LDRA
Software Technology

Technical White Paper

The Aerospace Security Framework

www.ldra.com

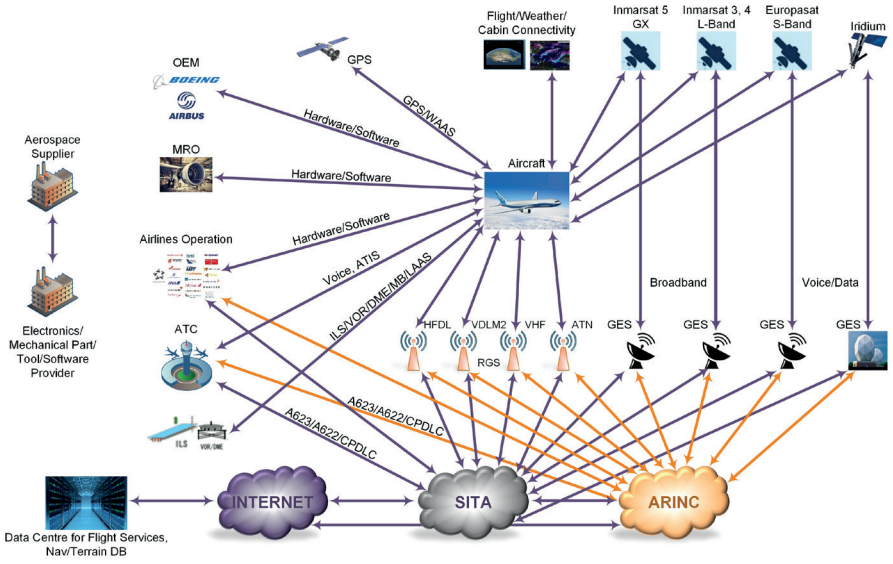
Contents

Introduction

The lineage of the aerospace certification process is derived from US Department of Defense (DoD) military standards (MIL-STD) and is heavily influenced by DoD/MIL system and software development practices. The core principle for certification is safety assurance in design, operation, and maintenance. Aerospace certification processes are tilted towards a rigorous verification process to ensure the safety-critical functions meet appropriate design assurance levels.

Today security has become a primary challenge in aerospace system development and certification. Increasingly the aviation network, as well as the aircraft, is connected to the internet (nose-to-tail) and other private networks (Figure 1). The connected services may include weather forecasts, maintenance data, and high-speed broadband in the cabin as in-flight entertainment (IFE).

The Aircraft Communication Addressing and Reporting System (ACARS) has traditionally utilized a digital datalink system for transmission of short messages between aircraft and ground stations via airband radio or satellite. ACARS is now integrating Internet Protocol (IP), database upload, and many other technologies. However, as a consequence of these advancements in communications an unsecured airborne system or aircraft can lead to a compromise in safety.



KEY		CPDLC	C ontroller–pilot data link com-munications	MB	Marker Beacon
		GES	Ground Earth Station	RGS	Remote Ground Station
ARINC	Aeronautical Radio, Incorporated	GPS	Global Positioning System	VDLM2	VHF Data Link-Mode 2
ATC	Air Traffic Controller	HFDL	High Frequency Data Link	VHF	Very High Frequency
ATIS	Automatic Terminal Information Service	ILS	Instrument Landing System	VOR/DME	VHF Omni-directional Range/ Distance Measuring Equipment
ATN	Aeronautical Telecommunications Network	LAAS	Local Area Augmentation System	WAAS	Wide Area Augmentation System

Figure 1: Connected aircraft ecosystem

The issues that exist in the cyber world have migrated to the connected aviation network, where the associated risks increase exponentially. Aerospace systems have not historically been developed with security in mind, and so software upgrades for security requirements on the post facto certification baselines are either costly or ineffective. Air travel has built an enviable reputation for reliability and trustworthiness over the years, and this situation has the potential to compromise it.

The challenge is to establish a common security framework underpinned by most appropriate best-practice guidelines to form a robust and secure ecosystem. For example, DO-326A based guidelines from RTCA would be most appropriate for the development of a Line Replacement Unit (LRU), whereas ISO 27000[1] and NIST[2] standards would be more applicable to the supporting Information Technology (IT) infrastructure.

[1] ISO/IEC 27001 INFORMATION SECURITY MANAGEMENT https://www.iso.org/isoiec-27001-information-security.html

[2] National Institute of Standards and Technology (NIST) https://www.nist.gov/topics/cybersecurity

Active participation by key government agencies together with private players (Original Equipment Manufacturers (OEMs), suppliers, and others) will be critical in developing a harmonized, unified and actionable framework from which a roadmap and strategy can evolve.

Sharing of current threats, recent security breaches, and evolving intelligence is essential in addressing future threats because successful cyber attacks, such as ransomware, are frequently copied. An awareness of the latest attack methods and the vulnerabilities exploited can help to ensure that the impact of new attacks is mitigated or thwarted completely.

The story so far

A detailed list of regulations and guidelines is presented in Figure 2.

