



Dissertations and Theses

4-2019

Building and Integrating an Information Security Trustworthiness Framework for Aviation Systems

Anna Baron Garcia

Follow this and additional works at: <https://commons.erau.edu/edt>



Part of the [Aerospace Engineering Commons](#), and the [Aviation Commons](#)

Scholarly Commons Citation

Garcia, Anna Baron, "Building and Integrating an Information Security Trustworthiness Framework for Aviation Systems" (2019). *Dissertations and Theses*. 439.

<https://commons.erau.edu/edt/439>

This Thesis - Open Access is brought to you for free and open access by Scholarly Commons. It has been accepted for inclusion in Dissertations and Theses by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.

BUILDING AND INTEGRATING AN INFORMATION SECURITY TRUSTWORTHINESS FRAMEWORK FOR AVIATION SYSTEMS

by
Anna Baron Garcia

A thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Science in Cybersecurity Engineering
at Embry-Riddle Aeronautical University

Department of Electrical, Computer, Software, and Systems Engineering
Embry-Riddle Aeronautical University
Daytona Beach, Florida

April 2019


BUILDING AND INTEGRATING AN INFORMATION SECURITY TRUSTWORTHINESS FRAMEWORK FOR AVIATION SYSTEMS

by Anna Baron Garcia

This thesis was prepared under the direction of the candidate's Thesis Committee Chair, Dr. Radu F. Babiceanu, and has been approved by the members of the thesis committee. It was submitted to the Department of Electrical, Computer, Software, and Systems Engineering in partial fulfillment of the requirements for the degree of Master of Science in Cybersecurity Engineering.




Radu F. Babiceanu, Ph.D.
Committee Chair



Remzi Seker, Ph.D.
Committee Member



Jiawei Yuan, Ph.D.
Committee Member



Timothy A. Wilson, Sc.D.
Chair, Electrical, Computer, Software, and Systems Engineering



Maj Mirmirani, Ph.D.
Dean, College of Engineering



Lon Moeller, J.D.
Senior Vice President for Academic Affairs and Provost

4/25/19

Date

Acknowledgements

First of all, I would like to express my utmost sincere gratitude to my advisor Dr. Radu F. Babiceanu and Dr. Remzi Seker for always providing insightful answers and expertise, and for pushing me to do better during these past 2 years. They encouraged me and guided me throughout the entirety of this Master's degree and prepared me to become a better researcher and student.

Secondly, I would like to thank my family for helping me achieve my dreams. I could have not done it without their support and inspiration, even when we are several thousand miles apart. It is my honor to dedicate this thesis to my late grandmother, who always knew I would succeed in my studies.

Also, I am grateful to Irina and Nick, who have cheered me on every step of the way. And finally, I would like to wholeheartedly thank Noe for her unconditional support, patience, and love, for being the backbone of my sanity, and for going on this crazy adventure with me.

Abstract

The aviation infrastructure is broadly composed of aircraft, air traffic control systems, airports and public airfields. Much attention has been given to physical security along the years this industry has been expanding; and now, in the new age of interconnection devices, a growing concern about cybersecurity has risen.

The never-ending improvement of new digital technology has given birth to a new generation of electronic-enabled (e-enabled) aircraft that implement a remarkable amount of new technologies such as IP-enabled networks, COTS (commercial off-the-shelf) components, wireless connectivity, and global positioning systems (GPSs). For example, aircraft manufacturers are building wireless systems to reduce the amount of wiring within an aircraft. The general purpose of this is the reduction in weight that helps an aircraft achieve lower fuel consumption, but it can result into a security issue since these wireless systems are vulnerable to cybersecurity threats.

Therefore, since the aviation infrastructure has taken advantages of the era of technology and is providing unprecedented global connectivity, there is a need for an in-depth study of the measures being taken to mitigate the security vulnerabilities that these e-enabled aircraft technologies introduce that may have not been considered in the traditional aircraft design.

Contents

Acknowledgements	i
Abstract	ii
Table of Contents	iv
List of Figures	v
List of Tables	vi
List of Abbreviations	vii
1 Introduction	ix
1.1 Statement of The Problem	1
2 Literature Review	2
2.1 Introduction	2
2.1.1 Safety and Security Engineering	4
2.2 Certification and Standards	6
2.3 Security Assessment	17
3 Discussion	22
3.1 Standards and Certification	23
3.1.1 Standard	23
3.1.2 Means of Compliance	26
3.2 Safety and Security Co-Engineering for Airworthiness	27
3.2.1 Safety Assessment Process and Security Assessment Process .	28
3.2.2 SAE ARP 4754A	30
3.2.3 SAE ARP 4761	33
3.2.4 Integration of Safety / Security Methodologies.	33
4 Conclusions and Future Research	38
4.1 Conclusions	38
4.2 Future Research	39

Bibliography	39
References	43

List of Figures

2.1	Aircraft or System Development Process Model (SAE-Aerospace, 2010)	2
2.2	Aircraft Information Interconnections	3
2.3	FAA Rule-making. (Pearson and Riley, 2015)	8
2.4	178C set and its supplementary documents.	14
2.5	Comparison between the two methodologies.	18
3.1	Framework for Aviation Airworthiness (United States)	23
3.2	Relations between Security Standards in Airworthiness Engineering. .	25
3.3	Design and Development Framework	28
3.4	ARP4754A Process - Interaction between safety and development processes	30
3.5	Modified ARP4754A Process - Interaction between safety, security and development processes	31
3.6	ARP4754A Process - Safety Assessment Process Model (SAE-Aerospace, 2010)	32
3.7	ARP4761 Process - Safety Assessment Diagram	33
3.8	Modified Design and Development Framework	34
3.9	Modified ARP4754A Process - Interaction between safety, security and development processes	35
3.10	Modified ARP4754A Process - Safety and Security Assessment Process Model	36
3.11	Modified ARP4761 Process - Safety and Security Assessment Diagram	37

List of Tables

2.1	Regulatory Framework.	7
2.2	Hard law and soft law entities.	7

List of Abbreviations

A

AEEC: Airlines Electronic Engineering Committee
 AFDX: Avionics Full Duplex Switched Ethernet
 API: American Petroleum Institute
 APTA: American Public Transportation Association
 ARINC: Aeronautical Radio, Incorporated
 ARP: Aerospace Recommended Practice
 ASA: Aircraft Safety Assessment
 AT: Attack Trees

C

CCA: Common Cause Analysis
 CIKR: Critical Infrastructure and Key Resources
 CMA: Common Mode Analysis
 COTS: Commercial Off-the-Shelf

D

DCS: Distributed Control System
 DHS: Department of Homeland Security
 DOD: Department of Defense
 DOE: Department of Energy
 DOT: Department of Transportation

E

EASA: European Aviation Safety Agency
 EFB: Electronic Flight Bag
 EO: Executive Order

F

FAA: Federal Aviation Administration

FHA: Functional Hazard Analysis
 FMEA: Failure Mode and Effects Analysis
 FMES: Failure Mode and Effects Summary
 FMVEA: Failure Mode, Vulnerabilities and Effects Analysis
 FTA: Failure Tree Analysis

G

GPS: Global Positioning System

H

HSPD: Homeland Security Presidential Directive

I

ICS: Industrial Control System
 IP: Internet Protocol
 ISAC: Information Sharing and Analysis Center
 ISO: International Organization for Standardization
 IT: Information Technology
 ITS: Intelligent Transportation System

L

LAN: Local Area Network

N

NAS: National Airspace System
 NCSD: National Cybersecurity Division (DHS)
 NIAC: National Infrastructure Advisory Council
 NIST: National Institute of Standards and Technology

P

PASA: Preliminary Aircraft Safety Assessment	S
PASecA: Preliminary Aircraft Security Assessment	SAE: Society of Automotive Engineers
PID: Passenger Information Display	SCADA: Supervisory Control and Data Acquisition
PSSA: Preliminary System Safety Assessment	SSA: System Safety Assessment
PSSecA: Preliminary System Security Assessment	T
R	TSA: Transportation Security Administration
R&C: Research and Development	W
RTCA: Radio Technical Commission for Aeronautics	WAN: Wide Area Network
	WLAN: Wireless Local Area Network

Chapter 1

Introduction

Aviation security for information systems, or aviation cybersecurity, is a growing concern from all parts of the industry. For a long time, aviation safety took the front seat in all aspects of the aircraft life-cycle, because it was hard to conceive any cyber-threat happening. Now, the tables have turned, and aviation cybersecurity has been awarded a critical place in *airworthiness*.

In 2016, the United States Government proposed a bill “Cybersecurity Standards for Aircraft to Improve Resilience Act of 2016” (United States, 2016):

To require the disclosure of information relating to cyber attacks on aircraft systems and maintenance and ground support systems for aircraft, to identify and address cybersecurity vulnerabilities to the United States commercial aviation system, and for other purposes.

The bill urged the Federal Aviation Administration (FAA) to disclose any attempted or successful cyber attack on any system on board an aircraft, whether the system was safety-critical or not. It also announced the prescription of regulations to incorporate requirements relating to cybersecurity into the requirements for obtaining an air carrier operating certificate or production certificate. These requirements focused on having reasonable measures to protect against cyber attacks, periodic evaluations on these measures and updating them if necessary.

The U.S. National Airspace System (NAS), which is governed by the FAA, consist of a ground-based air traffic control system that directs aircraft traffic on the ground and in the air. And, while NAS already has a mature cybersecurity program in place, there is a need for a specific framework that allows certification of compliance and for aviation safety and security airworthiness. The framework needs to address safety and security from the early stages of the aircraft life-cycle to be able to consider the newly included elements in modern aircraft properly: electronic control systems and software (e.g., those used to operate airlines, entertain passengers, and control systems associated with airline information systems).

1.1 Statement of The Problem

The modern aircraft has a different design than it did when it was first imagined, and it has become an extraordinary complex integrated system of systems.

In addition, as definitions are getting broader and modern systems are getting more sophisticated, their modeling is also gaining complexity. It seems logical that safety-critical systems such as aircraft must be analyzed from these new perspectives that include safety and security altogether, since aircraft are now considered to be 'flying computers' that are susceptible to safety-critical issues as they are susceptible to cybersecurity threats.

There is also the ongoing aviation paradigm of *globalization*: aircraft systems move from one country to another and have to comply with regulations from their countries of origin, destination and all countries that they fly over. Therefore, not only aircraft must be analyzed from a safety and security perspective, that analysis also needs to prove compliance with all possible regulations.

The Problem Questions this thesis addresses are:

1. Do safety and security have to be approached separately, or can they be tackled together, especially when it comes to software-intensive systems such as aviation systems?
2. Which are the standards that information security for aviation systems has to adhere to for compliance?
3. How does the process of standardization and compliance work? How can a framework that complies with the standard be created?
4. Which methodologies are optimal for security engineering for aviation systems? Can they merge with trusted safety engineering methodologies for aviation systems?

Chapter 2

Literature Review

2.1 Introduction

The development of an aircraft and its systems is very complex. It follows the Systems Engineering process during its life-cycle. In (SAE-Aerospace, 2010), the conceptual aircraft/systems development process is explained 2.1:

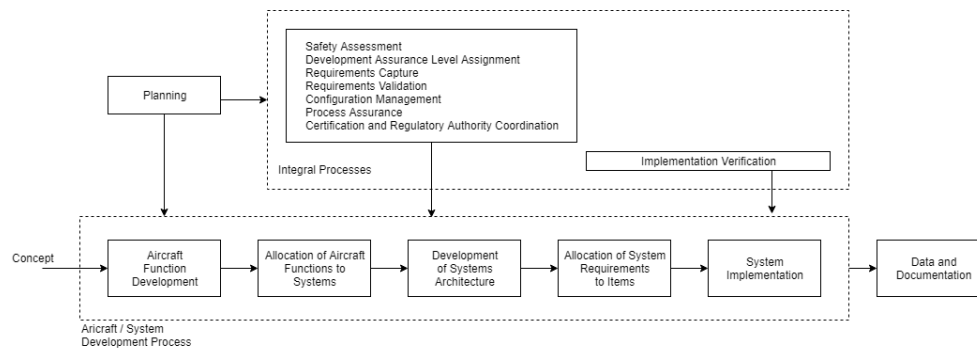


Figure 2.1: Aircraft or System Development Process Model (SAE-Aerospace, 2010)

In the standard, a generic approach is overviewed for developing aircraft and aircraft systems from conceptual definition to certification. The development life cycle has a beginning and an end, and can be re-entered to address aircraft or system changes.

And now the aircraft design and development has increased in complexity, due to the fact that the aircraft is interconnected: aircraft has network connectivity, and all of its subsystems are controlled by aviation electronic control systems and software. This leaves room for safety hazards and security vulnerabilities that could eliminate the airworthiness of an aircraft, in other words, make the aircraft unsuitable for flight operations. Therefore, a general overview of the new features (networks and connectivity) of the modern aircraft is needed:

Networks and Connectivity. In the design of the new generation of aircraft, there are new network connections to be considered: control systems associated with airline information services, passenger information and entertainment services. There are several connections that are provided by different internet service providers:

- Air-Ground Datalink Service (e.g. ACARS): uses Air Traffic Service providers and Airline Approved third party providers.
- Airport Network (e.g. GateLink): uses the Airline-Approved third party providers.
- Air-Ground Broadband Network (e.g. INMARSAT): uses Airline-Approved third party providers and Passenger-Accessed third party providers.

And there are several connections that allow for aircraft information interconnection:

- Control the Aircraft: it is in the Aircraft Control Domain. It uses VHF/H-F/SatCom.
- Operate the Aircraft: it contains the Airline Info Services and the Passengers Information and Entertainment Services Domain. It uses WirelessLAN and a Broadband/Cellular network.
- Passenger Use: it is in the Passenger-Owned Devices Domained.

