PROFESSIONAL MASTER'S DISSERTATION

DEVELOPMENT OF HOLISTIC FRAMEWORK TO PROTECTING EMBEDDED SOFTWARE AGAINST MALICIOUS ATTACKS

Mauri Sudário Ferreira Dantas

Professional Postgraduate Program in Electrical Engineering
DEPARTMENT OF ELECTRICAL ENGINEERING
FACULTY OF TECHNOLOGY
UNIVERSITY OF BRASILIA

UNIVERSITY OF BRASILIA

PROFESSIONAL MASTER'S DISSERTATION

DEVELOPMENT OF HOLISTIC FRAMEWORK TO PROTECTING EMBEDDED SOFTWARE AGAINST MALICIOUS ATTACKS

Mauri Sudário Ferreira Dantas

Professional Master's Dissertation submitted to the Department of Electrical Engineering as a partial requirement for obtaining the degree of Master in Electrical Engineering

Examining Board

Prof. Éder Souza Gualberto, Dr, FT/UnB _____
Supervisor

Prof. Edna Dias Canedo, Ph.D, FT/UnB _____
Internal Examiner

Prof. Giovanni Almeida Santos, Ph.D, FT/UnB _____
External Examiner

CATALOG CARD

DANTAS, MAURI SUDÁRIO FERREIRA
DEVELOPMENT OF HOLISTIC FRAMEWORK TO PROTECTING EMBEDDED SOFTWARE AGAINST MALICIOUS ATTACKS [Federal District] 2025.
xvi, 173 p., 210 x 297 mm (ENE/FT/UnB, Master, Electrical Engineering, 2025).
Professional Master's Dissertation - University of Brasilia, Faculty of Technology.
Department of Electrical Engineering

1. Inter-connectivity	2. Cybersecurity
3. Embedded Systems	4. Risk Assessment
I. ENE/FT/UnB	II. PPEE.MP.100

BIBLIOGRAPHICAL REFERENCE

DANTAS, M. S. F. (2025). *DEVELOPMENT OF HOLISTIC FRAMEWORK TO PROTECTING EMBEDDED SOFTWARE AGAINST MALICIOUS ATTACKS*. Professional Master's Dissertation, Department of Electrical Engineering, University of Brasilia, Brasilia, DF, 173 p.

ASSIGNMENT OF RIGHTS

AUTHOR: Mauri Sudário Ferreira Dantas
TITLE: DEVELOPMENT OF HOLISTIC FRAMEWORK TO PROTECTING EMBEDDED SOFTWARE AGAINST MALICIOUS ATTACKS.
DEGREE: Master in Electrical Engineering
YEAR: 2025

Mauri Sudário Ferreira Dantas
Dep. of Electrical Engineering (ENE) - FT
University of Brasilia (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasilia - DF - Brasil

DEDICATION

I dedicate this work to my family, whose unwavering support, love, and encouragement have been my constant source of strength and inspiration. To my parents, for instilling in me the value of education and perseverance. To my friends, for their companionship and motivation throughout this journey. And to all those who believed in me and supported my dreams.

A special thank you to Professor Giovanni Almeida, whose guidance and support were instrumental in my selection for the research project at Airbus. His mentorship played a crucial role in shaping this achievement, and I am deeply grateful for his encouragement and belief in my potential.

This achievement is as much yours as it is mine.

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to everyone who, in one way or another, contributed to the completion of this thesis. First, I would like to thank my advisors, whose guidance, patience, and expertise were fundamental to the development of this work. Your support and constant encouragement were essential in helping me overcome the challenges faced throughout this academic journey.

To my colleagues and friends, thank you for sharing your experiences and knowledge. The productive discussions and moral support made this path more motivating and enriching, contributing significantly to the progress of this research.

I am also deeply grateful to my family for their understanding, patience, and unconditional support throughout the entire research and writing process. You have been my foundation and source of inspiration every step of the way, and without your support, this achievement would not have been possible.

Finally, I would like to extend my thanks to Airbus Defense and Space, for the opportunity to carry out this research and for the support provided, which allowed me to delve deeper into the issues discussed here. To all of you, my heartfelt thanks!

RESUMO

Esta dissertação propõe um framework holístico para a proteção de sistemas embarcados contra ciberataques, com foco no setor aeroespacial. A crescente complexidade e interconectividade desses sistemas exigem uma abordagem que integre normas de segurança, avaliação de riscos e estratégias adaptativas, garantindo a proteção ao longo do ciclo de vida do software. O framework desenvolvido baseia-se em uma análise abrangente de ameaças e distingue entre abordagens genéricas (padrões globais, como a ISO/IEC 27001) e integradas (que combinam padrões globais com diretrizes setoriais, como a DO-178C, DO-254 e DO-326A). O foco está na identificação de ativos, ameaças e vulnerabilidades, bem como no uso de ferramentas de análise de código estática e dinâmica. Além da construção teórica do framework holístico, a pesquisa inclui uma validação prática por meio de entrevistas e formulários aplicados a especialistas, avaliando a coerência, aplicabilidade e efetividade do framework. A análise inicial sugere que a abordagem proposta oferece uma proteção mais eficaz e adaptável do que frameworks tradicionais baseados unicamente na conformidade normativa. Esta pesquisa fornece um framework holístico estruturado e validado, promovendo práticas de segurança mais integradas e proativas para sistemas embarcados críticos. Além de contribuir para a evolução dos padrões de segurança no setor aeroespacial, estabelece uma base metodológica que pode apoiar estudos futuros e sua aplicação prática em diferentes cenários.

ABSTRACT

This dissertation proposes a holistic framework for protecting embedded systems against cyberattacks, with a focus on the aerospace sector. The increasing complexity and interconnectivity of such systems demands an approach that integrates security standards, risk assessment, and adaptive strategies, ensuring protection throughout the software lifecycle. The framework is grounded in a comprehensive threat analysis and distinguishes between generic approaches (based on global standards such as ISO/IEC 27001) and integrated ones (which combine global standards with sector-specific guidelines, such as DO-178C, DO-254, and DO-326A). The focus is on the identification of assets, threats, and vulnerabilities, as well as the use of static and dynamic code analysis tools. In addition to the theoretical construction of the holistic framework, the research includes a practical validation conducted through interviews and questionnaires with domain experts, evaluating the coherence, applicability and effectiveness of the framework. Preliminary findings suggest that the proposed approach offers more effective and adaptable protection compared to traditional frameworks that rely solely on regulatory compliance. This study delivers a holistic structured and validated framework that promotes more integrated and proactive security practices for critical embedded systems. In addition to contributing to the advancement of security standards in the aerospace sector, it establishes a methodological foundation to support future research and practical application in diverse scenarios.

SUMMARY

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

Embedded systems play a crucial role in our society, serving as the backbone for critical industries such as aviation, healthcare, and infrastructure. These systems are essential for the operation of various devices and machinery, ranging from aircraft control systems to medical devices and smart grids (1). With advancements in technology and the increasing digitalization of these sectors, the interconnectivity of embedded systems has grown exponentially, enhancing efficiency and functionality. However, this expanded connectivity has also increased the attack surface for cyber threats, making these systems more vulnerable to malicious activities (2). The integration of embedded systems into essential services and infrastructures has raised concerns about their security, as any compromise can result in significant operational disruptions and even pose risks to human lives (3). Ensuring the robust protection of these systems against an evolving landscape of cyber threats has therefore become a critical priority for industry stakeholders and policymakers.

Embedded systems are computing devices dedicated to performing specific functions within a larger system, integrating hardware and software into a single platform to provide efficient control and monitoring (1). Unlike traditional computers, they are designed to operate with high reliability and real-time performance, characteristics essential for applications in critical environments such as aircraft and medical devices (4). Their specialized nature requires seamless integration between hardware and software, which increases system complexity and makes them susceptible to security vulnerabilities. Even a minor vulnerability can compromise the entire system's functionality, leading to severe consequences such as operational failures, service disruptions, and, in extreme cases, risks to safety and human life (5). For this reason, ensuring the security of these systems is imperative, especially in light of the growing cyber threats seeking to exploit their vulnerabilities and cause significant damage.

Embedded systems face a variety of security threats, including malware attacks, software vulnerability exploitation, and physical tampering. Malware can compromise the operation of critical systems, causing operational failures or leakage of sensitive information (6). Software vulnerabilities, such as coding errors or input validation flaws, are another common attack vector, enabling attackers to gain unauthorized control or induce undesired behaviors in the system (2). Additionally, physical tampering poses a significant risk, as direct access to the device can allow attackers to extract confidential information or alter hardware and firmware, compromising the system's integrity and authenticity (5).

Security challenges are exacerbated by the resource constraints inherent in embedded systems, such as processing capacity and energy consumption, which limit the implementation of more robust security measures like advanced encryption and intrusion detection systems (1). Additionally, many embedded systems in sectors such as avionics are distributed across large networks, making it difficult to update and maintain these devices, especially when addressing security vulnerabilities (4). The complexity of managing secure updates in avionics environments increases the risk of exposure to attacks, making these systems attractive targets for cybercriminals. Therefore, developing security strategies tailored to the characteristics and limitations of embedded systems is a continuous and crucial challenge for ensuring protection against cyber threats.

Security failures in embedded systems can have devastating consequences, not only for the integrity and functionality of the devices but also for the safety and well-being of people. A vulnerability exploited in these systems can lead to significant operational disruptions, as demonstrated by the cyberattack on the Ukrainian power grid in 2015, which left thousands of people without electricity for several hours and highlighted the fragility of industrial control systems (7). Additionally, security breaches can result in physical damage to equipment, as occurred in 2010 with the Stuxnet attack, which damaged nuclear centrifuges in Iran, demonstrating how attacks on embedded systems can be used for industrial sabotage (8). The exposure of sensitive data, such as medical or financial information, is also a potential consequence, endangering the privacy and security of individuals and organizations (3).

In avionics, security failures can pose direct risks to human life. In aviation, cybersecurity of embedded systems is even more critical, as a successful attack could compromise navigation or flight control systems, leading to catastrophic accidents. In 2018, Boeing had to review the software of its aircraft control systems following reports of software failures related to accidents involving 737 MAX aircraft, underscoring the importance of ensuring the integrity and security of embedded systems to prevent tragedies (9).

These incidents illustrate how security failures in embedded systems not only result in significant financial losses for the companies involved but can also endanger human life and critical infrastructure. The cost of a successful cyberattack can be incalculable, including damage to reputation, loss of consumer trust, and legal consequences. Thus, protecting embedded systems against cyber threats should not be viewed merely as a technical issue but also as a social and ethical responsibility essential for protecting human lives and ensuring the continuity of essential services.

Traditional security approaches for embedded software present several limitations, particularly in the context of an increasingly dynamic and complex cyber environment. These methodologies, often reactive, focus on isolated measures and do not integrate security comprehensively throughout the software life cycle, from initial design to operation and maintenance. This creates security gaps, as protection is applied only at specific stages, without considering the evolution of threats and changes in security requirements over time (2). Moreover, these approaches tend to prioritize security in either hardware or software aspects independently, neglecting the critical interdependence between them and the need to protect the integrity of the system as a whole (1).

Another significant limitation is the inability of these approaches to address emerging cyber threats, such as advanced denial-of-service (DoS) attacks, zero-day exploits, and firmware manipulation. With the increasing sophistication of attacks, traditional strategies that rely primarily on firewalls and antivirus have become insufficient to counter more advanced attack techniques, such as backdoor insertion and code injection attacks (5). Furthermore, many of these methodologies do not account for the need for frequent and secure security updates, which is particularly problematic for distributed embedded systems, where implementing security patches can be complicated and risky (4).

Therefore, there is an urgent need to develop a security approach that integrates protection measures holistically and continuously throughout the entire life cycle of embedded software. This new framework must be capable of proactively anticipating and mitigating new threats, adapting to changes in the security environment, and ensuring the integrity, confidentiality, and availability of systems. Only then will it be possible to effectively address emerging challenges and protect embedded systems that perform critical

functions across a variety of sectors.

Due to the complexity and criticality of embedded systems, adopting a holistic approach to software security is essential to ensure effective protection against cyber threats. These systems, used in avionics, perform critical functions that require high reliability and continuous performance, making them attractive targets for cyberattacks that can have severe consequences, including disruption of essential services and risks to human safety (1). Traditional security, focused on isolated protection measures such as firewalls and antivirus, is no longer sufficient to address the increasing sophistication of current threats. A holistic approach that integrates security measures at all stages of the software development life cycle—from conception and design to operation and maintenance—is necessary to proactively anticipate and mitigate emerging risks (2).

This integrated framework involves combining various security techniques, including secure coding practices, robust encryption, strict access control, and continuous monitoring, creating layers of defense that make the system more resilient to different types of attacks (5). For example, by implementing security from the early stages of development, it is possible to detect and correct vulnerabilities before they become entry points for attackers. During operation, applying continuous monitoring and security updates ensures that the system can quickly respond to evolving threats, minimizing the impact of potential security failures (4).

Therefore, a holistic approach not only improves the resilience of embedded systems against attacks but also promotes an integrated and proactive view of security, where each component and phase of development is considered part of an interdependent ecosystem. This is crucial to protect systems that perform vital functions in critical environments, where any vulnerability can result in catastrophic consequences. Integrating security comprehensively and continuously is the only way to ensure that these systems remain secure and reliable, even in the face of the most sophisticated cyber threats.

The primary objective of this research is to develop a holistic framework for embedded software security that systematically integrates all critical protection stages, from threat analysis to the continuous implementation of security measures throughout the entire system life cycle. This framework aims to incorporate detailed threat analysis, precise identification of attack vectors, and effective prioritization of countermeasures, ensuring that all identified vulnerabilities are mitigated with the most appropriate security practices. Furthermore, the proposal seeks to ensure that security is a constant concern from the initial software development, through rigorous testing and validations, to the operation and maintenance phases, where continuous monitoring and rapid incident response are essential. By providing an integrated and comprehensive view of security, this framework aims to enhance the resilience of embedded systems against cyberattacks, thereby protecting critical functions in sectors such as avionics, where reliability and safety are paramount.

The expected contributions of this research include the creation of a robust and adaptable security holistic framework for different types of embedded systems, offering a practical and efficient solution for protecting devices in sectors such as avionics. This mothodology will enable organizations to implement a customized security approach, adjusting practices and countermeasures according to the specific characteristics and vulnerabilities of their systems. Additionally, the research aims to improve security practices in the industry, promoting a more effective integration of security guidelines throughout the entire embedded

systems life cycle, from development to maintenance, which is essential for preventing critical failures and mitigating emerging risks. In the academic realm, the research will contribute to advancing knowledge on the security of critical systems, providing a theoretical and methodological foundation for future studies and fostering the development of new techniques and tools for protecting these systems.

Furthermore, the proposed framework has the potential to influence the evolution of security standards and practices within the industry, serving as a model for updating existing standards and developing new regulations that account for the complexity and interdependence of modern embedded systems. By establishing a holistic and adaptable approach, this research aims to address gaps in current security methodologies, promoting a more integrated and proactive view of cybersecurity in critical systems. Consequently, it is expected that the contributions of this work will not only enhance the operational security and resilience of embedded systems but also inspire future innovations and advancements in the field, aiding in the creation of a safer and more reliable environment for the deployment of emerging technologies.

The framework of this research will be based on a holistic approach to embedded systems security, encompassing all phases of the software life cycle, from development to continuous maintenance and updates. Initially, a detailed analysis of threats and vulnerabilities will be conducted, utilizing modeling techniques such as STRIDE and Attack Trees to identify potential attack vectors and assess their potential impacts. Subsequently, risk assessment tools such as Fault Tree Analysis (FTA) and Failure Mode and Effects Analysis (FMEA) will be employed to quantify and prioritize identified risks, guiding the efficient allocation of resources for mitigating critical threats.

The framework will also integrate security measures into each phase of software development, including secure coding practices, continuous security validation, and penetration testing to identify and rectify vulnerabilities before deployment. During operation and maintenance, intrusion detection and monitoring systems will be implemented to ensure that any anomalous behavior or attempted breaches are quickly identified and addressed. Additionally, an incident response plan will be developed to ensure a coordinated and efficient reaction to any eventuality, minimizing the impact of potential attacks.

By applying these methods in a structured and integrated manner, it is anticipated that comprehensive and proactive protection will be achieved, capable of effectively anticipating and mitigating cyber risks. This methodological approach will not only enhance the security of embedded systems but also establish an adaptable and replicable model that can be used as a reference in different contexts and critical sectors, thereby contributing to the strengthening of security practices in both industry and academia.

The comprehensive framework constitutes the generalizable conceptual foundation of this research, from which the specialized approach was derived. However, given the formal collaboration with specialists from Airbus Defence and Space and the domain focus on safety- and security-critical avionics systems, the empirical validation was deliberately concentrated on the integrated holistic framework. This integrated approach directly incorporates aviation-relevant DO standards (e.g., DO-178C for software, DO-326A for airworthiness security, and related companion documents), making it the most appropriate vehicle to elicit expert judgement and to assess applicability and effectiveness in the practitioners' real context. In short, the comprehensive framework provided the generalizable baseline; the integrated framework was validated empirically because it operationalizes that baseline under avionics-specific normative and certification constraints.

1.1 MOTIVATION

Protecting embedded systems against malicious attacks has become an increasing concern across various sectors, especially in the aviation industry, where the security and integrity of these systems are crucial for daily operations and public safety. Embedded systems in aircraft and defense equipment are responsible for critical functions such as avionics, communication, navigation, and control systems. Any compromise in their security could lead to severe operational failures, data breaches, or even catastrophic consequences.

The motivation for this research stems from the author's experience as a researcher at Airbus Defence and Space, where direct exposure to the challenges of protecting embedded systems in highly complex and regulated environments highlighted the need for a more integrated and holistic approach to cybersecurity. During this period, several vulnerabilities and limitations in existing security strategies became evident. For instance, while intrusion detection systems (IDS) and firewalls provide essential layers of protection, they often function in isolation and lack coordination with broader security frameworks. Similarly, encryption techniques safeguard data transmission, but they do not prevent unauthorized access from compromised internal components.

One critical example observed in the field was the challenge of securing legacy embedded systems that remain operational for decades in aircraft but were not originally designed with modern cybersecurity threats in mind. These systems often rely on outdated protocols that lack authentication mechanisms, making them susceptible to cyber threats such as spoofing and man-in-the-middle attacks. Additionally, compliance with multiple regulatory frameworks, such as DO-326A for aviation cybersecurity, often leads to fragmented security implementations, where different requirements are addressed separately rather than through a unified strategy.

The increasing interconnectedness and dependency of complex digital systems require a framework that goes beyond reactive threat mitigation and embraces proactive strategies. Traditional security approaches, which mainly focus on identifying and responding to known threats, are insufficient against the rapid evolution of cyber attack technologies, such as advanced persistent threats (APTs) and zero-day exploits. A more adaptive and resilient cybersecurity strategy is necessary to anticipate potential vulnerabilities before they are exploited.

This research proposes a holistic framework that integrates international best practices with industry-specific regulations, creating a more adaptive and resilient approach. By incorporating global standards such as NIST SP 800-53, ISO 27001, and sector-specific frameworks like DO-326A, this framework aims to provide a structured yet flexible approach to securing embedded systems. The proposed approach not only enhances security within Airbus Defence and Space but also serves as a model for the broader aviation industry and other sectors facing similar challenges.

Ultimately, the motivation for this thesis is driven both by the identified needs within the professional environment of Airbus Defence and Space and the ambition to contribute to a deeper understanding and more effective implementation of cybersecurity for embedded systems. Through rigorous research and an innovative methodological framework, this study seeks to bridge the gap between fragmented security practices and a unified, proactive approach capable of withstanding the evolving cyber threat landscape.

1.2 RESEARCH QUESTIONS

Developing a holistic framework for protecting embedded systems against malicious attacks requires meticulous and in-depth research. This chapter outlines three essential research questions that will guide the focus of this study, aiming to better understand how to integrate and apply security standards, develop adaptive risk mitigation strategies, and establish a robust validation framework to assess the effectiveness of security measures. These questions will not be answered immediately; instead, they will serve as the foundation for ongoing research and the development of the thesis.

The first question guiding this research addresses how the integration of international and industry standards impacts the effectiveness of information security management systems (ISMS). An ISMS refers to a set of policies, procedures, and controls designed to manage and protect an organization's information assets. This integration includes standards such as ISO/IEC 27001, NIST SP 800-53, DO-178C, DO-254, DO-326A, DO-355A, and DO-356A. This investigation will explore how the combination of these guidelines affects an organization's ability to defend its embedded systems against malicious intrusions. The complexity of these regulations requires a detailed analysis to understand whether the overlap of these standards provides a robust defense or if conflicts or redundancies create gaps in protection.

The second question investigates which security mechanisms and practices are most effective for embedded systems and how they can be selected and applied throughout the system's lifecycle. Instead of focusing on adaptive risk prediction, this part of the research emphasizes the practical integration of protective measures within design, development, verification, and maintenance processes. The analysis explores how security controls can be prioritized according to risk levels and operational constraints, ensuring that implementation remains feasible, verifiable, and aligned with the safety and performance requirements of critical environments.

The third question examines how the proposed holistic framework can be consistently incorporated into engineering and maintenance workflows to ensure long-term security assurance. It focuses on defining clear responsibilities, inputs and outputs, and verification points across each phase of the lifecycle, from initial design to system decommissioning. The investigation also addresses how traceability and governance can be maintained—through evidence records, risk tracking, and structured decision processes—so that the framework remains both auditable and adaptable to real-world operational contexts.

These questions form the backbone of the research and are vital to the development of a holistic framework that not only protects embedded systems effectively but also promotes a sustainable and adaptable security culture. As such, this chapter defines the questions that will shape the research objectives of this thesis, while also highlighting the importance of an integrated and adaptive approach to the security of critical systems. Through this study, we aim to make a significant contribution to safety practices, offering valuable insights that can be applied to protect embedded systems across various sectors, especially in aviation, where safety is of paramount importance.

1.3 OBJECTIVES

This chapter outlines the central objectives of this thesis, which aims to develop an integrated holistic framework for protecting embedded systems against malicious attacks. The proposed approach seeks to align international and industry standards in a way that creates a robust and adaptive security system. The specific objectives detailed below are designed to guide the research, providing a solid foundation for analysis, development, and evaluation within the context of critical systems security.

1.3.1 Main Objective

The objective of this research is to develop a holistic framework that integrates international and industry-specific standards to enhance the protection of embedded systems against cyber threats. The focus will be on mitigating key attack vectors relevant to embedded environments, particularly malware attacks that compromise system integrity, code injection techniques such as buffer overflow that allow unauthorized execution, firmware exploitation that targets vulnerabilities in system boot and updates, and man-in-the-middle attacks that intercept critical communications.

By addressing these core threats, the framework will provide a structured and adaptable framework, aligning with standards such as ISO/IEC 27001, NIST SP 800-53, and DO-326A. The goal is to strengthen cybersecurity in aviation and other critical sectors, ensuring embedded systems remain resilient and compliant with evolving security challenges.

1.3.2 Specific Objectives

1. Analyze the Impact of Integrating International and Sectoral Standards

   Investigate how the integration of different standards, such as ISO/IEC 27001, NIST SP 800-53, DO-178C, DO-254, DO-326A, DO-355A, and DO-356A, affects the effectiveness of information security management systems to protect against attacks on embedded systems. This objective involves a comparative analysis to identify synergies and possible redundancies or conflicts between these standards.

2. Define and Prioritize Security Controls Across the Lifecycle

   Specify which security controls are most effective for embedded systems and how they should be selected, tailored, and prioritized from requirements through maintenance and end-of-life. This objective emphasizes practical integration into engineering activities, considering real operational constraints such as timing, memory, reliability, and safety. The focus is on feasibility, clear responsibilities, and the production of verifiable evidence that supports audits and continuous oversight.

3. Validate the Framework through Expert Review and Structured Assessment

   The proposed framework will be validated primarily by domain experts using a structured questionnaire and guided reviews. Evaluations will examine clarity, completeness, applicability, feasibility of implementation, and consistency across lifecycle phases. Quantitative scores and qualitative feedback will be analyzed to identify strengths, limitations, and improvement points. Evidence produced

by the method (e.g., records, checklists, decision gates) will be checked for traceability and sufficiency. This process ensures the approach is both robust in theory and workable in real operational contexts.

The objectives outlined in this chapter define the trajectory of this research and are fundamental to addressing the complexities associated with the security of embedded systems. By achieving these objectives, this thesis will not only contribute to the academic body of knowledge in cyber security but will also provide practical guidelines for organizations operating with critical systems, significantly improving their defence capabilities against emerging and persistent cyber threats.

1.4 STRUCTURE OF THE WORK

The dissertation is designed to progressively build and validate a holistic framework that improves the security of embedded systems. After framing the research problem and objectives, Chapter 2 (Theoretical Foundation) reviews key concepts in cybersecurity, describes the characteristics of embedded systems, and discusses the main threats they face in critical sectors. This theoretical background equips the reader with a clear understanding of the context and challenges that justify the research.

Chapter 3 (Research Methods and Procedures) details the methodological framework. It introduces the holistic approach developed in this study, outlines methods for analysing threats and assessing risks, and explains how security measures are integrated throughout the software life cycle.

A rigorous assessment of the proposed methodologies is presented in Chapter 4 (Careful Evaluation of the Proposed Methodologies). In this chapter, the methods developed earlier are applied to practical scenarios, and the data collected are analysed using defined evaluation metrics. This provides a critical reflection on the effectiveness and applicability of the framework.

The same chapter includes Validation of the Framework, which describes how experts evaluated the proposed framework. It reports the criteria for selecting specialists, the procedures for data collection via a structured questionnaire, and the analytical techniques used to interpret the responses. This process highlights the strengths and limitations of the framework and identifies opportunities for improvement.

Chapter 5 (Collected Results) synthesizes the empirical findings, summarizing the quantitative and qualitative results of the evaluations. It highlights the contributions of the holistic framework and discusses potential enhancements. The chapter also addresses the remaining challenges in securing embedded systems against cyber threats.

Finally, the work concludes with Chapter 8 (Conclusions and Future Perspectives), which integrates the main theoretical and practical contributions of the research. It reflects on the broader implications for practice, acknowledges limitations, and outlines a future research agenda. This overall organization guides the reader through a coherent narrative, leading to an informed understanding of the proposed framework and its significance in the field.

2 THEORETICAL FOUNDATION

2.1 CURRENT OVERVIEW

Cybersecurity has become one of the most vital pillars in ensuring the integrity and functionality of technological systems in the modern era. Embedded systems, which consist of hardware components integrated with software, play a crucial role in critical sectors such as automotive, healthcare, and, notably, aviation. As the world becomes increasingly interconnected, these systems face rising threats due to their connectivity and reliance on networked operations. The sophistication of cyberattacks has evolved to exploit specific vulnerabilities in embedded systems, emphasizing the need for enhanced and proactive security strategies (10, 11).

Embedded systems are designed to perform specific tasks with high efficiency. In aviation, where these systems govern navigation, communication, and control, the increasing automation and continuous communication between aircraft and ground systems amplify their vulnerability to cyberattacks. The limited ability to regularly update or patch these systems, especially in distributed environments, exacerbates this risk. In avionics systems, failure to secure components effectively can compromise operations and, more critically, flight safety (12, 13).

The integration of emerging technologies in embedded systems introduces both opportunities and challenges. While these technologies enhance development processes and improve resilience, they also increase complexity, which may inadvertently introduce new vulnerabilities. The cybersecurity approach must therefore focus on embedding security into the system development lifecycle, ensuring that threats are mitigated at the design stage rather than reacting to them during operation (14).

In the aviation sector, the security of avionics systems is paramount due to the potential consequences of a successful cyberattack. The increasing interconnectivity of systems within aircraft requires particular attention to their development processes to ensure vulnerabilities are identified and mitigated early. The shared architecture and common software used across various devices, including avionics, underscore the importance of consistent security measures throughout the lifecycle of these systems. Developing secure systems necessitates a focus on designing resilience into the architecture, implementing robust testing, and adhering to industry-specific standards (15).

The global aviation supply chain adds complexity to cybersecurity efforts. Components and systems are often sourced from a diverse network of suppliers, each with varying levels of cybersecurity maturity. This creates the potential for vulnerabilities to be introduced during development. To mitigate this, organizations must prioritize rigorous vetting of suppliers and adhere to security-focused processes, such as those outlined in standards like DO-178C, DO-254, DO-326A, DO-355A, DO-356A, and ISO/IEC 27001, to ensure the integrity of the final product (16).

Regulation plays a critical role in establishing a baseline for cybersecurity practices in the aviation industry. Civil aviation authorities and organizations such as EASA (European Union Aviation Safety Agency) and FAA (Federal Aviation Administration) have issued guidelines requiring compliance with cy-

bersecurity standards specific to avionics, such DO-326A. However, variations in regulatory requirements across regions—such as Europe, North America, and Asia—pose challenges to developing a cohesive global cybersecurity strategy. Addressing these discrepancies requires coordination among regulators and manufacturers to align practices and ensure consistency in the protection of embedded systems (17).

Addressing insider threats is another critical aspect of cybersecurity. Employees or contractors with access to development environments or critical systems pose significant risks, either through malicious intent or inadvertent errors. Organizations must implement strict access control mechanisms, enforce the principle of least privilege, and foster a culture of cybersecurity awareness through continuous training and development programs. Building a strong security culture is integral to reducing human error and enhancing vigilance within the organization (13).

While no system can be made entirely immune to cyberattacks, effective incident response is essential to minimize the impact of breaches. Developing comprehensive incident response plans and conducting regular simulations are necessary to prepare teams for a variety of attack scenarios. This ensures that organizations can detect, contain, and recover from incidents efficiently. Cybersecurity for embedded systems must be viewed as a dynamic, ongoing process, requiring continuous investment in research, collaboration, and refinement of strategies (14, 18).

The future of cybersecurity in embedded systems will depend on the adoption of integrated and adaptive approaches to security. This includes embedding security measures into the earliest stages of system design, adhering to industry standards, and fostering international collaboration to develop global security frameworks. As systems become increasingly interconnected and threats grow in complexity, such measures are essential to ensuring the resilience of critical systems, particularly in aviation, where safety is paramount (18).

2.2 AVIONICS SYSTEMS

Avionics systems play a crucial role in the safe and efficient operation of modern aircraft. The increasing complexity and interconnectivity of these systems has made the security of embedded software a central concern. Avionics systems encompass all the electronic devices used in aircraft, including communications, navigation, flight control, systems monitoring, and mission management. These systems are essential for ensuring the safe and efficient operation of aircraft, providing critical information and facilitating real-time decision-making. For instance, communication systems such as VHF radios, satellite-based data links, and ADS-B (Automatic Dependent Surveillance-Broadcast) enable the transmission of data between aircraft and ground stations, as well as between different aircraft. These systems are critical for air traffic coordination and ensuring flight safety. Consequently, the reliability and security of avionics communication systems are vital to preventing accidents and incidents in increasingly congested airspace (19, 20).

Navigation is another essential component of avionics systems. Technologies such as the Global Positioning System (GPS) and Inertial Navigation Systems (INS) allow aircraft to determine their position and trajectory with high precision. These systems are integrated with flight control systems to ensure

that the aircraft follows its planned route safely and efficiently. The accuracy and reliability of navigation systems, particularly under adverse conditions, are fundamental to flight safety. For example, Traffic Collision Avoidance Systems (TCAS) rely on precise navigation inputs to alert pilots to potential conflicts, highlighting the importance of highly reliable and secure software for these systems (21).

Flight control systems, which govern the aircraft's movements, rely on sensors, actuators, and onboard computers to monitor and adjust the aircraft's attitude and trajectory in real time. These systems' integration with onboard software ensures rapid and precise responses to dynamic flight conditions. Technologies such as VHF radios and satellite networks are employed to maintain stable and secure communications, essential for flight operations. According to Jackson et al. in their book Software for Dependable Systems: Sufficient Evidence?, the complexity of flight control systems necessitates a high level of integration and coordination to maintain operational safety and efficiency (22).

Embedded software serves as the backbone of avionics systems, controlling and coordinating the operation of various components, from communication systems to flight controls. Not all software failures carry catastrophic consequences; the impact of a software issue depends on its classification under the RTCA DO-178C standard. This standard categorizes software by its potential effect on the aircraft, ranging from no safety impact to catastrophic failure. For instance, software directly involved in flight controls or collision avoidance typically falls under Level A, where failures could result in loss of the aircraft, while software managing less critical functions might be classified at lower levels (23, 24, 25, 26).

The security challenges in embedded avionics systems are numerous and multifaceted. The increasing interconnectivity of systems expands the attack surface, heightening their vulnerability to cyber threats. Moreover, integrating advanced technologies, such as wireless communication and cloud computing, introduces new risks that require careful management. For example, these technologies expose systems to vulnerabilities that malicious actors could exploit. Addressing these challenges necessitates a layered security approach, encompassing physical protection of devices, encryption of communications, and robust access control policies. The ISO/OSI reference model plays a vital role in structuring these measures, ensuring interoperability and clarity in the implementation of security protocols (27).

Ensuring the security of embedded software in avionics systems requires a holistic approach that addresses every phase of the software lifecycle—from development to maintenance. This holistic framework must integrate secure coding practices, comprehensive risk analysis, and adherence to security standards, such as DO-178C and DO-326A. Although the implementation of solutions like intrusion detection systems and risk mitigation strategies will be explored in later chapters, the current focus remains on the theoretical foundation underlying these measures. This ensures a comprehensive understanding of the challenges and sets the stage for practical solutions (28, 26).

Avionics systems represent a critical intersection between advanced technology and operational safety. The complexity and interconnectivity of these systems demand an integrated approach to ensure the resilience of embedded software. Adopting a robust framework based on industry best practices and established frameworks is essential to protect these systems from a broad spectrum of cyber and operational threats (28).

2.2.1 Embedded Software

With the increase in inter-connectivity and the growing complexity of embedded systems, the need to ensure the security of these systems has become even more pressing (29). Existing literature provides a comprehensive overview of the techniques and strategies developed to protect embedded software against a wide range of threats, from physical to cyberattacks. This chapter examines the most relevant studies and emerging trends, emphasizing proposed solutions while identifying gaps that need further exploration. By analyzing the literature, this work seeks to establish a solid foundation for developing a holistic approach to enhance the security of embedded systems against malicious attacks (30). Research has explored techniques such as encryption, access control, and intrusion detection to safeguard embedded systems (31, 32, 33, 29, 34, 35). Beyond isolated measures, holistic approaches are increasingly recognized for integrating multiple layers of defense, addressing both technical and procedural aspects to strengthen resilience.

These approaches encompass the software life cycle, combining secure development practices, continuous monitoring, and incident response mechanisms to mitigate threats effectively (36, 37). By integrating these elements, holistic strategies offer a more comprehensive response to the increasing sophistication of cyber threats. However, despite the advancements, significant gaps remain in the literature. One of the key challenges is the limited focus on holistic and integrated approaches that address the complexities of protecting embedded systems throughout their entire life cycle (36). While many studies emphasize specific security techniques, such as encryption and intrusion detection, few adopt a comprehensive perspective that aligns these methods with broader software engineering and operational processes.

Moreover, the rapid evolution of embedded technologies and the sophistication of cyberattacks demand adaptable and proactive solutions capable of keeping pace with emerging challenges. Addressing these gaps, this research proposes and validates a holistic approach to safeguarding embedded systems against malicious attacks. By integrating diverse security measures and accounting for the unique requirements of these systems, the work aims to advance the current state of embedded software security significantly.

2.2.2 Embedded Security Challenges

Embedded systems are integral to modern avionics, forming the backbone of critical operations such as flight control, navigation, and communications (33). The increasing interconnectivity and complexity of these systems present significant security challenges, particularly in aerospace applications where failures or breaches can have catastrophic consequences. Recent studies have demonstrated vulnerabilities within avionics networks, highlighting potential exploits in embedded systems that could lead to unauthorized access, system disruption, and safety risks (38, 31). These findings emphasize the urgency of addressing the unique security threats that arise within the context of avionics.

In avionics, embedded systems are interconnected through specialized networks, such as the Aircraft Data Network (ADN), which facilitates communication between sensors, actuators, and onboard computers. These networks are critical for real-time data exchange, including flight parameters like altitude, velocity, and environmental conditions. However, their complexity and the integration of legacy components with modern technologies expand the attack surface (39, 40). Attackers can exploit vulnerabilities

at multiple levels, including hardware, firmware, and software layers, to compromise the integrity and functionality of these systems.

For instance, researchers have identified specific vulnerabilities within the operating systems (OS) and kernel layers of avionics systems, such as insufficient isolation between processes and vulnerabilities in context-switching mechanisms (40, 32). These weaknesses could potentially allow attackers to escalate privileges or inject malicious code, undermining the reliability of the system. While OS kernels are designed to handle such challenges, the increasing sophistication of cyberattacks demands enhanced security measures and proactive defenses.

Furthermore, despite advancements in formal verification methods, achieving complete vulnerability-free systems remains an ongoing challenge due to the complexity and scale of modern avionics software (32). To mitigate these risks, robust security frameworks and practices must be implemented, encompassing secure coding, continuous monitoring, and rapid incident response. Emphasis should also be placed on securing the software supply chain to prevent the introduction of malicious code during development or updates (33).

Safeguarding embedded systems in avionics is essential not only to protect critical operations but also to ensure the safety of passengers and crew. As these systems continue to evolve, adopting a holistic approach that addresses vulnerabilities across all layers—from hardware to application—will be crucial in maintaining the integrity and resilience of avionics technologies (33, 41, 29).

2.2.3 Current Avionics Development Process

The development of avionics follows a rigorous process based on international standards that establish guidelines for the certification of embedded software and hardware in aircraft. Critical systems require formal development approaches to minimize failures and ensure operational safety, as emphasized by studies on system safety and reliability. Compliance with standards such as DO-178C for software and DO-254 for hardware is essential for obtaining certification from regulatory bodies such as the Federal Aviation Administration (FAA) and the European Union Aviation Safety Agency (EASA) (26, 42, 43).

The process begins with the planning phase, where development objectives, Design Assurance Levels (DAL), and verification methods are established. A structured planning process is crucial in reducing risks and improving requirements traceability throughout the software lifecycle, ensuring that all regulatory criteria are met from the outset. This early structuring of the project allows developers to maintain control over design changes while ensuring compliance with certification standards (44).

During the development phase, high-level requirements are refined and transformed into detailed specifications that guide system architecture and code implementation. Maintaining traceability between requirements, design, and code is fundamental to ensuring that all essential functions are correctly implemented while avoiding unnecessary code that could compromise security. A well-defined traceability matrix helps ensure that all safety-critical functions are accounted for and thoroughly tested (45).

Verification and validation (V&V) represent one of the most critical stages in avionics development. The certification of embedded software requires rigorous testing, including structural coverage analysis and

requirement-based test execution. Techniques such as Modified Condition/Decision Coverage (MC/DC) are widely used to ensure the logical robustness of the code, as required by regulators. By applying strict verification techniques, potential failures can be identified early in the development cycle, reducing the risk of costly corrections at later stages (46).

Formal methods and Model-Based Development (MBD) are also applied to improve software reliability. The use of formal modeling has been shown to detect errors early in the development process, reducing certification costs and time. The application of formal verification techniques allows for mathematically proving the correctness of software, an approach that has gained traction in safety-critical systems. The DO-331, a supplement to DO-178C, regulates the adoption of these techniques and their applicability in aerospace projects (47, 48).

Cybersecurity has become a fundamental aspect of modern avionics development. The increasing digitization of aircraft raises exposure to cyber threats, requiring the adoption of complementary standards such as DO-326A and DO-355A, which address data protection and the continuity of security measures. These standards help mitigate critical vulnerabilities that could compromise operational safety, ensuring that security is embedded throughout the system lifecycle rather than as an afterthought (49, 50).

In addition to software, the development of embedded hardware follows stringent requirements to ensure reliability and performance. The integration of software and hardware standards ensures that both components operate cohesively and securely. The use of DO-254 for critical electronic circuits allows the validation of Field-Programmable Gate Arrays (FPGA), Application-Specific Integrated Circuits (ASIC), and other essential devices for aircraft operation. Ensuring consistency between software and hardware certification processes is key to maintaining a high level of safety and compliance with regulatory requirements (51).

The software lifecycle in avionics requires an iterative process of continuous improvement. Periodic reviews and audits are necessary to ensure that systems maintain high safety and performance standards, meeting certification requirements and adapting to new technologies. This includes the revalidation of systems in response to software updates or changes in regulatory requirements. By maintaining a cycle of iterative updates, developers can ensure that avionics systems remain secure and operationally effective (52).

Documentation is another crucial factor for successful certification. Certification standards require detailed records of all phases of the software and hardware lifecycle, ensuring traceability and verifiability of requirements, which are fundamental for obtaining final certification. Proper documentation allows regulators and developers to track design decisions, making it easier to verify compliance with industry standards. This process ensures that embedded systems can be reviewed and validated even years after their implementation (53).

In summary, avionics development combines technical rigor, meticulous validation, and compliance with international standards to ensure that embedded systems meet the highest safety and reliability standards. The integration of software and hardware, the use of formal methodologies, and the implementation of cybersecurity measures ensure that these systems can operate efficiently and securely throughout their lifecycle. By maintaining strict adherence to regulatory frameworks and best practices, the aviation industry can continue to advance avionics technologies while ensuring safety and compliance (2, 43).

3 RESEARCH METHODS AND PROCEDURES

The proposed method for developing a holistic security approach for embedded software is grounded in a broad and structured analysis of threats, the identification of attack vectors, and the definition of criteria for countermeasure prioritization. The aim, therefore, is to promote the incorporation of protection mechanisms across all phases of the development life cycle, from initial conception through continuous maintenance—in order to ensure a robust, integrated, and adaptable defense against a diverse spectrum of cyber threats. This approach seeks not only to mitigate known vulnerabilities but also to strengthen system resilience in the face of emerging and complex attacks.

The methodological execution of the study comprised a set of structured stages, described below. Each phase was conducted to ensure coherence among theoretical foundations, applicable normative requirements, and the practical feasibility of application in the context of safety-critical embedded systems.

1. A literature review was conducted to identify references on the use, applicability, functionalities, and behavior of methods and tools for protecting embedded software against malicious attacks.

2. The collected material and acquired knowledge were used to develop a reference model, termed the Comprehensive Holistic framework, aimed at creating security applications for embedded software, integrating normative principles, secure engineering practices, and protection mechanisms throughout the entire life cycle.

3. Building on the collected material and consolidated technical knowledge, the Integrated Holistic framework for aeronautical embedded systems was developed, grounded in sector-specific standards—DO-178C, DO-254, DO-326A, DO-355A, and DO-356A—ensuring integration between functional safety and cybersecurity from development and certification through operation and continuous maintenance.

4. The process was modeled for aeronautical sectors in BPMN to enable application within the specific organizational context, ensuring consistency with operational workflows, traceability of activities, and standardization of procedures in accordance with process-management best practices.

5. An evaluation metric for the proposed holistic methodologies was devised and compared, defining criteria, weights, and the calculation procedure, in order to provide a consistent practical basis for comparative analysis and validation of results.

6. The Integrated Holistic framework was validated by means of a structured assessment instrument administered to experts in embedded-systems security, verifying its consistency, applicability, and comprehensiveness with respect to normative and operational requirements.

The empirical validation focuses almost exclusively on the Integrated Holistic Framework. This is a methodological decision anchored in the collaboration with Airbus Defence and Space specialists and the research context of safety and security critical avionics systems. While the Comprehensive Holistic

Framework serves as the generalizable conceptual foundation of this work, the integrated framework is the one that operationalizes such foundation under avionics-specific norms and certification constraints.

In particular, it explicitly aligns with DO-178C (software) and DO-326A (airworthiness security), among related companion documents, thereby offering direct relevance and evaluability for practitioners in the target domain. Accordingly, concentrating the empirical validation on the integrated framework maximizes ecological validity and practical insight without diminishing the conceptual contribution of the comprehensive baseline.

3.1 LITERATURE REVIEW

The Literature Review was conducted with the aim of mapping the state of the art in embedded software security, identifying gaps, and consolidating evidence to support the methodological proposal of this work. Specifically, it sought to answer the following research questions:

- *(Q1)* what are the main attack vectors and classes of threats that affect embedded software;
- *(Q2)* which mechanisms, controls, and practices have been reported as effective for prevention, detection, response, and recovery;
- *(Q3)* in what ways do existing approaches integrate security requirements and activities into the development, operation, and maintenance life cycle of embedded software.

A predefined protocol was adopted to ensure rigor, transparency, and reproducibility:

- **Information sources:** indexed databases (e.g., IEEE Xplore, ACM Digital Library, Scopus, Web of Science) and technical documents from recognized bodies (e.g., ISO/IEC, NIST, RTCA/DO).
- **Search strategy:** Boolean strings combining terms and synonyms related to embedded software/-firmware/RTOS, cybersecurity/secure development lifecycle, threat modeling/attack vectors, and controls/countermeasures/assurance.
- **Time frame and language:** prioritization of the last 10 years, without automatic exclusion of seminal references; English and Portuguese.
- **Inclusion criteria:** peer-reviewed studies or normative technical documents with scope on embedded software; explicit description of threats/vectors and/or mechanisms/controls; evidence of integration into the life cycle.
- **Exclusion criteria:** opinion pieces without empirical basis, duplicates, exclusively non-embedded scope, absence of minimum information for extraction.
- **Screening and extraction:** dual screening by title/abstract and full-text reading; standardized data extraction (domain, target, Threat→Vector→Control, life-cycle phase, metrics/results).

- **Quality appraisal:** checklist of internal/external validity and level of evidence; resolution of disagreements by consensus.
- **Synthesis:** thematic synthesis and mapping *Threat→Vector→Control→Evidence*, with descriptive statistics where applicable; traceability repository provided in an appendix.

For the development of the comprehensive framework, a corpus of 13 highly relevant references was consolidated (Table 3.1). Accordingly, this establishes a robust foundation for practices that are simultaneously comprehensive and integrated, aligned with the holistic approach adopted in this work, with balanced coverage of prevention, detection, response, and recovery functions.

Table 3.1: Highly Relevant References

Reference
STALLINGS, William; BROWN, Lawrie. *Computer Security Principles and Practice, Global Edition*. Pearson Deutschland, 2018. 986 p. ISBN 9781292220611. Available at: <https://elibrary.pearson.de/book/99.150005/9781292220635>.
SHOSTACK, Adam. *Threat Modeling: Designing for Security*. John Wiley & Sons, 2014.
ANDERSON, Ross; MOORE, Tyler. The economics of information security. *Science*, v. 314, n. 5799, p. 610–613, 2006. American Association for the Advancement of Science.
HOUMB, Siv Hilde; FRANQUEIRA, Virginia N. L.; ENGUM, Erlend A. Quantifying security risk level from CVSS estimates of frequency and impact. *Journal of Systems and Software*, v. 83, n. 9, p. 1622–1634, 2010. Elsevier.
ERICSON, C.A. *Fault Tree Analysis Primer*. CreateSpace Incorporated, 2011. ISBN 9781466446106. Available at: <https://books.google.de/books?id=jQtcmgEACAAJ>.
OR-MEIR, Ori et al. Dynamic malware analysis in the modern era—A state of the art survey. *ACM Computing Surveys (CSUR)*, v. 52, n. 5, p. 1–48, 2019. ACM New York, NY, USA.
OZKAYA, Erdal. *Incident Response in the Age of Cloud: Techniques and best practices to effectively respond to cybersecurity incidents*. Packt Publishing Ltd, 2021.
KNAPP, Eric D. *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*. Elsevier, 2024.
SALTZER, J.H.; SCHROEDER, M.D. The protection of information in computer systems. *Proceedings of the IEEE*, v. 63, n. 9, p. 1278–1300, 1975. DOI: 10.1109/PROC.1975.9939.
POLYSPACE. *Static Analysis and Verification Tools for Avionics Software*. 2024. Available at: <https://www.mathworks.com>.
HOWARD, Michael; LIPNER, Steve. *The Security Development Lifecycle*. Datenschutz Und Datensicherheit – Dud, v. 34, 2006. ISBN 0735622140. DOI: 10.1007/s11623-010-0021-7.
IDRIS, Muhammad; SYARIF, Iwan; WINARNO, Idris. Development of vulnerable web application based on OWASP API security risks. *2021 International Electronics Symposium (IES)*, p. 190–194, 2021. IEEE.
CHATTERJEE, Dave. *Cybersecurity Readiness: A Holistic and High-Performance Approach*. SAGE Publications, 2021.

Source: Prepared by the author.

3.2 A COMPREHENSIVE APPROACH

The decision to embrace a holistic framework for embedded software security arises from the escalating need for comprehensive protection in an increasingly interconnected and vulnerable digital landscape. The intricacy of modern embedded systems necessitates approaches that address all facets of the software lifecycle, from initial design to continuous maintenance. A holistic approach offers an integrated perspective on threats and countermeasures, ensuring that no development phase is overlooked in terms of security (54).

Adopting a holistic framework reflects the understanding that embedded systems security cannot be addressed in a piecemeal fashion. The multifaceted nature of contemporary cyber threats demands a synergistic integration of security practices. Security implementation should be viewed as an ongoing and dynamic process, involving collaboration across multiple disciplines, including software engineering, hardware design, systems architecture, and cybersecurity. In avionics, these disciplines align with standards such as DO-178C (software assurance), DO-254 (hardware design assurance), and ARP4754A (system-level design and integration), ensuring a unified and robust approach (26, 42, 55). This approach ensures that potential vulnerabilities are identified and mitigated proactively and in a coordinated manner (56).

Moreover, a holistic approach facilitates continual adaptation to emerging threats. In the context of embedded systems, where technological innovation varies by industry, the ability to swiftly respond to changes is crucial. Although technology in avionics progresses at a slower pace due to rigorous safety and certification requirements, the adoption of secure coding practices, lightweight intrusion detection systems (IDS), and regular security audits ensures that systems remain resilient against evolving threats while complying with strict standards like DO-326A (57, 49, 50, 58).

The choice of a holistic framework is also grounded in the need for strategic alignment between security and operational performance. In embedded systems operating in critical environments, such as avionics or industrial automation, security failures can have severe consequences. For instance, a failure in an avionics system can compromise flight safety, while in industrial settings, it can disrupt essential services. A holistic approach allows for careful integration of security measures without compromising system performance. By leveraging tools like model-based design (e.g., Simulink) and hardware redundancy, security and operational efficiency can coexist effectively (59, 60, 61).

The holistic framework was chosen for its capacity to foster a culture of security within organizations. By embedding security throughout all stages of development and maintenance, continuous awareness of the importance of secure practices is cultivated among developers, administrators, and end-users. This culture of security is critical in the context of aviation, where compliance with airworthiness regulations, such as those outlined in DO-326A, necessitates constant vigilance and adherence to secure practices. Therefore, integrating a holistic approach not only fortifies technical security but also reinforces an organizational commitment to resilience against cyber threats (62, 49, 63).

3.2.1 Asset Identification

This is a fundamental step in information security risk, particularly in embedded software systems due to their critical role in safety and real-time operations. This phase involves cataloging all assets that need protection, including hardware, software, data, and other critical components of the system. Proper identification of assets is essential to understand the value of information and the impact of potential threats. According to Stoneburner et al. (2002), "asset identification is a cornerstone of risk assessment, as it lays the foundation for all subsequent security measures." This phase allows organizations to determine which components are the most critical to their operations and prioritize their protection efforts accordingly (64).

In embedded systems, assets can be divided into several categories, each with specific protection needs. Firstly, hardware assets encompass physical components, such as microcontrollers, sensors, actuators, and communication interfaces. Pecht (2008) emphasizes that "the failure of hardware components can have cascading effects, significantly disrupting the overall operation of embedded systems" (65).

In addition to hardware, software assets are central to embedded system functionality. These include the embedded code, firmware, libraries, and development tools used to create and maintain the system. Software security begins with the implementation of secure coding practices, supported by guidelines such as OWASP, CERT Secure Coding Standards, and the MISRA guidelines. Developers must proactively follow these practices to minimize vulnerabilities and ensure secure operation (66).

Data represents another critical category of assets in embedded systems. This includes configuration settings, operation logs, sensor data, and other sensitive information stored or processed by the system. Ensuring data integrity and confidentiality is key to maintaining system reliability. To achieve this, asset identification must account for potential weaknesses, leveraging databases such as CWE (Common Weakness Enumeration), CVE (Common Vulnerabilities and Exposures), and CAPEC (Common Attack Pattern Enumeration and Classification) to establish a comprehensive understanding of data vulnerabilities and threats (67).

The network infrastructure, which enables communication between system components, is also a significant asset. Although essential for real-time operation and system integration, network connectivity introduces potential attack vectors. While intrusion detection and response are important for protecting network infrastructure, these measures are more relevant to the threat detection phase than to asset identification. The focus here remains on cataloging the network assets that are crucial to system operation and their interdependencies (68).

Asset identification in embedded software systems involves an exhaustive analysis of physical components, software, data, and supporting infrastructure. This process is methodically carried out by mapping the relationships and dependencies between these assets, identifying potential vulnerabilities, and documenting their criticality to overall system security. An effective framework for this process must incorporate precise definitions of weaknesses (internal flaws) and vulnerabilities (exploitable conditions) using standardized references such as CWE and CVE. This structured approach is essential for developing a robust holistic security strategy to defend against modern cyber threats (64, 66, 67, 68).

3.2.2 Identification of Threats and Vulnerabilities

Following asset identification, the next step is to identify the associated threats and vulnerabilities. This step is critical in information security risk assessment, especially for embedded software systems, as they often operate in environments with limited security resources and increased exposure to physical and cyber threats. This process involves a detailed analysis of potential attack vectors and the intrinsic system weaknesses and vulnerabilities that could be exploited by malicious actors. Accurate identification and categorization of these elements are fundamental to developing effective mitigation strategies.(19).

A clear distinction between weaknesses and vulnerabilities is essential for this process. According to the Common Weakness Enumeration (CWE), weaknesses refer to flaws in system design, development, or configuration that could potentially lead to vulnerabilities. On the other hand, the Common Vulnerabilities and Exposures (CVE) defines vulnerabilities as specific, exploitable weaknesses that can be directly used to compromise a system. Understanding this distinction ensures a more precise risk assessment approach and enables organizations to address both underlying issues and immediate threats (69, 70).

Precise identification of weaknesses, threats, and vulnerabilities allows organizations to better understand the risks their systems face and devise tailored protective measures. Threat modeling is a proactive process that involves identifying, understanding, and mitigating risks before they can be exploited. This framework offers a structured approach for analyzing potential threats and aligning security strategies with system priorities (19).

Threat identification typically involves employing various techniques to map potential sources of risk. One common approach is the use of attack diagrams, which visually represent how an attacker might exploit the system. These diagrams, combined with hypothetical attack scenarios, depict the paths an attacker could follow to exploit identified vulnerabilities, highlighting critical entry points and dependencies in the system architecture. An example of an attack diagram is shown in figure 3.1, which outlines the stages of exploitation from reconnaissance to privilege escalation (71, 72, 73).

