Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P576-cd

Implementation of STPA methodology into military jet aircraft certification process according to EMAR certification criteria for safety

Pšenička Milan

AERO Vodochody AEROSPACE a.s., Czech Republic. E-mail: milan.psenicka@aero.cz

Fukalová Michaela

AERO Vodochody AEROSPACE a.s., Czech Republic. E-mail: michaela.fukalova@aero.cz

Lališ Andrej

Faculty of Transportation Sciences, CTU in Prague, Czech Republic. E-mail: lalisand@fd.cvut.cz

Increasing requirements on reliability and safety of aircraft are emerging not only in civil aviation but also in the military aviation industry. In order to eliminate all possible safety risks, or to minimize them where they cannot be eliminated a lot of conventional methods are used, such as Failure Mode and Effects Analysis (FMEA), Failure Mode, Effects and Criticality Analysis (FMECA), Functional Hazard Assessment (FHA), Fault Tree Analysis (FTA) etc. Those are excellent system safety engineering methods widely used to ensure system operational integrity during the initial aircraft certification process. The European Military Airworthiness Requirements (EMAR) regulations explicitly mention the conventional methods as acceptable means of compliance for all safety related paragraphs. Nowadays, however, new approaches emerge that attempt to overcome some of the limitations of the conventional ones. One of the promising is the Systems Theoretic Accident Model and Process (STAMP) and the Systems-Theoretic Process Analysis (STPA) based on it. This method is based on qualitative analysis which, while very useful in the development phase of an aircraft, makes it difficult to directly connect the outputs of the analysis to the requirements of the military EMAR regulations, which explicitly call for some quantitative outputs. This paper presents a few cases where the STPA fits European Military Airworthiness Certification Criteria (EMACC), including how such qualitative method could be expanded to deliver some of the required quantitative outputs.

Keywords: Safety, military, aircraft, Functional Hazard Assessment, Failure Mode and Effects Analysis, Failure Mode, Effects and Criticality Analysis, Systems Theoretic Accident Model and Process, Systems-Theoretic Process Analysis, Aviation, European Military Airworthiness Requirements certification.

1. Introduction

Increasing requirements on reliability and safety of aircraft are emerging not only in civil aviation but also in the military aviation industry, in which safety and reliability play an important role. Higher complexity and coupling of systems are the leading reasons for safety and reliability to be given due attention. Leveson (2012).

Digitalization, artificial intelligence (AI) and other innovations are also coming to the fore in military aviation. Although these are beneficial technologies in aviation that should make flight safer, there are new hazards associated with them that need to be identified early in the system design. Li et al. (2022), Athavale et al. (2020) Even if it is not possible to identify all potential hazards of a given system, it is important to focus on safety analyses of the system already during the design and development phase, when potential hazards can be eliminated, or adequately mitigated (if elimination is not possible). Interventions in a system during the design and development phase are also more favourable from an economic point of view compared to possible interventions in a system already operated. Leveson (2012) As a result of more detailed safety analyses during design and development, subsequent maintenance can be made more efficient and the reliability of the aircraft overall increased.

In connection with the increasing requirements for the safety and reliability of

aviation technology, new safety methods and analyses have been developed that offer a more comprehensive approach to hazard identification. Khan and Salim Ahmed (2015), Underwood and Waterson (2013) They focus not only on hardware, but also software and the human factors, including their interactions, which are crucial for safety in highly interconnected systems.

The application of new safety methods and analyses appears today mainly in civil aviation, however, their use can also be assumed in the field of military aviation in alignment with the relevant military regulations (norms and standards). This paper addresses the issue by introducing the current military aviation requirements following the traditional approach to safety, then analysing and comparing the systemic approach to safety with the traditional one, and finally by investigating into how and to what degree the new safety methods could be used with the regulations as a valid means of compliance.

