Safety versus Security in Aviation, Comparing DO-178C with Security Standards

Christoph Torens*
German Aerospace Center (DLR), Institute of Flight Systems, Braunschweig, Germany

Software development in safety-critical domains is dictated by software standards, such as "Software Considerations in Airborne Systems and Equipment Certification" (DO-178C). This standard is an acceptable means of compliance for achieving the required level of software safety in aviation. In addition to software safety, the security aspects of cyber-physical systems has become increasingly important in recent years, especially for unmanned aircraft systems with an increasing number of autonomous functions. The importance of this topic has grown with recent updates to security standards in 2018 and new regulations proposed by EASA in 2019. However, in literature, software safety and cybersecurity often get handled completely separate. Since most software engineers in aviation need to consider software safety and the corresponding DO-178C standard in some form, this work offers an introduction to the more recent software security standards. To do this, a brief overview of software standards as well as security standards is presented. The focus of the comparison between software safety and cybersecurity will be on "Airworthiness Security Process Specification" (DO-326A), as well as "Airworthiness Security Methods and Considerations" (DO-356A), since these standards, similar to DO-178C, also handle the initial airworthiness considerations. Additional standards, such as the standard "Information Security Guidance for Continuing Airworthiness" (DO-355) and others will also be introduced.

I. Introduction

Software safety and cybersecurity are becoming increasingly important with the growing number of highly automated systems [1]. With the predicted market growth of unmanned aircraft this might pose a serious and pervasive safety risk. Furthermore, while there might be high inhibition threshold in addition to the technical challenges for attacks on transport aircraft, this might not be the case for cargo drones and other unmanned aircraft. Autonomous systems have a high degree of software components and are typically interconnected in a system of systems, such as a network, communication or traffic management system. Therefore, autonomous systems are exposed to the risk of cyber threats to a significantly larger degree than manually operated systems. In contrast to manned systems, there is no immediate oversight of the systems, therefore threats may only be detected, if the damage has already occurred. Finally, automated systems can be easily scaled to very large numbers, opening up the possibility of very large incidents. There are examples for simple but effective cyber attacks on consumer drones as well as police drones [2] that show how vulnerable the systems can be. It is therefore necessary to stress the importance of cybersecurity considerations for autonomous and highly automated systems for future developments.

The goal of software safety is to avoid any possible failures from random causal chain that can lead to safety hazards. The goal of cybersecurity is to avoid any unauthorized access to systems to protect the airworthiness. Such an access with malicious intent could willfully force a causal chain that leads to a safety hazard [3]. Both topics are highly complex and a challenge for the development of modern systems, each on their own. Furthermore, both topics are related to software. However, they usually get handled completely separately.

The de facto standard regarding software safety is DO-178C [4]. The standard has several supplements that can be used in combination with the base document regarding specific topics, such as model-based development [5], object orientation [6], and formal methods [7]. Furthermore, there is a standard document regarding tool qualification [8]. The most comparable software standards regarding security in the aerospace domain are "Airworthiness Security Process Specification" (DO-326A) [9], "Information Security Guidance for Continuing Airworthiness" (DO-355) [10], and "Airworthiness Security Methods and Considerations" (DO-356A) [11]. All these documents are relatively new, the earliest documents are from 2010 and the latter document has recently been updated in 2018. An overview of standard documents for software safety and cybersecurity is given in Table 4.

*Research Scientist, Department of Unmanned Aircraft, AIAA Senior Member.

This work gives an overview and an introduction to the software security standards for aviation from a DO-178C software safety perspective. After this introduction, there will be a discussion on related work on safety and security standards in the research community in section II. Next, a brief overview of software safety standards will be given in section III, as well as cybersecurity standards in section IV. An analysis in section V will compare software and safety standards and discuss differences, before concluding in section VI.

II. Related Work

An early comparative analysis of selected software safety standards was performed by Wallace [3] to identify the attributes necessary for providing reasonable assurance, as well as identifying relative strengths and weaknesses of the different standards. This work provides a general rationale for standards: Standards serve as a yardstick for comparing systems. Also they provide reference to indicate minimum acceptable requirements and represent a commonly agreed-upon set of requirements for developers. Furthermore, standards make quality products more economical by providing common requirements. Finally, standards are a means of improving the state of practice. The author already recognizes that the same concepts could be used for ensuring computer security issues. In this work fifteen standards from different domains are qualitatively compared in the following criteria:

- Levels of Criticality/Assurance
- Lifecycle Phases
- Documentation
- Required Functionality
- Engineering Practices
- Project Planning and Management
- Procurement Concerns
- Presentation
- Security/Software Safety Issues
- Assurance Activities
  - Software Verification and Validation (V&V)
  - Software Quality Assurance (SQA)
  - Software Configuration Management (SCM)
  - Hazard Analysis

With these criteria also the differences between safety versus security are briefly assessed as one aspect of the assessment criteria: It is identified that software safety has much in common with computer security. Both fields are concerned with preventing certain undesirable events. While software safety seeks to avoid accidents that present a hazard to life or property, security is concerned with both accidents and malicious attacks. However, despite this similarity of concerns, the safety and security documents reviewed in this study found significant contrasts in presentation, level of detail, and approaches to assurance.