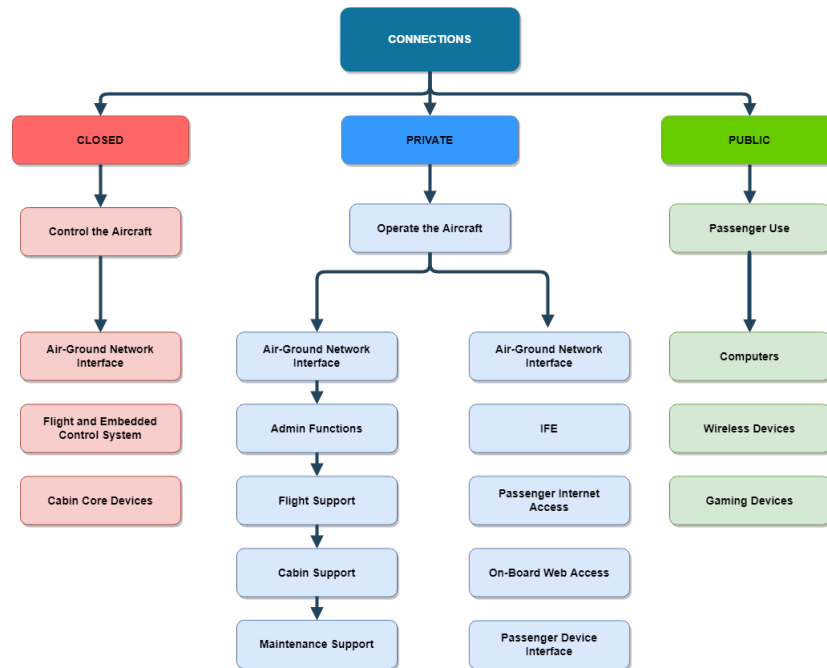


Figure 2.2: Aircraft Information Interconnections

2.1.1 Safety and Security Engineering

Safety and Security Co-Engineering. Historically, safety and security are two risk-driven activities that have been tackled separately; but, since new cybersecurity attacks are appearing every day, it is getting more and more recognized worldwide that both engineering specialties cannot continue to ignore each other.

In literature, (Paul and Rioux, 2015) provides a bibliography of research papers on safety and security (cybersecurity) co-engineering dating back to the early 90s. The author announces four common streams of research when it comes to the cross-fertilization between safety engineering and security engineering.

- **Treating issues related to safety engineering and security engineering separately:** The papers conclude that there is room for improvement for a possible co-engineering scenario, but they do not offer any clarification on how to achieve it. They might provide high-level recommendations on the directions in which there should be investigation, but they do not present the actual study. A peculiar conclusion is extracted from some papers that recall that even though safe systems were not explicitly designed to be secure, they often offer good properties against attacks.
- **Improving security engineering by adapting safety engineering techniques to security:** Since safety engineering is recognized as a more mature engineering specialty than security engineering, multiple papers present adaptations of safety engineering techniques into the security domain.
- **Extend the scope of safety engineering by adapting cybersecurity techniques:** The opposite of the previous research current, the papers push for adapting the overall good practices of cybersecurity to safety engineering.
- **Clean slate approach for co-engineering:** Not adapting any kind of technique from one discipline to the other, but starting to build new techniques that involve both of the disciplines.

(ITEA2, 2016) gives an overview of the instances in which safety and security co-engineering have resulted into positive results or prominent research in aviation systems, concluding that both disciplines -when adequately combined- can offer better results than when they are applied separately.

(Garcia et al., 2018) states that safety engineering cannot be understood as a standalone discipline that does not integrate nor correlate with security engineering, especially in safety-critical systems. As the systems elements keep increasing in complexity and offering more capabilities by becoming part of the Internet of Things, cybersecurity has to be a part of it since its conception and design.

Safety Assessment Process. (Balakrishnan, 2015) The safety assessment process is defined as a methodology to evaluate aircraft functions and the design of systems performing these functions to determine that the associated hazards for those functions have been properly addressed (Wang, 2017).

According to SAE ARP4761 (SAE-Aerospace, 1996), the safety assessment process in aviation includes other processes:

- **Functional Hazard Analysis (FHA):** should be carried out at both the aircraft and system levels. The goal in conducting this step is to clearly identify the circumstances and severity of each Failure Condition along with the rationale for its classification.

Aircraft FHA and System FHA refer to a systematic and comprehensive examination of aircraft or system functions to identify and classify the potential functional failure conditions according to the severity. The FHA is updated (a living document) throughout the development cycle.

- **Preliminary Aircraft / System Safety Assessment (PASA/PSSA):** it is a systematic evaluation of a proposed system architecture and implementation based on the Functional Hazard Assessment and failure condition classification to determine safety requirements for all items.

The PASA and PSSA is also a comprehensive examination of a proposed aircraft or system architecture to determine how failures can lead to the aircraft or system level failure conditions. In the PASA and PSSA requirements for the lower levels are established, and the PASA and PSSA are also updated throughout the development process.

- **Aircraft / System Safety Assessment (ASA / SSA):** A systematic, comprehensive evaluation of the implemented system to show that the relevant requirements are met. It shows that safety objectives from the Aircraft or System FHA and relevant requirements established by the PASA and PSSA are satisfied.

Security Assessment Process for Aviation Systems. The security assessment process is defined as a methodology to evaluate systems' design and system functions to discover the threats that these have associated and determine that they have been mitigated. The same way the safety assessment process had several processes to analyze and evaluate hazards, the security assessment process has several techniques to analyze and evaluate threats.

For the security assessment process, different methodologies are used: threat modeling and risk modeling techniques, which involve identifying, quantifying and addressing security risks that are associated with the system, in this case, the aircraft and all of its systems and items.

2.2 Certification and Standards

Regulatory Framework and Air Law. As (Kolle et al., 2015) explains, there is one problem with regulation and legislation when it comes to air law. A plane can leave the United States, with cargo from Brazil, heading to the European Union, and it has to comply with all regulation and laws (both international and local). This presents a paradigm of regulation and standardization that was not considered when the aircraft was first designed for commercial flight.

A conference for the formulation of international air law was held in Paris in 1900. However, international air travel only became a reality after World War I (1914 – 1918). The legal framework for international civil aviation first appears in October 1919. Twenty-six participants of the Paris Peace Conference signed the Convention for the Regulation of Aerial Navigation (Paris Convention). The Paris Convention coined the principle that every state has the absolute and exclusive sovereignty over the airspace above its territory. Later, fifty-four nations met in Chicago from November to December 1944 to “make arrangements for the establishment of world air routes and associated services” and “to set up an interim council to collect, record, and study data concerning international aviation with the aim to make recommendations for its improvement”. The Conference was also invited to “discuss the principles and methods to be followed in the adoption of a new aviation convention”. It also led to the creation of the agency of the International Civil Aviation Organization (ICAO). In 1947, ICAO became a United Nations specialized agency, even though it remained an independent and autonomous agency.

Three of the most relevant articles of the Chicago Convention, article 31 (Certificates of Airworthiness), article 32 (Licenses of personnel) and article 33 (Recognition of Certificates and Licenses) provide a collection of rules that allow for aircraft certification of airworthiness to be issued, provided by single states and also allow for those same certifications to be recognized by other states, as long as the requirements under which they have been issued are equal or above the minimum standards which may be established by ICAO. Therefore, a framework of regulatory oversight between states, operators, services providers and maintenance organizations was created. The relationships are shown in the following table 2.1.

The aforementioned regulatory legislative framework needs to make a clear distinction: the difference between a regulation and a standard. To answer this (ibid.), (Abeyratne, 2010), the concept of ‘hard law’ and ‘soft law’ of aviation need to be addressed. In aviation law, administrative law and decisions can have different names and come from different fields, and those are broken down into technical specifications, acceptable means of compliance and guidance material. Hard law is those regulations by authorities and government, which are legally binding in nature. Soft law refers to the non-legally binding nature of technical specifications and guidance

Table 2.1: Regulatory Framework.

Regulatory Legislative Framework		Actor	Action
International Conventions and Aviation Law		Government	Oversight
National Law	Regional Rules and Law	Government Authorities	Oversight
National Regulation	Regional Regulation	Authorities	Establish Rules and Requirements
National Law		Service Providers Manufacturers	Compliance

material. Even though they are not legally binding, they provide standardization and implementation of rules and requirements stipulated by regulations. In a way, ‘soft law’ is a detailed version of the simple and brief rules that make ‘hard law’.

Figure 2.2 shows the entities that are in charge of managing the different documents (e.g. regulations, specifications, standards) of aviation law:

Table 2.2: Hard law and soft law entities.

Law	Documents	Entity
Hard Law	International Convention / Law	ICAO
Hard Law	Regulation, Implementation Rules	FAA - EASA
Hard Law / Soft Law	Standards Technical Specification	EUROCAE - RTCA ARINC
Soft Law	Acceptable Means of Compliance	FAA - EASA
Soft Law	Guidance Materials	EUROCAE - RTCA

Cybersecurity Regulations. (Abeyratne, 2010) The Aviation Security Panel of ICAO met at its Twentieth Meeting in Montreal from 30 March to 3 April 2009. The Panel noted that significant progress in efforts to proactively identify vulnerabilities and potential gaps in existing measures had been made, but it was not enough: Annex 17 (Aviation Security) of the Convention on International Civil Aviation (Chicago Convention) was lacking in provisions for cyber-attacks. It was established that the threat of cyber-attacks was significant, and redacted a proposal to include a Recommended Practice in Annex 17 to ensure that information and communication technology systems used for civil aviation purposes would be protected from cyber attacks.

Standardization. (Pearson and Riley, 2015) The FAA is authorized to make rules regarding aviation. The agency’s rule-making procedures are found in 14 CFR Part 11. The FAA’s rule-making activities encompass all of the agency’s areas of responsibility, including air traffic control, aviation security, etc.

Figure 2.3 is a graphic representation of the process that the FAA follows when making significant rules.

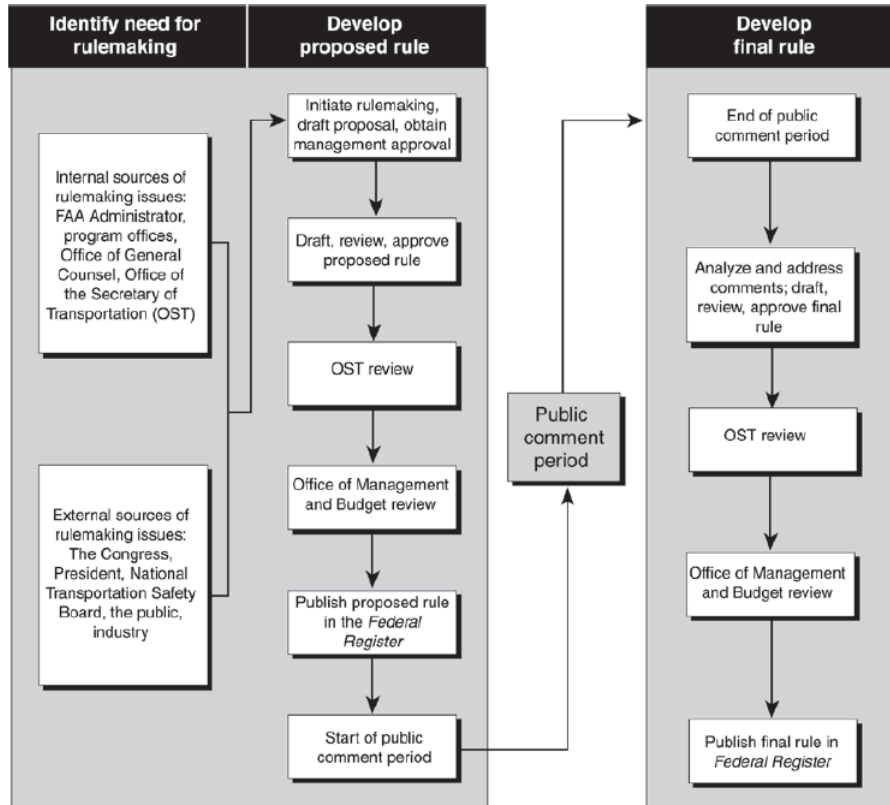


Figure 2.3: FAA Rule-making. (Pearson and Riley, 2015)

Regulations. The Code of Federal Regulations (CFR) is the codification, compilation and classification of the general and permanent rules and regulations published in the Federal Register by the executive departments and agencies of the Federal Government of the United States. In aviation airworthiness, 14 CFR, Advisory Circulars (AC) and Airworthiness Directives (AD) are the most relevant regulations that to be considered.

- **14 CFR.** The Federal Aviation Regulations are found in Title 14 of the Code of Federal Regulations (14 CFR). Since 1958, these rules have typically been referred to as “FARs,” short for Federal Aviation Regulations.
- **Advisory Circulars.** The FAA issues Advisory Circulars (ACs) to inform the aviation public in a systematic way of non-regulatory material. Unless incorporated into a regulation by reference, the contents of an advisory circular are not binding on the public. For example, (CAAS, 2017), (AIRCRAFT NETWORK

SECURITY PROGRAMME (ANSP)) and (Civil Aviation Safety Authority, 2016) (AC 20-01 Software configuration management).

- **Airworthiness Directives.** In accordance with Part 39 of Title 14 of the Code of Federal Regulations, the FAA issues Airworthiness Directives (ADs) in response to deficiencies and/or unsafe conditions found in aircraft, engines, propellers, or other aircraft parts. ADs require that the relevant problem must be corrected on all aircraft or aircraft parts using the same design.

Certification and Accreditation. The process of certification for Information Security, in aviation industry or any other industry that requires rigorous certification and accreditation. In order to understand C&A, it is important to distinguish between certification and accreditation.

- Certification: is the technical evaluation of the security components and their compliance for the purpose of accreditation.
- Accreditation: is the formal acceptance of the adequacy of the system's overall security by the management.

In (InfoSec, 2003) it is announced that going through the formal process of Certification and Accreditation (C&A) insures that a clearly established set of Security Requirements is developed and implemented, any residual risk is minimized and clearly understood, and all aspects of the development and deployment of security controls and policies are described in the System Authority Authorization Agreement (SSAA).

