30th Annual INCOSE international symposium
Virtual Event
July 20 - 22, 2020

Integrating Process Standards for System Safety Analysis to Enhance Efficiency in Initial Airworthiness Certification of Military Aircraft: A Systems Engineering Perspective

Morten Reinfjord Guldal
Norwegian Defence Materiel Agency
+47 920 83 605
morten.guldal@robotaviation.com

Jonas Andersson, CSEP
University of South-eastern Norway
+46 707 7070 14
jonas.andersson@usn.no

Abstract. When designing an aircraft, a System Safety Analysis (SSA) is an important part of the systems engineering activities related to initial airworthiness certification. For military aircraft, this requires not only a process to determine whether the system is safe enough, but also to identify an acceptable balance between safety, cost and military capability. In this paper, standards for performing the SSA, mainly for civilian aircraft, have been analyzed for their relevance to certifying military aircraft. Also, the systems engineering standard ISO/IEC/IEEE 15288:2015 have been analyzed for its applicability to integrate SSA with other activities in a military aircraft project. The purpose of the presented work is to analyze how these processes relate and how they can be integrated to create an effective and efficient process for developing and certifying aircraft in accordance with the EMAR 21 requirements for military design organizations.

Introduction

An aircraft in operational use constitutes a complex socio-technical system involving challenges related to humans, technology, and interaction between them. As a consequence, unwanted emergent properties of any aircraft system must be carefully managed to cope with risks that may impact its safety, effectiveness and cost. Emergent risks are the inevitable cost of unmanaged complexity and managing complexity has become the most important task in decreasing cost and development time of large aerospace systems (DeTurris & Palmer, 2018). Therefore, safety constitutes an inevitable part in any tradeoff related to the design and integration of an aircraft. Aircraft and its systems become more and more complex which make risks harder to identify. The human mind is biased by personal experience and risks may be subjectively assessed (Kahnemann, 2013). An objective process to assess the risks is therefore important to ensure systems meet their safety requirements. One example of this is the System Safety Analysis (SSA) employed to assess risks when certifying aircraft for initial airworthiness. An SSA is a systematic, comprehensive evaluation of the implemented system to show that the relevant requirements are met (SAE, 2010). SSA is also an important part of System Safety Engineering which contributes to Systems Engineering for safety critical system (INCOSE 2015).

This paper investigates how standards defining principles and processes for SSA and Systems Engineering may be applied and integrated to increase efficiency and cost-effectiveness of Systems Engineering activities related to initial airworthiness certification in general, as well as the overall

acquisition process of military aircraft. In particular the application of system safety standards for civilian aircraft (SAE, 2010) (SAE, 1996) for SSA of military aircraft and the impact of SSA on an overall acquisition process based on ISO/IEC/IEEE 15288:2015 (ISO, 2015), in this paper refered to as ISO 15288, is investigated. The purpose of the paper is to explore how investigated standards and principles relate, and how they may be combined to create an effective and efficient process for developing and certifying aircraft in accordance with EMAR 21 requirements (EDA, 2018) in the studied organization in particular, and for military design organizations at large.

The target organization for the presented investigation is the Norwegian Defence Materiel Agency/Air Systems Division (NDMA/ASD), a governmental organization responsible for the acquisition, sustainment and disposal of the Royal Norwegian Air Force's (RNoAF) equipment and systems. Presently, NDMA/ASD lacks an integrated process for performing SSA when certifying repairs or modifications for military aircraft, and NDMA's overall framework for lifecycle processes does not integrates SSA in other activities related to Systems Engineering. Reports from the Norwegian Defence Research Establishment have revealed that decisions early in projects are sometimes made by people without the right competencies (Presterud & Øhrm, 2015) and that practice of ensuring the quality of requirements have deficiencies (Presterud, et al., 2018). Consequences include increased cost, both for rectifying errors during development and sustaining the system throughout its operational lifecycle. For the NDMA/ASD, these results are also relevant from a system safety perspective. There is a potential for improvement regarding e.g. scoping the SSA as well as creating processes to ensure military aircraft systems meets both its safety target and its operational needs.

The investigation presented in this paper is the result of a Master's project in Systems Engineering at the University of South-eastern Norway.

Scope of this paper. This paper aims to investigate how an EMAR 21 compliant military design organization can use systems engineering processes and system safety standards for civilian aircraft to create an integrated process framework for efficient and effective airworthiness certification of military aircraft systems. Further, this paper investigates if implementing these processes has the potential to improve the operational effectiveness in the operational lifecycle of a military airborne system. The investigation of systems engineering lifecycle processes is limited to only the ISO 15288 standard due to time constraint. This is the most known systems engineering standard and most other standards within the systems engineering domain rely on or refer to this standard. The two system safety standards from SAE, ARP4754 and ARP4761 has been chosen since they are the two most renowned standards for civilian aircraft and because they are listed as "Information sources" in the European Military Airworthiness Certification Criteria (EMACC).

Method of attack. The research presented in this paper has been conducted as a longitudinal exploratory case study using mixed methods (Yin, 2018). Initial hypotheses and findings from an initial literature review was used to create an interview questionnaire. A series of semi-structured interviews were conducted with selected members (project managers and subject matter experts) of a project involving airworthiness certification in NDMA/ASD. The interview revealed several issues that were included in the case study protocol and used when conducting a document review of the standards analyzed in the study.

Outline of paper. The first part of this paper presents the research methodology and the design of the presented case study including a short summary of methods chosen and how they were performed. Thereafter an overview of SSA for airworthiness certification is provided including possible outcomes of an SSA. The airworthiness rules and regulations for civilian and military aircraft are elaborated to introduce the differences between them. This chapter also presents the requirements for a military design organization and why an SSA is necessary for airworthiness certification of a military aircraft. The system safety standards chapter presents the proposed SSA standards and outlines their approach to SSA. The analysis section links these standards together with the previous chapters and analyzes their relationship to the ISO 15288 systems engineering standard and

their significance in the initial airworthiness work. The paper ends with conclusions and further work.