A more recent investigation on safety related standards was done by Esposito [12]. This study compares twelve standards from different domains, however the selection of standards does only consider safety. The paper discusses five categories of systems, from non-critical to both security and safety-critical systems. Specifically applying lessons from safety-critical systems to security critical software is discussed in [13]. This paper is written in the inverse perspective, looking at safety-critical standards from a security engineer's perspective. It is said that safety-critical systems are generally built and tested to much higher standards than is typical for even mission-critical information processing systems. A research gap is identified between security critical information processing systems and safety-critical process control systems. Approaches are discussed that could be introduced into developing secure systems, learned from safety-critical development standards. An analysis of cybersecurity standards is done in [14]. This work discusses industry standards for industrial control systems and compares them for best practices. It is called for standards that will couple safety and security together. This need for safety and cybersecurity co-engineering and standardization is further highlighted by [1], specifically for automated and autonomous vehicles. Such vehicles combine the challenges of safety-critical systems and security engineering in an unparalleled importance. Only the 2nd edition of IEC 61508, the standard on Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems has provided a first approach on integrating security requirements for functional safety. Specifically, DO-178B for safety and ISO/IEC standard for security in IT systems, the so called Common Criteria standard for security are compared in [15]. Programming language requirements for safety and security issues are identified. Subsequently, common programming languages are compared with respect to these requirements. However, the author concludes that safety and security is more about processes than language features.

To further highlight the importance of cybersecurity standards, EASA has recently issued the NPA 2019-07, titled Management of information security risks [16] as well as a terms of reference document Cybersecurity risks ISSUE 1 [17]. The concern is that not enough focus has been put in addressing situations where individuals may have a malicious intent. Therefore hazardous situations may not only result of a random event, but an event that was purposely created.

The document presents proposed amendments for existing regulation to cope with this.

III. Software Safety Standards

The DO-178 safety standard for aeronautical software has been in use since 1981 [18]. Basically, this is the standard that has to be applied for any safety-critical software in the aerospace domain. Updates to the standard have been published in 1984 [19] and 1985 [20] and most recently in 2011 [4]. This is a history of 38 years of standards use for software safety in the aerospace domain. With the latest update, there have been additional supplements, that can be used in conjunction with the base document DO-178C. The supplement documents for model-based development and verification [5], object-oriented technology [6] and formal methods [7] closely resemble the structure of the base document. They modify and extend the existing standard document in minimal changes to consider the discussed techniques as part of the main document. Additionally, there is a separate document on tool qualification [8], that can be used without the base document. The standard defines five software levels: level A to level E. The rigor of the software development increases from level E, where no objectives have to be met, for each level, up to level A, where all the objectives of the standard have to be met. A mapping of software components to the software levels is dependent on the system safety assessment. The idea of the standard documents is to establish rigorous development processes in combination with requirements-based testing, so that the resulting software is safe. As a result, the structure of the document focuses on lifecycle aspects and their corresponding requirements. The software standards documents have been reviewed, analyzed and applied in literature and also by previous work of the author [21]. But to give a comparative overview to the security standards, the high-level structure of DO-178C will be introduced briefly. The DO-178C standard is mostly targeted around its lifecycle processes: software planning, software development, software verification, software quality assurance, software configuration management and certification liaison. These processes are shown in Fig. 1. For each of these processes, certain activities are detailed that address the objectives that need to be verified to achieve certification. Annex A of the document combines these software lifecycle processes and the required output documents for certification. It shows tables for each of the software lifecycle processes and details the objectives and corresponding outputs according to the given software level, an overview is shown in Table 1. With increasing severity additional objectives have to be met and the number of objectives increases. Additionally, some of the objectives need to be fulfilled with independence, i.e. the verification activity has to be performed by a different individual or entity that performed the development activity.