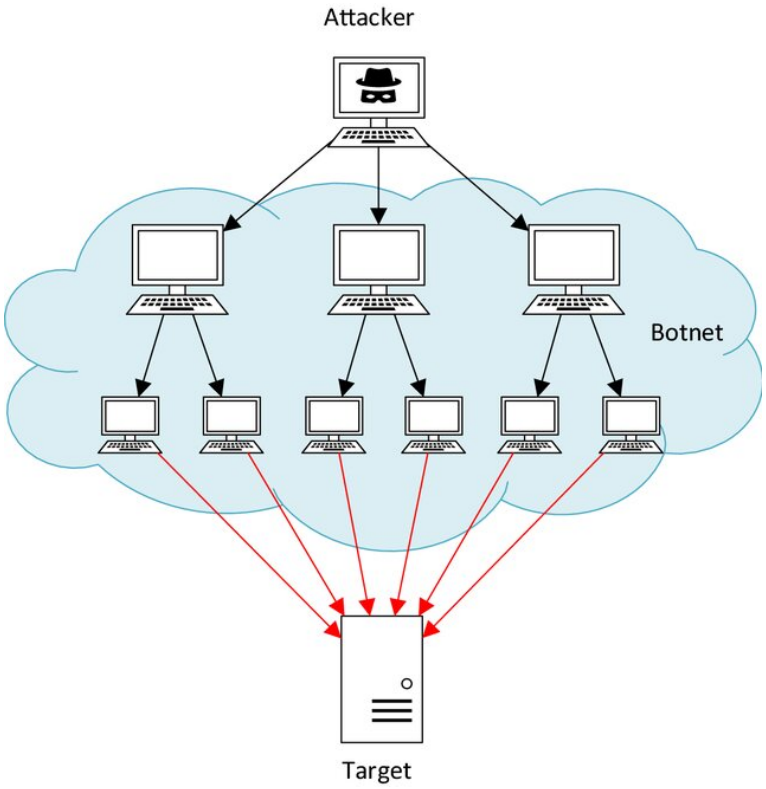

Figure 3.1: A diagram of a DDoS attack performed with a botnet

Threat modeling expands on these diagrams by integrating broader threat scenarios into a cohesive framework. This approach examines adversaries' motivations, technical capabilities, and potential attack paths. Tools and structured methods provide effective means to analyze and prioritize these threats (19).

Penetration testing, is another critical component in identifying vulnerabilities. These tests simulate real-world attacks on the system, uncovering security flaws that might not be apparent through static analysis alone. Penetration testing provides actionable insights into a system's robustness against specific attack vectors and validates the effectiveness of implemented countermeasures (74).

To complement penetration testing, static and dynamic code analysis tools are employed. Static analysis tools, such as SonarQube and Coverity, examine source code for patterns that could lead to security issues without requiring code execution. Dynamic analysis tools evaluate software during runtime, identifying vulnerabilities that manifest under specific conditions. By combining these techniques, organizations can uncover both design-level and operational vulnerabilities, ensuring comprehensive system evaluation (75, 76).

Consulting vulnerability databases such as CVE and CWE is another essential step. These databases provide up-to-date information on known vulnerabilities, their associated risks, and recommended mitigation measures. Regularly consulting such resources allows organizations to stay informed about emerging threats and maintain an adaptive security posture (69, 70).

In summary, identifying threats and vulnerabilities is a multifaceted process that involves leveraging various techniques and tools, such as threat modeling, penetration testing, static and dynamic code analysis, and vulnerability database consultation. By adopting a structured and comprehensive approach, organiza-

tions can gain a deep understanding of the security challenges they face and develop targeted strategies to safeguard their embedded systems effectively.

3.2.3 Threat Analysis and Modeling

This initial phase is deemed critical within the holistic framework for the protection of critical embedded systems, such as those used in aviation. Establishing a solid foundation of security is vital, allowing for the identification and understanding of potential threats that the system may encounter. The effectiveness of implemented defenses directly depends on the thoroughness and breadth of this preliminary analysis.

The process begins with the collection of threat intelligence, involving the acquisition of historical and current data related to cyberattacks, as well as the analysis of emerging trends that may impact embedded systems. This step ensures the analysis is informed by actual and pertinent data. Sources such as known vulnerability databases like CVE (Common Vulnerabilities and Exposures), previous incident reports, and threat intelligence feeds are crucial for this data collection. Stallings and Brown (2020) emphasize that keeping threat intelligence up-to-date is essential for addressing an ever-evolving threat landscape (2).

With the gathered intelligence, the subsequent step is threat modeling, which visualizes how various threats could interact with the system. Threat modeling enables security teams to systematically map potential vulnerabilities and risks. Tools such as Microsoft Threat Modeling Tool and open-source platforms provide frameworks to organize and analyze threats. To integrate these techniques, organizations often adopt workflows that combine modeling with established standards. For instance, modeling outputs can feed directly into risk management systems, ensuring alignment between identified threats and mitigation strategies (19).

Fault Tree Analysis (FTA) and Attack Diagrams are particularly useful in visualizing potential attack paths and failure combinations. Figure 3.2 illustrates an example of FTA. FTA organizes failures hierarchically, using logical operators ("AND" and "OR") to determine how various factors contribute to critical events. Anderson and Moore (2018) note that integrating FTA with Failure Modes and Effects Analysis (FMEA) offers a comprehensive view of system vulnerabilities by examining both potential failures and their cascading effects (56, 59, 77, 63).

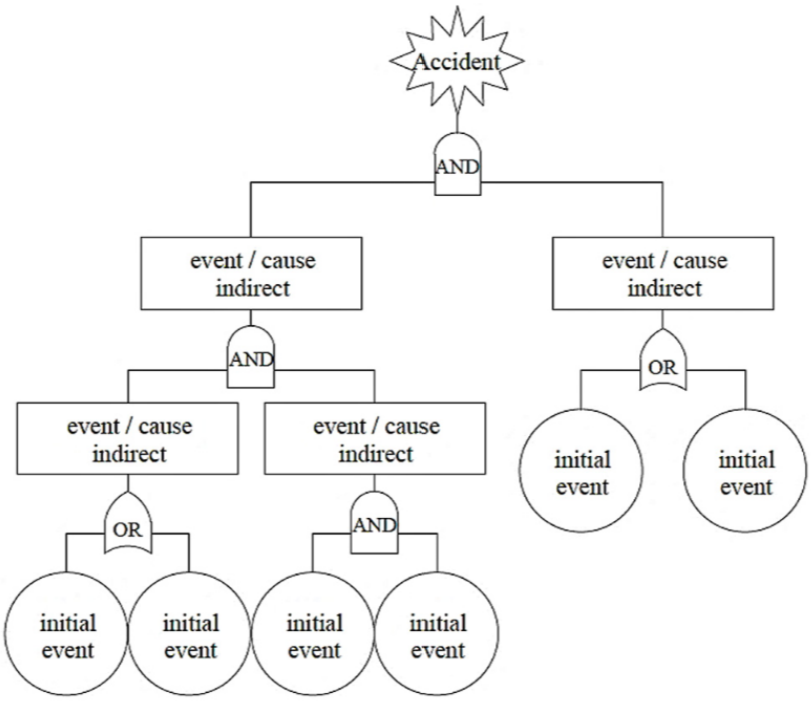

Figure 3.2: Fault Tree Diagram

Following threat modeling, it is necessary to assess the impact of identified threats. This involves evaluating the likelihood of each threat against its potential impact on the system. For example, in avionics, threats to navigation systems may have a higher criticality compared to threats affecting less safety-critical components. Prioritizing resources and efforts to mitigate the most significant threats ensures efficient application of defenses (59).

The classification and prioritization of threats are essential for organizing mitigation actions. Frameworks like STRIDE are widely used for categorizing threats. For instance, STRIDE identifies risks related to spoofing, tampering, repudiation, information disclosure, denial of service, and privilege escalation. Each category guides the development of targeted countermeasures, such as strong authentication mechanisms for spoofing or robust logging systems for repudiation. Figure 3.3 demonstrates how STRIDE categorizes threats, helping teams align mitigation strategies to specific vulnerabilities (78).

	Threat	Property Violated	Threat Definition
S	Spoofing	Authentication	Pretending to be something or someone other than yourself.
T	Tampering	Integrity	Modifying something on disk, network, memory, or elsewhere.
R	Repudiation	Non-Repudiation	Claiming that you didn't do something or we're not responsible. Can be honest or false.
I	Information Disclosure	Confidentiality	Providing information to someone not authorized to access it.
D	Denial of Service	Availability	Exhausting resources needed to provide service.
E	Elevation of Privilege	Authorization	Allowing someone to do something they are not authorized to do

Figure 3.3: STRIDE Frameworks

STRIDE's adaptability allows for its integration with methodologies like FTA and risk analysis to provide a comprehensive assessment of system security. For example, combining STRIDE with avionics risk management processes provides a structured way to address system-level vulnerabilities. This synergy between methodologies ensures a consistent approach to security across the system lifecycle (55).

Finally, the iterative nature of threat modeling and analysis demands regular revision and adjustments. As new threats emerge, the threat modeling process must evolve to ensure defenses remain effective. For instance, updates to threat models may require revalidation of certain software components or the integration of additional testing during the development cycle. This impacts the development process by necessitating continuous testing and iteration, which can lengthen development timelines but ultimately improves security resilience (63).

In summary, when conducted comprehensively and continually, threat analysis and modeling provide a solid foundation for constructing a robust and resilient security system for embedded systems. These processes ensure that vulnerabilities are identified early and mitigated effectively, fostering systems that are prepared for an ever-changing security landscape.

3.2.4 Risk Assessment Method

Embedded software security is a crucial component in the development of critical systems. Risk assessment constitutes an essential element in implementing a holistic security approach, as it enables the identification, analysis, and management of potential risks that could compromise the integrity and reliability of embedded systems. The ISO/IEC 27005 standard provides a consolidated framework for information security risk management and can be tailored to embedded environments (79).

Information security risk management involves a continuous process: identification of assets, determination of threats and vulnerabilities, assessment of potential consequences, and implementation of mitigation measures to reduce risks to an acceptable level (80, 81). The most recent update of ISO/IEC 27005 (2022) outlines a systematic approach to threat assessment and risk management for critical systems. As shown in Figure 3.4, the process begins with establishing context and assets, followed by threat and vulnerability analysis, risk evaluation, and implementation of controls. This structured framework ensures that

risks are addressed in a consistent way, preserving both operational safety and security (82, 83).

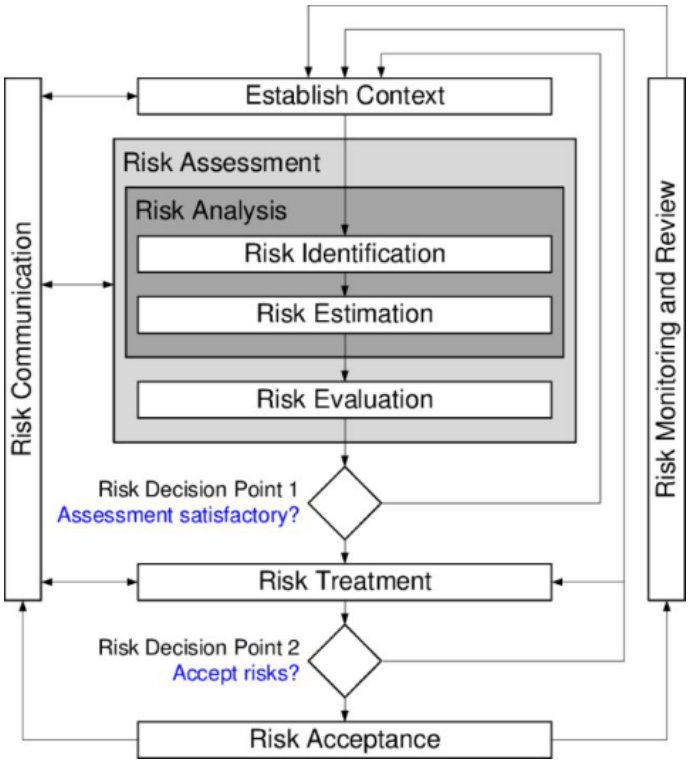

Figure 3.4: Risk management process (adapted from ISO/IEC 27005)

3.2.4.1 Procedural Workflow

The following workflow, grounded in the principles of ISO/IEC 27005, offers a systematic approach to risk assessment, adapted to the specific requirements of embedded systems (79, 80). Each step builds upon the previous one, forming a continuous cycle that ensures risks are identified, evaluated, and treated in a consistent and traceable manner:

Step 1: **Establish Context and Scope**: define boundaries, stakeholders, and criteria for risk acceptance.

Step 2: **Asset Identification**: inventory hardware, software, communication interfaces, and information assets.

Step 3: **Threat Identification**: identify potential threats (e.g., injection, spoofing, denial of service) using threat intelligence and literature (81).

Step 4: **Existing Controls Review**: record implemented controls and evaluate their effectiveness.

Step 5: **Vulnerability Identification**: link threats to specific weaknesses.

Step 6: **Impact Estimation**: assess consequences for confidentiality, integrity, availability, and reliability (82).

Step 7: **Likelihood Estimation**: estimate probability of occurrence using historical data, expert judgment, or probabilistic models (84).

Step 8: Risk Calculation and Evaluation: compute $RiskScore = Likelihood \times Impact$, classify risks, and decide acceptance.

Step 9: Risk Treatment Selection: apply strategies of mitigation, transfer, avoidance, or acceptance (85).

Step 10: Documentation and Monitoring: maintain a risk register, define review cycles, and track residual risks (86, 87).

This structured sequence provides not only methodological rigor but also practical value, as it ensures full traceability from the definition of context to the continuous monitoring of residual risks. By linking technical assessments to clear documentation and review processes, it supports evidence-based prioritization, resource allocation, and alignment with organizational objectives (80, 88).

3.2.4.2 Scales and Criteria

The evaluation of probability and impact requires structured scales to reduce subjectivity and support prioritization (80). Tables 3.2 and 3.3 show an example of scales.

Table 3.2: Likelihood scale

Score	Qualitative	Description
1	Rare	Very unlikely to occur
2	Unlikely	Low motivation or limited exposure
3	Possible	Plausible, already observed in similar contexts
4	Likely	Common vector, attacker capabilities available
5	Almost certain	Exploitation trivial or automated

Source: Prepared by the author.

Table 3.3: Impact scale

Score	Qualitative	Examples
1	Negligible	No operational effect; no regulatory impact
2	Minor	Limited degradation; small rework
3	Moderate	Partial disruption; manageable nonconformity
4	Major	Relevant functional loss; mission interruption
5	Catastrophic	Total compromise of system reliability

Source: Prepared by the author.

The final risk value is obtained by multiplying likelihood and impact:

$$\text{RiskScore} = \text{Likelihood} \times \text{Impact}$$

Table 3.4: Risk classification bands

Range	Class	Decision rule
1–4	Low	Accept/monitor
5–9	Medium	Mitigate if cost reasonable
10–14	High	Mitigation mandatory
15–25	Critical	Immediate action required

Source: Prepared by the author.

3.2.4.3 Worked Example: FTA and FMEA

Structured methods complement ISO/IEC 27005 to detail the origin of risks. Fault Tree Analysis (FTA) is a deductive, top-down method focusing on an undesired event and identifying its root causes. Failure Modes and Effects Analysis (FMEA) is inductive, bottom-up, starting from possible component failures and mapping their impact. Table 3.5 shows a simplified view (81, 82).

FTA (top-down). Example: undesired event "loss of communication integrity". Causes:

- malicious packet injection,
- firmware authentication failure,
- hardware transceiver fault.

FMEA (bottom-up).

Table 3.5: Excerpt of FMEA for communication module

Item/Function	Failure Mode	Cause	S	O	D	Current Controls
Update module	Unverified firmware	Weak signature verification	5	3	3	Code signing, secure boot
Comm interface	Message injection	Lack of message authentication	4	4	3	Segmentation, IDS

Source: Prepared by the author.

The Risk Priority Number (RPN) = $S \times O \times D$ supports prioritization. High RPN values require immediate mitigation.

3.2.4.4 Risk Register and Monitoring

Risk information must be consolidated in a structured register, which functions as a central repository for all identified threats, vulnerabilities, and corresponding treatment plans. This register ensures traceability across the entire risk management cycle, supports accountability by assigning clear ownership, and provides a historical record that facilitates audits and continuous improvement (85, 86). In addition, it

serves as a decision-making tool for managers, enabling the prioritization of mitigation actions, allocation of resources, and monitoring of residual risks over time. Table 3.6 provides an illustrative excerpt.

Table 3.6: Excerpt of risk register

Risk ID	Scenario	L	I	Class	Treatment	Owner	Due
R-01	Unverified firmware update	3	5	High	Mitigate (code signing)	SW team	Q1
R-02	Message injection in comm bus	4	4	High	Mitigate (auth + IDS)	Comm team	Sprint 5

Source: Prepared by the author.

3.2.4.5 Risk Evaluation and Acceptance Criteria

A risk is deemed acceptable when it falls into the Low category or, in specific cases, into the Medium category provided there is a documented cost-benefit justification and a defined monitoring plan. High and Critical risks, on the other hand, cannot be tolerated without the implementation of effective mitigation measures and explicit approval from management (87).

Establishing clear acceptance criteria ensures consistency in decision-making, aligns risk tolerance with organizational objectives, and prevents arbitrary judgments. Furthermore, all acceptance decisions must be properly documented, including the responsible owner, residual risk level, and review deadlines, guaranteeing accountability and enabling periodic reassessment throughout the system lifecycle.

3.2.4.6 Link to Resource Allocation

The quantitative assessment provides a rational basis for decisions concerning budget allocation and the distribution of development effort. One possible approach is to assign resources proportionally to the relative weight of each risk, as expressed by its score:

$$\text{Share}_i = \frac{\text{RiskScore}_i}{\sum_{j \in \text{Backlog}} \text{RiskScore}_j}$$

This formulation guarantees that higher-scoring risks receive a larger share of attention and resources. In parallel, the cost of each mitigation measure must be balanced against the expected loss to avoid disproportionate investments:

$$\text{Cost}_{mitigation} \leq \alpha \times \text{Expected Loss}$$

where α represents the acceptable investment ratio defined by the organization's risk policy (typically between 0.3 and 0.5). This cost–benefit relationship ensures that mitigation strategies remain economically viable while directing priority to the most critical risks, thereby aligning security actions with organizational objectives and operational constraints (88, 89, 90).

3.2.4.7 Continuous Review

Risk analysis should not be regarded as a static activity, since new vulnerabilities and evolving threat scenarios continually reshape the risk landscape. To remain effective, risk assessments must be revisited at regular intervals and systematically integrated into the development lifecycle. This integration allows early detection of emerging issues, timely adaptation of security controls, and validation of the effectiveness of previously implemented measures. Moreover, continuous monitoring ensures that residual risks are progressively reduced and that the organization maintains alignment with its security objectives and risk tolerance over time. In this way, risk management becomes a dynamic and iterative process, strengthening resilience against future challenges (86, 91).

3.2.5 Attack Vector Analysis

This section maps each attack vector to its primary defense objective(s) the rationale (why) and the protection goal (what) without prescribing implementation details. *Para a implementação detalhada das contramedidas correspondentes, ver Seção 3.2.7.*

- **Input tampering and injection** → Defense objective: preserve input/data integrity and prevent unintended code execution and malformed payloads (92, 93).
- **Service exhaustion (DoS)** → Defense objective: ensure availability through resource isolation, graceful degradation and back-pressure (94, 95, 96).
- **Unauthorized access / privilege escalation** → Defense objective: enforce strong authentication/authorization and least privilege; reduce attack surface of privileged paths (60).
- **Network interception and manipulation** (eavesdropping/MitM) → Defense objective: maintain confidentiality and authenticity of data-in-transit; detect manipulation attempts (92, 93).
- **Physical tampering** → Defense objective: protect devices and exposed interfaces; deter and detect physical compromise to limit impact (97, 98).

Practical realizations of these objectives are centralized in Section 3.2.8.8, and summarized controls are provided in Table 3.7.

3.2.6 Secure Design

This stage, marked by meticulous planning and the implementation of robust defense strategies, is essential for the creation of a resilient and reliable system. A cornerstone of secure design is the Defense in Depth strategy, a multifaceted approach that employs multiple layers of security across the entire system. This framework ensures that even if one layer of security is compromised, additional layers remain active to protect against intrusions. In the context of avionics, these layers include robust firewalls for segregating network domains, advanced encryption systems, and multifactor authentication mechanisms integrated

with cockpit access systems and maintenance interfaces. Each layer is tailored to mitigate specific risks, creating a computing environment that is exceptionally challenging to penetrate (99).

In parallel with Defense in Depth, the Principle of Least Privilege plays a crucial role in minimizing attack opportunities. As articulated by Saltzer and Schroeder in their seminal paper "The Protection of Information in Computer Systems" (1975), this principle mandates that each user or process should only be granted the access necessary to perform their tasks (100).

Furthermore, Secure Development is key to preventing vulnerabilities from the outset of the development process. Practices such as rigorous input validation, as outlined by the OWASP guidelines, data flow control, and careful memory management are critical for creating attack-resistant code. Static and dynamic code analysis tools, such as Polyspace, are commonly employed to detect and rectify security flaws before deployment (101, 102).

OWASP is a non-profit foundation working to improve software security. With a global community of security professionals, developers, and other stakeholders, OWASP offers tools, documents, forums, and conferences to help organizations identify and mitigate security risks in web applications. One of OWASP's main contributions is the Top 10 Figure 3.5, a list of the most critical security risks for web applications. In avionics, insecure design—one of the OWASP Top 10 risks—can translate into flaws in system architecture or inadequate threat modeling during the development of flight-critical systems. For example, failing to account for secure communication protocols or neglecting redundancy in system design could compromise both safety and security (102).

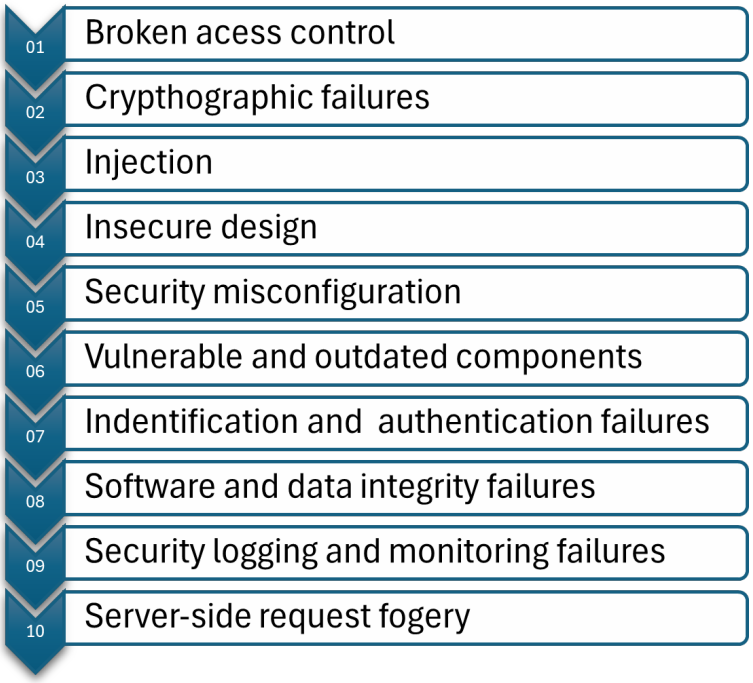

Figure 3.5: Open Web Application Security Project (OWASP)

Transitioning to these security practices involves not just a technical shift but also a cultural change within development organizations. In avionics, promoting ongoing cybersecurity awareness and training for developers and engineers is crucial, ensuring they are familiar with secure coding techniques. This

fosters a security-first mindset that integrates protection into every phase of software development (103).

By integrating the strategies of Defense in Depth, the Principle of Least Privilege, and Secure Development, organizations can significantly strengthen the security of their embedded systems. This integrated approach not only protects against known threats but also provides resilience against new vulnerabilities, ensuring the system's integrity and reliability throughout its lifecycle (99).

3.2.7 Mitigation Measures

The compiled mitigation measures aim to address the identified attack vectors, providing robust and comprehensive defense against cyber-threats (97). Secure coding practices are of paramount importance, such as input validation and data sanitization, acting as fundamental measures to prevent attacks (104). Additionally, some authors propose the implementation of firewalls and intrusion detection systems to protect against network attacks (105, 106, 107). Others suggest the use of encryption techniques to protect sensitive data from interception and manipulation (108, 109). (see Table 3.7).

To deal with denial-of-service (DoS) attacks, implementing rate-limiting mechanisms and traffic filtering is an effective action to mitigate the effects of these attacks . Access management and privilege control practices are used to prevent privilege escalation attacks . Implementing physical protection measures for devices to prevent physical tampering is also recommended . It is essential to integrate these measures into a cohesive framework, ensuring that each layer of defense complements the others. This provides comprehensive protection that addresses different security aspects, from software vulnerabilities to physical attacks . (97, 110, 111, 112, 113, 114, 98, 115) (see Table 3.7).

Furthermore, continuous monitoring and incident response are crucial to effectively detect and respond to threats in real time (116). Accordingly, the compilation of these mitigation measures reflects an integrated and multifaceted approach to protecting embedded systems against the various identified attack vectors.

The efficacy and applicability of the compiled mitigation measures to address the identified attack vectors vary according to the context and specific implementation. Secure coding practices, such as input validation and data sanitization, are essential for preventing code injection attacks and have significantly reduced the incidence of these attacks (104). However, the effectiveness of these practices depends on strict adherence to security guidelines throughout the software development lifecycle (117). (see Table 3.7).

The implementation of firewalls and intrusion detection systems has proven effective in mitigating network attacks by blocking malicious traffic and alerting to suspicious activities. However, these systems require proper configuration and maintenance to avoid false positives and ensure accurate detection of real threats (106). (see Table 3.7).

Access management and privilege control practices are crucial for preventing privilege escalation attacks, but their effectiveness hinges on the rigorous implementation of security policies and continuous user education on best security practices (112, 113). Additionally, the physical protection of devices is essential to prevent physical tampering, yet it can be challenging in environments where physical access cannot be completely controlled (114). (see Table 3.7).

Table 3.7: Controls Summary by Attack Vector

Attack Vector	**Defense Objective (What/Why)**	**Representative Controls (How)**	**Refs.**
Input tampering / injection	Preserve integrity of inputs and transactional data; prevent unintended code execution	Input validation, data sanitization, strict parsing/whitelists, schema validation	(92, 93)
Network-borne intrusion	Enforce perimeters and detect traffic anomalies; compartmentalize faults	Segmentation, firewalls, IDS/IPS, allowlists, protocol hardening	(118, 119, 105, 106)
Denial of Service (DoS)	Maintain availability and graceful degradation under load/abuse	Rate limiting, quotas, circuit breakers, back-pressure, ISP agreements	(94, 95, 96, 115)
Privilege escalation / unauthorized access	Restrict capabilities and sensitive operations to authorized principals	Strong authn/authz (MFA, RBAC/ABAC), just-in-time privileges, secrets hygiene	(60, 114)
Monitoring & response	Early detection, containment, and recovery; continuous assurance	Telemetry baselines, SIEM/SOAR, playbooks, exercises, post-incident hardening	(117)
Physical tampering	Deter, detect, and limit the impact of physical compromise	Tamper-evident seals, secure enclosures, port locking, secure boot	(97, 98)

Source: Prepared by the author.

3.2.8 Supply Chain Security

Supply chain issues are a central vector of risk in embedded systems, directly expanding the attack surface through third-party dependencies and reusable components (120, 11). To systematically handle vulnerabilities discovered in third-party components (hardware, firmware, libraries, containers, or services), the framework incorporates: (i) governance of the Software Bill of Materials (SBOM), (ii) provenance control (origin and build attestations), (iii) a response playbook with SLAs and stop-criteria, and (iv) contractual requirements for suppliers. This arrangement integrates with the risk management process (§ 3.2.4) and the set of mitigation measures (§ 3.2.7), aligned with principles from systems security engineering and organizational control management (62, 79, 121).

3.2.8.1 Triggers and Scope

The process is triggered by any of the events in Table 3.8, covering internal and third-party artifacts, and both direct and transitive dependencies. Adoption of *threat intelligence* and correlation with public or sector feeds strengthens early detection and prioritization (11, 7).

Table 3.8: Triggers for Supply Chain Response

Trigger	Description and Examples
Vendor advisory / CVE	Official vulnerability notice in an embedded component (e.g., a CVE in an RTOS cryptographic library).
Alerts via SBOM correlation	SBOM indicates the presence of an affected package/version in a firmware image or software module.
Provenance change	Break in the chain of trust (invalid signature, missing build attestation, unverified code origin).
External intelligence	Enrichment from public/private sources (e.g., sector reports and feeds) indicating an active exploit (11, 7).

Source: Prepared by the author.

3.2.8.2 SBOM Governance and Provenance Control

SBOM Policy. Each software/firmware release must include a complete SBOM (accepted formats: SPDX or CycloneDX) containing standardized identifiers (e.g., PURL/CPE), licenses, and the dependency tree (direct and transitive). The SBOM is:

1. Generated deterministically in the CI build pipeline, versioned in the artifact repository, and **cryptographically signed**.
2. Ingested into a corporate SBOM repository for asset management and vulnerability correlation.
3. Continuously monitored against vulnerability feeds; when there is *noise*, use VEX (*Vulnerability Exploitability eXchange*) statements to mark items as "*not affected*" or "*fixed*" and reduce false positives (62, 121).

Provenance (build, origin, and integrity). Every image/artifact must have a provenance attestation including, at minimum: code origin (repository/commit), build environment and recipe, builder identity, timestamp, and verifiable signature. Provenance validation is a **mandatory gate** prior to integration and deployment: verification failure implies an **automatic deployment block** until remediation (62, 121).

3.2.8.3 Playbook for Responding to Vendor Vulnerabilities

When a trigger occurs, follow the flow below (roles and SLAs in Table 3.9 and RACI in Table 3.10). The structure draws on good practices for incident handling and risk treatment to guide containment and remediation decisions (122, 79).

P1. Immediate triage (max. 24h): correlate the identifier (CVE/advisory) with the corporate SBOM; identify affected products/versions; create a single *ticket* and attach evidence (SBOM, VEX, attestations) (122).

P2. Exploitability check: verify whether the vulnerability is *reachable* in the execution context (e.g.,

unused function, feature disabled by configuration); if applicable, issue a VEX "not affected" with technical justification (62, 79).

P3. Temporary mitigation: apply *feature flags*, configuration *workarounds*, service isolation, filtering and pinning rules, or *rate limiting* to reduce exposure until definitive remediation (122).

P4. Definitive remediation: prefer vendor-supplied *minor/patch* updates; when unavailable, evaluate a governed *backport*, a temporary *fork*, or component replacement (with the minimum necessary requalification) (62, 121).

P5. Assurance and compliance: rebuild with **verified provenance**, regenerate the SBOM, validate signatures, and repeat functional/safety tests; update configuration documentation and *release notes* (62, 121).

P6. Controlled release and deployment: execute a *staged rollout* with *canary* and regression telemetry; keep a *rollback* ready (122).

P7. Communication and CVD: notify internal stakeholders; when applicable, coordinate *Coordinated Vulnerability Disclosure* with the vendor and appropriate channels (122, 11).

P8. Lessons learned and prevention: update dependency policies, SCA (Software Composition Analysis) rules, deny/allow lists, and supplier selection criteria (62, 121).

3.2.8.4 Severity, SLAs, and Stop Criteria

Severity classification and remediation deadlines should reflect the estimated likelihood and impact in the operational context, grounding containment and risk acceptance criteria (79).

Table 3.9: Severity, SLAs, and Containment Actions

Severity	**Criteria (summary)**	**Mandatory Actions**	**Remediation SLA**
Critical	Active exploit, RCE, safety/operational impact, break in chain of trust	Deployment *freeze*; **halt** integration; immediate mitigation; *out-of-band* update; telemetry and *kill-switch*	**72h** (mitigation), **7 days** (fix)
High	Privilege escalation or security bypass with no public exploit	Configuration mitigation; prioritize patch in the next window; enhanced monitoring	14 days
Medium	Requires specific/rare context or non-exposed surface	Planned correction; *reachable* assessment and VEX	Next release cycle
Low	*Hardening* and good practices with no immediate impact	Opportunistic adjustments; documentation	Backlog

Source: Prepared by the author.

3.2.8.5 Responsibilities (RACI)

The role matrix ensures accountability and efficient decision-making throughout the response cycle (122).

Table 3.10: RACI – Response to Third-Party Vulnerabilities

Activity	**Sec. Eng.**	**Product**	**PSIRT**	**Vendor/Procurement**
Triage and SBOM correlation	R	A	C	I
Provenance validation	R	A	C	I
Temporary mitigation	R	A	C	I
Remediation/rollout planning	C	A	C	I
Communication/CVD	C	I	A	R
Update policies and lists	R	C	C	A

Source: Prepared by the author.

3.2.8.6 Minimum Requirements for Suppliers

To reduce systemic risk, contracts must require: (i) SBOM delivery per release (accepted formats, minimum quality, and signature), (ii) vulnerability notifications and agreed patch windows (SLAs), (iii) build and code-origin provenance attestations, (iv) a coordinated vulnerability disclosure policy, (v) a technical channel for security advisories, (vi) a commitment not to introduce prohibited dependencies and to respect allow lists, and (vii) end-of-life with a supported migration path (62, 123, 121).

3.2.8.7 Integration with the Risk and Mitigation Processes

The results (SBOM, VEX, verified attestations, tests, and telemetry) feed the risk register and reestimate likelihood/impact in § 3.2.4; the applied controls (isolation, *hardening*, update, rollback) must be traced in § 3.2.7, preserving evidence for audit and continuous improvement (79, 121).

3.2.8.8 Mitigation Measures — Practical Examples

The practical implementation of mitigation measures can be illustrated through various specific examples. For instance, to prevent code injection attacks, many companies adopt secure development frameworks that include automated tools for input validation and data sanitization, such as OWASP ZAP (124). Firewalls and intrusion detection systems are frequently deployed in corporate and critical infrastructure networks using solutions like Snort and Suricata, which monitor traffic in real-time and block suspicious activities (125). Protection services such as Cloudflare or Akamai are employed to filter and distribute traffic, preventing overloads and mitigating denial-of-service (DoS) attacks (126).

Access management and privilege control can be enhanced through the use of multi-factor authentication (MFA) systems and the principle of least privilege, ensuring that users only have the necessary access

for their functions (127). Additionally, the physical protection of devices is implemented through measures such as security seals and intrusion sensors, especially in industrial or critical infrastructure environments where physical access may pose a threat (128).

These examples demonstrate how mitigation measures can be adapted and applied in various contexts to protect embedded systems against a wide range of attack vectors. Therefore, such challenges highlight the need for flexible and adaptable approaches, as well as an ongoing commitment to updating and maintaining security measures. While the compiled mitigation measures offer robust defense against various attack vectors, their effectiveness and applicability depend on proper implementation, continuous maintenance, and adaptation to the specific context of each embedded system.

3.2.9 Integration and Implementation

The integration and implementation of security measures within a holistic approach necessitate a meticulous process to fortify embedded systems against diverse cyber threats. The seamless integration of security measures spans from the initial design phases of the system throughout the entire software development lifecycle (129). Secure coding practices form a fundamental base, ensuring that vulnerabilities are minimized from the outset (104). Moreover, intrusion detection systems are strategically implemented to monitor and respond to potential threats in real time (105, 106, 107, 125). This comprehensive approach ensures a layered defense mechanism, where the layers include hardware (e.g., secure microcontrollers), firmware (e.g., digitally signed updates), software (e.g., secure coding and runtime protection), and network communication (e.g., encrypted data transmission and firewalls) (59).

The process of integrating and implementing security measures involves systematic planning and execution. It begins with a detailed analysis of system requirements and threat models to tailor security measures as needed. Each security measure is carefully integrated into existing development processes, such as continuous integration and continuous deployment pipelines, to maintain operational efficiency without compromising security (128, 130).

Despite the structured approach, challenges during integration and implementation are inevitable. These include complexities associated with adapting security measures to legacy systems, often requiring adjustments in existing architectures and workflows. Interoperability issues between newly integrated security components and legacy systems can also complicate integration. Furthermore, ensuring user acceptance and compliance with enhanced security protocols necessitates effective communication and training initiatives. Overcoming these challenges demands a collaborative effort among developers, system administrators, and end-users to optimize the integration process and maximize the effectiveness of implemented security measures (131, 132).

Evaluating the integration and implementation efforts is crucial to assess the effectiveness of the implemented security measures. Performance metrics such as intrusion detection rates and system response times are evaluated to measure the operational impact of integrated security solutions (133). Quantitative analysis of security incidents before and after implementation provides empirical evidence of risk reduction and operational improvements (134, 135). Additionally, qualitative feedback from stakeholders on usability and performance improvements offers valuable insights into the overall effectiveness of the inte-

grated security measures (136). Continuous monitoring and refinement based on evaluation results ensure that embedded systems remain resilient against evolving cyber threats, reinforcing the importance of a dynamic and adaptive security posture.

In conclusion, the integration and implementation of security measures within a holistic approach are essential to protect embedded software against malicious attacks. By incorporating security considerations throughout the development lifecycle, proactively addressing integration challenges, and rigorously evaluating outcomes, organizations can effectively enhance the security posture of embedded systems. This iterative process not only mitigates existing vulnerabilities but also prepares systems to confront future cyber threats, safeguarding critical assets and maintaining operational integrity (134, 135, 136).

In line with the collaboration with Airbus Defence and Space and the domain constraints of avionics, the empirical evaluation reported in this chapter concentrates on the Integrated Holistic Framework. The Comprehensive Holistic Framework remains the general-purpose conceptual baseline; the integrated framework is assessed here because it embeds the aviation-relevant DO standards (e.g., DO-178C, DO-326A and companions), which makes it the most appropriate artefact for practitioner-centred appraisal in the intended safety- and security-critical context.

3.2.10 Security Verification and Validation

Following the implementation of security controls, the next crucial step is the verification and validation of their effectiveness. This phase ensures that the system not only meets the security requirements but is also equipped to withstand actual intrusion and exploitation attempts. Penetration Testing plays a key role in this process. These tests involve simulated attacks on the system to identify vulnerabilities before they can be exploited by real attackers. Regularly conducting these tests, particularly after significant changes to the system, helps ensure that modifications do not introduce new vulnerabilities and that the security measures remain robust under updated operational conditions (134, 135, 136).

Moreover, Formal Security Analysis provides an additional layer of validation. This method involves the use of formal techniques to mathematically prove the effectiveness of specific security properties within the system. For example, tools such as Tamarin and ProVerif are often used in avionics to formally verify cryptographic protocols, ensuring that sensitive data transmissions comply with integrity and confidentiality requirements. This approach is crucial for systems requiring high levels of security assurance, as it provides a scientific basis for confidence in the implemented measures, particularly for systems handling critical information or high-risk operations (137, 138).

While formal methods are highly reliable, their application is limited due to the complexity and resource-intensive nature of the process. Formal analysis is often used in avionics for verifying specific, high-criticality components, such as flight control software or cryptographic implementations, rather than entire systems. This targeted application ensures a balance between assurance and practical feasibility. For less critical components, complementary methods such as penetration testing and security audits are more efficient and sufficient to identify vulnerabilities (63).

These three methods—penetration testing, security audits, and formal analysis—when combined, provide a comprehensive approach to the verification and validation of security for embedded systems. This

integrated approach ensures compliance with safety-critical standards and maintains system resilience in an evolving threat landscape. Together, they not only help identify and correct vulnerabilities before they can be exploited but also ensure that the system continues to operate safely and efficiently as new threats emerge and the technological landscape evolves.

3.2.11 Monitoring and Incident Response

The Monitoring and Incident Response step is crucial to maintaining the ongoing security of embedded systems following the implementation of security controls. This stage not only detects potentially malicious activities in real-time but also enables rapid and effective responses to security incidents. Intrusion Detection and Prevention Systems (IDS/IPS) in this context are configured to analyze data packets transmitted over these networks, identifying anomalies such as unauthorized commands, unexpected data injections, or unusual traffic patterns that may signal potential cyber threats (134, 135, 136, 103).

These systems are integrated with the aircraft's communication and maintenance subsystems. For instance, Aircraft Interface Devices (AIDs) often serve as a central point for monitoring network traffic and reporting anomalies to ground stations during flight. The configuration of IDS/IPS in avionics prioritizes real-time detection without compromising system performance, as latency or false positives could disrupt flight operations. Immediate alerts are transmitted to onboard or ground-based security administrators, who can take corrective actions swiftly to prevent potential damage (134, 135, 136, 103).

Concurrently, the incident response process in avionics is guided by rigorous airworthiness standards, which mandate detailed incident response plans to ensure both safety and compliance. These plans include predefined protocols for handling various types of security incidents, ranging from software anomalies to unauthorized access attempts. For example, during a detected anomaly, the system may initiate automatic containment measures such as isolating affected subsystems or restricting certain network commands. More complex incidents, such as potential tampering with flight-critical systems, require immediate coordination between onboard crew, ground operations, and potentially external regulatory bodies. This ensures rapid escalation and a well-coordinated response, minimizing operational disruptions (103).

Following the resolution of an incident, the post-incident recovery and analysis phase becomes essential. In avionics, this phase involves restoring service while ensuring that the aircraft remains airworthy and compliant with regulatory standards. Root cause analysis is conducted to determine whether vulnerabilities in systems like flight management software, navigation systems, or maintenance protocols were exploited. This learning process often leads to updating the aircraft's security baseline, revising risk assessments, and implementing new controls (103).

Additionally, incident recovery in avionics often involves collaboration with Original Equipment Manufacturers (OEMs) and system suppliers to address vulnerabilities in hardware or software. For example, the release of firmware patches or updates for flight control units must comply with certification processes, ensuring that changes do not introduce new risks or compromise the aircraft's airworthiness. This iterative process strengthens the system against future attacks and ensures continuous compliance with stringent regulatory requirements (121, 139, 123).

In summary, monitoring and incident response in avionics involve specialized systems and protocols

tailored to the critical and highly regulated nature of aviation. From real-time network traffic analysis to robust incident response frameworks, these measures ensure the security, safety, and operational continuity of flight-critical systems. By continuously adapting to new threats and leveraging lessons learned from incidents, avionics systems remain resilient in an evolving cybersecurity landscape (121, 139, 123).

3.2.12 Response Acceleration and Operational Automation

Critical systems cannot tolerate excessive latency between detection, decision, and action. To reduce dependence on manual intervention and accelerate response, the framework incorporates automation along three axes: (i) *automated threat modeling* driven by lifecycle artifacts, (ii) *pre-populated initial risk analysis* recalculated upon triggering events, and (iii) *compliance-as-code monitoring* across the *commit* $\rightarrow$ *build* $\rightarrow$ *deploy* $\rightarrow$ *runtime* continuum. Response orchestration relies on deterministic, machine-executable playbooks with *human-in-the-loop* only where operational impact is high, aligning security governance with modern DevOps/CI/CD practices (140, 141, 123, 121, 83).

3.2.12.1 Automated Threat Modeling

The pipeline exports structured data (DFD artifacts derived from architectural metadata, endpoints and queues, component inventory, and trust/communication parameters) to automatically produce:

- **Candidate threat lists** (e.g., applying pattern mappings by asset/flow category).
- **Initial attack trees** centered on critical components and trust relationships.
- **Coverage matrices** (threat $\times$ control) highlighting residual gaps.

Analysts *review/tune* the suggested set and approve material gaps. This reduces initial modeling time from days to hours while creating a structured backlog input for countermeasures (19, 120).

3.2.12.2 Pre-populated Initial Risk Analysis

At each *build* or *release*, the risk register is pre-filled by rules combining asset criticality, flow exposure, incident history, and current control effectiveness. The calculation follows an objective score (e.g., $R = f(\mathit{Impact}, \mathit{Likelihood})$) with project-level weights, yielding:

- **Automatic prioritization** of countermeasures (high $\rightarrow$ low).
- **Automatically opened tickets** with proposed mitigation actions and dependencies.
- **Event-driven re-evaluation**: any trigger in Table 3.8 recalculates risk and reorders the backlog.

Teams adjust weights/assumptions as needed, preserving decision traceability and evidentiary records (90, 86, 136).

3.2.12.3 Compliance as Code (Policies-as-Code)

Security and compliance requirements (e.g., cryptographic controls, hardening baselines, build integrity, network segmentation, and secret hygiene) are expressed as verifiable policies and evaluated at three gates:

a) **Commit/Build**: automatic rejection of artifacts that violate policies.

b) **Deploy**: promotion is gated when critical nonconformities are present.

c) **Runtime**: continuous verification with evidence archived for audit and continuous improvement.

Deviations create *tickets* with standard due dates and, for critical violations, **automatic deployment blocks** until remediation (121, 123, 140, 141, 116).

3.2.12.4 Orchestration and Latency Objectives

Consolidated alerts (e.g., SIEM) and software-supply triggers (Table 3.8) fire playbooks with steps labeled **[AUTO]** or **[HUMAN]**:

- **[AUTO]** isolate segment/host, perform version *rollback*, rotate keys/secrets, update blocklists, open and link *tickets* with evidence (component inventories and attestations).
- **[HUMAN]** approve actions with operational impact, durable configuration changes, and justified policy exceptions.

Operational indicators (suggested targets, project-tunable): **MTTD** (Mean Time to Detect) $\leq$ 5 min; **time-to-containment** $\leq$ 30 min; **MTTR** (Mean Time to Restore) $\leq$ 4 h for noncritical components and per agreed maintenance window for critical ones; **False Positive Rate (FPR)** $\leq$ 3% (83, 116, 136).

Table 3.11: Automation by Method Phase

Phase	Inputs (data)	Automated Outputs	Human Involvement	Indicators (targets)
Threat modeling	Architectural metadata, derived DFD, build metadata, pattern catalogs	Candidate threats, attack tree, coverage matrix	Review/validation	Coverage $\geq$ 80%; FPR $\leq$ 5%
Initial risk analysis	Inventory/criticality, exposure, incident history, control effectiveness	Pre-populated score, countermeasure prioritization, backlog items	Weight tuning	Prioritization in $<$ 10 min/release
Continuous compliance	Policies-as-code, CMDB, telemetry	Continuous reports, automatic tickets, evidence	Justified exceptions	Critical deviation fixed $\leq$ 24 h
Response & containment	SIEM alerts, supply triggers (Tab. 3.8)	Isolation, *rollback*, secret rotation, deploy block	Dual approval for critical	MTTD $\leq$ 5 min; containment $\leq$ 30 min
Post-incident	Artifacts, logs, lessons learned	Updated playbooks, blocklists, policies	Change control board	Recurring actions automated

Source: Elaborado pelo autor.

Governance and Safeguards. Any automatic action with material operational impact requires dual approval and a guaranteed rollback path. Periodic testing of playbooks and policies mitigates drift and over-automation risks, aligning change and exception management with recognized governance practices (123, 83).

Finally, the operational models and adoption roadmaps are detailed in Appendices H and H, which translate the principles of automation, *compliance as code*, and response orchestration for legacy contexts with objective operational targets (121, 139).

3.2.13 Guidance for Integration with Legacy Systems

The practical application of the framework in legacy environments—such as serial buses and proprietary protocols—requires a differentiated approach that prioritizes loose coupling, non-intrusive data collection, and assisted response orchestration. To this end, this subsection is grounded in three central axes: (i) *threat modeling* driven by operational artifacts, so as to ensure alignment with established risk-analysis practices in safety-critical systems (121, 123); (ii) the adoption of *compliance as code*, with the inclusion of *gates* in continuous integration and delivery (CI/CD) pipelines, in accordance with normative recommendations (121, 139, 123); and (iii) response orchestration by means of structured *playbooks*, with explicit demarcation of automated steps [AUTO] and expert-supervised stages [HUMAN], in line with the literature on operational security in embedded systems (121, 139, 123). The established operational objective is to ensure a *Mean Time to Detect* (MTTD) less than or equal to five minutes, with all evidence duly recorded in the Requirements Traceability Matrix (RTM, §D) and in the associated evidence catalog (EV-XXX).

Integration pattern. Integration with legacy systems should adopt collection in *read-only* mode so as not to introduce interference in certified environments, followed by event normalization and detection mechanisms based on behavioral profiles. Response is subsequently orchestrated in accordance with continuous monitoring practices (121, 139). In contexts lacking IP network connectivity, the local connector performs *edge buffering*, periodically exporting artifacts to the central evidence pipeline, thereby ensuring traceability and auditability.

Gates in legacy code. In situations where access to the source code is restricted, it is still feasible to implement minimal *gates* in the pipeline, such as mandating the presence of software bills of materials (SBOMs), secure configuration checks, and validations of normative evidence. Such mechanisms ensure the fulfillment of essential security and compliance requirements (121, 139, 123), even in systems whose codebase cannot be directly modified. The evidence and the respective normative mappings are described in detail in Appendices §H and §H.

3.2.14 Continuous Monitoring and Review

Continuous monitoring and review constitute essential elements in maintaining the efficacy of security measures in embedded software systems. The dynamic nature of cyber threats and the constant evolution of the operational environment necessitate a proactive approach to identify and mitigate emerging risks. This underscores the understanding that security is not a static product but an ongoing process requiring perpetual adjustments to counter new threats. Continuous monitoring in embedded systems involves lightweight mechanisms tailored to the system's resource constraints. For example, monitoring solutions often rely

on periodic integrity checks of firmware, lightweight intrusion detection systems (IDS) like Zeek, and event logging optimized for embedded architectures to detect anomalous or unauthorized activities without overloading the system (2, 142).

As Stallings and Brown (2018) assert, "continuous monitoring is crucial for the early detection of security incidents, enabling a swift response that can minimize damage." In embedded software systems, monitoring may encompass event log analysis, system integrity verification, intrusion detection systems (IDS), and behavioral analysis tools. In avionics, these include mechanisms like Aircraft Interface Devices (AIDs) to capture system logs and real-time anomaly detection frameworks that identify unauthorized access or malicious code execution (58, 2).

Implementing an effective continuous monitoring and review program poses various challenges. The sheer amount of log data and security event information can be overwhelming, and effective analysis of this data requires advanced tools for analysis and correlation. Big data analytics and machine learning tools are increasingly being employed to filter relevant information and identify anomalies indicating security issues. On aircraft with limited resources, lightweight analytics platforms integrated with ground-based monitoring systems can offload processing requirements. These systems transmit key telemetry and security data to centralized systems on the ground, where computationally intensive analysis is performed. This hybrid approach balances the need for real-time monitoring with the constraints of embedded avionics systems (96, 60).

Responding to incidents detected during monitoring is another critical aspect. According to NIST SP 800-61, "a well-defined incident response plan is essential to minimize the impact of an attack and restore normal operations quickly." While the figure 3.6 below illustrates the risk assessment process, it plays a key role in identifying priorities during incident response, such as containment, eradication, and recovery. For avionics, incident response often includes predefined safety measures, such as fallback to redundant systems, isolated communication modes, and system restarts in compliance with airworthiness requirements (122, 57). Regular exercises and simulation of these incident response plans in test environments ensure readiness for real-world scenarios and align with aviation industry standards (57).

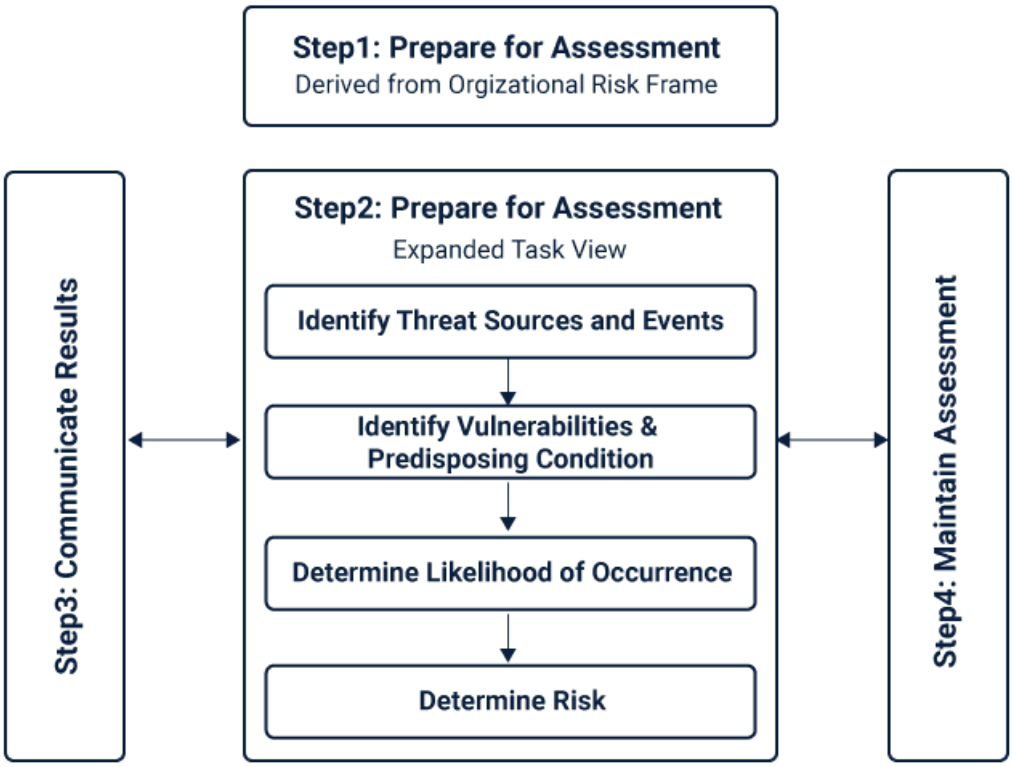

Figure 3.6: NIST risk assessment process

Finally, feedback obtained through monitoring and reviews should be utilized to continuously improve security policies and practices. Anderson and Moore (2021) highlight that "continuous learning and adaptation are essential for developing a resilient security posture." This may involve updating IDS rules and signatures, implementing new security measures in response to discovered vulnerabilities, and ongoing user education on security best practices. In avionics, this iterative cycle involves integrating lessons learned into updates for system components and ensuring that compliance with safety and security standards is maintained (63, 26).

Therefore, continuous monitoring and review are fundamental pillars for the security of embedded software systems. These practices ensure that defenses remain robust and adaptable in the face of an ever-changing threat landscape. Despite significant implementation challenges, leveraging advanced technologies and maintaining well-defined incident response processes can help mitigate these challenges. Systematic application of these practices is crucial to protect embedded systems from a wide array of cyber threats.

3.2.15 Continuous Maintenance and Updating

Continuous maintenance and updating are crucial steps in the security lifecycle, particularly when viewed within the holistic context of protecting embedded systems, where the effectiveness of implemented security measures is maintained and enhanced over time. This process is vital not only for addressing flaws but also for adapting the security system to changes in the technological environment and threat tactics, ensuring effective and updated protection that keeps system defenses resilient against the dynamic

landscape of cyber threats and technological developments.