Research design

From a Systems Engineering perspective, Safety Engineering is an Engineering specialty area. Systems Engineering must embed the system safety engineering effort into its engineering processes from the outset, in order to design and integrate safety into the system as engineering design decisions are made (INCOSE, 2015). The research presented in this paper therefore investigates how Systems Engineering can be used in conjunction with recognized system safety standards for civilian aircraft to improve quality and efficiency in airworthiness certification for military airborne systems. The resulting processes must therefore contribute to finding an acceptable balance, and critical tradeoffs between cost, risk (in terms of airworthiness) and the required military capability, as depicted in Figure 1.

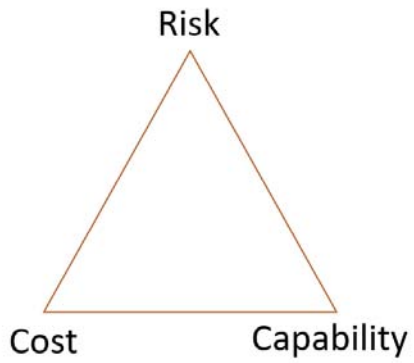

Figure 1: The investigated design space

Scope. The scope of this paper is limited to investigating the process related to performing a technical System Safety Assessment (SSA) of military airborne systems. Although Human factors assessment is an important part of a complete safety assessment and their behavior affect safety (De Florio, 2016) (Kritzinger, 2017), this has not been addressed in this study to limit its scope.

Research questions. How can an EMAR 21 compliant military design organization use systems engineering best practice and system safety standards for civilian aircraft to:
1. Find an acceptable scope of their airworthiness system safety assessment activities.
2. Establish an acceptable[1] balance between risk, cost and the required capability.
3. Provide other benefits for the operational lifecycle of a military airborne system?

Research methodology

As stated above, the research presented in this paper has been conducted as a longitudinal exploratory case study using mixed methods (Yin, 2018). The relationship between several system safety standards, MIL-STD-882, SAE ARP4761 and SAE ARP4754, and ISO 15288 has been investigated to reveal how they can be used to satisfy the initial airworthiness requirements of military aircraft and if they can contribute to meet these requirements more effectively and efficiently. A literature review was conducted to reveal the relationship between the standards and identify gaps in terms of airworthiness requirements not covered by the investigated standards. Interviews were conducted with participants in a project in the NDMA/ASD to relate the theory to a real-world case. In addition, the

[1] Note, that the term *acceptable* in this paper is defined as meeting the requirements of EMAR 21.

incident reporting system for aircraft safety in the Norwegian Defence has been reviewed in order to find any incidents where a poorly performed- or missing SSA has been a contributing factor.

Literature review. A literature review was conducted in the last months of 2018. Identified papers where first selected based on their title, then some of these where eliminated because of their content. Recommended literature from colleagues were reviewed and relevant books were found on Amazon using the search terms "Initial airworthiness" and "Aircraft system safety". In addition, relevant airworthiness regulations retrieved from the applicable airworthiness authorities' homepage and standards were found in *Intrasource*, which are the NDMA's database for standards.

Case study interviews. A project within NDMA/ASD was selected as a case based on identified issues related to diverging views on the scope of the SSA in different departments involved in the project. During the spring of 2019, a series of shorter semi-structured interviews were performed as a part of the overall case study. The interviewees were project managers and subject matter experts (engineers) related to the studied project. The interviewees were asked about their view on the SSA in terms of their own department's perspective, and they were also asked to speculate on their views of the other involved departments. The questions asked related e.g. to department's priorities based on Figure 1 and Figure 2. In addition, there were also several open-ended questions where the interviewees could freely explain their view and potential issues in the project.

A weakness of the interviews is that it is limited to just one project in the organization. This project was chosen because the author knew there were issues related to the SSA. Other projects may not have the same issues and the interviewees' statements may not necessarily represent the rest of the organization.

System Safety Analysis for Airworthiness Certification

The aim of airworthiness certification is to argue that the aircraft is safe and in compliance with the applicable safety requirements. This argument is supported by objective evidence from the SSA. This evidence forms the basis for the decision whether the aircraft is compliant or non-compliant according to these requirements. There are six potential outcomes of the SSA (Washington, et al., 2017) as depicted in Figure 2. Some of these outcomes are desirable, while others are not. Some of the outcomes are not desirable because they impose an unnecessary cost, and one of them may pose a hazard for flight safety, i.e. when the decision is that the aircraft is compliant when in fact it is not.

	Decision		
Reality	Compliant	Non-compliant	Requiring further data
Compliant	Desirable	Unnecessary cost	Unnecessary cost
Non-compliant	Undiscovered risks	Desirable	Less desireable SSA not complete

Figure 2: Outcome of an SSA

Goal-based vs. risk-based approach

The approach to determining the outcome of the SSA, depicted in Figure 2, can be a *goal-based* approach, a *risk-based* approach or a combination of them. A goal-based approach defines safety targets according to the potential severity and meeting them, while a-risk based approach is arguing that the risk is As Low As Reasonably Possible (ALARP) (Kritzinger, 2006). The former has a pre-determined acceptable level of safety based on historical data and is used in the certification of e.g. civilian aircraft and nuclear facilities. An example is the CS 25.1309 specification which require all failure conditions identified as catastrophic to be extremely improbable and that it does not result from a single failure (EASA, 2020). The latter, ALARP, does not have a predetermined level of safety and requires a cost-benefit analysis to determine whether the level of safety is acceptable or not. These two approaches can be combined primarily by using a goal-based approach to meet a goal and if that is not possible, use a risk-based approach and perform a cost-benefit analysis to determine if the risk can be accepted or has to be mitigated (Kritzinger, 2006).