SN	Issuing Authority/ Organization	Document Name/Description	Remark
1	FAA (Federal Aviation Administration)	PS-AIR-21.16-02 Rev. 2, "Establishment of Special Conditions for Aircraft Systems Information Security Protection" dated 22 FEB 2017	Published
2		Transport Airplane Issue List (TAIL) issue paper, "Aircraft Electronic System Physical/Electronic Security Protection"	Published
3		TAIL issue paper, "Isolation or Aircraft Electronic System Security Protection from Unauthorized Internal Access"	Published
4		TAIL issue paper, "Isolation or Aircraft Electronic System Security Protection from Unauthorized Internal Access"	Published
5		TAIL issue paper, "Aircraft Electronic System Security Protection from Unauthorized External Access"	Published
6		TAIL issue paper, "Use of Portable Electronic Flight Bags to Communicate with Installed Airplane Systems in the Flight Deck via an Interface Device"	Published
7		FAA Order 1370.82A Information Systems Security Program, and the FAA Information Systems Authorization Handbook.	Published
8		Advisory Circular (AC) 120-76D Authorization for Use of Electronic Flight Bags	Published
9	EASA (European Aviation Safety Agency)	Certification Review Items (CRI), "Security Protection of Aircraft Systems and Networks"	In Progress
10		NPA: Notice of Proposed Amendment 2019-01 Aircraft Cybersecurity	Published
11		Acceptable Means of Compliance (AMC) 20-42 Airworthiness Information Security Risk Assessment	Published
12		AMC 20-25 Airworthiness and operational consideration for Electronic Flight Bags (EFBs)	Published
13	ASTM (American Society for Testing and Materials)	F4450_Standard Practice for, "Protection of Aeroplane Systems and Information Security from Intentional Unauthorized Electronic Interactions" (WK56374 DRAFT)	In Progress Under review
14	GAMA (General Aviation Manufacturers Association)	Recommended Practices and Guidelines for Aircraft Systems Information Security Protection (ASISP, ad hoc)	Published
15	DO-326A	Airworthiness Security Process Specification	Published
16	ED-202A		Published
17	DO-355	Information Security Guidance for Continuing Airworthiness	Published
18	ED-204		Published
19	DO-356	Airworthiness Security Methods and Considerations	Published
20	ED-203A		Published
21	ED-201	Aeronautical Information System Security (AISS) Framework Guidance	Published
22	ED-205	Process Standard for Security Certification and Declaration of ATM ANS Ground Systems	Published

Figure 2: Regulatory guidance

The regulatory documents dealing with Certification Specifications for large aeroplanes, Part 25[3] and CS-25[4] from the FAA and EASA respectively, do not address information security. Indeed, the guidance documents detailing Acceptable Means of Compliance, AMC 25.1309[5] and AC 25.1309[6], explicitly exclude acts of sabotage, exploitation, or attack from the list of events to be addressed during the safety assessment.

In the European Union, the response to this information security anomaly was to leverage the initial airworthiness regulations CS-21[7] (equivalent to FAA Part 21[8]) as governed by regulation no.748/2012[9] (Figure 3).

The resulting new Special Condition (SC – see sidebar) in accordance with CS-21.B.75 (formerly CS-21.A.16B) was entitled "Information Security Protection of Aircraft Systems and Networks"/ "Aircraft Systems Information Security Protection" and was designed to ensure that safety would not be compromised by security threats.

This ensured that cybersecurity was addressed as part of the certification activities of new large airplane type (CS-25/Part 25) designs and STCs (Supplementary Type Certifications). An applicant was obliged to perform a "product information security risk assessment" to determine the operational environment for the information security of the product, identification of the possible threats, vulnerabilities, attack paths (access vector); possibilities of successful attack/exploitation, the impact of an attack and possible mitigation/countermeasures methods.

> *"For a change that contains new design features that are novel and unusual for which there are no later applicable certification specifications at a later amendment level, EASA will designate special conditions…*
>
> *EASA will impose later certification specifications that contain adequate or appropriate safety standards for this feature, if they exist, in lieu of special conditions."*
>
> - **EASA Annex to ED Decision 2019/018/R**

Amendment NPA 2019-01 Aircraft cybersecurity was then proposed by EASA, to formalise the situation further by introducing cybersecurity provisions into the applicable certification specifications while considering the existing special conditions and the recommendations of the Aviation Rulemaking Advisory Committee (ARAC) regarding aircraft systems information security/protection (ASISP).

