TRENDS AND CHALLENGES IN THE AVIATION SYSTEMS SAFETY AND CYBERSECURITY

JANUSZ ZALEWSKI[1] AND ANDREW KORNECKI[2]

[1]*Florida Gulf Coast University*
Ft, Myers, FL 33965, USA

[2]*Embry-Riddle Aeronautical University*
Daytona Beach, FL 32114, USA

(received: 4 February 2019; revised: 12 March 2019;
accepted: 20 March 2019; published online: 28 March 2019)

Abstract: Aviation systems are an essential component of every nation's critical infrastructure. Considering millions of passengers flying per year and busy airports, the safe and secure flight and traffic operation is of primary importance to the proper functioning of the society. This paper discusses fundamental problems of providing critical systems safety and cybersecurity in the aviation infrastructure including both airborne and ground systems such as avionics, navigation, air traffic control and management, as well as unmanned systems. It reviews the major challenges and current trends in providing viable solutions. Both industrial practices and research approaches are mentioned, including established methodologies and standards, as well as new developments in certification.

Keywords: aviation safety, cybersecurity, software safety, safety standards, safety guidelines, unmanned aircraft systems, aircraft certification

DOI: https://doi.org/10.17466/tq2019/23.2/a

1. Introduction

Transportation systems play a critical role in every nation's social and economic infrastructure. The most common examples include air, maritime, automotive and railway transportation. Their safe and secure operation is of primary importance to the proper functioning of the society and involves huge investments by the government and all respective industries.

The basic feature of all transportation systems is that they are a part of the environment and are widely used by millions of people. Systems supporting all kinds of transportation must be dependable, which means that users and customers can rely on their operation. However, the critical issue for such systems

is not only to provide dependable transportation services, but to avoid and prevent accidents. An accident is a specific, typically unpredictable and unintended event not necessarily with an apparent cause but with noticeable negative effects to the people and environment. Safety is a property of the system which is designed to assure that the accidents will not occur. If circumstances potentially leading to an accident are recognized and acted upon, prior to its occurrence, safety violation can be avoided.

Additionally, in a modern society, where literally everything is interconnected, the progress of computing technology and increasing reliance on software with its abundant features brought cybersecurity to the forefront as another aspect of safety consideration. In industrial computer systems, in general, and particularly in transportation systems, cybersecurity must be taken into account primarily for the reasons to assure safety. This contrasts with business systems, such as commerce, banking, insurance, *etc.*, for example, where cybersecurity is the sole critical issue.

While each individual segment of the transportation industry plays an important role in the entire picture, this paper focuses on the technical and procedural approaches required to provide safety and cybersecurity in aviation. The rest of the paper is structured as follows. The next section discusses basic concepts of computer safety in aviation. Section 3 covers the cybersecurity and its relationship to safety. Sections 4 and 5 discuss safety and cybersecurity issues in airborne systems and ground systems, respectively, as two sides of the same problem. Section 6 outlines the latest developments in unmanned systems' safety and security, Section 7 addresses certification issues and Section 8 presents the conclusions and future challenges.

2. Basic Concepts and Definitions of Computer Safety

Safety, as one of the dependability properties illustrated in Figure 1, is usually defined as a "negative" property. The user's or system designer's view is to strive achieve guarantees on system behavior in terms of risk, ensuring that "nothing bad will happen" or that the risk of "something bad may happen" is low. The safety risks are usually analyzed involving potential hazards that are related to computer failures (both hardware and software). In terms of risk and failures, the roles of three major system dependability properties from the perspective of the environment can be described as follows:

- *Safety*, when a failure leads to negative consequences (high risk) to the environment;
- *Security*, when a failure leads to negative consequences (high risk) to the computer system itself;
- *Reliability*, when failure may not necessarily lead to negative consequences (high risk) to the environment or a computer system, however, the system does not perform its expected functions.

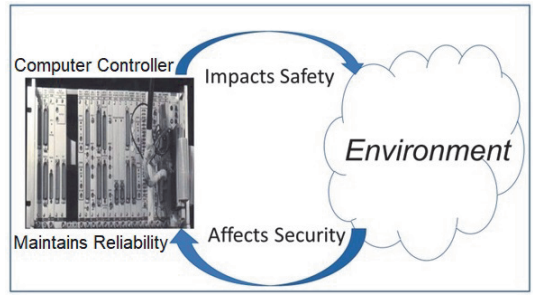

Figure 1. Illustration of dependability properties of computer control systems

In other words, safety is a system property that prevents the system from doing damage, regardless of any potential failures, not causing accidents, *i.e.*, undesirable events that may bring substantial harm to people or environment. Safe system has defined mechanisms able to control recognized hazards, thus achieving an acceptable level of risk. The risk management strategy is based on identification and analysis of hazards and application of mitigation measures using a systems-based approach. In this view, risk management is the basis of system safety.

3. Increasing Impact of Cybersecurity with Safety Implications

The progress of microelectronic technology, integrated scalable multiprocessor systems, better sensors and displays, increased interconnectivity, and powerful software tools are the basis for achieving greater flexibility of modern systems. The hardware is designed with spare capacity (memory, processor speed, data throughput) so limitless modifications and functionality upgrades are possible by the software implementation. All this causes increased concerns about security breaches by adversaries, which may have very negative impact on safety.