The C&A process is defined by using a four phase approach: definition, verification, validation, and post accreditation. Their tasks are:

1. A list of guidance documents is compiled from all applicable directives and policy guidelines to define the rules that the C&A process will follow, and to help define a set of Security Requirements for the system.
2. Persons and organizations are chosen to fill the roles defined by the C&A guidance documents
3. The scope of the system being certified is determined.
4. A list of Security Requirements that are relevant to the system are created based on the chosen guidance documents.
5. A System Security Authorization Agreement (SSAA) document is created containing all of the relevant information about the system.
6. A set of test procedures are developed from the security requirements.
7. A System Test and Evaluation (ST&E) is performed by the certifiers, and a report of the relevant findings is generated.

8. Once all of the security findings are sufficiently addressed and verified, a Risk Assessment is performed to describe the severity of the residual risk.
9. A recommendation is made by the Certifiers to the Designated Approving Authority (DAA).
10. The system is either accredited, granted an Interim Authority to Operate, or denied accreditation by the DAA.

In Aviation Systems, according to the guide (AIA et al., 2017), there have been significant changes in the certification processes over the last 10-15 years to improve the efficiency and effectiveness of the certification and design approval processes to enhance product safety.

The guide allows an applicant to: (1) lay out the information in such a way that an Applicant can understand the basic expectations and best practices for achieving a successful product approval process (2) provide experienced Applicants with guidance on how to move along the path toward a more systematic and mature process for product certification or approval (3) provide all stakeholders, including FAA staff, with the knowledge of how to maximize the potential of the existing processes in conducting efficient certification processes while maintaining the systems' health through risk based oversight through the use of the tools in this Guide.

Standards. According to (Kaiser, 2013) there are a several cybersecurity standards that are currently in place and others that are being developed to provide guidelines:

Organization	Title	Summary	Status
FAA	Information Security Certification and Accreditation (C&A) Handbook	The primary source of procedures and guidance that supports the C&A process in protecting the confidentiality, integrity, and availability of FAA's information that is collected, processed, transmitted, stored, or disseminated in its general support systems, major applications, ICSs, and other applications.	Published
RTCA	Airworthiness Security Methods and Considerations	This document is a resource for certification authorities and the aviation industry for developing or modifying aircraft systems and equipment when there is the possibility of danger to flight from volitional human action involving information or information system interfaces. It presents permissible methodologies to meet the data requirements and compliance objectives of an airworthiness security process.	Published
RTCA	Airworthiness Security Process Specification	The first of a series of documents on aeronautical systems security that together will address information security for the overall Aeronautical Information System Security (AISS) of airborne systems with related ground systems and environment. This document addresses only aircraft type certification and is not yet widely implemented, but is derived from understood best practices.	Published
AEEC	Guidelines for the Incorporation of Cyber Security in the Development of AEEC Documents	This Technical Application Bulletin represents the 2009-current cyber security thinking and experience useful in the development of further AEEC specifications. The intent is to periodically update the cyber security guidelines and disseminate them to AEEC Subcommittees as conditions warrant.	Review
ARINC	ARINC 811: Commercial Aircraft Information Security Concepts of Operation and Process Framework	The purpose of this document is to facilitate an understanding of aircraft information security and to develop aircraft information security operational concepts. This document also provides an aircraft information security process framework relating to airline operational needs that, when implemented by an airline and its suppliers, will enable the safe and secure dispatch of the aircraft in a timely manner. This framework facilitates development of cost-effective aircraft information security and provides a common language for understanding security needs.	Published

Comprehensive list of all authorities and the standards and guidelines that are referred when it comes to Information Security in Aviation Systems:

- **AIAA:** (AIAA, 2013) presents a Framework for Aviation Cybersecurity. It highlightens the need for a cybersecurity framework for aviation. The first steps to achieve it are:
 1. Establish common cyber standards for aviation systems.
 2. Establish a cybersecurity culture.
 3. Understand the threat.
- **(AEEC) ARINC:** In (Infrastructure and WG, 2012) a list of all ARINC Standards that are used to support the design and development of aircraft systems, avionics, networks and information security are listed and explained. It argues that the more consistently all elements work together over the aircraft life-cycle, the better. Its main security process (that offers an overview of aircraft security and the proper security considerations) is provided by ARINC Report 811 (Olive et al., 2007).
- **NIST:** For risk management, (Barrett et al., 2017) proposes a following the National Institute of Standards and Technology Institute Special Publication 800-x Series. NIST is responsible for developing standards and guidelines – including minimum requirements – to provide adequate information security for federal information and information systems. This suite of security and privacy risk management standards and guidelines provides guidance for an integrated, organization-wide program to manage information security risk. (NHTSA, 2014) and (NIST, 2017) have presented an Information Security Framework that works for automotives systems.
- **FAA:** (Administration, 2006) presents a public guideline for the Certification and Accreditation of all information systems owned or managed by the federal government. This Handbook describes the process that all FAA organizations must follow to conduct C&A. This handbook is required by FAA Order 1370.82, as amended, for the implementation of the FAA’s Information Systems Security Program defined in that order.
- **RTCA:** A list of all the RTCA standard documents published to date can be seen in (RTCA, 2016). RTCA, Inc. is a not-for-profit corporation formed to advance the art and science of aviation and aviation electronic systems for the benefit of the public. The organization functions as a Federal advisory committee and develops consensus-based recommendations on contemporary aviation issues.

RTCA’s goals include (1) combine aviation system user and provider technical requirements, knowledge and practices in a manner that helps government and

industry meet their mutual objectives and responsibilities (2) analyzing and recommending solutions to system technical issues (3) development of consensus on the application of pertinent technology to fulfill user and provider requirements and (4) assisting in developing the appropriate technical material upon which positions for the International Civil Aviation Organization.

RTCA has a set of standards (known as DO-326A set) for Security Airworthiness:

1. **DO-326A:** (RTCA DO-326A, 2014), previously (RTCA DO-326, 2010), states that the document:

[...] is a resource for Airworthiness Authorities (AA) and the aviation industry for certification when the development or modification of aircraft systems and the effects of intentional unauthorized electronic interaction can affect aircraft safety. It deals with the activities that need to be performed in support of the airworthiness process when it comes to the threat of intentional unauthorized electronic interaction [...]

[...] adds to current guidance for aircraft certification to handle the threat of intentional unauthorized electronic interaction to aircraft safety. It adds data requirements and compliance objectives, as organized by generic activities for aircraft development and certification, to handle the threat of unauthorized interaction to aircraft safety and is intended to be used in conjunction with other applicable guidance material, including SAE ARP 4754A, DO-178C, and DO-254.

2. **DO-356A:** (RTCA DO-356A, 2017), previously (RTCA DO-356, 2014), is a companion document of DO-326A that proposes methodologies to achieve the objectives and certification of Security Airworthiness. The document states:

[...] provides a set of methods and guidelines that may be used within the airworthiness security process defined in ED-202A / DO-326A. It is recognized that alternative methods to the processes described or references in this document may be available to an organization desiring to obtain certification.

3. **DO-355:** (RTCA DO-355, 2014) is a companion document of the DO-326A set that provides guidelines for aviation airworthiness once the aircraft has already been developed and is in service ongoing. It states:

[...] s a resource for civil aviation authorities and the aviation industry when the operation and maintenance of aircraft and the effects of information security threats can affect aircraft safety. It deals with the activities that need to be performed in operation and maintenance of the aircraft related to information security threats. This document gives also guidance that is related to operational and commercial effects (i.e. guidance that exceeds the safety-only effects).[...]

[...] addresses information security risks only. The security measures to mitigate these risks are not limited to information technology; they may also be physical or organizational. Apart from the classical Instructions for Continued Airworthiness that are directly related to aircraft parts and systems, this document also provides guidance on Ground Support Equipment and Ground Support Information Systems that are related to the security of aircraft information systems and data networks.

Since it is hypothesized that security and safety should go hand-in-hand, an overview of safety standards that are adaptable to security standards (RTCA standards and guidelines) is provided in Figure 2.4. The RTCA has released DO-178C and DO-278A as certification guidance for the production of airborne and ground-based air traffic management software, respectively. Additionally, RTCA has also produced at the same time, five other companion documents. These documents are RTCA DO-248C, DO-330, DO-331, DO-332, and DO-333. These supplements address issues about software certification, provide guidance on tool qualification requirements, and illustrate the modifications recommended to DO-178C when using model-based software design, object oriented programming, and formal methods.

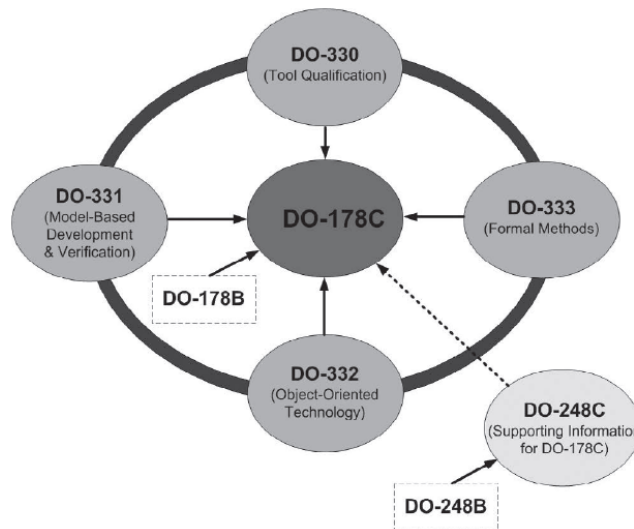


Figure 2.4: 178C set and its supplementary documents.

- **DO-178C:** (RTCA DO-178C, 2011) provides the aviation community with guidance for determining, in a consistent manner and with an acceptable level of confidence, that the software aspects of airborne systems and equipment comply with airworthiness requirements.
- **DO-330:** (RTCA DO-330, 2011) provides tool qualification guidance. It was developed to provide tool-specific guidance for developers of software and tool users, and provides examples of guidance for DO-178C and DO-278A.
- **DO-333:** (RTCA DO-333, 2011) provides guidance for the adoption of Formal Methods into an established set of processes for development and verification. The extent to which formal methods are used to satisfy the objectives of DO-178C can vary according to aspects such as preferences of the program management or choice of techniques specified in the document.
- **DO-254:** (RTCA DO-254, 2000) provides guidance for design assurance of airborne electronic hardware from conception through initial certification and subsequent post certification product improvements to ensure continued airworthiness.

As it is seen, there are different aspects that play a role into standardization: which authority and/or agency is publicizing the standard/guidelines and how they build a framework for information security for aviation or security airworthiness.

Aircraft Systems Development. There are also technical reports, standards and guidelines that are followed to develop the entirety of the aircraft systems. Those standards/recommendations are combined with the previously mentioned security standards and guidelines (RTCA DO-326A set) to achieve security airworthiness in the aircraft life-cycle.

- **SAE ARP4754A:** (SAE-Aerospace, 2010) document states:

[...]discusses the development of aircraft systems taking into account the overall aircraft operating environment and functions. This includes validation of requirements and verification of the design implementation for certification and product assurance.

[...] It provides practices for showing compliance with the regulations and serves to assist a company in developing and meeting its own internal standards by considering the guidelines herein. This document addresses the development cycle for aircraft and systems that implement aircraft functions [...].

- **SAE ARP4761A:** (SAE-Aerospace, 1996) document states:

[...] describes guidelines and methods of performing the safety assessment for certification of civil aircraft. The methods outlined here identify a systematic means, but not the only means, to show compliance.[...]

[...] presents guidelines for conducting an industry accepted safety assessment consisting of Functional Hazard Assessment (FHA), Preliminary System Safety Assessment (PSSA), and System Safety Assessment (SSA). This document also presents information on the safety analysis methods needed to conduct the safety assessment. These methods include the Fault Tree Analysis (FTA), Dependence Diagram (DD), Markov Analysis (MA), Failure Modes and Effect Analysis (FMEA), Failure Modes and Effects Summary (FMES) and Common Cause Analysis (CCA). [CCA is composed of Zonal Safety Analysis (ZSA), Particular Risks Analysis (PRA), and Common Mode Analysis (CMA). [...]

- **SAE ARP5150A:** (SAE-Aerospace, 2013a) document states:

[...] describes guidelines, methods, and tools used to perform the ongoing safety assessment process for transport airplanes in commercial service (hereafter, termed “airplane”). The process described herein is intended to support an overall safety management program. It is associated with showing compliance with the regulations, and also with assuring a company that it meets its own internal standards.[...]

[...] provides a systematic process to measure and monitor safety to help determine safety priorities and focus available resources in areas that offer the greatest potential to improve aviation safety. [...]

- **SAE ARP5151:** (SAE-Aerospace, 2013b) document states:

[...] provides a systematic process for assessing ongoing safety of General Aviation airplanes and Rotorcraft (GAR). This process is intended to assist in focusing available resources in areas that maximize the potential to improve commercial aviation safety.[...]

[...] To improve safety during the complete aircraft life cycle, it is not sufficient to assess the safety of the aircraft only during its design phase. Ongoing aircraft operations should be evaluated for safety (e.g., maintenance or operation procedures) [...]

2.3 Security Assessment

Methodologies and Techniques. As mentioned in the beginning of the chapter, there is a research current that tries to apply well-known safety engineering techniques to security engineering.

It seems to be a common pattern for safety/security approaches to introduce the concept of Tree Analysis. For safety assessment, Fault Tree Analysis is most common, and specified in SAE ARP4761. For security assessment, there are Attack Trees and Threat Trees.

Fault Tree Analysis was developed to represent possible ways a system could fail as a result of component or subsystem failures. It uses Boolean logic operations to represent how such failures are interrelated, and how they could result in failure. They are represented as networks of Boolean logic operators where a fault is considered to either have occurred or not occurred. Attack Trees or Threat trees are similar to fault trees but focus only on the security of a system and are an enumeration of possible attacks. The root of an attack tree represents a successful attack and the leaf nodes represent ways of achieving the planned attack. Like fault trees, attack trees also rely on binary-valued algebras (Ongsakorn et al., 2010).