2. European Military Airworthiness Certification Criteria

Within the framework of military aviation, the so-called European Military Airworthiness Certification Criteria (EMACC) EDA (2018) is a binding document setting up the airworthiness certification criteria for use and also engage with the relevant certifying National Military Airworthiness Authority (NMAA). Each Airworthiness Certification Criteria is matched with corresponding Title 14, Code of Federal Regulations reference (14CFR reference) and Joint Service Specification Guides (JSSG). In addition, cross-references are provided to the relevant sections within European Union Aviation Safety Agency (EASA) Certification Specifications (CS), Defence Standard 00-970 or 00-56, North Atlantic Treaty Organization Standardization agreement (NATO STANAG) documents and Military Standards MIL-STD. All the reference material in EMACC should be used as a guide and not purely for purposes of citing requirements. Any other additional Advisory Circulars, Def-Stan 00-970 leaflets or other acceptable means of compliance documents could be used as well to assist in understanding the implementation of the relevant regulatory requirements.

EMACC defines the minimum necessary criteria to establish, verify, and maintain an airworthy design of any military aircraft product, part, or appliance. Safety and Reliability topics are presented in almost all system related sections, but the main part is condensed in Section 14 - System Safety. The general breakdown of the Section 14 is shown in Figure 1. Individual aircraft system related sections explicitly mention following safety analyses:

- Failure modes, effects, and criticality analysis (FMECA) IEC (2018)
- Hazard analysis and classification
- System safety analysis report
- Safety certification program

On aircraft system level, the EMACC regulations focus on a combination of qualitative and quantitative safety assessment starting with identification of possible critical functional failures during failure modes analyses, followed up by hazard analysis and its classification. Based on those outputs the recognized system safety analysis (e.g. Fault Tree Analysis, IEC (2006)) is usually performed.

Safety certification program or Safety Program, mentioned also in system sections, is defined and described in detail in Section 14 – System Safety, specifically in paragraph 14.1. These are mainly general criteria for the creation and implementation of a comprehensive system safety program. It consists not only of description of safety analyses and processes but also includes implementation of hazard tracking system and its integration with system engineering processes. However, these criteria are rather general in nature, EMACC refers to other sub-documents that describe in more detail the way in which individual requirements should be met, primarily the military standard MIL-STD-882E, DoD (2012) FAA §23.1309 in 14 CFR part 23, FAA (2011) and the SAE ARP 4761 standard. SAE (1996) This allows to tailor (selection of subset of applicable airworthiness criteria) the certification basis for every type of military air vehicle, platform-wide, in order to fully address safety aspects of all unique configurations. Guidance for tailoring the certification basis within the EMACC is provided by the Type Certification Basis Tailoring Guidebook with attention to defining quantitative parameters compatible with performance requirements.

MIL-STD-882E is used as a standard, generic method for the identification, classification, and

mitigation of hazards. One of the most important parts of MIL-STD-882E used in accordance with EMACC is part about assessing and documentation of risks and also part about hazards classification. Tables I., II., III., in paragraph 4.3.3. directly set up classifications for severity categories, probability levels and risk levels for each Risk Assessment Code (RAC) respectively.

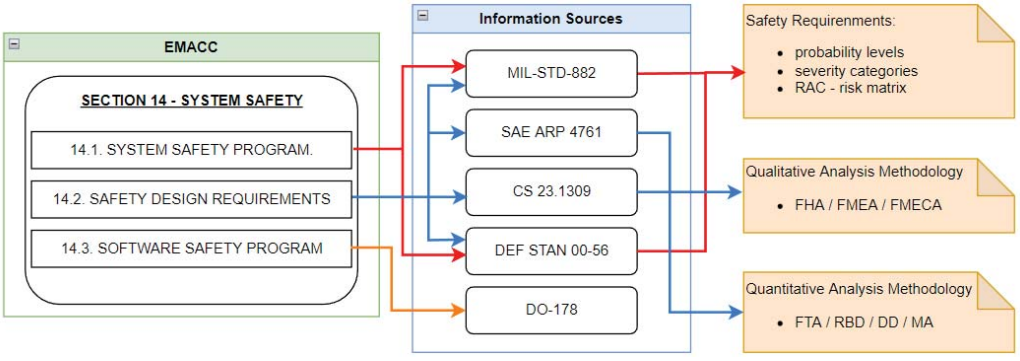

Figure 1: Schema of used informational sources in Section 14 System Safety of EMACC in terms of used safety and reliability methods

This is generally used for mechanical parts of the aircraft or at the system level, while the whole software safety assessment is individually described in paragraph 4.4. The need for standalone classification of software-controlled or software-intensive systems originated from the fact, that determining the probability of failure of a single SW function is by its nature impossible and cannot be based on historical data. Moreover SW-based systems are application-specific and therefore reliability parameters cannot be derived in the same manner as hardware.