Computer security has been understood primarily as the means to protect the system assets but this traditional view, entirely justified and warranted, obscures the scientific approach to security viewed as a system property. Cybersecurity can be thus viewed as the extent to which a computer system is protected from external threats and attacks on its information and data, so that unauthorized persons or systems cannot read or modify them, while authorized persons or systems are not denied access to them.

In this view, cybersecurity reflects three essential aspects. First, it pertains to protecting information from unauthorized reading, which means Confidentiality. Second, it concerns protecting information from unauthorized modification, which means keeping its Integrity. And finally, what the concept captures quite well is the fact that the secure system must be not only protected against unauthorized access and threats but also accessible to those authorized, which means its Availability. This is the real meaning of the often-quoted acronym: C-I-A = Confidentiality + Integrity + Availability. Even though this traditional

understanding of security properties is important, the critical cybersecurity aspect for transportation systems is that cybersecurity breach would not result in a safety violation and related accidents.

Safety and security are two sides of the same coin, as shown in Figure 1. Whereas safety is about negative consequences that the system may inflict on the environment, cybersecurity is considering how the environment may negatively affect the system (with subsequent impact on safety). According to International Electrotechnical Commission (IEC) [1], safety is defined as "freedom from unacceptable risk to the outside from the functional and physical units considered", whereas security is defined as "freedom from unacceptable risk to the physical units considered from the outside".

Safety and security both concern factors that can relate the computer system to its surroundings, commonly called the environment. The external influences are included as an unknown factor in the design, but because their detailed characteristics are unknown, they are collectively grouped into disturbances. Unintentional disturbances are known as hazards and are considered in processes assuring safety. Intentional disturbances are called threats and commonly used by attackers, so must be included in processes assuring security. Human errors, also called mistakes, obviously contribute to the problem. These factors are illustrated in Figure 2 showing how external events affect both safety and security.

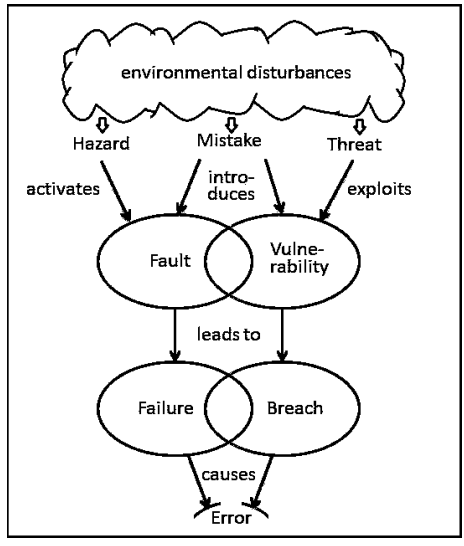

Figure 2. Parallels between external factors affecting safety and security [2]

These concepts showing mutual relationships between safety and security are additionally illustrated in Table 1, with definitions from respective professional vocabularies.

As transportation systems interact with and control the environment, safety and cybersecurity must be considered for the system operations in normal as well

Table 1. Illustration of a dualism between safety and security concepts [3]

Security			Safety		
Concept	Definition	Consequences	Concept	Definition	Consequences
threat	Any circumstance or event with the potential to adversely impact an information system through unauthorized access destruction, disclosure, modification of data, and/or denial of service. [CNSS]	Exploits vulnerabilities	hazard	Intrinsic property or condition that has the potential to cause harm or damage. [SSEV]	Activates a fault
vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that co exploited. [CNSS]	Results in a breach	fault	Manifestation of an error in software. [SSEV]	Results in a failure
breach	An event in which a system or system component is compromised, so its required functions within specified limits a impaired. [Author]	Leads to losses	failure	Termination of the ability of a system to perform a required function or i specified limits. [SSEV]	Leads to harm or damage
SSEV – Software and Systems Engineering Vocabulary [4] – `http://computer.org/sevocab` CNSS – Committee on National Security Systems Glossary [5] – `https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf`					

as in abnormal conditions. The approaches were developed to take a broader view of potential accident causes than just component failures. The emphasis is on building in safety and security rather than adding the related considerations to a completed design. The next sections review these aspects in airborne as well as ground-based systems.

4. Airborne Systems

Safety is a critical factor for aviation. The progress of technology, particularly in electronics and computing domains significantly transformed the aviation industry over the last decades. An aircraft is a large system composed of multiple mechanical and electronic sub-systems controlled by software. There is a popular saying in the community that modern aircraft is just "a computer with wings". Typical software-intensive systems in modern aircraft include flight control with autopilot, displays, navigation, communication, engine control, ground steering, thrust reversers, air data, landing gear, collision avoidance, environmental control,

electrical power, in-flight entertainment, and more. Evidently, different systems may have different impact on overall aircraft safety. For example, in-flight entertainment system will have lesser impact on overall aircraft safety than the engine control.

Therefore, there has been a need for professional standards to ensure aircraft safety. Such standards are being developed by professional organizations, among them the Radio Technical Commission for Aeronautics (RTCA), a private, not-for-profit association founded in 1935. Nowadays, RTCA is a venue for developing consensus among diverse, competing interests on critical aviation modernization issues in an increasingly global enterprise. Working jointly with the European Organisation for Civil Aviation Equipment, EUROCAE, its European counterpart, special committees are formed to issue aviation related guidance.

