EasyChair Preprint

№ 10711

Acceptance of Residual Risk in a Brazilian Military Aeronautical Project Through the Application of a Method

Daniel Rondon Pleffken, Vitor Oliveira Bourguignon, Guilherme Moreira and Christopher Shneider Cerqueira

August 15, 2023

Acceptance of Residual Risk in Brazilian Military Aeronautical Design through Methodology Application

Daniel Rondon Pleffken

Aeronautics Institute of Technology, Brazil. E-mail: rondon@ita.br

Vitor Oliveira Bourguignon

Aeronautics Institute of Technology, Brazil. E-mail: bourguignonvhob@fab.mil.br

Guilherme Moreira

Aeronautics Institute of Technology, Brazil. E-mail: moreira@ita.br

Christopher Shneider Cerqueira

Aeronautics Institute of Technology, Brazil. E-mail: chris@ita.br

The certification phase of military aeronautical design in Brazil necessitates the demonstration of compliance with mission-related requirements. Within the realm of engineering activities associated with initial airworthiness, the System Safety Analysis (SSA) assumes a critical role in the design process. This analysis entails determining the adequacy of system safety measures and striking a balance between safety, cost, and military capability. In some instances, the emphasis placed on military capacity equals or surpasses that placed on operational safety. Competent authorities ensure the safety of systems and products employed in fulfilling missions, necessitating a methodical assessment of associated risks. To address this need, the development of a comprehensive guide to support risk assessment decisions in specific operations becomes imperative. In this article, the authors draw upon their extensive experience in certifying military aeronautical products to accomplish the following objectives: (1) provide a concise overview of the concept of risk acceptance as applied to aeronautical design; (2) introduce the risk analysis methodology employed in military aeronautical projects in Brazil; (3) present a robust methodology that substantiates the acceptance of residual risk in Brazilian military aeronautical projects; and (4) demonstrate the practical application of this methodology in substantiating the acceptance of residual risk in the operation of remotely piloted aircraft systems.

Keywords: Airworthiness, risk, military design, quality.

1. Introduction

Aviation safety, as defined by the International Civil Aviation Organization (ICAO), pertains to the State in which the risk of causing harm to individuals or property is limited to or maintained at an acceptable level through continuous processes of hazard identification and risk management (Doc 9859/ICAO). Brazil, being one of the founding countries of ICAO, signed its participation in 1945 and ratified it on Jun. 8, 1946.

While aviation safety is governed by international agreements under the purview of ICAO, each country has the liberty to establish its own set of aeronautical regulations, provided they comply with the mandatory regulations set by the Organization.

In the context of military aircraft, the Brazilian Aeronautical Code (CBA) of the PRESIDENCY OF THE REPUBLIC - CASA CIVIL (1986) stipulates that the operation of these aircraft is subject to flight and air traffic protection provisions, except during wartime missions or specific training activities (Brasil, 1986).

The safety of Brazilian military aviation is upheld through a systemic approach, wherein the relevant authorities oversee all aircraft-related activities, from design and manufacturing to operation and maintenance, throughout the product's life cycle (Silva, 2017).

The Department of Aerospace Science and Technology (DCTA) is defined as the Certifying Authority of the Aeronautics Command for the space, aeronautics, and defense sectors. The

Industrial Fostering and Coordination Institute (IFI) is responsible for certification activities related to aerospace sector products/projects and quality management systems within the scope of the Brazilian Air Force (Brasil, 2016).

Conformity assessment of a military aeronautical product can be conducted by three different entities: the manufacturer or supplier (first party), the operator or customer (second party), and the certification authority, which has no direct interest in the product's commercialization (third party) (Brasil, 2019).

Certification activities involving the independent assessment of aeronautical product conformity by a third party compel aircraft and component manufacturers to incorporate quality mechanisms throughout all phases of their respective projects. The primary objective is to prevent accidents arising from design flaws. Furthermore, certification assists the military aeronautics industry in achieving high levels of reliability by employing tools that mitigate potential safety issues without rendering military use impracticable for fulfilling the product's intended mission.

Consequently, many potential issues that may arise with an aeronautical product are addressed early on during the initial development/certification phases, thereby averting the need for retrofits or financial burdens in later stages of the project that could render the product's manufacturing and operation infeasible.