Airworthiness standards, rules and regulations

In aviation, safety has always been a concern. The International Civil Aviation Organization (ICAO) defines safety as "*The state in which risks associated with aviation activities, related to, or in direct support of the operation of aircraft, are reduced and controlled to an acceptable level"* (De Florio, 2016). A part of this definition is the airworthiness of the aircraft itself, also known as technical airworthiness. "*An aircraft is defined as airworthy when the aircraft conforms to its type design, and is in a condition for safe flight"* (Gratton, 2018). This definition is twofold. Firstly, "*conforms to its type design,"* refers to meeting the applicable airworthiness requirements (airworthiness code) when designing an aircraft and ensure it is manufactured in accordance with its design. This is also known as aircraft certification, which leads to a type certificate. This is designated *initial airworthiness*. Second, "*in a condition for safe flight*", refers to sustaining the airworthiness requirements throughout the operational life of the system and not allow the safety to degrade below the certified standard (Gratton, 2018). This is designated *continuing airworthiness*. Continuing airworthiness includes several things, but particularly that the aircraft is maintained as specified and operated within the allowable limits. This is dependent on the initial airworthiness phase where the margin of safety is designed into the system.

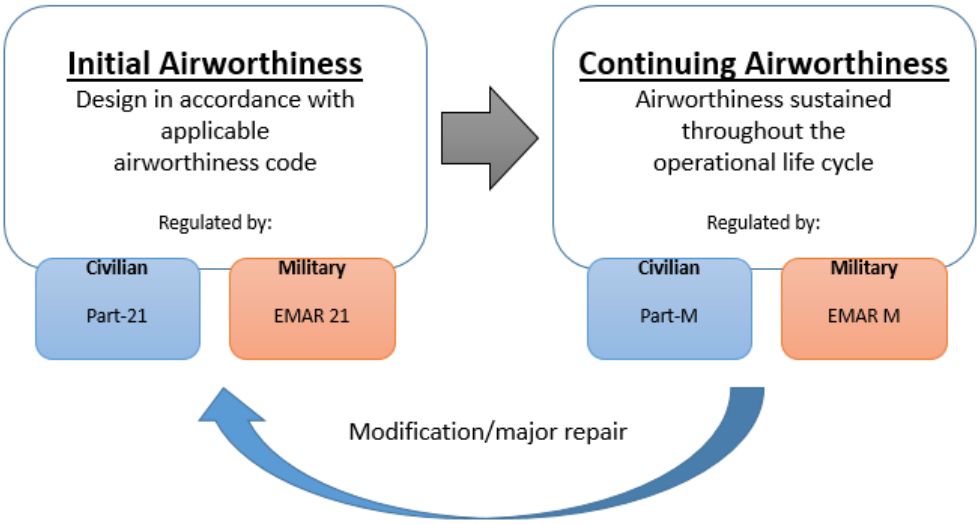

Figure 3: The relationship between initial- and continuing airworthiness.

Initial airworthiness assessment is primarily performed in the early stages of the lifecycle of an aircraft, but also revisited whenever an operational aircraft is modified or needs to undergo a major

repair that requires design. The relationship between initial- and continuing airworthiness is shown in Figure 3.

Civilian- and military airworthiness rules and regulation

As shown in Figure 3, different regulations govern the civilian and military aviation in Europe. European Aviation Safety Agency (EASA) issue the civilian airworthiness regulations in Europe[2]. The European Defence Agency (EDA) adopted and tailored the EASA's regulation in 2008 to fit military use. This has resulted in the European Military Airworthiness Requirements (EMAR) (MAWA, 2015). The regulations presented in Figure 3 provide requirements for the organizations responsible for initial- and continuing airworthiness. These are similar for civilian- and military aviation. The difference between civilian and military aviation is most obvious in the airworthiness design codes, which are the airworthiness requirements for the product (i.e. aircraft, subsystem etc.) used in the initial airworthiness phase. European civilian airworthiness codes, named Certification Specifications (CS), are clearly defined sets of airworthiness requirements. These are "pass/no-pass" requirements, which must be fully compliant[3] to certify a civilian aircraft (Gratton, 2018).

Certification of military aircraft is done with a combination of civilian airworthiness codes and military requirements. These requirements do not need to be fully compliant, and a higher risk is accepted to meet operational needs. Airworthiness requirements can be partially compliant, or omitted if necessary, to meet an operational need. This may imply an increased risk. European Military Airworthiness Certification Criteria (EMACC) lists the certification criteria and references to civilian airworthiness codes and military airworthiness specifications (EDA, 2018).

EMAR 21

EMAR 21 provides rules and regulations for organizations designing military aircraft, airborne systems or parts. According to the EMAR 21 regulation, a holder of a Design Organization Approval (DOA) shall have a design assurance system for the control and supervision of the design, and of design changes, of products, parts and appliances covered by the DOA application (EDA, 2018). This implies having a system for designing in accordance with applicable airworthiness requirements, demonstrate and verify the compliance with these requirements and show that no feature or characteristics makes it unsafe for the uses which certification is requested (EDA, 2018). This includes performing an SSA to argue that safety requirements have been met. The EMACC handbook provides requirements for the SSA in its section 14, containing the system safety requirements (EDA, 2018). This chapter mentions three system safety standards relevant for the study presented in this paper; MIL-STD-882, SAE ARP4761 and SAE ARP4754, presented in the sections below.

Analyzed Standards

MIL-STD-882. "MIL-STD-882E – System Safety" is a standard that identifies US Department of Defence Systems Engineering approach to eliminate hazards, where possible, and minimize risks where those hazards cannot be eliminated (US DoD, 2012). This standard is a general system safety standard used for acquisition of all types of systems within the US Defence sector. Furthermore, this standard contains a process consisting of eight elements describing the system safety approach on a high level (Figure 4), guidance for the system safety effort and several task descriptions for contractors and document deliverable requirements. It focuses on how to document the SSA approach, but does not provide guidance on how to perform the SSA and find the technical risks in a

[2] Other civil regulators and regulations in other parts of the world exist, but these are not included in this paper. An example is the US Federal Aviation Administration (FAA) issuing the Federal Aviation Regulations (FAR) for the USA.

[3] May have deviations accepted by the Aviation Authority (De Florio, 2016).

given design. In the standard, a hazard is defined as *"A real or potential condition that could lead to an unplanned event or series of events (i.e. mishap) resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment"* (US DoD, 2012). The level of severity of each risk is based on this definition and named "mishap result criteria".