For safety considerations, the civil aviation guidance classifies failure categories assigning to them appropriate Design Assurance Levels (DAL) A through E, related to the criticality of the top-level failure condition that the given system may cause [6]. The failure of a system level A could result in a catastrophic failure condition for the aircraft. The consecutive levels are categorized as hazardous (B), major (C), and minor (D). System level E has no effect on the operational capability of the aircraft or pilot workload therefore is not requiring any safety considerations. These levels are assigned accordingly to specific systems/subsystems based on a rigorous safety analyses identified in the Aerospace Recommended Practice ARP 4761 [7], developed by the Society of Automotive Engineers (SAE). The document describes recommended practices of safety assessment for civil aviation.

Subsequently any aviation system design is implemented with SAE ARP 4754A guidance [8], which addresses the development cycle for aircraft and systems that implement aircraft functions. This document includes guidelines on development, integral processes, DAL assignment, verification and validation (V&V), configuration control, *etc.* The guidelines provide recommended practices (but not regulatory requirements) for showing compliance with the regulations to assist a manufacturer in developing the products while meeting its own internal standards.

Software is critical in all aspects of modern aviation whether it is the development or operation flexibility or fault tolerance. Software for high integrity digital (fly-by-wire) FBW systems can account for 60–70% of the total development costs of the complete system due to the size and complexity to implement flight control functions as well as establishing the safety of the software. Over 60% of the code account for configuration and redundancy management. These tasks include failure detection/isolation, reconfiguration in event of detected failure with cross-lane data transfer, synchronization, fault data recording, system status and control [9]. This is to make sure that errors in data or executable code would not propagate eventually to the aircraft level.

For software intensive systems, the RTCA DO-178C/ED-12C guidance [6] with its associated supplements developed by the joint RTCA/EUROCAE committee SC215/WG72 must be used. Specific objectives are defined for each of the four relevant assurance levels (DAL's). The more critical the level, the more stringent and numerous objectives must be met in each of the lifecycle processes. Additionally, some of the objectives must be met with independence, which means that the objective must be verified by the entity different than the actual developer.

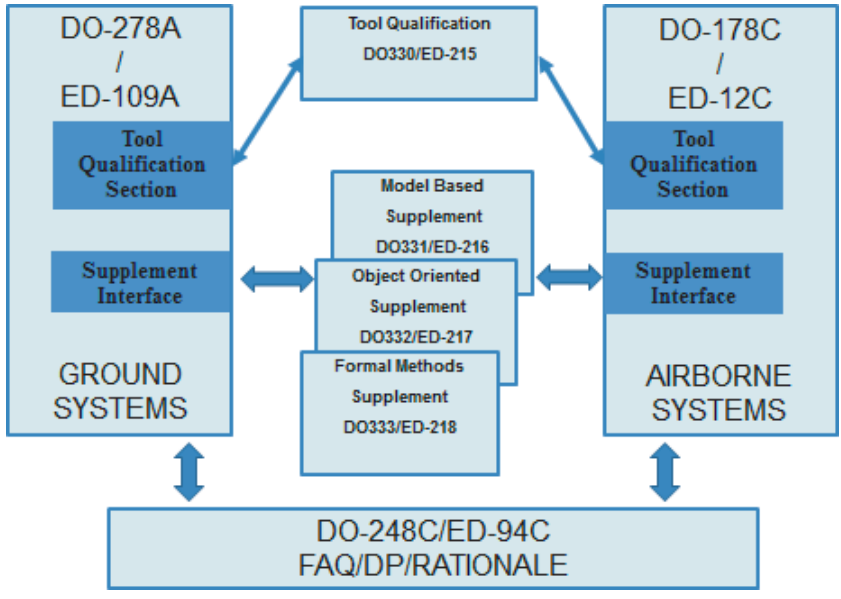

Figure 3. Overview of the RTCA/EURCAE airborne and ground software assurance guidelines

The supplements (see Figure 3) provide additional guidance regarding the following: tool qualification (DO330/ED215), model-based development (DO-331/ED218), object-oriented programming (DO-332/ED217), and formal methods (DO-333/ED216). There is an additional document on discussion papers, rationale, and frequently asked questions (DO-248C/ED78C). The significance of the supplements has been covered in several papers [10–12]. The most important from the software development perspective is the tool qualification process, which has been discussed by several authors, *e.g.*, [13, 14].

For complex electronic hardware the developers use guidance of RTCA DO-254/ED-80 [15]. The guidance is applicable to a wide range of hardware devices, from integrated technology hybrid and multi-chip components, to custom programmable micro-coded components, to circuit board assemblies (CBA), to entire line-replaceable units (LRU). This document also addresses the issue of commercial off-the-shelf (COTS) components. The document's appendices provide guidance for data to be submitted for certification, including: independence and

control data category based on the assigned assurance level, description of the functional failure path analysis (FFPA) method applicable to hardware with the highest design assurance levels (DAL), and discussion of additional assurance techniques, such as formal methods to support and verify analysis results.

Modern aircraft integrated architecture combining several subsystems within single processor, differentiated from traditional federated avionics, became inspiration to create dedicated Integrated Modular Avionic (IMA) guidance. RTCA DO-297 IMA Development Guidance and Certification Considerations provides guidance for IMA assurance [16].