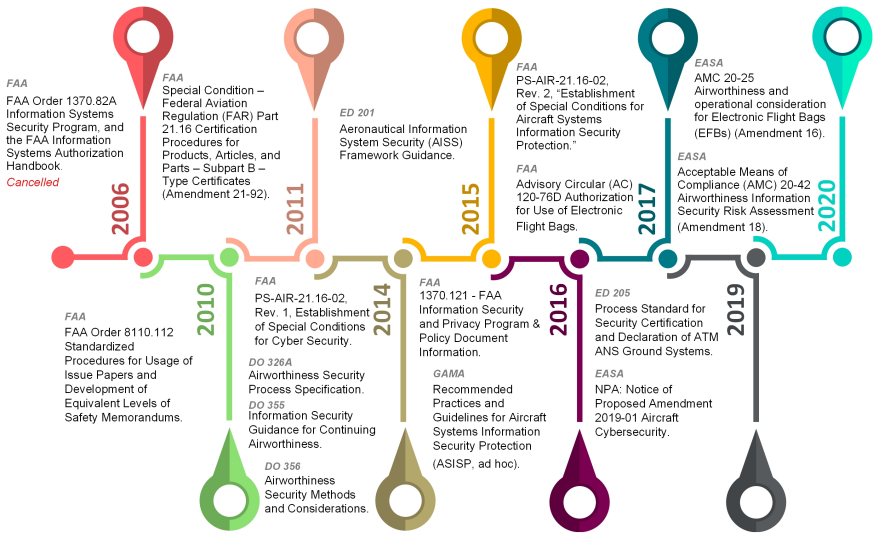


Figure 3. Timeline of regulatory evolution

[3] FAA 14 CFR Part 25 – "AIRWORTHINESS STANDARDS: TRANSPORT CATEGORY AIRPLANES"
[4] EASA CS-25 "Certification Specifications for Large Aeroplanes"
[5] EASA AMC 25.1309 "Acceptable means of compliance – System Design and Analysis"
[6] AC 25.1309 - FAA Advisory Circular "System Design and Analysis"
[7] Commission Regulation (EU) No 748/2012 of 3 August 2012 - Airworthiness and Environmental Certification https://www.easa.europa.eu/regulations#regulations-initial-airworthiness
[8] PART 21—CERTIFICATION PROCEDURES FOR PRODUCTS AND ARTICLES https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=2bc3151798fc28602bb9091abdd1b77c&mc=true&n=pt14.1.21&r=PART&ty=HTML#se14.1.21_116
[9] EASA Easy Access Rules for Airworthiness and Environmental Certification https://www.easa.europa.eu/document-library/general-publications/easy-access-rules-initial-airworthiness
[10] EASA NPA 2019-01 Aircraft cybersecurity https://www.easa.europa.eu/document-library/notices-of-proposed-amendment/npa-2019-01

NPA 2019-01 Aircraft cybersecurity introduced new acceptable means of compliance (AMC 20-42) which detailed changes to various existing certification specifications (CSs), upgraded to include new cybersecurity requirements.

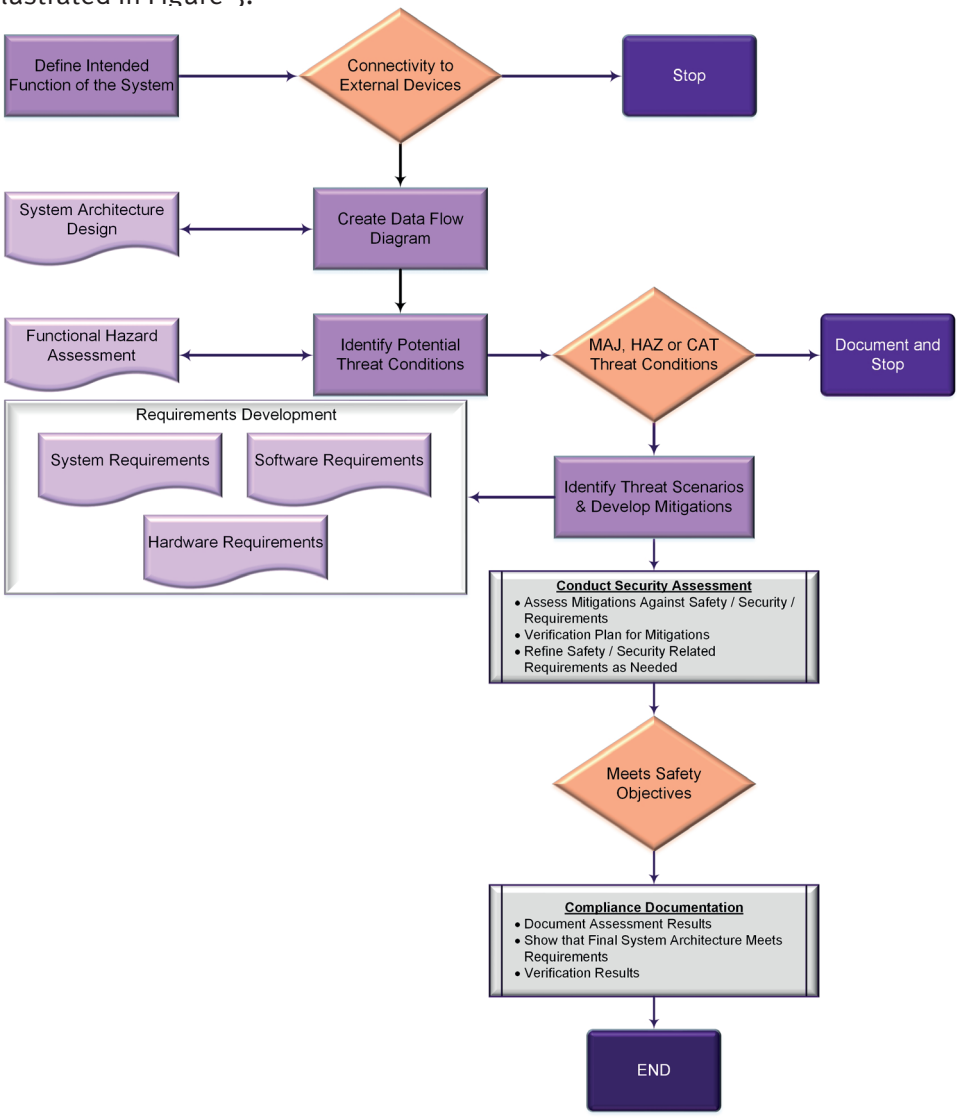
In 2019, the international guidelines DO-326A/ED-202A entitled "Airworthiness Security Process Specification" became the sole Acceptable Means of Compliance (AMC) for FAA and EASA cybersecurity airworthiness certification.