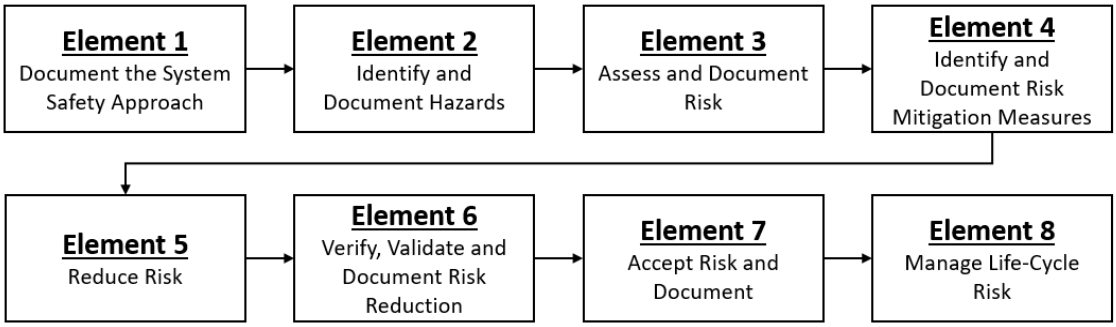

Figure 4: The eight elements of MIL-STD-882 (US DoD, 2012).

SAE ARP4761. "SAE ARP4761 – Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment" is an Aerospace Recommended Practice (ARP) providing guidelines and methods for showing compliance to safety requirements (SAE, 1996). It is primarily for large civilian transport aircraft, but may be used for other aircraft categories. This standard consists of several safety assessment methods, illustrated in Figure 5, which complement each other.

SAE ARP4761 uses the term "failure condition" to classify the severity of a risk instead of the term "hazard" as MIL-STD-882 use. The definition of a failure condition is *"A condition with an effect on the aircraft and its occupants, both direct and consequential, caused or contributed to by one or more failures, considering relevant adverse operation or environmental conditions."* (SAE, 1996). ARP4761 is intended to be used in conjunction with ARP4754, presented below. ARP4761 does not include safety assessment of software, but refers to ARP4754 regarding this. As depicted in

Figure 5, the level of detail of the SSA, as presented in ARP4761, is dependent on which phase the system is in, not the complexity of the system or the risk within it.

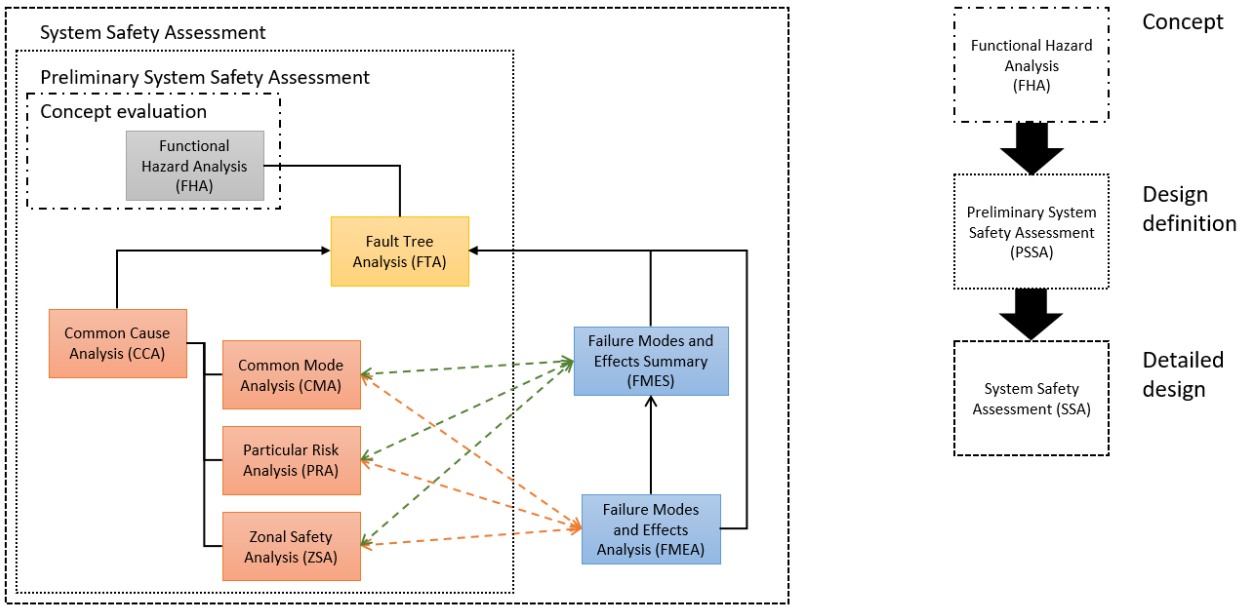

Figure 5: SAE ARP4761 SSA methods and stages

SAE ARP4754. "SAE ARP4754A - Guidelines for Development of Civil Aircraft and Systems" is an Aerospace Recommended Practice (ARP) providing guidelines for development of civilian aircraft systems (SAE, 2010). As ARP4761, the ARP4754 is primarily for large civilian transport aircraft, but may be used for other aircraft categories. This standard uses the same failure condition definition as ARP4761 to classify the severity of a risk. ARP4754 refers to, and complements, ARP4761 by presenting a systems engineering process model for airworthiness certification of aircraft, systems and items. ARP4754 includes safety assessment of software and electronic hardware, supported by DO-178 for software (RTCA, 2011) and DO-254 for electronic hardware (RTCA, 2000). In ARP4754, the Development Assurance Level (DAL) determines the validation rigor and the necessary independence[4]. A DAL is allocated to functions (FDAL) or items (IDAL) with a classification of the failure condition from E (no safety effect) to A (catastrophic). A higher DAL requires a more thorough process with more independent assessment of the airworthiness requirements. A level A DAL (catastrophic) requires the use of all methods of ARP4761 in

Figure 5, while a level E DAL (no safety effect) requires just the Functional Hazard Analysis (FHA).