Patch Management is one of the foundational pillars of this phase. Regular application of security patches is essential to address vulnerabilities that, if left untreated, could be exploited by attackers. This process must be systematic and meticulous, involving not only the application of patches provided by software and hardware manufacturers but also the verification of their effectiveness in a test environment before deployment on operational systems. In avionics, patch management follows strict guidelines, requiring extensive testing and validation to ensure that patches do not impact airworthiness or operational safety. Additionally, the process includes continuous monitoring of new security releases and a critical evaluation of how and when these patches should be applied, based on the criticality of the fixes and the specific infrastructure of the system (99).

Reviewing and Updating Security Policies is another essential component of this phase. An organization's security policy should be a living document that evolves to meet new challenges and incorporate lessons learned. This ongoing review ensures that the policies remain relevant and effective amidst changes in the threat environment and business practices. Updates may include changes in access control strategies, adjustments in incident response guidelines, and the introduction of new protective technologies (103).

Continuous Maintenance of the Security System complements policy reviews and training. Regular audits help identify not just technical failures but also operational and strategic lapses that could compromise security. These audits provide an unbiased view of the security state and are crucial for validating compliance with international standards and evolving privacy and security regulations. Audits are performed to ensure compliance with standards like ISO/IEC 27001, to validate the robustness of implemented security measures. These evaluations are essential to ensure that the security system remains effective and aligned with the latest industry requirements (143, 123).

The ISO/IEC 27001 is a widely recognized international standard that establishes the requirements for an Information Security Management System (ISMS). This strategic framework provides a systematic approach to managing sensitive information, ensuring its confidentiality, integrity, and availability. While ISO/IEC 27001 is not specific to avionics, its principles can be integrated into the broader security framework to complement aviation-specific standards. Recently, the updated version of the standard, ISO/IEC 27001:2022, introduced improvements that reflect changes in the cyber threat landscape and technological evolutions, reinforcing the need for adaptability and resilience in information security practices (123).

Training and Awareness are equally crucial to this process. Security is only as strong as its weakest link, which is often the human factor. Ongoing training and awareness programs are essential to keep all users informed about security risks, best practices, and updated policies. These programs not only educate users on how to avoid risky behaviors but also reinforce a security culture within the organization. In avionics, training programs must address the unique requirements of aviation security, including simulations of cyberattacks on aircraft systems, and updates on regulatory changes. These targeted programs are designed to ensure that all stakeholders, from developers to maintenance personnel, are equipped to uphold high security standards in their respective roles (103, 143).

Integrating these three pillars patch management, policy review, and Integration and Implementation training—creates an adaptive and resilient security environment that can effectively respond to changes in both the threat landscape and technology itself. This maintenance and updating cycle not only protects the

organization's information assets but also sustains the trust of clients and partners, ensuring that robust and current security practices are always in place.

3.2.15.1 Field Updates, Obsolescence Management, and Secure Decommissioning

Ensuring the continued safety, reliability, and sustainability of aeronautical systems over their full operational life cycle requires an integrated view that unifies field updates and retrofits, systematic obsolescence management, and secure decommissioning. Rather than treating these activities as isolated episodes, a life cycle perspective connects short-term corrective or capability-enhancing interventions with medium-term component refresh strategies and end-of-life practices that preserve information security and operational assurance. This integrated approach responds to emerging vulnerabilities, technological change, and evolving operational needs while maintaining service continuity and engineering consistency (38, 31, 40).

Within this continuum, field updates introduce software corrections or new functionalities on in-service platforms, whereas retrofits typically encompass the replacement of hardware elements or the integration of new technologies into existing architectures . Both demand structured planning to avoid unanticipated behaviors and to preserve baseline dependability, beginning with an impact assessment that examines risks, dependencies, and the fit within legacy systems and interfaces. When sequenced within planned maintenance windows, these actions reduce downtime and sustain operational availability (31, 40, 32).

For software-centric updates, the literature emphasizes robust verification and validation before release and after installation. Regression testing, targeted safety-relevant checks, and system-level performance evaluations help ensure that new code paths neither degrade stability nor introduce security regressions. Pre-deployment trials in simulation or representative testbeds increase confidence that the modification will behave as intended once exposed to operational loads and real-world data (33, 41, 29).

Hardware-oriented retrofits often revolve around line-replaceable units (LRUs) or the insertion of higher-performance processing modules. These interventions must respect physical constraints (space, weight, power), thermal budgets, and electromagnetic compatibility across adjacent components and harnesses. Because hardware changes frequently imply firmware and driver adaptations, coordinated software reconfiguration is commonly required to exploit new capabilities without compromising integration boundaries. Early prototyping and interface conformance checks reduce rework and curb latent defects during fleet rollout (38, 39, 40, 32, 33).

Logistical coordination is a recurrent limiting factor for all field interventions. Operators must balance limited maintenance windows against aircraft and crew availability, inventory constraints, and specialized team scheduling. Successful programs align update packages with pre-existing maintenance cycles, bundle compatible tasks, and pre-position material to compress time on ground while preserving quality assurance gates. Clear work instructions and acceptance criteria further reduce variability across line stations and MRO facilities (38, 31, 40).

Cybersecurity assurance is central to update orchestration for interconnected embedded systems. Authenticated update channels, digital signatures, and integrity verification are necessary to prevent the injection of malicious code or tampering during transit and installation. Post-deployment monitoring (e.g., integrity checksums, anomaly detection on update-touched modules) complements pre-release testing, cre-

ating a defense-in-depth posture across the update pipeline. Isolation of update services, least-privilege credentials, and auditable logs strengthen traceability and incident response if anomalies arise (33, 41, 29).

Documentation binds these practices and sustains long-term maintainability. Update bulletins, configuration records, and revised technical manuals capture what changed, why it changed, and how it was validated, enabling reproducibility and supporting future troubleshooting, audits, and airworthiness evidence. Mature configuration management ensures that software baselines, hardware bills of material, and parameter sets remain coherent across the fleet (38, 40, 29).

Obsolescence management complements near-term updates by proactively addressing the discontinuation of hardware and software elements across the aircraft's life. In fast-moving supply ecosystems, critical parts may reach end-of-support well before platform retirement, risking availability and reliability if left unmanaged. Effective programs monitor vendor notices, forecast end-of-life timelines, and maintain visibility into inventories and last-time-buy opportunities to bridge gaps (31, 39, 32, 41).

Forecasting methods, including Prognostics and Health Management (PHM), help anticipate degradation and remaining useful life, aligning replacement plans with observed performance rather than calendar age alone. Where market availability tightens, strategies such as lifetime buys, qualified alternates, and use of recertified parts mitigate risk, provided that traceability and quality screening are maintained. These measures reduce exposure to single-source dependencies and smooth demand across the fleet (31, 40, 32, 33, 41).

Each substitution decision warrants systems-engineering analysis to assess impacts on interfaces, timing budgets, failure modes, and associated software requirements. Even functionally equivalent components can alter thermal behavior, timing determinism, or electromagnetic emissions; structured impact analysis and targeted verification reduce incompatibilities and latent hazards. Where changes enable new capabilities, coordinated firmware and software updates are planned to preserve architectural integrity (33).

Supply-chain collaboration is decisive. Continuous communication with suppliers about roadmaps, lead times, and second-source options enables earlier pivots; in selected cases, co-development of custom parts extends platform longevity when justified by fleet size and remaining service life. Diversifying sources where feasible increases resilience to shocks and supports predictable maintenance planning (31, 40, 32).

Because timing affects both cost and risk, obsolescence planning relies on cost-benefit trade studies. Premature replacement raises operating expenses; delayed action heightens the probability of stockouts, schedule slips, and reliability degradation. Incorporating inventory realities, remaining useful life estimates, and risk exposure informs the optimal intervention window. Embedding obsolescence policies into life-cycle governance ensures periodic review and early detection of emerging risks (38, 40, 41, 29).

When systems or components reach end-of-service, secure decommissioning protects sensitive information and assures orderly retirement. The process begins with the identification and classification of stored data—including operational logs, credentials, and cryptographic keys—followed by sanitization with irreversible erasure methods commensurate with data criticality. Verification of sanitization outcomes (e.g., sampling, checksum invalidation) reduces the chance of forensic recovery (39, 40).

Hardware is then dismantled, reused, recycled, or destroyed in accordance with environmental and

regulatory policies. Parts unsuitable for reuse are physically destroyed to preclude reassembly or data extraction; assets retained for repurposing undergo evaluation and testing to confirm fitness for their new roles. Chain-of-custody records and disposal certificates reinforce accountability and auditability (38, 41).

Logical off-boarding is essential for interconnected fleets. Credentials, keys, and certificates associated with decommissioned elements are revoked; access control lists and trust stores on remaining systems are updated to prevent residual access paths. This step closes the loop between physical removal and cybersecurity posture, preventing orphaned identities or stale trust relations (32, 33, 41, 29).

Transparent communication with stakeholders—operators, suppliers, and relevant authorities—supports alignment on scope, timing, and evidentiary expectations, while comprehensive documentation of actions taken enables later review and compliance checks . Lessons learned from decommissioning feed forward into update planning, obsolescence roadmapping, and design choices for the next generation, strengthening the overall life-cycle strategy (38, 31, 40, 32, 33).

Viewed as an integrated discipline, the combined practice of field updates and retrofits, obsolescence management, and secure decommissioning equips organizations to adapt to technological change, manage supply dynamics, and safeguard information—without overreliance on sector-specific prescriptions. The result is a more resilient, traceable, and secure evolution of aeronautical systems across their entire service life (38, 31, 39, 40, 32, 33, 41, 29).

3.2.15.2 Operational Maintenance Procedures

In a domain-agnostic setting, continuous maintenance must be governed by formal change and configuration management, regression verification, and post-deployment monitoring, ensuring evidence-based assurance across the lifecycle (123, 139, 121). The procedure below consolidates these requirements into auditable steps.

Inputs: maintenance windows, approved change requests, configuration baselines, open risks.
Activities: plan per window; pre/post checks; regression verification; post-deploy monitoring (logs, KPIs); configuration record updates.
Outputs: approved maintenance bulletin; verification logs; updated CM records.
Evidence IDs: `EV-050` (maintenance bulletin + approval), `EV-051` (pre/post checks + regression report).

3.2.15.3 Retrofit Governance and Change Classification

Retrofits require impact analysis, structured V&V, and explicit decision records to preserve safety, reliability, and security in complex embedded systems (121, 123, 139, 20). The following governance flow classifies changes and ties acceptance to objective evidence.

Inputs: impact analysis (interfaces/timing/EMC), test plan, parts availability.
Activities: bench/prototype; directed tests; SW/FW integration; acceptance criteria; CAB decision.
Outputs: impact & V&V report; CAB minutes/decision.
Evidence IDs: `EV-052` (impact report), `EV-053` (V&V results + CAB approval).

3.2.15.4 Obsolescence Planning and PHM Integration

Lifecycle closure depends on proactive obsolescence management supported by inventory accuracy and health/prognostics data, enabling risk-informed replacement and sustainment decisions (121, 123, 65). The plan below focuses on traceable trade-offs and inventory currency.

Inputs: supplier roadmaps, inventory and health data, RUL/PHM indicators.
Activities: lifetime-buy; qualification of alternates; cost–risk–window trade-off; parts tree update; CMDB sync.
Outputs: obsolescence plan; updated risk matrix; updated inventory/CMDB.
Evidence IDs: `EV-054` (obsolescence plan + trade study), `EV-055` (inventory/CMDB update).

3.2.15.5 Secure Decommissioning Playbook

Secure end-of-life requires verifiable data sanitization, credential revocation, asset disposition with chain of custody, and audit closure—mapped to widely adopted security control sets (121, 139). The playbook below ensures reproducible artifacts for assurance and auditability.

Inputs: logical/physical inventory; data/classification; credentials/keys.
Activities: media sanitization with verification; credential/key revocation; asset recycling/disposal with chain of custody; audit closure.
Outputs: sanitization certificate; disposal/recycling statement; revocation publication/propagation logs.
Evidence IDs: `EV-056` (sanitization certificate + KMS/logs), `EV-057` (chain of custody + disposal), `EV-058` (revocation propagation proof).

3.2.16 Integration with Risk Management

Integrating with Risk Management is crucial to align the security practices of embedded systems with the broader risk management strategies of an organization. This process ensures that security measures are effective and synchronized with the global objectives and challenges of the business. This step goes beyond the traditional application of security controls, promoting an approach that aligns cybersecurity with broader business strategy and operations. Effective integration with risk management enables a holistic and strategic approach to managing uncertainties and threats, thereby strengthening organizational resilience.

Initially, Continuous Risk Assessment involves constant monitoring of the environment to identify new threats and assess existing risks. In the context of embedded systems, this means evaluating threats specific to hardware and software vulnerabilities, such as supply chain risks, unpatched software, or evolving attack vectors like zero-day exploits. This assessment enables the organization to proactively adapt its security practices in response to changes in the threat landscape, ensuring that measures remain relevant and effective.

Risk Governance is a fundamental component of this integration. It involves establishing structured frameworks and processes that ensure risk-related decisions are made systematically and reflect the organization's values, regulatory requirements, and risk tolerance. For embedded systems, this might include

creating a governance structure that incorporates standards like ISO/IEC 27001 or NIST frameworks, ensuring alignment between technical and business-level risk management. Implementing a robust governance framework facilitates the creation of a common language for discussing risks, thereby easing communication and understanding across different departments and stakeholders (103, 123).

Subsequently, Aligning Security Practices with Business Objectives is essential. Security policies and procedures should actively support the strategic goals of the business. For example, in the aerospace industry, ensuring the security of flight-critical embedded systems supports the overarching goal of operational safety and regulatory compliance, which in turn protects brand reputation and customer trust. This alignment ensures that security efforts positively contribute to the growth and success of the organization, rather than being viewed merely as a regulatory necessity or operational expense. Security therefore becomes an integral part of business strategy, facilitating the acceptance and implementation of robust security practices across the organization (144).

Furthermore, Effective Communication between risk managers and security teams is imperative. Promoting a risk-aware culture within the organization involves educating everyone, from senior management to operational staff, about the importance of security and the role each individual plays in risk management. For embedded systems, this means ensuring developers, engineers, and even non-technical staff understand the implications of poor security practices, such as leaving sensitive ports open or failing to apply timely patches. Efficient integration requires that information flows freely between these groups, allowing risk-based decisions to be made with all relevant information at hand. This continuous communication helps ensure that security measures are understood and implemented within the broader context of business risks (103).

Lastly, Reviewing and Updating Risk Management Strategies based on lessons learned and changes in the external environment is essential to maintaining the relevance and effectiveness of security practices. For instance, an organization might adjust its risk management approach if a new vulnerability database, such as CVE (Common Vulnerabilities and Exposures), highlights emerging threats to embedded systems. Periodic reviews of risk management strategies and policies enable the organization to dynamically adapt and maintain a resilient security stance in the face of constantly evolving threats (103).

3.3 AN INTEGRATED APPROACH

Building upon the framework introduced in the previous chapter, an integrated approach for protecting embedded systems against malicious attacks is paramount. This approach entails a multidisciplinary strategy that incorporates international security standards, industry-recommended practices, and the continuous integration of technological advancements. Such a framework is essential in a technological landscape where the complexity and interconnectedness of avionics systems continuously expand the attack surface and potential vulnerabilities, ensuring all aspects of security, from risk management to incident response, are addressed cohesively and effectively (36).

The integration of standards such as ISO 31000 and ISO/IEC 27005, alongside industry-specific guidelines like DO-178C, DO-254, DO-326A, DO-355A, and DO-356A, ensures that the framework is tailored

to aviation while aligning with global best practices in risk management and information security. These standards are critical for safeguarding avionics systems throughout their lifecycle, covering aspects from software and hardware development to operational security and maintenance, thereby ensuring compliance with airworthiness regulations (79, 145, 57, 49, 26, 55).

3.3.1 Risk Assessment in Avionics

Risk assessment is prioritized initially, following ISO 31000, which guides the systematic identification and treatment of risks in a structured manner. This standard establishes a robust framework for risk management, emphasizing the need to tailor these practices to the specific context of aviation, ensuring an effective response to the unique threats faced by avionics systems. This global standard provides a solid foundation for the systematic identification, analysis, evaluation, and treatment of risks, ensuring that avionics manufacturers and operators implement risk-based decision-making (145).

In parallel, ISO/IEC 27005 complements ISO 31000 by specifically focusing on information security risk management. This standard outlines procedures for identifying and assessing risks related to avionics systems' embedded software and data, addressing the need to protect critical aviation assets against potential cyber threats. By integrating these two standards, a comprehensive framework is created that recognizes general business risks while delving into specific aspects of information security (79, 145).

For avionics, DO-178C (Software Considerations in Airborne Systems) and DO-254 (Design Assurance Guidance for Airborne Electronic Hardware) establish the required processes and rigor for developing software and hardware in compliance with safety and security regulations. Risk assessment in this context ensures that security measures align with airworthiness requirements, addressing system integrity, redundancy, and failure mitigation strategies in airborne environments (26, 55).

Furthermore, DO-326A introduces specific guidelines for cybersecurity in avionics, critical for protecting flight safety systems and sensitive data. By integrating the principles of ISO 31000 and ISO/IEC 27005 with DO-178C, DO-254, and DO-326A, aviation stakeholders ensure a proactive cybersecurity approach, from aircraft design to operation and maintenance (79, 145, 57, 49, 26, 55).

3.3.2 Implementing Security Controls in Avionics

ISO/IEC 27001 serves as a central pillar, providing a detailed framework for establishing and managing an Information Security Management System (ISMS). This standard sets stringent criteria not only for implementation and operation but also for continuous review, maintenance, and improvement of information security policies. In the aviation sector, ISO/IEC 27001 is used alongside DO-326A to ensure systematic alignment between security policies and identified risks, covering software, hardware, and operational security (146).

Additionally, best practices recommended by NIST SP 800-53 can reinforce policies already established by ISO/IEC 27001. The 2020 revision of NIST SP 800-53 emphasizes adaptive security planning, which is particularly relevant for avionics, given the long lifecycle of aircraft and the necessity to continuously update security controls while maintaining compliance with regulatory frameworks (79, 146, 121).

DO-178C and DO-254 establish strict guidelines for implementing security controls in software and hardware, ensuring compliance with airworthiness and cybersecurity requirements. These standards mandate rigorous verification and validation (V&V) processes, including static and dynamic code analysis, formal methods, and hardware testing, to prevent security flaws in flight-critical systems.

Moreover, NIST SP 800-53 provides a structured set of controls covering access management, data protection, incident response, and operational continuity. The ISO/IEC 27002 standard complements these guidelines by detailing specific implementation practices for protecting avionics systems' confidentiality, integrity, and availability (139).

In this section, we implement security controls becomes the next critical step for effectively protecting the embedded system. In this stage, theory is transformed into practice through the application of various techniques and technologies designed to enhance the system's security at multiple levels. In avionics, these levels include the hardware layer (e.g., secure microcontrollers), the software layer, the network communication layer (e.g., ARINC 664-based AFDX networks with encryption), and the operational layer (e.g., secure maintenance practices and physical access control). Each layer contributes to a defense-in-depth approach tailored to the stringent requirements of aviation security (143).

A fundamental control is encryption, utilizing robust cryptographic algorithms to protect data at rest, in transit, and in use. In avionics, this means ensuring that sensitive data, such as flight telemetry or system health reports, is encrypted according to airworthiness standards. For instance, encryption protocols like AES-256 or RSA are commonly employed for securing communications between onboard systems and ground stations, preventing unauthorized interception or tampering (99, 147, 148).

Moreover, Intrusion Detection and Prevention Systems (IDS/IPS) play a crucial role by continuously monitoring network traffic and system behavior to detect and respond to suspicious or anomalous activities. The difference between IDS and IPS lies in their functionality: IDS identifies and alerts on potential threats, while IPS actively blocks them in real time. In avionics, these systems are typically implemented within Aircraft Interface Devices (AIDs) or integrated into the AFDX network to monitor for unauthorized traffic or system anomalies. Unlike corporate networks, where IDS/IPS monitor general traffic, in avionics they are configured to detect protocol-specific anomalies, such as unauthorized ARINC 429 commands or unexpected packet injection into critical networks (149, 143).

Physical security is also critical, especially for embedded systems operating in critical environments. Measures include shielding hardware against electromagnetic interference (EMI) to protect avionics from both accidental disruptions and deliberate electromagnetic attacks. For example, military-grade shielding is applied to flight control units to ensure their operation in high-EMI environments. Additionally, physical access controls, such as secure enclosures and tamper-evident seals, prevent unauthorized personnel from accessing onboard hardware (60).

This multidimensional implementation of security controls not only addresses the risks identified earlier but also prepares the system to face real and emerging challenges in the operational environment. This is an ongoing process that requires regular review and updating to maintain the effectiveness of the controls as threat types evolve and new vulnerabilities are discovered. Such practices require evidence of continued compliance for airworthiness approval (26).

Aviation security standards such as DO-355A ensure that security measures extend beyond software and hardware development into operational phases, providing guidelines for securing maintenance processes, managing software configurations, and preventing unauthorized access to avionics systems (50).

3.3.3 Security Training and Awareness in Avionics

Human factors remain a major source of security failures in aviation. To mitigate risks associated with operator errors or insider threats, ISO/IEC 27001 and DO-326A require comprehensive security training and awareness programs. These initiatives educate personnel on cyber threats, secure maintenance practices, and compliance requirements, reinforcing a security-first culture within aviation organizations (123).

Furthermore, NIST SP 800-50 provides guidelines for structuring effective security awareness programs, ensuring that aviation professionals remain informed about emerging threats, evolving attack tactics, and new cybersecurity protocols affecting avionics systems (150).

3.3.4 Continuous Monitoring and Incident Response in Avionics

Continuous monitoring is a key requirement for avionics cybersecurity, as outlined in DO-356A, which specifies stringent procedures for real-time threat detection and incident response. Given the safety-critical nature of avionics systems, monitoring tools such as Intrusion Detection and Prevention Systems (IDS/IPS) must be tailored to aviation environments, focusing on ARINC 664 (AFDX) and ARINC 429 network traffic to detect unauthorized access or anomalous system behavior (57, 151, 149, 143).

Within the integrated approach, resilience to zero-day attacks is strengthened by extending continuous monitoring (as required for avionics environments) with behavioral analytics and predictive modeling. Concretely, the framework establishes normal baselines of operation across aircraft data networks and execution paths e.g., ARINC 664/AFDX and ARINC 429 traffic patterns, timing profiles, memory allocation behavior, and system call sequences so that anomaly-based intrusion detection can flag statistically significant deviations without relying on prior signatures (151, 149, 143).

Predictive techniques are incorporated in two complementary layers: (i) unsupervised outlier detection (e.g., autoencoders, Isolation Forest) and sequence-aware models (e.g., n-gram/HMM or LSTM over system-call traces) to surface previously unseen behaviors, and (ii) supervised classifiers to reinforce detection for known patterns and reduce false positives over time (79, 121). These analytics are integrated into a lifecycle-oriented security process consistent with DO-326A, DO-355A, and the incident-handling guidance of NIST SP 800-61, ensuring that alerts trigger graded responses ranging from rate-limiting and interface isolation to safe-mode fallback and forensic capture while preserving airworthiness and traceability (57, 50, 123).

In alignment with ISO/IEC 27001 and ISO/IEC 27005, the resulting evidence (profiles, thresholds, detection logs, and response records) feeds risk reviews and control effectiveness assessments, reducing mean-time-to-detect/contain and directly addressing the limitations most often associated with zero-day vulnerabilities in avionics contexts (146, 79).

Incident response follows a structured framework based on NIST SP 800-61, which emphasizes in-

cident identification, containment, eradication, recovery, and post-incident analysis. By integrating DO-356A, NIST SP 800-61, and ISO/IEC 27001, aviation organizations can ensure a coordinated response to security incidents while maintaining compliance with global cybersecurity standards (123, 151).

3.3.4.1 Lifecycle Security and Sustainability in Aerospace Systems

The life cycle of critical aeronautical systems involves multiple interdependent phases, notably security retrofits, obsolescence management, and secure decommissioning. The effectiveness of this approach depends on the harmony between engineering practices and sectoral standards such as DO-326A, DO-355A, DO-356A, ARINC, ISO/IEC 27001, and aircraft certification processes. By articulating these phases in a single chapter, it becomes clear that security and regulatory compliance must permeate every stage of the life cycle of embedded systems (38, 31, 39, 49, 26, 123, 57, 50, 55, 149, 143).

Retrofits are planned interventions in embedded systems aimed at correcting vulnerabilities, updating functionalities, or incorporating additional safeguards. In the context of civil aviation, the DO-326A standard establishes a structured process for risk assessment and threat mitigation, providing guidelines to ensure that modifications maintain airworthiness certification and do not introduce new vulnerabilities. Periodic review of requirements and architecture, combined with an impact analysis plan, forms the basis for successful retrofits (38, 31, 39).

Complementing the DO-326A process, the DO-355A and DO-356A standards provide specific guidance for the operation and maintenance of aircraft regarding information security. The former directs Design Approval Holders and operators to demonstrate that security threats remain confined to acceptable levels, providing an acceptable means of compliance for approving information security aspects in continuing airworthiness activities. The latter describes security methods and considerations to be used within the security process defined in DO-326A, recognizing that equivalent alternatives may be adopted. These documents guide retrofits aligned with hardware and software security practices, including the application of cryptography, digital signatures, and isolation techniques in embedded architectures (49, 26, 123, 57, 50, 55, 149, 143).

A subsequent phase is obsolescence management, which addresses the inevitable discontinuation of components in systems with long life cycles. The literature highlights that obsolescence arises from technological cycles shorter than the service life of aircraft and represents a complex problem requiring proactive measures, planning, and risk modeling (41, 29). Research reports identify patterns, tools, and standards used in the industry, underlining the need to minimize financial impacts and ensure continuous compliance (30, 34). Standards such as ARINC 662 recommend strategies to address electronic component obsolescence in commercial aircraft, promoting design practices tolerant of obsolescence and planning of replacements (35, 152).

Obsolescence management also depends on internal manufacturer policies and advance procurement plans. Manuals and technical guides suggest implementing lifetime buy policies, inventory monitoring, and contracting alternative suppliers to ensure the availability of critical parts (36, 37). The integration of ARINC guidelines into life cycle planning is essential, as many aircraft operate decades beyond the active support period of components. By aligning these practices with preventive maintenance processes and

PHM (Prognostics and Health Management) mechanisms, it is possible to schedule replacements before failures and optimize costs (153, 154).

Finally, secure decommissioning addresses the removal of systems, ensuring that sensitive data is eliminated and that hardware is responsibly disposed of. Although there is no specific regulation for aircraft decommissioning, information security standards provide the basis for robust procedures. ISO/IEC 27001 defines requirements for information security management systems, encouraging a holistic approach to risk assessment, technical safeguards, and organizational policies (155, 156, 123). Its specific controls, such as those related to the secure disposal or reuse of equipment, require documented policies and procedures to ensure data removal, through encryption and secure wiping of storage media, and the recording of all disposal steps (129, 157).

The IEC 62443 series complements this framework by offering a security structure for automation and control systems, organized into categories covering concepts, policies, systems, and components (158, 159). Considering that these systems remain connected throughout the life cycle, the standard encourages the application of security measures in all phases, including deactivation and decommissioning. From this perspective, secure decommissioning in aeronautics involves not only data elimination but also the disconnection of keys and credentials, environmentally appropriate recycling of hardware, and compliance documentation to meet certification requirements (160, 120).

Aircraft certification processes, such as DO-178C and its complementary documents, establish that significant modifications or removals of systems cannot compromise the safety premises used in certification. Therefore, when decommissioning or replacing a system, it is essential to demonstrate that the aircraft continues to meet airworthiness requirements, including those related to cybersecurity. The integration of ISO 27001 requirements into certification processes ensures that both information security and automation aspects are considered (161, 162, 123).

In summary, the coordination of the phases of retrofits, obsolescence management, and secure decommissioning within the same chapter reveals the need for an integrated regulatory framework. DO-326A, DO-355A, and DO-356A direct interventions in embedded systems; ARINC and manufacturer policies structure obsolescence management; ISO/IEC 27001 provide comprehensive guidelines for information security and industrial control. Together with certification processes, these standards enable organizations to keep aircraft safe, resilient, and compliant throughout the life cycle (163, 164, 123, 57, 49, 50, 152).

3.3.5 Alignment with Avionics Certification Processes

The proposed holistc framework is not conceived as an isolated framework, but as an integrated process that generates evidence directly aligned with certification requirements in the aviation domain. Standards such as DO-178C and DO-254 establish rigorous guidance for the development and assurance of airborne software and hardware, respectively, mandating processes of verification, validation, and traceability that are essential for safety- critical systems (26, 42). By addressing phases such as threat analysis, risk management, control implementation, and continuous monitoring, the framework ensures that its deliverables can be reused as certification artifacts.

A central example of this alignment appears in the context of retrofits and system updates. According

to DO-254, any hardware modification requires a structured Change Impact Analysis to assess the potential effects on safety and compliance (42). The framework embeds change management activities that naturally produce such analyses, ensuring that recertification after retrofits or updates is supported by systematically generated documentation. This reduces the regulatory burden while ensuring that modifications remain consistent with certification objectives.

Beyond software and hardware assurance, cybersecurity standards play a vital role. DO-326A defines the processes for identifying and mitigating cyber risks throughout the avionics lifecycle, while DO-355A focuses on maintaining security for continued airworthiness and DO-356A provides technical measures for evaluating and mitigating cyberattacks (57, 49, 50). The outputs of the framework, such as threat models, mitigation plans, and incident response records—are fully compatible with the evidence required under these standards, strengthening both certification and operational resilience.

In addition, the framework integrates controls relevant to avionics data networks governed by ARINC specifications. ARINC 664 (AFDX) establishes the requirements for deterministic Ethernet-based communication in aircraft, while ARINC 429 specifies data transfer protocols for avionics subsystems (149, 143). The framework's structured documentation of communication security ensures that certification artifacts demonstrate not only functional compliance but also robustness against cyber threats at the network level.

Another dimension of alignment lies in traceability, a cornerstone of both DO-178C and DO-254. By ensuring that every security control and monitoring action is mapped to specific requirements and system components, the framework facilitates the generation of traceability matrices. These matrices can be directly used in certification audits to prove conformity with regulatory requirements, minimizing redundancy and ensuring efficient reuse of evidence across different lifecycle stages.

In summary, the framework consolidates certification alignment by producing artifacts that interact directly with mandatory processes. Rather than existing as a parallel structure, it supports compliance with DO-178C, DO-254, DO-326A/355A/356A, and ARINC specifications, providing evidence for recertification after retrofits and ensuring continuous conformity throughout the aircraft lifecycle. This guarantees that the framework enhances both the cybersecurity posture and the certification readiness of avionics systems.

3.3.6 Phase Mapping Matrix (Standards $\times$ Method Phases)

To make explicit the normative traceability of the *method phases*, independently of the modeling notation adopted, we present Table 3.12. This matrix establishes the direct correspondence between each phase and: (i) the families/controls of NIST SP 800-53 Rev. 5 (121), (ii) the themes and controls of ISO/IEC 27001:2022 and ISO/IEC 27002:2022 (123, 139), and (iii) the objectives/processes of the aeronautical standards DO-178C, DO-254, DO-326A, DO-356A, and DO-355A (26, 42, 49, 57, 50). The rationale for risk assessment and treatment that underpins the structuring of the phases follows the principles of ISO/IEC 27005:2022 (79).

Table 3.12: Phase Mapping Matrix (Standards × Method Phases)

Method Phase	NIST SP 800-53 (representative families/controls)	ISO/IEC 27001/27002 (relevant items/themes)	DO Objectives/Processes (DO-178C/254/326A/356A/355A)	Refs.
Threat Analysis	RA-1..RA-8 (Risk Assessment), CA-2/CA-7, SA-8, SR-2/SR-3	Risk management and threat intelligence; monitoring and vulnerabilities	DO-326A (SRA; requirements); DO-356A (*threat/attack* modeling)	(121, 79, 49, 57)
Secure Design	SA-3, SA-8, SA-11, SC-7, AC-3/AC-6, SR-5	Secure architecture, secure coding, configuration management, cryptography, project security	DO-178C/DO-254 (requirements, design, verification); DO-326A (architecture/mitigation)	(121, 123, 26, 42, 49)
Implementation of Security Controls	AC-, IA-, SC-, SI-, CM-, AU-, PE-, MP-	Access control, cryptography, monitoring, configuration management	DO-178C/254 (implementation + QA); DO-356A (cryptography, partitions, trusted channels)	(121, 123, 26, 42, 57)
Incident Monitoring & Response	AU-2/AU-6, IR-4/IR-5, SI-4, CA-7	Incident lifecycle; logging/monitoring	DO-326A (Operational Security); DO-355A (airworthiness)	(121, 123, 49, 50)
Integration with Risk Management	RA-, PM-, PL-2, CA-5	Context/risk/operation/performance evaluation; policies and ICT readiness	DO-326A (risk acceptance, *security credit*); CM/QA integration (DO-178C/254)	(121, 123, 79, 49, 26, 42)
Continuous Maintenance	MA-*, SI-2, CM-2/CM-3	Vulnerabilities, configuration management, continuity; training	DO-326A (bulletins/*patches*); DO-178C/254 (changes, traceability); DO-355A (*airworthiness*)	(121, 123, 49, 26, 42, 50)
Secure Decommissioning	MP-6, CM-8, PE-16, SC-12	Secure deletion, asset disposal/reassignment	DO-326A/DO-356A (sanitization and closure); DO-178C/254 (traceability)	(121, 123, 49, 57, 26, 42)

Source: Prepared by the author.

Assurance case derived from phase-based traceability. Beyond making explicit the normative coverage by method phase, Table 4.10 enables the construction of *assurance cases* grounded in the same traceability chain. In particular, Appendix H presents a GSN prototype for REQ-SEC-014, linking activities, controls (NIST SP 800-53; ISO/IEC 27001/27002), and evidence (EV-014; POAM) (121, 123, 139). This integration reduces ambiguity in demonstrating multi-standard conformity and facilitates the generation of auditable evidence throughout the life cycle (26, 42, 49, 57, 50).

3.3.7 Traceability and Audit Harmonization

Tables 3.12 and 4.1 establish a traceability chain that enables unequivocal demonstration of conformity to multiple frameworks with *a single evidence repository*:

Method phase → **Activity** → **NIST SP 800-53 Control** (121) ‖ **ISO/IEC 27001/27002 Item** (123, 139) ‖ **DO Objective** (26, 42, 49, 57, 50) → **Evidence** → **Status/Action**.

This structure harmonizes audit cycles because a single evidence artifact simultaneously covers NIST controls, ISO/IEC 27001/27002 items, and DO objectives/processes, thereby reducing redundancies and verification costs. Risk prioritization and treatment that feed the action plans are conducted according to ISO/IEC 27005:2022 (79), while gaps are managed via POAM (NIST CA-5) (121) and CM/QA mechanisms as provided in DO-178C/DO-254 (26, 42).

Operational elements of traceability. (i) *Unique evidence identifiers (EV-XXX)* linked to the rows of Tables 3.12 and 4.1; (ii) *Evidence catalog* with metadata (type, source, update frequency, owner, audit due date); (iii) *Change rule*: any change to an activity/phase implies updating the linkage to controls (bidirectional), with registration in CM; (iv) *Closure of nonconformities*: each finding references the corresponding risk (ISO/IEC 27005 (79)) and action plan (CA-5 (121)), preserving the chain through to the applicable DO objective (26, 42, 49, 57, 50).

Table 3.13: Evidence Registry (multi-standard crosswalk)

Phase/Activity	NIST SP 800-53	ISO/IEC 27001/27002	DO Objective	Evidence (ID, location, frequency, owner)	Status
Secure Development	SA-11, CM-3 (121)	A.8.28, A.8.9 (123, 139)	DO-178C: verification/coverage (26)	EV-012 *(code review checklist + test report; /evid/EV-012; monthly; owner: SW Eng.)*	Valid
Continuous Monitoring	SI-4, CA-7 (121)	A.8.16 (123)	DO-355A: continued airworthiness (50)	EV-021 *(SIEM dashboard + audit trails; /evid/EV-021; daily; owner: SecOps)*	Valid
Patch Management	SI-2, CM-4 (121)	A.8.8, A.8.9 (123, 139)	DO-326A: bulletins/changes (49); DO-254: CM (42)	EV-030 *(Bulletins + CR/PR + CM approval; /evid/EV-030; per release; owner: Config Eng.)*	In progress

Source: Prepared by the author.

3.3.8 Continuous Review and Improvement

To ensure long-term resilience, DO-355A mandates continuous security reviews throughout the operational lifecycle of avionics systems. These reviews involve security audits, penetration testing, and configuration management validation, ensuring compliance with evolving regulatory requirements and best practices (50).

Furthermore, ISO 31000 emphasizes ongoing risk management, integrating cybersecurity considerations into broader aviation safety strategies. This framework ensures that aviation organizations dynamically adapt their security measures to mitigate emerging threats and maintain compliance with industry standards (145).

3.3.9 End-of-Life in Avionics

In civil and military aviation, continued airworthiness demands that maintenance, retrofit, obsolescence planning, and secure decommissioning activities be not only systematic but also demonstrably compliant with recognized certification frameworks.

In this context, the evidence set `EV-050`–`EV-058`, originally defined in a domain-neutral manner, is aligned with domain-specific standards and assurance expectations. The security risk assessment principles of DO-326A (26), the operational continuity guidance of DO-355A (57), and the methodological safeguards defined in DO-356A (49, 50) provide a regulatory and technical basis for mapping maintenance and end-of-life activities into a certification-compatible framework. Additionally, software assurance considerations from DO-178C (42) complement this mapping by ensuring that any retrofit or software-related maintenance adheres to safety-critical development and verification requirements.

For instance, `EV-050` and `EV-051` (maintenance bulletins and regression checks) demonstrate conformance with DO-355A's requirements on continued operational suitability, while `EV-052` and `EV-053` (retrofit impact and V&V reports) can be directly associated with DO-178C verification objectives. Similarly, obsolescence governance artifacts (`EV-054`, `EV-055`) provide the traceability demanded by DO-326A's risk assessment obligations, and the secure decommissioning outputs (`EV-056`–`EV-058`) support DO-356A's emphasis on secure disposal and credential revocation.

This alignment ensures that the generic lifecycle closure is not only conceptually comprehensive but

also operationally recognized under the frameworks that govern avionics certification and oversight. By explicitly mapping EV-050–EV-058 to DO-326A, DO-355A, DO-356A, and DO-178C, the integrated framework extends its applicability from a generic systems-security context (123, 121) to a domain-specific regime where continued airworthiness and secure lifecycle termination are mandatory assurance objectives.

Table 3.14: EV-050–EV-058: mapping to NIST, ISO/IEC, and DO objectives (Integrated/Avionics)

Phase/Activity	NIST SP 800-53	ISO/IEC 27001/27002	DO Objective (aviation)	Evidence (ID, location, frequency, owner)	Status
Operational Maintenance (maintenance window)	CM-3/CM-4 (config. change), SI-2 (remediation), CA-7 (monitoring) (121)	A.8.9 (configuration), A.8.8 (vulnerabilities), A.8.16 (monitoring) (123, 139)	Demonstrate maintenance consistent with *continued airworthiness* (DO-355A); assess change risk (DO-326A) (57, 26)	EV-050 — Approved maintenance bulletin; repository: CM/SGI; freq.: per window; owner: Operations/CM	–
Regression checks & post-deployment	SI-2, CA-7, AU-12 (logs) (121)	A.8.15 (log records), A.8.16 (monitoring) (139)	Operational suitability (DO-355A) and, if SW is involved, verification objectives (DO-178C) (57, 42)	EV-051 — Pre/post checks and regression report; CM/QA; per window; QA/Operations	–
Retrofit — Impact analysis	RA-3 (risk assessment), CM-3, SA-11 (testing) (121)	Change and development/testing controls (A.8.*) (123, 139)	Security risk analysis (DO-326A) and evidence of operational suitability (DO-355A) (26, 57)	EV-052 — Impact report (interfaces/-timing/EMC); Systems Eng.; per change; Eng./GRC	–
Retrofit — V&V and CAB decision	SA-11, CA-2 (assessment), CA-7 (121)	Testing/acceptance/monitoring controls (A.8.*) (123, 139)	Verification/acceptance: DO-178C (if SW/FW), security methods: DO-356A, decision record for *continued airworthiness*: DO-355A (42, 49, 57)	EV-053 — V&V results + CAB minutes/decision; QA/CM; per change; QA/-GRC	–
Obsolescence — Plan and PHM	CM-8 (inventory), SR-6 (supply chain), RA-3 (121)	Asset, change, and technical risk management (A.5/A.8) (123, 139)	Sustainment planning with risk assessment (DO-326A) and evidence for *continued airworthiness* (DO-355A) (26, 57)	EV-054 — Obsolescence plan + *trade study*; Supply/CM; semiannual/annual; Supply/GRC	–
Updated inventory/CMDB	CM-8, CM-2/CM-3 (121)	A.8.9 (configuration), asset management (A.5/A.8) (123, 139)	Configuration control and traceability for airworthiness audits (DO-355A) (57)	EV-055 — CMDB/inventory updated; CM/SGI; continuous; CM/Ops	–
Disposal — Verified sanitization	MP-6 (media sanitization) (121)	A.8.10 (information disposal) (139)	Secure decommissioning and controlled disposal (DO-356A); logistical evidence for *continued airworthiness* (DO-355A) (49, 57)	EV-056 — Sanitization certificate + KMS logs; SecOps; per asset; SecOps/CM	–
Disposal — Chain of custody	MP-6; AU-12 (audit trail) (121)	A.8.10 (disposal), A.5 (policies/assignment) (123, 139)	Documentary proof of disposal/recycling for audit (DO-355A) and security (DO-356A) (57, 49)	EV-057 — Chain of custody + disposal/recycling form; Operations; per asset; Operations/GRC	–
Cryptographic offboarding — Revocation	SC-12/SC-13 (crypto/key management), IA-5 (credentials) (121)	A.8.24 (use of cryptography), A.8.15/8.16 (logs/-monitoring) (139)	Revocation/rotation and propagation of trust states per DO-356A; record for *continued airworthiness* (DO-355A) (49, 57)	EV-058 — Proof of revocation/propagation (CRL/OCSP, fleet telemetry); SecOps/PKI; per event; SecOps	–

Source: Prepared by the author.

3.4 THE INTEGRATED BPMN DIAGRAM

The integrated diagram was conceived based on BPMN (Business Process Model and Notation) to represent, in a clear and systematic way, the holistic framework for protecting embedded systems. Each "pool" corresponds to a major area of responsibility (e.g., systems engineering, risk management, operations, compliance), while the "lanes" describe specific tasks or subprocesses. The BPMN, ilustrated in Figure 3.7, ensures the representation of interactions, dependencies, and feedback loops, enabling a continuous improvement approach, in line with information security management standards (165).

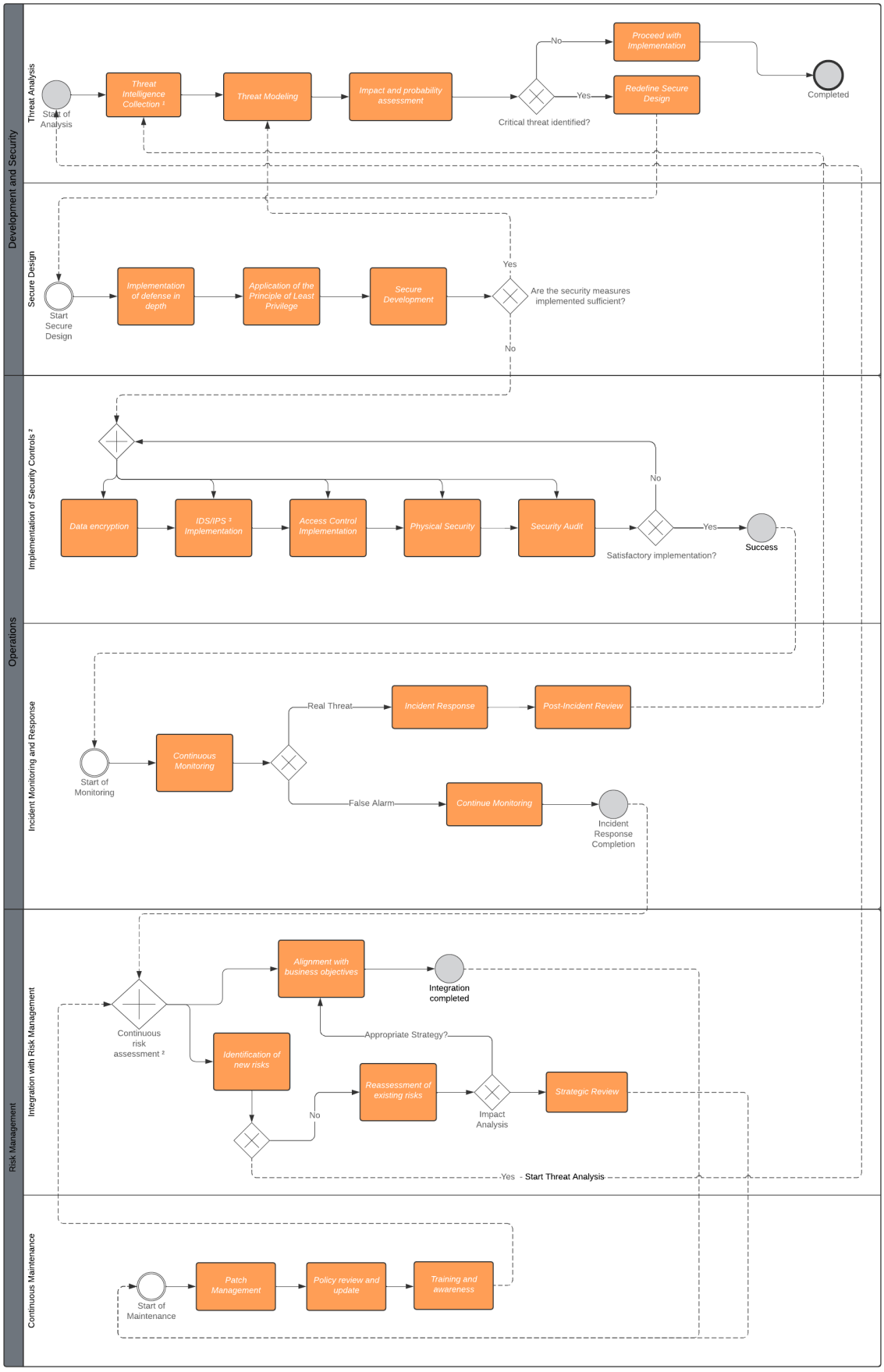

Figure 3.7: The Integrated BPMN Diagrams

The structure encompasses the full system life cycle: threat analysis, secure design, implementation of controls, monitoring and incident response, integration with risk management, continuous maintenance, and secure decommissioning. Each subprocess is detailed below with its inputs, activities, outputs, and connections to international standards.

3.4.1 Description of Main Components

This section, elucidates the BPMN diagram representing the security life cycle for embedded or safety-critical systems. Each pool, lane, step and decision is identified, as are the flows connecting one activity to another.

3.4.1.1 Pool "Development and Security"

Lane: Threat Analysis. The analysis begins with an initial event (a grey circle). The steps occur sequentially and are linked by direct arrows:

1. **Threat intelligence collection → Threat modelling → Impact and probability assessment**. The output of the latter stage is forwarded to a decision.
2. **Decision gateway: "Critical threat identified?"**
    - *No:* the arrow leads directly to **"Proceed with implementation"**, which in turn leads to the terminating event "*Completed*."
    - *Yes:* the arrow returns via a feedback flow to **"Redefine secure design."** This step connects, via a dashed line, to the beginning of the *Secure Design* phase, because the security requirements must be redefined before proceeding.

Lane: Secure Design. This begins with an event labelled **"Definition of safe design."** The activities are chained as indicated by arrows:

1. **Implementation of defence in depth → Application of the principle of least privilege → Secure development**.
2. After development, a decision follows: **"Are the security measures implemented sufficient?"**
    - *Yes:* the flow proceeds to the lane *Implementation of Security Controls*. This jump is represented by an arrow towards a gateway at the beginning of the next lane.
    - *No:* there is a return arrow (dashed line) to the *Threat Analysis* lane, indicating that new threats must be re-assessed and the design redefined.

Lane: Implementation of Security Controls. This lane begins at a gateway receiving the approved design. The activities follow sequentially:

1. **Data encryption → IDS/IPS implementation → Access control implementation → Physical security → Security audit**.

2. At the end of the audit there is a decision: **"Implementation satisfactory?"**

    - *Yes:* the flow proceeds to the final event "*Success*," concluding the development cycle.
    - *No:* a return arrow points back to the first gateway in this lane, indicating that the controls need to be reviewed and reapplied.

3.4.1.2 Pool "Operations"

Lane: Incident Monitoring and Response. The operational phase begins with an initiating event. The connections between activities are as follows:

1. **Start of monitoring** → **Continuous monitoring**.
2. The result of monitoring leads to a decision (gateway) that evaluates whether the alert is a *false alarm* or a *real threat*.

    - *False alarm:* the arrow leads directly to **"Continue monitoring,"** and then returns to the start of the *continuous monitoring* activity, forming a loop.
    - *Real threat:* the arrow proceeds through **Incident response** → **Post-incident review** → **Continue monitoring**. After this cycle, a terminating event marks the *completion of the incident response*.

3.4.1.3 Pool "Integration with Risk Management"

Integration lane. This pool integrates security into the corporate risk management processes. The connections are as follows:

1. **Start of integration** → **Continuous risk assessment** → **Identification of new risks** → **Reassessment of existing risks**.
2. A gateway then poses the question: **"Impact analysis / Appropriate strategy?"**

    - *Yes:* the arrow advances to **Alignment with business objectives**, which in turn is linked to the final event "*Integration completed*."
    - *No:* the arrow directs the flow to **Strategic review**. From this stage a return arrow leads back to **Reassessment of existing risks**, enabling iteration until an adequate strategy is identified.

3.4.1.4 Pool "Continuous Maintenance"

Lane: Continuous Maintenance. Maintenance begins at an initial event and traverses three aligned activities, interconnected by direct arrows:

1. **Patch management** → **Policy review and update** → **Training and awareness**.

At the end, an arrow connects the output of this lane back to the start of the *continuous risk assessment* lane in the *Integration with Risk Management* pool. This indicates that the maintenance activities feed the risk management process, closing the continuous improvement cycle.

3.4.2 Outputs and Feedback

Each subprocess not only feeds the subsequent phase but also establishes mechanisms for providing feedback to earlier ones, ensuring that the framework functions as a dynamic and adaptive cycle rather than a linear sequence. For instance, monitoring results generate actionable insights that directly influence risk management decisions and may trigger revisions in the implementation of security controls. Likewise, maintenance activities often uncover new vulnerabilities or configuration weaknesses, which can restart the threat analysis cycle and lead to updated secure design requirements.

At the end of the lifecycle, decommissioning processes provide valuable lessons learned regarding asset retirement, data sanitization, and cost-effectiveness of implemented safeguards; these lessons are systematically incorporated into the requirements and design of new systems. This continuous feedback loop reinforces the integration of security across all stages, promotes resilience against evolving threats, and consolidates the framework as a living process capable of adapting to technological changes, regulatory updates, and emerging adversarial tactics.

4 EVALUATION OF THE PROPOSED FRAMEWORKS

In the current landscape of increasing complexity and interconnection of embedded systems, particularly in critical sectors such as avionics, cybersecurity has become a paramount concern to protect digital assets and ensure operational continuity. To address the continuously evolving threat landscape, organizations have adopted holistic methodologies that combine international standards, sector-specific regulations, and global best practices. However, to ensure the effectiveness of these approaches, it is essential to develop robust evaluation metrics that can objectively and continuously measure their efficiency and adaptability (2).

During the course of this thesis, two holistic methodologies were developed: the comprehensive and the integrated approaches. The comprehensive framework focuses on applying general practices and widely recognized standards, such as ISO/IEC 27001 and NIST SP 800-53, which provide global guidelines for information security management and risk control. In contrast, the integrated framework incorporates these global standards while simultaneously aligning security practices with specific sectoral guidelines, such as DO-326A, DO-355A, DO-356A, DO-254, and DO-178C for aviation security. This combination allows for a more tailored approach adapted to the context of flight-critical operations, potentially enhancing effectiveness against targeted threats (123, 57, 49, 121, 50, 166, 26, 42).

To assess the effectiveness of these security methodologies, it is crucial to adopt an evaluation metric that considers a diverse range of criteria and performance indicators. The metric should measure compliance with standards and regulations, coverage of threats and vulnerabilities, operational efficiency, adaptability to new threats, and overall system resilience. The proposal to develop a comprehensive metric arises from the need to ensure that all critical dimensions of cybersecurity—such as airworthiness security, embedded software integrity, hardware assurance, and operational resilience—are covered in a balanced and integrated manner. For example, when evaluating compliance with standards, it is possible to verify not only adherence to regulatory requirements but also the alignment of practices with the aircraft certification process, ensuring compliance with DO-178C for software and DO-254 for airborne electronic hardware (167, 42).

Furthermore, the evaluation metric should integrate both quantitative and qualitative methods, allowing for a more thorough and comprehensive analysis. Quantitative methods, such as penetration testing, risk analysis, and software verification techniques required by DO-178C, provide empirical data that can be used to measure the effectiveness of implemented security controls. Meanwhile, qualitative methods, such as security audits, compliance assessments, and operational safety evaluations required by DO-355A, allow for the assessment of the maturity and effectiveness of security practices in avionics maintenance and operational environments. This combination of methods ensures that the evaluation metric is robust enough to capture the complexity of avionics systems and the dynamic nature of the cybersecurity threat environment (50, 2, 26).

The adoption of an evaluation metric for holistic methodologies, both comprehensive and integrated, should also emphasize the importance of continuous assessment. The cybersecurity environment is highly dynamic and requires that avionics security practices be regularly reviewed and improved. Therefore, an

effective metric should include mechanisms to continuously monitor the effectiveness of security methodologies, allowing for rapid adaptation to new threats and vulnerabilities. This is particularly relevant in airworthiness security, where compliance with DO-326A and DO-355A mandates ongoing risk assessments and periodic security updates to ensure that aircraft remain protected throughout their operational lifecycle (49, 50, 167).

Therefore, developing an appropriate evaluation metric for holistic security methodologies is a critical step to ensure that these approaches are both effective and adaptable. This metric should consider multiple dimensions of avionics security, integrate both quantitative and qualitative approaches, and emphasize the importance of continuous assessment. By adopting this integrated approach, aviation organizations will be better equipped to face the complex and evolving cybersecurity challenges that threaten aircraft safety and operational resilience.

To develop the evaluation metrics for the proposed holistic methodologies, the following sources were utilized:

Stallings, W., & Brown, L. (2018). *Computer Security: Principles and Practice (4th ed.). Pearson.* This book provides a solid foundation for understanding the fundamental principles of information security and security practices, including compliance methods with global standards such as ISO/IEC 27001 and NIST SP 800-53. It was instrumental in supporting the criteria for compliance with standards, threat coverage, and operational efficiency.

Whitman, M. E., & Mattord, H. J. (2022). *Principles of Information Security (7th ed.). Cengage Learning.* This source offers a comprehensive overview of best practices in information security, focusing on security management strategies, audits, training, and security awareness. It was used to underpin the criteria of organizational security culture, adaptability, resilience, and the importance of feedback and continuous improvement.