The "DO-326/ED-202 set" also includes the following companion documents:

- DO-356A/ED-203A: "Airworthiness Security Methods and Considerations"
- DO-355/ED-204: "Information Security Guidance for Continuing Airworthiness"
- ED-201: "Aeronautical Information System Security (AISS) Framework Guidance"
- ED-205: "Process Standard for Security Certification and Declaration of ATM ANS Ground Systems"

Security assessment and development process overview

Applicants seeking to develop a system that is compliant with this DO-326/ED-202 set are required to follow the process illustrated in Figure 3.



KEY	MAJ	MAJOR	HAZ	HAZARDOUS
	CAT	CATASTROPHIC	RGS	Remote Ground Station

Figure 4: Security process overview

Some of the key phases in this process are outlined below.

Define the intended function of the system

This phase involves the definition and documentation of the intended functions of the system, to include customer-facing features, and maintenance/support functions. Increased connectivity in aircraft system functionality may introduce new risks associated with security vulnerabilities because Aerospace Recommended Practice ARP 4761[11] and similar safety guidelines do not consider deliberate unauthorized electronic interactions through exploits/attack. An initial assessment is also required to discover the security aspects of the interfacing system.

Connectivity to external devices or networks

It is necessary to determine whether any elements of the system are connected to external devices or networks. For each such connection, there needs to be consideration of whether the external device is trusted or non-trusted, authentication methods, data sharing mechanisms (source/sink), access mechanisms (read-only, read/write) and protection mechanisms.

Create (the) data flow diagram(s)

These data flow diagram(s) describe the communication between the components of the systems and components to external systems (networks/devices). The data flow diagram(s) should include both physical and logical flows.

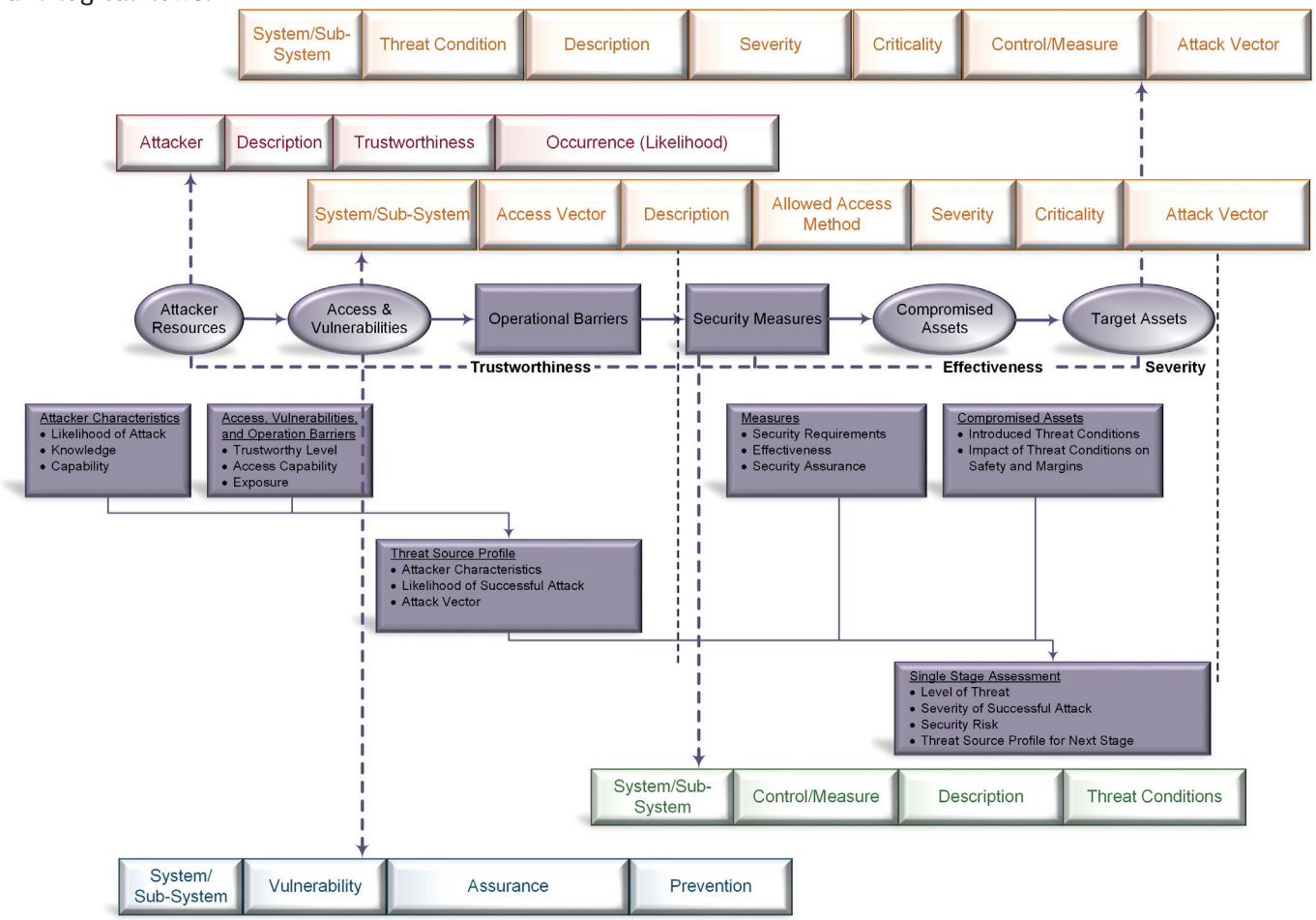


Figure 5: Security risk assessment (Image adopted from DO-356)

Evaluate connectivity impact to safety, and develop mitigations

Threat modelling is a structured approach to identifying and prioritizing potential threats to a system, and determining the value that potential mitigations would have in reducing or neutralizing those threats[12]. It defines threats and their mitigation in terms of assets, attackers, vulnerabilities access vectors, threat conditions, threat scenarios, and security measures.