Appendix A of ARP4574, presented in Figure 6, outlines the objectives and data for each of its eight processes. Together, they outline a process for planning, developing and certifying an aircraft as airworthy. These processes are focused on the airworthiness certification and the assurance of the implementation of the airworthiness requirements. The process ends at aircraft verification, which verify that all safety requirements have been implemented. It does not include validation of the implemented safety requirements at aircraft/complete system level. ARP4754 defines validation as *"The determination that the requirements for a product are correct and complete. [Are we building the right aircraft/ system/ function/ item?]"* (SAE, 2010).

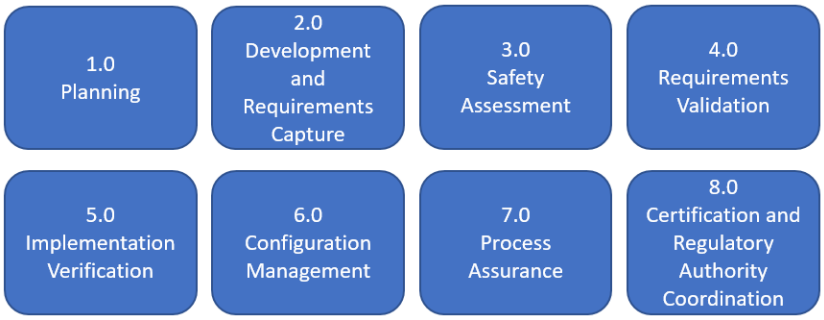

Figure 6: ARP4754A processes

ISO 15288. "ISO/IEC/IEEE 15288 – Systems and Software Engineering – Lifecycle Processes" is an international standard that establishes a common framework of lifecycle processes for describing the activities performed during the lifecycle of man-made systems (ISO, 2015). This standard divides the lifecycle processes into four categories or groups: the Agreement processes, the Organizational Project-enabling processes, the Technical Management processes, and the Technical processes. The purpose of the ISO 15288 is to provide a defined set of processes to facilitate communication among procurers, suppliers and other stakeholders in the lifecycle of a system (ISO, 2015).

Analysis

System safety in ISO 15288. An analysis conducted revealed that none of ISO 15288's processes contain specific outcomes for conducting an SSA in the development of a system, even though the standard mentions the word safety in several of its *tasks* and *notes,* mainly in the Technical Processes

[4] Of functions or items, and the process for development of- and checking the design

group. Figure 7 shows the processes in ISO 15288 that mention safety in one or several task(s) or note(s), marked green or red.

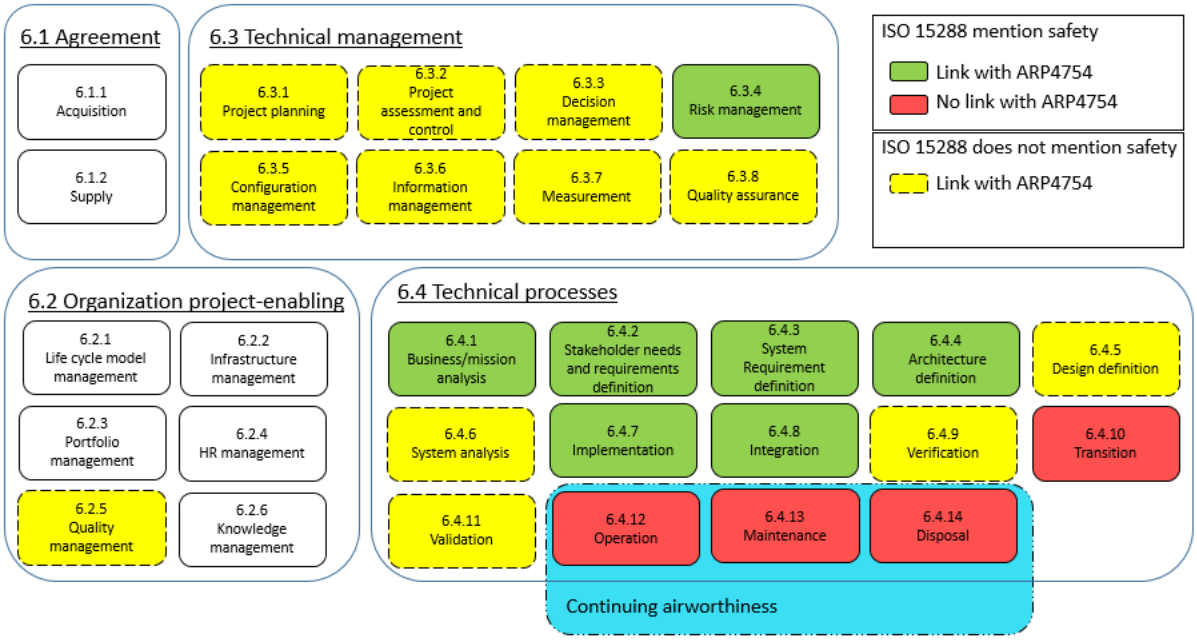

Figure 7: ISO 15288 – Processes mention safety & link with ARP4754.

ISO 15288 in an airworthiness perspective. The agreement-, organizational- and process-enabling process groups relates to both initial- and continuing airworthiness. The technical process group provides a clearer distinction between initial- and continuing airworthiness. Operation, maintenance and disposal belongs to the continuing airworthiness phase, as depicted in Figure 7. The remainder of the Technical Processes belong primarily to the initial airworthiness phase, although some activities related to them may be relevant for the continuing airworthiness phase.

ISO 15288 compared with ARP4754. A mapping was conducted to compare ARP4754's processes in Figure 6 with ISO 15288's lifecycle processes. The result is presented in Figure 7. This mapping revealed that all of the technical management processes of ISO 15288 can be mapped to ARP4754. For the Technical processes, most of the processes relate to initial airworthiness, except for the transition process. As mentioned earlier, ARP4754 ends at verification and it does therefore not include activities for the continuing airworthiness/operational phase of its lifecycle. For Agreement- and Organizational, project-enabling processes, only the Quality management process has a relation to process assurance in ARP4754.