Another widely used EMACC compliant standard related to safety is FAA §23.1309 (25.1309) for equipment, systems, and installations in 14 CFR part 23 civil airplanes and its advisory circular AC 23.1309-1E. General paragraph §23.1309 establishes schema about identification and classification of potential hazards and its AC details the guide for acceptable means of compliance in terms of methodology as well as individual safety analyses methods. This AC refers to another civil aerospace recommended practice SAE ARP 4761, that is also compatible guide for compliance with EMACC section 14. The whole safety assessment process according to SAE ARP 4761 has three parts:

- FHA - Functional Hazard Analysis
- PSSA - Preliminary System Safety Analysis
- SSA - System Safety Analysis

The main goal of this approach is to identify all the functions associated with the selected level (aircraft, system, subsystem etc.), its failure conditions, end effects and severity classification. After the requirements for failure conditions are assigned with the method used to verify compliance with those requirements, quantitative analysis if performed in order to predict the probability levels. Methods explicitly mentioned in SAE ARP61 are Fault Tree Analysis (FTA), Dependence Diagram (DD) and Markov Analysis (MA).

The software itself is again managed separately from hardware. Design assurance level (DAL) is assigned to each software-related component depending on its safety-criticality. Based on this DAL classification various Radio Technical Commission for Aeronautics (RTCA) standards, such as DO-178C, RTCA (2011) DO-278, RTCA (2011) DO-294, RTCA (2008), establish design, certification and verification procedures. Splitting the hardware and software parts of the aircraft systems for the purpose of safety analysis leads to some inherent feedback loops because problems can occur at the hardware, software or integration level.

3. Systemic Approach to Safety

The aforementioned documents (MIL-STD-882E, SAE ARP 4761) refer to the use of conventional quantitative methods such as FHA, FTA, FMEA/FMECA for system safety assessment. All of these methods are certainly suitable for safety assessment, however, when considering the increasing complexity of systems,

they may seem inadequate. They mainly focus on failures and malfunctions of elements, which is not sufficient for assessing the contribution of humans and software in the system.

In aviation, when evaluating safety, there is an increasing tendency towards a systemic approach, according to which the system should be taken as a whole, i.e. with consideration of all its elements that interact with each other, whether it is hardware, software or people. The System-Theoretic Accident Model and Process (STAMP) Leveson (2012) safety model is based on this approach.

4. STAMP

STAMP is based on the assumption that undesirable events arise on the basis of unsuccessfully enforced safety constraints. It follows that STAMP treats safety as a control problem, unlike FHA, FTA or FMEA which treat safety as a reliability problem. To establish safety constraints, the model recommends creating a hierarchical control structure that describes how control takes place between individual hierarchical levels. The hierarchical structure is made up of feedback control loops (Figure 2), where the controller enforces safety constraints in the controlled process. In order for the controller to have information about the status of the controlled process, it needs feedback, which is conveyed through sensors. Based on the feedback, the controller can decide about and apply control, which is conveyed to the controlled process by the actuators. Important for decision-making process is the model of the controlled process, which is updated based on feedback from the controlled process.