The FAA Order 8040.4B [17] establishes the Safety Risk Management (SRM) policy for the Federal Aviation Administration (FAA). It also identifies Safety Assurance over the lifecycle phases and establishes common terms and processes used to analyze, assess, mitigate, and accept safety risk in the aerospace system (see Figure 4).

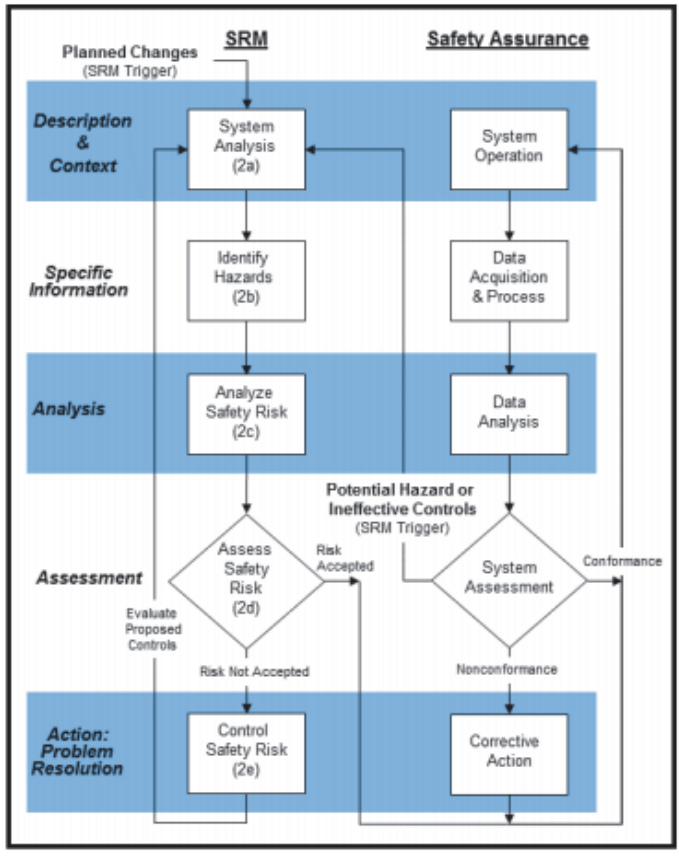

Figure 4. FAA safety management process

The principles, techniques and tools for rigorous safety assurance are used by manufacturers and vendors to assure high quality of their products

and protect the users and the public from inadvertent consequences of using these products. The orderly safety process includes a variety of hazard and risk analyses with preliminary (PHA), system (SHA), subsystem (SSHA), and operating and support (O&SHA) analyses using such assessment techniques as Functional Hazard (FHA), Fault Tree (FTA), Failure Mode and Effect (FMEA), Functional Failure Path (FFPA), Common Cause Analyses (CCA) described in the ARP 4761 [7]. The ultimate responsibility for accepting the vendors' claims rests with the certification authorities, which in the United States is the Federal Aviation Administration. The certification process is covered in Section 7.

All the aircraft subsystems are interconnected by an arcane bus system and related software protocols running on dedicated processors to assure the selection of proper subsystems and appropriate switch in case of failure detection. In the past the systems were separated and thus protected from the environment, therefore the cybersecurity had not been an issue. However, in modern aircraft, the systems may be sharing connections with non-critical subnets and additionally they may be externally accessible from the ground for uplink data and maintenance. Therefore, serious considerations need to be given to security, since violation of security may result in safety hazards, which may lead in turn to aircraft's loss of airworthiness.

The most recent industry-government discussions resulted in establishing joint RTCA/EUROCAE special committee SC-216/WG-72 dedicated to address the issues of aviation security and its impact on airworthiness. The committee created three documents:

- DO-326A/ED-202A "Airworthiness Security Process Specification" [18], which addresses security aspects of aircraft certification,
- DO-356A/ED-203A "Airworthiness Security Methods and Considerations" [19], which is to be applied in the context of 14 CFR Part 25 to provide guidance for accomplishing the airworthiness security process activities identified in DO-326A/ED-202A, and
- DO-355/ED-204 "Information Security Guidance for Continuing Airworthiness" [20], which addresses security aspects for continued airworthiness.

5. Ground Systems

Aircraft operate within constraints of a National Airspace System (NAS) – a meta-system including, in addition to the thousands of aircraft, air traffic management with command center, towers, terminals, en-route, oceanic and long-range radars, weather services, satellite navigation aids, airline and airport operations, communication facilities, navigation infrastructure, *etc.*, termed as a whole "ground systems". Ground systems support communication, navigation, surveillance and air traffic management (ATM). Ground systems also include Automatic Terminal Information Services (ATIS), and Airline Operations Centers (AOC). ATM combines airborne and ground-based functions which involves conflict detection and resolution ensuring a safe separation between aircraft. Air traffic controllers

use the aircraft position information received from radar, or more recently from Controller Pilot Data Link Communication (CPDLC) or from Automatic Dependent Surveillance-Broadcast (ADS-B), where aircraft transmits its position based on the Global Navigation Satellite System (GNSS). ADS-B ground receivers transfer the data to ATM systems. It is an extremely software-intensive interconnected system of systems with multiple stakeholders and incredible complexity. Due to recent proliferation of uplink/downlink functionalities the ground threats may affect the airworthiness of civil aircraft. With this level of complexity, regulations have been introduced to improve safety.

