da Boeing (FAA, 2008). Na realidade, foram emitidas não apenas uma condição especial, mas duas: uma para abordar a conectividade externa à aeronave, e outra para abordar a conectividade interna. A preocupação com a conectividade interna trata do isolamento necessário das redes de dados internas de entretenimento de passageiros em relação aos domínios *Aircraft Control Domain* (ACD) e *Aircraft Information Services Domain* (AISD). Por outro lado, a conectividade externa aborda as demais interfaces da aeronave (ver Figura 3). Ambas as Condições Especiais se tornaram efetivas no início de 2008.

Embora as primeiras versões das Condições Especiais não referenciassem especificamente os documentos da RTCA e EUROCAE, elas já introduziam a necessidade de um *Security Assurance Process* que contemplasse a avaliação no nível aeronave e nível sistema, estabelecendo os riscos em potencial e as vulnerabilidades introduzidas pela conectividade das redes de dados disponíveis (interna e externamente). A partir de tal avaliação, requisitos devem ser estabelecidos e implementados no desenvolvimento de forma a minimizar os riscos de *security* a níveis aceitáveis. Alguns pontos específicos de preocupação das Condições Especiais incluem:

- A necessidade de um *system security audit* que permita gravar *security audit logs* relativos aos acessos às redes relativas ao *Aircraft Control Domain (ACD)*.
- O desenvolvimento de um plano de teste denominado *"security risk and vulnerability penetration testing"*, que deve ser revisado e executado por pessoal independente do desenvolvimento, a fim de confirmar a robustez do sistema com as medidas de *security* implementadas.
- A necessidade de estabelecer instruções de aeronavegabilidade continuada para que as proteções de *security* sejam mantidas.
- A necessidade de reportar às autoridades as condições inseguras associadas a eventos de *security* ocorridos em campo durante a operação.

Como forma de estabelecer requisitos explícitos de certificação e remover a necessidade de estabelecimento de Condições Especiais para cada projeto, a FAA lançou, no início de 2015, o *Aviation Rulemaking Advisory Committee* (ARAC) em Proteção e Segurança da Informação de Sistemas da Aeronave (ASISP). Esse ARAC tem como objetivo prover recomendações ao FAA sobre os novos requisitos necessários, *policy* e material interpretativo para tratar a questão de ASISP, tanto para certificação como para a aeronavegabilidade continuada. Os trabalhos do comitê estão em andamento e o relatório com as recomendações finais deverá ser emitido até o final de 2016.

No ARAC, dois grupos foram formados para tratar da regulamentação de diferentes categorias:

- Grupo 1: aviões categoria transporte (i.e. que seguem os regulamentos 14 CFR/RBAC 25);
- Grupo 2: aviação geral e helicópteros (i.e. que seguem os regulamentos 14 CFR/RBAC 23, 27 e 29).

Para os aviões categoria transporte, o grupo 1 está trabalhando na implementação dos *standards* da RTCA/EUROCAE para ASISP, tendo processos paralelos entre desenvolvimento de sistemas e *security*, conforme

explicado nas seções anteriores deste artigo. Enquanto isso, a fim de simplificar a análise para aviação geral e helicópteros, o grupo 2 está propondo abordar os requisitos de *security* utilizando os mesmos processos tradicionais de sistemas, hardware e software, sem a necessidade de um processo de *security* totalmente independente.

Paralelamente ao ARAC, também existem esforços para eliminar as diferenças entre as normas RTCA DO-356 e a EUROCAE ED-203. A RTCA já iniciou os trabalhos no início deste ano e pretende concluir uma revisão à DO-356 até dezembro de 2017. Os pontos que precisam ser contemplados na revisão e harmonizados com a EUROCAE, conforme indicação do próprio ARAC sobre ASISP, são os seguintes:

1. Prover uma definição de quais ativos precisam ser protegidos baseados no *safety effect*, determinado pelo *security assessment*.
2. Prover uma definição de "*intentional unauthorized electronic interaction*".
3. Prover orientações de como identificar um risco de *security*, incluindo instrução sobre *o quê* pode ser considerado como confiável no ambiente de *security*.
4. Prover uma matriz de aceitabilidade de risco harmonizada, tomando crédito de matrizes previamente aceitas, conforme apropriado.
5. Prover orientações sobre como demonstrar que o risco residual é aceitável.
6. Prover orientações sobre como mudanças ao Projeto de Tipo devem ser consideradas (tais como aquelas introduzidas por um Certificado Suplementar de Tipo), incluindo mudanças por terceiros que não têm acesso aos dados de projeto do fabricante original.
7. Definir o que constitui evidência aceitável de certificação.
8. Definir o escopo das Instruções de Aeronavegabilidade Continuada relativas à *security*, incluindo orientações adicionais sobre o que deve ser gerado pelo detentor da aprovação do projeto.
9. Prover orientações para o registro (*logging*) dos eventos e o cumprimento com o requisito 14 CFR/RBAC 21.3, relativo à comunicação de falhas, mau funcionamento e defeitos.
10. Definir o papel da confiança no ambiente de *security*, incluindo quais provedores de serviços podem ou não podem ser confiáveis.

O item 10 acima é bastante polêmico, pois existem fortes discrepâncias entre o ambiente europeu e os ambientes norte-americano e brasileiro. No caso da Europa, o controle de trafego aéreo pode ser terceirizado, o que não ocorre nos Estados Unidos e no Brasil, onde é necessariamente, realizado por um órgão governamental.

Assim, para a Europa, a comunicação com o controle de tráfego aéreo pode ser considerada como não confiável, enquanto que nos Estados Unidos e no Brasil poderia se argumentar que, uma vez que o controle é governamental, então os dados são sim confiáveis. No caso europeu, a ED-205 – *Airworthiness Security CNS/ATM* irá tratar da *security* da comunicação advinda dos equipamentos de solo responsáveis pelo controle do espaço aéreo, sendo sua edição liderada pela EUROCONTROL.

Como se pode perceber, embora muito já se tenha avançado em relação ao assunto ASISP, há ainda atividades regulatórias em andamento e inúmeras questões a serem definidas.

8 CONSIDERAÇÕES ADICIONAIS

As autoridades e os fabricantes de aviões e de sistemas aeronáuticos têm trabalhado ativamente para proteger os sistemas das aeronaves e suas redes de possíveis ataques cibernéticos. Fabricantes de aeronaves podem projetar sistemas mais robustos, entretanto, eles não são responsáveis por todo o ciclo de vida da aeronave. Isto significa que outras partes interessadas precisam ter o mesmo nível de consciência e cuidado durante a operação das aeronaves.

Além disso, as aeronaves vão sofrer muitas mudanças durante a sua vida útil, desde simples atualizações de software até reconfigurações completas. Se essas mudanças não forem tratadas adequadamente, elas podem abrir portas na security dos sistemas criando novas vulnerabilidades. Portanto, é necessário que operadores aéreos e organizações de manutenção controlem todo o fluxo de dados dentro e fora da aeronave, monitorando as mídias eletrônicas e o acesso aos sistemas da aeronave. Os documentos ED-204 (EUROCAE, 2014b) e DO-355 (RTCA, 2014b) – Information Security Guidance for Continuing Airworthiness tratam das questões de ASISP para a aeronavegabilidade continuada.

Nos últimos anos, houve uma série de incidentes aparentemente atribuídos a ataques cibernéticos, que demonstram que existem outras vulnerabilidades no sistema de aviação civil que devem ser abordadas com urgência (LIM, 2014).

Por exemplo:

- Um ataque na Internet, em 2006, que forçou a *Federal Aviation Administration* (FAA) a desligar parte do dos sistemas de controle de tráfego aéreo (ATC) no Alasca (FAA, 2009).
- Um ataque a um computador da FAA, em fevereiro de 2009, onde *hackers* obtiveram acesso às informações pessoais de 48.000 funcionários da FAA (FAA, 2009).
- Um ataque cibernético que levou ao desligamento dos sistemas de controle de passaportes nos terminais de embarque dos aeroportos de Istambul Ataturk e Sabiha Gokcen, em julho de 2013, causando atrasos em muitos voos (PAGANINI, 2013).
- Um aparente ataque cibernético, que possivelmente envolveu ações maliciosas de *hacking* e *phishing*, direcionadas a 75 aeroportos nos Estados Unidos, em 2013 (WELSH, 2013).