Severity classification. The classification of the severity in the different safety standards varies. ARP4754 and ARP4761 have the same definition, which is based on the functional failure of the system. MIL-STD-882's classification, named "mishap result criteria", is not based on the functional failure as in the ARP standards, but on the outcome of an accident. Many functional failures will not necessarily result in an accident and therefore MIL-STD-882's classification cannot directly allocate a severity to a failure mode (Kritzinger, 2017). The severity definition from the two ARP standards are therefore better to use when performing an SSA since their severity definition focus on the failure of the system itself.

Goal- or risk-based approach for military aircraft. For military aircraft, the level of risk can be increased as a tradeoff to get the required military capability. An example is sacrificing backup systems to make the aircraft lighter to increase its maneuverability and speed. Putting these two approaches in context of the tradeoff space in Figure 1 produces a different result for the two. The goal-based approach for civilian airworthiness codes implies a predetermined maximum level of risk, a minimum level of capability and cost as the largest variable. For a risk-based ALARP approach, the

capability is mostly fixed with both the cost and risk as the largest variables. The risk is weighed against the cost of mitigating it. A reduced risk may imply an increased cost and vice versa. ARP4754 and 4761 are goal-based in their approach since they are standards developed for civilian airworthiness codes. MIL-STD-882 on the other hand has a risk-based approach. For military aircraft, the goal should be to strive for the same level of safety as for civilian aircraft. Therefore, the goal-based approach towards civilian airworthiness codes, using ARP4754 and 4761 should be the primary objective, but this is not always possible. A combined approach is therefore necessary for military aircraft by using a risk-based approach whenever there is a deviation towards the goals in the goal-based approach. Residual risks as a result of not meeting the safety goal should be assessed, documented and, if possible, mitigated by other means (processes, maintenance, limitations, etc.). This implies that the MIL-STD-882 definition of severity is aligned with the ARP standards.

The NDMA/Air Systems Division. The results of the interviews with a few key personnel in a project in the NDMA/ASD, revealed that the project department (project managers) and the technical department (engineers) view on the SSA process was misaligned. The technical department's view was that the project department focused too much on cost in the tradeoff space in Figure 1, while the project department thought their focus on risk and capability were aligned with the technical department. Some misalignments related to the decisions on the outcome of the SSA, presented in Figure 2 was also found. The interviews revealed uncertainties in both department about which framework to use for an SSA to determine whether a system is compliant or not and who is responsible for this decision. Both departments agreed that there was a lack of communication and information flow between the two departments and that some of the friction between the two departments can be related to poor system requirements. However, no incidents directly related to a design made by the NDMA/ASD was found during the research for this paper. The one incident found, was related to a modification that the Royal Norwegian Air Force (RNoAF) made without approval from the NDMA/ASD (RNoAF Air Safety Inspectorate, 2011). This was a minor modification done to improve a noise related issue which in hindsight could have been a potential hazard.

Standards for System Safety Analysis – strengths and weaknesses.

The ARP4761 provides methods for conducting the SSA that are thorough and detailed. It can be used, both for qualitatively and quantitatively assessment when certifying military aircraft. Even though it has not been updated since 1996, the methods are still relevant. However, it has gained critique for lacking methods for performing SSA on software (Leveson, 2018), but using ARP4761 together with ARP4754 fills this gap because the latter includes methods for how to perform SSA on software. Not all ARP4761 methods needs to be conducted for lower level Development Assurance Levels (DALs)/severity if the processes of ARP4754 are followed. This is a more efficient approach than what ARP4761 presents, which is a full SSA for all types of DALs/severities. ARP4754's approach is therefore preferred for performing an efficient and effective SSA. This SSA approach will discover the most risks, but it has some potential deficiencies.

ARP4754 has gained critique for lacking procedures for analyzing whether systems are truly integrated. This increases the likelihood that integration requirements may not be captured in highly integrated systems (FAA, 2016). It has been suggested that ARP4754 should be improved by providing additional guidance on the modification of existing systems (FAA, 2016). The standard is currently written as if the system is developed from the beginning, which is rarely the case. Modifying an aircraft or its subsystems is more common than developing a completely new system. ARP4754 does therefore need additional processes in addition to ARP4761 to perform a complete SSA. Another challenge with using these SSA standards is that they only focus on the airworthiness certification and assurance of the implementation of safety requirements. SSA processes can be used to assure the system is safe, but does not necessarily confirm that the system has met the operational requirements. The term "validation" in ARP4754 means "requirement validation", not "system validation" and this standard ends at aircraft verification. ARP4754 does not include processes for how to

develop the concept or the operational requirements ahead of its procedures or how to transition to the operational life when the certification is complete. It also lacks general organizational/project-enabling processes which are necessary to run an aircraft development project.

Integrating ISO 15288 and standards for System Safety Analysis

Certification of a military aircraft must always be seen in the larger context of proofing safety while also meeting the operational requirements of the aircraft in a cost-effective way. SSA must be an integrated activity in projects delivering military capability. System-level properties such as safety must be designed into systems. They cannot be added on afterward and expected to be safe (INCOSE 2015). It is recommended to introduce airworthiness in the design stage (Gratton, 2018). In addition, it is important to ensure both system performance and safety to fully understand the risk exposure (Farnell, et al., 2019). A holistic approach is therefore required to strike the right balance between risk, cost and capability. A way to do this is to integrate ARP4754 with ISO 15288. These two standards overlap in several areas as revealed in the analysis presented in Figure 7. ISO 15288 contains processes for the full lifecycle of a system, but does not contain specific procedures or methods for performing an SSA. ARP4754, together with ARP4761 and MIL-STD-882, contain processes for performing an SSA for military aircraft, but have several shortcomings, as presented in the previous chapter.

Organizational project-enabling processes. The SSA standards' lack of organizational project-enabling processes are likely because this is fulfilled by requirements in EMAR 21, or its equivalent civilian regulation EASA Part 21. These documents define requirements for the organization and the competency of required personnel (EDA, 2018). Organizational project-enabling processes are important to build an organization that can develop a system and correctly perform an SSA and ISO 15288 supports this. In ISO 15288, the Quality management process in organizational project-enabling processes is of particular importance as it relates to ARP4754's assurance process, which is important for the quality and integrity of the SSA. ISO 15288's Human resource, Knowledge management, and Lifecycle model management processes are also important from a safety perspective as they contribute to assure that the right competences are available to perform the SSA and that the methodology employed is improved continuously.