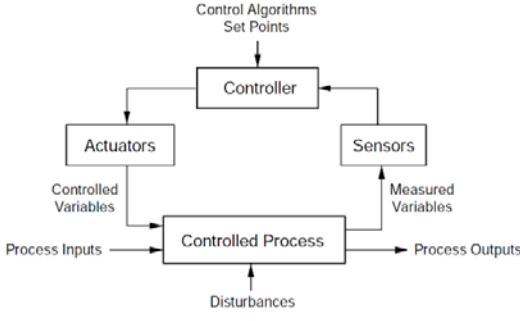

Figure 2: Feedback Control Loop, Leveson (2012)

5. System-Theoretic Process Analysis

System-Theoretic Process Analysis (STPA), Leveson and Thomas (2018) is based on the STAMP model. It is a hazard analysis method that focuses on the interactions of components in a system from a control perspective. Its use is particularly beneficial in the early stages of system development and design, as it enables the definition of safety constraints and requirements that the system should meet from a safety point of view. STPA consists of 4 basic steps, which are shown in Figure 3. STPA is (like FTA) top-down analysis, starting with the identification of losses at the system level and progressing through system hazards and unsafe control actions to loss scenarios.

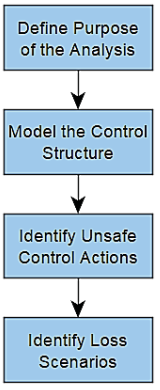

Figure 3: STPA steps (adapted from Leveson and Thomas (2018))

5.1. *Defining the purpose of the analysis*

The first step of the STPA aims primarily to determine the losses to be avoided in the given system. Next is identification of system-level hazards, meaning the system condition that, together with a specific set of worst-case environmental conditions, will lead to a given loss. Subsequently, system-level constraints are established, which determine what must be met in order to prevent the occurrence of hazard and subsequent loss.

5.2. *Modeling the control structure*

The second step involves the modeling of a hierarchical control structure of the analysed system, which is made up of the already mentioned feedback control loops. If it is a very complex system, it is advisable to start creating

the control structure from the highest abstract level and then iteratively proceed to greater detail.

5.3. *Identifying unsafe control actions*

As part of the third step of STPA, unsafe control actions (UCAs) are identified and subsequently the relevant safety constraints of the controller. Unsafe control action is a control action that, in a certain context and in the worst environmental conditions, can lead to hazard. Control action can be unsafe in the following four ways:

- Not providing the control action leads to a hazard
- Providing the control action leads to a hazard
- Providing a potentially safe control action but too early, too late, or in the wrong order
- The control action lasts too long or is stopped too soon

5.3. *Identifying loss scenarios*

The fourth step identifies loss scenarios. These are usually divided into two groups. The first type of scenarios describes the causal factors that can lead to the occurrence of UCAs and subsequently to hazards. The second group of scenarios is based on identification of improperly or not executed control actions. Based on the list of loss scenarios, the safety constraints for the given system are determined.

6. STPA Compliance with Military Regulations

The outputs from STPA are safety constraints and requirements, i.e. qualitative statements aiming to prevent certain system behavior, due to STAMP treating safety as a control problem. Conventional methods (such as FHA, FTA, FMEA/FMECA), treat safety as a reliability problem, i.e. they are aimed at probability estimates resulting in quantitative outputs that are favored in certification (which also treats safety as a reliability problem). For example, the SAE ARP 4761 standard primarily requires the determination of quantitative safety requirements when evaluating system safety. It allows qualitative requirements where probability estimates are impossible, but this does not change their probabilistic nature. The schematic representation of the STPA-based methods approach and conventional ones is shown in Figure 4.

However, if we focus not only on the outputs that SAE ARP 4761 requires, we can certainly find compliance of STPA with ARP 4761 in the process by which system safety is assessed. Leveson et al. (2014) The STPA process, as in SAE ARP 4761, is an iterative process that starts at the system level and continues into greater system detail until hazards are adequately analyzed and managed. The objective of STPA is very similar to that of conventional methods, which is to find out how the identified hazards might occur, so that their cause/causes can be eliminated or mitigated through modification of the system design or through adjustment of maintenance or pilot manuals. What certainly lies in the advantages of STPA over SEA ARP 4761 is the approach to the human factor as part of almost every system. Above all, it is the interaction of the human element with other parts of the system, which is also essential from a safety point of view, and STPA focuses on this interaction, which is missing in conventional quantitative methods. This interaction is typically represented by systematically pointing out that some systems hazards can occur when the manipulation with the system is inappropriate, takes too long or too short time of in case if any human misjudgment. Similarly, we find a difference in approach to the role of software. In the SAE ARP 4761 process, probabilities are not assigned to the software, instead the Design Assurance Level (DAL) is assigned for the hardware component with some software related functions. STPA approaches software in the same way as any other controller (hardware, human) and analyzes the impact of software behavior on associated system hazards directly and not indirectly through design assurance.