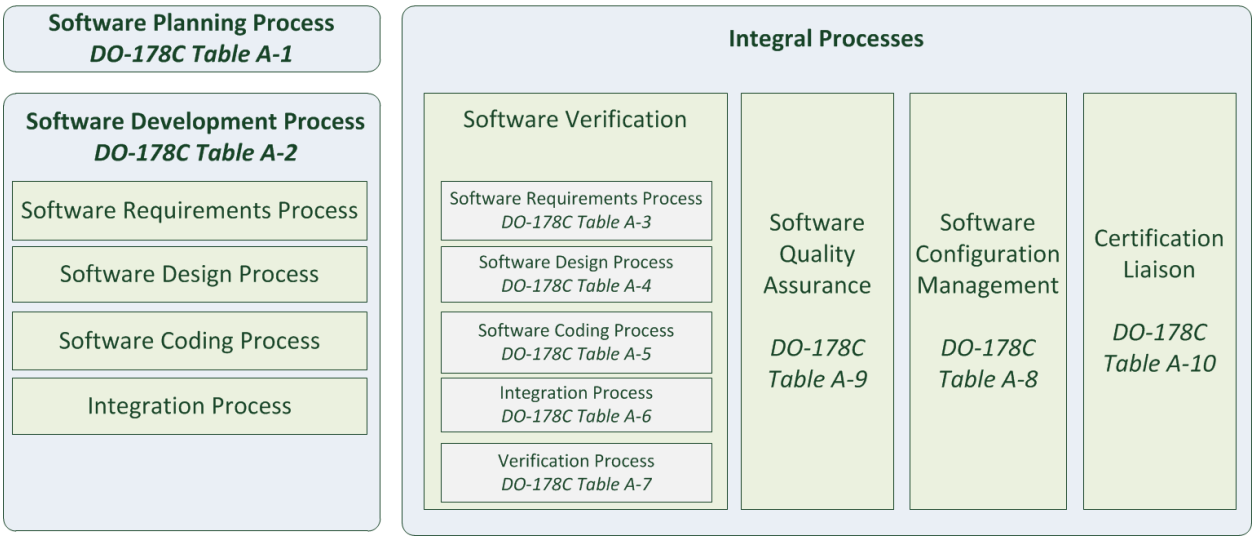

Fig. 1 Overview of DO-178C processes and sub-processes.

IV. Cybersecurity Standards

This section will briefly introduce each of the cybersecurity standards for the aerospace domain. To give a better overview, all mention standards are further detailed in the appendix in Table 4. The focus for comparison with software

Table 1 DO-178C Objectives and Data Items by software level, summarized from DO-178C [4].

Software Level	Failure Condition Category	Objectives	w. Independence
A	Catastrophic	71	30
B	Hazardous	69	18
C	Major	62	5
D	Minor	26	2
E	No Safety Effect	0	0

safety standards will be on DO-326A and DO-356A, since these standards are all related to the initial airworthiness of the aircraft.

A. ED-201 Aeronautical Information System Security (AISS) Framework Guidance

ED-201 is an overview document, giving context to the other mentioned standard documents. It was issued in 2014 by EUROCAE and there is no counterpart on US side. The document summarizes briefly each of the cybersecurity standards and gives an overview of the standard documents. The standard is helpful when starting with the cybersecurity topic, and introduces basic concepts, but it does not contain specific guidance information. Additionally, the cybersecurity standard package is compared to similar standards from ISO, ICAO, and NIST.

B. DO-356A / ED-203A Airworthiness Security Methods and Considerations

DO-356A acts as a companion document to DO-326A and describes the activities for security risk management and security assurance. These documents are codependent on each other, as DO-326A describes the activities and DO-356A describes the guidance information for that activities. There is also an appendix that maps activities and guidance between these standards. With 370 pages, this is the largest document of the security package. It contains detailed information on the risk assessment of cybersecurity threats, information that is relating to the aircraft level of development. But the document also contains details on security specific assurance as well as security development assurance, which is information on the system and item development level. Furthermore, this document introduces security assurance levels 0 to 3, with increasing level of criticality. Security architecture principles are detailed at aircraft level, system-level and item level. An extensive appendix details on security assurance objectives, security assurance guidance and give several other guidance information, including examples.

C. DO-355 / ED-204 Information Security Guidance for Continuing Airworthiness

DO-355 is the counterpart for DO-356A for continuing airworthiness. This document provides guidance for the continuing airworthiness of an aircraft, specifically for the following lifecycle processes: operation, support, maintenance, administration and deconstruction. The document gives information on airborne software, components, ground support equipment and operator roles, responsibilities and training. The idea is that in combination with DO-326A, the complete product lifecycle is covered. The document is structured, so that for each topic, there are general information, operational security measures, design approval holder responsibilities and operator responsibilities.

D. ED-205 Process Standard for Security Certification and Declaration of ATM ANS Ground Systems

This document handles the cybersecurity aspects for ATM/ANS ground system considerations for certification. There is no US counterpart for the standard. One argument is that in the US, in contrast to Europe, ATM is performed by the government. As such, in the US there is no need for guidance for commercial service providers, so the document is not needed. The security process describes planning for security aspects, management of security risks, certification claims and evidences and compliance verification. For software safety, there are also separate documents for aircraft certification and ground systems certification DO-278A. However, these documents are very much alike and differ mostly in the assurance level definition.

E. ER-013 Aeronautical Information System Security Glossary

This document is a glossary containing all the definitions for terms used within the discussed cybersecurity standard package.

F. ER-017 International Aeronautical Information Security Mapping Summary

This document can be described as a reference document. Existing standards as well as ongoing standardization efforts were conducted in a joint EASA/EUROCAE workshop in 2017. The document lists all these standards and gives information on the status and links if these are available.