Tipton, H. F., & Krause, M. (2017). *Information Security Management Handbook (7th ed.). CRC Press.* This source was employed to consolidate the importance of continuous improvement and the adaptation of security practices based on audits, reviews, and feedback. The handbook provides detailed guidance on integrating continuous feedback to ensure the effectiveness of security practices and discusses methods for auditing and monitoring to validate the effectiveness of security methodologies.

These sources provided the theoretical foundation necessary to develop a comprehensive evaluation metric that encompasses various criteria and both qualitative and quantitative methods for assessing security methodologies, such as compliance with standards, threat coverage, operational efficiency, adaptability, organizational culture, and continuous improvement.

4.1 EVALUATION METRIC FOR COMPREHENSIVE HOLISTIC FRAMEWORK

The comprehensive holistic framework for the security of embedded systems is based on the application of widely recognized standards and general practices, such as ISO/IEC 27001 and NIST SP 800-53, to create a robust and effective cyber protection framework. In order to assess the effectiveness of this

approach, it is necessary to adopt a metric that considers the various aspects that contribute to the security of critical systems.

The following describes the fundamental criteria, performance indicators and data collection methods specific to the comprehensive framework.

1. Compliance with Global Standards

   The criterion used was to verify whether the framework complies with global standards and regulations that define best security practices, such as ISO/IEC 27001 and NIST SP 800-53. Compliance ensures that the framework adheres to rigorous information security standards, establishing adequate controls to mitigate risks.

   Performance indicators:

   - Percentage of compliance with all the mandatory controls of the ISO/IEC 27001 and NIST SP 800-53 standards.
   - Frequency of internal and external compliance audits.
   - Number of non-conformities and recommendations resulting from audits.

   Data collection methods:

   - Periodic audits conducted by internal teams or independent certifiers.
   - Review of compliance documentation, such as audit reports and incident logs.
   - Interviews with compliance managers and information security professionals.

2. Coverage of Generic Threats and Vulnerabilities

   For this criterion, the framework must be effective in identifying and mitigating common vulnerabilities, covering a wide range of threats, from known cyberattacks to new emerging vulnerabilities. Threat coverage must be constantly reviewed to ensure that the framework not only reacts to existing threats, but also incorporates predictive assessment processes, using threat intelligence to anticipate new types of attacks and vulnerabilities.

   Performance Indicators:

   - Number of vulnerabilities corrected in relation to the total number of vulnerabilities identified.
   - Average response time to a detected threat (MTTD and MTTR).
   - Frequency and results of penetration tests and security scans.

   Data collection methods:

   - Vulnerability scan reports carried out by automated tools such as security scanners.
   - Analysis of security incident reports and incident response logs.
   - Penetration tests conducted regularly to identify new vulnerabilities.

3. Operational Efficiency in the General Context

   Operational efficiency measures how the framework impacts the organization's daily operations. Security must be implemented in such a way as not to jeopardize workflows or business continuity, balancing protection with efficiency. The evaluation should include long-term monitoring of the impact of implemented security controls, checking whether the solutions remain effective or need to be revised to meet new operational or infrastructure challenges.

   Performance indicators:

   - Reduction in average operational downtime due to the implementation of new security controls.
   - Total cost of maintaining and updating security systems, compared to the allocated security budget.
   - Impact on business processes during the implementation of controls, such as downtime or rework.

   Data collection methods:

   - Financial reports detailing security costs and investments in risk mitigation technologies.
   - Monitoring of operational efficiency indicators, such as incident response times or staff overload.
   - Interviews with IT managers and business leaders to analyze the impact of security on workflow.

4. Adaptability and Resilience to Diversity of Threats

   The framework must be able to adapt quickly to new threats and failures, while maintaining the integrity and continuous operation of the systems. Adaptability must be reinforced by the implementation of continuous monitoring processes that enable detection and response to incidents, minimizing reaction time and improving resilience.

   Performance Indicators:

   - Number of security updates successfully implemented following the detection of new threats.
   - Average recovery time of critical systems after cyber attacks or technical failures.
   - Reduction in the impact of new types of attacks or emerging vulnerabilities after adapting controls.

   Data Collection Methods:

   - Reports on changes and updates to security systems.
   - Post-incident audits that verify the effectiveness of recovery measures.
   - Interviews with cyber security teams to understand how emerging threats have been dealt with and mitigated.

5. Generalist Organizational Safety Culture

   Organizational safety culture is assessed through employee engagement with safety practices, including participation in training and commitment to established policies. Safety culture should include gamification mechanisms to improve employee engagement, as well as recognition programs that encourage adherence to best safety practices.

   Performance indicators:

   - Percentage of employees who regularly participate in security training and updates.
   - Number of security incidents attributable to human error or failure to comply with policies.
   - Results of security awareness assessments carried out with all employees.

   Data collection methods:

   - Surveys and questionnaires for employees on their perception of and involvement with cyber security.
   - Analysis of security incidents to determine the root cause related to human failings.
   - Reports on participation in training and the effectiveness of awareness programs.

6. Feedback and Continuous Improvement in General Security Practices

   The framework should include a continuous cycle of feedback and improvements, based on audits, incidents and policy reviews, ensuring that security practices are always up-to-date and effective. Continuous improvement should be accompanied by metrics on the effectiveness of each adjustment or improvement implemented, ensuring that each change has a measurable positive impact on overall security.

   Performance indicators:

   - Frequency of reviews of security policies and procedures.
   - Number of improvements implemented based on feedback from audits and lessons learned from incidents.
   - Average time between internal audits and implementation of recommended improvements.

   Data collection methods:

   - Internal and external audit reports.
   - Stakeholder feedback and post-incident analysis.
   - Security policy reviews and documentation updates.

The evaluation metric for the comprehensive holistic framework has been supplemented to include a more detailed and comprehensive analysis of all critical security dimensions, specifically focusing on compliance with aviation-specific standards such as DO-178C for software, DO-254 for hardware, and DO-355A for maintenance security.) By incorporating regulatory compliance, threat coverage, operational

efficiency, adaptability, security culture, and continuous improvement, this metric offers a complete and detailed view of the effectiveness and sustainability of security practices. Structured data collection through security audits (aligned with DO-355A requirements), penetration testing, compliance evaluations (DO-178C/DO-254), operational feedback, and continuous monitoring (aligned with DO-326A) ensures that the assessment is objective, practical, and capable of identifying areas for continuous improvement, keeping embedded avionics systems resilient against evolving cyber threats.

In addition, this metric enables a proactive response to emerging threats, providing an essential tool for adapting security policies and practices in real time. Through continuous assessment and dynamic responsiveness, the organization can not only react quickly to security incidents, but also improve its ability to prevent future attacks, creating a virtuous cycle of defence and resilience. Integrating compliance and adaptation practices into the organizational culture also promotes greater stakeholder involvement, ensuring that security is understood and applied at all levels of the company.

This integrated and multidimensional approach provides a solid basis for strategic decision-making in relation to cyber security, promoting effective alignment between day-to-day operations and global security best practices. By prioritizing resilience, adaptation and continuous improvement, the metric not only strengthens cyber defences, but also makes the organization better prepared to face future challenges, ensuring sustainable, long-term protection for critical embedded systems.

4.2 EVALUATION METRIC FOR AN INTEGRATED HOLISTIC FRAMEWORK

The integrated holistic framework for embedded systems security goes beyond the application of general standards, combining widely recognized international standards (such as ISO/IEC 27001 and NIST SP 800-53) with sector-specific standards, including DO-178C, DO-254, DO-326A, DO-355A, and DO-356A for the aerospace sector. This approach aims to address the specific needs of each sector by adapting global best practices to the organization's unique requirements. The following outlines the fundamental criteria, performance indicators, and data collection methods for evaluating the integrated framework.

1. Compliance with Global and Sector-Specific Standards

   This criterion assesses the framework's compliance with global standards, such as ISO/IEC 27001 and NIST SP 800-53, as well as sector-specific standards like DO-178C (software certification for airborne systems), DO-254 (hardware certification), DO-326A (cybersecurity management for aviation), DO-355A (information security for continued airworthiness), and DO-356A (mitigating cyber-attacks in aviation systems). Compliance with sector-specific standards should be monitored through regular security practice review reports to ensure that new regulations and industry-specific requirements are incorporated promptly.

   Performance Indicators:

   - Percentage of compliance with global and sector-specific standards (ISO/IEC 27001, DO-178C, DO-254, DO-326A, DO-355A, etc.).

- Frequency of internal and external audits verifying compliance with industry-specific standards.
- Number of non-compliance findings in audits.

Data Collection Methods:

- Audits conducted by cybersecurity certification bodies and sectoral compliance specialists.
- Review of reports and records documenting compliance with aerospace industry standards.
- Interviews with compliance managers and operational teams to verify the implementation of sector-adapted policies.

2. Coverage of Global and Sector-Specific Threats

   The integrated framework must be capable of identifying, mitigating, and responding to both global and sector-specific threats. In the aviation sector, for instance, besides traditional cyber threats such as phishing and malware, specific threats related to physical security and control of critical systems must be addressed. Threat coverage evaluation should incorporate intelligence on sector-specific threats and proactive practices to mitigate new types of attacks that could directly affect embedded systems in sectors like aerospace.

   Performance Indicators:

   - Number of sector-specific threats and vulnerabilities (such as interference in flight control systems) identified and mitigated.
   - Mean Time to Response and Recovery (MTTR) following a sector-specific incident.
   - Frequency and effectiveness of penetration tests and simulations of industry-specific cyberattacks.

   Data Collection Methods:

   - Simulations of sector-specific attack scenarios (e.g., failures in critical aircraft systems).
   - Vulnerability reports including both global and sector-specific threats.
   - Post-incident analysis of attacks involving critical systems.

3. Operational Efficiency in the Sectoral Context

   The integrated framework should be implemented efficiently, minimizing the impact on daily operational processes while meeting specific sectoral requirements, such as continued airworthiness and the security of critical systems. Operational efficiency should be tracked by cybersecurity impact assessments, ensuring that sector-specific security measures are implemented and monitored while maintaining operational continuity and safety.

   Performance Indicators:

   - Average time required to implement new sector-specific security controls without compromising operational continuity.

- Reduction in operational impact caused by introducing security measures, particularly in critical systems.
- Total cost of ownership (TCO) of security controls, considering sector-specific requirements.

Data Collection Methods:

- Operational reports detailing the impact of security changes on critical systems.
- Monitoring of operational efficiency indicators, such as downtime and productivity metrics.
- Interviews with operations and IT managers to assess the impact of security measures within the sector.

4. Adaptability and Resilience in Sectoral Environments

   This criterion evaluates the framework's ability to adapt quickly to new threats, incorporating both global and emerging sector-specific threats. Resilience measures an organization's ability to continue operating securely despite attacks or failures, while adaptability assesses the framework's flexibility to evolve and respond to technological changes or emerging threats. Sectoral resilience must be strengthened with incident response strategies incorporating standards like DO-355A to ensure continued airworthiness, even under cyberattack scenarios.

   Performance Indicators:

   - Time required to adapt security controls following the identification of new sector-specific threats.
   - Capability to respond to and recover from incidents in critical systems.
   - Efficiency of business continuity and disaster recovery procedures in industry-specific systems.

   Data Collection Methods:

   - Logs and reports from sector-specific incidents.
   - Post-incident audits to evaluate the effectiveness of responses and recovery measures in critical systems.
   - Simulations of industry-specific threats and analysis of system resilience to such threats.

5. Sectoral Organizational Security Culture

   This criterion assesses employees' adherence to security policies adapted to the sector, considering training and awareness programs that address both global standards and industry-specific requirements, such as the security of critical systems in aircraft. The security culture should include sector-specific evaluations, with training tailored to cover industry-specific threats and standards, such as those related to DO-178C, DO-254, DO-326A, and DO-356A.

   Performance Indicators:

   - Percentage of employees trained in sectoral and global security.

- Number of security incidents attributed to human errors or lack of adherence to sector-specific policies.
- Results of security awareness assessments focused on the sector.

Data Collection Methods:

- Training reports including participation and results of awareness assessments.
- Interviews and surveys with employees to verify their understanding of sector-specific security.
- Analysis of incidents related to human errors in critical systems.

6. Feedback and Continuous Improvement in Sectoral Practices

   The framework must incorporate mechanisms for continuous feedback and the implementation of improvements based on audits, incidents, and reviews, ensuring that security practices remain up-to-date in relation to new sector-specific challenges. Continuous improvement should align with recommended practices from sectoral standards, including proactive improvements based on feedback from past incidents and regulatory changes.

   Performance Indicators:

   - Number of improvements implemented based on feedback and sector-specific audits.
   - Frequency of sectoral policy reviews based on standards such as DO-355A.
   - Average time taken to adapt to regulatory changes or new sectoral requirements.

   Data Collection Methods:

   - Internal and external audit reports focused on sectoral compliance.
   - Feedback from stakeholders, especially critical systems operation teams.
   - Monitoring of reviews and updates to sectoral security policies.

The evaluation metric for the integrated holistic framework offers a comprehensive and balanced analysis, encompassing both globally recognized standards and specific guidelines for critical sectors such as aerospace. With criteria assessing regulatory compliance, threat coverage, operational efficiency, adaptability to new threats, organizational security culture, and continuous improvement mechanisms, the metric provides a thorough approach to measuring the effectiveness of security practices.

By integrating global standards like ISO/IEC 27001 and NIST SP 800-53 with sector-specific standards such as DO-178C, DO-254, DO-326A, DO-355A, and DO-356A, the metric ensures that embedded systems are prepared to address both common cyber threats and those unique to highly critical sectors such as aerospace. This integrated approach allows organizations not only to meet regulatory requirements but also to enhance the resilience of their systems against emerging threats, ensuring compliance with stringent safety and security regulations while fostering greater agility in adapting to new challenges.

Furthermore, by offering a strategic and operational perspective on security, the metric fosters a sustainable security culture, engaging all organizational levels and encouraging continuous improvement of

the implemented practices. Through this evaluation, organizations can align cybersecurity protections with sector-specific needs, ensuring compliance with DO-178C for software certification, DO-254 for hardware security and cybersecurity frameworks such as DO-326A, DO-355A, and DO-356A for airworthiness security. This comprehensive approach creates a proactive and robust security environment capable of mitigating risks in an increasingly complex and dynamic threat landscape while ensuring system integrity, operational safety, and regulatory adherence in aerospace applications.

4.3 A COMPARATIVE ANALYSIS

It is understood that the adoption of holistic security methodologies is fundamental to protecting embedded systems against a wide range of cyber threats, especially in critical sectors such as aerospace. However, the effectiveness of these methodologies depends on careful evaluation, which must be carried out using robust evaluation metrics. In this chapter, a comparison will be made between the evaluation metrics developed for the holistic comprehensive and integrated methodologies, highlighting their differences, strengths, and limitations. The analysis will help to understand how each metric adapts to different contexts and security requirements.

Compliance with Standards and Regulations

Compliance with standards and regulations is a key criterion for both metrics, but with different emphases. The metric for the comprehensive framework focuses on compliance with global standards, such as ISO/IEC 27001 and NIST SP 800-53, which offer broad guidelines applicable to various industries. The metric for the integrated framework includes, in addition to global standards, compliance with sector-specific standards, such as DO-178C (software considerations in airborne systems), DO-254 (design assurance for airborne electronic hardware), DO-326A (cybersecurity management for aviation), DO-355A (information security for continued airworthiness), and DO-356A (mitigating cyber-attacks in aviation systems), which are essential for sectors with stringent safety requirements, such as aerospace (2).

This difference is reflected in the performance indicators: while the comprehensive metric checks the percentage of compliance with global standards and the occurrence of non-conformities in internal and external audits, the integrated metric also assesses compliance with sector standards, which increases the scope and complexity of the assessment. The inclusion of specific sector standards in the integrated framework ensures that safety is not only comprehensive but also adapted to the operational and regulatory particularities of the sector.

Threat and Vulnerability Coverage

Both metrics emphasize the importance of covering a wide range of threats and vulnerabilities, but the way this coverage is evaluated varies between the two approaches. In the comprehensive framework, the metric measures effectiveness in identifying and mitigating common cyber threats such as malware, phishing, and DDoS attacks, reflecting a generalist approach to security. This approach is suitable for organizations that need to protect their systems from widely known and standardized threats.

On the other hand, the integrated framework metric goes further, also incorporating the identification

and mitigation of sector-specific threats, such as attacks that compromise the integrity of flight control systems or exploit vulnerabilities in critical aircraft systems. This is key to ensuring that all possible attack vectors are covered, including emerging and sophisticated threats that may not be considered in the global standards (166).

Operational Efficiency

Operational efficiency is an essential criterion for measuring the impact of implementing security practices on the organization's daily operations. In the metric for the comprehensive framework, operational efficiency is evaluated based on the overall impact of security practices on business processes, such as incident response time and total cost of ownership of security controls. This metric is more suitable for organizations looking to balance security with efficiency and cost-effectiveness.

In the integrated framework, the operational efficiency metric considers not only the impact on general operations but also the continuity of critical systems and compliance with specific operational requirements, such as continued airworthiness. This means that, as well as assessing the impact on business processes, the integrated metric also checks the ability to keep critical operations running safely, even under pressure from cyber incidents or technical failures. Compliance with DO-178C and DO-254 ensures that both software and hardware development align with operational efficiency requirements (167).

Adaptability and Resilience

Adaptability and resilience are criteria that measure the framework's ability to quickly adjust to new threats and maintain the security of systems even under attack. The metric for the comprehensive framework assesses the overall ability to adapt to new threats and the efficiency of the response and recovery mechanisms implemented. This includes the frequency of security updates and the time taken to apply patches and corrections in response to new vulnerabilities.

In the integrated framework, adaptability and resilience are assessed with a focus on sector-specific threats, considering not only the application of security patches but also the ability to respond to incidents affecting critical systems, such as aircraft control systems or navigation devices. This sector focus allows for a faster and more effective response to complex incidents, ensuring the continuity of critical operations, which is essential in highly regulated and security-sensitive environments. Compliance with DO-178C and DO-254 enhances resilience by ensuring that all system components are designed with security and adaptability in mind (2, 26, 42).

Organizational Security Culture

Organizational security culture is a criterion that measures the organization's commitment to cybersecurity, covering employee awareness and training. The metric for the comprehensive framework focuses on measuring the effectiveness of general security awareness programs, evaluating the percentage of employees trained and the reduction in incidents due to human error.

In the integrated framework, the security culture metric is more specific, evaluating employees' understanding of industry standards and practices. This includes specific training on how to handle critical systems and respond to incidents that could compromise the safety of embedded systems in sectors such as aerospace. Ensuring compliance with DO-178C and DO-254 requires continuous training of engineers and operators in secure development practices, further strengthening security awareness and adherence to

best practices.

Feedback and Continuous Improvement

Continuous improvement is fundamental to the sustainability of security practices. In the comprehensive framework, the feedback and continuous improvement metric evaluates the frequency and effectiveness of reviews of security policies and practices, ensuring that lessons learned from incidents are proactively incorporated.

In the integrated framework, the continuous improvement metric also considers adaptation to industry-specific regulatory and operational changes, ensuring that the organization not only responds to incidents but also anticipates changes that could affect compliance and operational safety. This approach ensures that the organization keeps up to date with best practices and that policies and controls are reviewed dynamically and in line with new industry requirements. Compliance with DO-178C and DO-254 requires iterative improvements and validation to ensure security is continuously refined throughout the system lifecycle.

4.3.1 Lessons Learned

The lessons learned indicate that the comprehensive framework offers a broad and general security framework, ensuring compliance with global standards such as ISO/IEC 27001 and NIST SP 800-53, which establish essential security controls applicable across multiple industries. This framework is effective in addressing common cybersecurity threats, such as malware, phishing, and DDoS attacks, and in optimizing operational efficiency through cost-effective security measures. However, due to its generalist nature, it lacks sector-specific depth, which may limit its application in highly regulated environments that require adherence to strict safety and airworthiness regulations.

In contrast, the integrated framework provides a specialized security approach tailored to critical sectors such as aerospace, where cybersecurity must align with strict safety and compliance standards. This framework extends beyond general security controls by integrating sector-specific standards such as:

- **DO-178C** (Software Considerations in Airborne Systems) – ensuring that security and functional safety are incorporated into airborne software development and verification.
- **DO-254** (Design Assurance for Airborne Electronic Hardware) – ensuring that hardware security aligns with aviation safety requirements, preventing vulnerabilities in critical avionics components.
- **DO-326A** (Cybersecurity Management for Aviation) – establishing a structured approach to cyber risk management in airborne systems.
- **DO-355A** (Information Security for Continued Airworthiness) – ensuring that aircraft security remains robust throughout its operational lifecycle.
- **DO-356A** (Mitigating Cyber-Attacks in Aviation Systems) – providing specific defensive measures to counter cyber threats against onboard and communication systems.

By incorporating these sector-specific regulations, the integrated framework ensures that security does

not compromise safety or operational resilience, which is essential in aviation and other safety-critical environments.

The primary distinction between the two methodologies lies in their scope and applicability:

- The comprehensive framework is ideal for general embedded systems security, ensuring broad compliance with global security standards while maintaining flexibility across multiple industries.
- The integrated framework is critical for mission-critical embedded systems, where cybersecurity, airworthiness, and functional safety must be seamlessly integrated within a highly regulated, high-risk operational context.

This comparative analysis reinforces that while the comprehensive framework provides broad security coverage, only the integrated framework ensures compliance with industry-specific safety and operational constraints. In sectors such as aerospace, where both cybersecurity and functional safety must coexist, the adoption of DO-178C, DO-254, DO-326A, DO-355A, and DO-356A is indispensable for achieving high-assurance security and regulatory compliance.

4.4 EXPLICIT LINK BETWEEN THE METHOD PHASES AND THE MODELED PROCESS

The operational process modeled in this section constitutes the concrete instantiation of the *method phases* previously defined in *framework*. To preserve the generality of the method and, at the same time, make compliance "black-and-white," we established bidirectional traceability between (i) the method phases (mapped in Table 3.12) and (ii) the *activities* of the process described here. The logic for risk assessment and prioritization that links the activities follows the principles of ISO/IEC 27005:2022 (79), while the implementation and verification of controls are grounded in NIST SP 800-53 Rev. 5 (121), ISO/IEC 27001/27002:2022 (123, 139), and the aeronautical DO standards (with emphasis on DO-178C, DO-254, DO-326A, DO-356A, and DO-355A) (26, 42, 49, 57, 50).

Table 4.1 makes explicit the connection between each *activity* of the modeled process and the corresponding normative controls/objectives, enabling auditing, verification, and maintenance with direct traceability (activity control/objective).

Table 4.1: Mapping Matrix by Activity (BPMN × NIST SP 800-53 × ISO/IEC 27001/27002 × DO Standards)

Activity (BPMN)	NIST SP 800-53	ISO/IEC 27001/27002	DO Standards	Refs.
Threat Intelligence Collection	RA-3/RA-5, PM-15, CA-7	Threat intelligence, continuous monitoring	DO-326A (inputs for SRA); DO-356A (use of threat intel)	(121, 79, 49, 57, 11)
Threat Modeling	SA-8, RA-3, SR-2, CA-2	Secure architecture; security in projects	DO-326A (security requirements/architecture); DO-356A (*attack trees*/DFD)	(121, 123, 49, 57, 19)
Impact and Probability Assessment	RA-2/RA-3, PM-9	Risk assessment and treatment; feedback through monitoring	DO-326A (severity vs. likelihood; acceptance criteria)	(121, 79, 49)
Implementation of Defense in Depth	SC-7, SC-5, AC-3, SI-7	Secure engineering principles; configuration management	Partitioning/architecture (DO-326A); layered controls (DO-356A)	(121, 123, 49, 57)
Principle of Least Privilege	AC-6, AC-2, IA-2/IA-5	Access controls (authentication/authorization)	Authorization and segregation; review evidence (DO-178C)	(121, 123, 26)
Secure Development	SA-3, SA-11, SI-10, CM-3	Secure coding; security in projects; configuration	Development/verification objectives (DO-178C); HW design (DO-254)	(121, 123, 26, 42)

Activity (BPMN)	NIST SP 800-53	ISO/IEC 27001/27002	DO Standards	Refs.
Data Encryption	SC-12/SC-13, SC-28, IA-7	Use of cryptography; key management	Cryptographic methods and key management (DO-356A)	(121, 123, 57)
Access Control Implementation	AC-2/AC-3/AC-6, IA-2/IA-5, SC-23	Access; secure configuration	Access mechanisms; traceability/QA (DO-178C)	(121, 123, 26)
Security Audit / Logging	AU-2, AU-6, AU-8, CA-2	Logging and monitoring	V&V and audits; CM/QA (DO-178C/254)	(121, 123, 26, 42)
Continuous Monitoring	SI-4, CA-7, AU-6	Continuous monitoring	Continued Airworthiness (DO-326A/DO-355A)	(121, 123, 49, 50)
Incident Response	IR-4/IR-5, AU-6, SI-4	Incident cycle (assessment, response, lessons)	Operational response; testing/forensics (DO-356A)	(121, 123, 57)
Post-Incident Review	IR-8, PM-6, CA-5	Learning from incidents; improvement	Continuous improvement and evidence (DO-326A/DO-355A)	(121, 123, 49, 50)
Patch Management	SI-2, CM-3/CM-4, MA-2	Technical vulnerabilities; configuration	Bulletins/change management (DO-326A); CR/PR/CM (DO-178C/254)	(121, 123, 49, 26, 42)
Training and Awareness	AT-2/AT-3, PS-7	Training and security awareness	Operational readiness (training evidence)	(121, 123, 49)
Data Sanitization (Decommissioning)	MP-6, SC-12, CM-8	Secure deletion; asset disposal/reassignment	Sanitization/termination (DO-326A/DO-356A)	(121, 123, 49, 57)
Asset Inventory, Recycling/Destruction	CM-8, MP-2/MP-6, PE-16	Asset inventory; return and disposal	Inventory update and secure termination (DO-326A)	(121, 123, 49)

Source: Prepared by the author.

From BPMN to assurance case evidence. The activity/BPMN mapping in Table 4.1 operationally indicates which artifacts are produced or consumed at each step of the workflow, allowing the chaining of *detection* $\rightarrow$ *correction* $\rightarrow$ *verification* with direct traceability to the RTM and to control elements (NIST/ISO/DO). Based on this chaining, Appendix H materializes a prototypical *assurance case* (REQ-SEC-014), demonstrating how EV-014 and the POAM consolidate a structured and auditable argument (121, 123, 139, 26, 42).

During thematic audits (e.g., ISO/IEC 27001/27002 (123, 139)) or sector-specific audits (DO-178C/DO-254/DO-326A/DO-356A/DO-355A (26, 42, 49, 57, 50)), the team demonstrates compliance starting from Table 4.1: the sampled activity is selected, the corresponding NIST control(s) (121) and the related ISO item or DO objective are consulted, and the artifact EV-XXX is presented in the Evidence Register (Table 3.13). Findings feed into risk assessment and treatment according to ISO/IEC 27005 (79) and POAM (CA-5) (121), ensuring end-to-end traceability and controlled closure.

The adoption of BPMN enabled a clear and systematic visualization of these processes, ensuring logical consistency, operational efficiency, and alignment with best practices. The expanded diagram consolidates the framework as a practical reference for implementing, monitoring, and continuously improving protection strategies for embedded systems against malicious attacks.

4.5 VALIDATION OF THE FRAMEWORK

Validating the proposed holistic framework for protecting embedded systems is essential to assess its applicability, effectiveness and alignment with real-world requirements, especially in highly regulated and critical sectors such as aerospace. The assessment of methodologies aimed at the security of embedded systems requires not only verifying compliance with standards and best practices, but also analysing the perceptions and experiences of specialists who deal directly with the challenges of the sector.

In this context, qualitative and quantitative analysis emerges as an essential tool for understanding

the depth and complexity of technical judgements, providing insights that go beyond quantitative data and reveal aspects often invisible to mere statistical measurement. Such an approach is especially recommended when seeking to test the effectiveness of technical methodologies in real professional contexts (168, 169, 170).

For this purpose, a team of cybersecurity and embedded systems specialists analysed a diagram drawn up on the basis of the proposed holistic framework and, from this analysis, answered a questionnaire. When analysing the diagram, the specialists used it as a structured assessment tool, illustrating how the framework integrates security controls, mitigation strategies and compliance requirements. This type of approach follows evaluation principles employed in literature reviews, such as those defined by Okoli and Schabram, who emphasise the need for transparent and reproducible processes in the selection and extraction of relevant information (171).

This chapter aims to interpret, categorise and critically discuss the answers obtained through a structured questionnaire answered by specialists in the cybersecurity of embedded systems. The qualitative approach adopted follows methodological principles that advocate coding and the identification of recurring patterns as instruments for building analytical understanding. The fundamentals of thematic analysis were also used, allowing analytical categories to be derived from the data (172, 173).

To this end, a validation process was conducted with specialists, anchored in international normative references and structured into eight thematic axes that reflect the essential dimensions of embedded security (174, 175).

4.5.1 Sample Composition

The sample consisted of 10 specialists with extensive experience in sectors sensitive to embedded security, such as defence, transport and critical infrastructure. The selection was conducted by means of purposive sampling, an acceptable criterion in qualitative-quantitative studies with a technical focus (176).

The ten specialists who made up the sample in this study have a senior technical profile, with a strong presence in the defence and aerospace sectors, belonging to a specific embedded systems development department of Airbus Defence and Space, located in Manching, Germany. Most work as *Cyber Security Architects*, a strategic role in the design and implementation of secure architectures for critical systems such as satellites, command and control systems, guided missiles and space and ground communications infrastructures.

These professionals have solid backgrounds in Computer Engineering, Electrical Engineering or Computer Science, and accumulate significant experience with military and civil embedded systems, working directly with security standards such as ISO/IEC 27001, NIST SP 800-53, RTCA DO-326A and DO-355, among others.

In addition, the specialists demonstrate familiarity with risk modelling and cryptographic security, developing concepts such as incident response plans, backup and recovery policies, defence-in-depth strategies and the integration of legal requirements in regulated environments. This highly qualified profile ensures a validation process that adheres to the operational reality of mission-critical systems, as advo-

cated by Hevner et al.(170) when justifying the use of specialists with domain expertise for the validation of technical artefacts.

This composition of the sample is also aligned with methodological guidelines for validation by specialists in software engineering (177), which highlight the importance of applied experience in real contexts as a criterion for the reliability of the data collected.

4.5.2 Data Collection Instrument

A structured questionnaire with 30 questions was developed, written in technical English. The combined use of multiple-choice questions, both with single and multiple selections, makes it possible to capture not only the specialists' preferred answer but also the recognition of multiple relevant dimensions in certain analytical categories. This strategy is especially useful in technical-qualitative studies in which the same concept can be associated with various practical or normative perspectives (170, 177).

In addition, the use of closed alternatives ensures greater uniformity in statistical analysis, facilitating the measurement of the degree of agreement among participants and comparability between thematic axes, as recommended by empirical validation guidelines in software engineering and information security (178).

Complementarily, the application of 4- and 5-point Likert scales made it possible to quantify subjective perceptions with sensitivity appropriate to the nuances of the specialists' opinions. The 5-point scale, traditional in applied social research, offers a balance between discrimination and simplicity of response, while the 4-point scale, by eliminating the neutral option, forces more assertive decisions in contexts where technical judgement is required (179, 180).

Finally, the inclusion of items geared towards perception, effectiveness, applicability, integration and barriers seeks to encompass complementary dimensions which, although not always formalised in standards, are critical for the real adoption of methodologies in embedded systems. This holistic approach allows both the technical validity and the organisational feasibility of the proposal to be captured (181, 182).

The questions were organised into eight thematic axes, with the related questions as shown in Table 4.2. The thematic segmentation facilitates analysis according to distinct criteria, such as normative coverage, adaptability, life cycle and practical barriers, promoting greater clarity in identifying the proposal's strengths and gaps (170, 177).

Table 4.2: Thematic axes analysed in the validation of the framework

Axis	Topic analysed	Related questions
A1	Coverage of security requirements	1
A2	Adaptation to different scenarios	2, 28, 29
A3	Coverage of the system life cycle	3
A4	Efficiency in detection and response	4, 5, 6, 7, 8, 9
A5	Resilience and recovery	10, 11, 12, 13
A6	Integration with normative frameworks	14, 15, 16, 17, 18
A7	Operational benefits	23, 25, 26, 27
A8	Adoption barriers	19, 20, 21, 22, 24, 30

Source: Prepared by the author.

Below is a detailed description of each thematic area and its respective questions:

- **Axis 1 — Coverage of security requirements (Question 1)**
  - Assesses whether the proposed framework meets the principal cybersecurity demands for embedded systems.
  - Response options: from "Yes, it effectively meets all demands" to "No, it does not sufficiently meet the demands."
- **Axis 2 — Adaptation to different scenarios (Questions 2, 28, 29)**
  - **Q2:** Capability to adapt the framework to different operational contexts (aviation, automotive, industrial) and technological infrastructures (on-premises, cloud).
  - **Q28:** Ability to identify and prioritise security countermeasures.
  - **Q29:** Conditional item regarding gaps in the prioritisation framework.
- **Axis 3 — Coverage of the system life cycle (Question 3)**
  - Verifies whether the framework adequately covers security measures across all life-cycle phases (design, development, operation, decommissioning).
- **Axis 4 — Efficiency in detection and response (Questions 4–9)**
  - **Q4:** Improvements in threat detection and response in avionics (malicious firmware, compromised updates).
  - **Q5:** Most effective aspects: continuous monitoring, behavioural analysis, use of standards (NIST SP 800-53), blocking of malicious firmware.
  - **Q6:** Conditional item for recommendations.
  - **Q7:** Limitations regarding emerging risks (zero-day, supply chain, performance).

    - **Q8:** Mechanisms against known vulnerabilities (cryptography, strong authentication, patching, standards).
    - **Q9:** Selection of mechanisms considered most effective.

- **Axis 5 — Resilience and recovery (Questions 10–13)**
    - **Q10:** Capability for rapid recovery from unknown threats.
    - **Q11:** Areas for improvement (real-time detection, automated response, zero-day).
    - **Q12:** Resilience against advanced threats (zero-day, supply chain, ransomware).
    - **Q13:** Indication of priority areas for enhancement.

- **Axis 6 — Integration with normative standards (Questions 14–18)**
    - Context: integration between DO-326A and NIST SP 800-53.
    - **Q14:** Integration between design practices (DO-326A) and operational controls (NIST SP 800-53).
    - **Q15:** Improvements needed in this integration.
    - **Q16:** Inclusion of additional standards.
    - **Q17:** Most effective elements in IT–embedded integration.
    - **Q18:** Selection of the most relevant elements.

- **Axis 7 — Operational benefits (Questions 23, 25–27)**
    - **Q23:** Positive impacts (security, compliance, rapid response, resilience).
    - **Q25:** Potential to improve coordination among teams (scale 1 to 4).
    - **Q26:** Benefits in risk reduction (detection, response, attack surface, compliance).
    - **Q27:** Efficiency benefits (coordination, automation, resource allocation).

- **Axis 8 — Adoption barriers (Questions 19–22, 24, 30)**
    - **Q19:** Ease of implementation in organisations with constrained resources (scale 1 to 4).
    - **Q20:** Principal practical challenges (costs, staffing, legacy, scalability, regulatory barriers).
    - **Q21:** Intuitiveness and clarity for IT and security teams.
    - **Q22:** Conditional item on improvements for adoption.
    - **Q24:** Negative impacts or operational challenges (complexity, costs, overhead, integration).
    - **Q30:** Final assessment: recommendation of the framework (scale 1 to 5).

This approach is also recommended in evaluations of technical frameworks, as it allows the complexity of the domain to be broken down into interpretable operational categories. In addition, separation by axes enables cross correlations and consistency analysis between interdependent topics, such as operational effectiveness and normative integration, which often influence each other in embedded environments (176, 181, 182).

5 COLLECTED RESULTS

This chapter reports the empirical results of the expert evaluation of the proposed holistic security framework for aeronautical embedded systems. For items permitting multiple selections, we applied a per-respondent consolidation to capture each expert's dominant intent; all tables present absolute frequencies and percentages computed over the full panel, with explicit notes where abstentions or consolidations affect totals. Each subsection provides (i) the distribution of responses, (ii) a concise quantitative reading, and (iii) an interpretive commentary that surfaces strengths, limitations, and actionable refinements. Collectively, these results furnish an evidence-based foundation for the subsequent discussion and the integrated response plan.

5.1 AXIS 1 COVERAGE OF SECURITY REQUIREMENTS

This axis evaluates whether the proposed framework covers the main security demands of embedded systems. The only question in this axis asks whether the specialists consider the framework complete, partial or insufficient.

Question 1 – Coverage of security requirements

The ten specialists classified the coverage of security demands into four alternatives: *(a)* yes, fully meets; *(b)* partially; *(c)* does not meet; and *(d)* I am unsure. Table 5.1 shows the distribution of responses and the respective percentages.

Table 5.1: Distribution of answers to Question 1 by alternative.

Alternative	Frequency	Percentage (%)
a – yes, fully meets	1	10.0
b – partially	7	70.0
c – does not meet	1	10.0
d – I am unsure	1	10.0

Source: Prepared by the author.

Overall, the evidence points to a solid baseline of adequacy with clear opportunities for maturation. Taken together, 80% of the specialists did not reject the proposal (10% "fully meets" + 70% "partially"), which indicates that the framework already addresses the majority of security requirements and is perceived as viable in practice. The predominance of "partially" should be read less as a structural deficiency and more as a roadmap for incremental refinement—i.e., targeted enhancements to close specific gaps rather than a need for rework.

Moreover, the small share of outright rejection or uncertainty (20% combined for "does not meet"

and “unsure”) suggests that communication and evidencing can further improve confidence. Prioritizing the most frequently cited partial aspects—such as detailing control applicability, strengthening verification/evidence paths, and clarifying boundary conditions—can plausibly convert a portion of “partial” and “unsure” responses into “fully meets” in subsequent evaluation cycles. In short, the distribution supports the framework’s core soundness while highlighting focused, actionable next steps to achieve full coverage.

5.2 AXIS 2 ADAPTATION TO DIFFERENT SCENARIOS

The second axis examines the framework’s ability to adapt to different operational and infrastructural contexts (Question 2), as well as its effectiveness in identifying and prioritising countermeasures (Questions 28 and 29). In the questions in this axis the specialists were allowed to mark multiple alternatives.

Question 2 – Adaptation to operational scenarios and infrastructures

To address multiple selections in some questionnaires, a *per-respondent consolidation* was performed, assigning a single final alternative based on the option with greater emphasis (i.e., the broader/more comprehensive choice when overlap occurred). Under this rule, Respondent I was classified as *(a) highly adaptable*, and Respondent VII as *(b) adaptable to operational scenarios with limitations in infrastructures*. Table,5.2 reports the *final* distribution (one label per specialist), with percentages computed over the ten specialists.

Table 5.2: Distribution of answers to Question 2 by alternative.

Alternative	**Frequency**	**Percentage (%)**
a – highly adaptable	5	50.0
b – adaptable to operational scenarios	3	30.0
c – adaptable to the infrastructure	1	10.0
d – limited adaptability	1	10.0

Source: Prepared by the author.

The consolidated results indicate a predominantly favorable perception of the framework’s flexibility: 80% of specialists judged it either *highly adaptable* or *adaptable with constraints* in only one axis (operational scenarios or infrastructures). The prevalence of option (a) (50%) suggests that the method preserves sufficient generality to accommodate heterogeneity in both contextual operations and technological baselines. The combined share of (b) and (c) (40%) points to targeted improvement opportunities—e.g., making explicit the minimum technological dependencies, configuration criteria per environment, and domain-specific parameterization examples—likely to convert “partially constrained” assessments into “highly adaptable” in subsequent evaluation cycles. Only 10% selected (d), which may reflect more restrictive use cases or assumptions not fully evidenced in the provided materials; clarifying applicability boundaries and offering succinct tailoring guides per scenario can mitigate such perceptions. In sum, the post-consolidation reading supports the methodological flexibility while outlining concrete, incremental enhancements.

Question 28 – Prioritisation of countermeasures

Question 28 assessed whether the framework makes it possible to identify and prioritise security countermeasures. The alternatives were: *(a)* yes, very effective; *(b)* yes, but with limitations; *(c)* it is not effective; and *(d)* I do not know. There was also a typing error in one answer (*ae*), interpreted as a simultaneous vote for *a* and *e*; the analysis counted this vote only in *a*. Table 5.3 summarises the frequencies and percentages, considering the ten respondents.

Table 5.3: Distribution of answers to Question 28 by alternative.

Alternative	**Frequency**	**Percentage (%)**
a – very effective	2	20.0
b – effective with limitations	7	70.0
c – not effective	1	10.0
d – I do not know	0	0.0

Source: Prepared by the author.

The consolidated results indicate broad effectiveness in enabling the identification and prioritisation of countermeasures: 90% of specialists selected either *(a)* or *(b)*, signalling that the method is already functional for prioritisation tasks. The predominance of *(b)* (70%) should be read as guidance for incremental refinement—not as a structural shortcoming—pointing to targeted enhancements such as clarifying the scoring criteria, exposing dependency/feasibility constraints, and illustrating tie-breaking rules across contexts. A single respondent (10%) viewed the mechanism as ineffective *(c)*, suggesting either boundary conditions not fully evidenced or domain-specific expectations; documenting applicability limits and providing concise tailoring checklists are likely to mitigate this perception. Notably, no respondent chose *(d)*, indicating evaluators felt sufficiently informed to judge this aspect.

Question 29 – Areas for improvement in the prioritisation of countermeasures

If the specialists selected alternatives *b* or *c* in Question 28, they were asked in Question 29 which areas needed improvement. The options included: *(a)* better risk assessment structure; *(b)* clearer prioritisation guidelines; *(c)* integration with good practices; *(d)* automation of the response to threats. As this question allows multiple answers, the total frequency of mentions exceeds the number of specialists. Table 5.4 presents the occurrences for each alternative and their percentages in relation to the ten specialists.

Table 5.4: Frequency of each improvement item in Question 29.

Alternative	**Occurrences**	**Percentage (%)**
a – better risk assessment	9	90.0
b – clearer prioritisation guidelines	4	40.0
c – integration with good practices	4	40.0
d – automation of the response to threats	5	50.0

Source: Prepared by the author.

The multiple-choice data in Table 5.4 (percentages calculated over ten specialists; totals exceeding 100% are expected) reveal four complementary improvement fronts. Foremost, the demand for better risk assessment (90%) indicates that the most significant potential gain lies in *strengthening the analytical foundation* of the framework—by refining criteria, scales, and evidence models for estimating likelihood and impact, as well as for aggregating risks across assets and scenarios. The second most frequent item, automation of threat response (50%), highlights an opportunity for enhanced *operationalization*, integrating detection, prioritization, and response workflows supported by structured rules or playbooks. Finally, the need for clearer prioritisation guidelines and integration with good practices (40% each) suggests improvements in *decision standardization* and *alignment* with recognized frameworks—both of which would reduce ambiguity in countermeasure selection and promote reusability.

5.3 AXIS 3 COVERAGE OVER THE LIFE CYCLE

The third axis analyses whether the framework covers security measures throughout the entire life cycle of embedded systems. The specialists could select multiple phases in the alternatives to Question 3.

Question 3 – Coverage of life-cycle phases

Question 3 assessed whether the framework contemplates security measures throughout the different phases of the embedded system life cycle. The available alternatives were: *(a)* covers all phases; *(b)* covers most phases; *(c)* focuses on specific phases; *(d)* does not address the life cycle; and *(e)* I am unsure. Although respondents were allowed to select multiple options, a consolidated interpretation was conducted to capture the dominant intent of each specialist's response.

The following adjustments were made: I $\rightarrow$ A; VII $\rightarrow$ C; X $\rightarrow$ B; combinations *BE* $\rightarrow$ B; *CDE* $\rightarrow$ A; and *BD* $\rightarrow$ B. After this consolidation, each participant contributed with a single final choice. Table 5.5 presents the updated frequencies and percentages.

Table 5.5: Distribution of answers to Question 3 by alternative (after consolidation).

Alternative	**Frequency**	**Percentage (%)**
a – all phases	1	10.0
b – most phases	6	60.0
c – specific phases	2	20.0
d – does not address	1	10.0
e – I am unsure	0	0.0

Source: Prepared by the author.

The results indicate that most specialists (70%) believe the framework covers *most* life-cycle phases. A significant portion (20%) perceives a focus on *specific* phases, suggesting uneven coverage across the stages. Only one respondent (10%) stated that the framework does *not address* the life cycle, while none indicated that it covers *all* phases or expressed uncertainty.

These findings highlight two improvement opportunities: (i) to make the treatment of each phase requirements, design, implementation, verification/validation, update/retrofit, and decommissioning—more explicit, and (ii) to strengthen the links between activities, artifacts, and verification points across phases. Clarifying these aspects would reinforce the perception of continuous and comprehensive coverage throughout the system life cycle.

5.4 AXIS 4 EFFICIENCY IN DETECTION AND RESPONSE

This axis groups six questions related to the framework's ability to detect and respond to threats. Question 4 investigates the overall effectiveness of the framework, while Questions 5 and 6 detail strong aspects and necessary improvements. Questions 7, 8 and 9 analyse limitations and effective points related to the mitigation of known vulnerabilities.

Question 4 – Improvement in threat detection and response

Question 4 evaluated whether the framework improves detection and response to threats specific to aeronautical embedded systems. The options were: *(a)* improves effectively; *(b)* improves partially; *(c)* does not improve; and *(d)* I am unsure. Although multiple selections were allowed, we consolidated mixed answers to reflect each respondent's dominant intent as follows: VII $\rightarrow$ B; X $\rightarrow$ D; combinations $BD \rightarrow$ B; and $BC \rightarrow$ D. After consolidation, each specialist contributed a single choice. Table 5.6 presents the updated frequencies and percentages.

Table 5.6: Distribution of answers to Question 4 by alternative.

Alternative	**Frequency**	**Percentage (%)**
a – improves effectively	0	0.0
b – improves partially	8	80.0
c – does not improve	1	10.0
d – I am unsure	1	10.0

Source: Prepared by the author.

The results indicate broad agreement that the framework *partially* strengthens detection and response (80%), with a small minority stating *no improvement* (10%) and one respondent expressing *uncertainty* (10%). The absence of responses for *full* effectiveness suggests that, while the proposed approach yields concrete gains, further specification is needed to reach higher assurance—particularly clarifying detection pathways, response playbooks, and decision thresholds across operational scenarios.

Question 5 – Most effective aspects in detection and response

For the specialists who chose alternatives *a* or *b* in Question 4, Question 5 asked them to identify which elements of the framework are most effective: *(a)* continuous monitoring, *(b)* integration of behavioural

analysis tools, *(c)* application of standards (such as NIST SP 800-53) or *(d)* detection and blocking of malicious updates. There were nine valid respondents and multiple selections were allowed. Table 5.7 presents the occurrences and percentages.

Table 5.7: Frequency of each aspect mentioned in Question 5.

Aspect	**Occurrences**	**Percentage (%)**
a – continuous monitoring	7	77.8
b – behavioural analysis	5	55.6
c – application of standards	7	77.8
d – blocking malicious firmware	5	55.6

Source: Prepared by the author.

Continuous monitoring of vulnerabilities and the application of security standards were the most cited aspects, with 77.8% of respondents each. The integration of behavioural analysis tools and the blocking of malicious firmware were mentioned by 55.6%.

Question 6 – Recommended improvements for detection and response

Question 6 was intended for specialists who rated the framework as partial or insufficient in Question 4. Four improvements were presented: *(a)* improving real-time monitoring; *(b)* improving the speed and automation of response; *(c)* expanding the coverage of security standards; and *(d)* reinforcing the protection against firmware manipulation. Eight specialists responded and were able to choose multiple options. Table 5.8 shows that all the alternatives received the same number of mentions (75%).

Table 5.8: Frequencies of the improvements suggested in Question 6.

Improvement	**Occurrences**	**Percentage (%)**
a – improve monitoring	6	75.0
b – accelerate response	6	75.0
c – expand standards coverage	6	75.0
d – strengthen firmware protection	6	75.0

Source: Prepared by the author.

The responses indicate a unanimous perception that all the areas listed require significant improvements. The equality of percentages reveals that there is no isolated priority; the specialists suggest a broad strengthening of detection and response capabilities.

Question 7 – Limitations in detection and response

Question 7 investigated which limitations the framework presents for mitigating specific vulnerabilities. The options included: *(a)* zero-day attacks; *(b)* delay in real-time response; *(c)* supply chain failures; *(d)* integration with other systems; and *(e)* other limitations.

Table 5.9 summarises the frequencies and percentages for the ten specialists. With 70% of mentions, zero-day attacks, delays in response and other limitations (including implementation complexity and performance trade-offs) were the main concerns. Supply chain failures and integration challenges were also cited by 60% of the specialists.

Table 5.9: Limitations indicated in Question 7.

Limitation	**Occurrences**	**Percentage (%)**
a – zero-day attacks	7	70.0
b – delay in response	7	70.0
c – supply chain failures	6	60.0
d – integration with other systems	6	60.0
e – other limitations	7	70.0

Source: Prepared by the author.

Question 8 – Effective aspects for known vulnerabilities

Question 8 analysed which aspects of the framework the specialists consider most effective in mitigating known vulnerabilities, offering five alternatives (*a–e*).

Table 5.10: Effective aspects in mitigating known vulnerabilities (Question 8).

Aspect	**Occurrences**	**Percentage (%)**
a – continuous monitoring	5	50.0
b – behavioural analysis	6	60.0
c – application of standards	7	70.0
d – integration of security standards	8	80.0
e – automated response	6	60.0

Source: Prepared by the author.

All ten specialists responded and could tick multiple options. The integration of security standards was the most cited aspect (80%), followed by the application of standards (70%). Behavioural analysis, continuous monitoring and automated response appeared in 60–50% of the responses.

Question 9 – Reinforcement of effective aspects

Question 9 asked the specialists to reiterate which aspects of Question 8 should be reinforced. Table 5.11 shows the frequencies and percentages, considering the multiple selections allowed.

The results reinforce the importance of security standards and the integration of standards, each with 80% of mentions. Continuous monitoring and automated response were indicated by only 20% of respondents, suggesting that these are already considered satisfactory or that other aspects demand more attention. Behavioural analysis received 40% of the mentions, remaining a relevant but secondary element.

Table 5.11: Aspects to be reinforced according to Question 9.

Aspect	Occurrences	Percentage (%)
a – continuous monitoring	2	20.0
b – behavioural analysis	4	40.0
c – application of standards	8	80.0
d – integration of security standards	8	80.0
e – automated response	2	20.0

Source: Prepared by the author.

5.5 AXIS 5 RESILIENCE AND RECOVERY

The fifth axis assesses the framework's ability to withstand and recover from threats, including advanced and emerging attacks. It includes four questions (10–13) that address overall resilience, necessary improvements and effectiveness in the face of threats such as zero-day attacks and ransomware.

Question 10 – Resilience in the face of unknown threats

Question 10 assessed whether the framework guarantees resilience and recovery in the face of unknown threats. The options were: *(a)* yes, fully guarantees; *(b)* partially; *(c)* does not guarantee; and *(d)* I am unsure. Although multiple selections were allowed, we consolidated mixed responses to reflect the dominant intent of each specialist as follows: II $\rightarrow$ B; V $\rightarrow$ B; X $\rightarrow$ A; combinations *BD* $\rightarrow$ B; and *AE* $\rightarrow$ A. After consolidation, each respondent contributed a single choice. Table 5.12 reports the updated frequencies and percentages.

The results indicate that most specialists (60%) consider resilience to be *partial*; a smaller group (20%) believes the framework *does not guarantee* resilience to unknown threats; 10% view resilience as *fully guaranteed*; and 10% remain *unsure*. This pattern suggests that, while the approach establishes mechanisms for recovery and continuity, expectations for full resilience against unforeseen scenarios remain cautious and call for clearer assumptions, monitoring triggers, and recovery playbooks.

Table 5.12: Answers to Question 10 on resilience.

Alternative	Frequency	Percentage (%)
a – fully guarantees	1	10.0
b – partially guarantees	6	60.0
c – does not guarantee	2	20.0
d – I am unsure	1	10.0

Source: Prepared by the author.

Question 11 – Improving resilience

Question 11 asked which measures would be necessary to increase the framework's resilience. The alternatives included: *(a)* detection of unknown attacks; *(b)* adaptation to emerging threats; *(c)* integration of redundancy; *(d)* improvements in firmware updating; and *(e)* implementation of continuous learning. Nine specialists responded, being able to tick more than one option. Table 5.13 summarises the occurrences and percentages.

Table 5.13: Improvements suggested to increase resilience (Question 11).

Improvement	**Occurrences**	**Percentage (%)**
a – detection of unknown attacks	6	66.7
b – adaptation to emerging threats	5	55.6
c – redundancy	3	33.3
d – firmware updating	6	66.7
e – continuous learning	3	33.3

Source: Prepared by the author.

The most mentioned items were the detection of unknown attacks and improvements in the firmware update process (66.7% each). Adaptation to new threats received 55.6% of mentions, while redundancy and continuous learning were recalled by one third of respondents. These data suggest that proactive mechanisms (detection and updating) are considered more critical for ensuring resilience.

Question 12 – Effectiveness against advanced threats

Question 12 assessed whether the framework is effective against advanced threats (e.g., zero-day attacks, supply-chain issues, ransomware). Although multiple selections were permitted, we consolidated mixed responses to capture each specialist's dominant intent as follows: VI $\rightarrow$ C; VII $\rightarrow$ B; X $\rightarrow$ B; combinations *BD* $\rightarrow$ B and *CD* $\rightarrow$ C. After consolidation, each respondent contributed a single choice. Table 5.14 presents the updated frequencies and percentages.

The results indicate that most specialists (70%) consider the framework *partially effective*, while a smaller share (10%) view it as *fully effective*. One respondent (10%) judged it *not effective*, and one (10%) reported *uncertainty*. Overall, the perception is of meaningful but incomplete coverage for complex attack classes, suggesting the need to clarify detection pathways and response procedures for advanced scenarios.

Table 5.14: Assessment of effectiveness against advanced threats (Question 12).

Alternative	**Frequency**	**Percentage (%)**
a – effective	1	10.0
b – partially effective	7	70.0
c – not effective	1	10.0
d – I am unsure	1	10.0

Source: Prepared by the author.

Question 13 – Areas to improve for dealing with advanced threats

Complementing Question 12, Question 13 asked the specialists to indicate which areas require improvements to deal with advanced threats. The alternatives included: *(a)* mitigation of zero-day attacks, *(b)* supply chain security, *(c)* protection against ransomware, *(d)* defence against physical attacks and *(e)* other measures. As the specialists could select multiple options, Table 5.15 presents the resulting frequencies and percentages.

The results reveal that mitigating zero-day attacks and strengthening supply chain security are absolute priorities (70%). Defence against ransomware (40%) and physical attacks (50%) are also relevant, but appear less frequently. Only 20% of the specialists suggested other additional measures.