A comparison of the MIL-STD-882E standard with STPA, Leveson (2020) shows that the STPA steps meet and support the individual tasks within this standard. From task section 200 MIL-STD-882E, which deals with hazard analysis, the requirements for hazard identification early in the system design, their preliminary analysis, determination of design requirements to eliminate hazards or reduce related risks, etc. are evident (see Leveson (2020)). STPA is in general a systemic top-down hazard analysis. The creation of a control

structure in STPA directly supports the subsequent analysis of how the identified hazards could occur through unsafe control actions and related loss scenarios. In addition, the specific causal scenarios defined within STPA help ensure that hazards are not incorrectly categorized in the analysis by prematurely assessing probability without causal information.

7. Supplementing STPA with Quantitative Outputs

Although STPA appears unsuitable as a standalone method for certification purposes due to its pure qualitative nature (and the conflict how the method views safety compared to certification processes today), it is possible to augment it with other methods that meet the requirements for quantitative outputs and thus meet the requirements of military aviation regulations. Although such augmentation may lead to questionable outputs (typically for software or human factors related issues), it could be reasonable and useful where safety and reliability are truly dependent (typically for mechanical and electric components or systems). In such cases, STPA could be supplemented e.g. with Reliability Block Diagrams (RBD), IEC (2016) directly linked to individual loss scenarios for selected UCAs. This would in principle bring up the desirable combination of qualitative and quantitative methods, that are explicitly requested by certification authorities.

8. Conclusions

Even the fact that traditional safety analyses provide all required information by the military

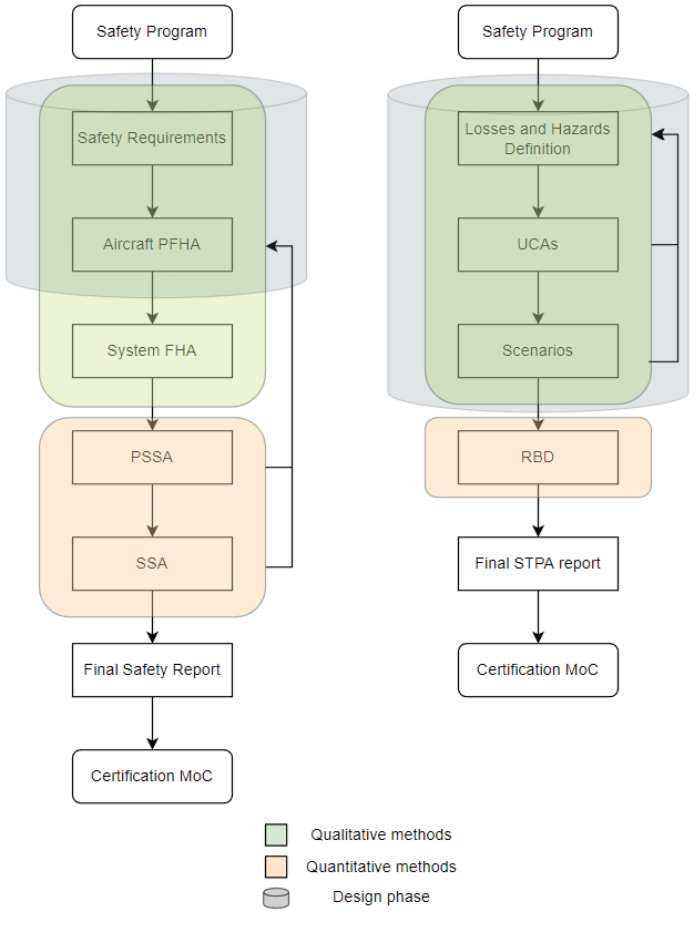

Figure 4: Schematic comparison of the whole Safety Assessment process by traditional and STPA methods