G. DO-326A/ED-202A Airworthiness Security Process Specification

The standard DO-326 Airworthiness Security Process Specification was issued in 2010. The latest update, DO-326A was issued in 2014. It is the oldest of the three main discussed standards for security in this work. Compared to the almost 40 years in software safety, the history in security standards is only 9 years. The document provides guidance for the development and certification processes to include aspects of safety of the aircraft. It defines Airworthiness security as the protection of the airworthiness of an aircraft from unauthorized interaction. Similar to the software safety standards mentioned above, this standard also handles the initial airworthiness, i.e. the software lifecycle phases until the type certification is issued. Due to the conceptual similarity DO-178C, this comparison focuses mainly on DO-326A for security aspects. The main content is the description of the airworthiness security processes: security risk assessment process and security development process, see Fig. 2. Compared to the traditional aircraft development process, the standard introduces two additional layers into the development process with two activities each. On the left-hand of the V-Model the two development activities are a preliminary security risk assessment (PASRA) on aircraft level and a on system level (PSSRA). Of course, these two activities have the corresponding verification activities on the right hand side of the V-Model, a security risk assessment for aircraft level (ASRA) and system level (SSRA). The Fig. 3 is a combination of the aircraft development process shown in ED-79A/ARP 4754A and the information on security risk assessment and security development activities from DO-326A. The purpose of the Airworthiness Security Process (AWSP) is that when there is an unauthorized interaction, the aircraft will always remain in a condition for safe operation. The goal is to establish the security risk to the aircraft and its systems is acceptable (as analyzed by the AWSP). Furthermore, it must be shown that the airworthiness security risk assessment is complete and correct. The process uses the same model as the safety process and allows for the adaptation of the effort needed to establish security, depending on the severity of failure/threat.

Besides describing the Airworthiness Security Process itself, the document emphasizes on explaining fundamental security concepts and definitions. Concepts such as Security Scope Definition, Security Risk Assessment, considerations about the Security Development activities, and the assignment of security effectiveness requirements are explained. Additionally, there is a chapter regarding modifications to aircraft and systems, including Supplemental Type Certification (STC) and Amendments to Type Certification. Appendix A introduces the details of the Airworthiness Security Process activities, their interfaces and artifacts, the dependencies between those activities and the dependencies with activities that are part of the safety assessment process or the system development process, as per ED-79A/ARP 4754A. For each of these plans, the appendix shows a description, detailing the purpose, details, input and output, and compliance objectives. An overview of security certification plans by severity of effect is given in Table 2. This table is similar to Table 1. However, the granularity is given at the level of plans and not at the level of objectives. Furthermore, there are plans that are categorized "as negotiated", this means that it has to be agreed on a case-by-case basis if this plan needs to be submitted to the certification authority.

Table 2 Overview of Security Certification Plans by Severity Effect, summarized from DO-326A [9]

Security Assurance Level	Severity	Recommended	w. Independence	AsNegotiated
3	Catastrophic/Hazardous	5	2	3
2	Major	5	0	3
1	Minor	0	0	8
0	None	0	0	0

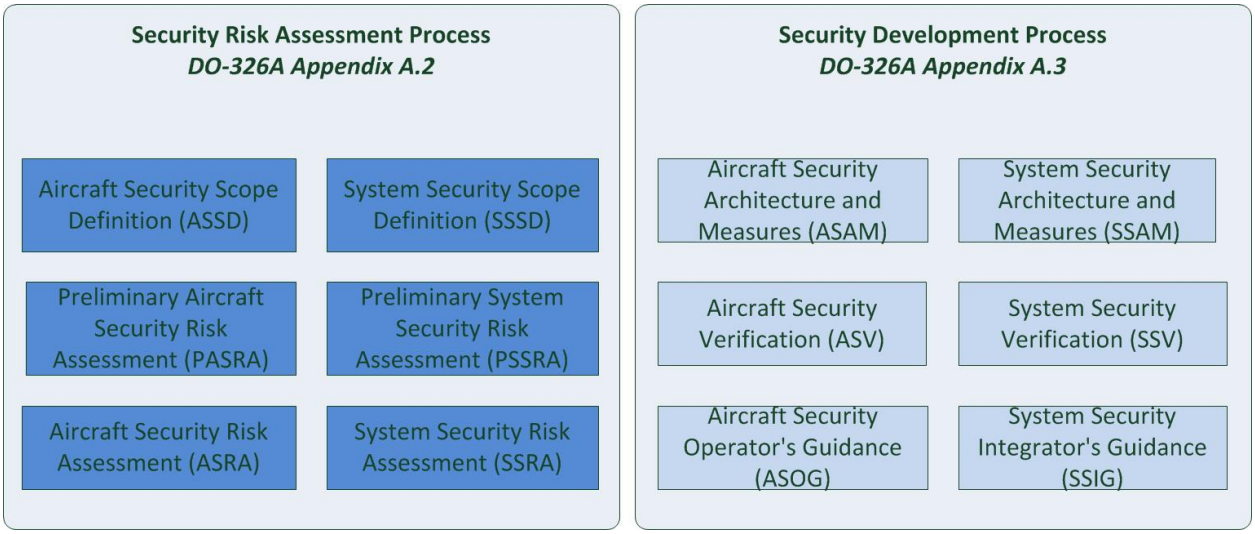

Fig. 2 Overview of DO-326A processors and corresponding activities. Security risk assessment activities are colored dark blue and security development activities are colored light blue to match the colors in Fig. 3.