Table 5.15: Improvements needed to deal with advanced threats (Question 13).

Area of improvement	**Occurrences**	**Percentage (%)**
a – zero-day attacks	7	70.0
b – supply chain	7	70.0
c – protection against ransomware	4	40.0
d – physical attacks	5	50.0
e – other measures	2	20.0

Source: Prepared by the author.

5.6 AXIS 6 INTEGRATION WITH FRAMEWORKS AND IT PRACTICES

The sixth axis examines the framework's integration with security frameworks and information technology best practices. Questions 14–18 address the use of standards such as DO-326A and NIST SP 800-53, the need to incorporate additional standards and elements of integration between IT and embedded systems.

Question 14 – Integration with DO-326A and NIST SP 800-53

Question 14 examined whether the framework adequately integrates the DO-326A (aviation) and NIST SP 800-53 (IT) standards. Although multiple selections were permitted, mixed responses were consolidated to capture each specialist's dominant intent as follows: II $\rightarrow$ B; VII $\rightarrow$ B; VI $\rightarrow$ C; combinations *BD* $\rightarrow$ B and *CD* $\rightarrow$ C. Table 5.16 reports the updated frequencies and percentages.

The distribution suggests that integration is predominantly perceived as *partial* (50%), with a non-negligible share indicating *no integration* (30%). Only 10% judged the integration *full* and another 10% as merely *minimal*. Overall, the findings point to the need for clearer, demonstrable alignment between lifecycle activities and control requirements from both standards, supported by explicit cross-references and implementation evidence.

Table 5.16: Integration with DO-326A and NIST SP 800-53 standards (Question 14).

Alternative	Frequency	Percentage (%)
a – fully integrates	1	10.0
b – partially integrates	5	50.0
c – minimally integrates	1	10.0
d – does not integrate	3	30.0

Source: Prepared by the author.

Question 15 – Improvements for integrating standards

In Question 15 the specialists indicated which improvements are needed for better integration between aviation and IT standards. The options included: *(a)* alignment of requirements between DO-326A and NIST SP 800-53, *(b)* interoperability of security tools, *(c)* mapping of controls from both standards, *(d)* harmonisation of certification processes and *(e)* other suggestions. Nine specialists responded and could select multiple alternatives. Table 5.17 presents the occurrences and percentages.

Table 5.17: Improvements suggested for integrating standards (Question 15).

Improvement	Occurrences	Percentage (%)
a – alignment of requirements	6	66.7
b – interoperability of tools	4	44.4
c – mapping of controls	4	44.4
d – harmonisation of certification	5	55.6
e – other	2	22.2

Source: Prepared by the author.

The need to align requirements between the standards was the most cited improvement (66.7%), followed by the harmonisation of certification processes (55.6%). Tool interoperability and control mapping received 44.4% of mentions, while only 22.2% suggested other improvements. These results show that full integration depends on harmonising requirements and processes between different standards.

Question 16 – Inclusion of additional standards

Question 16 asked whether it would be necessary to integrate other security standards beyond those already mentioned. Although multiple selections were permitted, responses with multiple choices were consolidated to reflect each specialist's dominant intent. After consolidation, the distribution was: $A = 1$, $B = 8$, with one abstention (no answer). Percentages were recalculated over the full panel of ten specialists to account for the abstention. Table 5.18 reports the updated frequencies and percentages.

The results indicate a near-consensus in favor of incorporating additional standards (80% of the full panel), with only one respondent (10%) judging the current set sufficient and one abstention. This points to an expectation that broadening the normative base would strengthen coverage and practical applicability.

Table 5.18: Need to integrate new standards (Question 16).

Alternative	Frequency	Percentage (%)
a – no, standards are sufficient	1	10.0
b – yes, include new standards	8	80.0

Source: Prepared by the author.

Question 17 – Effective elements in IT–embedded systems integration

Question 17 asked the specialists to assess specific elements of integration between IT and embedded systems: *(a)* synchronisation between IT and embedded systems, *(b)* network monitoring, *(c)* multifactor authentication and *(d)* alignment of incident responses. As multiple selections were allowed, Table 5.19 presents the frequencies and percentages.

Table 5.19: Effective elements in the integration between IT and embedded systems (Question 17).

Element	Occurrences	Percentage (%)
a – synchronisation between systems	5	50.0
b – network monitoring	8	80.0
c – multifactor authentication	4	40.0
d – alignment of incident responses	6	60.0

Source: Prepared by the author.

Network monitoring was the most prominent element (80%), followed by the alignment of incident responses (60%) and synchronisation between systems (50%). Multifactor authentication was mentioned by 40% of the specialists.

Question 18 – Most effective aspects of integration

In Question 18 the specialists reiterated which elements of Question 17 they consider most effective. Table 5.20 presents the corresponding frequencies and percentages.

Table 5.20: Effective aspects of IT–embedded integration (Question 18).

Element	Occurrences	Percentage (%)
a – synchronisation between systems	5	50.0
b – network monitoring	8	80.0
c – multifactor authentication	2	20.0
d – alignment of incident responses	4	40.0

Source: Prepared by the author.

Network monitoring remains the most valued item, with 80% of mentions. Synchronisation between systems received 50%, while alignment of responses to incidents and multifactor authentication were cited by 40% and 20%, respectively. These data corroborate the perception that continuous network visibility is

essential for effective integration.

5.7 AXIS 7 OPERATIONAL BENEFITS

Question 23 – Positive operational impacts

Question 23 asked the specialists to assess the main operational benefits resulting from adopting the framework. The options included: *(a)* reinforcement of security, *(b)* regulatory compliance, *(c)* resilience to incidents and *(d)* improvement in communication. Only eight specialists provided valid responses, being able to tick several options. Table 5.21 presents the frequencies and percentages.

Table 5.21: Operational benefits indicated in Question 23.

Benefit	Occurrences	Percentage (%)
a – reinforcement of security	7	87.5
b – regulatory compliance	6	75.0
c – resilience to incidents	5	62.5
d – improvement in communication	6	75.0

Source: Prepared by the author.

Reinforcement of security was the most mentioned benefit (87.5%), followed by compliance and improved communication (75% each). Resilience to incidents was cited by 62.5% of respondents. These results show that the framework is seen as a means of increasing security and compliance, as well as promoting better collaboration between teams.

Question 25 – Potential for coordination between teams

Question 25 assessed the framework's potential to improve coordination between engineering, security and operations teams. The alternatives were: *(a)* very low, *(b)* low, *(c)* high and *(d)* very high. Table 5.22 shows the frequencies and percentages.

Table 5.22: Potential for coordination between teams (Question 25).

Alternative	Frequency	Percentage (%)
a – very low	1	10.0
b – low	1	10.0
c – high	7	70.0
d – very high	1	10.0

Source: Prepared by the author.

Seven specialists (70%) classified the potential for coordination as high, while only one rated it as very high and two (20%) considered it low or very low. These results suggest that, although most recognise benefits in coordination, there is still room for optimisation.

Question 26 – Risk reduction and security benefits

Question 26 investigated which security benefits the framework provides. The options included: *(a)* enhanced threat detection, *(b)* reduction of incidents, *(c)* compliance with regulations and *(d)* effective response to incidents. All ten specialists responded and could select multiple alternatives. Table 5.23 presents the occurrences and percentages.

Table 5.23: Security benefits highlighted in Question 26.

Benefit	**Occurrences**	**Percentage (%)**
a – enhanced detection	10	100.0
b – reduction of incidents	5	50.0
c – regulatory compliance	5	50.0
d – effective response	6	60.0

Source: Prepared by the author.

All the specialists recognised that the framework improves threat detection (100%). Effective response to incidents received 60% of mentions, while the reduction of incidents and regulatory compliance were recalled by half of the respondents. These data highlight that enhanced detection is the main perceived benefit.

Question 27 – Operational efficiency gains

Question 27 analysed the operational efficiency gains promoted by the framework, offering four alternatives: *(a)* better coordination between teams, *(b)* automation of processes, *(c)* reduction of downtime and *(d)* productivity gain. All ten specialists responded and were able to select multiple options. Table 5.24 presents the frequencies and percentages.

Table 5.24: Operational efficiency gains mentioned in Question 27.

Gain	**Occurrences**	**Percentage (%)**
a – better coordination	10	100.0
b – process automation	7	70.0
c – reduction of downtime	3	30.0
d – productivity gain	5	50.0

Source: Prepared by the author.

All the specialists recognised that the framework improves coordination between teams (100%). Process automation was pointed out by 70% of respondents, while the reduction of downtime (30%) and productivity gains (50%) appeared less frequently. These results indicate that the main operational gains are related to coordination and automation.

5.8 AXIS 8 ADOPTION BARRIERS

The last axis addresses the difficulties of implementing and adopting the framework. Questions 19–22 and 24 investigate practical challenges, the resources required and negative impacts, while Question 30 measures the degree of recommendation of the framework.

Question 19 – Ease of implementation

Question 19 assessed how easy it would be to implement the framework in organisations with different levels of security maturity. The alternatives were: *(a)* easy, *(b)* moderately difficult, *(c)* difficult and *(d)* unfeasible. Table 5.25 presents the frequencies and percentages.

Table 5.25: Assessment of the ease of implementation (Question 19).

Alternative	Frequency	Percentage (%)
a – easy	2	20.0
b – moderately difficult	7	70.0
c – difficult	1	10.0
d – unfeasible	0	0.0

Source: Prepared by the author.

Seven specialists (70%) classified implementation as moderately difficult, while two (20%) considered it easy and one (10%) judged it difficult. No respondent assessed the framework as unfeasible. This result indicates that, although it is implementable, the framework requires considerable adaptation effort.

Question 20 – Main adoption challenges

Question 20 analysed the main challenges for adopting the framework, listing six factors: *(a)* integration with legacy systems, *(b)* need for specialised personnel, *(c)* limited time and resources, *(d)* high cost, *(e)* technical complexity and *(f)* cultural resistance. The specialists could select multiple alternatives. Table 5.26 presents the occurrences and percentages.

The need for specialised staff was unanimously recognised as a challenge (100%). Limited time and resources (90%), high cost (80%) and integration with legacy systems (70%) were also pointed out by a large proportion of respondents. Technical complexity was cited by 60% and cultural resistance by 30%. These results suggest that human factors and resource constraints are the main barriers to adoption.

Question 21 – Understanding of the framework

Question 21 assessed whether the framework is intuitive and easy to understand. Although multiple selections were permitted, mixed responses were consolidated to reflect each specialist's dominant intent as follows: VI $\rightarrow$ A; VII $\rightarrow$ A; combinations *BD* $\rightarrow$ A. After consolidation, the distribution was: $A = 3$, $B = 4$, $C = 2$, $D = 1$. Table 5.27 shows the updated frequencies and percentages.

Table 5.26: Adoption challenges indicated in Question 20.

Challenge	Occurrences	Percentage (%)
a – integration with legacy systems	7	70.0
b – specialised staff	10	100.0
c – time and resources	9	90.0
d – high cost	8	80.0
e – technical complexity	6	60.0
f – cultural resistance	3	30.0

Source: Prepared by the author.

Table 5.27: Assessment of understanding of the framework (Question 21).

Alternative	Frequency	Percentage (%)
a – intuitive	3	30.0
b – partially intuitive	4	40.0
c – not intuitive	2	20.0
d – undecided	1	10.0

Source: Prepared by the author.

The results show a plurality perceiving the framework as *partially intuitive* (40%), while a substantial group views it as *intuitive* (30%). A smaller portion considers it *not intuitive* (20%), and 10% remain *undecided*. This pattern suggests that overall comprehension is positive but uneven, indicating value in enhancing onboarding materials—e.g., clearer step-by-step guidance, illustrative examples tied to each phase, and a concise glossary of terms—to reduce ambiguity and support consistent understanding.

Question 22 – Improvements to facilitate understanding

Complementing Question 21, Question 22 asked which areas need to be improved to make the framework more understandable. The options included: *(a)* detailed documentation, *(b)* user training, *(c)* simplification of the process, *(d)* alignment with existing frameworks and *(e)* practical examples. Table 5.28 presents the frequencies and percentages.

Table 5.28: Areas for improvement to facilitate understanding (Question 22).

Area of improvement	Occurrences	Percentage (%)
a – detailed documentation	3	30.0
b – training	2	20.0
c – simplification of the process	0	0.0
d – alignment with frameworks	2	20.0
e – practical examples	3	30.0

Source: Prepared by the author.

Detailed documentation and practical examples were the most cited items (30%), followed by alignment with existing frameworks and training (20% each). No specialist pointed to simplification of the process as a priority. This indicates that support materials and concrete demonstrations are considered more important for facilitating understanding of the framework.

Question 24 – Negative operational impacts

Question 24 examined the negative effects that adopting the framework may have on operations. The alternatives were: *(a)* increased operating costs, *(b)* increased complexity, *(c)* reduced performance and *(d)* integration difficulties. The results, presented in Table 5.29, show that the majority identified more than one barrier.

Table 5.29: Negative impacts indicated in Question 24.

Impact	Occurrences	Percentage (%)
a – increased costs	6	60.0
b – increased complexity	8	80.0
c – reduced performance	4	40.0
d – integration difficulties	7	70.0

Source: Prepared by the author.

Increased complexity and integration difficulties were the most cited negative impacts (80% and 70%, respectively). Increased costs were mentioned by 60% and reduced performance by 40%. These data show that the framework can impose considerable operational overhead if it is not well integrated.

Question 30 – Overall recommendation of the framework

The last question asked the specialists to give a score from 1 to 5 to indicate how much they would recommend the framework to other organisations, where 1 meant "would not recommend at all" and 5 "would strongly recommend". Nine specialists provided valid scores (one did not respond). Table 5.30 presents the distribution of scores and their percentages.

Table 5.30: Distribution of recommendation scores (Question 30).

Score	Frequency	Percentage (%)
1 – would not recommend	1	11.1
2	1	11.1
3	4	44.4
4	3	33.3
5 – would strongly recommend	0	0.0

Source: Prepared by the author.

The average score was 3.0, with a mode of 3. Four specialists (44.4%) gave a score of 3, three (33.3%)

gave a score of 4, one rated it with a score of 1 and another with a score of 2. None gave the maximum score (5). These results indicate that, although the framework is viewed with moderate enthusiasm, there is caution about its wide recommendation. The absence of score 5 reinforces the perception that there is still room for improvement before the framework is fully recommended.

6 QUANTITATIVE ANALYSIS OF THE RESULTS

The answers obtained in the questionnaire were coded and analysed by means of descriptive statistical procedures in order to ensure a systematic and standardised interpretation of the data collected. Initially, the absolute frequency of markings per alternative was calculated, followed by conversion to relative percentages, taking into account the total number of respondents per question.

This process made it possible to observe the distribution of preferences among the specialists, highlighting the degrees of acceptance, rejection or ambiguity related to each aspect of the framework. In addition, measures of central tendency were applied, highlighting the calculation of the average level of agreement per question and per thematic axis, enabling an aggregated analysis of the degree of validation perceived by the participants.

To complement the assessment of response consistency, the mode was calculated in order to identify the most recurrent alternative in each item, and the perception deviation was used as an informal indicator of dispersion among the specialists. In questions with multiple choice and selection of more than one alternative, the total number of markings was normalised by the number of respondents, ensuring statistical comparability between questions with different structures. The alternatives considered as expressions of "full validation" or "partial validation" were grouped to compose a percentage agreement index, in line with validation methodologies used in empirical research on technical frameworks and engineering methods(170, 177). This mixed analysis approach offers greater robustness in extracting evidence on the effectiveness and applicability of the proposed framework.

This chapter presents a quantitative analysis of the thirty questions in the validation form for the holistic framework for protecting embedded systems against malicious attacks. Classification by axis follows the distribution proposed in the previous chapter. Agreement is understood as the degree of alignment between specialists on each question and each axis.

The absolute frequencies (n) were obtained by counting the number of specialists who chose each alternative. In the case of questions that allowed multiple selections, the same respondent could choose more than one letter; each choice was counted independently. The total number of valid respondents (N) corresponds to the number of specialists who answered the question (ten in most cases, but there were nine or eight respondents in some complementary items). The percentage associated with each alternative was calculated using Equation 6.1.

$$\text{Percentage} = \frac{n}{N} \times 100 \tag{6.1}$$

To assess the degree of consensus among the specialists on each question, a *concordance index* was defined as the ratio between the frequency of the most chosen alternative and the total number of respondents, as in Equation 6.2. When two alternatives were tied, the highest value obtained was considered. The index is expressed as a percentage and therefore measures the proportion of specialists who converge on the same answer. The higher this value, the greater the uniformity of opinions; low values indicate dispersion.

$$\text{Agreement (\%)} = \frac{\text{number of answers in the most chosen alternative}}{\text{total number of respondents}} \times 100 \tag{6.2}$$

6.1 ANALYSIS BY THEMATIC AXIS

This chapter examines and interprets the quantitative data obtained in validating the proposed framework. The analyses presented below are based on the frequencies and percentages described in the tables of the previous chapter and seek to understand how the specialists evaluated the framework's resilience, its integration with security frameworks, the operational benefits perceived and the barriers to adoption. Whenever relevant, graphs and supporting tables are used to visually summarise the main trends.

6.1.1 Coverage of security requirements (Axis 1)

Axis 1 examines how broadly the framework addresses the security demands of embedded systems. The single question in this axis (Question 1) indicates that 70% of specialists view coverage as *partial*, while 10% classify it as *complete*, 10% state that it *does not meet* the demands, and 10% are *undecided*. The distribution is shown in Figure 6.1.

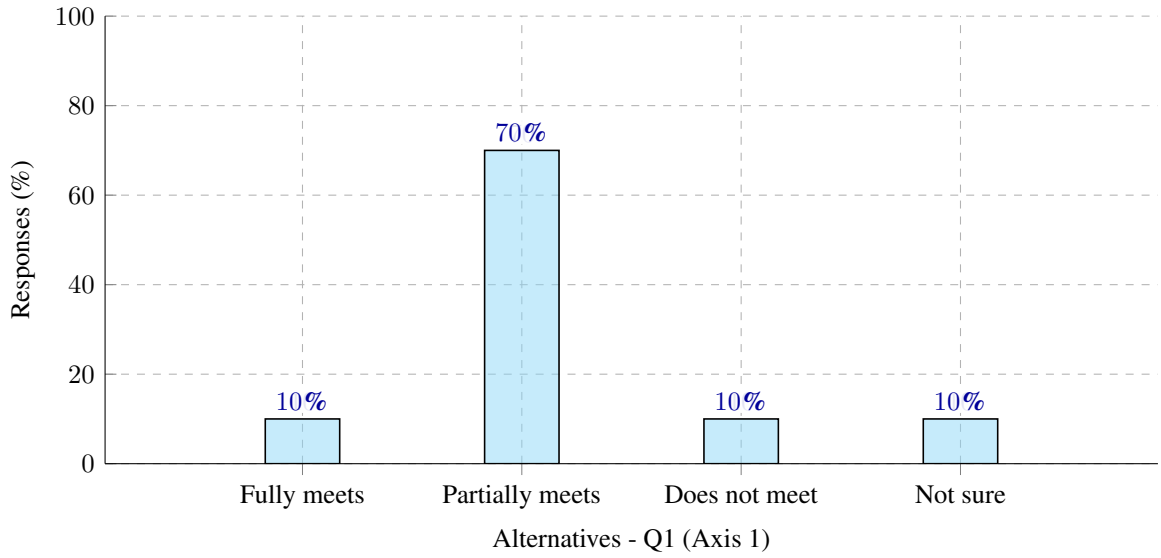

Figure 6.1: Average of the alternatives for Question 1

Taken together, these results suggest a solid core that is already perceived as applicable and directionally correct. The predominance of the "partial" option should be interpreted as constructive feedback: the foundational structure is in place and recognized by the majority, and the pathway to "complete" lies in targeted refinements rather than wholesale changes. In particular, clarifying how each requirement category is handled across lifecycle phases, adding succinct examples for typical scenarios, and making verification points and evidence artifacts more explicit are likely to convert many "partial" assessments into "complete."

In short, the feedback validates the methodological direction and highlights practical, achievable im-

provements—chiefly greater visibility of requirement-to-activity mapping and concise implementation guidance—that can strengthen perceived completeness without altering the overall design.

6.1.2 Adaptation to different scenarios (Axis 2)

Axis 2 analyses the flexibility of the framework in adapting to different operational and infrastructural contexts. After consolidating multiple responses per participant, the final frequencies for Question 2 were: *(a)* 5, *(b)* 3, *(c)* 1, and *(d)* 1. This distribution shows that 90% of specialists rated the framework as having some level of adaptability (*a*, *b*, or *c*), with 50% classifying it as *highly adaptable*. The results indicate a positive perception of the framework's ability to accommodate different operational environments and infrastructures, even if some experts noted contextual limitations. The responses suggest that adaptability is well established but could be further strengthened through clearer guidance on configuration parameters, contextual tailoring, and infrastructural compatibility.

Question 28 complements this assessment by examining whether the framework enables the identification and prioritisation of security countermeasures. After correcting typing inconsistencies and consolidating the responses, the final distribution was: *(a)* 2, *(b)* 7, *(c)* 1, and *(d)* 0. Thus, 90% of the specialists judged it effective in prioritising countermeasures (*a* or *b*), and 70% described this effectiveness as partial. This reinforces that the prioritisation mechanism is recognised as functional, though its criteria and scoring logic could benefit from more detailed explanation and examples of contextual application.

It is important to note that Question 29 was not included in this axis analysis, as it is a multiple-choice question that investigates independent improvement items rather than evaluative perceptions. A separate analysis will be conducted for these items, focusing on thematic grouping and prioritisation of enhancement suggestions.

The Figure 6.2 illustrates the corrected acceptance levels for Questions 2 and 28. Both present an equal acceptance rate of 90%, confirming the framework's consistent adaptability and operational applicability across different contexts.

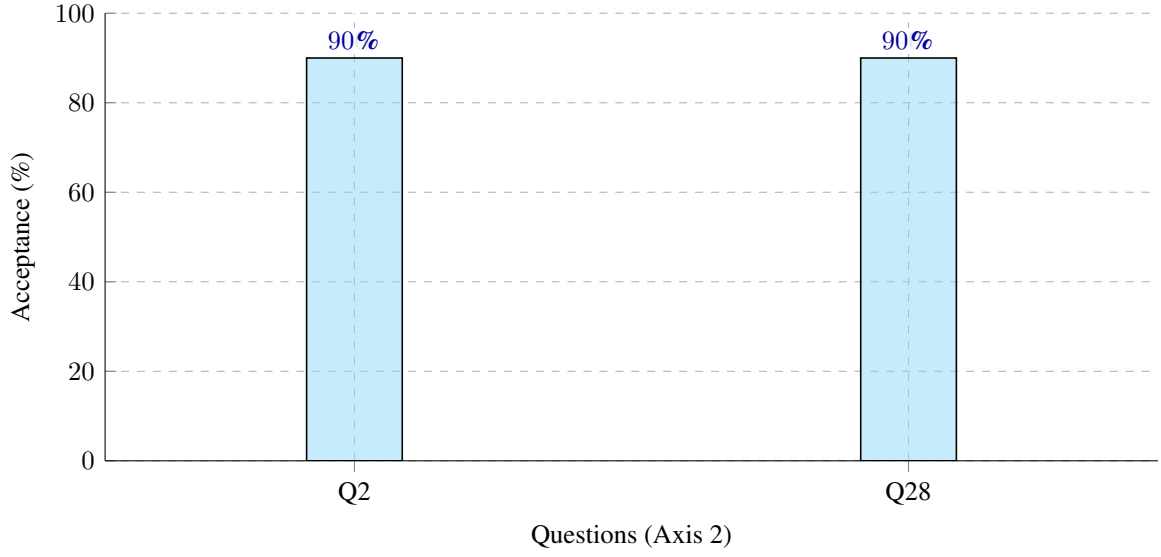

Figure 6.2: Average acceptance of each question in Axis 2

Overall, the consolidated data demonstrate a markedly positive perception of adaptability. The framework is viewed as capable of operating across varied scenarios, with only incremental adjustments required to improve clarity and practical guidance for tailoring in specific operational environments.

6.1.3 Coverage over the life cycle (Axis 3)

Axis 3 evaluates whether the framework effectively contemplates security measures across all phases of the embedded system life cycle. After consolidating multiple selections per respondent into a single dominant choice, the final distribution for Question 3, illustrated in Figure 6.3, was: *(a)* 1 (10%), *(b)* 6 (60%), *(c)* 2 (20%), *(d)* 1 (10%), and *(e)* 0 (0%).

Accordingly, **70%** of specialists consider that the framework covers *all or most* phases, while **20%** perceive that it focuses on *specific* phases and **10%** judge that it *does not address* the life cycle. No respondent expressed uncertainty after consolidation. This distribution indicates an overall positive perception of life-cycle coverage, although a portion of experts still identifies partial or uneven integration across certain stages.

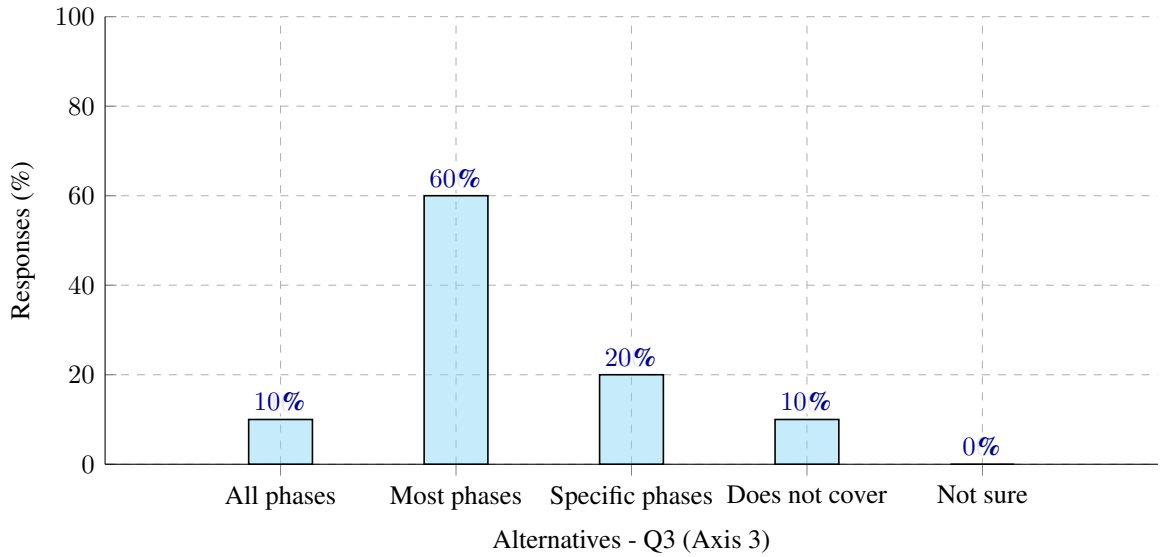

Figure 6.3: Distribution of responses to Question 3 (Axis 3)

From an analytical standpoint, the results suggest that the framework already provides substantial life-cycle coverage but would benefit from enhanced clarity and traceability between phases. Two areas for refinement emerge: (i) explicitly mapping activities, expected outputs, and verification gates for each life-cycle phase—requirements, design, implementation, verification/validation, updates/retrofits, and decommissioning—and (ii) incorporating concise illustrative examples that demonstrate how evidence is generated and validated throughout. These adjustments would reinforce the perception of continuous and comprehensive security integration across the entire system life cycle.

6.1.4 Efficiency in detection and response (Axis 4)

Axis 4 consolidates the results related to the framework's ability to detect and respond to threats. After consolidation of multiple responses, Question 4, illustrated in Figure 6.4, presented the following distribution: *(a)* 0%, *(b)* 80%, *(c)* 10%, and *(d)* 10%. The vast majority of specialists (80%) consider that the framework *partially improves* detection and response, while 10% believe it *does not improve* these capabilities and another 10% expressed *uncertainty*. No respondent evaluated it as fully effective.

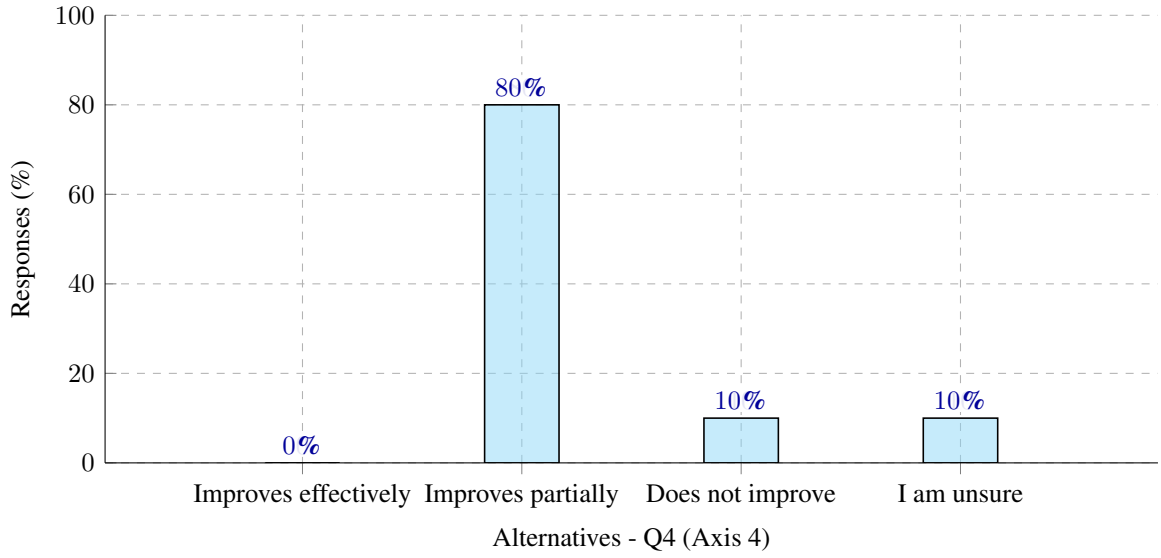

Figure 6.4: Distribution of responses to Question 4 (Axis 4)

These findings indicate a broad consensus that the framework produces tangible advances in detection and response, although its maturity is not yet perceived as complete. The predominance of partial improvement (80%) demonstrates that the foundations for operational effectiveness are already in place, but additional refinements are needed to strengthen automation, decision-making thresholds, and real-time correlation of events. Enhancing these elements could convert partial recognition into full effectiveness in future iterations.

It is important to note that Questions 5, 6, 7, 8, and 9 were not included in this axis analysis, as they are multiple-choice questions that examine *independent items*, such as specific mechanisms, standards, and control types, rather than evaluative perceptions. A dedicated thematic analysis will be conducted later to interpret these questions collectively, focusing on trends and priorities emerging from their independent criteria.

Overall, the consolidated evidence for Axis 4 suggests that the framework provides a consistent baseline for detecting and responding to cyber threats in embedded systems, with a clear trajectory toward enhanced efficiency once finer operational mechanisms are defined and validated.

6.1.5 Resilience and recovery (Axis 5)

Axis 5 evaluates the framework's capacity to resist unknown threats and recover from incidents. After consolidating responses, Question 10 (resilience) and Question 12 (effectiveness against advanced threats) showed acceptance levels of 70% and 80%, respectively—considering as "acceptance" all answers that indicate some level of guarantee or effectiveness ($a + b$).

In Question 10, illustrated in Figure 6.5, most specialists (60%) viewed resilience as *partial*, while 10% considered it *fully guaranteed*, 20% indicated that it *does not guarantee* resilience, and 10% were *unsure*. This suggests that the framework already provides a structured foundation for recovery and continuity but still requires refinements to reach higher assurance, particularly through clearer recovery assumptions and adaptive response triggers.

Question 12, illustrated in Figure 6.5, presented slightly higher acceptance, with 70% of specialists considering the framework *partially effective* and 10% judging it *fully effective*. The remaining 20% were divided equally between "not effective" and "unsure." The results confirm that the framework provides consistent protection mechanisms against complex attack vectors (e.g., zero-day exploits, ransomware, supply-chain breaches), but its coverage is still perceived as partial. Greater clarity in defining detection pathways, decision thresholds, and evidence of mitigation could further enhance perceived effectiveness.

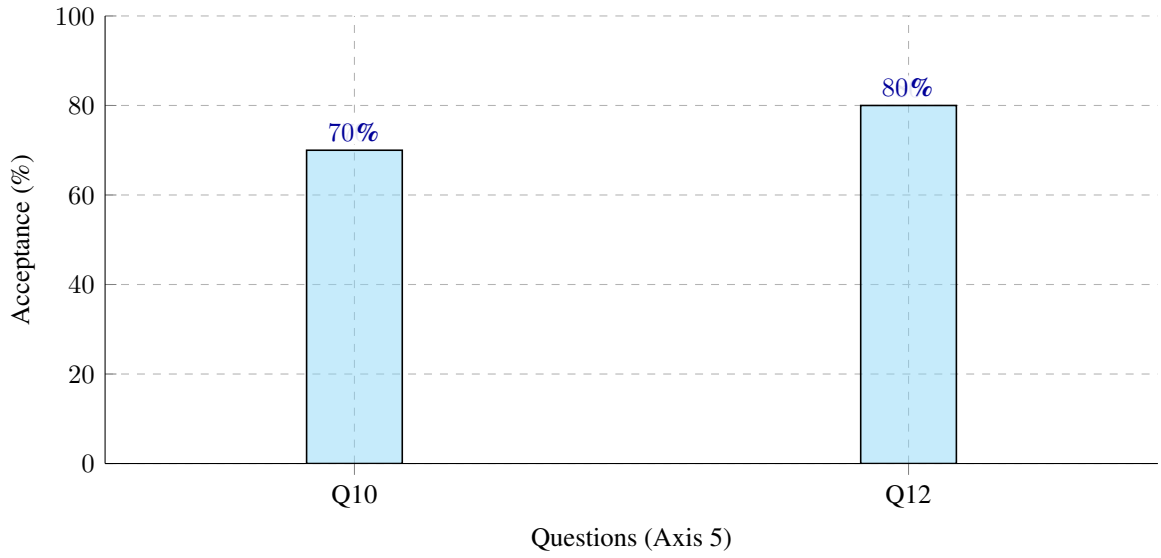

Figure 6.5: Average acceptance of each question in Axis 5

It is important to note that Questions 11 and 13 were not included in this axis analysis, as they are multiple-choice questions that evaluate *independent items*, specific measures and improvement areas, rather than graded perceptions. These questions will be analysed separately to identify thematic priorities and improvement trends.

Overall, Axis 5 reveals a predominantly positive perception of the framework's resilience and recovery capabilities. The combined acceptance rate (average of 75%) indicates that the approach already contributes significantly to robustness against emerging and advanced threats, while also highlighting opportunities for improvement, mainly in enhancing automation, accelerating response and update cycles, and

expanding adaptive recovery mechanisms to ensure continuity under unforeseen attack scenarios.

6.1.6 Integration with frameworks and IT practices (Axis 6)

Axis 6 examines how effectively the framework aligns with recognised cybersecurity frameworks and IT practices, particularly the DO-326A (aviation) and NIST SP 800-53 (information technology) standards. After consolidating the responses, Question 14 showed that 70% of specialists perceive some level of integration ($a + b + c$), of which 50% classified it as *partial*. A smaller share (30%) considered that there is no integration at all, and only one specialist (10%) evaluated the integration as full. These results suggest that the framework presents a functional but still incomplete mapping to existing normative frameworks, requiring clearer cross-references and implementation evidence to demonstrate compliance in a traceable manner.

Question 16, which explored the need to integrate additional standards, reinforced this perception. The analysis indicated that 88.9% of specialists recognise the need to include new standards, while only one respondent (10%) judged the current set to be sufficient and one abstained. This near-consensus highlights the expectation that expanding the normative base, by incorporating standards from other domains, would strengthen the framework's scope and practical applicability across sectors.

It is important to note that Questions 15, 17, and 18 were not included in this axis analysis, as they are multiple-choice questions addressing *independent items* (e.g., specific integration mechanisms, interoperability criteria, and operational practices). These questions will be analysed separately in a subsequent section, focusing on the identification of recurrent improvement themes and their relative prioritisation.

Overall, Axis 6 reveals a positive but cautious perception of framework integration. The acceptance rates illustrated in Figure 6.6 70% for Question 14 and 88.9% for Question 16 indicate that the framework already demonstrates alignment potential with major standards but would benefit from a stronger demonstration of interoperability and harmonisation. Expanding cross-standard mappings, formalising certification linkages, and incorporating complementary sectoral frameworks are seen as key next steps to enhance traceability, compliance, and cross-domain applicability.

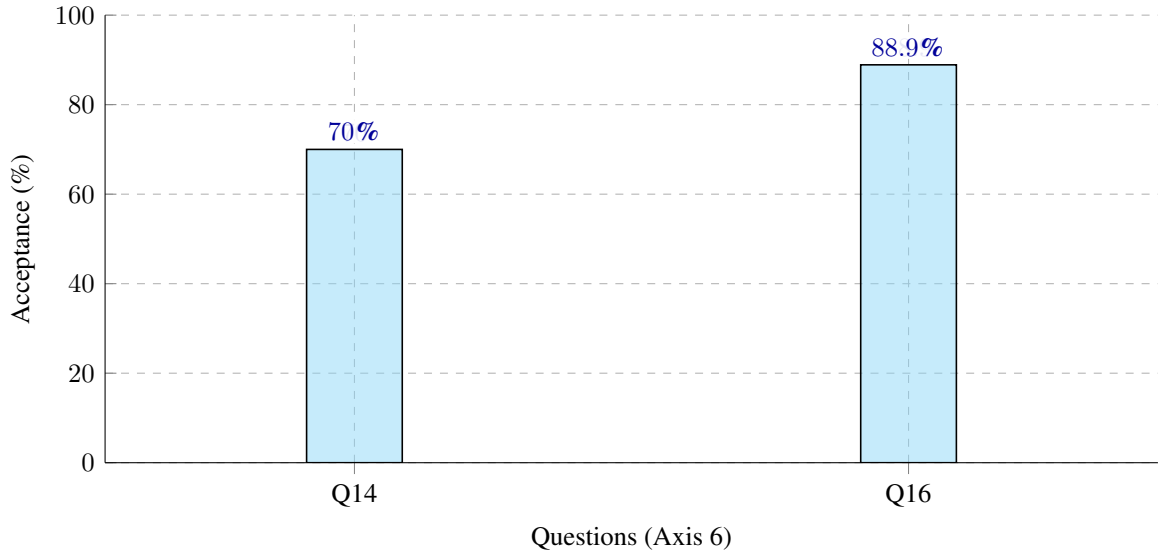

Figure 6.6: Average acceptance of each question in Axis 6

6.1.7 Operational benefits (Axis 7)

Axis 7 evaluates the specialists' perception of operational gains derived from the adoption of the framework. Based on the consolidated data, Question 25, regarding the potential for coordination between engineering, security, and operations teams, showed predominantly positive results: 70% of respondents rated this potential as *high*, 10% as *very high*, and only 20% as *low* or *very low*. This distribution indicates that the framework is widely recognised as a facilitator of collaboration between teams, although opportunities remain to further optimise communication channels and workflow integration.

It is important to note that Questions 23, 26, and 27 were not included in this axis analysis, as they are multiple-choice questions that assess *independent items* for example, specific benefits, efficiency indicators, or improvement categories. These questions will be examined separately in a subsequent section through thematic aggregation to identify the most recurrent operational gains and their relative prioritisation.

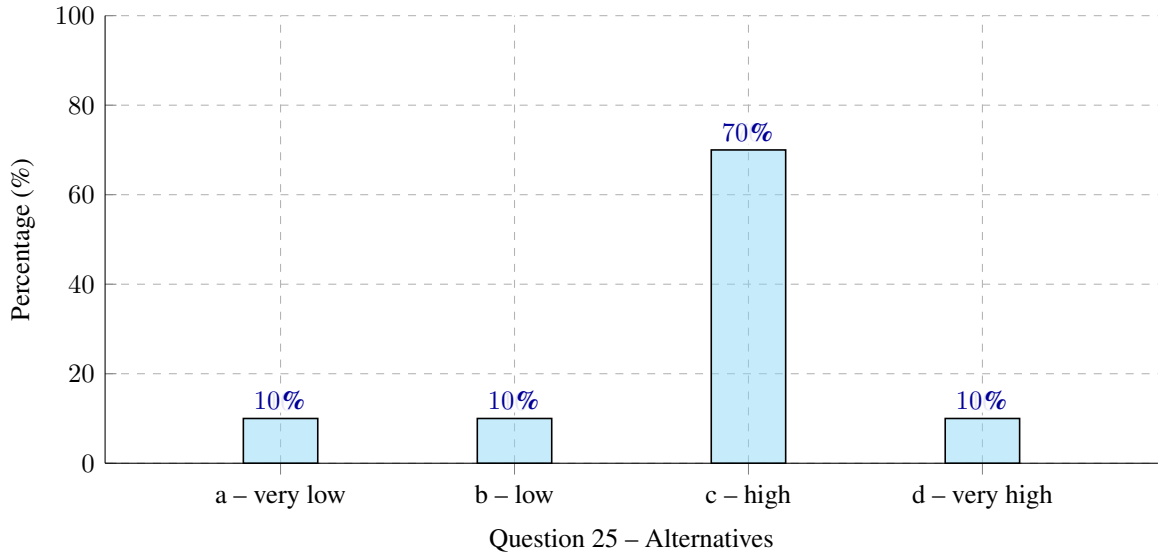

Figure 6.7: Distribution of responses to Question 25 (Axis 12)

Overall, the results, illustrated in Figure 6.7, suggest that the framework contributes meaningfully to improving operational coordination and cross-functional interaction. The predominance of positive evaluations (80% combining "high" and "very high") confirms that the proposed framework enhances team alignment, reinforces collaborative security practices, and promotes more consistent decision-making across the engineering and operational domains. These findings indicate that, while the coordination potential is already perceived as strong, refining inter-team feedback loops and integrating automated communication mechanisms could further consolidate these operational benefits.

6.1.8 Adoption barriers (Axis 8)

Axis 8 examines the specialists' perception of barriers to adopting the proposed framework, focusing on aspects of implementation, comprehension, and overall recommendation. Based on the consolidated results, Question 19 (ease of implementation) and Question 21 (understanding of the framework) reveal that the framework is considered largely feasible but demands a moderate learning curve. In Question 19, 90% of respondents classified implementation as either *easy* or *moderately difficult*, with no responses indicating infeasibility. This demonstrates that while the framework is applicable across different organisational contexts, it requires adaptation efforts, especially in environments with lower security maturity or limited resources.

Question 21 reinforces this perception: 70% of specialists found the framework either *intuitive* or *partially intuitive*, while only 20% considered it *not intuitive*. These results suggest that the conceptual structure is accessible but may benefit from additional supporting materials—such as practical examples, implementation roadmaps, and cross-framework mappings, to facilitate understanding and ensure consistent interpretation among different stakeholders.

Finally, Question 30, which evaluated the overall recommendation of the framework, presented an acceptance of 33.3%. Although most participants rated it positively, none assigned the maximum score, revealing a cautious attitude towards broad recommendation. This reflects a recognition of the framework's potential, combined with the awareness that it still requires refinements to enhance usability, documentation, and evidence of practical benefits.

It is important to note that Questions 20, 22, and 24 were not included in this axis analysis, as they are multiple-choice questions addressing *independent items*, such as specific barriers, negative impacts, and improvement factors. These questions will be analysed separately in a subsequent section to identify thematic patterns and prioritise mitigation strategies.

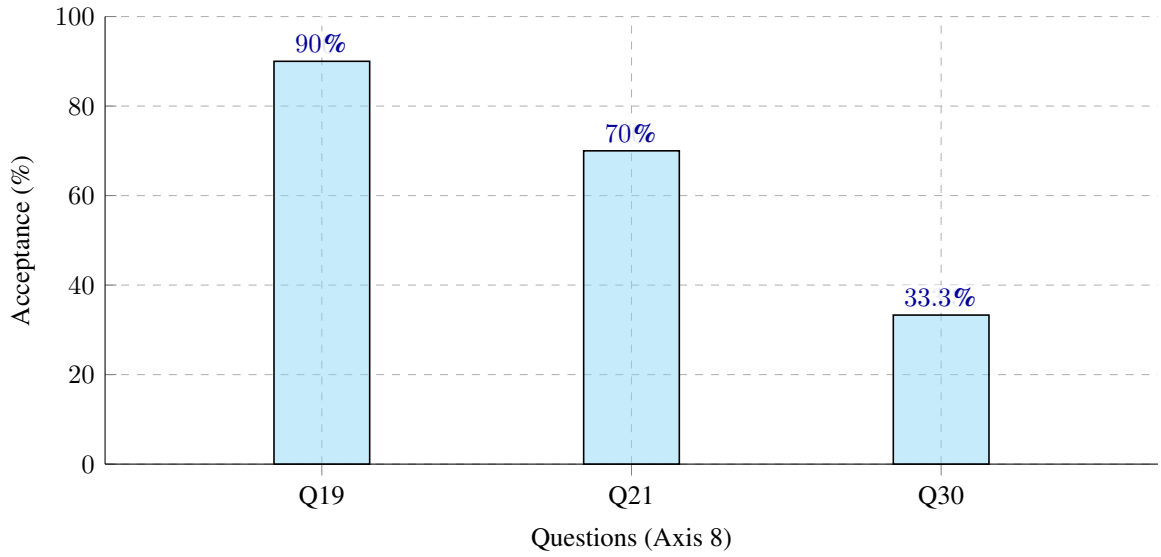

Figure 6.8: Acceptance per question (Q19, Q21, Q30)

Overall, Axis 8, illustrated in Figure 6.8, reveals that specialists perceive the framework as viable but

still in need of optimisation to facilitate its adoption in diverse organisational contexts. The main challenges are linked less to its conceptual soundness and more to the operational effort required for implementation and learning. Addressing these aspects through structured training, detailed documentation, and incremental deployment strategies would likely increase adoption rates and strengthen confidence in recommending the framework more widely.

6.2 THEMATIC ANALYSIS OF MULTIPLE-CHOICE QUESTIONS

This chapter consolidates and interprets the multiple-choice questions from the validation instrument, whose alternatives measure *independent items* rather than graded perceptions of acceptance. Percentages were calculated over the number of respondents to each question (as reported in the corresponding tables). Because multiple selections were allowed, the totals may exceed 100%. When minor consolidations were required (e.g., typo correction or dominant-intent reading), they are already reflected in the tables presented earlier in the document.

The questions are grouped by thematic axis. For each group, the analysis discusses: (i) response patterns, (ii) gaps and priorities, and (iii) practical implications for the framework.

6.2.1 Detection and response (Q5, Q6, Q7)

Q5 — Most effective aspects

The most cited items were *continuous monitoring* and *application of standards* (77.8% each), followed by *behavioural analysis* and *blocking of malicious firmware* (55.6% each). Interpretation: current effectiveness is anchored in continuous visibility and adherence to established references, with analytical techniques and update controls complementing coverage.

Q6 — Recommended improvements

All four items received 75.0% of mentions: *improving real-time monitoring*, *speeding and automating response*, *expanding the coverage of standards*, and *strengthening protection against firmware manipulation*. Interpretation: there is no single "point of failure"; respondents call for *cross-cutting strengthening* of detection and response mechanisms.

Q7 — Observed limitations

Zero-day attacks, *response latency*, and *other limitations* (e.g., implementation complexity and performance trade-offs) each reached 70.0%. *Supply-chain failures* and *integration with other systems* were cited by 60.0%. Interpretation: weaknesses cluster around highly novel threats, time to react, and ecosystem integration.

Priorities should include: (i) real-time telemetry and correlation with actionable playbooks, (ii) hardening of update processes and secure rollback, (iii) integration paths and tabletop tests with adjacent systems, and (iv) objective prioritisation criteria where standards overlap.

6.2.2 Resilience and advanced threats (Q11, Q13)

Q11 — Gains required for resilience

Detection of unknown attacks and *improvements to the firmware update process* lead with 66.7%, followed by *adaptation to emerging threats* at 55.6%, and, to a lesser extent, *redundancy* and *continuous learning* at 33.3%. Interpretation: *proactive* mechanisms (detection and updating) are viewed as more critical than general structural capabilities.

Q13 — Gaps regarding advanced threats

Clear priorities are *zero-day mitigation* and *supply-chain security* (70.0%). *Physical attacks* (50.0%) and *ransomware* (40.0%) form the second tier. Interpretation: explicit practices and evidence are required for supply chain and for response to vulnerabilities without available patches.

Establish: (i) triage and containment paths for zero-day scenarios, (ii) SBOM and VEX governance with risk criteria for dependencies, and (iii) tabletop exercises for physical-attack and ransomware scenarios with decision thresholds and recovery metrics.

6.2.3 Integration between standards and IT–embedded convergence (Q15, Q17, Q18)

Q15 — Improvements for standards integration

Alignment of requirements (66.7%) and *harmonisation of certification* (55.6%) are the main demands; *tool interoperability* and *control mapping* appear with 44.4%. Interpretation: full integration depends less on creating new artefacts and more on *harmonising* what already exists.

Q17 and Q18 — Effective elements of IT–embedded integration

Network monitoring leads in both questions (80.0%). *Alignment of incident responses* (60.0% and 40.0%), *synchronisation across systems* (50.0% in both), and *multifactor authentication* (40.0% and 20.0%) complete the picture. Interpretation: visibility and tactical coordination across domains are the practical pillars of integration.

Consolidate: (i) a matrix of equivalence between aviation and IT requirements, (ii) shared evidence flows, (iii) minimum viable integrations for telemetry and incident management, and (iv) scenario-based interoperability guides.

6.2.4 Operational benefits (Q23, Q26, Q27)

Q23 — Perceived benefits

Security reinforcement (87.5%), *regulatory compliance* and *team communication* (75.0% each), followed by *incident resilience* (62.5%). Interpretation: operational value arises from security gains and improved collaboration.

Q26 — Security benefits

Enhanced detection is unanimous (100.0%); *effective response* is 60.0%; *incident reduction* and *compliance* are 50.0%. Interpretation: perceived benefit is more consolidated in *detection* than in *prevention*.

Q27 — Operational efficiency

Better coordination across teams 100.0%; *process automation* 70.0%; *productivity* 50.0%; *downtime reduction* 30.0%. Interpretation: coordination and automation are the central vectors of perceived efficiency.

Document representative use cases with: (i) detection KPIs and MTTR, (ii) cadences for cross-team integration, and (iii) incremental automations with productivity and availability metrics.

6.2.5 Adoption barriers and comprehension (Q20, Q22, Q24)

Q20 — Principal challenges

Specialised personnel 100.0%; *time and resources* 90.0%; *cost* 80.0%; *legacy integration* 70.0%; *technical complexity* 60.0%; *cultural resistance* 30.0%. **Interpretation**: adoption hinges on *capacity* and *funding*, with legacy integration as a critical factor.

Q22 — Facilitating understanding

Detailed documentation and *practical examples* 30.0% each; *alignment with existing frameworks* and *training* 20.0% each; *process simplification* 0.0%. **Interpretation**: the demand is for *supporting artefacts* (guides and examples) rather than scope reduction.

Q24 — Negative operational impacts

Increased complexity 80.0%; *integration difficulties* 70.0%; *costs* 60.0%; *performance* 40.0%. **Interpretation**: adverse effects stem from integration and governance overhead rather than intrinsic technical infeasibility.

A mitigation plan should include: (i) maturity-based adoption tracks with *quick wins*, (ii) resource

planning and capacity building, (iii) integration guides for legacy environments and performance impact tests, and (iv) a minimal viable evidence catalogue.

6.2.6 Cross-cutting synthesis and priorities

Main points of consensus

- **Monitoring and detection** are widely recognised pillars (Q5, Q8, Q17, Q18, Q26).
- **Standards integration and harmonisation** across domains recur as priorities (Q15, Q17, Q18).
- **Supply chain and zero-day** require targeted reinforcement (Q7, Q13).
- **Adoption depends on organisational capacity** and resources (Q20), supported by documentation and examples (Q22).

Bottlenecks and risks

- *Response time* and *legacy integration* as limiting factors (Q7, Q24).
- *Operational complexity* and *cost* as sources of overhead (Q24).

Recommended high-level roadmap

1. **Strengthen telemetry and response** (Q6): real-time correlation, versioned playbooks, decision thresholds, and secure firmware rollback.
2. **Harmonise standards** (Q15): requirement matrices, control mappings, equivalent evidence, and cross-certification paths.
3. **Establish supply-chain governance** (Q13): SBOM and VEX, risk criteria for dependencies, and tabletop exercises for zero-day scenarios.
4. **Adopt maturity-based rollout** (Q20, Q22): documentation and example kits, training tracks, minimum useful integrations, and benefit measurement (MTTD/MTTR, productivity).

In line with the methodological orientation of the dissertation, the multiple-choice questions are analysed separately because they measure independent items. Axis-level acceptance analyses, where applicable, remain based on the single-choice questions appropriate to each axis.

6.3 DISCUSSION OF THE QUANTITATIVE RESULTS

The quantitative analysis examines the distribution of concordance and acceptance indices derived from the questionnaire. By separating the results at the level of individual questions and aggregating them by

thematic axis, the discussion identifies where the framework is well received and where divergences occur. The following subsections organise the findings accordingly.

6.3.1 Concordance by Question

Figure 6.9 shows the distribution of the concordance index by question, with the questions organised by thematic axis and differentiated by colours. The green line reference the overall average acceptance per question 70.06%, enable a direct comparison between the uniformity of responses and the overall perception of approval of the framework.

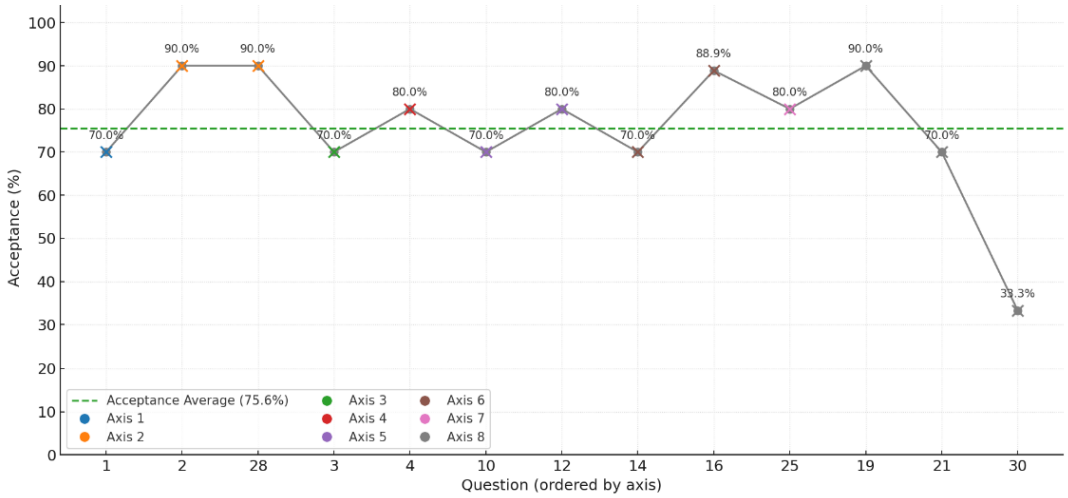

Figure 6.9: Concordance index by question with the average acceptance and the overall mean of concordance.