Technical management processes. All technical management processes in ISO 15288 do somewhat relate to ARP4754's processes, as revealed in the comparison of these two standards. All of them affect the SSA. Of these, the Risk management process of the ISO 15288 has the strongest relationship to ARP4754's processes as it contains the assessment and management of risks. The main difference between the standards is that ARP4754 focuses on technical risks while ISO 15288 also includes project risks. This is common for the processes in the technical management group. The ARP4754 processes manage the certification project only, while ISO 15288 has a wider scope and includes the whole project. The technical management processes are therefore important to manage both the development project and the SSA. The Decision management process affects the SSA, as it can be used to determine the design trade-offs related to risks, and the decision on whether the SSA is compliant or not. It is important that the decision of the outcome of the SSA is well grounded and in accordance with reality to avoid unnecessary risk or cost, as described in Figure 2.

The remaining Technical management processes support the decision management process by providing input to the decision. They contribute with information that supports the decisions. Status of risks from the risk management process and technical measurement from the measurement process are two examples. The Measurement process can be used to support the Safety Management System (SMS). An SMS is a systematic approach for measuring the performance of an organization to proactively identify aviation hazards. This is not presently mandatory for EMAR 21 organizations, but may very well be in the future, as EMAR 21 is based on an equivalent civilian regulation, the EASA

Part 21. There is work in progress to make SMS mandatory for EASA Part 21 design organizations (EASA, 2017).

The Technical processes of ISO 15288 is the most important process group related to safety. This process group mentions safety in most of its processes, as seen in Figure 7. Most of ISO 15288's technical processes have a relationship to ARP4754. Those without a direct relationship are the Transition process and those classified as continuing airworthiness processes in Figure 7. Processes related to initial airworthiness, consist of processes for analyzing the mission and system, and defining requirements, design and architecture up front in the process. These processes contribute to finding and creating the correct requirements, both operational and safety related. They provide the necessary input to the SSA in ARP4754.

Also, in ARP4754, supporting its output, are ISO 15288's Verification, Validation, Implementation, Integration and Transition processes. These processes can be used to close some gaps in ARP4754; the Verification and Validation processes to verify that the system fulfills the operational need in addition to being safe; the Integration process to find integration requirements and ensure that systems are truly integrated; the Transition process to have an efficient and effective transition from initial- to continuing airworthiness and the airborne system's operational lifecycle stages.

Other processes that can contribute to an effective and efficient transition and operational life are the processes related to continuing airworthiness. Even though these processes are mostly relevant for the continuing airworthiness phase, they can be used to discover requirements for enabling systems for operation and maintenance when designing a system. ARP4754 has a short paragraph for the capturing of maintenance requirements for in-service use to be included in the Instructions for Continuing Airworthiness (ICA). The ICA covers maintenance of continuing airworthiness in the operational phase. Analyzing the need for enabling systems will contribute to effective and efficient maintenance in the operational life of the system.

Agreement processes. The last process group in ISO 15288, agreement processes, have no direct connection to ARP4754. However, is important to stress that while these processes are not relevant for the SSA itself, they are relevant to safety aspects related to how the design organization interacts with its stakeholders, e.g. subcontractors and partners. EMAR 21 contains requirements to ensure that correct design data is provided to a subcontractor (EDA, 2018).

Norwegian Defence Materiel Agency/Air Systems Division

So far, only a small number of design efforts have been completed organically within the Norwegian Defence Materiel Agency/Air Systems Division (NDMA/ASD), and they have gone well despite the lack of processes and competencies related to SSA. No incidents or accidents within the RNoAF could be linked to failure in the SSA process. Most modifications have been performed by- or in cooperation with the Original Equipment Manufacturer (OEM) of the aircraft. The OEM's knowledge has therefore compensated for the NDMA/ASD's gaps related to SSA processes.

Based on the case study interviews, lacking or inadequate communication and information flow between the two departments in NDMA/ASD seems to be the most prominent reason for the misalignment between them. One reason for this is the lack of a framework for performing the SSA, defining the roles, responsibilities and formalizing information flow. This is further supported by findings that indicates that poor integration between systems engineering and project management is a contributor to tension in projects (Rebentisch, 2017).

Conclusions and further work

Implementing the presented findings, or parts of it, for improving the practice of Systems Safety Analysis in NDMA/ASD, including the use of ISO 15288 to support that NDMA/ASD's EMAR 21

design assurance system has the potential to increase the quality and efficiency of its airworthiness certification process. In particular, the implementation of ISO 15288 has the potential to provide better communication, improved information flow between stakeholders, and a clearer picture of the responsibilities and the scope related to the SSA. Furthermore, a safety critical design under scrutiny will go through a more thorough analysis using such a procedure, reducing the risk for features and functions that may have a negative impact on safety. Also, increased performance of the NDMA/ASD's organization will most likely reduce the processing time of requests from the RNoAF, providing incentives for the end-customer to involve NDMA/ASD also for minor modifications of airborne systems.

The SSA in the initial airworthiness phase defines the margin of safety and assures that the design is safe before it is transitioned into operational life. The outcome of the SSA is used as the basis for defining operational limitations and maintenance requirements. These limitations and requirements maintain the safety margin in the operational/continuing airworthiness phase. ARP4754 does not provide any guidance for how to implement these efficiently and effectively. Capturing requirements for effective and efficiently operation and maintenance can be done by using ISO 15288. ISO 15288 has a broader perspective than the SSA and Systems Safety Engineering, and do not only analyze the safety aspect. ISO 15288 includes processes for transition and validation of the complete system, which contribute to a smooth transition to operational life and assuring that stakeholder needs are met. The presented analysis therefore supports that combining ISO 15288 with SSA standards increases the possibility of an effective and efficient system in the operational life.