In (Kornecki and Liu, 2013), a Fault Tree Analysis (FTA) for Safety/Security verification in Aviation Software is presented. It aims to go from Hazards and Threat to the requirements specification. It argues that, since the requirements are most probably the element that makes a project succeed or fail (in terms of development), it will find requirements using a well-known technique (Fault Tree Analysis). To test its theory, it applies FTA to the analysis of a component of NextGen simulation (ASN Gateway); building the appropriate FTA models to develop safety/security requirements. The paper's main contribution is to show how application of the FTA technique leads to identification of safety and security requirements of the gateway and, subsequently, proposing appropriate mitigation. Its chosen measurable and repeatable scientific elements applicable to assuring the security of software systems included: threats, vulnerabilities, security violations, attack integrity confidentiality, among others.

(Ongsakorn et al., 2010) introduces a new type of tree: Cyber Threat Trees. They are a superset of Fault and Attack trees since they are based on multiple-valued or radix- p valued algebras over a finite and discrete set of values. For example, when the radix $p=2$, the cyber threat tree reduces to a fault or attack tree depending on the nature of the disruptive events. It explains that cyber threat trees have usually $p \geq 2$ to allow for more complicated interactions to be modeled.

In addition to Attack Trees to model threat scenarios, there are also Attack-Defense Trees (ADT), as presented in (Aslanyan and Nielson, 2015). An ADT describes the interaction between an attacker and a defender, and is evaluated by assigning parameters to the nodes, such as probability or cost of attacks and defences. Attack-Defence Trees are a useful tool to study attack-defence scenarios and present the interaction between an attacker and a defender in an intuitive way. It argues that in cases of multiple parameters, most analytic methods optimize one parameter at a time, (for example, minimize cost or maximize probability of an attack); and that leads to sub-optimal solutions when the two parameters that have to be optimized are conflicting parameters. The paper presents evaluation techniques for multi-parameter ADT that optimize all parameters at once.

Fault Tree Analysis is not the only safety assessment methodology that is analogously implemented in security assessment. In (Schmittner et al., 2014), the security adapted version of Failure Mode and Effect Analysis is proposed: Failure Mode, Vulnerabilities and Effects Analysis (FMVEA). The Failure Mode and Effect Analysis (FMEA) is a structured technique which investigates failure modes and their effects. The aim is to identify potential weaknesses and improve reliability, availability or safety. A system or process is hierarchically decomposed into its basic elements and then the failure modes of the elements are examined for causes and effects.

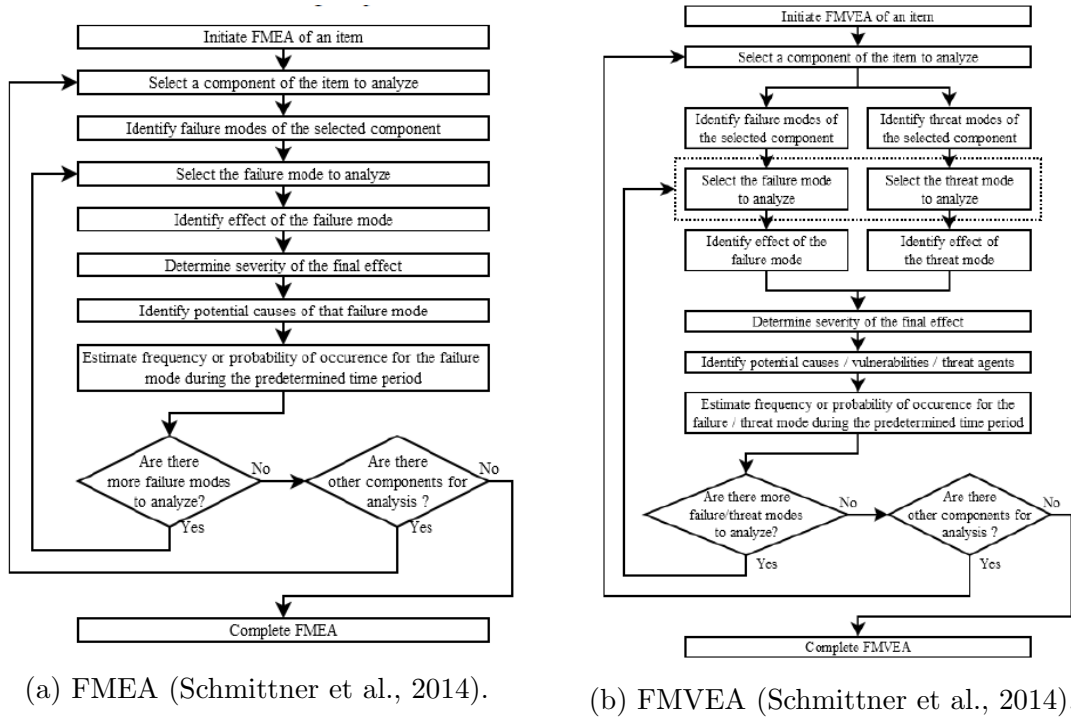


Figure 2.5: Comparison between the two methodologies.

The process to achieve FMEA is described in Figure 2.5a, whereas in Figure 2.5b the process has been adapted to include security in the analysis (FMVEA). As it has been stated throughout this chapter, there are different ways in which security and safety properties of a system can influence one another. Therefore, while the consideration of failure or threat modes of an item is split, the analysis of effects and causes combines both viewpoints.

Another technique used in safety that is applied in security appears in (Jimenez et al., 2017). It consists in the generation of checklists for standards; arguing it can be considered as a "best practice" which provides a set of notes and conclusions to the reviewer (in the end these items will serve to detect and fix defects). Nowadays, most companies have checklists applicable to its specific development methodology but not focused on this any type of standards. Depending on the standard, the complexity of the checklist can increase exponentially, that is why it proposed a set of checklists for the newest revision of RTCA DO-178C and DO-278A.

Threat Modeling. Threat modeling is an activity for creating an abstraction of a software system—aimed at identifying attackers' abilities, motivations, and goals—and using it to generate and catalog possible threats. As defined in (Shostack, 2014), there are very important reasons to threat model in the design phase:

- **Find Security Bugs Early:** Threat modeling can help you find design issues even before software has been developed or implemented.
- **Understand Security Requirements:** As threats are found and there is an assessment of how they are going to be mitigated, requirements become more clear. With more clear requirements, a consistent set of security features and properties can be build. In threat modeling, there is an important interplay between requirements, threats, and mitigations.
- **Engineer and Deliver Better Products:** When requirements and design are considered along with threats, there is a significant lower probability of having to re-design due to security bugs.
- **Address Issues Other Techniques Will Not:** Threat modeling can lead you to categories of issues that other tools will not find, e.g. errors of omission, failure to authenticate a connection. That's not something that a code analysis tool is going to determine.

In (Shull, 2016), Carnegie Mellon University prepared a comparison and evaluation of threat modeling methodologies: STRIDE, Security Cards and Personan non Grata (PnG). The most common is STRIDE, even though the evaluation does not conclude is the best threat modeling methodology.

STRIDE The STRIDE model was developed by Microsoft *STRIDE* n.d. as a threat risk modeling technique. The STRIDE model considers the effect of each threat type and assumes the cause of each threat will be uncovered during analysis activities. It is the responsibility of the individuals performing threat modeling and analysis to discover and describe the cause and effect of threats and attack vectors, which requires the unique context of a system under analysis. When STRIDE is applied to an application, one should consider how each of the threats in the model affects each component and each of its connections or relationships with other application components. STRIDE is composed by S, T, R, I, D, and E threat categories, which stand for:

- Spoofing Identity.
- Tampering with data.
- Repudiation.
- Information disclosure.
- Denial of service.
- Elevation of privilege.

DREAD. DREAD is another threat risk model that can complement the preliminary analysis in STRIDE, that was used previously in Microsoft. DREAD is a model also based on categorizing threats as D, R, E, A and D, but they are analyzed from a different point of view. These dimensions help determine what the impact of these security threat really mean. DREAD modeling influences the thinking behind setting the risk rating and can be used directly to categorize the risks. The DREAD algorithm (3.1) is used to compute a risk value, which is an average of all five categories *OWASP* n.d.

- Damage potential.
- Reproducibility.
- Exploitability.
- Affected users.
- Discoverability.

There is not a consensus on how the actual risk point scale should be, since it all depends on the individuals performing the thread modeling. It is recommended to not have a large scale (e.g. from 0 to 10). For example, a simple scheme would be: High (10 points), Medium (5 points), and Low (0 points) when it comes to Damage

potential, and Hard (0 points), Medium (5 points), Easy (0 points) when it comes to Reproducibility. After, all points are computed and result into a risk value:

$$RiskDREAD = \frac{D + R + E + A + D}{5} \quad (2.1)$$

Trustworthiness. Trustworthiness by definition used to interchangeable with dependability, before the complexity of interconnected systems increased drastically. While this is nowadays still accurate, the definition of trustworthiness has expanded to include privacy and cybersecurity when applicable. Dependability, which in its turn includes safety, reliability, availability and security, has also evolved since the introduction of information systems embedded into everyday objects (Garcia et al., 2018).

Therefore, trustworthiness is now also an implicit requirement of the Security Assessment. In (R. F. Babiceanu and R. Seker, 2017) and (Radu F. Babiceanu and Remzi Seker, 2017), different trustworthiness frameworks are developed to enhance the establishment of the requirements in cyber-physical systems and small Unmanned Aerial Systems.

Chapter 3

Discussion

Aviation systems are complex systems. They are usually broken down to simpler sub-systems which perform the same task, for example, 'Communication'. Almost all aviation systems are tied to one or more avionics functions, which increase their complexity and cost.

That is why their design, development, testing, verification and certification has become also increasingly more complicated. But, no matter how complex aviation systems are, their main purpose is to ensure airworthiness of the aircraft.

Airworthiness is the measure of an aircraft's suitability for safe flight, as defined in (RTCA DO-326A, 2014).

It is the measure in which the aircraft service is attested to throughout its own life-cycle: (1) aircraft operators use Airworthiness as the principal certification instrument (2) aircraft manufacturers have to prove through a stage-based approach that the design and development of the aircraft have resulted in an aircraft that can be safely operated (3) airline operators have to ensure continued airworthiness through the establishment of processes for operations and maintenance.

Therefore, if a framework were to be implemented to assure airworthiness in aviation systems, which standards, guidelines, regulations should it comply with?

Furthermore, it has been established that in the current networked aviation paradigm an aircraft's suitability for a safe flight does not only include safety engineering, but security engineering as well. There is a need for both disciplines to be applied in the aircraft life-cycle; but can the safety assurance process for Airworthiness be done in coordination with the security assessment process?

3.1 Standards and Certification

To be able to develop and implement a framework for information security for aviation systems, the current security standards had to be analyzed. As seen in the previous chapter, there are a significant number of security standards that one could choose from to start building a security framework. But, depending on which standards are chosen, how do we make sure they guarantee airworthiness?

3.1.1 Standard

Standards arise from Aviation's "hard law", and are meant to be compliant with (1) international conventions (2) international laws and (3) regulations and implementation rules.

For airworthiness, the following regulatory framework is applied 3.1:

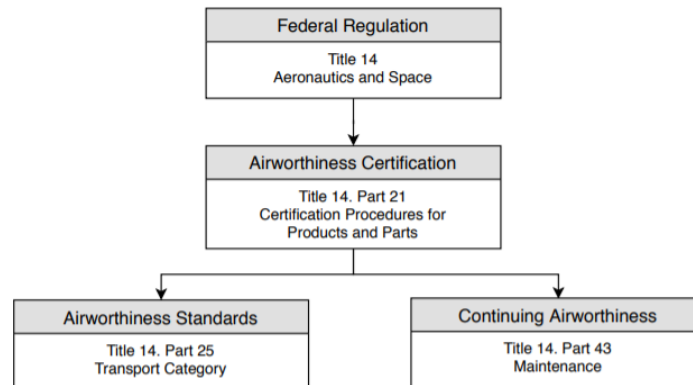


Figure 3.1: Framework for Aviation Airworthiness (United States)

Industry standards are defined and accepted as the minimum requirements in order to comply with an industry code of practices or regulations; therefore, standards are a means of regulatory compliance. In other words, operators and service providers that are being trusted to comply with regulation and legislation will not procure systems do not adhere or that are not produced according to a minimum set of practices and demonstrate required performance.

For the purpose of the framework design, the RTCA Security Process Airworthiness Standards are chosen. They define Airworthiness security as:

[...] Airworthiness security is the protection of the airworthiness of an aircraft from intentional unauthorized electronic interaction. Existing safety processes have not had to consider intentional disruption. Intentional unauthorized electronic interaction (also known as "unauthorized interaction") is defined as human-initiated

actions with the potential to affect the aircraft due to unauthorized access, use, disclosure, denial, disruption, modification, or destruction of electronic information or electronic aircraft system interfaces. This definition includes the effects of malware on infected devices and the logical effects of external systems on aircraft systems, but does not include physical attacks or electromagnetic jamming.

In 2010, RTCA developed the Airworthiness Security Process Specification (RTCA DO-326, 2010), a first document intended to increase current guidance for aircraft certification to handle the information security threats to aircraft safety. The document established compliance objectives and data requirements paralleled with the expected activities for aircraft development and certification. The document was later updated (Airworthiness Security Process Specification, RTCA DO-326A, 2014), and currently offers guidance for aircraft certification to handle threats of intentional unauthorized electronic interaction to aircraft safety. At the same time, RTCA developed another document, the Information Security Guidance for Continuing Airworthiness (RTCA DO-355, 2014), which addresses concerns regarding continuing airworthiness and development. The document became a resourceful guideline for the operation and maintenance of an aircraft, and the actions that need to be taken during those stages related to information security threats. It also acknowledges the effects of information security threats that could affect aircraft safety. Another document, Airworthiness Security Methods and Considerations (RTCA DO-356, 2014) provides guidance in the areas of Security Risk Assessment and Analysis, and Effectiveness Assurance, which were previously identified in RTCA DO-326, and presents methodologies for Security Risk Analysis and Network Security Domains.