Considering the proposed changes of airspace management identified by the NextGen [21] concept, Air Traffic Control (ATC) and Communication, Navigation, Surveillance (CNS) ground systems are more closely interconnected with the aircraft and thus may directly impact safety of flight. Such interconnectivity and evident exposure to external, potentially malicious access brings attention to security issues traditionally not considered in this context but now being inseparable part of the picture. The implementation of CNS and ATC systems, jointly called CNS/ATM, include ground, airborne, and space-based systems, has resulted in increased interdependence of systems providing Air Traffic Services (ATS) and systems onboard aircraft. Modern interconnectivity with uplink/downlink features the ground-based CNS and ATM systems software typically using extensive COTS components that may have an impact on safety.

To address these issues, DO-278A/ED-109A guidance has been developed [22], which provides guidelines for the assurance of software contained in non-airborne systems. The guidance applies to software in CNS/ATM systems used in ground or space-based applications shown by a system safety assessment process to affect the safety of aircraft occupants or airframe in its operational environment. As for the airborne systems, the guidance specific objectives must be met depending on the level of system criticality identified by the system safety assessment. The relationship between airborne and ground aviation software guidelines, *i.e.*, DO-178C and the DO-278A, has been covered in multiple documents, first by industry [23, 24] and later by the academia [25]. The overall picture and relationships of the safety and security guidelines for the aircraft and ground systems is shown in Figure 5.

6. Unmanned Systems

Recent proliferation of Unmanned Aircraft Systems (UAS) and plans to use them for commercial purposes, as announced by large companies, pose obvious questions on the additional congestion and unpredictability in the airspace, which may lead to new issues in flight safety and security. Drones or Unmanned Aerial Vehicles (UAV) are two more popular terms used for the UAS. Obviously, through the nature of their operations, be it remotely controlled or autonomous, UAS are different than manned aircraft. They rely heavily on the quality of the communication links and software controlling not only the flight but also executing

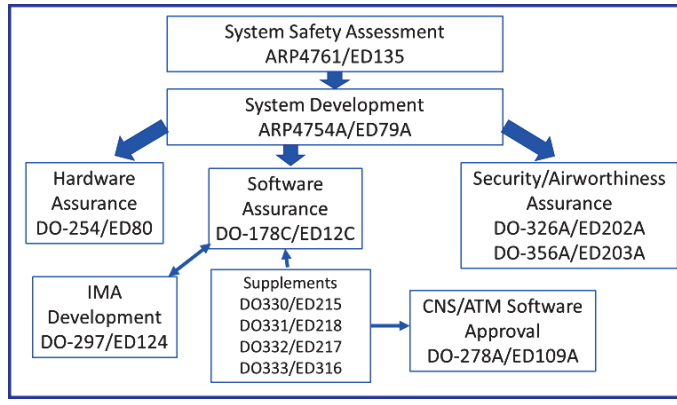

Figure 5. Compilation of guidance documents for aircraft safety and security (based on [26])

the mission profile. UAS systems may cause challenges when integrating them into the National Airspace System, due to their still unclear role in the airspace.

All air traffic, as designated by the Federal Aviation Administration, the agency regulating respective activities in the U. S., is subject to federal regulations. A UAS is defined as "an unmanned aircraft and its associated elements related to safe operations, which may include control stations (ground, ship, or air-based), control links, support equipment, payloads, flight termination systems, and launch/recovery equipment" [27]. Thus, for a UAS the tasks equivalent to those carried out by the pilot in a manned aircraft could be automated by software aboard a UAV, or the pilot could fly the aircraft from the ground. This changes the division of responsibility between the aircraft and the ground systems, thus impacting the original division documented in DO-178C/ED-12C [6] and DO-278A/ED-109A [22]. Three major UAS segments include air, ground and communication.

There is a substantial range of different UAS categories with a wide variety of potential uses in locations ranging from urban to extremely remote. The categories include public (government related missions, such as law enforcement, firefighting, border patrol, disaster relief, search and rescue, military training), civil (experimental operations for research and development, demonstrations and training, but not for carrying people or property for compensation or hire), and model (used by hobbyists and modelers for recreational purposes). It has been proposed that developmental relief may be granted by the certification authorities based on the associated operational risk. An example on such risk-based approach is shown in Figure 6.

The full integration of UAS into the national air space is a very complicated problem and several documents have been produced, sponsored by the RTCA and the FAA [29, 30], to facilitate the understanding of problems and plan the work on guidelines. More recently, the RTCA issued an internal report on the applicability of the DO-178C/ED-12C for the development of UAS software [31]. The proposed UAS system certification basis is still under discussion and certification