Ensuring the safety of systems and products employed in fulfilling military missions is the responsibility of competent authorities who prioritize safety as an imperative aspect, eliminating unnecessary or unjustifiable risks that could compromise it.

Therefore, in designing a system, the System Safety Analysis (SSA) assumes a vital role in engineering activities associated with initial airworthiness certification.

This analysis necessitates a systematic process for military designs to ascertain whether the system is adequately secure and to establish an acceptable equilibrium among safety, cost, and military capability (Brasil, 2019).

Despite using SSA to fulfill mission requirements, a certain degree of residual risk may persist. Consequently, developing a guide that substantiates the acceptance of residual risk in military designs becomes imperative, facilitating risk assessment-based decision-making in specific military operations (Brasil, 2022).

2. Review of Risk Acceptance in Aeronautical Designs and Its Application to the Military Context

Airworthiness certification ensures an aircraft is safe and adheres to relevant safety requirements. Determining airworthiness-related risk levels specified in certification standards has evolved, drawing upon conventional approaches. These risk levels have been refined in recent years by considering historical accident data, engaging in discussions and deliberations, and striving for more rational requirements. The incorporation of Safety Analysis approaches has further contributed to this improvement. For instance, according to the European Aviation Safety Agency's (EASA) document GM AMC 21.A.3B "Defect Correction - Sufficiency of proposed corrective action," airworthiness-related risk levels, or the airworthiness risk objective, are expressed as a numerical value representing the rate of airworthiness-related fatal accidents per flight hour or flight cycle. In civil transport aviation, the safety objective, focusing solely on accidents resulting from aircraft system failures, typically aims to achieve no more than one catastrophic accident per every 10,000,000 flight hours.

The nature of military aviation operations possesses distinct characteristics. Military aircraft missions often unfold in extreme environmental conditions. Furthermore, civil airworthiness standards do not encompass criteria or requirements applicable to systems equivalent to weaponry and mission systems (such as radars, sensors, pods, etc.). Additionally, the flight quality requirements for civil aircraft do not account for the unique operational environments in which military aircraft operate. The operation of military aircraft in hostile environments necessitates exposure to aerodynamic loads significantly higher than those experienced by civil aircraft. The qualification of military aircraft for using self-defense technologies like chaff,

flares, and others is frequently demanded. Military functions, missions, and tasks entail distinctive aspects without civil aviation counterparts. War-related operations involve hazardous missions conducted in hostile territories. The technical requirements for military aircraft entail the rapid integration of technological advancements, often before reaching the maturity level typically expected in civil aviation.

Given the peculiarities mentioned above and recognizing that the core activities of the Armed Forces differ from those of civilian airlines, a higher level of risk acceptance is permissible for military aircraft. Specifically, the acceptance level for military transport aircraft, for example, is determined by multiplying the relevant factor for civil aviation by a factor of 10. Moreover, different categories of military aircraft are also taken into consideration. Generally, the following probabilities of occurrence for catastrophic failure conditions per flight hour can be adopted:

- 10^{-8} for military transport aircraft;
- 10^{-7} for military helicopters; and
- 10^{-6} for military fighter aircraft.

Owing to its unique nature, military aviation necessitates greater flexibility in safety levels, encompassing a spectrum ranging from acceptable to unacceptable. In this context, it is crucial to consider the principle of military necessity in light of applying international law governing armed conflict in air force operations. This principle underscores that the defense of the homeland constitutes the primary mission of the Armed Forces. It is imperative to recognize that actions undertaken during armed conflict situations must always prioritize the maintenance of the sovereignty of the Brazilian State. Thus, for a specific military mission, the competent authority may accept residual risk levels below those previously mentioned, as the core activity of military operations may require increased exposure to risks, demanding urgency and readiness. (Brasil, 2017).

3. Risk Analysis Method for Military Aeronautical Projects in Brazil

The MIL-STD-882E standard, issued by the United States Department of Defense (DoD), is a comprehensive document that outlines the standard practice of system safety. This standard aims to eliminate hazards whenever possible and minimize risks when hazards cannot be entirely eliminated. It encompasses hazards applicable to systems, products, and equipment (including hardware and software) throughout their lifecycle, including design, development, testing, production, service life, and decommissioning.

The standard practice of system safety analysis described in MIL-STD-882E provides a method for identifying, classifying, and mitigating hazards in a standardized manner. It is essential to note that this document has a military focus and was developed with a commitment to protecting personnel and materials against fatal injuries and accidents and safeguarding defense systems and the environment.