Concordance varies substantially across questions, ranging from 100% to 30%. Despite this variability, the acceptance line consistently lies above the overall concordance mean, indicating that, even when responses are not fully aligned, the framework is largely perceived in a positive light.

The pattern of dispersion also differs across axes. Some groups of questions display a cluster of points above both reference lines, reflecting simultaneous consensus and acceptance. Others alternate sharply between higher and lower values, suggesting that perceptions depend strongly on the specific context or subtheme addressed. This heterogeneity indicates that targeted adjustments could increase convergence of responses without undermining aspects of the framework that are already consolidated.

In sum, the figure suggests that the central challenge is not primarily to raise acceptance—which is already high—but to reduce variability in concordance. Greater uniformity of perceptions, particularly in the axes with more pronounced oscillations, is likely to be achieved through clarifications and focused guidance.

7 QUALITATIVE ANALYSIS OF THE RESULTS

A qualitative approach based on axial and categorical coding was adopted in order to deepen the interpretation of the open rationales and additional comments provided by the experts. This method enabled the identification of recurrent themes and patterns of meaning, allowing the textual corpus to be structured into analytical categories consistent with the validation objectives. The initial coding was carried out inductively and later organized into relational axes, which contributed to a more refined analysis of the perceptions expressed by the participants (183).

The most recurrent emerging categories included: (i) clarity and documentary structure of the framework, reflecting concerns with the form of presentation and organization of the methodological components; (ii) normative alignment, with an emphasis on the compatibility between the proposal and international standards such as NIST SP 800-53 and ISO/IEC 27001; (iii) practical implementation barriers, such as operational costs and integration limitations with legacy systems; and (iv) perceptions about adaptability, training and automation, which indicate critical factors for adoption in different sectors. The interpretation of these categories was carried out in the light of contemporary literature on embedded security, which recognizes the technical and organizational challenges in consolidating robust methodological approaches for critical contexts. This triangulation between empirical data and theoretical references reinforces the interpretive validity of the findings (182, 184).

The previous chapter presented a quantitative analysis of the thirty questions of the validation questionnaire of the holistic framework for the protection of embedded systems. Absolute and percentage frequencies were displayed for each response alternative and the general perceptions of the specialists were discussed. However, percentages and averages can conceal relevant nuances that only emerge when the data are interpreted from a qualitative perspective. This chapter, therefore, resorts to axial and categorical coding to explore patterns and relationships between the responses, allowing a richer understanding of the meanings attributed by the experts.

Coding in the context of qualitative research consists of assigning labels to data fragments (codes) and subsequently grouping these codes into categories or analytical themes. Whereas codes represent simple initial tags, such as “partially satisfactory” or “resilient”, the categories correspond to more abstract analytical constructs that connect different codes to each other. In this study, a process based on the principles of Grounded Theory is adopted, in which coding unfolds in three stages: open, axial and selective coding (183, 185, 186).

The axial stage is central to this process, as it seeks to reorganize the fragmented data from open coding, establishing connections between categories and subcategories. Axial coding consists of “assembling the data in a new way by making connections between categories”. It is at this moment that the researcher seeks to understand how the elements are articulated to form a coherent and explanatory whole. This phase makes it possible to identify the conditions, contexts, actions/interactions and consequences associated with each category, providing a robust theoretical framework for the analysis (183, 185).

The categories that emerge from axial coding thus function as organizing axes of understanding. They

not only group related concepts but also reveal how different dimensions of the specialists' experience influence each other. This approach makes it possible to capture in greater depth the perceptions, uncertainties and expectations expressed in the responses to the questionnaire, complementing and enriching the purely statistical analysis carried out in the previous chapter.

7.1 QUALITATIVE METHODOLOGY ADOPTED

The present qualitative analysis followed an approach with emphasis on the stages of open (initial), axial and categorical coding. This approach is widely used in qualitative studies to construct meanings from empirical data and generate interrelated conceptual categories (183, 187).

7.1.1 Stages of Coding

Initial (open) coding – Based on the frequencies and descriptions of the questions in the eight thematic axes of the questionnaire, codes representing the perceptions expressed by the specialists were identified. Open coding consists of fragmenting the data into smaller conceptual units, labelled with terms that capture the meaning of the responses. For example, in Question 1 the code *partial coverage* was created for the most chosen alternative and *total coverage* for the minority alternative. In multiple-choice questions, each option ticked generated a distinct code (such as *high adaptability*, *limitations in prioritization* or *need for automation*). This stage resulted in a broad list of codes that reflect the nuances of the experts' responses (185, 186).

Axial coding – In the second stage, the codes were grouped into categories and subcategories associated with the thematic axes of the questionnaire. Axial coding aims to reorganize the deconstructed data, connecting categories based on their properties and dimensions. In this stage, we sought to identify relationships between perceptions arising from different questions. For example, codes that reflected partiality (present in several axes) were brought together in the category *Perception of incomplete implementation*. Codes linked to the need for improvements were organized in the category *Demands for improvement*. The analysis of the relationship between these categories made it possible to observe how one perception (such as partiality) influences others (such as *adoption barriers*) (183, 188, 189).

Categorical coding – After the formation of the main categories, a categorical map was constructed in which each category was described by subcategories and linked to the corresponding axes. This process makes it possible to synthesize a large number of codes into a relatively small set of central themes (173).

7.1.2 Analysis Criteria

Frequency and emphasis – Although the analysis is qualitative in nature, the frequency with which certain codes appeared, based on the percentages of the most voted alternatives in each question, was taken into account. This triangulation between qualitative analysis and quantitative data aims to reinforce the internal validity of the results (190, 191). Codes associated with the most frequently chosen alternatives

were prioritized in the formation of categories because of their interpretive relevance.

Convergence – Codes that emerged in different questions or axes were grouped to reveal transversal themes. For example, the idea of *automation* appeared in questions relating to the prioritization of countermeasures, improvements in detection and response mechanisms, and integration with standards, thus forming a subcategory within the category *Demands for improvement*.

Interconnection – Axial coding is based on the premise that categories are not isolated entities but interdependent elements that may have relationships of causality, implication or mutual reinforcement. In this study, an attempt was made to highlight these relationships, such as the connection between *Perception of incomplete implementation* and *Demands for improvement*, since the identification of gaps in the application of the framework tends to generate suggestions for improvement (183).

7.2 CODING RESULTS

To facilitate the interpretation of the data, the categories and subcategories were organized in Table 7.1, using only keywords and short phrases in order to avoid redundancies and maintain clarity.

Table 7.1: Main categories and subcategories derived from the responses

Main category	**Related axes**	**Subcategories (keywords)**
Perception of incomplete implementation	Axis 1 (coverage of demands), Axis 3 (life cycle), Axis 4 (detection and response), Axis 5 (resilience)	Partial coverage; Partial improvement; Partial resilience; Doubts about effectiveness
Demands for improvement	Axis 2 (prioritization of countermeasures), Axis 4 (detection improvements), Axis 5 (improvements for resilience), Axis 6 (integration of standards)	Risk assessment; Clear guidelines; Automation; Detection of unknown attacks; Redundancy; Adaptation to new threats
Recognized value	Axis 7 (operational benefits), Axis 4 (effective aspects), Axis 6 (elements of integration)	Reinforcement of security; Compliance; Improved coordination; Network monitoring; Application of standards
Integration and alignment of frameworks	Axis 6 (integration with DO-326A and NIST SP 800-53), Axis 6 (need for new standards), Axis 6 (TI–on-board synchronization)	Partial integration; Alignment of requirements; Harmonization of certifications; Mapping of controls; Inclusion of new standards
Barriers and challenges to adoption	Axis 8 (ease of implementation, challenges, understanding), Axis 6 (integration limitations), Axis 7 (negative impacts)	Need for specialized personnel; Resources and costs; Technical complexity; Integration with legacy systems; Cultural resistance

Source: Prepared by the author.

7.2.1 Axial Relations between Categories

After building the categorical matrix, a set of relationships between the categories was established using axial coding. The most relevant connections were:

- **Perception of incomplete implementation → Demands for improvement.** The recognition that the framework covers only partially the security demands (70 % in Question 1) or that it only partially improves detection and response (90 % in Question 4) leads the experts to point out areas for improvement. The subcategories *risk assessment*, *automation*, *firmware improvements* and *detection of unknown attacks* emerge directly from this perception.

- **Demands for improvement ↔ Integration and alignment of frameworks.** Many of the proposed improvements involve aligning the framework with standards such as DO-326A and NIST SP 800-53, interoperating tools and mapping controls. Most of the specialists requested the inclusion of new standards (88.9 % in Question 16) and harmonization improvements (66.7 % in Question 15), showing that the demands for improvement involve normative integration.

- **Integration and alignment of frameworks → Barriers and challenges to adoption.** Partial integration and lack of alignment contribute to the perception of difficulty in implementation. In fact, seven specialists considered the implementation moderately difficult (70 % in Question 19) and identified challenges such as the need for specialized personnel (100 % in Question 20), integration with legacy systems (70 %) and high costs (80 %).

- **Recognized value ↔ Perception of incomplete implementation.** Despite the criticisms, the experts acknowledge clear benefits of the framework. All stated that it improves threat detection (100 % in Question 26) and coordination between teams (100 % in Question 27). This *recognized value* balances the perception of partiality and explains why the average recommendation score was 3.0 (Question 30), indicating moderate approval.

- **Recognized value → Demands for improvement.** The identification of effective aspects – such as *continuous monitoring*, *application of standards* and *integration of security standards* – motivates the prioritization of these same areas for future reinforcement. In Question 9, 80 % of respondents suggested strengthening the application of standards and the integration of frameworks, showing that strong points also guide improvement priorities.

These relationships reveal a central narrative: there is a generalized perception that the framework is promising but incomplete. The experts value its impact on security and coordination, while at the same time calling for improvements, especially in the integration with standards and in the automation of processes. The difficulty of adoption is largely due to shortcomings in this integration and to requirements for specialization and resources.

7.3 INSIGHTS FROM THE QUANTITATIVE ANALYSIS

7.3.1 Partial Coverage of Security Demands (Axes 1-4)

The data analysed reveal a balanced panorama between strengths and weaknesses of the framework. In the first four axes it was noted that the approach covers the security demands predominantly partially (Axis 1) and shows a good capacity to adapt to different scenarios, although with limitations that vary between operational and infrastructural contexts (Axis 2). The prioritisation of countermeasures is considered effective, but requires better risk assessment, clearer guidelines and greater automation. Axis 3 showed that the framework covers most of the life cycle phases, but not all, suggesting the need to better specify and integrate stages such as maintenance and decommissioning. In Axis 4, the specialists recognised advances in detection and response, but emphasised that these improvements are only partial; there was consensus that all components – real-time monitoring, automation of response, standards coverage and protection against firmware manipulation – need to be reinforced. The limitations most cited involve zero-day attacks, delays in response and challenges in integration with supply chain and other systems.

7.3.2 Recognised Benefits and Areas for Improvement (Axes 5-8)

On the other hand, the last four axes show that the framework brings tangible benefits, especially in strengthening security, improving coordination between teams and gaining operational efficiency. These aspects presented high concordance indices, indicating collective confidence in the positive effects of the proposal. However, doubts persist as to its resilience in the face of unknown and advanced threats and its ability to fully integrate with consolidated security frameworks. Suggestions for improvement focus on proactive detection, continuous firmware updating, mitigation of zero-day attacks and greater harmonisation with standards from different sectors.

7.4 ADOPTION BARRIERS AND RECOMMENDATIONS

The adoption barriers stand out as a significant challenge: specialised personnel, financial resources and integration with legacy systems are critical factors that can limit the applicability of the framework. The moderate average recommendation (score 3 out of 5) reflects this balance between the perception of benefits and the awareness of constraints. In short, although the framework proves promising and offers concrete value in various aspects, its effective adoption will depend on investment in training, careful integration processes and technical improvements aimed at resilience, full life cycle coverage and compatibility with consolidated standards.

7.4.1 Discussion of the Qualitative Results

The qualitative analysis complements the quantitative findings by capturing expert perceptions that go beyond numerical measures. Through axial coding of open-ended responses, recurring themes were

identified that shed light on both the perceived value of the framework and the limitations that hinder its full adoption. The following subsections organise these themes.

In several axes, the most voted alternatives correspond to intermediate responses (*partially*, *with limitations*). In Question 1, 70 % of the experts stated that the framework only partially covers security demands; none indicated full coverage. Similarly, 60 % considered that the framework covers most phases of the life cycle (Axis 3), but none stated that all phases are contemplated. In the field of detection and response (Axis 4), 90 % stated that the framework only partially improves these processes. These data indicate that there is consensus that the proposal has merit but does not deliver a fully integrated solution.

7.4.2 Demands for Improvement

The improvements suggested by the specialists focus on three areas:

1. **Risk assessment** – 90 % of the participants who identified limitations in the prioritization of countermeasures requested a better risk assessment structure;
2. **Automation and response time** – 75 % of the respondents suggested automating the response to threats and speeding up detection;
3. **Adaptation to emerging threats** – more than 60 % highlighted the need for detection of unknown attacks and to improve the firmware update process.

These demands reflect the expectation of a more proactive and efficient approach.

7.4.3 Recognised Value and Integration with Frameworks

Even with criticisms, the framework is seen as capable of bringing concrete benefits. Reinforcement of security and compliance was cited by more than 75 % of the experts (Question 23), and all acknowledged gains in threat detection (Question 26) and coordination between teams (Question 27). Elements such as network monitoring and alignment of incident responses were pointed out as effective aspects of the integration between IT and embedded systems.

On the other hand, only 10 % believe that the framework fully integrates the DO-326A and NIST SP 800-53 standards, and 88.9 % ask for the inclusion of new standards (Question 16). Partial integration of the frameworks is therefore simultaneously a benefit and a limitation.

7.4.4 Barriers and Challenges to Adoption

The main implementation barriers are associated with human and organizational factors. The need for specialized personnel was unanimously recognized, followed by time and resource limitations and high adoption costs. Technical complexity and integration with legacy systems appear as limiting factors, reflecting the variable maturity of organizations.

In addition, 60 % of the experts consider the framework only partially intuitive (Question 21), and 30 %

suggest that the lack of documentation and practical examples makes it difficult to understand. The negative impacts include increased complexity and integration difficulties (80 % and 70 % in Questions 24), which are closely related to the need for better alignment with existing frameworks.

7.4.5 Synthesis of Qualitative Findings

The qualitative analysis based on axial coding made it possible to go beyond the simple counting of responses and identify patterns in the specialists' perceptions. Five main categories structured this interpretation: *perception of incomplete implementation*, *demands for improvement*, *recognized value*, *integration and alignment of frameworks* and *barriers and challenges to adoption*. The categories are interrelated and converge on a common narrative: respondents recognize the relevance of the framework and the concrete benefits it offers but point out significant gaps – especially in the full coverage of the life cycle, in resilience to advanced threats and in the integration with security standards.

This ambivalence is reflected in the recommendation scores, with an average of 3.0 out of 5, indicating moderate acceptance. The axes that obtained the highest agreement were those related to operational benefits, while axes such as life cycle coverage and adoption barriers showed greater dispersion of opinions.

8 CONCLUSIONS AND FUTURE PERSPECTIVES

This chapter reorganizes the dissertation's takeaways into an *integrated response plan*. Instead of merely summarizing results, it translates empirically grounded findings from Chapter 6 into directives and executable paths, each anchored in existing assets (e.g., Appendix G for risk) and connected to limitations previously identified in Section 8.3. The orientation is decisional and verifiable: findings motivate implications; implications justify directives; directives unfold into implementation paths that specify evaluation criteria and milestones.

8.1 FINAL SYNTHESIS AND CONTRIBUTIONS

This dissertation consolidated and compared two families of approaches for the protection of embedded systems—*comprehensive* (general-purpose, anchored in global information-security standards) and *integrated* (domain-aware, aligning global frameworks with sectoral standards for safety- and security-critical systems). Building on the comparative evidence reported in Chapter 6, the integrated framework demonstrated superior fitness for highly regulated and mission-critical contexts (e.g., aerospace), where safety, certification, and operational continuity impose stringent constraints on design and assurance activities.

Three contributions stand out. First, the framework operationalises a risk-driven security program by combining ISO 31000 for enterprise risk governance with ISO/IEC 27001 for ISMS and control selection guided by NIST SP 800-53 (145, 123, 121). Second, it brings safety and security together along the development lifecycle by incorporating DO-178C and DO-254 process evidence into security assurance claims, and by adopting aviation-specific security standards DO-326A/DO-355A/DO-356A for threat assessment, mitigation, and continued airworthiness (57, 26, 42, 23). Third, it crystallises roles, handoffs, and decision gates in a BPMN model to make the workflow auditable and reproducible across engineering, certification, and operations teams (165).

Empirically, the quantitative study showed high perceived *acceptance* of the proposal (average per-question acceptance $\approx 70.06\%$) with a more heterogeneous *concordance*. Axes related to operational benefits and to efficiency in detection/response outperformed others (e.g., lifecycle coverage and adoption barriers), signalling where the framework already delivers tangible value and where refinements are expected. The qualitative analysis corroborated this picture: specialists recognised concrete gains (coordination, compliance, and early detection), while demanding clearer risk prioritisation, greater automation in response, and stronger coverage of the full lifecycle and emerging threats.

The decisions reported here are operationalized in §8.4 as an integrated response plan that directly reflects quantified expert feedback ($\approx 90\%$ for risk clarity, $\approx 60\%$ for lifecycle coverage, $\approx 70\%$ for countermeasure prioritization).

8.2 IMPLICATIONS FOR PRACTICE

For organisations operating embedded and safety-critical systems, the results support four practical recommendations:

1. **Adopt a security-by-design lifecycle that is safety-aware.** Tie security requirements, verification evidence, and change control to the same artefacts required by DO-178C/DO-254, so that security becomes a first-class citizen in development, verification, and airworthiness processes (57, 26, 42).

2. **Institutionalise risk governance and control baselining.** Use ISO 31000 to frame risk ownership and appetite, ISO/IEC 27001 to structure the ISMS, and NIST SP 800-53 to baseline controls, tailoring them with sectoral guidance from DO-326A/DO-355A/DO-356A (145, 123, 121, 23).

3. **Engineer detect–respond capabilities for the embedded context.** Combine defence-in-depth, least privilege, and secure coding practices with asset-aware monitoring and incident playbooks specific to avionics and supply-chain interfaces (100, 192, 121, 23). Emphasise cryptography, secure boot, and tamper resistance for confidentiality and integrity at rest, in transit, and in execution (2, 139).

4. **Standardise the workflow and interfaces.** Maintain the BPMN process as a living asset linking policy, engineering tasks, and audit trails; this enhances cross-team alignment and reduces MTTR/MTTD through unambiguous responsibilities and escalation paths (165).

8.3 LIMITATIONS OF THE CURRENT PROPOSAL

The proposed framework now provides explicit coverage of the end-of-life stage of the system lifecycle, encompassing continuous maintenance, retrofit governance, obsolescence planning, and secure decommissioning. These activities are operationalized through clearly defined processes, well-specified inputs and outputs, and traceable, auditable evidence artifacts (`EV-050`–`EV-058`), ensuring systematic management and accountability across the final phases of system operation.

In the avionics domain, this evidence set aligns with DO-326A (airworthiness security process), DO-355A (continued airworthiness), DO-356A (methods and considerations), and DO-178C (software assurance) (26, 57, 49, 42), while remaining consistent with the general security control scaffolding of ISO/IEC 27001/27002 and NIST SP 800-53 (123, 139, 121).

Despite these expansions, two critical limitations remain and were forcefully underscored by Airbus specialists during validation. Two fronts require immediate attention: (i) end-of-life and retrofit governance remain only partially operationalised, with open decisions on asset baselining, evidence carryover, and retrofit-triggered re-assurance still demanding structured trade-off studies; and (ii) automation and response latency, which the Airbus specialists characterised as urgent for operational viability at scale.

A second critical limitation involves automation and response latency. As mapped in Table 3.11, the current workflow still depends on human intervention at specific steps (e.g., evidence consolidation, change-impact triage, and certain detect–respond handoffs). This dependency introduces operational la-

tencies that can be unacceptable for safety- and mission-critical contexts, especially where zero-day exploits and advanced firmware manipulation evolve on timelines that outpace manual coordination. This concern was strongly echoed by the specialists: 75% (Question 6) explicitly demanded greater agility in detection–response, citing the need to reduce time-to-detection, containment windows, and mean time to recovery (MTTR) under realistic operating constraints.

Operationally, the net effect is a significant and predictable widening of the detection–to–containment interval under pressure, increasing exposure windows and the probability of cascading effects in avionics mission scenarios. In other words, the current degree of human-in-the-loop coordination—although understandable in early deployments—constitutes a significant operational challenge to the framework's viability at scale in high-threat environments.

Addressing these gaps will require coordinated efforts across engineering, certification, operations, and security governance, with particular emphasis on scaling automation safely in aviation and other critical domains (57, 166, 26, 42).

These limitations directly motivate the directives in §8.4. In particular, we classify the automation–latency limitation as a Priority 1 item and establish Directive D4 to formalise machine-assisted detection–response, compress decision and handoff latency, and accelerate automation for zero-day–class events.

8.4 FUTURE RESEARCH (INTEGRATED RESPONSE PLAN)

The future work presented here is a sequenced response to quantified expert feedback from Chapter 6. Three high-salience findings structure the plan: the request for a clearer and operational risk assessment (90%), the perception of uneven lifecycle coverage with emphasis on end-of-life (60%), and the view that countermeasure prioritization is adequate yet constrained (70%). Each finding motivates an implication, which justifies a directive articulated as a compact implementation path with explicit evaluation criteria. A fourth strand addresses automation and rapid response identified in §8.3.

8.4.1 Strengthening Lifecycle Governance (Directive D1)

Evidence in Chapter 6 indicates that a significant share of experts (Question 3) perceive gaps across the system lifecycle, with particular concern for end-of-life and retrofit activities. The implication is straightforward: without explicit governance and acceptance criteria per lifecycle phase, assurance evidence drifts over time, certification linkages weaken, and change management becomes error-prone.

Directive D1 formalizes lifecycle governance with emphasis on sustainment and retirement. The implementation path is intentionally conservative and evidence-driven. First, existing phase definitions and artifacts are consolidated and extended to cover end-of-life and retrofit decisions, ensuring that activities, evidence types, and acceptance criteria are specified per phase. Second, the evidence trail previously introduced (e.g., EV-050–EV-058) is operationalized to preserve traceability between safety-relevant artifacts (DO-178C/DO-254) and the security control baseline (NIST SP 800-53). Third, a pilot application—using real or semi-synthetic data—tests whether the extended governance reduces rework and increases com-

pleteness over phase transitions.

Evaluation is defined by measurable endpoints rather than narrative claims: coverage per phase (percentage of mandated evidence actually produced), completeness of evidence sets, defects detected per phase, and lead time to update evidence under retrofit. These indicators enable external verification and future replication, addressing the very gaps that motivated D1.

8.4.2 Risk Assessment Structure, Version 2 (Directive D2)

The results (Question 29) show an almost unanimous expectation for a clearer and more operational risk assessment structure. The operational implication is that ambiguity in taxonomies and thresholds inflates inter-rater variability and undermines decision stability across projects and evaluators.

Directive D2 publishes a Version 2 of the risk structure grounded in ISO/IEC 27005 and aligned with the existing materials in Appendix G. The implementation path refines the taxonomy of assets, threats, and vulnerabilities, calibrates scoring rules and decision thresholds, and provides fully reproducible exemplars. Rather than expanding theory, D2 privileges clarity and repeatability and an accompanying reproducible worksheet that encodes the scoring logic, the mapping to NIST SP 800-53/800-30, and several worked examples.

Evaluation focuses on decision quality and efficiency: inter-rater agreement (e.g., Cohen's κ), average assessment time, re-open rates for risk decisions, and stability of outcomes within pre-defined risk bands. Improvements in these indicators constitute the acceptance condition for D2 and provide a cumulative baseline for later refinements.

8.4.3 Countermeasure Prioritization, Version 2 (Directive D3)

Expert feedback indicates that, while the current prioritization approach is directionally sound, it remains constrained for decision-making under resource, schedule, and certification pressure (70% reporting limitations). The implication is that a single-criterion or loosely weighted scheme fails to capture trade-offs among risk reduction, residual risk, deployability, assurance impact, and operational continuity.

Directive D3 delivers a multi-criteria, evidence-based prioritization structure aligned with ISO/IEC 27005 risk treatment and the control selection logic underpinning NIST SP 800-53. The implementation path is deliberately compact: a normalized taxonomy of criteria (e.g., expected risk reduction, residual risk after treatment, time-to-deploy, cost-of-change, safety/certification impact), a transparent weighting scheme with explicit tie-break rules, and a reproducible decision worksheet that encodes the scoring and sensitivity analysis. The structure must remain auditable and lightweight enough to be applied during change and sustainment.

Evaluation focuses on decision robustness and efficiency: inter-rater agreement on top-k selections, sensitivity of rankings to plausible weight perturbations, elapsed time to reach a decision, and the rate of post-decision reversals during assurance reviews. Acceptance is defined as (i) improved agreement relative to the current baseline, (ii) stability of top-k under bounded weight shifts, and (iii) non-inferior time-to-decision.

8.4.4 Automation and Rapid Response (Directive D4)

Building on the limitations discussed in §8.3, this strand targets detection–response latency, including zero-day exposure. The plan operationalizes SBOM→VEX→alert pipelines, telemetry and threat-intelligence consolidation, and playbooks aligned with DO-326A/DO-355A, with evaluation centered on MTTA/MTTR, 24-hour containment rates, and false-positive control. .

Directive D4 accelerates detection–response by integrating software bill of materials (SBOM) with vulnerability exploitability (VEX), threat-intelligence ingestion, and runtime telemetry. The implementation path proceeds in three steps. First, a proof-of-concept pipeline SBOM→VEX→alert establishes end-to-end traceability from component disclosure to actionable cues. Second, telemetry and intelligence feeds are consolidated to support containment playbooks in line with DO-326A/DO-355A. Third, an operational dashboard tracks latency metrics and supports controlled exercises that test *zero-day* playbooks.

Evaluation is centered on latency and control efficacy: mean time to acknowledge (MTTA), mean time to recover (MTTR), percentage of events contained within 24 hours, and false-positive rates. These indicators provide a falsifiable yardstick for D4 and make the response capability auditable over time.

8.5 LONG-TERM VISION AND SECURITY CULTURE

Sustained effectiveness in protecting embedded systems requires more than the technical implementation of standards and controls; it also depends on cultivating a mature security culture. In the aerospace domain, safety and security cannot be treated as separate concerns. Both are intertwined properties of airborne systems, where a single vulnerability can compromise operational integrity, passenger safety, and regulatory compliance. Therefore, the vision for long-term protection must emphasize that safety assurance (as defined by DO-178C and DO-254) and cybersecurity assurance (as structured by DO-326A, DO-355A, and DO-356A) are complementary pillars that reinforce each other (57, 26, 42). This integrated mindset requires organisations to align governance frameworks, operational policies, and engineering practices so that safety and security evolve in tandem across the lifecycle of avionics systems.

Training and awareness initiatives play a central role in consolidating this vision. Programs must go beyond generic cybersecurity courses and instead be tailored to the specific regulatory and operational realities of aviation. For instance, engineers working on airborne software should be trained not only in secure coding practices, but also in how those practices intersect with DO-178C verification evidence. Similarly, hardware specialists must understand how DO-254 assurance activities overlap with physical security mechanisms and cryptographic validation. Operational and maintenance teams, on the other hand, need to be familiar with cyber incident playbooks that directly affect aircraft operability and continued airworthiness, in line with DO-355A requirements (23, 26).

Another key element of this long-term vision is the establishment of institutionalised feedback loops. Security is not static, and neither are the threats that target embedded systems. Periodic exercises, red-team simulations, and scenario-based drills allow organisations to test their preparedness against advanced adversarial tactics. Post-incident reviews provide equally important opportunities to learn from operational

disruptions and to adjust policies, controls, and processes accordingly. These activities should feed directly into a continuous-improvement cycle, ensuring that both policies and practices remain current and resilient to the evolving threat landscape (123, 145, 121).

Finally, fostering a security culture also involves creating organisational incentives and governance structures that reward proactive engagement with cybersecurity. Security champions within engineering, operations, and management teams can act as multipliers, disseminating knowledge and reinforcing best practices across departments. Leadership must promote an environment where reporting vulnerabilities and near-misses is encouraged, not penalised, thereby reducing the risk of latent failures remaining hidden until they cause major incidents. Moreover, collaboration with regulators, industry partners, and academic institutions strengthens collective resilience by sharing threat intelligence, harmonising certification approaches, and advancing research into emerging risks (23, 26, 42).

8.6 CONCLUDING REMARKS

In conclusion, this dissertation has demonstrated that the integrated framework represents a significant advancement in the protection of embedded systems against malicious attacks. By combining ISO/IEC 27001 and NIST SP 800-53 with sector-specific standards such as DO-178C, DO-254, DO-326A, DO-355A, and DO-356A, the framework establishes a robust and auditable framework capable of addressing both the technical and regulatory dimensions of cybersecurity. This alignment ensures that organisations can simultaneously achieve compliance and resilience, thereby strengthening their capacity to withstand evolving cyber threats in environments where operational continuity and safety are non-negotiable (123, 57, 121, 23).

The empirical findings highlighted high acceptance rates among specialists, particularly regarding operational benefits and efficiency in detection and incident response. At the same time, the analysis revealed variability in concordance across certain axes, indicating that while the framework is broadly approved, its implementation requires refinements in areas such as lifecycle completeness and automation of response mechanisms. Qualitative insights complemented these results, showing that experts recognise the framework as a concrete and effective step forward, but also expect improvements in risk prioritisation, integration with legacy systems, and resilience against zero-day threats (166, 26, 42).

To strengthen methodological rigour, an initial GSN-based assurance case prototype was developed (Appendix H), linking the RTM, EV-014, and the POA&M under NIST SP 800-53, ISO/IEC 27001/27002, and DO-326A/DO-356A/DO-355A (121, 123, 139, 26, 42, 49).

From a practical standpoint, the institutionalisation of the BPMN-based workflow emerges as one of the most valuable contributions of this work. By formalising interactions, decision points, and responsibilities, the BPMN model ensures that complex processes are transparent, reproducible, and auditable across different teams and organisations. This approach facilitates communication between IT and operational stakeholders, shortens the mean time to detection (MTTD) and response (MTTR), and strengthens the alignment of safety and security practices. Moreover, it offers a concrete instrument for certification and auditing, enabling regulators and industry partners to verify that processes comply with both global

information-security standards and domain-specific safety/security regulations (165, 23, 26).

Looking ahead, the integrated framework should not be viewed as a static solution but as a living framework subject to continuous improvement. Extending coverage to all lifecycle phases, developing more automated detection and response mechanisms, and strengthening integration with supply-chain security processes will be key priorities. Investments in training, awareness, and skills development will also be crucial for addressing adoption barriers and ensuring sustainability in practice. Ultimately, the integrated framework proposed here offers both a solid foundation for current applications and a flexible platform for future innovations, consolidating its role as a benchmark for cybersecurity in critical embedded systems (57, 121, 23, 26, 42).

BIBLIOGRAPHICAL REFERENCES

1 HEATH, S. *Embedded Systems Design*. 2. ed. Oxford, UK: Newnes, 2002. ISBN 978-0-7506-5546-0. Available in: <https://www.elsevier.com/books/embedded-systems-design/unknown/978-0-7506-5546-0>.

2 STALLINGS, W; BROWN, L. *Computer Security: Principles and Practice, Global Edition*. 4. ed. Pearson, 2018. ISBN 9781292220611. Available in: <https://www.pearson.de/computer-security-principles-and-practice-ebook-global-edition-9781292220635>.

3 HUMAYED, A; LIN, J; LI, F; LUO, B. Cyber-physical systems security—a survey. *IEEE Internet of Things Journal*, 2017, vol. 4, no. 6, p. 1802–1831. Available in: <https://doi.org/10.1109/JIOT.2017.2703172>.

4 MARWEDEL, P. *Embedded System Design: Embedded Systems Foundations of Cyber-Physical Systems, and the Internet of Things*. 4. ed. Cham: Springer, 2021. ISBN 978-3-030-60909-2. Available in: <https://doi.org/10.1007/978-3-030-60910-8>.

5 WOLF, M. *Computers as Components: Principles of Embedded Computing System Design*. 4. ed. Boston, MA: Morgan Kaufmann, 2016. ISBN 978-0-12-805387-4. Available in: <https://www.elsevier.com/books/computers-as-components/wolf/978-0-12-805387-4>.

6 MITCHELL, R; CHEN, I. A survey of intrusion detection techniques for cyber-physical systems. *ACM Computing Surveys*, 2014, vol. 46, no. 4. Available in: <https://doi.org/10.1145/2542049>.

7 E-ISAC; SANS Industrial Control Systems. *Analysis of the Cyber Attack on the Ukrainian Power Grid*. [S.l.], 2016. Defense Use Case (DUC-5). Available in: <https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf>.

8 LANGNER, R. Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy*, 2011, vol. 9, no. 3, p. 49–51. Available in: <https://doi.org/10.1109/MSP.2011.67>.

9 ROBISON, P. *Boeing's 737 Max Software Outsourced to $9-an-Hour Engineers*. 2019. Bloomberg. Available in: <https://www.bloomberg.com/news/articles/2019-06-28/boeing-s-737-max-software-outsourced-to-9-an-hour-engineers>.

10 PANDEY, AB; TRIPATHI, A; VASHIST, PC. A survey of cyber security trends, emerging technologies and threats. In *Cyber Security in Intelligent Computing and Communications*. Singapore: Springer, 2022. p. 19–33. Available in: <https://doi.org/10.1007/978-981-16-8012-0_2>.

11 European Union Agency for Cybersecurity (ENISA). *ENISA Threat Landscape 2021*. 2021. Available in: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021>.

12 PETIT, J; SHLADOVER, SE. Potential cyberattacks on automated vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 2015, vol. 16, no. 2, p. 546–556. Available in: <https://doi.org/10.1109/TITS.2014.2342271>.

13 BODEAU, DJ; GRAUBART, R; PICCIOTTO, J; MCQUAID, R. *Cyber Resiliency Engineering Framework*. [S.l.], 2011. Sem DOI; relatório técnico MTR110237; Approved for Public Release: 11-4436. Available in: <https://www.mitre.org/news-insights/publication/cyber-resiliency-engineering-framework>.

14 WIRKUTTIS, N; KLEIN, H. Artificial intelligence in cybersecurity. *Cyber, Intelligence, and Security*, 2017, vol. 1, no. 1, p. 103–119. Sem DOI atribuído. Available in: <https://www.inss.org.il/publication/artificial-intelligence-cybersecurity/>.

15 DAVI, L; GÖTZFRIED, J; SADEGHI, AR. Holistic approaches to embedded system security. *IEEE Security & Privacy*, 2021, vol. 19, no. 2, p. 24–31. Available in: <https://www.computer.org/csdl/magazine/sp/2021/02/>.

16 ZETTER, K. *Contagem Regressiva até Zero Day: Stuxnet e o lançamento da primeira arma digital do mundo*. Brasport, 2017. Tradução brasileira; sem DOI. ISBN 9788574528274. Available in: <https://books.google.com/books?id=tKIoDwAAQBAJ>.

17 KARPIUK, M. Crisis management vs. cyber threats. *Sicurezza, Terrorismo e Società*, 2022, vol. 16, no. 2, p. 113–123. Sem DOI atribuído. Available in: <https://www.sicurezzaterrorismosocieta.it/wp-content/uploads/2022/12/SicTerSoc16-Karpiuk-Crisis-management-vs.-cyber-threats.pdf>.

18 POLLINI, A; CALLARI, TC; TEDESCHI, A; RUSCIO, D; SAVE, L; CHIARUGI, F; GUERRI, D. Leveraging human factors in cybersecurity: an integrated methodological approach. *Cognition, Technology & Work*, 2022, vol. 24, no. 2, p. 371–390. Available in: <https://doi.org/10.1007/s10111-021-00683-y>.

19 SHOSTACK, A. *Threat Modeling: Designing for Security*. Indianapolis, IN: John Wiley & Sons, 2014. ISBN 978-1118809990. Available in: <https://www.wiley.com/en-us/Threat%2BModeling%3A%2BDesigning%2Bfor%2BSecurity-p-9781118809990>.

20 SCHOITSCH, E. Design for safety and security of complex embedded systems: A unified approach. In *Cyberspace Security and Defense: Research Issues. Proceedings of the NATO Advanced Research Workshop, Gdańsk, Poland, 6–9 September 2004*. Springer, 2005. p. 161–174. Available in: <https://doi.org/10.1007/1-4020-3381-8_9>.

21 KUCHAR, JK; DRUMM, AC. The traffic alert and collision avoidance system. *Lincoln Laboratory Journal*, 2007, vol. 16, no. 2, p. 277–296. Available in: <https://www.ll.mit.edu/r-d/publications/traffic-alert-and-collision-avoidance-system>.

22 MILLETT, LI; THOMAS, M; JACKSON, D. *Software for Dependable Systems: Sufficient Evidence?* National Academies Press, 2007. Available in: <https://doi.org/10.17226/11923>.

23 KLEIDERMACHER, D; KLEIDERMACHER, M. *Embedded Systems Security: Practical Methods for Safe and Secure Software and Systems Development*. Newnes (Elsevier), 2012. ISBN 9780123868862. Available in: <https://doi.org/10.1016/C2010-0-67275-0>.

24 SPITZER, CR (Ed.). *Avionics: Development and Implementation*. CRC Press, 2018. ISBN 9780849384417. Available in: <https://doi.org/10.1201/9781315222233>.

25 MOIR, I; SEABRIDGE, A; JUKES, M. *Civil Avionics Systems*. 2. ed. Chichester: Wiley, 2013. ISBN 978-1-118-34180-3. Available in: <https://doi.org/10.1002/9781118536704>.

26 RTCA, Inc. *DO-178C: Software Considerations in Airborne Systems and Equipment Certification*. Washington, D.C.: RTCA, 2012.

27 MITTAL, K; BATRA, PK. A survey on iot security challenges and solutions. In *Futuristic Sustainable Energy & Technology*. CRC Press, 2022. p. 417–426. Available in: <https://doi.org/10.1201/9781003272328-45>.

28 RAVI, S; RAGHUNATHAN, A; KOCHER, P; HATTANGADY, S. Security in embedded systems: Design challenges. *ACM Transactions on Embedded Computing Systems*, 2004, vol. 3, no. 3, p. 461–491. Available in: <https://doi.org/10.1145/1015047.1015049>.

29 LOVELESS, A. *Overcoming the Performance and Security Challenges of Building Highly-Distributed Fault-Tolerant Embedded Systems*. PhD thesis (PhD Thesis) — University of Kansas, Lawrence, KS, USA, 2023. Available in: <https://kuscholarworks.ku.edu/handle/1808/34330>.

30 BOUMEZRAG, MB. The importance of literature review in research: An overview and guidelines. *The Journal of El-Rissala for Studies and Research in Humanities*, 2022, vol. 7, no. 5, p. 402–410. ISSN 2716-930X. Available in: <https://asjp.cerist.dz/en/article/202872>.

31 FYSARAKIS, K; HATZIVASILIS, G; RANTOS, K; PAPANIKOLAOU, A; MANIFAVAS, C. Embedded systems security challenges. In *Proceedings of the 2nd International Workshop on Measurable Security for Embedded Computing and Communication Systems (MeSeS 2014)*. Vienna, Austria: SCITEPRESS, 2014. p. 255–266. ISBN 978-989-758-032-1.

32 PAPP, D; MA, Z; BUTTYAN, L. Embedded systems security: Threats, vulnerabilities, and attack taxonomy. In *2015 13th Annual Conference on Privacy, Security and Trust (PST)*. Izmir, Turkey: IEEE, 2015. p. 145–152. ISBN 978-1-4799-9967-1. Available in: <https://doi.org/10.1109/PST.2015.7232966>.

33 UKWANDU, E; BEN-FARAH, MA; HINDY, H; BURES, M; ATKINSON, R; TACHTATZIS, C; ANDONOVIC, I; BELLEKENS, X. Cyber-security challenges in aviation industry: A review of current and future trends. *Information*, 2022, MDPI, vol. 13, no. 3, p. 146. ISSN 2078-2489. Available in: <https://doi.org/10.3390/info13030146>.

34 SREENIVASAN, R. An overview of embedded systems security. *International Journal of Advances in Engineering Research*, 2018, vol. 15, no. 3, p. 66–74. ISSN 2231-5152. Print ISSN 2454-1796. Available in: <https://ijaer.com/admin/upload/07%20Sreenivasan%20R%2001361.pdf>.

35 LENARD, T; COLLEN, A; NIJDAM, NA; GENGE, B. A key to embedded system security: Locking and unlocking secrets with a trusted platform module. In *2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. Delft, Netherlands: IEEE, 2023. p. 329–335. ISBN 979-8-3503-2721-2. Available in: <https://doi.org/10.1109/EuroSPW59978.2023.00041>.

36 CHATTERJEE, D. *Cybersecurity Readiness: A Holistic and High-Performance Approach*. Thousand Oaks, CA: SAGE Publications, Inc., 2021. ISBN 978-1-0718-3733-7. Available in: <https://doi.org/10.4135/9781071837313>.

37 HUSSAIN, A; MOHAMED, A; RAZALI, S. A review on cybersecurity: Challenges & emerging threats. In *Proceedings of the 3rd International Conference on Networking, Information Systems & Security (NISS '20)*. New York, NY, USA: Association for Computing Machinery, 2020. p. 1–7. ISBN 978-1-4503-7634-1. Available in: <https://doi.org/10.1145/3386723.3387847>.

38 KOSCHER, K; CZESKIS, A; ROESNER, F; PATEL, S; KOHNO, T; CHECKOWAY, S; MCCOY, D; KANTOR, B; ANDERSON, D; SHACHAM, H; SAVAGE, S. Experimental security analysis of a modern automobile. In *2010 IEEE Symposium on Security and Privacy*. Oakland, CA, USA: IEEE, 2010. p. 447–462. ISBN 978-1-4244-6895-8. Available in: <https://doi.org/10.1109/SP.2010.34>.

39 ZHOU, Y. [retracted] a summary of pid control algorithms based on ai-enabled embedded systems. *Security and Communication Networks*, 2022, Wiley-Hindawi, vol. 2022, no. 1, p. 7156713. ISSN 1939-0114. Retracted article. Available in: <https://doi.org/10.1155/2022/7156713>.

40 ROSSOW, C; DIETRICH, CJ; GRIER, C; KREIBICH, C; PAXSON, V; POHLMANN, N. Prudent practices for designing malware experiments: Status quo and outlook. In *2012 IEEE Symposium on Security and Privacy*. IEEE, 2012. p. 65–79. Available in: <https://ieeexplore.ieee.org/document/6234405>.

41 SMITH, B. *System and Method for Data Collection in an Avionics Network*. Google Patents, 2006. US Patent App. 11/092,470, filed March 28, 2005, and published September 28, 2006. US Patent Application 11/092,470. Available in: <https://patents.google.com/patent/US20060218071A1/en>.

42 RTCA, Inc. *DO-254: Design Assurance Guidance for Airborne Electronic Hardware*. Washington, D.C.: RTCA, 2000.

43 LEVESON, NG. *Engineering a Safer World: Systems Thinking Applied to Safety*. Cambridge, MA: MIT Press, 2011. ISBN 978-0-262-01662-9. Available in: <https://doi.org/10.7551/mitpress/8179.001.0001>.

44 BOYER, RS; MOORE, JS. *A Computational Logic Handbook*. 2. ed. Academic Press, 1998. ISBN 0-12-122955-6. Available in: <https://www.cs.utexas.edu/~boyer/aclh2-blurb.html>.

45 LAPLANTE, PA. *Requirements Engineering for Software and Systems*. 2. ed. [S.l.]: CRC Press, 2017. ISBN 978-1-138-19780-5.

46 RUSHBY, J. *Formal Methods and their Role in the Certification of Critical Systems*. [S.l.], 2013.

47 RTCA, Inc. *DO-331: Model-Based Development and Verification Supplement to DO-178C and DO-278A*. Washington, DC, 2011.

48 WOODCOCK, J; LARSEN, PG; BICARREGUI, J; FITZGERALD, J. Formal methods: Practice and experience. *ACM Computing Surveys*, 2009, vol. 41, no. 4, p. 1–36. Available in: <https://doi.org/10.1145/1592434.1592436>.

49 RTCA, Inc. *DO-326A: Airworthiness Security Process Specification*. Washington, DC, 2014.

50 RTCA, Inc. *DO-355A: Information Security Guidance for Continued Airworthiness*. Washington, DC, 2020.

51 WIPF, H. *Safety Versus Security in Aviation*. Springer, 2020. 29–41 p. (SpringerBriefs in Applied Sciences and Technology). Available in: <https://doi.org/10.1007/978-3-030-47229-0_4>.

52 HAYHURST, KJ; VEERHUSEN, DS; CHILENSKI, JJ; RIERSON, LK. *A Practical Tutorial on Modified Condition/Decision Coverage*. Hampton, VA, 2001. Available in: <https://shemesh.larc.nasa.gov/fm/papers/Hayhurst-2001-tm210876-MCDC.pdf>.

53 KNIGHT, JC. *Fundamentals of Dependable Computing for Software Engineers*. Boca Raton, FL: CRC Press, 2012. ISBN 9781439862559.

54 WOLF, M; WEIMERSKIRCH, A; PAAR, C. Security in automotive bus systems. In *Workshop on Embedded Security in Cars (ESCAR)*. Bochum, Germany: [s.n.], 2004. p. 1–13. Available in: <https://www.weimerskirch.org/files/WolfEtAl_SecureBus.pdf>.

55 SAE International. *ARP4754A: Guidelines for Development of Civil Aircraft and Systems*. Warrendale, PA, 2010. Available in: <https://www.sae.org/standards/content/arp4754a/>.

56 ANDERSON, R; MOORE, T. The economics of information security. *Science*, 2006, AAAS, vol. 314, no. 5799, p. 610–613. Available in: <https://doi.org/10.1126/science.1130992>.

57 RTCA, Inc. *DO-356A: Airworthiness Security Methods and Considerations*. Washington, DC, 2018.

58 International Civil Aviation Organization (ICAO). *Cybersecurity in Civil Aviation*. [S.l.]. Acesso em 2025-04-09. Available in: <https://www.icao.int/Security/Pages/CYSEC-Home.aspx>.

59 HOUMB, SH; FRANQUEIRA, VNL; ENGUM, EA. Quantifying security risk level from cvss estimates of frequency and impact. *Journal of Systems and Software*, 2010, vol. 83, no. 9, p. 1622–1634. Available in: <https://doi.org/10.1016/j.jss.2009.08.023>.

60 VACCA, JR (Ed.). *Computer and Information Security Handbook*. 2. ed. Amsterdam: Morgan Kaufmann (Elsevier), 2012. ISBN 978-0-12-394397-2. Available in: <https://www.sciencedirect.com/book/9780123943972/computer-and-information-security-handbook>.

61 MathWorks. *Model-Based Design for Aerospace and Defense*. [S.l.], n.d. White paper institucional, disponível no site da MathWorks. Available in: <https://www.mathworks.com/content/dam/mathworks/handout/model-based-design-for-aerospace-and-defense.pdf>.

62 ROSS, R; MCEVILLEY, M; OREN, J. *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*. Gaithersburg, MD, 2016. Available in: <https://doi.org/10.6028/NIST.SP.800-160>.

63 ANDERSON, R; MOORE, T. The economics of information security. *Science*, 2006, vol. 314, no. 5799, p. 610–613. Available in: <https://www.science.org/doi/10.1126/science.1130992>.

64 STONEBURNER, G; GOGUEN, A; FERINGA, A. *Risk Management Guide for Information Technology Systems*. Gaithersburg, MD, 2002. Available in: <https://doi.org/10.6028/NIST.SP.800-30>.

65 PECHT, M. Prognostics and health management of electronics. In *Encyclopedia of Structural Health Monitoring*. Wiley, 2009. Available in: <https://doi.org/10.1002/9780470061626.shm118>.

66 VIEGA, J; MCGRAW, G. *Building Secure Software: How to Avoid Security Problems the Right Way*. Boston, MA: Addison-Wesley, 2001. ISBN 978-0-201-72152-2. Available in: <https://www.informit.com/store/building-secure-software-how-to-avoid-security-9780201721522>.

67 ALBERTS, CJ; DOROFEE, AJ. *Managing Information Security Risks: The OCTAVE SM Approach*. Boston, MA: Addison-Wesley Professional, 2002. 512 p. (SEI Series in Software Engineering). ISBN 978-0-321-11886-8. Available in: <https://www.informit.com/store/managing-information-security-risks-the-octave-sm-approach-9780321118868>.

68 SCARFONE, K; MELL, P. *Guide to Intrusion Detection and Prevention Systems (IDPS)*. [S.l.], 2007. Available in: <https://doi.org/10.6028/NIST.SP.800-94>.

69 HUUHTANEN, O. *The Use of CVE-related Databases in Improving the Cybersecurity of Embedded Systems*. Master's thesis (Master's Thesis) — University of Jyväskylä, Jyväskylä, Finland, 2021. Available in: <https://jyx.jyu.fi/handle/123456789/76801>.

70 MARTIN, RA. Managing vulnerabilities in networked systems. *Computer*, 2001, vol. 34, no. 11, p. 32–38. Available in: <https://doi.org/10.1109/2.963441>.

71 XIONG, W; GÜLSEVER, M; KAYA, KM; LAGERSTRÖM, R. A study of security vulnerabilities and software weaknesses in vehicles. In *Secure IT Systems (NordSec 2019), Lecture Notes in Computer Science*. Springer, 2019. p. 204–218. Available in: <https://doi.org/10.1007/978-3-030-35055-0_13>.

72 ASLAN, Ö; AKTUĞ, SS; OZKAN-OKAY, M; YILMAZ, AA; AKIN, E. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, 2023, vol. 12, no. 6, p. 1333. Available in: <https://doi.org/10.3390/electronics12061333>.

73 NAJAFIMEHR, M; ZARIFZADEH, S; MOSTAFAVI, S. A hybrid machine learning approach for detecting unprecedented ddos attacks. *The Journal of Supercomputing*, 2022, vol. 78, no. 6, p. 8106–8136. Available in: <https://doi.org/10.1007/s11227-021-04253-x>.

74 SHAMELI-SENDI, A; AGHABABAEI-BARZEGAR, R; CHERIET, M. Taxonomy of information security risk assessment (isra). *Computers & Security*, 2016, vol. 57, p. 14–30. Available in: <https://doi.org/10.1016/j.cose.2015.11.001>.

75 RIVAL, X; YI, K. *Introduction to Static Analysis: An Abstract Interpretation Perspective*. Cambridge, MA: MIT Press, 2020. ISBN 978-0-262-04341-0. Available in: <https://mitpress.mit.edu/9780262043410/introduction-to-static-analysis/>.

76 OR-MEIR, O; NISSIM, N; ELOVICI, Y; ROKACH, L. Dynamic malware analysis in the modern era—a state of the art survey. *ACM Computing Surveys*, 2019, vol. 52, no. 5, p. 1–48. Available in: <https://doi.org/10.1145/3329786>.

77 ERICSON, CA. *Fault Tree Analysis Primer*. CreateSpace, 2011. ISBN 9781466446106. Available in: <https://books.google.de/books?id=jQtcmgEACAAJ>.

78 OZKAYA, E. *Incident Response in the Age of Cloud: Techniques and Best Practices to Effectively Respond to Cybersecurity Incidents*. Packt Publishing, 2021. Sem DOI. ISBN 9781800569928. Available in: <https://www.packtpub.com/en-us/product/incident-response-in-the-age-of-cloud-9781800569928>.

79 INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO/IEC 27005:2022 — Information security, cybersecurity and privacy protection — Guidance on managing information security risks*. Geneva, CH, 2022. International Standard. Available in: <https://www.iso.org/standard/80585.html>.

80 HAIMES, YY. *Risk Modeling, Assessment, and Management*. 4. ed. Hoboken, NJ: John Wiley & Sons, 2015. ISBN 978-1-119-01798-1. Available in: <https://www.wiley.com/en-mx/Risk+Modeling%2C+Assessment%2C+and+Management%2C+4th+Edition-p-9781119017981>.

81 SOMMESTAD, T; EKSTEDT, M; HOLM, H. The cyber security modeling language: A tool for assessing the vulnerability of enterprise system architectures. *IEEE Systems Journal*, 2013, vol. 7, no. 3, p. 363–373. Available in: <https://doi.org/10.1109/JSYST.2012.2221853>.

82 MAGLARAS, L; FERRAG, M; DERHAB, A; MUKHERJEE, M; JANICKE, H; RALLIS, S. Threats, countermeasures and attribution of cyber-attacks on critical infrastructures. *EAI Endorsed Transactions on Security and Safety*, 2018, vol. 5, no. 16, p. e1. Available in: <https://doi.org/10.4108/eai.15-10-2018.155856>.

83 CICHONSKI, P; MILLAR, T; GRANCE, T; SCARFONE, K. *Computer Security Incident Handling Guide*. Gaithersburg, MD, 2012. Available in: <https://doi.org/10.6028/NIST.SP.800-61r2>.

84 BAYUK, JL; HEALEY, J; ROHMEYER, P; SACHS, MH; SCHMIDT, J; WEISS, J. *Cyber Security Policy Guidebook*. Wiley, 2012. Available in: <https://doi.org/10.1002/9781118241530>.

85 KAUR, R; GABRIJELČIČ, D; KLOBUČAR, T. Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, 2023, vol. 97, p. 101804. Available in: <https://doi.org/10.1016/j.inffus.2023.101804>.

86 ECKHART, M; EKELHART, A; WEIPPL, E. Automated security risk identification using automationml-based engineering data. *IEEE Transactions on Dependable and Secure Computing*, 2022, vol. 19, no. 3, p. 1655–1672. Available in: <https://doi.org/10.1109/TDSC.2020.3033150>.

87 KURE, HI; ISLAM, S; GHAZANFAR, M; RAZA, A; PASHA, M. Asset criticality and risk prediction for an effective cybersecurity risk management of cyber-physical system. *Neural Computing and Applications*, 2022, vol. 34, no. 1, p. 493–514. Available in: <https://doi.org/10.1007/s00521-021-06400-0>.

88 SÖNMEZ, FÖ; HANKIN, C; MALACARIA, P. Attack dynamics: An automatic attack graph generation framework based on system topology, capec, cwe, and cve databases. *Computers & Security*, 2022, vol. 123, p. 102938. Available in: <https://doi.org/10.1016/j.cose.2022.102938>.

89 CEZAR, A; CAVUSOGLU, H; RAGHUNATHAN, S. Outsourcing information security: Contracting issues and security implications. *Management Science*, 2014, INFORMS, vol. 60, no. 3, p. 638–657. Available in: <https://doi.org/10.1287/mnsc.2013.1763>.