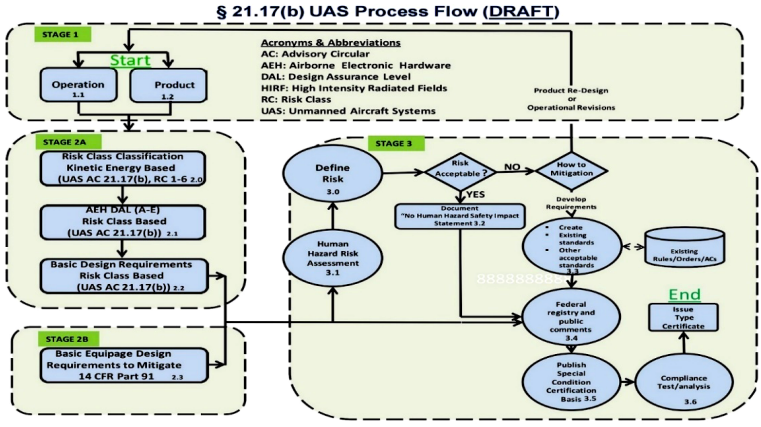

Figure 6. Proposed process flow for risk-based UAS certification [28]

process with respective assessment and responsibilities has not been defined by certification authorities at the time of this writing. Once the certification authority identifies the certification basis for the UAS's it will be possible to provide a mapping from Software Levels or Assurance Levels to the Failure Conditions.

7. Certification

The term "certification" in engineering disciplines is typically associated with three meanings: certifying product, process, or personnel. The ISO/IEC and IEEE sources [4] define certification as the process of making sure that the system is acceptable for operational use by showing its compliance with its specified requirements. The basis for certification is the collection of appropriate supporting evidence, particularly safety-related, in a format defined by standards and guidelines issued by the regulatory agencies or regulated industries themselves. Such supporting evidence is a used process, written guarantee, and formal demonstration.

Certification of airborne equipment in the United Sates is achieved through the FAA acting as the certification authority. There are various certifications types: authorization of a Type Certificate (TC – for the entire aircraft), Supplemental Type Certificate (STC – for a new equipment in a specific aircraft), or a Technical Standard Order (TSO – related to minimum performance standard for materials, parts, and appliances used on civil aircraft). Certification must adhere to the Code of Federal Regulations, Title 14: Aeronautics and Space, Part 25 [32]. Subpart F – FAR/JAR 25.1309 identifies requirements for equipment, systems, and installations that "... they must be designed to ensure that they perform their intended functions under any foreseeable operating condition" and that "... the occurrence of any failure condition which would prevent the continued safe flight and landing of the airplane is extremely improbable, and the occurrence of any other failure conditions which would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions is improbable".

A Certificate of Airworthiness is issued for an aircraft by the national aviation authority to attest that the aircraft is airworthy – it conforms to its type design. Certification regulations require the manufacturer to develop Instructions for Continued Airworthiness and conduct on-going monitoring of the fleet including regulated reporting of failure, malfunctions, and defects. These considerations apply to all certifications: TC, STC, and TSO. The registered owner of an aircraft is responsible for having in the aircraft current Airworthiness Certificate and Certificate of Aircraft Registration while maintaining the aircraft in an airworthy condition.

The FAA issues Advisory Circulars (AC) which are the legal base to provide guidance for compliance with airworthiness regulations. The AC's define acceptable means, but not the only means, of accomplishing or showing such compliance. The circulars make appropriate reference to the documents that achieved consensus among the stakeholders including the industry, government, and academia.

Advisory Circular AC-20-174 [33] recognizes the ARP-4754A document as an acceptable method for establishing a development assurance process for civil aircraft. The ARP-4754A discusses the development of aircraft and systems considering the overall aircraft operating environment and functions. This includes validation of requirements and verification of the design implementation for certification and process assurance.

For airborne software the major FAA guidance document is Advisory Circular 20-115D [34] describing possible means of compliance with the applicable airworthiness regulations. This AC recognizes the current RTCA DO-178C and EUROCAE ED12C documents with related supplements on tool qualification DO-330/ED215, model-based development and verification DO-331/ED218, object-oriented technology DO-332/ED109A, as well as on formal methods DO-333/ED-216 (see Figure 3). Additionally, the FAA Order 8110.49 [35] compiles a variety of guidelines related to the use of software in airborne systems.

Security issues have been on the forefront of ARINC Industry Activities and the Airlines Electronic Engineering Committee (AEEC) [36]. There are a variety of ARINC (Aeronautical Radio, Inc.) standards addressing the role that cybersecurity plays in definition of system, functions, equipment, *etc.*, responsible for communication, navigation, surveillance, avionics, and on-board operations. The major effort is focused on data communication and related Internet protocols. Aircraft onboard computer network must be secure from external threats. The AC 119-1 Airworthiness and Operational Approval of Aircraft Network Security Program (ANSP) [37] describes acceptable means of obtaining operational authorization for an aircraft related to security of the onboard computer network.

Software and electronic hardware in the aircraft systems are always evaluated from the perspective of the entire aircraft incorporated into a certification effort for a specific subsystem or an entire aircraft. Typically, an on-site Designated

Engineering Representative (DER) – either the FAA employee or an independent contractor – in continuous communication with the applicant (the organization developing the system) performs or recommends certification to the FAA. The DER is ultimately responsible that safe engineering practices are used during the entire development lifecycle. The other stakeholders include Aircraft Certification Engineers (ACE), Project Managers (PM), Developers, Testers, Quality Assurance Personnel, *etc.*