Upon initiation of the certification process with the Department of Aerospace Science and Technology (DCTA)/Industrial Fostering and Coordination Institute (IFI), the MIL-STD-882E serves as a framework, defining the necessary definitions and minimum mandatory requirements that the requesting industry must fulfill. This process aims to ensure an acceptable level of safety in the certified system's operation.

The system safety analysis process, comprising eight elements, follows a logical sequence of execution. The following provides an overview of these elements and their sequential implementation:

ELEMENT 1

Planning the Systems Safety Analysis Documentation: The applicant must develop a plan incorporating hazard management as an integral part of the Systems Engineering process.

ELEMENT 2

Identification and Documentation of Hazards: A systematic review process is employed to identify hazards, encompassing hardware, software systems, and the operator interface system.

ELEMENT 3

Risk Assessment and Documentation: The evaluation of risk involves the assessment of severity categories, probability levels, and the utilization of a risk assessment matrix. Severity considers factors such as fatalities, injuries, environmental impacts, and material losses, while probability assesses the likelihood of failure or hazardous conditions.

ELEMENT 4

Identification and Documentation of Risk Mitigations: Potential risk mitigations are identified, and their expected reduction or workaround is estimated and documented. The primary objective is to eliminate the hazard, if feasible. However, if elimination is not possible, the associated risk can be reduced to an acceptable level with minimal cost, time, and performance impact.

ELEMENT 5

Risk Reduction: Assessed risks are prioritized, and appropriate mitigations are implemented to achieve an acceptable level of risk. The selection of risk reduction methods should consider factors such as cost, feasibility, and effectiveness.

ELEMENT 6

Verification, Validation, and Documentation of Risk Reduction: The implementation and effectiveness of selected risk mitigations must be verified through suitable analysis, testing, demonstration, or verification procedures.

ELEMENT 7

Risk Acceptance and Documentation: Before exposing personnel, equipment, or the environment to a known system hazard, the responsible authority must accept the risk.

ELEMENT 8

Performance throughout the System Lifecycle: The system safety assessment process continues throughout the system's lifecycle, ensuring ongoing safety considerations and analysis as the system operates.

By adhering to this systematic approach outlined in MIL-STD-882E, military aeronautical projects in Brazil can effectively analyze risks, identify hazards, implement risk mitigations, and ensure safety throughout the lifecycle of the system.

4. Residual Risk Acceptance Method of Military Aeronautical Projects in Brazil

The described method is applicable for establishing the certification basis of any military design that requires a military-type certificate to ensure the safety of the systems and products employed in fulfilling its missions. The residual risk acceptance process is a support tool for making risk assessment decisions within a given operation.

Following the requirements stipulated in acquisition contracts, the authority (DCTA/IFI) can certify a military aircraft, including all its systems, in a basic "green" version based on Brazilian airworthiness requirements (RBAC), with exceptions agreed upon between the Brazilian Air Force and the respective company. However, for military projects, it is deemed necessary to tailor the certification process to RBAC section 2X.1309 (25.1309, 27.1309, and 29.1309) as the underlying safety assessment process. This consideration is rooted in the understanding that the civil approach focuses on safety objectives and that an acceptable level of safety is already defined and captured in the respective Civil Airworthiness Code.

It is essential to recognize that a military aircraft is primarily oriented toward conducting missions with the highest possible level of safety. Therefore, it is acknowledged that the risks associated with military missions may involve operational scenarios beyond the aircraft developer's control.

Companies must submit the acceptable levels of safety expected for the systems, equipment, and installations, as well as the criteria for risk acceptance, through the System Safety Analysis (SSA) to the Certification Organization.

The approach to determining the outcome of the SSA can be either objective-based or risk-based, or a combination of both:

Objective-based approach: This approach establishes safety goals based on the potential severity of hazards.

The risk-based approach ensures that risks are minimized to the lowest reasonably achievable level without predetermined safety levels. It requires a cost-benefit analysis to determine the acceptability of the safety level.

These two approaches can be combined to achieve specific safety objectives, primarily utilizing a goal-based approach. However, if this is not feasible, a risk-based approach is employed, and a cost-benefit analysis is conducted to determine whether the risk can be accepted or needs to be mitigated.