[11] GUIDELINES AND METHODS FOR CONDUCTING THE SAFETY ASSESSMENT PROCESS ON CIVIL AIRBORNE SYSTEMS AND EQUIPMENT ARP4761, SAE International, 1996-12-01 https://www.sae.org/standards/content/arp4761/

[12] OWASP cheat sheet series – Threat Modeling Cheat Sheet https://cheatsheetseries.owasp.org/cheatsheets/Threat_Modeling_Cheat_Sheet.html

Threat conditions reflect the potential impact on the function under evaluation. This may include considerations of the loss of integrity, availability, or confidentiality associated with a function manifesting into a misleading or malfunctioning condition. Threat conditions may include failures that only have a safety effect in combination which might therefore be overlooked in the function-by-function, top-down deductive qualitative examination of Functional Hazard Analysis (FHA)[13], or the similarly granular bottom-up process deployed during System Safety Assessment (SSA)[14].

The risk associated with each threat depends on the likelihood of occurence, impact (severity) and remediation cost. The sophistication of the mitigation mechanism to be developed depends on the overall risk factor/score.

Conduct security assessment

Security threats identified in prior phases of the process are now evaluated. A popular threat assessment methodology is "DREAD" (**D**amage, **R**eproducibility, **E**xploitability, **A**ffected Users and **D**iscoverability). The probability of occurrence(**P**), Impact (**I**) and the risk are defined as (**R**+**E**+**DI**), (**D**+**A**) and (**P** x **I**) respectively. The threats are then prioritized according to risk score, and proprotionate actions (mitigations) are developed for each. These mitigations then need to be accounted for in the requirements process, verified, and validated.

The security assessment is then performed, during which the identified mitigations are reviewed against security, safety requirements and identified failures from the FHA (Figure 5).

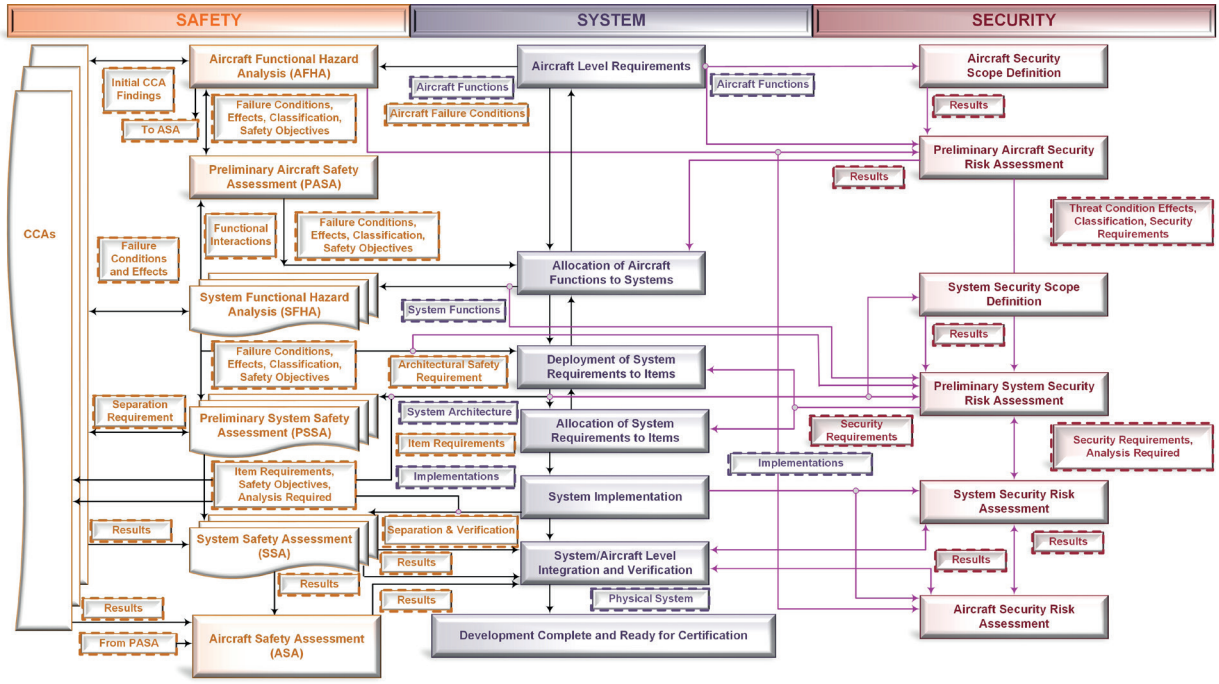


Figure 6: Security considerations as a sunset of the aircraft certification process (Image adopted from DO-356)