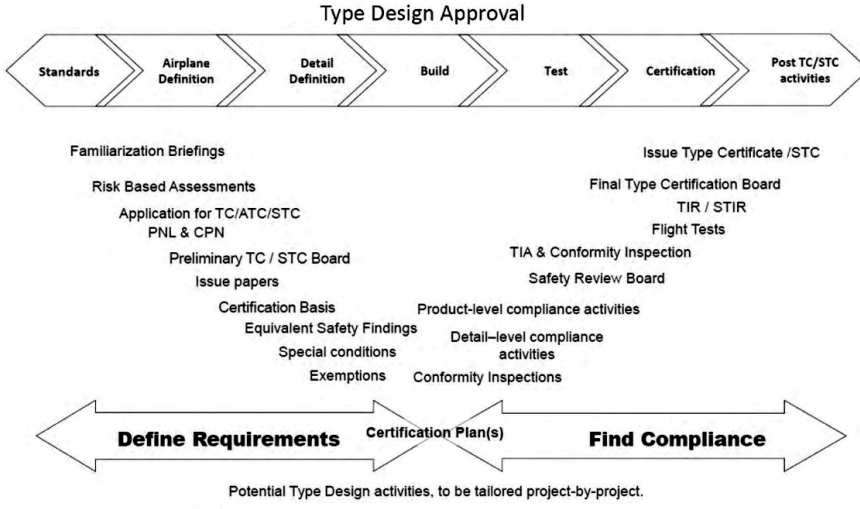

Figure 7. Typical project phases compared to 8110.4 [38] certification process [28]

The certification authority primarily controls the development process and checks the evidence that the process was followed. The starting point is an agreement that must be reached between the developer and certification authority on acceptable means of compliance, the certification team involvement in the compliance determination process, the need for test witnessing by certification authority, and any significant decisions affecting the result of the certification process. The current guideline for type certification was published in 2017 [39], and the general overview of certification phases compared to the development process are presented in Figure 7. Most recently, though, the certification rules are being revised due to rapid technological developments and flight accidents [40].

8. Conclusion and Future Work

The paper presented an overview of trends and challenges in aviation systems' safety and cybersecurity, including airborne and ground based systems, as well as UAS's. The emphasis has been placed on the computer hardware and software aspects and related certification processes. The major theme is the dominance of safety in aviation to which cybersecurity earned a significant

contribution, making the relationship between safety and cybersecurity the critical issue in all transportation industries.

Current guidelines for designing computer systems for aviation, with focus on safety and cybersecurity have been covered, including those developed by RTCA, in the U. S., and EUROCAE, in Europe, as well as SAE, ARINC and others, including advisory circulars and orders from the U. S. Federal Aviation Administration. One of the key points in developing the guidelines is to find the appropriate balance between safety risks to the public and the cost of implementing the guidelines and regulations.

The most pressing issue, at this time, is the development of guidelines for UAS's, due to the rapid proliferation of numerous unmanned vehicles that have begun saturating the air space. Another important factor to consider, which has not yet been paid enough attention to, is the cross section of critical industry sectors, such as transportation and energy or medical, for example, and addressing the safety and cybersecurity issues as a whole in the nation's critical infrastructure. Finally, standardization efforts must include, at some point, the technology of the Internet of Things (IoT), which is spreading across the entire economy posing new types of risks.

Additionally, due to the rapid development of technologies in aviation and related industries there are several significant research challenges remaining, which have to be addressed in the near future. One can look at these challenges from the safety perspective, as well as have a complementary view from the cybersecurity perspective. Safety related challenges have been recently covered in a report by the International Transport Forum [41]. Among the four components of the Safety Management Framework, Safety Risk Management has been mentioned and its two factors: Hazard Identification and Safety Risk Assessment, listed as key elements of that aspect. In the Safety Assurance component, the major element involves Safety Performance Monitoring and Measurement.

On the other hand, from the cybersecurity perspective, a recent report on strengthening the cyber resilience of air traffic control systems [42] takes a holistic approach to risk analysis of critical infrastructures in aviation, by providing eight general recommendations for improvement. One of them explicitly concerns "Safety & Security". In the words of the authors: "Since cyber threats and potential cyber-attacks can have a direct impact on safety-critical system functions, we recommend developing a comprehensive risk management approach aligning the formerly separated considerations of safety and security under a common roof. For this purpose, we found some new criteria, which have to be added to development processes to apply findings and results of comprehensive risk assessments in a suitable way to the air traffic system".

Separately, multiple research challenges have been listed in the literature for safety and cybersecurity of UAV system, for example in [43]. Regarding security aspects in UAV, the authors focus particularly on issues related to new attack vectors and the taxonomy of cybersecurity attacks. From the perspective of safety,

collision avoidance and swarming issues and related challenges are discussed. Finally, nearly all authors of the articles and reports reviewed emphasize that one of the most critical issues that must be addressed in the future is the incorporation of human factors in the risk assessment for the analysis of safety and cybersecurity in aviation systems. For example, one of the latest IATA reports on safety [44], while discussing circumstances contributing to accidents, clearly mentions that "human factors are often the weak link".