Estes incidentes mostram que os países também precisam reforçar os seus próprios sistemas para não se tornarem um caminho de entrada para ataques cibernéticos.

Em 2012, a Organização de Aviação Civil Internacional (OACI) publicou o Anexo 17 sobre Security e em 2013 introduziu uma nova recomendação, onde "cada Estado

Contratante deve desenvolver medidas para proteger os sistemas de informação e a tecnologia de comunicação, utilizados para fins de aviação civil, de interferências que possam comprometer a segurança da aviação civil".

Em dezembro de 2014, as 5 maiores organizações de aviação civil assinaram um novo acordo de cyber security, formalizando sua posição contra hackers, "hacktivistas", criminosos e terroristas, agora focados na intenção maliciosa, que vai desde o roubo de informações e perturbação geral à perda potencial de vidas (ICAO, 2014). A OACI, o Conselho Internacional de Aeroportos (ACI), a Organização Civil de Serviços de Navegação Aérea (CANSO), a Associação Internacional de Transporte Aéreo (IATA) e o Conselho de Coordenação Internacional das Associações da Indústria Aeroespacial (ICCAIA) chegaram a um acordo sobre um roteiro comum para alinhar suas respectivas ações sobre ameaças cibernéticas. Para coordenar melhor suas ações e respostas, os signatários de acordos cibernéticos serão mais proativos no compartilhamento de informações críticas como: a identificação de ameaças, as avaliações de risco e as melhores práticas de security cibernética. Eles também deverão incentivar a coordenação, em nível nacional, entre os órgãos governamentais e indústria, de todas as estratégias, políticas e planos de security cibernética, (ICAO, 2014).

O documento EUROCAE ED-201 – Aeronautical Information System Security Framework Guidance (EUROCAE, 2015b), trata dos riscos compartilhados da segurança da informação inerente à aviação civil como um todo.

9 CONCLUSÃO

O uso de sistemas eletrônicos sofisticados e conexões de rede nas operações aéreas vai continuar expandindo e as ameaças cibernéticas crescem na mesma velocidade que a evolução tecnológica. Para manter a segurança da aviação nos níveis atuais é inevitável considerar as questões de ASISP em cada elemento do sistema da aviação.

As autoridades de aviação civil e a indústria já avançaram bastante no que tange à avaliação de security nos projetos aeronáuticos, mas ainda há muito a ser feito. Até o presente momento, não há requisitos de certificação efetivamente publicados e o ARAC sobre ASISP deve apresentar uma proposta de regra para a FAA até o fim de 2016.

As discussões sobre os métodos aceitáveis para realização do security risk assessment também precisam avançar e, os grupos WG-72 da EUROCAE e SC-216 da RTCA já estão trabalhando para harmonização do material orientativo. As normas RTCA DO-356 e EUROCAE ED-203 devem ser revisadas até dezembro de 2017.

É necessário que haja colaboração ente governos e indústria para que atuem proativamente contra as ameaças eletrônicas e para fortalecer a resiliência do sistema da aviação contra ataques cibernéticos (AIAA, 2013). É fundamental que todos os stakeholders (i.e. a Organização de Aviação Civil Internacional (OACI), as autoridades de aviação civil, os fabricantes de aeronaves, fornecedores de sistemas aeronáuticos, operadores, provedores de serviços de aviação, etc.) trabalhem em conjunto para reconhecer as ameaças e tomar ações para proteger e mitigar aquelas que têm o potencial de impactar safety.

Dessa forma, a aviação poderá continuar avançando tecnologicamente sem colocar em risco a sua reputação de meio de transporte seguro e com baixos índices de acidente.

REFERÊNCIAS

AIAA. The Connectivity Challenge: Protecting Critical Assets in a Networked World. A Framework for Aviation Cybersecurity. Reston: American Institute of Aeronautics and Astronautics. 2013.