V. Comparison and Analysis of Software Safety versus Cybersecurity

Specifically the standards DO-178C and DO-326A both address the initial airworthiness of the aircraft certification process. The structure of the documents are different, although both standards define process requirements. Also, both standards define activities, the relationship between the activities and outputs for these activities. The comparison of these activities is shown in Fig. 3.

Although the software safety standards mentioned above are directly targeted towards software, the cybersecurity standards do not focus on software but rather on a system and aircraft perspective. However, as discussed in the related work section, there is a huge connection and demand for stronger combination of the two topic areas. The following sections will discuss the corresponding cybersecurity standards by comparison with the software standards in those categories that were used for the comparison and assessment of standards by Wallace [3].

A. Levels of Criticality/Assurance

This criteria assesses if software requirements are based on the consequence of system failure. If there are different levels of criticality established, it is possible to scale the efforts of the development towards the risk that is involved with running the software.

DO-178C defines five software levels, level A (highest criticality), to E (no criticality). These levels are mapped to failure condition category levels (catastrophic, hazardous, major, minor, no safety effect) by a higher level risk assessment. Similar, but not identical to this, DO-326A does not define security levels, but directly addresses the aircraft security by reference to the aforementioned failure condition categories levels. The difference originates in the different scope of the standards as discussed in the next subsection. DO-356A defines four security assurance levels 0 to 3, with 0 having no security impact and 3 having the largest security impact. Compared to software levels or failure condition categories, there is one level less for security. The relation is that catastrophic and hazardous failure conditions both map to a minimum security assurance level of 3. However, catastrophic failure conditions require not one but two independent, diverse and isolated security measures, one at level 3 and one at level 2. While DO-178C details the requirements for each software level on objectives level (cf. Table 1) and differentiates that these requirements need to be fulfilled, fulfilled with independence or else do not have to be fulfilled; the cybersecurity standards detail the requirements for each safety assurance level on the software plan level (cf. Table 2) and differentiates between recommended plans, recommended plans with independence and else as negotiated with the certification authority. Thus, these concepts differ largely between the software and cybersecurity standards.

B. Lifecycle Phases

This criteria looks at the lifecycle phases. Does the standard cover the complete system lifecycle, including the integration of software within the total system, or does it cover specific software lifecycle phases?

The standard DO-178C itself defines only processes for the software lifecycle phases, cf. Fig. 1. However, the overall process is embedded into the higher level aircraft development process, as described in ARP4754A/ED-79A. The aircraft development process is described as a V-Model, with the software development being the most inner part of the V-Model. Reference to the higher level aircraft development process is given by discussing the software levels in context of the failure condition categories and its required integration into the safety assessment process. On the other hand, the software security standards integrate tightly within the aircraft development process. The processes described in DO-326A complement the aircraft safety risk assessment with a security risk assessment. Therefore, the scope of the standards is quite different. In terms of scope the standard DO-326A is more comparable to the scope of ARP4754A/ED-79A for aircraft development, cf. Fig. 3.

C. Documentation

With this characteristic, the question is if there are any requirements for the software documentation. Does the standard specify the contents that must be described or does it specify the description of elements?

Both safety and security standards define documents, and detail the requirements for these documents in the form of objectives and activities. However, while DO-178C describes software plans, objectives and activities, DO-356A does not describe plans but only objectives. It is worth noting, that the combined cybersecurity guidance exceeds software safety guidance not only in standard document pages (Table 4), but also in the number of objectives required for certification (Table 3).

Table 3 Overview of Plans and Objective Requirements for Safety and Seccurity Standards

Standard	Topic	Plans	Objectives
DO-178C / ED-12C	Software	5	71
DO-326A / ED-202A	Cybersecurity	2	54
DO-356A / ED-203A	Cybersecurity	-	39

D. Required Functionality

This criteria asks if there are requirements specified for failsafe systems, failure detection, or fail operational behavior. Is the crash of the system or the system restart discussed by standards?

In this category, both types of standards do not mandate any requirements on the functionality. The goal for software safety is of course a failsafe system, a system that can fail without the loss of life. As such, there is some discussion on redundancy and also monitoring as discussed in the software safety standard to detect failures. However, in general the standards do not mandate requirements and functionality, since these standards are mostly process driven.

E. Engineering Practices

Is there guidance on recommended engineering practices, such as formal specifications, critical component isolation, modularity, high order languages or deprecated programming practices?