References

[1] International Electrotechnical Commission 2019 *Electropedia: The World's Online Electrotechnical Vocabulary*, Geneva, Switzerland

[2] Kornecki A J and Zalewski J 2015 *Aviation Software: Safety and Security*, *Wiley Encyclopedia of Electrical and Electronics Engineering* Webster J G (Ed.), Wiley & Sons

[3] Zalewski J 2019 *IEEE IT Professional* **21** (1) 16

[4] IEEE *Software and Systems Engineering Vocabulary*, IEEE Computer Society, Washington, URL: `https://computer.org/sevocab`

[5] Committee on National Security Systems 2017 *CNSS Glossary* URL: `https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf`

[6] DO-178C 2011 *RTCA 12-13-11, SC-205*

[7] ARP4761 1995 *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*, Society of Automotive Engineers

[8] ARP4754A 2010 *Guidelines for Development of Civil Aircraft and Systems*, Society of Automotive Engineers

[9] Kornecki A 2008 *Scalable Computing: Practice and Experience* **9** (1) 77

[10] Potter B 2012 *Complying with DO-178C and DO-331 using Model-Based Design*, 12AEAS-0090, Mathworks

[11] Elliott M R 2017 *CrossTalk – The Journal of Defense Software Engineering* **30** (2) 11

[12] Gigante G and Pascarella D 2012 *Proc. ISoLA 2012, Int'l Symp. on Leveraging Applications of Formal Methods, Verification and Validation* 205

[13] Gallina B *et al.* 2014 *Proc. SAFECOMP 2014, Int'l Symp. on Computer Safety, Reliability, and Security* 255

[14] Marques J and da Cunha A M 2017 *Proc. DASC 2017, 36th IEEE/AIAA Digital Avionics Systems Conference*

[15] DO-254 2000 *Design Assurance Guidance for Airborne Electronic Hardware*, SC-180, RTCA Inc., Washington, DC

[16] Eveleens R L C 2006 *Integrated Modular Avionics Development Guidance and Certification Considerations*, *Mission Systems Engineering*, Paper 4 Educational Notes RTO-EN-SCI-176, NATO Research and Technology Organization, Neuilly-sur-Seine, France

[17] Federal Aviation Administration 2017 *Order 80404B: Safety Risk Management Policy*, Washington, DC

[18] DO-326A 2014 *Airworthiness Security Process Specification*, RTCA Inc., Washington, DC

[19] DO-356 2014 *Airworthiness Security Methods and Considerations*, RTCA Inc., Washington, DC

[20] DO-355 2014 *Information Security Guidance for Continuing Airworthiness*, RTCA Inc., Washington, DC

[21] 2016 *NextGen: Next Generation Air Transportation System Implementation Plan*, Federal Aviation Administration, Washington, DC

[22] DO-278A/ED-109A 2012 *Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*, RTCA Inc., Washington, DC
[23] Lougee H 2012 *Transitioning to RTCA DO-178C/DO-278A: A Business Manager Brief*, Foliage Inc.
[24] Potton F 2012 *DO-178C/ED-12C versus DO-178B/ED-12B Changes and Improvements*, ACG Solutions
[25] Jimenez J A, Medina-Merodio J A and Sanz L F 2017 *Computer Standards & Interfaces* **42** 41
[26] Batuwangala E *et al.* 2017 *Proc. 17th Australian Aerospace Congress*, Melbourne
[27] Joint Planning and Development Office (JPDO) 2013 *Unmanned Aircraft Systems (UAS) Comprehensive Plan A Report on the Nation's UAS Path Forward*, U S Department of Transportation
[28] Ryan W *et al.* 2017 *FAA Annual Unmanned Aircraft Systems (UAS) Symposium*, Reston, Virginia
[29] Drone Advisory Committee 2017 *Drone Access to Airspace*, RTCA Inc., Washington, DC
[30] Federal Aviation Administration 2018 *Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap*, Second Edition, Washington, DC
[31] EUR 048-19/TAC-126 2019 *RTCA Paper No: 054–19/PMC-1859*, RTCA Inc., Washington, DC
[32] Code of Federal Regulations, Title 14 Aeronautics and Space, Part 35 Airworthiness Standards: Transport Category Airplanes 2013
[33] Federal Aviation Administration 2011 *Advisory Circular AC-20-174: Development of Civil Aircraft and Systems*, Washington, DC
[34] Federal Aviation Administration 2017 *Advisory Circular AC-20-115D: Airborne Software Development Assurance Using EUROCAE ED-12( ) and RTCA DO-178( )*, Washington, DC
[35] Federal Aviation Administration 2003 *Order 811049: Software Approval Guidelines*, Washington, DC
[36] Prisaznuk P J 2018 *Aviation Cyber Security Efforts*, ARINC Airlines Electronic Engineering Committee
[37] Federal Aviation Administration 2015 *Advisory Circular AC 119-1: Airworthiness and Operational Approval of Aircraft Network Security Program (ANSP)*, Washington, DC
[38] Federal Aviation Administration 2007 *Order 81104: Type Certification*, Washington, DC
[39] Federal Aviation Administration 2017 *The FAA and Industry Guide to Product Certification*, Third Edition
[40] U S Department of Transportation 2019, DOT Announces Special Committee to Review FAA's Aircraft Certification Process Press Release
[41] International Transport Forum 2018 *Safety Management Systems*, OECD, Paris
[42] Kiesling T and M Kreuzer 2017 *Recommendations to Strengthen the Cyber Resilience of the Air Traffic System*, Version 20, ARIEL Project
[43] Shakhatreh H *et al.* 2019 *IEEE Access* **7** 48572
[44] International Air Transport Association 2018 *IATA Safety Report 2017*, Montreal, Canada, and Geneva, Switzerland