90 ROSS, R; MCEVILLEY, T; OREN, J. *Guide for Conducting Risk Assessments*. Gaithersburg, MD, 2012. Available in: <https://doi.org/10.6028/NIST.SP.800-30r1>.

91 WEIPPL, E; SCHRITTWIESER, S. Introduction to security and privacy. In WERTHNER, H; GHEZZI, C; KRAMER, J; NIDA-RÜMELIN, J; NUSEIBEH, B; PREM, E; STANGER, A (Ed.). *Introduction to Digital Humanism: A Textbook*. Springer, 2024. p. 397–414. Available in: <https://doi.org/10.1007/978-3-031-45304-5_26>.

92 National Institute of Standards and Technology. *FIPS PUB 197: Advanced Encryption Standard (AES)*. [S.l.], 2001. Available in: <https://doi.org/10.6028/NIST.FIPS.197>.

93 HANKERSON, D; MENEZES, A; VANSTONE, S. *Guide to Elliptic Curve Cryptography*. New York, NY: Springer, 2004. ISBN 978-0-387-95273-2. Available in: <https://doi.org/10.1007/b97644>.

94 Cloudflare, Inc. *Understanding DDoS Protection*. [S.l.], s.d. Available in: <https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/>.

95 Akamai Technologies. *DDoS Mitigation Solutions*. [S.l.], 2021. Available in: <https://www.akamai.com/solutions/security/ddos-protection>.

96 CARDENAS, AA; AMIN, S; SASTRY, S. Research challenges for the security of control systems. In *Proceedings of the 3rd USENIX Workshop on Hot Topics in Security (HotSec'08)*. [s.n.], 2008. Available in: <https://www.usenix.org/event/hotsec08/tech/full_papers/cardenas/cardenas.pdf>.

97 KHAN, SK; SHIWAKOTI, N; STASINOPOULOS, P; CHEN, Y. Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions. *Accident Analysis & Prevention*, 2020, Elsevier, vol. 148, p. 105837. Available in: <https://doi.org/10.1016/j.aap.2020.105837>.

98 ESTAY, DA S.; SAHAY, R; BARFOD, MB; JENSEN, CD. A systematic review of cyber-resilience assessment frameworks. *Computers & Security*, 2020, Elsevier, vol. 97, p. 101996. Available in: <https://doi.org/10.1016/j.cose.2020.101996>.

99 KNAPP, ED. *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. 3. ed. Elsevier, 2024. Sem DOI (edição 2024). ISBN 9780443137372. Available in: <https://shop.elsevier.com/books/industrial-network-security/knapp/978-0-443-13737-2>.

100 SALTZER, JH; SCHROEDER, MD. The protection of information in computer systems. *Proceedings of the IEEE*, 1975, vol. 63, no. 9, p. 1278–1308. Available in: <https://doi.org/10.1109/PROC.1975.9939>.

101 MathWorks. *Polyspace: Static Analysis and Verification Tools for Avionics Software*. [S.l.], s.d. Available in: <https://www.mathworks.com/products/polyspace/industry-standards/avionics.html>.

102 OWASP. *Top 10 Security Risks*. [S.l.], 2024. Available at: <https://owasp.org>.

103 HOWARD, M; LIPNER, S. *The Security Development Lifecycle*. Redmond, WA: Microsoft Press, 2006. ISBN 978-0-7356-2214-2. Available in: <https://www.microsoftpressstore.com/store/security-development-lifecycle-9780735622142>.

104 GRAFF, MG; WYK, KR van. *Secure Coding: Principles and Practices*. Sebastopol, CA: O'Reilly Media, Inc., 2003. No DOI. ISBN 978-0-596-00242-8. Available in: <https://www.oreilly.com/library/view/secure-coding-principles/0596002424/>.

105 HUSSAIN, A. Use of firewall and ids to detect and prevent network attacks. *International Journal of Technical Research & Science*, 2018, vol. 3, no. 9, p. 289–292. Available in: <https://doi.org/10.30780/IJTRS.V3.I9.2018.002>.

106 COULIBALY, K. An overview of intrusion detection and prevention systems. *arXiv preprint arXiv:2004.08967*, 2020. Available in: <https://doi.org/10.48550/arXiv.2004.08967>.

107 GANESH, V; SHARMA, M. Intrusion detection and prevention systems: A review. In RANGANATHAN, G; CHEN, J; ROCHA, Á (Ed.). *Inventive Communication and Computational Technologies: Proceedings of ICICCT 2020*. Singapore: Springer, 2021. (Lecture Notes in Networks and Systems, vol. 145). p. 835–844. Available in: <https://doi.org/10.1007/978-981-15-7345-3_71>.

108 FARAYOLA, OA; OLORUNFEMI, OL; SHOETAN, PO. Data privacy and security in it: a review of techniques and challenges. *Computer Science & IT Research Journal*, 2024, Fair East Publishers, vol. 5, no. 3, p. 606–615. Available in: <https://doi.org/10.51594/csitrj.v5i3.909>.

109 JYOTHI, VE; PRASAD, BDCN; MOJJADA, RK. Analysis of cryptography encryption for network security. In IOP PUBLISHING. *IOP Conference Series: Materials Science and Engineering*. 2020. vol. 981, no. 2, p. 022028. Available in: <https://doi.org/10.1088/1757-899X/981/2/022028>.

110 DALMAZO, BL; MARQUES, JA; COSTA, LR; BONFIM, MS; CARVALHO, RN; SILVA, AS da; FERNANDES, S; BORDIM, JL; ALCHIERI, E; SCHAEFFER-FILHO, A et al. A systematic review on distributed denial of service attack defense mechanisms in programmable networks. *International Journal of Network Management*, 2021, Wiley, vol. 31, no. 6, p. e2163. Available in: <https://doi.org/10.1002/nem.2163>.

111 WU, Z; LI, W; LIU, L; MENG, Y. Low-rate dos attacks, detection, defense, and challenges: A survey. *IEEE Access*, 2020, IEEE, vol. 8, p. 43920–43943. Available in: <https://doi.org/10.1109/ACCESS.2020.2976609>.

112 YAMAUCHI, T; AKAO, Y; YOSHITANI, R; NAKAMURA, Y; HASHIMOTO, M. Additional kernel observer: privilege escalation attack prevention mechanism focusing on system call privilege changes. *International Journal of Information Security*, 2021, Springer, vol. 20, p. 461–473. Available in: <https://doi.org/10.1007/s10207-020-00514-7>.

113 MEHMOOD, M; AMIN, R; MUSLAM, MMA; XIE, J; ALDABBAS, H. Privilege escalation attack detection and mitigation in cloud using machine learning. *IEEE Access*, 2023, IEEE, vol. 11, p. 46561–46576. Available in: <https://doi.org/10.1109/ACCESS.2023.3273895>.

114 YAACOUB, JPA; SALMAN, O; NOURA, HN; KAANICHE, N; CHEHAB, A; MALLI, M. Cyber-physical systems security: Limitations, issues and future trends. *Microprocessors and Microsystems*, 2020, Elsevier, vol. 77, p. 103201. Available in: <https://doi.org/10.1016/j.micpro.2020.103201>.

115 NUIAA, RR; MANICKAM, S; ALSAEEDI, AH. Distributed reflection denial of service attack: A critical review. *International Journal of Electrical and Computer Engineering (IJECE)*, 2021, vol. 11, no. 6, p. 5327–5341. Available in: <https://doi.org/10.11591/ijece.v11i6.pp5327-5341>.

116 GEACH, D. Grid cyber security: secure by design, continuous threat monitoring, effective incident response and board oversight. *Network Security*, 2021, vol. 2021, no. 6, p. 9–12. Available in: <https://doi.org/10.1016/S1353-4858(21)00064-7>.

117 ALOSEEL, A; HE, H; SHAW, C; KHAN, MA. Analytical review of cybersecurity for embedded systems. *IEEE Access*, 2021, vol. 9, p. 961–982. ISSN 2169-3536. Available in: <https://doi.org/10.1109/ACCESS.2020.3045972>.

118 PAXSON, V. Bro: A system for detecting network intruders in real-time. *Computer Networks*, 1999, vol. 31, no. 23–24, p. 2435–2463. Available in: <https://doi.org/10.1016/S1389-1286(99)00112-7>.

119 ROESCH, M. Snort — lightweight intrusion detection for networks. In *Proceedings of the 13th USENIX Conference on System Administration (LISA '99)*. USENIX Association, 1999. p. 229–238. Available in: <https://www.usenix.org/legacy/event/lisa99/full_papers/roesch/roesch.pdf>.

120 GASHI, I; POVYAKALO, AA; STRIGINI, L. Diversity, safety and security in embedded systems: Modelling adversary effort and supply chain risks. In *2016 12th European Dependable Computing Conference (EDCC)*. Gothenburg, Sweden: IEEE, 2016. p. 13–24. ISBN 978-1-5090-1582-5. Available in: <https://doi.org/10.1109/EDCC.2016.27>.

121 National Institute of Standards and Technology. *Security and Privacy Controls for Information Systems and Organizations*. Gaithersburg, MD, 2020. Available in: <https://doi.org/10.6028/NIST.SP.800-53r5>.

122 CICHONSKI, P; MILLAR, T; GRANCE, T; SCARFONE, K. *Computer Security Incident Handling Guide*. [S.l.], 2012. Available in: <https://doi.org/10.6028/NIST.SP.800-61r2>.

123 INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. 2022. Available in: <https://www.iso.org/standard/27001>.

124 ALTHUNAYYAN, M; SAXENA, N; LI, S; GOPE, P. Evaluation of black-box web application security scanners in detecting injection vulnerabilities. *Electronics*, 2022, vol. 11, no. 13, p. 2049. Available in: <https://doi.org/10.3390/electronics11132049>.

125 EFE, A; ABAC1, . Comparison of the host based intrusion detection systems and network based intrusion detection systems. *Celal Bayar University Journal of Science*, 2022, vol. 18, no. 1, p. 23–32. Available in: <https://doi.org/10.18466/cbayarfbe.832533>.

126 RAJ, R; SRIRAM, R; RAKESH, R; RAJEEV, P; LATHA, EV. Low-rate denial of service attack mitigation using resource usage tracking. In IEEE. *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*. 2023. p. 1–5. Available in: <https://doi.org/10.1109/ICCCNT56998.2023.10307051>.

127 SIZOV, N. *Securing Organizational Assets: A Comprehensive Analysis of Privileged Access Management*. 2024. 63 p. Bachelor's thesis. Available in: <https://www.theseus.fi/handle/10024/850550>.

128 LU, MC; HUANG, QX; CHIU, MY; TSAI, YC; SUN, HM. Psps: A step toward tamper resistance against physical computer intrusion. *Sensors*, 2022, vol. 22, no. 5, p. 1882. Available in: <https://doi.org/10.3390/s22051882>.

129 KBAR, G; ALAZAB, A. A comprehensive protection method for securing the organization's network against cyberattacks. In *Proceedings - 2019 Cybersecurity and Cyberforensics Conference (CCC 2019)*. Melbourne, Australia: Institute of Electrical and Electronics Engineers, 2019. p. 118–122. ISBN 978-1-7281-2600-5. Available in: <https://doi.org/10.1109/CCC.2019.00005>.

130 BUEDE, DM; MILLER, WD. *The Engineering Design of Systems: Models and Methods*. 4. ed. Hoboken, NJ: John Wiley & Sons, 2024. ISBN 978-1-119-98401-6. Available in: <https://books.google.com/books?id=yWX7EAAAQBAJ>.

131 HWANG, I; WAKEFIELD, R; KIM, S; KIM, T. Security awareness: The first step in information security compliance behavior. *Journal of Computer Information Systems*, 2021, Taylor & Francis, vol. 61, no. 4, p. 345–356. Available in: <https://doi.org/10.1080/08874417.2019.1650676>.

132 PETRASCH, RJ; PETRASCH, RR. Data integration and interoperability: Towards a model-driven and pattern-oriented approach. *Modelling*, 2022, MDPI, vol. 3, no. 1, p. 105–126. Available in: <https://doi.org/10.3390/modelling3010008>.

133 HASAN, S; ALI, M; KURNIA, S; THURASAMY, R. Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, 2021, Elsevier, vol. 58, p. 102726. Available in: <https://doi.org/10.1016/j.jisa.2020.102726>.

134 GEORGE, PG; RENJITH, VR. Evolution of safety and security risk assessment methodologies towards the use of bayesian networks in process industries. *Process Safety and Environmental Protection*, 2021, Elsevier, vol. 149, p. 758–775. Available in: <https://doi.org/10.1016/j.psep.2021.03.031>.

135 HUBBARD, DW. *The Failure of Risk Management: Why It's Broken and How to Fix It*. 2. ed. Hoboken, NJ: John Wiley & Sons, 2020. ISBN 978-1-119-52203-4. Available in: <https://doi.org/10.1002/9781119521914>.

136 HERATH, TC; HERATH, HSB; CULLUM, D. An information security performance measurement tool for senior managers: Balanced scorecard integration for security governance and control frameworks. *Information Systems Frontiers*, 2023, Springer, vol. 25, no. 2, p. 681–721. Available in: <https://doi.org/10.1007/s10796-022-10246-9>.

137 BLANCHET, B. *ProVerif: Cryptographic Protocol Verifier in the Formal Model*. 2019. <https://proverif.inria.fr>. Acessado em 2025-01-27.

138 MEIER, S; SCHMIDT, B; BASIN, D. *Tamarin Prover: Tool for Security Protocol Analysis*. 2020. <https://tamarin-prover.github.io>. Acessado em 2025-01-27.

139 INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO/IEC 27002:2022 — Information security, cybersecurity and privacy protection — Information security controls*. Geneva, CH, 2022. Available in: <https://www.iso.org/standard/75652.html>.

140 MOYÓN, F; SOARES, R; PINTO-ALBUQUERQUE, M; MENDEZ, D; BECKERS, K. Integration of security standards in devops pipelines: An industry case study. In *Product-Focused Software Process Improvement (PROFES 2020), Lecture Notes in Computer Science*. Springer, 2020. vol. 12562, p. 434–452. Available in: <https://doi.org/10.1007/978-3-030-64148-1_27>.

141 RANGNAU, T; BUIJTENEN, R van; FRANSEN, F; TURKMEN, F. Continuous security testing: A case study on integrating dynamic security testing tools in ci/cd pipelines. In *2020 IEEE 24th International Enterprise Distributed Object Computing Conference (EDOC)*. IEEE, 2020. p. 145–154. Available in: <https://doi.org/10.1109/EDOC49727.2020.00026>.

142 Zeek Project. *Zeek IDS (formerly Bro)*. [S.l.], s.d. Available in: <https://zeek.org>.

143 SAE ITC / ARINC. *ARINC 664, Part 7 — Avionics Full-Duplex Switched Ethernet (AFDX)*. [S.l.], 2009. Available in: <https://www.sae-itc.com/arinc-standards/664p7>.

144 IDRIS, M; SYARIF, I; WINARNO, I. Development of vulnerable web application based on owasp api security risks. In IEEE. *2021 International Electronics Symposium (IES)*. 2021. p. 190–194. Available in: <https://doi.org/10.1109/IES53407.2021.9593934>.

145 International Organization for Standardization. *ISO 31000:2018 — Risk Management — Guidelines*. Geneva: ISO, 2018. Available in: <https://www.iso.org/standard/65694.html>.

146 INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. 2022. Available in: <https://www.iso.org/standard/27001>.

147 DAEMEN, J; RIJMEN, V. *The Design of Rijndael: AES — The Advanced Encryption Standard*. Berlin, Heidelberg: Springer, 2002. ISBN 978-3-540-42580-9. Available in: <https://link.springer.com/book/10.1007/978-3-662-04722-4>.

148 RIVEST, RL; SHAMIR, A; ADLEMAN, L. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 1978, vol. 21, no. 2, p. 120–126. Available in: <https://doi.org/10.1145/359340.359342>.

149 SAE ITC / ARINC. *ARINC Specification 429: Digital Information Transfer System (DITS)*. [S.l.], 2010. Available in: <https://www.sae-itc.com/arinc-standards/429>.

150 SCARFONE, K; MELL, P. *Building an Information Technology Security Awareness and Training Program*. Gaithersburg, MD, 2003. Available in: <https://doi.org/10.6028/NIST.SP.800-50>.

151 CICHONSKI, P; MILLAR, T; GRANCE, T; SCARFONE, K. *Computer Security Incident Handling Guide*. Gaithersburg, MD, 2012. Available in: <https://doi.org/10.6028/NIST.SP.800-61r2>.

152 Avionics Maintenance Committee. *Obsolescence Management Strategies for Commercial Aircraft (ARINC Report 662-1)*. Washington, D.C., 2019. Information Report. Available in: <https://standard.globalspec.com/std/13310583/arinc-662>.

153 SEACORD, RC; RAFAIL, JA. Secure coding standards. In *Proceedings of the Static Analysis Summit*. Gaithersburg, MD, USA: National Institute of Standards and Technology (NIST), 2006. (NIST Special Publication 500-271), p. 17–23.

154 POPEK, GJ; KLINE, CS. Encryption and secure computer networks. *ACM Computing Surveys*, 1979, Association for Computing Machinery, New York, NY, USA, vol. 11, no. 4, p. 331–356. ISSN 0360-0300. Available in: <https://doi.org/10.1145/356789.356794>.

155 KORCHENKO, A; KRYVORUCHKO, O; KOSTIUK, M; KAZMIRCHUK, S; SYNICHUK, O; ZAKHAROV, R. Methods of security authentication and authorization into informationals systems. In *2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT)*. Kyiv, Ukraine: IEEE, 2020. p. 270–274. ISBN 9781728198002. Available in: <https://doi.org/10.1109/ATIT50783.2020.9349333>.

156 BRUEGGER, P. Authentication and authorization. In FUHRER, P; PASQUIER, J (Ed.). *Advanced Software Engineering Topics: Aspect-Oriented Programming*. Fribourg, Switzerland: University of Fribourg, 2006. Course compendium, Summer Semester 2006.

157 ZAVE, P. An operational approach to requirements specification for embedded systems. *IEEE Transactions on Software Engineering*, 1982, IEEE, vol. 8, no. 3, p. 250–269. ISSN 0098-5589. Available in: <https://doi.org/10.1109/TSE.1982.235254>.

158 HONG, JB; KIM, DS. Towards scalable security analysis using multi-layered security models. *Journal of Network and Computer Applications*, 2016, Elsevier, vol. 75, p. 156–168. ISSN 1084-8045. Available in: <https://doi.org/10.1016/j.jnca.2016.08.024>.

159 YOUNG, W; LEVESON, NG. An integrated approach to safety and security based on systems theory. *Communications of the ACM*, 2014, Association for Computing Machinery, New York, NY, USA, vol. 57, no. 2, p. 31–35. ISSN 0001-0782. Available in: <https://doi.org/10.1145/2556938>.

160 GASHI, I; POVYAKALO, AA; STRIGINI, L; MATSCHNIG, M; HINTERSTOISSER, T; FISCHER, B. Diversity for safety and security in embedded systems. In *2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) — Fast Abstracts*. Atlanta, GA, USA: IEEE, 2014. Fast Abstract. Available in: <https://openaccess.city.ac.uk/id/eprint/3521/>.

161 HÖLLER, A; RAUTER, T; IBER, J; KREINER, C. Towards dynamic software diversity for resilient redundant embedded systems. In FANTECHI, A; PELLICCIONE, P (Ed.). *Software Engineering for Resilient Systems: 7th International Workshop, SERENE 2015, Paris, France, September 7–8, 2015. Proceedings*. Cham: Springer, 2015. (Lecture Notes in Computer Science, vol. 9274), p. 16–30. ISBN 978-3-319-23128-0. Available in: <https://doi.org/10.1007/978-3-319-23129-7_2>.

162 PAPP, D; MA, Z; BUTTYÁN, L. Embedded systems security: Threats, vulnerabilities, and attack taxonomy. In *2015 13th Annual Conference on Privacy, Security and Trust (PST)*. Izmir, Turkey: IEEE, 2015. p. 145–152. ISBN 978-1-4673-7828-4. Available in: <https://doi.org/10.1109/PST.2015.7232966>.

163 CHAMELOT, T; COUROUSSÉ, D; HEYDEMANN, K. Mafia: Protecting the microarchitecture of embedded systems against fault injection attacks. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2023, vol. 42, no. 12, p. 4555–4568. Available in: <https://doi.org/10.1109/TCAD.2023.3276507>.

164 LONG, M; WU, CH; HUNG, JY. Denial of service attacks on network-based control systems: Impact and mitigation. *IEEE Transactions on Industrial Informatics*, 2005, vol. 1, no. 2, p. 85–96. Available in: <https://doi.org/10.1109/TII.2005.844422>.

165 WHITE, SA. *Introduction to BPMN*. 2006. <https://www.omg.org/bpmn/Documents/OMG_BPMN_Tutorial.pdf>.

166 WHITMAN, ME; MATTORD, HJ. *Principles of Information Security*. 7. ed. Cengage Learning, 2021. ISBN 9780357506431. Available in: <https://www.cengage.com/c/principles-of-information-security-7e-whitman-mattord/9780357506431/>.

167 TIPTON, HF; KRAUSE, M (Ed.). *Information Security Management Handbook*. 7. ed. Boca Raton, FL: CRC Press, 2017.

168 PATTON, MQ. *Qualitative Research & Evaluation Methods*. 3. ed. Thousand Oaks, CA: SAGE Publications, 2002. URL original indisponível; disponível no catálogo da SAGE. ISBN 9780761919735. Available in: <https://uk.sagepub.com/en-gb/eur/qualitative-research-evaluation-methods/book232962>.

169 DENZIN, NK; LINCOLN, YS (Ed.). *The SAGE Handbook of Qualitative Research*. 4. ed. Thousand Oaks, CA: SAGE Publications, 2011. ISBN 9781412974172. Available in: <https://books.google.com/books/about/The_SAGE_Handbook_of_Qualitative_Research.html?id=qEiC-_ELYgIC>.

170 HEVNER, AR; MARCH, ST; PARK, J; RAM, S. Design science in information systems research. *MIS Quarterly*, 2004, vol. 28, no. 1, p. 75–105. Available in: <https://doi.org/10.2307/25148625>.

171 OKOLI, C; SCHABRAM, K. *A Guide to Conducting a Systematic Literature Review*. 2010. Working paper. Available in: <https://doi.org/10.2139/ssrn.1954824>.

172 MILES, MB; HUBERMAN, AM; SALDAÑA, J. *Qualitative Data Analysis: A Methods Sourcebook*. 3. ed. [S.l.]: SAGE Publications, 2014. ISBN 978-1-4522-5787-7.

173 BRAUN, V; CLARKE, V. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 2006, vol. 3, no. 2, p. 77–101.

174 GARRETT, GA. *Cybersecurity in the Digital Age*. [S.l.]: Wolters Kluwer Law & Business, 2018. ISBN 9781454899471.

175 ALOSEEL, A; HE, H; SHAW, C; KHAN, MA. Analytical review of cybersecurity for embedded systems. *IEEE Access*, 2020, PP, no. 99, p. 1–1. Available in: <https://doi.org/10.1109/ACCESS.2020.3045972>.

176 YIN, RK. *Qualitative Research from Start to Finish*. 2nd. ed. New York: Guilford Press, 2016. Available in: <https://www.guilford.com/books/Qualitative-Research-from-Start-to-Finish/Robert-K-Yin/9781462521340>.

177 KITCHENHAM, B; BRERETON, OP; BUDGEN, D; TURNER, M; BAILEY, J; LINKMAN, S. Systematic literature reviews in software engineering. *Information and Software Technology*, 2009, vol. 51, no. 1, p. 7–15. Available in: <https://doi.org/10.1016/j.infsof.2008.09.009>.

178 CRESWELL, JW. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. 4. ed. Thousand Oaks, CA: SAGE Publications, 2014. ISBN 9781452226101. Available in: <https://books.google.com/books/about/Research_Design.html?id=4uB76IC_pOQC>.

179 JOSHI, A; KALE, S; CHANDEL, S; PAL, DK. Likert scale: Explored and explained. *British Journal of Applied Science & Technology*, 2015, vol. 7, no. 4, p. 396–403. Available in: <https://doi.org/10.9734/BJAST/2015/14975>.

180 BOONE, HN; BOONE, DA. Analyzing likert data. *Journal of Extension*, 2012, vol. 50, no. 2, p. 1–5. Available in: <https://tigerprints.clemson.edu/joe/vol50/iss2/48/>.

181 SADEGHI, A; WACHSMANN, C; WAIDNER, M. Security and privacy challenges in industrial internet of things. In *Proceedings of the 52nd Annual Design Automation Conference (DAC '15)*. [s.n.], 2015. p. 1–6. Available in: <https://doi.org/10.1145/2744769.2747942>.

182 DAVI, L; GöTZFRIED, J; SADEGHI, AR. Security of embedded systems: An introduction and overview. In SADEGHI, AR; NACCACHE, D (Ed.). *Embedded Systems Security*. Cham: Springer, 2020. p. 1–33. ISBN 9783030381274.

183 STRAUSS, A; CORBIN, J. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. 2. ed. Thousand Oaks, CA: SAGE Publications, 1998. ISBN 0803959400. Available in: <https://books.google.com/books/about/Basics_of_Qualitative_Research.html?id=wTwYUnHYsmMC>.

184 BOTTA, A; DONATO, W de; PERSICO, V; PESCAPÉ, A. Integration of cloud computing and internet of things: A survey. *Future Generation Computer Systems*, 2016, vol. 56, p. 684–700. Available in: <https://doi.org/10.1016/j.future.2015.09.021>.

185 SALDAÑA, J. *The Coding Manual for Qualitative Researchers*. 3. ed. London: SAGE Publications, 2016. ISBN 9781473902497.

186 GIBBS, GR. *Analyzing Qualitative Data*. London: SAGE Publications, 2007. Sem DOI (livro). Parte da coleção Qualitative Research Kit. ISBN 9780761949800. Available in: <https://lccn.loc.gov/2006929360>.

187 CHARMAZ, K. *Constructing Grounded Theory: A Practical Guide Through Qualitative Analysis*. London: SAGE Publications, 2006. ISBN 9780761973522.

188 BAZELEY, P. *Qualitative Data Analysis: Practical Strategies*. London: SAGE Publications, 2013. ISBN 9781847875815.

189 FLICK, U. *An Introduction to Qualitative Research*. 6. ed. London: SAGE Publications, 2018. ISBN 9781526445650.

190 MAXWELL, JA. *Qualitative Research Design: An Interactive Approach*. 3. ed. Thousand Oaks, CA: SAGE Publications, 2013. ISBN 9781452271002.

191 CRESWELL, JW. *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*. 3. ed. Thousand Oaks, CA: SAGE Publications, 2013. ISBN 9781412995306.

192 OWASP Foundation. *OWASP Secure Coding Practices — Quick Reference Guide*. [S.l.]. Version 2.0. Available in: <https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/>.

APPENDICES

A. GLOSSARY AND ACRONYMS

Table A.1: Vocabulary and brief definitions

Term	Brief definition
Asset	Anything that has value to the organization (information, processes, people, hardware, software, facilities). (139)
Control (security)	A measure that maintains and/or modifies risk (it may be a policy, process, procedure, organizational structure, software/hardware function). (139)
Access control	Mechanisms to ensure that physical/logical access to assets occurs only when authorized and in accordance with requirements. (139)
Authentication	Provision of assurance that a characteristic claimed by an entity is correct. (139)
ISMS/SGSI	Information Security Management System: requirements to establish, implement, maintain, and continually improve information security management. (123)
Confidentiality/Integrity/Availability (CIA)	Objectives preserved by an ISMS to protect information. (123)
Risk (IS)	Effect of uncertainty on information security objectives; assessed through context, identification, analysis, evaluation, and treatment. (79)
Risk assessment	Process that includes risk identification, analysis, and evaluation. (79)
Risk treatment	Selection and implementation of options to modify risk (mitigate, avoid, transfer, retain). (79)
Risk acceptance	Decision to take on residual risk based on defined criteria. (79)
Security perimeter	Delimitation of the assets/environments covered by the analysis and airworthiness security measures. (49)
SRA (Security Risk Assessment)	Set of activities for identifying threat conditions and scenarios, assessing severity/threat level, and defining security measures. (49)
IUEI	*Intentional Unauthorized Electronic Interaction* — intentional unauthorized electronic interactions with potential effects on flight safety. (57)
Defense in depth	Principle of complementary protection layers (architecture, segregation, monitoring, recovery) to mitigate attack scenarios. (57)
SAL (Security Assurance Level)	Level of security assurance required/assigned to evidence the effectiveness of measures and the fulfillment of security objectives. (57)
Continued airworthiness	Set of activities and guidance to maintain information security protection during aircraft operation/maintenance. (50)
AISP	*Aircraft Information Security Plan*: the operator's operational information security plan, aligned with the organization's programs/ISMS. (50)
BPMN	*Business Process Model and Notation*: notation for modeling business processes used to describe the activities/phases of the proposed method.
Traceability	Capability to relate requirements, artifacts, verifications, and evidence across the life cycle, demonstrating compliance. (32)
SCM/CM	*(Software) Configuration Management*: identification of items, baselines, change control, status, and release/archive. (32)
SQA/QA	*Software Quality Assurance*: independent activities to ensure conformity with plans, standards, and life-cycle objectives. (32)
Verification evidence (EV-XXX)	Internal identifier in this dissertation for artifacts (e.g., verification results, test reports, reviews, CM/QA records) used as proof of objectives. (32)

Source: Prepared by the author.

A.0.1 List of Acronyms

Table A.2: List of acronyms used in the dissertation

Acronym	Description
AISP	Aircraft Information Security Plan (50)
ARINC	Aeronautical Radio, Inc.
AT	Awareness and Training (NIST control family) (121)
AU	Audit and Accountability (NIST) (121)
BPMN	Business Process Model and Notation
CA	Assessment, Authorization and Monitoring (NIST) (121)
CIA	Confidentiality, Integrity, Availability (123)
CM/SCM	(Software) Configuration Management (32)
DO-178C	Software Considerations in Airborne Systems and Equipment Certification
DO-178B	Previous version (basis for terminology/life-cycle artifacts) (32)
DO-254	Design Assurance Guidance for Airborne Electronic Hardware
DO-326A	Airworthiness Security Process Specification (49)
DO-355A	Information Security Guidance for Continued Airworthiness (50)
DO-356A	Airworthiness Security Methods and Considerations (57)
EV-XXX	Verification Evidence indexed in this dissertation (32)
FHA/PSSA/SSA	Functional Hazard Assessment / Preliminary/System Safety Assessment (49)
IA/AC/SC/SI	NIST families (Identification & Authentication; Access Control; System & Communications; System Integrity) (121)
ISMS/SGSI	(Information) Security Management System (123)
IUEI	Intentional Unauthorized Electronic Interaction (57)
MA/MP/PE/PM/PL/RA	NIST families (Maintenance; Media Protection; Physical; Program; Planning; Risk Assessment) (121)
NIST SP 800-53	Security and Privacy Controls for Information Systems (121)
POA&M	Plan of Actions & Milestones (NIST)
QA/SQA	(Software) Quality Assurance (32)
SAL	Security Assurance Level (57)
SRA	Security Risk Assessment (49)
V&V	Verification and Validation (32)
ISO/IEC 27001	ISMS — Requirements (123)
ISO/IEC 27002	Information security controls (139)
ISO/IEC 27005	Risk management guidelines (79)

Source: Prepared by the author.

B. EXPANDED NORMATIVE CROSSWALK (CONTROL LEVEL)

This appendix unfolds, at the *control level*, the phase-based matrix presented in the Framework, establishing unambiguous traceability among the **method phases**, the **NIST SP 800-53 Rev. 5 controls** (121), the **ISO/IEC 27001/27002:2022 items/themes** (123, 139), and the **objectives/processes of the DO standards** (DO-178C/DO-254/DO-326A/DO-356A/DO-355A) (26, 42, 49, 57, 50), with a direct link to the **evidence (EV-XXX)**. Risk prioritization, acceptance, and treatment follow ISO/IEC 27005:2022 (79).

Table B.1: Control-level crosswalk: Method phase × NIST SP 800-53 Rev. 5 × ISO/IEC 27001/27002:2022 × DO Standards × Evidence × Rationale

Method phase	NIST (ID—title)	ISO/IEC 27001/27002:2022	DO Standards	EV	Rationale / Note (incl. N/A)
Threat Analysis	RA-3 — Risk Assessment	A.5.7 Threat intelligence; A.8.16 Monitoring activities; A.8.8 Management of technical vulnerabilities	DO-326A — Security Risk Assessment (SRA)	EV-001	Consolidates threat intelligence and risk assessment; derives requirements/mitigations and acceptance criteria (79, 49, 121).
Threat Analysis	RA-5 — Vulnerability Monitoring and Scanning	A.8.8 Management of technical vulnerabilities; A.8.16 Monitoring activities	DO-326A — identification of operational vulnerabilities	EV-002	Scanning and analysis feed the SRA and the POA&M (traceable closure of gaps) (121, 49).
Threat Analysis	SR-2 — Supply Chain Risk Management Plan	A.5.19–A.5.21 (supplier & ICT supply chain)	DO-326A — assessment of suppliers/critical items	EV-044	Supply chain risk plan (criteria, *due diligence*, monitoring) (49).
Threat Analysis	SR-3 — Supply Chain Controls and Processes	A.5.19–A.5.21 (supplier & ICT supply chain)	DO-326A — contractual requirements/delivery controls	EV-045	Defines minimum controls required of suppliers and verification upon acceptance (49).
Threat Analysis	CA-7 — Continuous Monitoring	A.8.16 Monitoring activities	DO-355A — Continued Airworthiness Security	EV-003	Monitoring strategy and metrics support situational awareness and in-service risk feedback (121, 50).
Secure Design	SA-3 — System Development Life Cycle	A.5.24 Information security in project management; A.8.27 Secure system architecture & engineering principles	DO-178C/DO-254 — planning/architecture and V&V objectives	EV-010	Integrates security into the life cycle and the reference architecture, with traceable DO objectives (121, 26, 42).
Secure Design	SA-8 — Security Engineering Principles	A.8.27 Secure architecture; A.8.9 Configuration management	DO-326A — architecture/mitigations; DO-356A — partitions/trusted channels	EV-011	Secure engineering principles applied to partitioning and isolation of domains (49, 57).
Secure Design	SA-11 — Developer Testing	A.8.28 Secure coding; A.8.27 Secure system architecture	DO-178C — verification (analysis, testing, coverage)	EV-014	Evidence of developer V&V (reviews, tests, coverage), reducing defects prior to integration (26, 121).
Secure Design	AC-6 — Least Privilege	A.5.15 Access control; A.5.16 Identity management; A.5.17 Authentication information; A.5.18 Access rights	DO-356A — authorization/segregation; DO-178C — design/code reviews	EV-012	Implements least privilege and permission reviews by role/function (121, 123, 26).
Secure Design	SC-7 — Boundary Protection	A.8.27 Secure architecture; A.8.9 Configuration management	DO-356A — segmentation, trusted channels	EV-013	Defines perimeters, domains, and secure routes consistent with the target architecture (57).
Implementation of Security Controls	AC-2 — Account Management	A.5.16 Identity management; A.5.18 Access rights	DO-356A — account/credential management in critical environments	EV-020	Account life cycle with authorization, periodic review, and change logs (121, 123).
Implementation of Security Controls	AC-3 — Access Enforcement	A.5.15 Access control; A.5.18 Access rights	DO-356A — authorization mechanisms; DO-178C — test evidence	EV-035	Enforces authorization decisions (RBAC/ABAC), logging denials and exceptions (57, 26).
Implementation of Security Controls	IA-2 — Identification and Authentication (Users)	A.5.17 Authentication information; A.5.15 Access control	DO-356A — strong authentication; DO-178C — V&V evidence	EV-021	Robust I&A implemented and verified with DO test cases (121, 57, 26).
Implementation of Security Controls	IA-5 — Authenticator Management	A.5.17 Authentication information	DO-356A — secure management of secrets/credentials	EV-034	Governs the life cycle of authenticators (complexity, rotation, secure storage, revocation) (57).
Implementation of Security Controls	SC-23 — Session Authenticity	A.5.17 Authentication information; A.5.15 Access control	DO-356A — session/channel protection; DO-178C — interface testing	EV-033	Protects sessions (tokens, mTLS, revalidation, *timeouts*) against hijacking/impersonation (57, 26).
Implementation of Security Controls	SC-12 — Cryptographic Key Establishment and Management	A.8.24 Use of cryptography	DO-356A — key management; compliance evidence	EV-022	Policy and key life cycle (generation, rotation, revocation, destruction) (57).

Method phase	NIST	ISO/IEC 2022	DO	EV	Rationale / Note
Implementation of Security Controls	SC-13 — Cryptographic Protection	A.8.24 Use of cryptography	DO-356A — approved algorithms/modes; DO-178C — testing/validation	EV-023	Protects confidentiality/integrity in transit and at rest, with documented validation (57, 26).
Implementation of Security Controls	SC-28 — Protection of Information at Rest	A.8.24 Use of cryptography; A.8.9 Configuration management	DO-356A — protection of data at rest	EV-024	Disk/media/partition encryption and strengthened access controls (57).
Implementation of Security Controls	SI-7 — Software, Firmware, and Information Integrity	A.8.28 Secure coding; A.8.9 Configuration management	DO-356A — validation/anti-tamper; DO-178C — build integrity	EV-029	Ensures integrity (hash/signature, boot/update checks, verified SBOM) (57, 26).
Implementation of Security Controls	CM-3 — Configuration Change Control	A.8.9 Configuration management	DO-178C/DO-254 — CM/QA; DO-326A — impact assessment	EV-025	CR/PR, CCB, and impact analysis ensure traceability and an intact baseline (26, 42, 49).
Implementation of Security Controls	CM-6 — Configuration Settings	A.8.9 Configuration management	DO-178C/DO-254 — baseline/hardening; DO-326A — impact assessment	EV-028	Defines and validates hardening baselines by component type, with exceptions approved via CM/CCB (26, 42, 49).
Implementation of Security Controls	AU-2 — Event Logging	A.8.15 Logging; A.8.16 Monitoring activities	DO-326A — evidence collection; DO-178C/254 — audits	EV-026	Coverage of security-relevant events with retention and protection of audit trails (121, 123, 26).
Implementation of Security Controls	SR-5 — Acquisition Strategies, Tools, and Methods	A.5.20 Addressing IS within supplier agreements; A.5.21 ICT supply chain	DO-326A — security clauses; DO-254 — HW acquisition	EV-046	Evidence of contractual clauses, SBOM, acceptance tests, and rejection criteria (49, 42).
Implementation of Security Controls	AU-6 — Audit Record Review, Analysis and Reporting	A.8.15 Logging; A.8.16 Monitoring activities	DO-178C/DO-254 — audits; DO-326A — evidence collection	EV-027	Ensures periodic audit review, event correlation, and findings reports with actions (121, 26, 42).
Incident Monitoring & Response	IR-4 — Incident Handling	A.5.25–A.5.28 (planning, response, lessons, evidence)	DO-326A — operational response; DO-355A — continued airworthiness	EV-030	Playbooks, roles, and post-incident activities with lessons learned and evidence (49, 50).
Incident Monitoring & Response	IR-5 — Incident Monitoring	A.8.16 Monitoring activities; A.8.15 Logging	DO-355A — in-service monitoring	EV-031	KPIs and dashboards enable measurement of effectiveness and trends (50).
Incident Monitoring & Response	SI-4 — System Monitoring	A.8.16 Monitoring activities	DO-326A/DO-355A — anomaly detection/correlation	EV-032	Detection rules and alerts support early threat detection (49, 50).
Integration with Risk Management	PL-2 — System Security and Privacy Plan	A.5.1 Policies for information security; A.5.30 ICT readiness for business continuity	DO-326A — acceptance baseline/objectives	EV-040	The SSP consolidates scope, requirements, and controls linked to policies (121, 49).
Integration with Risk Management	PM-9 — Risk Management Strategy	A.6.3 Awareness, education & training; A.5.1 Policies	DO-326A — risk/acceptance criteria	EV-041	Formal strategy defines severity/likelihood criteria and review triggers (79, 121).
Integration with Risk Management	CA-2 — Control Assessments	*Clause 9.2 (Internal audit)*; A.5.1 Policies (support)	DO-178C/DO-254 — audits/independence; DO-326A — credit/security evidence	EV-043	Assessment reports (independent/internal), control coverage, and action plans (121, 26, 42, 49).
Integration with Risk Management	CA-5 — Plan of Action and Milestones (POA&M)	A.8.8 Technical vulnerabilities; A.8.9 Configuration management	DO-178C/DO-254 — CM/QA; DO-326A — mitigating actions	EV-042	Closes gaps with deadlines, owners, and traceable completion evidence (121, 26, 42, 49).
Integration with Risk Management	AT-2/AT-3 — Awareness and Training	A.6.3 Awareness, education and training	DO-326A — operational readiness and roles	EV-053	Role-based training program for critical roles, with records, frequency, and effectiveness (49, 123).
Continuous Maintenance	SI-2 — Flaw Remediation	A.8.8 Management of technical vulnerabilities	DO-326A — bulletins/patches; DO-355A — in-service maintenance	EV-050	Remediation pipeline and documented revalidation in production (49, 50).
Continuous Maintenance	CM-2 — Baseline Configuration	A.8.9 Configuration management	DO-178C/DO-254 — baseline control and traceability	EV-051	Approved baseline (reference artifact) facilitates audit and reproduction (26, 42).
Continuous Maintenance	MA-2 — Controlled Maintenance	A.7 (physical controls) — per SoA; A.7.14 Secure disposal or re-use of equipment	DO-326A — secure maintenance with authorized personnel	EV-052	Work order and checklist ensure safeguards during maintenance (49).
Secure Decommissioning	MP-6 — Media Sanitization	A.8.10 Information deletion; A.7.14 Secure disposal or re-use of equipment	DO-326A/DO-356A — sanitization/termination	EV-060	Certificates and reports demonstrate methods and results of deletion/disposal (49, 57).
Secure Decommissioning	CM-8 — System Component Inventory	A.5.9 Inventory of information & associated assets; A.5.11 Return of assets	DO-326A — termination with reconciled inventory	EV-061	Final inventory and return terms ensure asset reconciliation (49).
Secure Decommissioning	PE-16 — Delivery and Removal	A.7 (physical controls) — per SoA; A.7.14 Secure disposal or re-use of equipment	DO-326A — physical/logistical control	EV-062	Chain of custody tracks delivery/removal of components (49).
Secure Design	PS-7 — Third-Party Personnel Security	*N/A within the technical scope of this artifact*	*N/A*	*N/A*	*Contextual N/A*: predominantly an HR control; refer to the corporate policy when required by audit.

Source: Prepared by the author.

C. PROCESS ACTIVITY CROSSWALK (EXPANDED)

This *activity-level* breakdown links each task of the modeled process (BPMN) to the controls of NIST SP 800-53 (121), the items/themes of ISO/IEC 27001/27002:2022 (123, 139), and the objectives/processes of the DO standards (DO-178C/DO-254/DO-326A/DO-356A/DO-355A) (26, 42, 49, 57, 50), with a direct link to evidence (EV-XXX), accountable roles, and update cadence. The activities follow the enumeration (A1, A2, . . .) and the diagram's *swimlane*/role.

Table C.1: Activity Crosswalk (BPMN × NIST SP 800-53 × ISO/IEC 27001/27002 × DO Standards × Evidence)

ID (BPMN)	Activity	Swimlane/Role	NIST SP 800-53 (IDs)	ISO/IEC 27001/27002	DO Objective/Process	Evidence	Owner	Cadence
A1	Threat Intelligence Collection	SecOps	RA-3, RA-5, PM-15, CA-7 (121)	A.5.7; A.8.16 (123)	DO-326A (SRA inputs); DO-356A (threat intel) (49, 57)	EV-001 (Threat intel report + IOC feed; EV-001)	SecOps	daily
A2	Threat Modeling	Security Architecture	SA-8, RA-3, SR-2, CA-2 (121)	A.8.27; A.5.24 (123, 139)	DO-326A (requirements/architecture); DO-356A (attack trees/DFD) (49, 57)	EV-002 (Attack tree + DFD + risk register; EV-002)	SecArch	per release
A3	Impact and probability assessment	Risk Management	RA-2, RA-3, PM-9 (121)	6.1.2/6.1.3; A.8.16 (123)	DO-326A (severity×likelihood; criteria) (49)	EV-003 (Risk matrix + decision; EV-003)	RiskMgr	monthly
A4	Implementation of defense in depth	Security Architecture	SC-7, SC-5, AC-3, SI-7 (121)	A.8.27; A.8.9 (123, 139)	DO-326A (partitions/architecture); DO-356A (layers) (49, 57); (100)	EV-004 (Architecture + CM baseline; EV-004)	SecArch	per release
A5	Principle of Least Privilege	Software Eng.	AC-6, AC-2, IA-2, IA-5 (121)	A.5.15–A.5.18 (123)	DO-178C (design/code review evidence) (26)	EV-005 (RBAC matrix + reviews; EV-005)	SWE	per sprint
A6	Secure Development	Software Eng.	SA-3, SA-11, SI-10, CM-3 (121)	A.8.28; A.5.24; A.8.9 (123, 139)	DO-178C (dev/verification); DO-254 (if HW) (26, 42); (192)	EV-006 (Code review checklist + TR/TC; EV-006)	SWE	per commit/release
A7	Data Encryption	Software Eng. / SecOps	SC-12, SC-13, SC-28, IA-7 (121)	A.8.24 (123)	DO-356A (cryptography/key management) (57)	EV-007 (Key policy + KMS logs; EV-007)	SecOps	quarterly
A8	Access Control Implementation	SecOps	AC-2, AC-3, AC-6, IA-2, IA-5, SC-23 (121)	A.5.15–A.5.18; A.8.9 (123, 139)	DO-356A (access mechanisms); DO-178C (traceability/QA) (57, 26)	EV-008 (Access report + account CM; EV-008)	SecOps	monthly
A9	Security Audit	SecOps / QA	AU-2, AU-6, AU-8, RA-5, CA-2 (121)	A.8.15; A.8.16 (123)	DO-178C/DO-254 (audits); DO-326A (operational V&V) (26, 42, 49)	EV-009 (SIEM dashboard + audit trails; EV-009)	SecOps	daily
A10	Continuous Monitoring	SecOps	SI-4, CA-7, AU-6 (121)	A.8.16 (123)	DO-355A (continued airworthiness); DO-326A (operations) (50, 49)	EV-010 (KPIs + alarms; EV-010)	SecOps	continuous
A11	Incident Response	CSIRT / SecOps	IR-4, IR-5, AU-6, SI-4 (121)	A.5.25–A.5.28 (123)	DO-356A (testing/forensics); DO-326A (operational response) (57, 49)	EV-011 (Tickets + custody + postmortem; EV-011)	CSIRT	per incident
A12	Post-Incident Review	CSIRT / QA	IR-8, PM-6, CA-5 (121)	A.5.27 (123)	DO-355A (continuous improvement); DO-326A (lessons) (50, 49)	EV-012 (Lessons learned + POA&M; EV-012)	CSIRT	per incident
A13	Patch Management	Config Eng. / SecOps	SI-2, CM-3, CM-4, MA-2 (121)	A.8.8; A.8.9 (123, 139)	DO-326A (bulletins/changes); DO-254 (CM) (49, 42)	EV-013 (Bulletins + CR/PR + CM approval; EV-013)	ConfigEng	per release
A14	Training and awareness	HR / SecOps	AT-2, AT-3, PS-7 (121)	A.6.3 (123)	DO-326A (operational readiness) (49)	EV-014 (Attendance list + LMS; EV-014)	HR	semiannual
A15	Data Sanitization (Decommissioning)	Operations	MP-6, SC-12, CM-8 (121)	A.8.10; A.7.14 (123)	DO-326A/DO-356A (sanitization/termination) (49, 57)	EV-015 (Sanitization certificate + KMS logs; EV-015)	Ops	per event
A16	Asset Inventory, Recycling/Destruction	Operations / CM	CM-8, MP-2, MP-6, PE-16 (121)	A.5.9; A.5.11; A.7.14 (123)	DO-326A (secure closure); DO-254 (baseline) (49, 42)	EV-016 (Inventory + return terms; EV-016)	CM	monthly
A17	Incident Response Preparation	CSIRT / SecOps	IR-8, IR-3, CP-2 (121)	A.5.25–A.5.28 (123)	DO-356A (preparedness and testing); DO-326A (readiness) (57, 49)	EV-017 (IR plan + tabletop; EV-017)	CSIRT	semiannual
A18	Formal Design Reviews	QA / SecArch	SA-11, SA-8, CA-2 (121)	A.8.27; A.5.24; A.8.28 (123, 139)	DO-178C/DO-254 (reviews, QA/PA, evidence) (26, 42)	EV-018 (SRR/PDR/CDR minutes + checklists; EV-018)	QA	per milestone
A19	Physical Security	Operations	PE-2, PE-3, PE-6, MP-2 (121)	A.7.x (relevant physical controls) (123)	DO-326A/DO-356A (anti-tamper; physical protection) (49, 57)	EV-019 (inspections, seals; EV-019)	Ops	semiannual

ID (BPMN)	Activity	Swimlane/Role	NIST	ISO/IEC	DO	Evidence	Owner	Cadence
A20	Policy Review and Update	GRC (Information Sec.)	PL-1, PL-2, PM-1, PM-9, CA-5 (121)	A.5.1; A.5.2; A.5.24 (123)	DO-178C/DO-254 (QA/PA); DO-326A (governance) (26, 42, 49)	EV-020 (revised policy + approvals; EV-020)	GRC	annual
A21	Automated Threat Modeling	SecArch / SWE	RA-3, RA-5, SA-8 (121)	6.1.2/6.1.3; A.8.27 (123)	DO-326A (SRA/architecture); DO-356A (attack trees/DFD) (49, 57)	EV-021 (DFD artifacts + attack trees; EV-021)	SecArch	per release
A22	Pre-populated Initial Risk Analysis	Risk Management	RA-1, RA-2, RA-5, PM-9 (121)	6.1.2/6.1.3; A.8.16 (123)	DO-326A (acceptance criteria); DO-355A (feedback) (49, 50)	EV-022 (pre-populated risk register; EV-022)	RiskMgr	per build/release
A23	Compliance as Code (Policies-as-Code)	DevOps / SecOps / QA	CM-2, CM-3, CM-6, CA-7, SI-10 (121)	A.8.9; A.8.28; A.8.24 (123, 139)	DO-178C/DO-254 (V&V and assurance); DO-326A (safe operations) (26, 42, 49)	EV-023 (pipelines with gates + reports; EV-023)	DevOps	per commit/deploy
A24	Orchestration & Latency Objectives	SecOps / CSIRT	IR-4, IR-5, IR-8, CP-2 (121)	A.5.25–A.5.28 (123)	DO-355A (target MTTD/MTTR); DO-326A (operational response) (50, 49)	EV-024 (AUTO/HUMAN playbooks + metrics; EV-024)	SecOps	continuous
A25	Governance & Safeguards	GRC / CAB	PM-1, PM-9, PL-2, CA-6 (121)	A.5.1; A.5.2; A.5.24 (123)	DO-326A (governance); DO-178C/DO-254 (QA/PA) (49, 26, 42)	EV-025 (policies, approved exceptions; EV-025)	GRC/CAB	quarterly
A26	Maintenance Window Preparation	Operations / CM	CM-3; CM-4; SI-2; CA-7 (121)	A.8.9; A.8.8; A.8.16 (123, 139)	DO-355A — Continued Airworthiness; DO-326A — Risk of Change (57, 26)	Maintenance bulletin + approval (EV-050)	Operations/CM	per window
A27	Retrofit Impact Analysis	Systems Eng. / QA	RA-3; SA-11; CM-3 (121)	Change control, testing and acceptance (A.8.) (123, 139)	DO-326A — SRA; DO-355A — Operational suitability (26, 57)	Impact report (interfaces/-timing/EMC) (EV-052)	Systems Eng. / GRC	per change
A28	Retrofit Verification & Fleet Rollout	QA / Operations	SA-11; CA-2; CA-7 (121)	Testing/acceptance/monitoring (A.8.) (123, 139)	DO-178C — SW verification (when applicable); DO-355A; DO-356A (42, 57, 49)	V&V results + CAB minutes/decision (EV-053)	QA / CAB	per change
A29	Obsolescence Scan & Roadmap Update	Procurement / CM	CM-8; SR-6; RA-3 (121)	Asset management, changes and technical risks (A.5/A.8) (123, 139)	DO-326A — Risk; DO-355A — Sustainment/obsolescence (26, 57)	Obsolescence plan + trade study (EV-054); updated CMDB (EV-055)	Procurement / CM	semiannual/annual
A30	Decommissioning Authorization	GRC / CAB	CM-3; CA-2; PM-9 (121)	Governance & changes (A.5/A.8) (123, 139)	DO-355A — Decision record; DO-356A — Secure termination (57, 49)	Decommissioning plan/authorization (EV-056)	GRC / CAB	per asset
A31	Cryptographic Offboarding (Revocation)	SecOps / PKI	SC-12; SC-13; IA-5 (121)	A.8.24 (cryptography); A.8.15/8.16 (logs/monitoring) (139)	DO-356A — Revocation/rotation; DO-355A — Record (49, 57)	Proof of revocation/propagation (CRL/OCSP, telemetry) (EV-058)	SecOps / PKI	per event
A32	Compliance Closure & Lessons	QA / GRC	AU-6; CA-7; PM-6 (121)	A.5 (policies and roles); A.8.16 (monitoring) (123, 139)	DO-355A — Closure evidence and audit (57)	Audit closure & chain of custody (EV-057)	QA / GRC	per cycle

Source: Prepared by the author.

C.1 VISUAL CORRESPONDENCE OF DIAGRAM ELEMENTS

Table C.2 unambiguously names the main elements of the diagram *as labeled in the figure*, assigning a short identifier (A) to each *activity* and recording the respective *swimlane/role*.

Table C.2: Activity Correspondence A# ↔ Diagram Label (BPMN) ↔ Swimlane

A#	Diagram Label (Activity)	Swimlane/Role
A1	Threat Intelligence Collection	SecOps
A2	Threat Modeling	Arq. Segurança
A3	Impact and probability assessment	Gestão de Risco
A4	Implementation of defense in depth	Arq. Segurança
A5	Principle of Least Privilege	Eng. SW
A6	Secure Development	Eng. SW

A#	Diagram Label (Activity)	Swimlane/Role
A7	Data Encryption	Eng. SW / SecOps
A8	Access Control Implementation	SecOps
A9	Security Audit	SecOps / QA
A10	Continuous Monitoring	SecOps
A11	Incident Response	CSIRT / SecOps
A12	Post-Incident Review	CSIRT / QA
A13	Patch Management	Eng. Config. / SecOps
A14	Training and awareness	RH / SecOps
A15	Data Sanitization (Decommissioning)	Operações
A16	Asset Inventory, Recycling/Destruction	Operações / CM
A17	Incident Response Preparation	CSIRT / SecOps
A18	Formal Design Reviews	QA / ArqSeg
A19	Physical Security	Operações
A20	Policy Review and Update	GRC (Seg. Informação)
A21	Automated Threat Modeling	ArqSeg / EngSW
A22	Pre-populated Initial Risk Analysis	Gestão de Risco
A23	Compliance as Code (Policies-as-Code)	DevOps / SecOps / QA
A24	Orchestration & Latency Objectives	SecOps
A25	Governance & Safeguards	GRC / CAB
A26	Maintenance Window Preparation	Operações / CM
A27	Retrofit Impact Analysis	Eng. Sistemas / QA
A28	Retrofit Verification & Fleet Rollout	QA / Operações
A29	Obsolescence Scan & Roadmap Update	Suprimentos / CM
A30	Decommissioning Authorization	GRC / CAB
A31	Cryptographic Off-boarding (Revocation)	SecOps / PKI
A32	Compliance Closure & Lessons	QA / GRC

Source: Prepared by the author.