Depending on the defensive strategies for different programs, the system safety analysis can be divided into two parts:

Civil Safety Assessment Process: Based on RBAC section 2X.1309 (System Safety Analysis and Assessment).

Military Safety Assessment Process: Based on MIL-STD-882E. However, the utilization of tables and tasks from this standard must be determined on a case-by-case basis in collaboration between the applicant and the Certification Organization.

Generally, a "green" aircraft complies with §2X.1309 requirements and other related safety requirements that comprise the "civil safety assessment."

The design of systems, equipment, and facilities essential for the safe execution of military missions must take into account the military operational scenario.

The safety assessment for military aviation is more appropriately referred to as a risk assessment. The Military Risk Assessment (MRA) complements the safety assessment to demonstrate compliance with RBAC 2X.1309 for the "green" platform in a civil flight profile.

The Military Risk Assessment (MRA) process, based on MIL-STD-882E, involves the following steps:

Hazard identification: Identification and classification of hazards.

Risk assessment: Categorization of risks into high, serious, medium, and low categories.

Risk mitigation and review: Risk mitigation is conducted at two levels: design precautions and operational mitigation. Design precautions involve measures taken to mitigate risks associated with military missions, such as design selection, safety devices, and system warnings. Operational mitigation entails creating and evaluating operational procedures that provide mitigating actions for the identified risks. All risk mitigation activities aim to reduce risks to the lowest possible level across all categories.

If the residual risks remain higher than the low level even after completing mitigation activities, the risks must be internally accepted within COMAER. A specific competent authority must accept each level of risk. The acceptance of residual risks may be based on a comparison with other aircraft models operating under similar conditions and criteria additionally defined by the competent authority.

Contracts for the acquisition and development of systems and products for the Brazilian Air Force (COMAER) must include relevant clauses referring to the requirements for the delivery and approval of the System Safety Program Plan, and the respective drafts must be previously agreed upon with the Competent Certification Organization.

These contracts should also contain or reference the regulations and standards that are considered as a reference for the preparation of the Systems Safety Plan.

The acceptance of risk by the appropriate level is determined based on the specific certification process, considering each process's peculiarities according to the risk category (High, Serious, Medium, and Low). If applicable, alternative means of compliance may be proposed through the Control Sheet for Military Certification Issues (FCAR-M) or the System Safety Program Plan.

5. Example of Application of the Residual Risk Acceptance Method in Military Aeronautical Projects in Brazil

5.1 Contextualization of the Example

In this example, we consider applying the residual risk acceptance method to a specific scenario involving a Remotely Piloted Aircraft System (RPAS). Initially, traditional methodologies employed in civil aviation were utilized for risk acceptance. However, due to regulatory limitations and a lack of statistical accident data specific to the RPAS system under study, there needed to be more data to support the decision-making process of the competent authorities. Consequently, a technical impasse was reached, resulting in the denial of authorization for the RPAS missions and the inability to issue the Certificate of Airworthiness.

5.2 Risk-Based Navigation Methodology

To address this situation, the Risk-Based Navigation methodology was employed to assess the safety of the RPAS operation. The operation safety indices obtained through this methodology aligned with aviation reality. The number of fatalities resulting from design flaws for the RPAS was considered fixed at 10-5 fatalities per hour, similar to the prescribed standard for small civil human-crewed aircraft of class I in RBAC 23.

However, it is essential to note that the RPAS is intended for Air Control tasks involving the Brazilian Air Force's responsibility to dominate the airspace and space of interest, preventing the enemy from doing so. Within the context of certification, all the missions for which the RPAS will be employed were defined to comprehensively assess the situations that could significantly impact the safety indices of the operation.

For instance, in a hypothetical RPAS operation over Rio de Janeiro, the calculated risk was determined to be at a medium level.

5.3 Residual Risk and Application of the Method

Considering the regulations and standards that serve as a reference for preparing the Systems Safety Plan, the acceptance of residual risk was based on a comparison with other models operating under similar conditions, considering additional criteria defined by the competent authority.

The competent authorities are responsible for accepting the respective levels of residual risk identified using the Control Sheet for Military Certification Issues (FCAR-M). (See Table 1).