The primary goal of the RTCA DO-326A, DO-355 and DO-356A standards was to provide a much-needed framework for Airworthiness Security that was also intended to be part of the Systems Engineering and system life-cycle. This allows for a sense of holistic security in airworthiness certification, which was not previously provided, since most security standards that were previously published did not strive to achieve a well-rounded framework to cover the complete spectrum of the system's life-cycle, and it can be mapped onto a system engineering perspective. This includes the certification of the assessment of the system for compliance with the appropriate aviation rules. Airworthiness certificates are issued for aircraft that are built (designed and assembled) according to accepted standards by a holder of a production certificate for manufacturing and based on evidence (standard practices/methods, testing) of compliance with a type certificate.

The RTCA DO-326A, DO-355 and DO-356A standards have a rather complex relation with other existing standards, technical reports and regulations for aviation security. Therefore, a relation framework overview is needed to understand the intricacies of information security standards and documents 3.2:

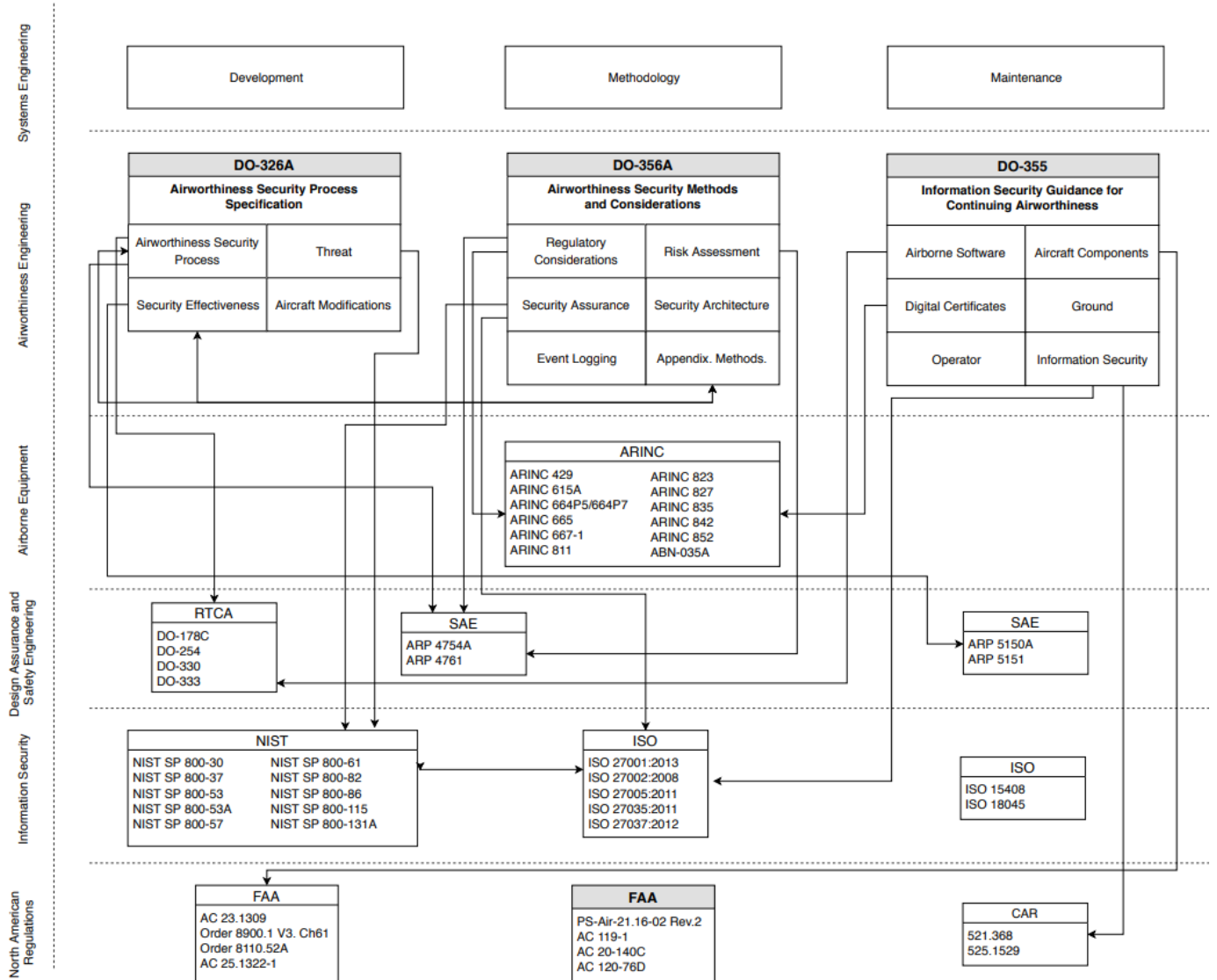


Figure 3.2: Relations between Security Standards in Airworthiness Engineering.

Standards integrated with the Systems Engineering approach:

- **Development (*RTCA DO-326A - Airworthiness Security Process Specification*):** Standards and technical specifications for the development of aviation systems, software and hardware. *RTCA DO-178C - Software Considerations in Airborne Systems and Equipment Certification* and *RTCA DO-254 - Design Assurance Guidance for Airborne Electronic Hardware*; and their corresponding supplement documents and considerations *RTCA DO-330 - Software Tool Qualification Considerations* and *RTCA DO-333 - Formal Methods Supplement to DO-178C and DO-278A*.

- **Methodology (*RTCA DO-356A - Airworthiness Security Methods and Considerations*):** Standards, technical specifications and guidance material that describe/propose methodologies for security and safety. *SAE ARP4754A - Guidelines for Development of Civil Aircraft and Systems* and *SAE ARP4761 - Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems Equipment* are guidelines for safety for the development of the aircraft. Whereas the ARINC documents are technical specifications for industry; they are referenced in the RTCA standards in regards to technical aspects.
- **Maintenance (*RTCA DO-355 - Information Security Guidance for Continuing Airworthiness*):** Standards, guidelines and technical specifications that focus on ongoing service. *SAE ARP 5150A - Safety Assessment of Transport Airplanes in Commercial Service* and *SAE ARP 5151 - Safety Assessment of General Aviation Aircraft and Rotorcraft in commercial use*.

They are also classified in the following groups:

- **Airworthiness Engineering:** Engineering discipline that contains the processes that ensure the aircraft's suitability for safe flight.
- **Airborne Equipment:** Avionics.
- **Design Assurance and Safety Engineering:** Safety assurance for aviation systems.
- **Information Security:** Information Security frameworks that are not aviation industry specific.
- **North American Regulations:** Regulations that play a substantial part in airworthiness security in North America (United States of American and Canada).

The RTCA DO-326A set guideline documents and standards are intended to be used with other development assurance activities described in the previous chapter, outlined in frameworks and standards such as SAE ARP 4754A, SAE ARP 4761, RTCA DO-178C, and RTCA DO-254, in substantiation of compliance to the applicable Code of Federal Regulations.

3.1.2 Means of Compliance

Acceptable means of compliance (AMC) target the uniform application and implementation of the regulation. The principal purpose of AMCs is to further qualify material used for certification and demonstrate compliance with these requirements. Although regulated entities are not bound by AMCs and may choose to demonstrate

compliance through other means, AMCs provide a means to the presumption of compliance.

In our case, Means of Compliance for Security Airworthiness would result in regulations referring to the Security Airworthiness standards RTCA DO-326A, DO-355, DO-356A and providing evidence of complying with those standards.

- FAA AC 119-1: (2015) Airworthiness and Operational Authorization of Aircraft Network Security Program (ANSP).
- FAA AC 20-140C: (2016) Guidelines for Design Approval of Aircraft Data Link Communication Systems Supporting Air Traffic Services (ATS).
- FAA PS-Air-21.16-02 Rev. 2: (2017) Establishment of Special Conditions for Aircraft Systems.
- FAA AC 120-76D: (2017) Authorization for Use of Electronic Flight Bags, New Security Procedures.

In a way, Means of Compliance is a way to facilitate the certification task for both the regulator and the entity. The adherence to those ensures recognition of compliance with rules. If an applicant chooses to comply by other means, it must show that it provides for compliance with the applicable specification or requirement. In these cases, the burden of proof of compliance wholly rests with the applicant. This is why most authorities and applicants try to adhere to the Means of Compliance of a set of standards or regulations because proving compliance in any other way can result in an arduous task.

3.2 Safety and Security Co-Engineering for Airworthiness

Safety and security are both risk-driven activities necessary to ensure airworthiness. Even though historically they have been conceived as different engineering specialties, it is obvious they cannot continue to ignore each other. As a matter of fact, current research concludes that safety and security assessments can improve when they are considered together or partially together.

The concurrent security and safety assurance processes are used as inputs to the aircraft design and development process, and as a means for aircraft implementation verification, and validation and certification processes.

3.2.1 Safety Assessment Process and Security Assessment Process

Just as failures and errors are treated as manageable risks to aircraft safety by the airworthiness certification process, the threat of Unauthorized Interaction is treated equally through the airworthiness security activities.

A framework that integrates the Security Assessment Process with the Safety Assessment Process was proposed in the paper (Garcia et al., 2018).

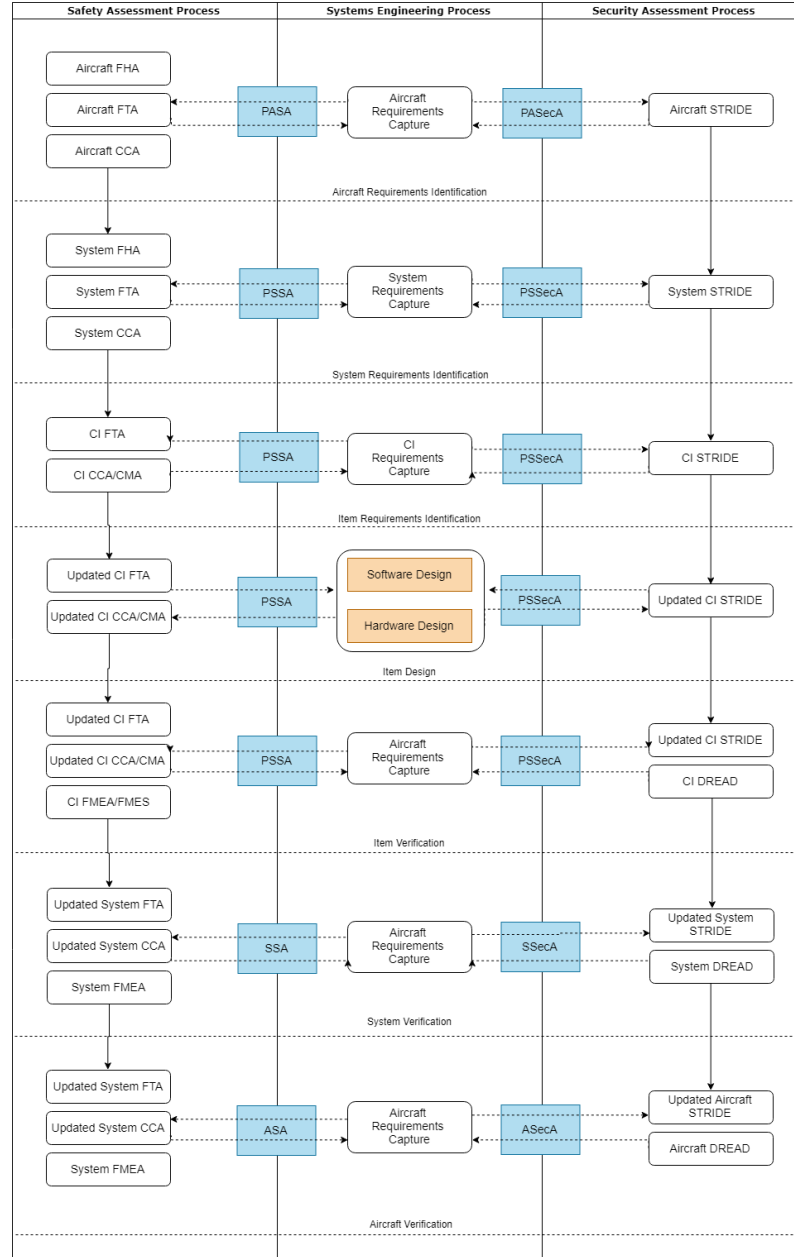


Figure 3.3: Design and Development Framework

The framework exploits the analogous nature of Safety and Security Engineering. It follows the Safety Assessment Process explained in the previous chapter, as detailed in (SAE-Aerospace, 1996). As methodologies, it uses:

- Fault Tree Analysis (FTA): uses Boolean logic gates to show the relationship of failure effects to failure modes.
- Functional Hazard Analysis (FHA): A systematic, comprehensive examination of functions to identify and classify Failure Conditions of those functions according to their severity.
- Common Cause Analysis (CCA): support the development of the specific system architecture and that of related systems by evaluating the overall architecture sensitivity to common cause events.
- Common Mode Analysis (CMA): is a qualitative analytical tool used to ensure the “goodness” of a design.
- Failure Mode and Effects Analysis (FMEA): is a systematic, bottom-up method of identifying the failure modes of a system, item, or function and determining the effects on the next higher level.
- Failure Modes and Effects Summary (FMES): is a grouping of single failure modes which produce the same failure effect.

The methodologies chosen for the Security Assessment (the threat modeling and analysis) are STRIDE and DREAD, detailed in the previous chapter.

The difference presented between the Safety Assessment Process and the Security Assessment Process is the resulting action after the requirements have been established and the design and development has been done. The third of the security engineering process establishes a critical point: there are cyber-threats and vulnerabilities that are dormant to attack or unknown to the vendor until they are exploited.

The framework has to comply with the DO-326A set Means of Compliance and be able to be integrated into the standards that allow for aircraft development. Otherwise, it becomes an standalone framework, which is not optimal. Looking at Figure 3.2, it can be seen that if the Framework can adapt with industry standards SAE ARP 4761 (ibid.) and SAE ARP 4754A (SAE-Aerospace, 2010), using their proposed methodologies, it could comply with RTCA DO-326A set for development.