The discussion in Wallace [3] declares that DO-178A does not contain any guidance on engineering practices. However, since then follow-up documents, including the supplement documents on object-oriented techniques, model-based development, and formal methods has been published. With these additional documents, there is a lot of guidance material on engineering practices. On the cybersecurity part, the document DO-356A gives guidance material on implementing security aspects into system architectures.

F. Assurance Activities

This criteria discusses the requirements for Software Verification and Validation (V&V), Software Quality Assurance (SQA), Software Configuration Management (SCM), and Hazard Analysis.

DO-178C contains process descriptions for V&V, SQA, and SCM, while hazard analysis is performed on the aircraft development process level. The cybersecurity package contains guidance on hazard analysis, and also some guidance on V&V and configuration management.

G. Project Planning and Management

This criteria discusses the requirements and guidance on project planning and management.

Both standards detail on the planning and management of the development processes. DO-178C describes plans for the processes as shown in Fig. 1. The cybersecurity standards add the plan for security aspects of certification as well as a summary document.

H. Procurement Concerns

This criteria discusses concerns about the people developing and evaluating the system. Are there requirements on quality management and independence? And what are the qualifications for developing these kind of systems?

There is no specific requirement on the qualification for developers. However they is the requirement of independence for verification activities for certain objectives, specifically for objectives for higher software level as well as for higher security assurance level.

I. Presentation

This criteria discusses the presentation of the standard and its requirements. Are the requirements specified disorderly or ambiguous? Are different categories of requirements intermixed or are they specified in different sections?

The main issue about the presentation for the software standards is that the level of scope is different for the software safety and for the cybersecurity standards. While these software safety standards does focus on the software development processes, embedded in the higher level aircraft development process, this cannot be said for the cybersecurity standards. Cybersecurity integrates into the aircraft development process at different stages throughout the development processes.

J. Security/Software Safety Issues

Is software security discussed in combination with software safety or is only one topic addressed by the standard?

DO-178C does not contain any guidance on cybersecurity. The cybersecurity standards also refer to the software safety guidance, since there are some development activities identified that also support cybersecurity aspects. As such, the security objectives are differentiated into security specific assurance and security development assurance. A section in DO-356A describing these objectives also details so called development assurance augmentation considerations that explain how an existing development process can be augmented to fulfill these objectives. Also, the appendix details for each objective if it is security specific assurance or not.

VI. Conclusion

The two worlds of safety and security have in the past been considered mostly separated. On one hand, there exist industrial control systems and information management systems that needs to be secured against cyber threats, but in most cases without concerns on safety. On the other hand, there exist safety-critical systems, such as aircraft that historically have had only limited interfaces to external systems. Often in such cases, the interfaces can be access controlled to further limit the threat. However, aircraft are increasingly exposed to external systems with increasing levels of data exchange for flight systems. And in addition to that, supporting the use of mobile phones, laptops, wireless networks in aircraft as well as the flight entertainment system for passengers pose additional security risks. With the increasing automation of systems and the integration of unmanned aircraft into the airspace, a new dimension of security concerns is coming up. It is therefore necessary to consider cybersecurity concerns in addition to existing safety processes. Updated standards and regulations highlight the importance of security for future developments.

Software and security standards are focused on process assurance in the aviation domain. One of the main information of the standards are the required processes, their plan descriptions, required activities and their objectives. Although there are a lot of commonalities between software standards and the security standards, there are also a lot of differences. Arguments for both can be found in the assessment of the specific criteria for standard documents. The main issue is that the scope and structure of the security standards is completely different to the traditional aircraft and software development standards. The security standards contain information at different levels of scope, and with

different numbers for criticality levels. From a software development perspective, cybersecurity is mainly integrated into the development process through processes at aircraft development level that assess and verify additional security requirements. But there are also additional security development and security specific activities and objectives.

This work tries to give an introduction to the cybersecurity standards from the software safety perspective. The goal is that more developers can integrate aspects of security into their development activities and thinking. It is a huge effort to go through almost 500 pages of standard documentation for cybersecurity with its over 90 activities. And this is only considering the cybersecurity standards DO-326A and DO-356A. Although all standards are important, these two standards consider the initial airworthiness and thus are most related to the development processes known to engineers concerned with the software development and the DO-178C standards. But since the cybersecurity standards directly relate to safe software development activities for certification credit, it is necessary to learn about the standards and incorporate cybersecurity thinking into the development activities, especially for safe software developers in the aerospace domain. However, assessing the security standards and processes, it is evident that security is a topic that is not a pure software topic and instead has to be integrated into the aircraft development process at the highest level.

References

[1] Schoitsch, E., Schmittner, C., Ma, Z., and Gruber, T., "The Need for Safety and Cyber-Security Co-engineering and Standardization for Highly Automated Automotive Vehicles," *Lecture Notes in Mobility*, 2015.

[2] Tewes, J., "Cybersecurity as Airworthiness," *Available at SSRN 3033898*, 2017.