Validation & verification of security architecture, design, and implementation

The following verification and validation techniques are used to ensure that the mitigations are effective:

- security requirements testing
- threat mitigation testing
- abuse case testing
- static code analysis
- attack surface analysis
- known vulnerability scanning
- software composition analysis
- penetration testing

[13] Functional Hazard Analysis - Duane Kritzinger, in Aircraft System Safety, 2017 https://www.sciencedirect.com/topics/engineering/functional-hazard-analysis

[14] System Safety Assessment - Peng Wang, in Civil Aircraft Electrical Power System Safety Assessment, 2017 https://www.sciencedirect.com/topics/engineering/system-safety-assessment

The security development and risk assessment process V-model

The DO-326/ED-202 set provides a holistic life cycle approach for aerospace security , encompassing the planning stage, impact analysis, security risk assessment, security architecture design, security component implementation, validation/verification of security requirements, and security considerations for continuing airworthiness. It also provides a unified collaboration of system, safety, and security processes, activities and lifecycle products.

From security assessment, the threats, threat scenarios, and severity are analysed for impact on failure/ hazard conditions. Security architecture, design, and requirements are also coordinated with system development. Security implementation should not be attempted retrospectively, once system development is completed. The unified lifecycle approach calls for greater collaboration with multiple stakeholders from the safety, system, and security processes.

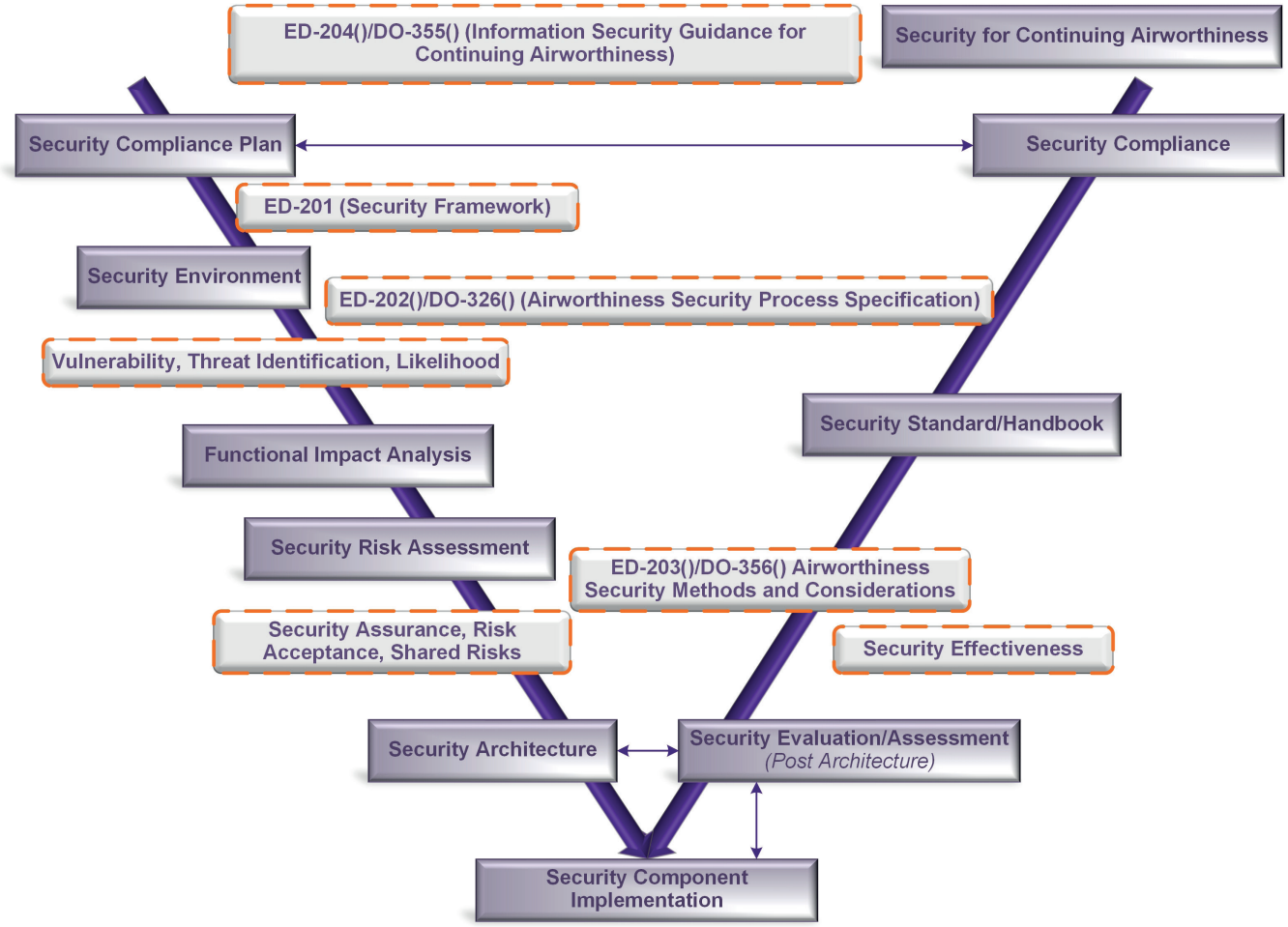


Figure 7: Security development and risk assessment process

Figure 7 illustrates how a security development life cycle can be represented in a V model-like requirement-based, safety-critical system/software development lifecycle.