SAE ARP4754 has gained critique for lacking processes to assure that systems are truly integrated and would therefore benefit from providing more guidance for performing modifications (FAA, 2016). This paper advocates that the processes of ISO 15288 may be used to avoid this issue. This requires tailored processes and methods, and needs to be researched further. During this research project, the authors have noted that INCOSE and SAE have signed a Memorandum of Understanding to formalize a partnership to improve processes together (INCOSE, 2018).

References

De Florio, Filippo. *Airworthiness: An introduction to Aircraft Certification and Operations, Third Edition.* Elsevier Ltd., 2016.

DeTurris, Dianne, and Andrew Palmer. *Perspectives on Managing Emergent Risk due to Rising Complexity in Aerospace Systems.* Washington: INCOSE, 2018.

EASA. "Easy Access Rules for Large Aeroplanes (CS-25) - Initial issue & amendment 1 - 21." 2020.

—. "Terms of Reference for rulemaking task RMT.0251(b) (MDM.055-MDM.060)." *Embodiment of safety management system requirements into Commission Regulations (EU) Nos 1321/2014 and 748/2012.* European Aviation Safety Agency, July 12, 2017.

EDA. "EMACC Handbook Ed. 3.1." *European Military Airworthiness Certification Criteria.* European Defence Agency, September 25, 2018.

—. "EMAR 21 AMC & GM Ed. 1.3." *Acceptable means of compliance and guidance material for the certification of military aircraft and related products, parts and appliances, and design and production organisations.* European Defence Agency, February 1, 2018.

—. "EMAR 21 Ed. 1.3." *Certification of military aircraft and related products, parts and appliances, and design and production organisations.* European Defence Agency, February 1, 2018.

FAA. "DOT/FAA/TC-16/39." *Safety Issues and Shortcomings With Requirements Definition, Validation, and Verification Processes Final Report.* Atlantic City: Federal Aviation Administration, December 2016.

Farnell, G.P., A.J. Saddington, and L.J. Lacey. "A new systems engineering structured assurance methodology for complex systems." *Reliability Engineering & System Safety, Volume 183*, March 2019: 298-310.

Gratton, Guy. *Initial Airworthiness: Determining the Acceptability of New Airborne Systems, Second Edition.* Cranfield: Springer, 2018.

INCOSE. *INCOSE and SE News.* November 9, 2018. https://www.incose.org/events-and-news/incose-and-se-news/2018/11/09/.

—. *Systems Engineering Handbook - A Guide for System Life Cycle Processes and Activities, 4th Ed.* San Diego, CA: Wiley, 2015.

ISO. *ISO/IEC/IEEE 15288:2015 Systems and software engineering - System life cycle Processes.* Geneva, CH: ISO/IEC/IEEE, 2015.

Kahnemann, Daniel. *Thinking, fast and slow.* Farrar Straus Giroux, 2013.

Kritzinger, Duane. *Aircraft System Safety: Assessments for Initial Airworthiness Certification.* Cambridge: Woodhead Publishing, 2017.

—. *Aircraft System Safety: Military and civil aeronautical applications.* Cambridge: Woodhead Publishing, 2006.

Leveson, Nancy G. *Safety Analysis in Early Concept Development and Requirements Generation.* Washington: INCOSE, 2018.

MAWA. "Frequently Asked Questions (FAQs) Ed. 1.1." MAWA Forum, October 2015.

Presterud, Ane Ofstad, and Morten Øhrm. *Effective materiel acquisitions in the Norwegian Defence Sector - A study of incentives in the investment process.* Kjeller: Norwegian Defence Research Establishment, 2015.

Presterud, Ane, Morten Øhrn, Kristin Waage, and Helene Berg. *Effective materiel acquisitions in the Norwegian Defence Sector - Mapping of time spent, delays and execution costs.* FFI-Raport no. 18/00231, Kjeller: Norwegian Defence Research Establishment, 2018.

Rebentisch, Eric. *Integrating program management and systems engineering.* Hoboken: Wiley, 2017.

RNoAF Air Safety Inspectorate. "Incident Report no. 2011/0039." 2011.

RTCA. "DO-178C." *Software Considerations in Airborne Systems and Equipment Certification.* RTCA, Inc., December 13, 2011.

—. "DO-254." *Design Assurance Guidance For Airborne Electronic Hardware.* RTCA, Inc., April 19, 2000.

SAE. "ARP 4754A." *Guidelines for Development of Civil Aircraft and Systems.* SAE Aerospace, December 2010.

—. "ARP4761." *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment.* SAE International, December 1996.

US DoD. "MIL-STD-882E." *System Safety.* May 11, 2012.

Washington, Achim, Reece A. Clothier, and Brendan P. Williams. "A Bayesian approach to system safety assessment and compliance assessment for Unmanned Aircraft Systems." *Journal of Air Transport Management, Volume 62*, July 2017: 18-33.

Yin, Robert K. *Case Study Research and Application - Sixth Edition.* Los Angeles: SAGE Publishing, 2018.

Biography

Morten Reinfjord Guldal. Has spent more than 14 years in the technical branch in the Royal Norwegian Air Force; first as an aircraft technician, then as an aeronautical engineer with responsibilities spanning from technical support and sustainment to implementing airworthiness rules and regulation. He holds a B.Sc. in aeronautical engineering from the University of Agder and a master's degree in Systems Engineering from the University of South-eastern Norway. Currently, he is the senior test manager for Robot Aviation – a Norwegian based company designing and producing Unmanned Aircraft Systems.

Jonas Andersson. has spent more than 25 year as lecturer, researcher, leader, and practitioner within the domains of systems engineering and engineering management. Currently, he leads Decisionware AB – a Swedish based company devoted to industrial continued competence development in product creation and technical leadership. He is also Associate professor at the University of South-eastern Norway in Kongsberg. Jonas holds a Ph.D. in Industrial Information and Control Systems from the Royal Institute of Technology in Stockholm, and is a Certified Systems Engineering Professional. He is also a former adjunct professor in military-technology at the Swedish Defence University. Within INCOSE, Jonas is a founding member and a past president of the Swedish INCOSE Chapter. He has also served Associate director for Events and Director for Strategy in its international Board of Directors.