3.2.2 SAE ARP 4754A

The aim of the framework is to allow Safety and Security co-engineering when it comes to developing methodologies and frameworks for Airworthiness (both Safety and Security). It is necessary to see if it can be integrated to the industry standards frameworks:

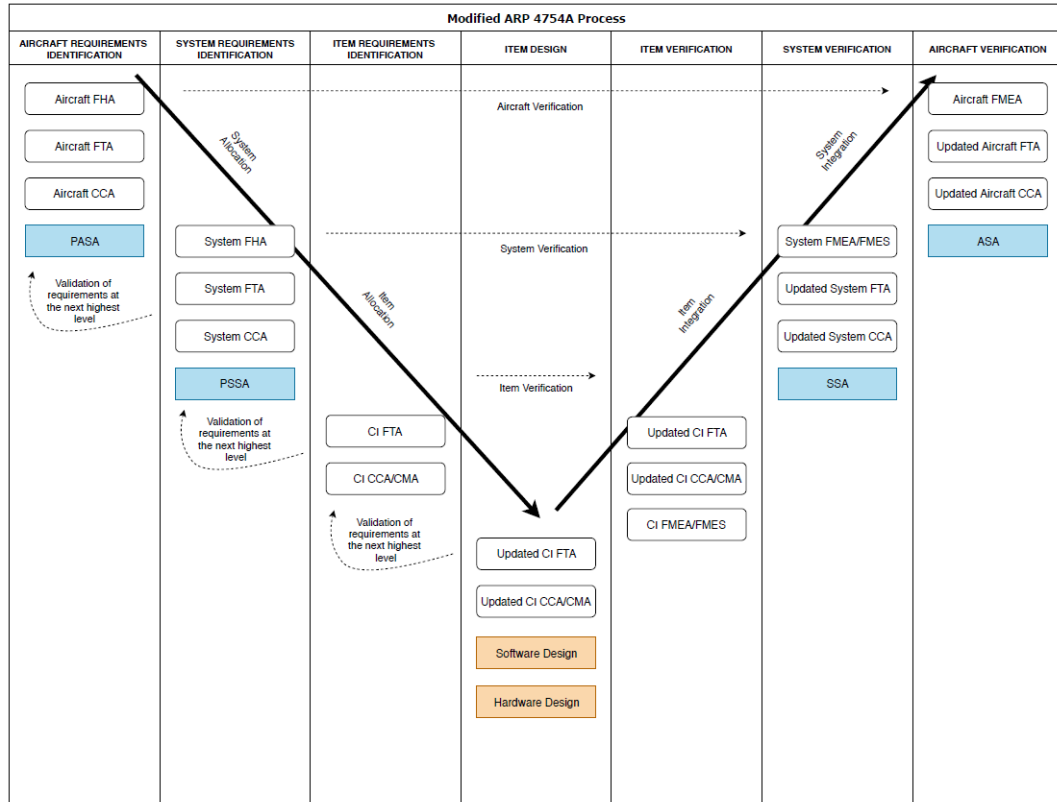


Figure 3.4: ARP4754A Process - Interaction between safety and development processes

If the ARP4754A Process is modified, it can accommodate both Safety and Security, Figure 3.5:

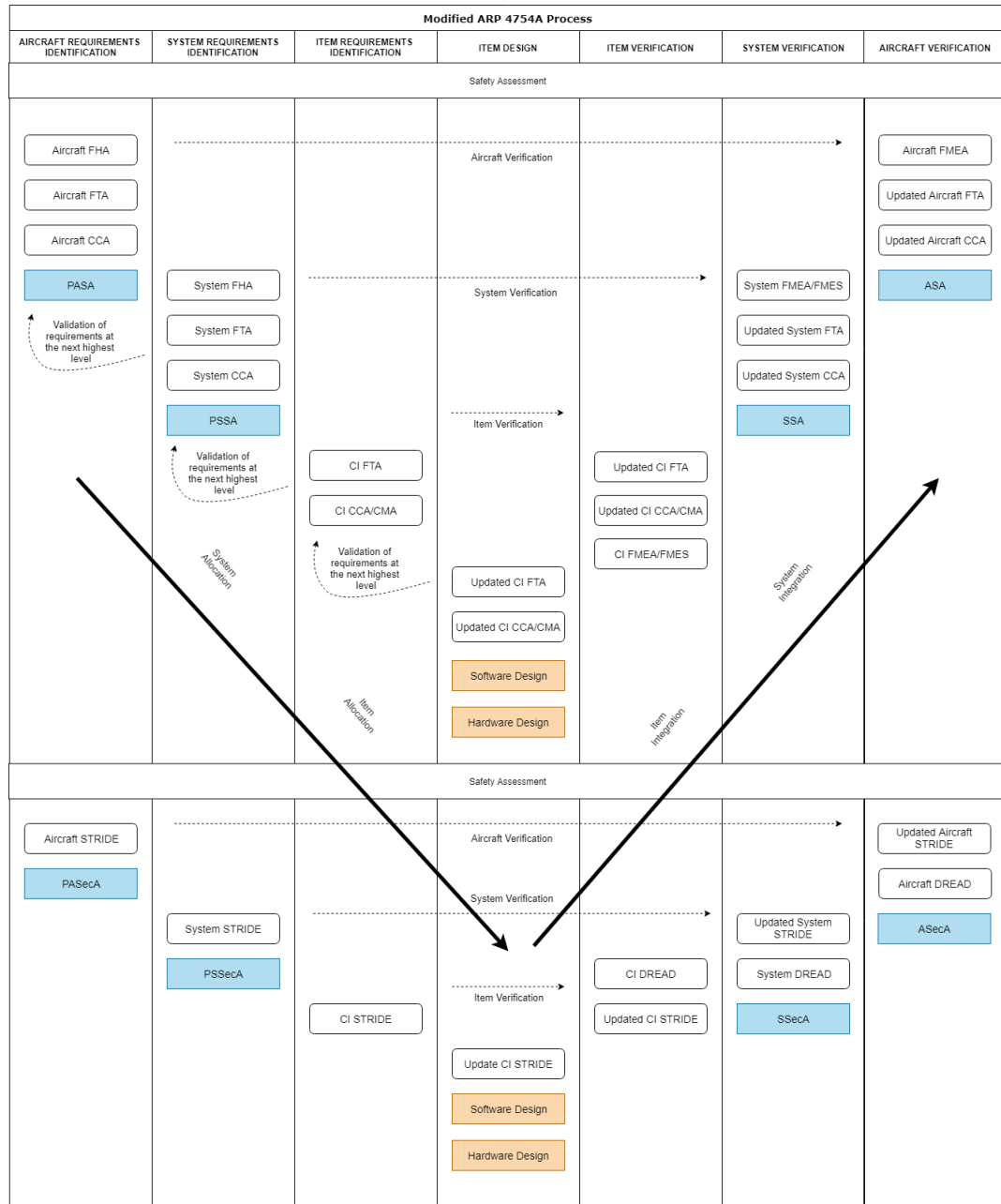


Figure 3.5: Modified ARP4754A Process - Interaction between safety, security and development processes

Once there is a clear vision of how Safety and the Development Process interact, according to SAE ARP 4754A, the Safety Assessment Process has to be seen in more detail, as in Figure 3.6.

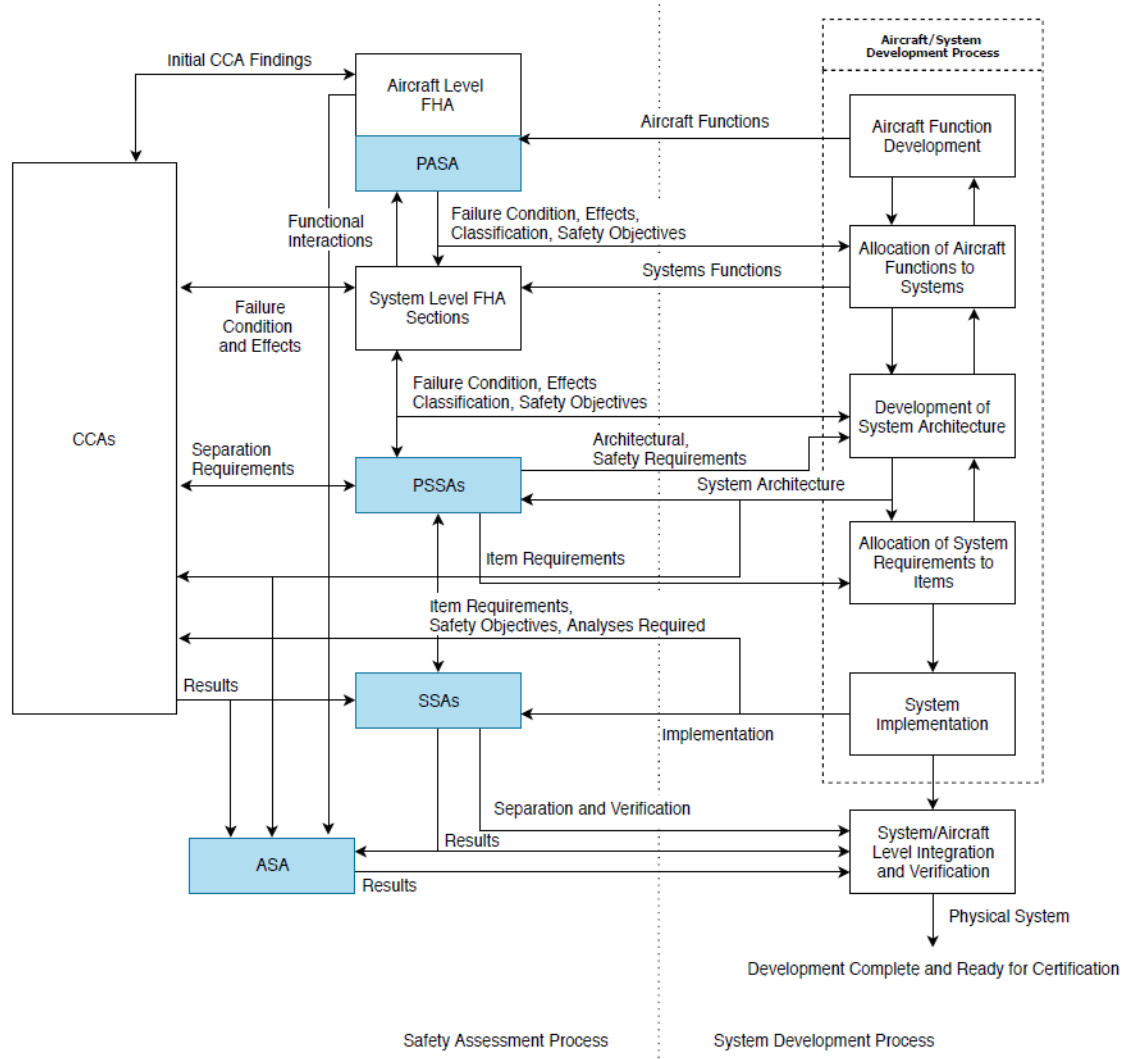


Figure 3.6: ARP4754A Process - Safety Assessment Process Model (SAE-Aerospace, 2010)

In Figure 3.6, there is a representation of all the parameters and documents that each step of the Safety Assessment Process and System Development Process needs. PASA, PSSAs, SSAs and ASA are given information as input from the Development Process and the CCAs, FHAs and FEMAs, and FTAs.

3.2.3 SAE ARP 4761

In SAE ARP 4761 (SAE-Aerospace, 1996), the Safety Assessment Diagram is detailed as follows:

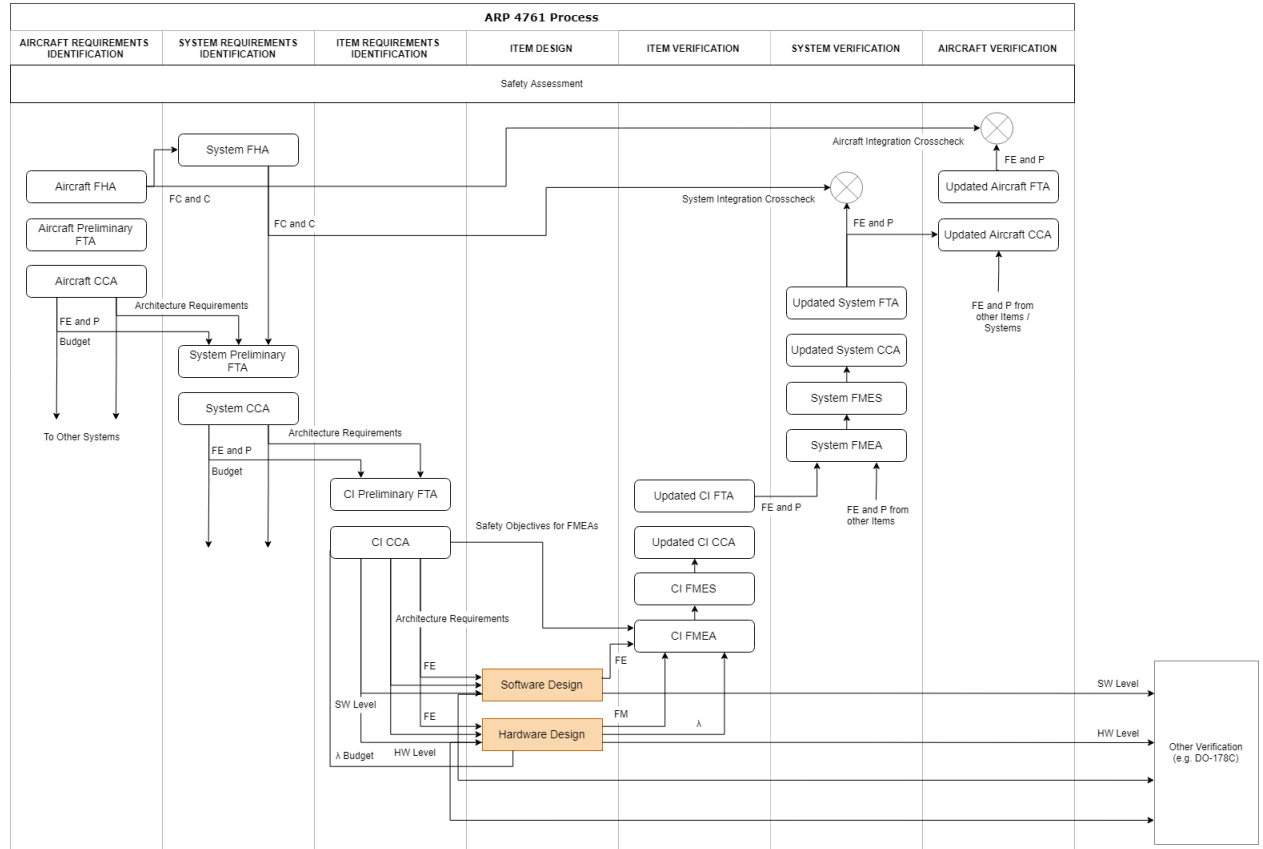


Figure 3.7: ARP4761 Process - Safety Assessment Diagram

The needed parameters/variables and inputs needed to complete the path from Requirements Identification to Verification are detailed in the diagram. It is also indicated that some parameters from the Security Assessment, can be used for other types of verification, for example, using the RTCA DO-178C set verification tools.