The top guiding document is a security compliance plan; it is like any system/software certification plan, but the focus is entirely on the security layers within a defence-in-depth strategy (including embedded, system-level and network-level layers). The security environment encompasses the surrounding external/internal environment of the system under consideration.

Threats, vulnerabilities, and the probability of threat realization (leading to exploitation) are assessed thereafter. Each potential exploitation is considered for its potential impact on functionality and safety, and an initial risk assessment is carried out to know the extent of the impact of a possible attack/exploitation.

The mitigation methods or countermeasures are designed to thwart a possible attack or reduce the impact to an acceptable level. Once the security architecture and design are implemented, multiple verification techniques are employed to ensure that the mitigation/measures are effective against an attack.

There are other security considerations aside from the aerospace connected system. Associated systems could also be targeted, or sources of attack. These include:

- data centres for flight services
- database suppliers
- airline operations
- Maintenance, Repair and Overhaul (MRO) centres
- datalink service providers
- Central Maintenance Computer/Onboard Maintenance Systems (CMC/OMS)
- remote diagnostics units

The aerospace connected ecosystem is complex; due diligence and planning are required to ensure a safe working system without compromising airborne safety.

Using consultants for compliant projects

Aviation standards are demanding because they encompass systems (ARP 4754A/DO-297), safety (ARP 4761), security (DO-326A), software tool qualification (DO-330), software development (DO-178C) and programmable electronic hardware (DO-254). Some are long standing. For example, DO-178 was first published in its original form way back in 1981. Many development teams in companies across the world therefore have a great deal of experience in meeting the challenges posed by its latest successor, DO-178C.

For development teams new to this established sector, the existence of competitors who are more accustomed to finding a path through the maze of complex acronyms, terminology and cross references make it even more important to get it right first time and achieve certification goals. Conversely, more established players can always benefit from an optimized path through that aviation standards maze to keep cost and time overheads to a minimum.

It is, of course, entirely possible to develop a compliant system or application with no outside assistance at all. But to do so in a fashion that ensures a product of optimal quality, safety and cost is often far easier with a little help.

Developing systems and software that can be certified and used for safety- and security- critical functions in today's aircraft can be an extremely difficult task, with engineers constantly facing challenges related to cost, schedule, product safety, defects, regulations and other related factors. Although standards such as those in the DO-326/ED-202 set are logically structured and mandate recommended processes, they do not prescribe the characteristics and behaviour of the product. Engaging Subject Matter Experts (SMEs) to facilitate and reduce the cost of qualification and certification of systems and software seems an obvious way to mitigate those challenges.

Structured consultancy

When working within a context as clearly defined as a compliant flight system project, an expert consultancy can be equipped to define in quite specific detail just how their advice will be delivered, and what form it will take.

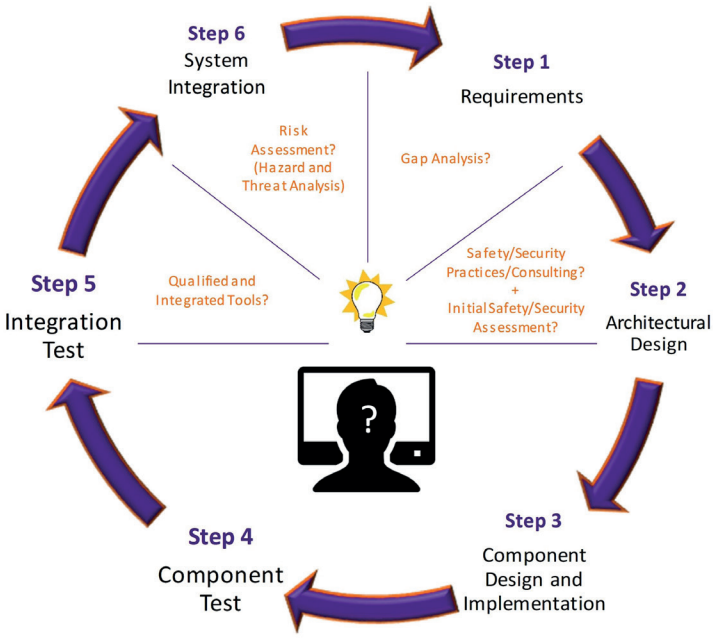


Figure 8: LDRA Safety & Security Services

LDRA Certification Services (LCS)[15] provides full life cycle solutions for suppliers, integrators and OEMs (Figure 7). LCS solutions help clients achieve compliance with aerospace security standards (in their totality or as tailored) and to safely clear their certification hurdles.

Support for projects compliant with the DO-326/ED-202 set

With specific reference to the DO-326/ED-202 set, LCS offers training on DO-326/ED-202 and associated guidelines (DO-355/ED-204, DO-356/ED-203, and ED-201) compliance, lifecycle process implementation and the creation of compliant life cycle data.

Process compliance support includes project and organizational Gap Analysis to determine the steps required to achieve compliance with DO-326, and assistance with the development of cybersecurity plans. Liaison services with interested parties including FAA, EASA, other government regulators, and end-customers help to ensure that communication remains unambiguous and fruitful. And Independent Verification and Validation (IV&V) services ensure end-customer and certification authority acceptance.