[3] Wallace, D. R., Kuhn, D. R., and Ippolito, L. M., "An Analysis of Selected Software Safety Standards," *COMPASS '92 Proceedings of the Seventh Annual Conference on Computer Assurance*, 1992.

[4] Radio Technical Commission for Aeronautics, *DO-178C/ED-12C Software Considerations in Airborne Systems and Equipment Certification*, RTCA, Washington, D.C., 2011.

[5] Radio Technical Commission for Aeronautics, *DO-331/ED-218 Model-Based Development and Verification Supplement to DO-178C and DO-278A*, RTCA, Washington, D.C., 2011.

[6] Radio Technical Commission for Aeronautics, *DO-332/ED-217 Object-Oriented Technology and Related Techniques Supplement to DO-178C and DO-278A*, RTCA, Washington, D.C., 2011.

[7] Radio Technical Commission for Aeronautics, *DO-333/ED-216 Formal Methods Supplement to DO-178C and DO-278A*, RTCA, Washington, D.C., 2011.

[8] Radio Technical Commission for Aeronautics, *DO-330/ED-215 Software Tool Qualification Considerations*, RTCA, Washington, D.C., 2011.

[9] Radio Technical Commission for Aeronautics, *DO-326A Airworthiness Security Process Specification*, RTCA, Washington, D.C., 2014.

[10] Radio Technical Commission for Aeronautics, *DO-355 Information Security Guidance for Continuing Airworthiness*, RTCA, Washington, D.C., 2014.

[11] Radio Technical Commission for Aeronautics, *DO-356A Airworthiness Security Methods and Considerations*, RTCA, Washington, D.C., 2018.

[12] Esposito, C., Cotroneo, D., and SIlva, N., "Investigation on Safety-Related Standards for Critical Systems," *2011 First International Workshop on Software Certification*, IEEE, 2011. doi:10.1109/wosocer.2011.9.

[13] Axelrod, C. W., "Applying Lessons from Safety-Critical Systems to Security-Critical Software," *2011 IEEE Long Island Systems, Applications and Technology Conference*, IEEE, 2011.

[14] Piggin, R. S. H., "Development of Industrial Cyber Security Standards: IEC 62443 for SCADA and Industrial Control System Security," *IET Conference on Control and Automation 2013: Uniting Problems and Solutions*, 2013.

[15] Brosgol, B., "Safety and Security: Certification Issues and Technologies," *The Journal of Defense Software Engineering*, 2008.

[16] European Union Aviation Safety Agency, "Notice of Proposed Amendment 2019-07, Management of information security risks, RMT.0720," Tech. rep., 2019.

[17] European Union Aviation Safety Agency, "Terms of Reference, Cybersecurity risks Issue 1, RMT.0720," Tech. rep., 2019.

[18] Radio Technical Commission for Aeronautics, *DO-178 Software Considerations in Airborne Systems and Equipment Certification*, RTCA, Washington, D.C., 1981.

[19] Radio Technical Commission for Aeronautics, *DO-178A Software Considerations in Airborne Systems and Equipment Certification*, RTCA, Washington, D.C., 1985.

[20] Radio Technical Commission for Aeronautics, *DO-178B/ED-12B Software Considerations in Airborne Systems and Equipment Certification*, RTCA, Washington, D.C., 1992.

[21] Torens, C., Adolf, F.-M., and Goormann, L., "Certification and Software Verification Considerations for Autonomous Unmanned Aircraft," *Journal of Aerospace Information Systems*, Vol. 11, No. 10, 2014, pp. 649–664.

VII. Appendix

A. Software Safety and Cybersecurity Standards Overview

Table 4 Overview of active and *superseded (displayed in italics)* standard documents for software safety and cybersecurity.

RTCA Std	EUROCAE Std	Title	Published*	Pages†
DO-178C	ED-12C	Software Considerations in Airborne Systems and Equipment Certification	2011	144
DO-178B	*ED-12B*‡	*Software Considerations in Airborne Systems and Equipment Certification*	*1985*	*116*
DO-178A	*ED-12A*‡	*Software Considerations in Airborne Systems and Equipment Certification*	*1984*	*68*
DO-178	*ED-12*‡	*Software Considerations in Airborne Systems and Equipment Certification*	*1981*	*76*
DO-330	ED-215	Software Tool Qualification Considerations	2011	138
DO-331	ED-218	Model-Based Development and Verification Supplement to DO-178C and DO-278A	2011	136
DO-332	ED-217	Object-Oriented Technology and Related Techniques Supplement to DO-178C and DO-278A	2011	150
DO-333	ED-216	Formal Methods Supplement to DO-178C and DO-278A	2011	118
DO-278A	ED-109A	Software Integrity Assurance Considerations for CNS/ATM Systems	2011	150
-	ED-201	Aeronautical Information System Security (AISS) Framework Guidance	2015	60
DO-326A	ED-202A	Airworthiness Security Process Specification	2014	88
DO-326	*ED-202*‡	*Airworthiness Security Process Specification*	*2010*	*102*
DO-356A	ED-203A	Airworthiness Security Methods and Considerations	2018	370
DO-356	*ED-203*‡	*Airworthiness Security Methods and Considerations*	*2014*	*80*
DO-355	ED-204	Information Security Guidance for Continuing Airworthiness	2014	78
-	ED-205	Process Standard for Security Certification and Declaration of ATM ANS Ground Systems	2019	62
-	ER-013	Aeronautical Information System Security Glossary	2015	37
-	ER-017	International Aeronautical Information Security Mapping Summary	2018	28