certification authorities about the aircraft systems and the aircraft itself to allow designers to say their product is reliable and safe enough, the difficulties with description of highly complex, software-based avionics or AI-based solutions with many interfaces increase. This leads to new and innovative ways to think about aircraft systems using a model-oriented approach with a very different foundation than the current techniques offer. The new methods (such as STPA) are valid means of compliance in military aviation in terms of all qualitative safety analyses, as it was shown here with EMACC, or as it was already published with MIL-STD-882. Leveson, (2020).

In order to use the STPA as standalone safety solution of the whole section 14 of the EMACC, we would need to extend the analysis by some quantitative part. It seems very useful and straightforward to use RBD as it could be easily linked with the Loss Scenarios for individual UCAs. This quantitative output could be then connected to hazards and losses definitions from the first step of STPA and due to that directly linked to safety requirements according to MIL-STD-882.This approach gives the opportunity to certification authority to validate those numbers explicitly, as they are already used to. In a longer-term, however, the paradigm change behind the new methods like STPA will likely lead to a more significant changes to how we assess the safety of aircraft today.

References

Athavale, J., A. Baldovin, R. Graefe, M. Paulitsch and R. Rosales (2020). AI and Reliability Trends in Safety-Critical Autonomous Systems on Ground and Air. In *Proceedings - 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN-W 2020,* pp. 74-77. IEEE.

DoD (2012). MIL-STD-882E, Department of Defense Standard Practice: System Safety. Standard, Department of Defense (DoD).

EDA (2018). European Military Airworthiness Certification Criteria (EMACC): EMACC Handbook. European Defence Agency (EDA).

FAA (2011). AC 23.1309-1E - System Safety Analysis and Assessment for Part 23 Airplanes. Advisory Circular, Federal Aviation Administration (FAA).

IEC (2006). IEC 61025:2006 Fault tree analysis (FTA). Standard, International Electrotechnical Commission (IEC).

IEC (2018). IEC 61078:2016 Reliability block diagrams. Standard, International Electrotechnical Commission (IEC).

IEC (2018). IEC 60812:2018 Failure modes and effects analysis (FMEA and FMECA). Standard, International Electrotechnical Commission (IEC).

Khan, F. and S. R. Salim Ahmed (2015). Methods and models in process safety and risk management: Past, present and future. *Process Safety and Environmental Protection 98*, Page 116–147.

Leveson, N. (2012). *Engineering a Safer World: Systems Thinking Applied to Safety*. MIT Press.

Leveson, N., Ch. Wilkinson, C. Fleming, J. Thomas and I. Tracy (2014). A Comparison of STPA and the ARP 4761 Safety Assessment Process. Technical Report, Massachusetts Institute of Technology (MIT).

Leveson, N. and J. Thomas (2018). *STPA Handbook*. https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

Leveson, N. (2020). STPA (System-Theoretic Process Analysis) Compliance with MIL-STD-882E and other Army Safety Standards. White paper. http://sunnyday.mit.edu/compliance-with-882.pdf

Li, H., J. Li, J. Pimentel, G. Gruska, R. Xu and F. Xu (2022). Complete Safety Analysis of Known and Unknown Scenarios in Autonomous Vehicles Based on STPA Loss Scenarios. SAE Technical Paper 2022-01-7023. SAE International.

RTCA (2008). DO-294: Guidance on Allowing Transmitting Portable Electronic Devices. Standard, Radio Technical Commission for Aeronautics (RTCA).

RTCA (2011). DO-178C: Software Considerations in Airborne Systems and Equipment Certification. Standard, Radio Technical Commission for Aeronautics (RTCA).

RTCA (2011). DO-278: S Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems. Standard, Radio Technical Commission for Aeronautics (RTCA).

SAE (1996). ARP4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment. Standard, SAE International.

Underwood, P. and P. Waterson (2013). Accident Analysis Models and Methods: Guidance for Safety Professionals. Report, Loughborough University.