ARINC. ARINC 811 - Commercial Aircraft Information Security Concepts of Operation and Process Framework. Aeronautical Radio, Incorporated. 2005.

BELLAMY III, W. 2013. FAA Dismisses Aircraft FMS Hacking Claim. Disponível em:

<http://www.aviationtoday.com/av/web-exclusives/FAA-Dismisses-Aircraft-FMS-Hacking-Claim_78985.html>. Acesso em: 03 jun. 2016.

BLOOMBERG. 2013. Hacking an Airplane With Only an Android Phone. Disponível em:

<http://www.bloomberg.com/news/articles/2013-04-12/hacking-an-airplane-with-only-an-android-phone>. Acesso em: 03 jun. 2016.

EUROCAE. ED-202A - Airworthiness Security Process Specification. Malakoff: European Organization for Civil Aviation. 2014a.

EUROCAE. ED-204 - Information Security Guidance for Continuing Airworthiness. Malakoff: European Organization for Civil Aviation. 2014b.

EUROCAE. ED-203 - Airworthiness Security Methods and Considerations. Malakoff: European Organization for Civil Aviation. 2015a.

EUROCAE. ED-201 - Aeronautical Information System Security Framework Guidance. Malakoff: European Organization for Civil Aviation. 2015b.

FAA. 2008. Special Conditions: Boeing Model 787-8 Airplane; Systems and Data Networks Security-Protection of Airplane Systems and Data Networks from Unauthorized External Access. Disponível em: <http://rgl.faa.gov/Regulatory_and_Guidance_Library/rgSC.nsf/0/3DB883B91F1829D3862573BF0056C213?OpenDocument&Highlight=security>. Acesso em: 05 jul. 2016.

FAA. FI-2009-049 - Review of Web Applications Security and Intrusion Detection in Air Traffic Control Systems. Memorandum. 2009.

FAA. PS-AIR-21.16-02 - Establishment of Special Conditions for Cyber Security. National Policy. 2014.

ICAO. 2014. Aviation Unites on Cyber Threat. Disponível em:

<http://www.icao.int/Newsroom/Pages/aviation-unites-on-cyber-threat.aspx>. Acesso em: 03 jun. 2016.

LIM, B. Aviation Security - Emerging Threats from Cyber Security in Aviation – Challenges and Mitigations. Journal of Aviation Management, pp. 83-90. 2014.

PAGANINI, P. 2013. Media agencies reported news of a cyber attack against the Istanbul Ataturk International Airport, the passport control system at the departure terminal was hit causing many problems at the airport. Disponível em:

<http://securityaffairs.co/wordpress/16721/hacking/istanbul-ataturk-international-airport-targeted-by-cyber-attack.html>. Acesso em: 05 jul. 2016.

RTCA. DO-254 – Design Assurance Guidance for Airborne Electronic Hardware. Washington, DC: Radio Technical Commission for Aeronautics. 2000.

RTCA. DO-178C – Software Considerations in Airborne Systems and Equipment Certification. Washington, DC: Radio Technical Commission for Aeronautics. 2011.

RTCA. DO-326A - Airworthiness Security Process Specification. Washington, DC: Radio Technical Commission for Aeronautics. 2014a.

RTCA. DO-355 - Airworthiness Security Process Specification. Washington, DC: Radio Technical Commission for Aeronautics. 2014b.

RTCA. DO-356 - Airworthiness Secutiry Methods and Considerations. Washington, DC: Radio Technical Commission for Aeronautics. 2014c.

SAE. ARP 4761 - Guidelines And Methods For Conducting The Safety Assessment Process On Civil Airborne Systems And Equipment. Society of Automotive Engineers International. 1996.

SAE. ARP 4754A - Guidelines for Development of Civil Aircraft and Systems. Society of Automotive Engineers International. 2010.

WELSH, W. 2013. Phishing Scam Targeted 75 US Airports. Disponível em: <http://www.informationweek.com/government/cybersecurity/phishing-scam-targeted-75-us-airports/d/d-id/1278762>. Acesso em: 05 jul. 2016.