3.2.4 Integration of Safety / Security Methodologies.

The initial proposed framework is updated to add more security methodologies for the Security Assessment Process. After researching different security methodologies for designing, developing and implementing security with safety co-engineering, the followin have been added:

- Attack Trees (AT). Attack Trees or Threat trees are similar to fault trees but focus only on the security of a system and are an enumeration of possible attacks.

The root of an attack tree represents a successful attack and the leaf nodes represent ways of achieving the planned attack.

- Failure Mode, Vulnerabilities and Effects Analysis (FMVEA): is structured technique which investigates failure modes and their effects, as well as vulnerabilities. It is split at the item level, so instead of being purely a Security Assessment methodology, it gets input from the Safety Assessment as well.

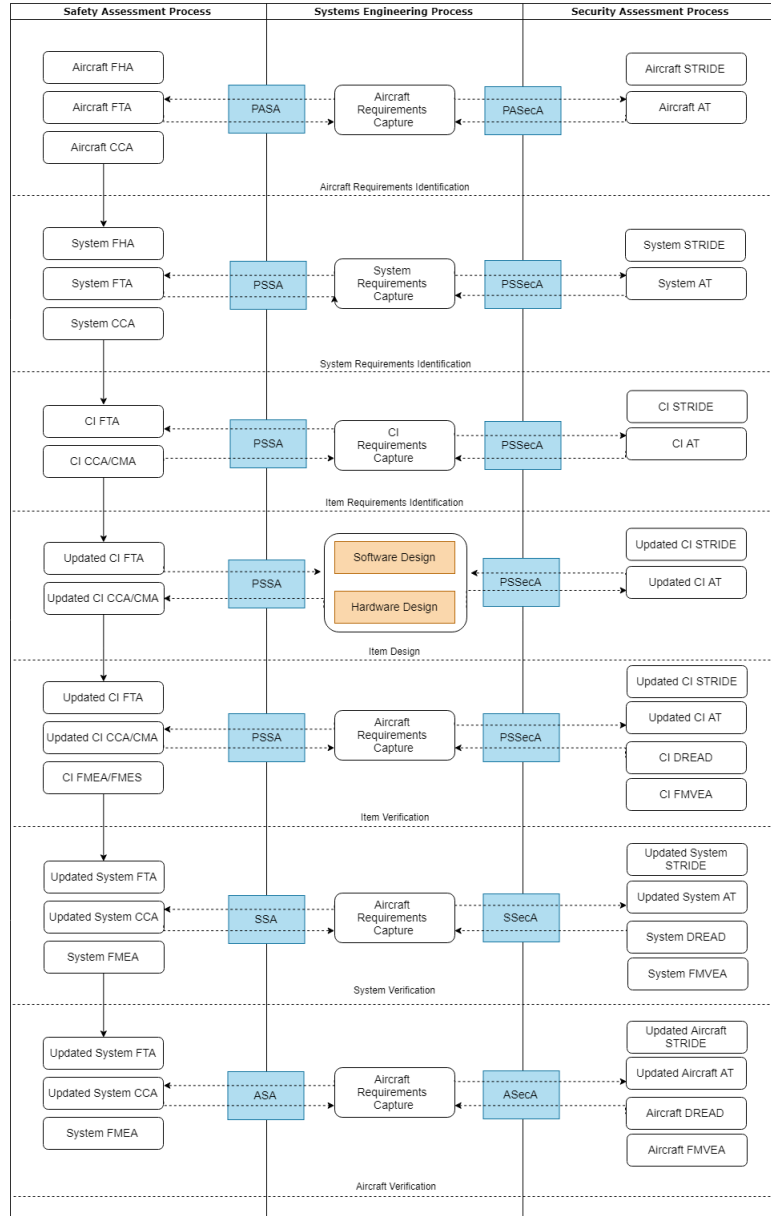


Figure 3.8: Modified Design and Development Framework

The ARP4754A Process is modified once again, so it can accommodate both Safety

Assessment and the new Security Assessment (same as Figure 3.5, but with the new security methodologies):

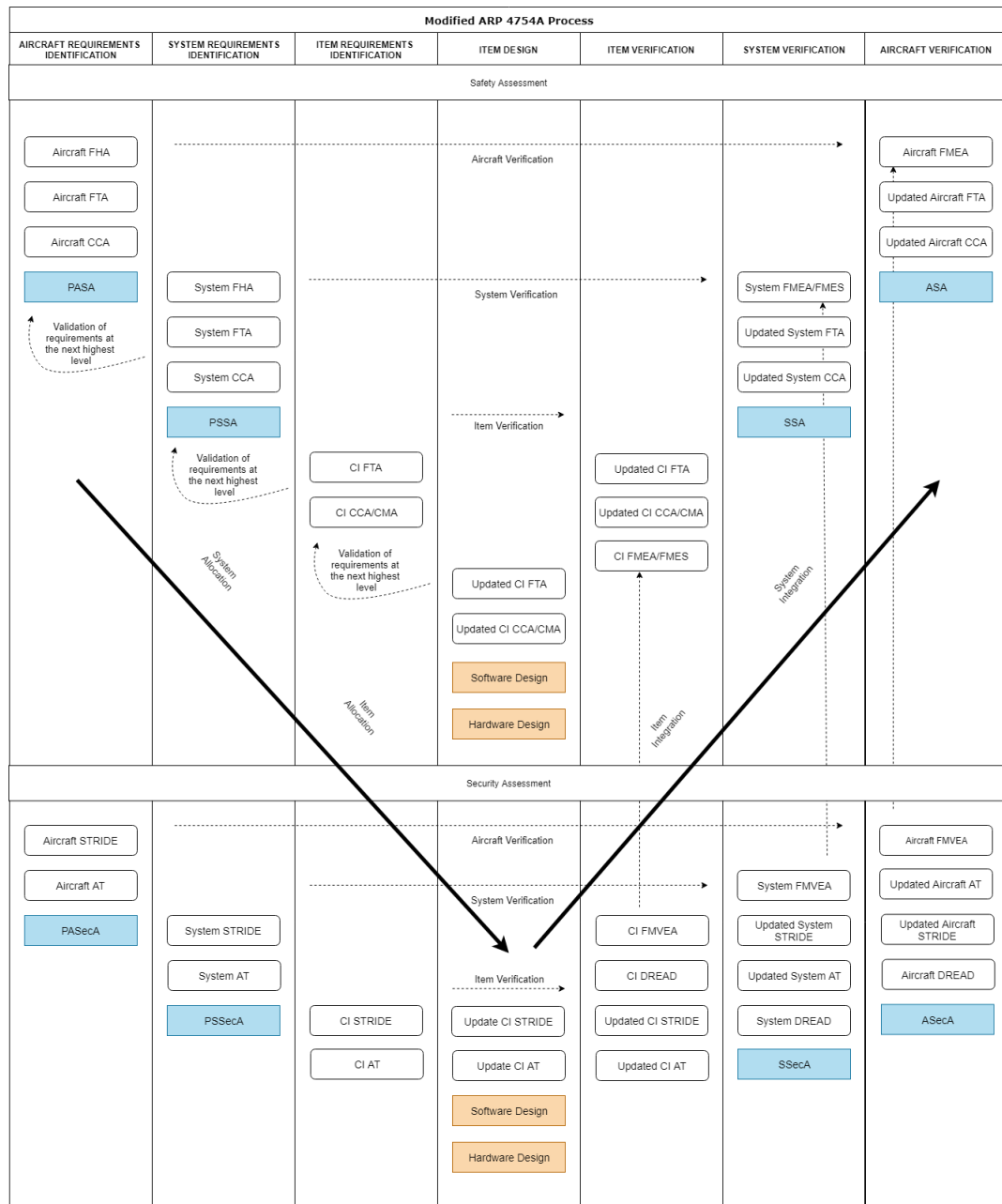


Figure 3.9: Modified ARP4754A Process - Interaction between safety, security and development processes

The detailed Safety Assessment Process in ARP4754A has been modified to accommodate the Security Assessment Process too. Now the parameters and documents needed for PASEcA, PSSEcA, SSecAs and ASecA are given from the Attack Trees, the STRIDE and DREAD Analysis, and the FMEAs of the Safety Engineering.

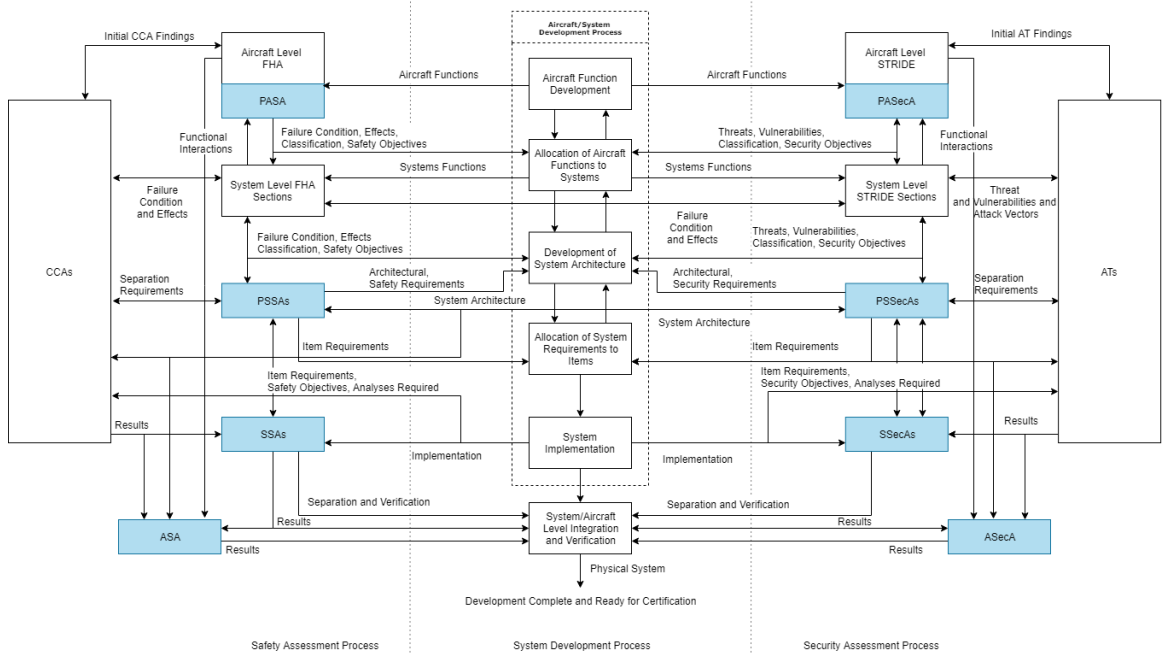


Figure 3.10: Modified ARP4754A Process - Safety and Security Assessment Process Model

In Figure 3.11, the needed parameters/variables and inputs needed to complete the path from Requirements Identification to Verification are detailed in the new diagram. It is also indicated that some parameters from the Safety Assessment, such as the ones needed to perform the FMVEAs, are given as input for the Security Assessment.

Since the FMVEA methodology is a split methodology one has to be very careful not miss any parameter, or duplicate the work. If work were duplicated, for example, the safety assessment team performed FMEAs and unbeknownst to the security assessment team they performed FMVEAs in their totality, it could lead to duplicated results and an increase on cost and wasted resources.