As development progresses through the lifecycle, more specific support is available for the specific actions incumbent on the the development team. For example, assistance is available with tool qualification (whether home-grown or Commercial Off-The-Shelf, or "COTS"), security assessments, and the development of manuals. LCS can also supervise and guide applicants in the development of vulnerability assessments, threat modeling, security design risk scoring (CVSS or FMECA – sidebar[16] [17]), and security verification. LCS can also call upon the integrated LDRA tool suite® for requirement traceability, static analysis, dynamic analysis, structural coverage, and system-level testing, and to ensure compliance with security coding standards including those from MISRA and CERT.

"The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes."

- **The FIRST organization**

"Failure Mode and Effects Criticality Analysis (FMECA) is an analysis technique which facilitates the identification of potential problems in the design or process by examining the effects of lower level failures.

Recommended actions or compensating provisions are made to reduce the likelihood of the problem occurring, and mitigate the risk, if in fact, it does occur."

- **FMEA-FMECA**

[15] LDRA Certification Services https://ldra.com/aerospace-defence/services-support/certification-services/

[16] CVSS: Common Vulnerability Scoring System https://www.first.org/cvss/

[17] FMECA: Failure Mode, Effects, and Criticality Analysis https://www.fmea-fmeca.com/what-is-fmea-fmeca.html

Summary

The challenge for authorities across the world is to establish a common security framework underpinned by most appropriate best-practice guidelines to form a robust and secure ecosystem. In 2019, the international guidelines DO-326A/ED-202A entitled “Airworthiness Security Process Specification” became the sole Acceptable Means of Compliance for FAA and EASA cybersecurity airworthiness certification.

The DO-326/ED-202 set provides a holistic life cycle approach for aerospace security, encompassing the planning stage, impact analysis, security risk assessment, security architecture design, security component implementation, validation/verification of security requirements, and security considerations for continuing airworthiness.

Tackling the technicalities can be a daunting task for newcomers and experienced pratitioners alike. LCS is engaged with multiple OEMs supporting their functional safety and cybersecurity goals, including compliance with the DO-326A/ED-202A set. LCS also supports suppliers in various capacities ranging from training, gap analysis, process compliance, and other customized solutions.

References

- ISO/IEC 27001 INFORMATION SECURITY MANAGEMENT
  https://www.iso.org/isoiec-27001-information-security.html
- National Institute of Standards and Technology (NIST)
  https://www.nist.gov/topics/cybersecurity
- FAA 14 CFR Part 25 – “AIRWORTHINESS STANDARDS: TRANSPORT CATEGORY AIRPLANES”
- EASA CS-25 “Certification Specifications for Large Aeroplanes”
- EASA AMC 25.1309 “Acceptable means of compliance – System Design and Analysis”
- AC 25.1309 - FAA Advisory Circular “System Design and Analysis”
- Commission Regulation (EU) No 748/2012 of 3 August 2012 - Airworthiness and Environmental Certification
  https://www.easa.europa.eu/regulations#regulations-initial-airworthiness
- PART 21—CERTIFICATION PROCEDURES FOR PRODUCTS AND ARTICLES
  https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=2bc3151798fc28602bb9091abdd1b77c&mc=true&n=pt14.1.21&r=PART&ty=HTML#se14.1.21_116
- EASA Easy Access Rules for Airworthiness and Environmental Certification
  https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=2bc3151798fc28602bb9091abdd1b77c&mc=true&n=pt14.1.21&r=PART&ty=HTML#se14.1.21_116
- EASA NPA 2019-01 Aircraft cybersecurity
  https://www.easa.europa.eu/document-library/notices-of-proposed-amendment/npa-2019-01
- GUIDELINES AND METHODS FOR CONDUCTING THE SAFETY ASSESSMENT PROCESS ON CIVIL AIRBORNE SYSTEMS AND EQUIPMENT ARP4761, SAE International, 1996-12-01
  https://www.sae.org/standards/content/arp4761/
- OWASP cheat sheet series – Threat Modeling Cheat Sheet
  https://cheatsheetseries.owasp.org/cheatsheets/Threat_Modeling_Cheat_Sheet.html

- Functional Hazard Analysis - Duane Kritzinger, in Aircraft System Safety, 2017
  https://www.sciencedirect.com/topics/engineering/functional-hazard-analysis

- System Safety Assessment - Peng Wang, in Civil Aircraft
  https://www.sciencedirect.com/topics/engineering/system-safety-assessment

- LDRA Certification Services
  https://ldra.com/aerospace-defence/services-support/certification-services/

- CVSS: Common Vulnerability Scoring System
  https://www.first.org/cvss/

- FMECA: Failure Mode, Effects, and Criticality Analysis
  https://www.fmea-fmeca.com/what-is-fmea-fmeca.html

www.ldra.com
LDRA

LDRA UK & Worldwide
Portside, Monks Ferry,
Wirral, CH41 5LH
Tel: +44 (0)151 649 9300
e-mail: info@ldra.com

LDRA Technology Inc.
2540 King Arthur Blvd, 3rd Floor, 12th Main Lewisville Texas 75056
Tel: +1 (855) 855 5372
e-mail: info@ldra.com

LDRA Technology Pvt. Ltd.
Unit B-3, Third floor Tower B, Golden Enclave
HAL Airport Road Bengaluru 560017
Tel: +91 80 4080 8707
e-mail: india@ldra.com

The Aerospace Security Framework v2.0 12/20