Table 1. Risk Acceptance

Risk category	Level of acceptance in COMAER
High	Risk Assessment Committee (CAR)
Seriously	DCTA
Medium	IFI
Low	Specialist Certification

In Table 1, This process involved the involvement of the CAR (Committee for Airworthiness Regulation), a permanent committee comprised of representatives from various sectors of the Brazilian Air Force's highest echelon. The CAR deliberates on resolving Service Difficulties with Limiting Airworthiness and establishes and maintains Airworthiness Limitations resulting from these difficulties.

The members of the CAR include:

General Staff of the Air Force – EMAER

General Support Command – COMGAP

Preparation Command – COMPREP

Aerospace Operations Command – COMAE

Department of Aerospace Science and Technology – DCTA

Center for Research and Prevention of Aeronautical Accidents – CENIPA

To effectively address the high-risk scenarios identified, the method establishes a technical-operational collegiate to deliberate on high-risk situations. Lima (2016) states, "The essence of a multimethod logical approach is the association of the parts of the participating methodologies, combined by juxtaposition or agglutination." Given the multiple biases, interests, and conflicts inherent in the selected problem, utilizing a multimethod logical approach proves opportune when dealing with high-risk situations.

In the presented example, the acceptance of the residual risk was categorized as MEDIUM, thus being accepted by the director of the IFI (Institute of Industrial Facilities).

6. Conclusions

In conclusion, this study has examined various methods and their contributions to the practice of Systems Safety Analysis in aeronautical projects. The residual risk acceptance process has emerged as a valuable tool within the certification process, providing several benefits for design developers in improving safety practices. These contributions include:

Improved communication: The process enhances communication between the applicant and the certification body, facilitating a clearer understanding of requirements and responsibilities.

Enhanced information flow: Stakeholders involved in the project benefit from improved information flow, ensuring that all relevant parties have access to necessary data and insights.

More precise delineation of responsibilities: The process establishes a clearer picture of the responsibilities and scope of the Systems Safety Analysis (SSA), enabling effective coordination and collaboration among project participants.

Overcoming operational limitations: The process enables operating systems that would otherwise be deemed inoperable when solely relying on traditional methods. Collegiate decisions, which consider the problem from various perspectives, play a crucial role in allowing such operations.

Furthermore, applying this process to safety-critical projects leads to comprehensive analysis, mitigating risks associated with features and functions that could impact the operation's safety.

During the initial airworthiness phase, the SSA defines the safety margin and ensures the design is safe before entering service. The results of the SSA serve as a basis for establishing operational limitations and maintenance requirements, ensuring continued safe operation throughout the operational airworthiness phase.

Adopting the concepts presented in this process can improve the acceptance of new aerospace projects/products. The analysis of residual risk, accepted by competent authorities within specific contexts, allows for enhanced Verification and Validation (V&V) processes. Such projects/products include electric aircraft, Remotely Piloted Aircraft Systems (RPAS), flying vehicles, suborbital vehicles, satellites, and more.

This study has provided an overview of risk acceptance in aeronautical projects, focusing on the methods applied to military aerospace projects in Brazil and the method underpinning the acceptance of residual risk in such projects. Furthermore, the application of the method in remotely piloted aircraft systems has been discussed.

In summary, utilizing the presented process can lead to significant advancements in the acceptance and safety analysis of aerospace projects, promoting effective risk management and improving the overall safety standards in the field.

Acknowledgment

This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Finance Code 001.

References

Brazil (1986) “Presidency of the republic. Law 7.565 - Brazilian Aeronautics Code”. Brasilia, Dec. 19. 1986.Available:<http://www.planalto.gov.br/ccivil_03/leis/L7565.htm> Access on Feb. 28, 2023.

Brasil(2016). COMAER, Dca 800-2 “Quality assurance and safety of systems and products at the computer," Brazilian Air Force.

Brazil (2017) COMAER. Ica 57-21 “Military airworthiness regulation – procedures for certification of aeronautical products," Brazilian Air Force.

Brasil(2019). COMAER, Ica 60-2 “Procedure for product and quality management system certification in the space sector," Brazilian Air Force.

Brasil(2022). COMAER, Ica 57-25 “Methodology for accepting residual risk in military projects," Brazilian Air Force.

Lima(2016) Lima and Eliomar Araújo. "Soft methods of operations research for structuring problems in complex scenarios." Brazilian Symposium on Operations Research, September 27-30, 2016

Silva(2017) C. Silva, G. Moreira, M. Souza, “Proposals for a space product assurance process improvement based on an aeronautical process," IEEE,218, pp.1–9.