*The date of publication can vary about one year between RTCA and EUROCAE documents, due to individual publication of the document.
†The number of pages can vary slightly between RTCA and EUROCAE documents, due to different formatting.
‡Superseded ED documents are not longer available for access.

B. Cybersecurity as Part of Aircraft Development Lifecycle

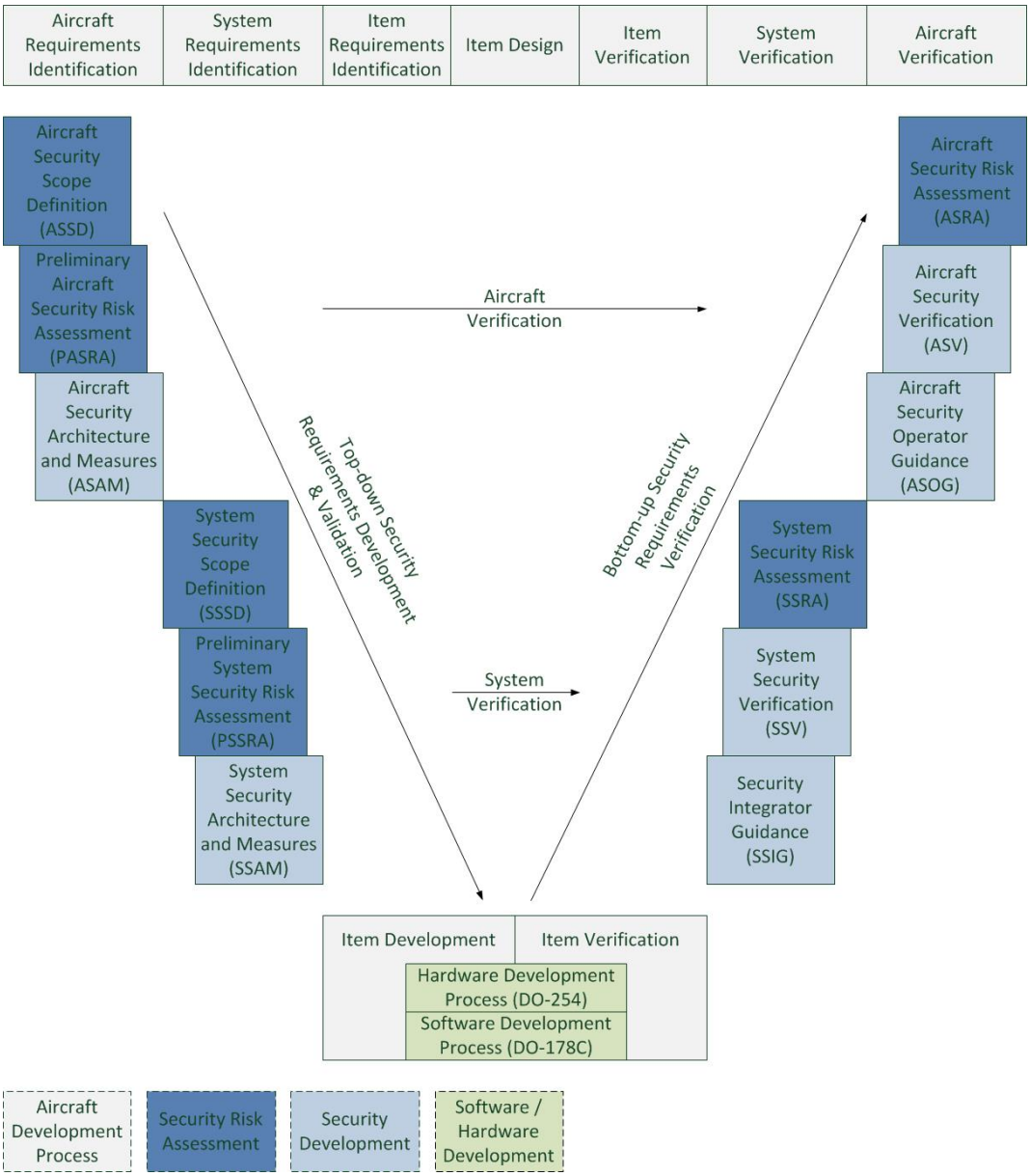

Fig. 3 Security process and software development process as part of the aircraft development process, adapted from DO-326A [9] and ARP4754A/ED-79A.