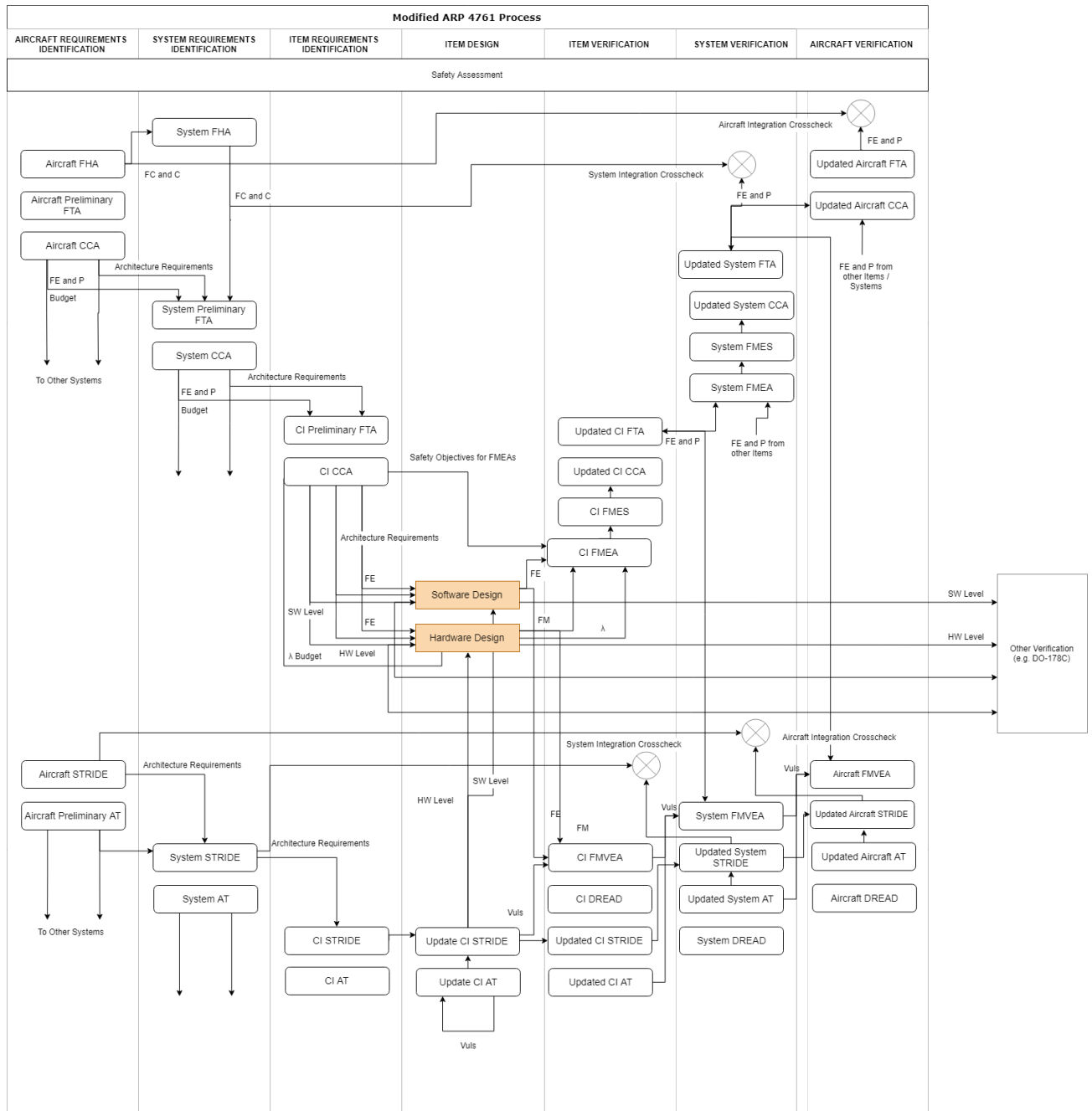


Figure 3.11: Modified ARP4761 Process - Safety and Security Assessment Diagram

The Design and Development Framework in this process leaves to a constant state of updating CI STRIDE that is not factored in. Therefore, a continuous security assessment model integrated into the security assessment model (which had, in its turn, been integrated into the safety assessment model) was proposed to be able to contemplate this possibility. The CI STRIDE is updated and forwarded to the verification stage, where it is monitored to see if there are any new vulnerabilities that might affect the configuration item.

Chapter 4

Conclusions and Future Research

4.1 Conclusions

This thesis premise was the study of the intricacies of building and designing an information security framework for aviation systems. It had to comply with the most relevant Airworthiness Security standards (the RTCA DO-326A set), meet their means of compliance, and be able to be integrated into the most used technical documents and standards for aircraft systems development and certification.

To be able to ensure an understanding of the certification and standardization process of a technical document, guidance or standard for the proposed framework (in a hypothetical case), an in-depth study of the regulatory process of aircraft regulations and aviation law has been done.

The study of the state-of-the-art techniques and methodologies to do the security assessment of the framework while also taking advantage of the safety assessment methods already established (to prove the validity of security and safety co-engineering in aircraft development) have been studied.

Furthermore, two frameworks have been proposed in the discussion carried out in this thesis, given a broad overview of the different approaches for Security Assessment and Safety Assessment.

4.2 Future Research

There is always future research in an emerging topic as cybersecurity in aviation. Aircraft are becoming more complex and sophisticated as they have ever been, and that includes taking advantage of all the new technology that is constantly being developed. As future research topics, this thesis proposes:

- An extrapolation of the ‘Hazard Space Analysis’ of Safety Engineering and Safety Assessment applied to the ‘Threat Space Analysis’ of Security Engineering and Security Assessment (Aceituna, 2017).
- An implementation of SAHARA: STRIDE approach and HARA (Hazard Analysis and Risk Assessment). (Macher et al., 2015) The process quantifies the security impact on dependable safety-related system development at system level. The inductive analysis methods HARA and SAHARA to also enable the quantification of additional dependability features (such as reliability and availability).

Bibliography

- Abeyratne, Ruwantissa (2010). *Aviation Security Law*. Springer.
- Aceituna, Daniel (2017). “A Means of Assessing the Entire Functional Safety Hazard Space”. In: *SAE International*.
- Administration, Federal Aviation (2006). *Information Security Certification and Accreditation (C&A) Handbook*. Tech. rep.
- AIA, AEA, GAMA, and FAA (2017). *The FAA and Industry Guide to Product Certification*. Third Edition.
- AIAA (2013). “A Framework for Cybersecurity”. In: *The Connectivity Challenge: Protecting Critical Assets in a Networked World*.
- Aslanyan, Zaruhi and Flemming Nielson (2015). “Pareto Efficient Solutions of Attack-Defence Trees”. In: *Principles of Security and Trust - 44th International Conference*.
- Babiceanu, R. F. and R. Seker (2017). “Formal Verification of Trustworthiness Requirements for Small Unmanned Aerial Systems”. In: *2017 Integrated Communications, Navigation and Surveillance Conference (ICNS)*, pp. 1–8.
- Babiceanu, Radu F. and Remzi Seker (2017). “Trustworthiness Requirement for Manufacturing Cyber-Physical Systems”. In: *Procedia Manufacturing* 11, pp. 973–981.
- Balakrishnan, N. (2015). “An Overview of System Safety Assessment”. In: Springer International. Chap. 2.
- Barrett, Matt, Jeff Marron, Victoria Yan Pillitteri, Jon Boyens, Greg Witte, and Larry Feldman (2017). *Draft NISTIR 8170 The Cybersecurity Framework*. Tech. rep.
- CAAS (2017). *Aircraft Network Security Programme (ANSP)*. Tech. rep.
- Civil Aviation Safety Authority (2016). *Software Configuration Management*. Tech. rep.
- Garcia, A. B., R. F. Babiceanu, and R. Seker (2018). “Trustworthiness Requirements and Models for Aviation and Aerospace Systems”. In: *2018 Integrated Communications, Navigation, Surveillance Conference (ICNS)*, pp. 1–10.
- InfoSec, SANS Institute (2003). *An Introduction to Certification and Accreditation*. SANS Institute.
- Infrastructure, Network and Security (NIS) Subcommittee Network Security WG (2012). “Considerations for Incorporation of Cyber Security in the Development of Industry Standards”. In: *AEEC*.
- ITEA2 (2016). *Recommendation for Security and Safety Co-engineering*. Tech. rep.

- Jimenez, Jose Andres, Jose Amelio Medina Merodio, and Luis Fernandez Sanz (2017). "Checklists for Compliance to DO-178C and DO-278A Standards". In: *Computer Standards & Interfaces*.
- Kaiser, Lisa (2013). *Transportation Industrial Control Systems (ICS) Cybersecurity Standards Strategy*. Tech. rep.
- Kolle, Rainer, Garik Markarian, and Alex Tarter (2015). *Aviation Security Engineering: A Holistic Approach*. CRC Press.
- Kornecki, A. J. and M. Liu (2013). "Fault Tree Analysis for Safety/Security Verification in Aviation Software". In: *Electronics* 2, pp. 41–56.
- Macher, Georg, Andrea Holler, Harald Sporer, Eric Armengaud, and Christian Kreiner (2015). "A Comprehensive Safety, Security, and Serviceability Assessment Method". In: *Computer Safety, Reliability, and Security - 3434th International Conference*.
- NHTSA (2014). *National Institute of Standard and Technology Cybersecurity Risk Management Framework Applied to Modern Vehicles*. Standard.
- NIST (2017). *Framework for Cyber-Physical Systems*. Standard.
- Olive, Michael L., Roy T. Oishi, and Stephen Arentz (2007). "Commercial Aircraft Information Security - An Overview of ARINC Report 811". In: *2006 IEEE/AIAA 2525th Digital Avionics Systems Conference*.
- Ongsakorn, P., K. Turney, S. Nair M. Thornton, S. Szygenda, and T. Manikas (2010). "Cyber Threat Trees for Large System Threat Cataloging and Analysis". In: *2010 IEEE International Systems Conference*.
- OWASP (n.d.). URL: https://www.owasp.org/index.php/Threat_Risk_Modeling.
- Paul, S. and L. Rioux (2015). "Over 20 years of research into cybersecurity and safety engineering: a short bibliography". In: *WIT Transactions on The Build Environment. Safety and Security Engineering VI* 151, pp. 335–349.
- Pearson, Michael W. and Daniel S. Riley (2015). *Foundations of Aviation Law*. Ashgate.
- RTCA (2016). *List of Available Documents*. Standard.
- RTCA DO-178C (2011). *Software Considerations in Airborne Systems and Equipment Certification*. Standard.
- RTCA DO-254 (2000). *Design Assurance Guidance for Airborne Electronic Hardware*. Standard.
- RTCA DO-326 (2010). *Airworthiness Security Process Specification*. Standard.
- RTCA DO-326A (2014). *Airworthiness Security Process Specification*. Standard.
- RTCA DO-330 (2011). *Software Tool Qualification Considerations*. Standard.
- RTCA DO-333 (2011). *Formal Methods Supplement to DO-178C and DO-278A*. Standard.
- RTCA DO-355 (2014). *Information Security Guidance for Continuing Airworthiness*. Standard.
- RTCA DO-356 (2014). *Airworthiness Security Methods and Considerations*. Standard.
- RTCA DO-356A (2017). *Airworthiness Security Methods and Considerations*. Standard.
- SAE-Aerospace (1996). *ARP4761*. Standard.

- SAE-Aerospace (2010). *ARP4754A*. Standard.
- (2013a). *ARP5150A*. Standard.
- (2013b). *ARP5151*. Standard.
- Schmittner, Christoph, Thomas Gruber, Peter Puschner, and Erwin Schoitsch (2014). “Security Application of Failure Mode and Effect Analysis (FMEA)”. In: *Computer Safety, Reliability, and Security - 333rd International Conference*.
- Shostack, Adam (2014). *Threat Modeling: Designing for Security*. WILEY.
- Shull, Forrest (2016). “Evaluation of Competing Threat Modeling Methodologies”. In: *Carnegie Mellon University*.
- STRIDE* (n.d.). URL: <http://blogs.microsoft.com/cybertrust/2007/09/11/stride-chart/>.
- United States, Senate of the (2016). *Cyber AIR Act*. Tech. rep. Senate of the United States.
- Wang, P. (2017). *Safety Management*. Civil Aircraft Electrical Power System Safety Assessment: Issues and Practices. Butterworth-Heinemann.

References

The following standards are cited in this thesis.

#	Reference	Document
1	ABN-035A	ARINC Technical Application Bulletin ABN-035A, "Considerations for the Incorporation of Cyber Security in the Development of Industry Standards", October 2012
2	ARINC 615A	ARINC 615A, "Software Data Loader Using Ethernet Interface", May 2002
3	ARINC 665	ARINC Report 665, "Electronic Distribution of Software", August 2002
4	ARINC 667	ARINC 667, "Field Loadable Software", November 2010
5	CFR Title 14 25	Code of Federal Regulations Title 14, "Airworthiness Standards: Transport Category Airplanes"
6	EASA CS-25 AMC 25.1309	EASA AMC 25.1309,"Systems Design and Analysis", CS-25 Book 2 Subpart F, "Acceptable Means of Compliance", October 2003
7	FAA AC 119-1	FAA Advisory Circular 119-1, "Airworthiness and Operational Authorization of Aircraft Network Security Program (ANSP)", September 2015
8	FAA AC 120-76	FAA Advisory Circular 120-76A, "Guidelines for the Certification, Airworthiness, and Operational Approval of Electronic Flight Bag Computing Devices", March 2003
9	FAA AC 25.1322-1	FAA Advisory Circular 25.1322-1, "Flightcrew Alerting", December 2010
10	FAA Order 8110.52A	FAA Order 8110.52A, "Type Validation and Post-type Validation Procedures", December 2014
11	FAA PS-AIR-21.16-02 Rev. 2	FAA Policy Statement PS-AIR-21.16-02, "Establishment of Special Conditions for Cyber Security, February 2017"

12	ISO/IEC 27001:2013	ISO/IEC 27001:2013 "Information technology – Security techniques – Information security management systems – Requirements", June 2013
13	ISO/IEC 27005:2011	ISO/IEC 27005:2011 "Information Security Risk Management", June 2011
14	ISO/IEC 27035:2011	ISO/IEC 27035:2011 "Information Security Incident Management", June 2011"
15	NIST SP 800-30	NIST SP 800-30 Rev. 1, "Guide for Conducting Risk Assessments", September 2012
16	NIST SP 800-37	NIST SP 800-37 Rev. 1, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach", February 2010
17	RTCA DO-178C	RTCA DO-178C, "Software Considerations in Airborne Systems and Equipment Certification", December 2011
18	RTCA DO-254	RTCA DO-254, "Design Assurance Guidance for Airborne Electronic Hardware", April 2000
19	RTCA DO-326A	RTCA DO-326A, "Airworthiness Security Process Specification", August 2014
20	RTCA DO-330	RTCA DO-330, "Software Tool Qualification Considerations", January 2012
21	RTCA DO-355	RTCA DO-355, "Information Security Guidance for Continuing Airworthiness", June 2014
22	RTCA DO-356A	RTCA DO-356A, "Airworthiness Security Methods and Considerations", June 2018
23	SAE ARP 4754A	SAE ARP 4754A, "Guidelines for Development of Civil Aircraft and Systems", December 2010
24	SAE ARP 4761	SAE ARP 4761, "Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment", December 1996
25	SAE ARP 5150A	SAE ARP 5150, "Safety Assessment of Transport Airplanes in Commercial Service", November 2013