O ChatGPT disse:

C.1.1 Gateways (Decisions)

For audit reference, the gateways are named according to the labels displayed in the diagram.

Table C.3: Gateway Naming (G#)

G#	Diagram Label (Gateway)
G1	Critical threat identified?

G#	Diagram Label (Gateway)
G2	Are the security measures implemented sufficient?
G3	Satisfactory implementation?
G4	Appropriate Strategy?
G5	Real Threat / False Alarm
G6	End-of-Life criteria met?
G7	Sanitization verified?
G8	Revocation propagated?

Source: Prepared by the author.

C.1.2 Events (Start/End/Intermediate)

Table C.4: Event Naming (E#)

E#	Diagram Label (Event)
E1	Start of Analysis
E2	Start Secure Design
E3	Start of Monitoring
E4	Start of Maintenance
E5	Incident Response Completion
E6	Integration completed
E7	Success
E8	Completed
E9	Start of Decommissioning
E10	Decommissioning Completed (Artifacts Filed)

Source: Prepared by the author.

D. REQUIREMENTS TRACEABILITY MATRIX (SECURITY)

This appendix presents the security *Requirements Traceability Matrix (RTM)*, establishing bidirectional and unambiguous traceability among: (i) security requirements derived from DO-326A; (ii) threats and risks according to ISO/IEC 27005; (iii) applicable controls (NIST SP 800-53 Rev. 5; ISO/IEC 27001/27002:2022); (iv) verification/validation cases (DO-178C/DO-254); and (v) objective evidence of compliance (49, 79, 121, 123, 139, 26, 42, 57, 50).

"Security Credit" Criteria. A requirement is marked as **YES** (*technical security credit*) when: (a) it measurably reduces risk; (b) it is technically verifiable/validatable; and (c) it generates objective evidence. Requirements with predominantly procedural or planning-related credit are marked **NO**.

RTM Dimensions. ID | Security Requirement (DO-326A) | Threat/Risk (ISO/IEC 27005) | Controls (NIST/ISO/DO) | V&V Cases (DO-178C/254) | Evidence | Security Credit.

Table D.1: Requirements Traceability Matrix (RTM) — Security

ID	Security Requirement (DO-326A)	Threat/Risk (ISO/IEC 27005)	Controls (NIST/ISO/DO)	V&V Cases (DO-178C/254)	Evidence	Credit
REQ-SEC-001	Aircraft Security Scope Definition (ASSD)	ISO 27005 §7 (context definition: criteria, scope, boundaries)	NIST: PM-1, PL-2, RA-1; ISO/IEC 27001/27002: context and criteria; DO-326A: aircraft scope (49, 79, 121, 123)	Definition of V&V artifacts and baseline (26, 42)	EV-001 — Approved scope document (ASSD), criteria and boundaries	**YES**
REQ-SEC-002	Preliminary Aircraft Security Risk Assessment (PASRA)	ISO 27005 §§8.2–8.4 (identify, analyze, assess preliminary risks)	NIST: RA-3, RA-5, CA-2; ISO: risk assessment; DO-326A: preliminary assessment (aircraft level) (79, 121, 49)	Risk-oriented V&V planning (26, 42)	EV-002 — PASRA report with ranking and acceptance criteria	**YES**
REQ-SEC-003	Aircraft Security Risk Assessment (ASRA)	ISO 27005 §§8.2–8.4, §9 (full cycle and iterations)	NIST: RA-2..RA-8, CA-7; ISO: treatment; DO-326A: consolidated ASRA (79, 121, 49)	Update of test cases and exit criteria (26, 42)	EV-003 — ASRA report with treatment decisions and residual risk	**YES**
REQ-SEC-004	System Security Scope Definition (SSSD)	ISO 27005 §7 (system-specific context)	NIST: PL-2, CM-8; ISO: inventory/scope; DO-326A: system security scope (79, 121, 123, 49)	Baseline of SW/HW items and configuration (26, 42)	EV-004 — SSSD with boundaries, assets and interfaces	**YES**
REQ-SEC-005	Preliminary System Security Risk Assessment (PSSRA)	ISO 27005 §§8.2–8.4 (system risk triage)	NIST: RA-3, RA-5, SA-8; ISO: IS risk; DO-326A: PSSRA (79, 121, 49)	Component verification planning (26, 42)	EV-005 — PSSRA report with prioritization	**YES**
REQ-SEC-006	System Security Risk Assessment (SSRA)	ISO 27005 §§8–10 (analysis, treatment, acceptance)	NIST: RA-*, CA-5 (POA&M), PM-9; ISO: treatment/acceptance; DO-326A: SSRA (79, 121, 49)	Acceptance criteria and verification of mitigations (26, 42)	EV-006 — SSRA, residual risk and approval	**YES**
REQ-SEC-007	Aircraft Security Architecture and Measures (ASAM)	ISO 27005 §9 (selection/implementation of controls)	NIST: SA-8, SC-7, AC-3, SI-7; ISO: architecture/controls; DO-326A/DO-356A: mitigations and partitioning (123, 121, 49, 57)	Design evidence and independent verification (26, 42)	EV-007 — ASAM specification; defense-in-depth	**YES**
REQ-SEC-008	System Security Architecture and Measures (SSAM)	ISO 27005 §9 (treatment at system level)	NIST: SA-3, SA-11, AC-6, SC-13; ISO: technical controls; DO-326A/DO-356A: system-level mitigations (123, 121, 49, 57)	V&V of components, partitions and trusted channels (26, 42)	EV-008 — SSAM specification; control allocation	**YES**
REQ-SEC-009	Aircraft Security Verification (ASV)	ISO 27005 §§11–12 (communication, monitoring and critical review)	NIST: CA-2, SI-4, AU-6; ISO: audit/monitoring; DO-326A: ASV; DO-355A: *continued airworthiness* (79, 121, 49, 50)	Test campaigns; robustness; independent verification (26, 42)	EV-009 — ASV reports; nonconformities and actions	**YES**
REQ-SEC-010	System Security Verification (SSV)	ISO 27005 §§11–12 (monitoring and improvement)	NIST: CA-7 (continuous monitoring), SI-2; ISO: improvement; DO-326A: SSV (79, 121, 49)	Integration/system tests and coverage (26, 42)	EV-010 — SSV reports per item/component	**YES**
REQ-SEC-011	Aircraft Security Operator Guidance (ASOG)	ISO 27005 §11 (communication/consultation)	NIST: AT-2/AT-3, PL-4; ISO: awareness/training (79, 121, 123)	Training and usability evidence (26, 42)	EV-011 — Operational manuals/bulletins; training records	**NO**
REQ-SEC-012	System Security Integrator Guidance (SSIG)	ISO 27005 §12.2 (process improvement)	NIST: CM-3/CM-4, PM-9; ISO: change management (79, 121, 123)	Configuration management; *delta analysis* (26, 42)	EV-012 — Integrator guides; checklists; lessons learned	**NO**

ID	Security Requirement (DO-326A)	Threat/Risk (ISO/IEC 27005)	Controls (NIST/ISO/DO)	V&V Cases (DO-178C/254)	Evidence	Credit
REQ-SEC-013	Security Effectiveness Requirements	ISO 27005 §§9–12 (effectiveness and monitoring)	NIST: CA-7, SI-4, MA-2; ISO: KPIs/KRIs and performance (79, 121, 123)	Effectiveness and acceptance criteria for mitigations (26, 42)	EV-013 — Effectiveness metrics; trends; alert thresholds	**YES**
REQ-SEC-014	Vulnerability Assessment and Testing	ISO 27005 Annex D; §8.2.5 and §12 (assessment/monitoring)	NIST: RA-5, SI-2, CM-6; ISO: vulnerability management; DO-356A: crypto/channels/threats (79, 121, 123, 57)	Structural tests; static/dynamic analysis (26, 42)	EV-014 — Scanning, *pentest*, fixes (POA&M)	**YES**
REQ-SEC-015	Plan for Security Aspects of Certification (PSecAC)	ISO 27005 §7.2–§10 (criteria, treatment, acceptance)	NIST: PL-2, PM-*, CA-5; ISO: planning and improvement (79, 121, 123)	V&V plans and schedules; alignment with authority (26, 42)	EV-015 — PSecAC plan; schedule; responsibilities	**NO**

Source: Prepared by the author.

Operational Note. This RTM serves as a single repository for multi-standard compliance: each row links an evidence artifact (EV-XXX) to corresponding NIST/ISO/DO controls, enabling the demonstration of parallel compliance using the same set of evidence. Any change to a requirement, risk, or control requires an update to the RTM and the corresponding *POA&M* (NIST CA-5 (121)) and must preserve cross-referencing with the Phase and Activity matrices (Table 3.12 and Table 4.1) (49, 79, 123, 139, 26, 42, 57, 50).

E. EVIDENCE REGISTER AND POAM

This appendix consolidates (i) the *Evidence Catalog* (EV-XXX) and (ii) the *Plan of Actions and Milestones* (POAM), in accordance with control **CA-5** of NIST SP 800-53 Rev. 5 (121). The Catalog defines a standardized model for evidence sources that demonstrate compliance, while the POA&M records findings, associated risks, corrective actions, deadlines, responsible parties, and the respective closure confirmations. The proposed structure establishes bidirectional traceability with the RTM in Appendix C (§D) and aligns with the risk cycle of ISO/IEC 27005:2022 (79).

As the framework was not applied in a production environment in this study, the example entries are illustrative, derived from best practices and commonly available sources (e.g., SIEM, GRC, ITSM, QA/V&V, audits). Each piece of evidence must have a unique identifier (EV-NNN), type, location, collection/generation frequency, responsible person, and, when applicable, audit due date. Table E.1 presents the standardized model with representative examples, which can be mapped to both the RTM and the POA&M.

Table E.1: Evidence Catalogue (EV-XXX)

EV-ID	Type	Storage Location	Frequency	Responsible Role	Audit Due
EV-001	Log	Centralised SIEM	Daily	SecOps Team	N/A
EV-002	Report	GRC Portal	Monthly	Risk Manager	N/A
EV-003	Checklist	SharePoint Repository	Weekly	Compliance Analyst	N/A
EV-004	CR/PR (Change)	ITSM Tool	Per change	Change Manager	N/A
EV-005	Audit	Internal Audit System	Annual	Internal Audit Team	N/A
EV-006	Log	Firewall	Daily	Network Security	N/A
EV-007	Report	Vulnerability Management Tool	Quarterly	Vulnerability Team	N/A
EV-008	Checklist	QA Document	Pre-release	QA Lead	N/A
EV-009	Audit	External Audit	Biennial	Third-Party Auditor	N/A
EV-010	Test Evidence	V&V Repository	Per campaign	V&V Lead	N/A
EV-011	Risk Register	GRC Tool	Continuous	Risk Owner	N/A
EV-012	DR/BC Report	BC/DR Repository	Annual	BC/DR Coordinator	N/A
EV-050	CR/PR (Change)	ITSM/CM (change repository)	Per window	Change Manager / Operations	N/A
EV-051	Report	QA/V&V Repository	Per window	QA / Operations	N/A
EV-052	Report	Systems Engineering Repository	Per change	Systems Eng. / GRC	N/A
EV-053	Test Evidence	QA/V&V Repository	Per change	QA / CAB	N/A
EV-054	Report	Procurement/CM Repository	Semiannual/Annual	Procurement / GRC	N/A
EV-055	Report	CMDB/Inventory Repository	Continuous	Configuration Management / Operations	N/A
EV-056	Report	SecOps/KMS Repository	Per asset	SecOps / CM	N/A
EV-057	Report	Logistics Archive (Operations)	Per asset	Operations / GRC	N/A
EV-058	Log	SecOps/PKI Repository	Per event	SecOps (PKI)	N/A
EV-059	Telemetry	Evidence Repository	Each release	Read-only/tap collection implemented and validated	N/A
EV-060	Test Record	Evidence Repository	Per event	Legacy bus integrity alarm	N/A
EV-061	Configuration	Evidence Repository	Each release	Critical parameter checklist (CI/CD gate)	N/A
EV-062	Incident	Evidence Repository	Per event	Telemetry failure log and response	N/A
EV-063	POA&M	Evidence Repository	Monthly	Corrective actions and mitigation status	N/A
EV-064	Technical Audit	Evidence Repository	Quarterly	EMC/EMI and side-channel verification	N/A
EV-065	RTM	Evidence Repository	Continuous	Linking EV-059–EV-064 to RTM items	N/A
EV-066	KPI	Evidence Repository	Monthly	MTTD/MTTR/% gates active	N/A

Source: Prepared by the author.

Best Practices (Catalog). (i) Standardize repository naming conventions; (ii) version control all exported documents and logs; (iii) record responsible owners and *backup owners*; (iv) link each EV-XXX to one or more RTM items (Appendix C) to ensure bidirectional traceability.

The POA&M materializes NIST control CA-5 (121), linking findings to risks, corrective actions, deadlines, status, and closure evidence. Table E.2 presents the recommended model.

Table E.2: POA&M: Findings, Corrective Actions, and Milestones (NIST CA-5)

ID	Finding	Associated Risk	Corrective Action	Owner	Due	Status	Closure Evidence
PM-01	Segregation of duties failure	Unauthorised data access	Review and implement RBAC control	IT Security Lead	N/A	In progress	EV-010: RBAC adjustment report
PM-02	Application logs not configured	Lack of event traceability	Enable and validate application logging	DevOps Team	N/A	Open	EV-011: Example of configured log
PM-03	Outdated vulnerability controls	Exploitation of known vulnerabilities	Schedule weekly scans and patching	Vulnerability Team	N/A	Completed	EV-007: *Patching* report
PM-04	Business continuity plan not tested	Service interruption without recovery	Execute DR test and update the plan	BC/DR Coordinator	N/A	Open	EV-012: DR test report

Source: Prepared by the author.

POA&M Governance. (i) Minimum monthly update during the security committee meetings; (ii) risk-based prioritization (ISO/IEC 27005) (79); (iii) mandatory objective evidence for closure; (iv) *due dates* and responsible parties reviewed upon each scope change; (v) maintain a full change history.

Conclusion. This chapter establishes an operational framework for evidence recording and findings management, enabling the demonstration of continuous compliance with NIST SP 800-53 Rev. 5 (particularly CA-5) (121), harmonized with the ISO/IEC 27005 risk cycle (79) and the traceability defined in the RTM (Appendix C). The linkage EV-XXX $\leftrightarrow$ POA&M $\leftrightarrow$ RTM enables more efficient audits and greater transparency regarding the security posture.

F. RISK ASSESSMENT METHODOLOGY (ISO/IEC 27005)

This appendix provides an operational and reproducible description of the adopted risk assessment method, in conformity with ISO/IEC 27005:2022 (79), harmonized with NIST SP 800-53 Rev. 5 controls (121), ISO/IEC 27001/27002:2022 requirements (123, 139), and relevant aeronautical objectives/processes (DO-178C, DO-254, DO-326A, DO-356A, DO-355A) (26, 42, 49, 57, 50). The method is supported by spreadsheets (measurement plans, catalogues, and a risk register) and by event-driven re-assessment triggers, integrating with the POA&M (CA-5) (121) and with configuration management (CM) required by DO-178C/DO-254 (26, 42).

F.1 SCOPE, ROLES, AND ARTIFACTS

Scope. Covers assets, interfaces, and operational processes of the embedded system, including software/hardware components, supply chains, and maintenance/update operations (per DO-326A) (49).

Roles. (i) *Risk Owner* (approves risk and treatment); (ii) *Control Owner* (implements/generates evidence); (iii) *SecOps/Monitoring* (collects continuous indicators); (iv) *CM/QA* (traceability and baselines) (26, 42).

Artifacts. (a) Catalogue of assets, threats, and vulnerabilities; (b) Impact and likelihood scales; (c) 5×5 risk matrix with color bands (green/amber/red); (d) Risk Register; (e) POA&M; (f) Event-driven re-assessment triggers; (g) EV-XXX evidence and crosswalks to controls (NIST/ISO/DO).

F.2 RISK CRITERIA (ISO/IEC 27005)

Risk appetite/tolerance statement

(i) Risks classified as **High** are unacceptable and require mitigation prior to operational release; (ii) **Medium** requires planned mitigation with deadlines and formal risk acceptance; (iii) **Low** may be accepted with monitoring. Criteria align with (79) and are integrated with the POA&M (CA-5) (121).

Impact Domains

Weighted composite impact: **Safety** (S) (49), **Integrity** (I), **Availability** (A), **Confidentiality** (C), and **Compliance/Regulatory** (R). Default weights prioritize Safety:

$$w_S = 0.40, \quad w_I = 0.20, \quad w_A = 0.20, \quad w_C = 0.10, \quad w_R = 0.10, \quad \sum w = 1.0.$$

Weights may be adjusted by *Risk Owner* decision (controlled via CM (26, 42)).

F.3 MEASUREMENT SCALES

Impact (1–5)

1: negligible; 2: minor; 3: moderate; 4: severe; 5: catastrophic (with particular emphasis on *Safety* under DO-326A (49)). Score each domain (S, I, A, C, R) in 1–5.

Likelihood (1–5)

Likelihood combines *Exploitability* (E), *Exposure* (X), and *Detectability* (D'):

$$L = \mathrm{round}\big(0.5E + 0.3X + 0.2D'\big)\,, \quad D' = 6 - D$$

with $E, X, D \in \{1, \ldots, 5\}$. Higher Detectability means easier to detect; hence $D' = 6 - D$ (the harder to detect, the higher L). E and X are informed by threat intelligence and operational context (11, 79).

F.4 5×5 RISK MATRIX AND BANDS

Composite Impact Calculation

$$I_{\text{comp}} = \mathrm{round}(w_S S + w_I I + w_A A + w_C C + w_R R,\, 1)$$

Inherent Risk

$$\text{Risk}_{\text{inherent}} = I_{\text{comp}} \times L$$

Bands and Colors (default)

Green (**Low**): $1 \leq$ Risk ≤ 7; Amber (**Medium**): $8 \leq$ Risk ≤ 14; Red (**High**): $15 \leq$ Risk ≤ 25. Bands are configurable (recorded via CM) (26, 42).

F.5 PRIORITIZATION, TREATMENT, AND RESIDUAL RISK

Prioritization rule

Sort by $\text{Risk}_{\text{inherent}}$ in descending order; break ties by S (safety) and then by exposure X. Map to actions: *avoid*, *reduce*, *transfer*, *accept* (79).

Effect of controls and residual risk

Implemented controls reduce E, X (likelihood) and/or impact components (typically I, A, C, R). **Simplified model**:

$$E' = \max\{1, E - \Delta E\}, \quad X' = \max\{1, X - \Delta X\}, \quad I'_{\text{comp}} = \text{round}\big(\alpha\, I_{\text{comp}}, 1\big)$$

where $\Delta E, \Delta X \in \{0, 1, 2\}$ represent control effectiveness (e.g., AC-6, SC-7, SI-4 (121)) and $\alpha \in (0, 1]$ models impact mitigation (e.g., SC-12/SC-13 cryptography (121)). Then:

$$L' = \text{round}\big(0.5E' + 0.3X' + 0.2(6 - D)\big)\,, \qquad \text{Risk}_{\text{residual}} = I'_{\text{comp}} \times L'$$

Residual acceptance requires *risk owner sign-off* and, when $\text{Risk}_{\text{residual}} \geq 8$, mandatory POA&M logging (CA-5) (121).

F.6 SPREADSHEET TEMPLATES (TABS) AND FORMULAS

Workbook structure

1. **Assets** (AS-ID, name, owner, criticality S/I/A/C/R, interfaces).
2. **Threats** (TH-ID, category *e.g., tampering, spoofing* (19), threat-intel source (11)).
3. **Vulns** (VU-ID, description, affected component, bulletin reference).
4. **Scenarios** (RSK-ID, AS-ID, TH-ID, VU-ID, scenario description, assumed vectors).
5. **Scales** (dictionary 1–5 for S,I,A,C,R,E,X,D).
6. **Controls Map** (RSK-ID $\rightarrow$ NIST/ISO/DO; EV-IDs).
7. **Risk Register** (computes $\text{Risk}_{\text{inherent}}$ and residual).
8. **POA&M** (finding, action, owner, due, status) (121).
9. **Triggers** (re-assessment triggers, source, SLA).

G. THREAT CATALOGUE AND MODELLING ARTIFACTS

This appendix consolidates threat-modelling artifacts and traceability to controls and evidence, supporting the risk management process (ISO/IEC 27005) and demonstrating conformity with ISO/IEC 27001/27002 controls and with aeronautical security objectives/processes (DO-326A/DO-356A/DO-355A). The catalogue follows the methodological chain of risk identification–analysis–evaluation (ISO/IEC 27005, Sections 6–9), and uses data-flow diagrams (DFDs), attack trees, and STRIDE/kill-chain taxonomies, adopting *defence-in-depth* and *segregation* as architectural principles (DO-356A) (79, 123, 139, 49, 57, 50).

CONVENTIONS AND SCOPE

- **IDs**: threats are identified by `T-F#-NN`, e.g., `T-F1-01`. Vectors by `Vx`. NIST controls by code (e.g., `AC-6`), ISO/IEC 27002 by clause (e.g., `8.24`), and DO objectives by concise reference (e.g., `DO-326A SRA`, `DO-355A Logging`).
- **Level of detail**: DFDs are presented in a structured textual form that is readily convertible to TikZ/‘dfd‘ without semantic loss.
- **Reference frameworks**: risk management (ISO/IEC 27005), ISMS requirements (ISO/IEC 27001), controls (ISO/IEC 27002), the Security Risk Assessment process and integration with the certification lifecycle (DO-326A), architectural/assurance/recording methods and principles (DO-356A), and operational/continuity guidelines (DO-355A) (79, 123, 139, 49, 57, 50).

G.1 EXAMPLE F1 GSE DATA LOAD INJECTION (DL PORT)

Summary: risk of tampering with aeronautical navigation databases by ground support equipment (GSE) connected to the *data loading* port.
Target asset: aeronautical software/data distribution and loading chain.
DFD (textual):

1. **External Entities**: Data provider; Maintenance team (GSE).
2. **Processes**: P1 Package reception/validation; P2 Signing/verification; P3 Loading into LRU.
3. **Data Stores**: D1 Secure repository; D2 Distribution log; D3 Keystore.
4. **Flows**: F1 Signed package $\rightarrow$ P1; F2 Verified package $\rightarrow$ P3; F3 Evidence $\rightarrow$ D2; F4 Keys $\leftrightarrow$ P2.

Attack tree (summary):

- T-F1-01 (root): Load a tampered package *OR* (a) compromise GSE ∧ bypass verification; *OR* (b) replace the package in the repository; *OR* (c) use uncontrolled removable media during P3.

STRIDE: Tampering, Repudiation, Information Disclosure. **Kill chain**: Recon→Weaponisation (tampered package)→Delivery (GSE/media)→Exploitation (bypass validation)→Actions.
Vectors: V1 uncontrolled USB media; V2 unhardened GSE; V3 weak/exposed keys.
Controls (sample):

- **NIST SP 800-53**: SC-12/SC-13 (cryptography/key management), AC-6 (least privilege), CM-3/CM-5 (baseline/*hardening*), AU-2/AU-6 (audit), SI-7 (software protection), MP-6 (media sanitisation).
- **ISO/IEC 27002**: 8.24 (use of cryptography), 8.32 (change management), 8.15/8.16 (logging/-monitoring), 7.10 (media), 8.27/8.25 (secure architecture/SDLC).
- **DO**: DO-326A (SRA; lifecycle integration), DO-356A (secure architecture, SAL, logging; defence-in-depth), DO-355A (operational measures for distribution and *data loading*), DO-178/254 (verification/CM evidence).

Expected evidence (examples): PSecAC/Executive summary, Secure distribution plan, Inventory/Keystore, signature-validation records (hash/cert), secure acceptance test results, loading audit trail, SVP/SCMP/SQAP, configuration review minutes.

G.2 EXAMPLE F2 CABIN NETWORK (IFE) PIVOT INTO AERONAUTICAL DOMAIN

Summary: attacker attempts to pivot from IFE to critical systems.
DFD (textual): E1 Passenger; P1 IFE; P2 Gateway/Firewall; P3 IDS/Monitoring; D1 Logs; D2 Rules; segmented telemetry flows.
Attack tree:

- T-F2-01: Successful pivot *IF* (a) segregation failure ∨ (b) gateway bypass ∨ (c) privileged credentials exposed in the management domain.

STRIDE: Spoofing, Elevation of Privilege.
Kill chain: Recon (scanning)→Delivery (IFE network exploit)→C2 (persistence)→Actions (inter-domain traversal attempt).
Vectors: V4 permissive firewall rules; V5 exposed services; V6 lack of L3–L7 monitoring.
Controls: NIST SC-7/SC-7(5) (boundary protection/DMZ), AC-4 (information flow control), IA-2/IA-5 (authentication), SI-4 (monitoring); ISO 27002 8.20-8.23 (network/service security), 8.18 (privileged utilities), 8.22 (network segregation), 8.15/8.16; DO-356A (architecture principles, ARINC domains, defence-in-depth), DO-355A (operations/monitoring).
Evidence: segmentation design, rule sets & review artefacts, IDS/IPS records, inter-domain penetration tests, gateway hardening, audit trails.

G.3 EXAMPLE F3 CERTIFICATE COMPROMISE IN THE UPDATE CHAIN

Summary: risk of accepting a forged update due to certificate/PKI compromise.
DFD: E1 Signing authority; P1 Package generation; P2 Onboard verification; D1 HSM/Keystore; D2 Repository; F1–F4 signing/validation flows.
Attack tree: `T-F3-01`: malicious package signed *IF* (a) key extraction ∨ (b) CA/RA compromise ∨ (c) verification disabled.
STRIDE: Tampering, Spoofing.
Kill chain: Recon→Exploitation (key theft)→Delivery/Actions.
Controls: NIST `SC-12`/`SC-13` (keys/cryptography), `CM-6` (secure defaults), `AU-10` (non-repudiation), `IA-7` (cryptographic authentication); ISO 27002 `8.24` (cryptography), `5.31` (legal/contractual requirements), `5.25-5.27` (incident management); DO-356A (assurance, security-requirements verification, logging), DO-355A (operational certificate management).
Evidence: key/certificate policy, rotation/rollover, *HSM attestation*, recorded *CRL/OCSP*, negative tests (reject invalid package), verified code-signing pipeline.

G.4 EXAMPLE F4 SAFEGUARDS DISABLED DURING MAINTENANCE

Summary: use of maintenance accounts/tools to alter security parameters.
DFD: E1 Technician (*privileged*); P1 Maintenance session; P2 Change management; D1 CMDB; D2 Logs/Audits; F1 Request→Approval→Execution→Closure.
Attack tree: `T-F4-01`: unauthorised change *IF* (a) segregation of duties failure ∨ (b) approval-flow bypass ∨ (c) incomplete audit trails.
STRIDE: Repudiation, Elevation of Privilege.
Kill chain: Recon (processes)→Exploitation (privilege abuse)→Actions.
Controls: NIST `AC-2`/`AC-6` (account/privilege management), `CM-3`/`CM-5` (changes/*hardening*), `AU-2`/`AU-6` (audit), `PS-7`/`AT-2` (training); ISO 27002 `5.2`/`5.3` (roles/responsibilities), `8.18` (privileged utilities), `8.32` (changes), `5.35-5.36` (compliance/review); DO-356A (tool control/assurance), DO-355A (roles/-training; incident management).
Evidence: privilege matrices, controlled *break-glass*, approval records, session recording, post-change verification, independent audits.

G.5 EXAMPLE F6 ZERO-DAY IN ARINC 429/AFDX (BEHAVIOURAL DETECTION)

Summary: detection of *zero-day* anomalies without signatures in aeronautical networks (ARINC 429 and ARINC 664/AFDX) via behavioural analysis, using operational baselines and predictive models (Isolation Forest and LSTM autoencoder).

Target asset: integrity/temporal characteristics of data-bus traffic; functions relying on ARINC/AFDX

messages (navigation, monitoring, maintenance).

DFD (textual):

1. **External Entities**: Sensors/EFIS; AFDX gateway; Collection tool.
2. **Processes**: P1 Capture; P2 Feature extraction; P3 Training; P4 Detection; P5 Response/isolation.
3. **Data Stores**: D1 Baselines; D2 Models; D3 Thresholds/Profiles; D4 Logs/Alerts.
4. **Flows**: F1 ARINC/AFDX traffic $\rightarrow$ P1; F2 Feature windows $\rightarrow$ P3/P4; F3 Alerts $\rightarrow$ P5; F4 Evidence $\rightarrow$ D4.

Data and baseline (features) *ARINC 429*: frequency per *label*/SDI, SSM distribution, inter-word (jitter), parity/error rate.
AFDX: utilisation per VL, interframe jitter, sequence, BAG/latency, loss/delay, ratios per port/partition.

Step-by-step procedure

1. **Baseline collection** (>N hours in controlled flight/ground); export PCAP/CSV and metadata. *Evidence:* EV-050 (collection plan), EV-051 (anonymised dataset).
2. **Feature engineering** (window $w = 1$–5 s); aggregate mean, stdev, p95, entropy, jitter per label/VL. *Evidence:* EV-052.
3. **Models**:
   - *Isolation Forest* (unsupervised): train on baseline; threshold at p99.7; validate with synthetic anomalies (jitter $+3\sigma$, rare label, invalid SSM). *Evidence:* EV-053.
   - *LSTM autoencoder* (sequences): reconstruct series; alarm by reconstruction error at p99.7; report MTTD and FP. *Evidence:* EV-054.
4. **Experimental validation** (*network replay*/bench): bursts on critical VL; BAG manipulation; rare labels. *Evidence:* EV-055, EV-056.
5. **Operationalisation** (runbook): integration in gateway/IDS; graduated actions (rate limiting, isolation, *safe mode*, forensic capture). *Evidence:* EV-057, EV-058.

Acceptance criteria (example) MTTD ≤ 2 s for deviations $> 3\sigma$; FP $<$ 1/h on critical VL; log retention ≥ 180 days; regression upon each baseline update.

Traceability (summary) NIST: RA-5, CA-7, SI-4, AU-6; ISO/IEC 27002: A.8.16, A.8.8, A.8.9; DO: DO-326A (SRA), DO-356A, DO-355A.

G.6 TRACEABILITY TABLE

Threat (ID)	Vector	Primary Controls (NIST / ISO 27002 / DO)	Evidence (examples)
T-F1-01	V1, V2, V3	NIST: SC-12, SC-13, AC-6, CM-3/5, AU-2/6, SI-7, MP-6; ISO: 8.24, 8.32, 8.15–8.16, 7.10, 8.27/8.25; DO: DO-326A SRA, DO-356A (architecture, SAL, logging), DO-355A (distribution/*data loading*)	Key policy; verification logs; rejection tests; SVP/SCMP/SQAP; loading audit trails
T-F2-01	V4, V5, V6	NIST: SC-7, AC-4, IA-2/5, SI-4; ISO: 8.20–8.23, 8.22, 8.18, 8.15–8.16; DO: DO-356A (domains, defence-in-depth), DO-355A (operational)	Segmentation design; reviewed rule sets; evidenced IDS/IPS; inter-domain *pentest*
T-F3-01	—	NIST: SC-12/13, CM-6, AU-10, IA-7; ISO: 8.24, 5.31, 5.25–5.27; DO: DO-356A (assurance/verification), DO-355A (certificates)	*HSM attestation*; *CRL/OCSP*; negative tests; signing trails
T-F4-01	—	NIST: AC-2/6, CM-3/5, AU-2/6, PS-7, AT-2; ISO: 5.2–5.3, 8.18, 8.32, 5.35–5.36; DO: DO-356A (tools/assurance), DO-355A (roles/training)	Documented SoD; approvals; session recording; post-change verification; audits

Source: Prepared by the author.

Normative references mobilised in this appendix (for traceability): ISO/IEC 27002 (structure of organisational/people/physical/technological controls; topics 8.15–8.16 logging/monitoring; 8.20–8.23 networks; 8.24 cryptography; 8.25–8.29 SDLC/architecture/testing; 8.32 changes) (139); ISO/IEC 27001 (ISMS requirements and risk assessment/treatment, Section 6) (123); ISO/IEC 27005 (risk management process; annexes with threat examples) (79); DO-326A (SRA and integration with the certification lifecycle) (49); DO-356A (methods, architectural principles, SAL, logging and effectiveness assessment) (57); DO-355A (operations, *data loading*, incident/certificate management) (50). For lifecycle evidence, see also DO-178/DO-254 datasets/plans (26, 42).

H. ASSURANCE CASE PROTOTYPE (GSN)

This appendix presents a prototype *assurance case*, structured according to Goal Structuring Notation (GSN), applied to a critical requirement of the framework. The objective is to demonstrate, in a formal and auditable manner, how the evidence already catalogued in the security RTM (Appendix D) supports a guarantee argument (claim → strategy → evidence) aligned with NIST SP 800-53 Rev. 5 (121), ISO/IEC 27001:2022 and ISO/IEC 27002:2022 (123, 139), as well as aeronautical security guidance DO-326A/DO-356A/DO-355A and related standards (26, 42, 49, 57, 50).

The selected requirement is **REQ-SEC-014 — Vulnerability Assessment and Testing**, chosen because it represents the link between detection, remediation, and continuous monitoring of vulnerabilities in embedded systems. In the RTM (Appendix D), REQ-SEC-014 is tied to evidence items **EV-014** (scan reports, penetration tests, and tracked fixes) and to **POA&M** entries (Appendix E), composing the cycle identification → prioritisation → mitigation (NIST RA-5/CA-5/CA-7; ISO/IEC 27001/27002; DO-356A) (121, 123, 139, 42).

Table H.1: Textual GSN Prototype for REQ-SEC-014 (Assurance Case)

GSN Element	Description
Claim (G1)	The system maintains exposure to vulnerabilities at an acceptable level throughout the lifecycle, in accordance with REQ-SEC-014, NIST SP 800-53 requirements (RA-5, CA-5, CA-7) (121), and ISO/IEC 27001:2022/27002:2022 good practices (123, 139).
Context (C1)	Scope: aeronautical embedded software; acceptability criteria by severity/criticality (ISO/IEC 27001/27002) (123, 139); control baseline and corrective governance via POA&M (NIST CA-5) (121); aeronautical security guidelines DO-326A/DO-356A/DO-355A (26, 42, 49).
Strategy (S1)	Argument based on (i) objective evidence (EV-014), (ii) RTM traceability (Appendix D), and (iii) corrective plan and deadlines (POA&M; Appendix E), demonstrating systematic detection, timely remediation, and continuous monitoring (121, 123, 139).
Sub-claim (G1.1)	*Systematic detection:* periodic execution of scans, penetration tests, and analyses (static/dynamic) with coverage of critical components (NIST RA-5; DO-356A) (121, 42).
Sub-claim (G1.2)	*Traceable and timely remediation:* recording findings, prioritising by severity, linking RTM↔EV-014↔POA&M, and verifying effectiveness (NIST CA-5; ISO/IEC 27001/27002) (121, 123, 139).
Sub-claim (G1.3)	*Post-deployment continuous monitoring:* effectiveness indicators (e.g., MTTD/MTTR) and lifecycle feedback (NIST CA-7; ISO/IEC 27001/27002; DO-355A for maintenance/operational aspects) (121, 123, 139, 49).
Evidence (E1)	**EV-014:** scan/pen-test reports, remediation and re-assessment trails, linked to the RTM (Appendix D).
Evidence (E2)	**POA&M:** CA-5 items with deadlines, accountable owners, and status, evidencing corrective governance (Appendix E) (121).
Evidence (E3)	Effectiveness metrics (e.g., indices derived from REQ-SEC-013 where applicable), demonstrating reduced exposure and absence of recurrence (123, 139).
Acceptance Criteria	*Critical/High* findings mitigated within $\leq$ 15 days; MTTD $<$ X h; MTTR $<$ Y h; zero recurrence across two successive scan/test cycles (121).

Source: Prepared by the author.

This prototype demonstrates the feasibility of constructing security assurance cases from the artefacts already available (RTM, EV-014, POA&M), strengthening methodological rigor and facilitating the harmonisation of audits (NIST/ISO/DO) with a unified evidence repository (121, 123, 139, 26, 42, 49, 57, 50).

Although focused on a single requirement, the model scales to other critical requirements mapped in the phase- and activity-based matrices, with gains in repeatability and governance.

INTEGRATION GUIDANCE FOR LEGACY SYSTEMS

Non-intrusive collection architecture

For legacy environments (e.g., ARINC 429), we recommend *read-only* instrumentation via tap/mirroring, observing bus-specific rate limits and constraints. Data are normalised into events and forwarded to behavioural detection and response-orchestration mechanisms, ensuring traceability to evidence items and normative controls (121, 123, 139, 57, 50). In non-IP topologies, use edge buffering and periodic shipment of artefacts to the central evidence repository.

Threat → Vector → Controls → Evidence mapping

Table H.2 relates legacy threat scenarios, their technical vectors, the method's activities/controls, and the supporting evidence (EV-059–EV-066), with cross-references to the RTM (Appendix C) (121, 139, 57).

Table H.2: Examples of Legacy Threats, Vectors, Controls, and Evidence

Threat	**Legacy vector**	**Method controls/activities**	**Evidence (EV-059–EV-066)**
Bus word injection	Alteration of *labels*/bits in serial flow	Behavioural baseline; integrity alarm; [AUTO] containment playbook	EV-059, EV-060
Configuration drift	Parameters outside the approved baseline	Secure-configuration gate in CI/CD; [HUMAN] review	EV-061
Telemetry drop/noise	Anomalous silence / noise above threshold	Periodic health-check; controlled failover; incident record	EV-062, EV-063
Side channel/EMI	Unplanned couplings	Physical/EMC hardening; route audit; risk-driven testing	EV-064

Source: Prepared by the author.

Step-by-step procedure

(1) Inventory assets and flows; **(2) Instrumentation** (tap/mirror); **(3) Normalisation** to events; **(4) Behavioural** baseline; **(5) Detection** and alarms; **(6) Response** via [AUTO]/[HUMAN] playbook; **(7) Validation and POA&M**; **(8) Metrics** (MTTD, MTTR, FPR), with registration in RTM/EV-059–EV-066 (121, 50).

Maturity playbooks (L1–L3)

L1 (Initial): one compliance gate, one simple detector, one playbook; *L2 (Intermediate):* multiple gates, extended coverage, response exercises; *L3 (Advanced):* advanced (behavioural/predictive) detection, orchestration with continuous KPIs, and iterative hardening (139, 26, 42).

Exit criteria (done)

(i) **MTTD** $\leq$ **5 min**; (ii) **% of pipelines with active gates**; (iii) **minimum EV-XXX** per deployed scenario and auditable; (iv) **false-positive rate** within the agreed threshold; (v) **RTM updated** and **POA&M** actions closed (121, 123, 50).

IMPLEMENTATION QUICK-START GUIDE

Prerequisites

Version-controlled repository; active CI/CD pipeline; repository for RTM/EV; roles defined for execution of [AUTO]/[HUMAN] playbooks; operational target **MTTD** $\leq$ **5 min** (121, 139, 26).

Ten steps (MVP in 1–2 weeks)

1) Enable minimal collection (tap); 2) Normalise events; 3) Define baseline; 4) Build one simple behavioural detector; 5) Create one [AUTO]/[HUMAN] playbook; 6) Activate one *compliance-as-code* gate in CI/CD; 7) Register generated EV-XXX; 8) Measure MTTD/MTTR; 9) Run a tabletop exercise; 10) Tune thresholds and publish updates to RTM/POA&M (121, 123, 50).

Templates

Example CI/CD gate (generic).

```
policy:
  require:
    - sbom.present == true
    - evidence.has(["EV-059","EV-060"])
    - config.checks >= minimal_set
on_fail:
  action: "block_release"
  notify: ["SecEng [HUMAN]"]
```

Playbook skeleton (summary). [AUTO] isolate suspicious flow $\rightarrow$ [AUTO] attach EV-062 $\rightarrow$ [HUMAN] service-return decision $\rightarrow$ [AUTO] update POA&M/RTM (50).

KPIs and acceptance criteria

MTTD, MTTR, % pipelines with gate, % events covered, evidence quality, false-positive rate — all linked to RTM items (121, 139).

Evolution roadmap

Scale from MVP (L1) to extended coverage (L2) and advanced orchestration (L3), integrating additional controls, predictive detection, and periodic exercises (139, 26, 42).

I. SURVEY INSTRUMENT AND SAMPLING PLAN

This appendix provides a detailed account of the survey instrument used to validate the holistic framework proposed in this thesis, together with the sampling plan and data collection procedures employed. The empirical validation was conducted with aerospace industry experts—specifically, professionals from Airbus Defence and Space—with the objective of assessing the applicability, effectiveness, and practical relevance of the framework.

I.1 RESEARCH CONTEXT AND OBJECTIVES

The framework proposed in this thesis integrates internationally recognised security standards—such as ISO/IEC 27001, NIST SP 800-53, DO-326A, DO-356A, and DO-355A—with risk assessment strategies and adaptive measures to ensure protection throughout the software life cycle of embedded systems. Given the critical nature of avionics systems and the complexity of contemporary cyber threats, it was essential to subject the framework to evaluation by practitioners directly involved in the development and protection of safety-critical software.

The specific validation objectives were: (1) to evaluate the adequacy of the framework vis-à-vis the cybersecurity demands of embedded systems; (2) to identify strengths and gaps in the proposed approach; (3) to verify implementation feasibility in real organisational environments; (4) to collect suggestions for improvements and adjustments; and (5) to obtain an overall assessment of whether the framework should be recommended to other organisations.

I.2 SAMPLING PLAN

I.2.1 Target Population

The target population comprised professionals with experience in embedded systems and cybersecurity in the aerospace sector. Airbus Defence and Space was selected as the research context because it is a global leader in the development of safety-critical avionics systems, where cybersecurity is a central concern and aerospace security standards are rigorously applied.

I.2.2 Participant Selection Criteria

A purposive sampling strategy was adopted, which is appropriate for qualitative studies seeking analytical depth and specific expertise. Participants were selected based on the following inclusion criteria:

- Demonstrated professional experience in the development, architecture, or security of embedded

systems;

- Technical knowledge of cybersecurity as applied to the aerospace sector;
- Familiarity with relevant security standards, such as DO-326A (avionics security) and NIST SP 800-53 (security controls for information systems);
- Direct involvement in projects related to safety-critical aviation software; and
- Ability to evaluate security methodologies from technical, operational, and strategic perspectives.

No explicit exclusion criteria were defined, as all invited professionals met the minimum expertise requirements.

I.2.3 Sample Size and Characterisation

Ten experts from Airbus Defence and Space were invited to participate. This sample size is appropriate for qualitative studies that prioritise response quality and depth over statistical generalisability. Validation by a select group of specialists enables a rigorous, contextualised, and technically grounded analysis of the proposed framework.

Participants included systems architects, embedded software developers, cybersecurity specialists, avionics security engineers, and project managers involved in protecting safety-critical software. This diversity of professional profiles contributed to a multidimensional assessment of the framework.

I.3 SURVEY INSTRUMENT

I.3.1 Questionnaire Development

The survey instrument was a structured questionnaire designed specifically to evaluate the proposed framework along multiple dimensions. The development process included: (1) a literature review on the validation of cybersecurity methodologies; (2) identification of critical dimensions to be evaluated; (3) formulation of clear and objective questions; (4) inclusion of follow-up items to elicit depth; and (5) incorporation of an explanatory diagram of the framework to facilitate respondent understanding.

The questionnaire was delivered as a fillable PDF, as requested by the Airbus board, to facilitate digital completion and email return, thereby eliminating the need for printing and physical collection.

I.3.2 Questionnaire Format and Presentation

The questionnaire was distributed as a fillable PDF file, as shown at the end of this appendix (see **??**), allowing participants to respond digitally without the need for printing. A visual diagram of the proposed framework was included at the beginning of the questionnaire to serve as a reference during completion, facilitating understanding of the holistic approach and the integration among the framework's components.

Questions were formatted with checkboxes for response selection, and text fields were provided for open-ended items and additional comments. The form design prioritised clarity, objectivity, and ease of completion.

I.4 DATA COLLECTION PROCEDURES

I.4.1 Recruitment Strategy

Recruitment was conducted in two stages. First, an online meeting was scheduled via Airbus's divMeet platform, during which the master's thesis and the proposed framework were presented to potential participants. The objectives of this presentation were: (1) to contextualise the research; (2) to explain the framework in detail; (3) to demonstrate the practical relevance of validation; (4) to clarify the data collection process; and (5) to formally invite participation by the experts.

The meeting was coordinated by Dr. Andreas Schweiger, systems architect at Airbus Defence and Space, who served as the local supervisor and facilitated access to experts within the organisation.

I.4.2 Data Collection Process

Initially, the use of a physical drop-box for printed questionnaires was proposed, located in room B302 of building 362 at Airbus. This approach, however, proved unsuccessful, as no questionnaires were deposited during the initial collection period.

Given this difficulty, the collection method was adjusted. As requested by the Airbus board, the questionnaire in fillable PDF format was emailed to participants, who could complete it digitally and return it by email, with a copy to Dr. Andreas Schweiger. This approach proved more effective and convenient, removing logistical barriers and facilitating participation.

I.4.3 Collection Timeline

The data collection process followed the timeline presented in Table I.1.

Table I.1: Data collection timeline

Date	Activity
19 March 2025	Initial invitation to the thesis presentation sent
24 March 2025	Online meeting to present the framework and explain the research process
07 April 2025	Follow-up email reinforcing the invitation and adjusting the collection method (from physical to digital)
April–May 2025	Period for receiving participant responses

Source: Prepared by the author.

I.5 ETHICAL CONSIDERATIONS

I.5.1 Informed Consent

The research was conducted on a voluntary participation basis. The purpose of the study was clearly communicated during the presentation meeting and reiterated in the invitation emails. Participants were informed that the data would be used exclusively for validating the master's thesis and that their participation would contribute to advancing knowledge in cybersecurity for safety-critical embedded systems.

I.5.2 Confidentiality and Data Protection

Confidentiality of responses was ensured. Data were treated in aggregate form, with no individual identification in the analyses and results presented. Data storage adhered to best practices in information security, and access was restricted to the researcher and the thesis supervisor.

I.5.3 Institutional Compliance

The data collection process complied with Airbus's institutional policies. The Airbus board specifically requested that the questionnaire be presented as a fillable PDF, which was implemented. In addition, the research had the support and supervision of a senior member of the organisation (Dr. Andreas Schweiger), ensuring alignment with internal guidelines.

J. RAW DATA AND QUANTITATIVE ANALYSES

This appendix documents the anonymised raw data, the variable dictionary, descriptive statistics, and the composite indices used to interpret the results of the expert questionnaire. Items flagged as *multi-selection* permit multiple choices per respondent.

J.1 CODEBOOK

Table J.1: Variable dictionary (selected questions)

Code	Prompt (summary)	Type	Options (codes → meaning)
Q1	Coverage of key cybersecurity demands	single	a=Yes (full); b=Partial; c=No; d=Undecided
Q2	Adaptability to scenarios/infrastructures	multi	a=High in both; b=Better in scenarios; c=Better in infra; d=Limited
Q4	Detection and response (avionics/embedded)	multi	a=Yes; b=Partial; c=No; d=Undecided
Q5	Most effective aspects (detect/response)	multi	a=Continuous monitoring; b=Behavioural analysis; c=NIST/DO standards; d=Malicious FW blocking
Q6	Recommended improvements (detect/response)	multi	a=Real-time monitoring; b=Automated response; c=Zero-day; d=Adaptability
Q7	Potential limitations (emerging risks)	multi	a=Zero-day; b=Real-time response; c=Compliance vs. flexibility; d=Performance; e=Supply-chain/FW
Q8	Most effective mechanisms (known vulns)	multi	a=Crypto; b=AuthN; c=Vuln/patching; d=Standards; e=Real-time monitoring
Q9	Reinforcement of Q8 (most effective)	multi	a=Crypto; b=AuthN; c=Vuln/patching; d=Standards; e=Real-time monitoring
Q10	Resilience to unknown threats	single	a=Yes; b=Partial; c=No; d=Undecided
Q11	Improvements for resilience (reinforces Q10)	multi	a=Zero-day detection; b=Automation/recovery; c=Mitigate zero-day; d=Adaptability; e=A or D
Q12	Advanced threats (zero-day/supply/ransom)	single	a=Yes; b=Partial; c=No; d=Undecided
Q13	Improvements vs. advanced threats	multi	a=Zero-day; b=Supply chain; c=Ransomware/recovery; d=Automation; e=Other
Q14	Integration DO-326A & NIST 800-53	single	a=Yes; b=Partial; c=No; d=Undecided

Code	Prompt (summary)	Type	Options
Q15	Where to improve integration (reinforces Q14)	multi	a=Alignment; b=Adaptation; c=Interoperability; d=Lifecycle; e=Other
Q16	Do we need *additional standards*?	single	a=No; b=Yes
Q17	Most effective IT↔Embedded elements	multi	a=AuthN/AC; b=Network monitoring; c=IR (NIST/ITIL); d=IT↔ES sync
Q18	Reinforcement of Q17 (most effective)	multi	a=AuthN/AC; b=Monitoring; c=IR; d=Sync
Q19	Ease of implementation (1–4)	single	a=1; b=2; c=3; d=4
Q20	Adoption challenges	multi	a=Cost; b=Staffing; c=Legacy; d=Time/resources; e=Scalability; f=Regulatory
Q21	Clarity/Intuitiveness	single	a=Clear; b=Partial; c=Complex; d=Undecided
Q22	Where to improve understanding (reinforces Q21)	multi	a=Documentation; b=Examples; c=Training; d=Alignment; e=A or D
Q23p	Positive operational impacts	multi	a=Security; b=Compliance; c=IR; d=Resilience
Q24n	Negative impacts / challenges	multi	a=Complexity; b=Cost; c=Performance; d=Integration
Q25	Team coordination (1–4)	single	a=1; b=2; c=3; d=4
Q26	Risk reduction benefits	multi	a=Detection; b=IR; c=Attack surface; d=Compliance
Q27	Operational efficiency benefits	multi	a=Coordination; b=Automation; c=Resources; d=Downtime
Q28	Countermeasure prioritisation	single	a=Highly effective; b=With limitations; c=No; d=Undecided
Q29	If 28=B/C: where to improve	multi	a=More structured risk; b=Priority guidance; c=Align frameworks; d=Automation; e=A or D
Q30	Recommend (1–5)	scale	1–5

Source: Prepared by the author.

J.2 ANONYMISED RAW COUNTS

Table J.2: Counts by alternative (selected questions)

Q	a	b	c	d	e	Resp.	Notes
Q1	1	7	1	1		10	single
Q2	5	4	5	1		10	multi
Q4	0	9	2	1		10	multi
Q5	7	5	7	5		9	multi
Q6	6	6	6	6	3	8	multi; ‘e’=A or D
Q7	7	7	6	6	7	10	multi
Q8	5	6	7	8	6	10	multi
Q9	2	4	8	8	2	10	multi

Q	a	b	c	d	e	Resp.	Notes
Q10	1	6	2	3		10	single
Q11	6	5	3	6	3	9	multi
Q12	1	6	2	2		10	single
Q13	7	7	4	5	2	10	multi
Q14	1	5	2	3		10	single
Q15	6	4	4	5	2	9	multi
Q16	1	8				9	single; 1 blank
Q17	5	8	4	6		10	multi
Q18	5	8	2	4		10	multi
Q19	2	7	1	0		10	scale 1–4
Q20	7	10	9	8	6	10	multi
Q21	1	6	2	1		10	single
Q22	3	2	0	2	3	10	multi
Q23p	7	6	5	6		8	multi
Q24n	6	8	4	7		10	multi
Q25	1	1	7	1		10	scale 1–4
Q26	10	5	5	6		10	multi
Q27	10	7	3	5		10	multi
Q28	2	7	1	0		10	single (includes ‘ae’ as ‘a’)
Q29	9	4	4	5		10	multi
Q30						9	mean=3.0; mode=3; 1 missing

Source: Prepared by the author.

Table J.3: Variable dictionary (concise)

Code	Label (prompt)	Type	Positive
Q1	Coverage of key demands	single	a,b
Q2	Adaptability scenarios/infra	multi	a,c
Q4	Detection and response	multi	a,b
Q5	Effective aspects (D/R)	multi	a,b,c,d
Q7	Potential limitations	multi	–
Q8	Effectiveness (known vulns)	multi	a,b,c,d,e
Q10	Resilience (unknown threats)	single	a,b
Q14	DO-326A & NIST integration	single	a,b
Q16	Additional standards	single	b
Q17	IT↔Embedded (elements)	multi	a,b,d
Q19	Ease of implementation 1–4	scale	higher=better
Q20	Adoption challenges	multi	–
Q21	Clarity/Intuitiveness	single	a,b
Q23p	Positive impacts	multi	a,b,c,d
Q24n	Negative impacts	multi	–
Q25	Coordination 1–4	scale	higher=better
Q26	Risk reduction	multi	a,b,c,d
Q27	Operational efficiency	multi	a,b,c,d
Q28	Countermeasure prioritisation	single	a,b
Q30	Recommendation 1–5	scale	higher=better

Source: Prepared by the author.

Anonymisation note. Respondent identification uses only codes ($I \ldots X$) with no personal metadata. For multi-selection items, responses were recorded as reported by participants (e.g., "`b; c`").

J.3 RESPONSE DISTRIBUTIONS BY PARTICIPANT

Table J.4 presents the consolidated response matrix for blocks I to X, organised by participant (rows) and selected alternatives (columns). This register enables traceability between each respondent and their choice patterns, providing the basis for subsequent quantitative and qualitative analyses. For transparency and reproducibility, complete questionnaires are available as PDFs from the next page onward.

Table J.4: Responses by participant

	I	II	III	IV	V	VI	VII	VIII	IX	X
1	b	b	a	b	b	c	b	b	b	d
2	abc	b	a	c	a	d	bc	c	b	a
3	cde	c	b	b	b	d	cd	b	b	be
4	b	b	b	b	b	c	bd	b	b	bc
5	abcd	ac	abcd	ac	a	-	abcd	abcd	ac	abc
6	abcd	d	abcd	b	-	abcd	cd	abcd	-	ab
7	e	ce	b	ad	e	abcde	abcde	abde	ab	abcde
8	cd	cd	bce	e	c	abcd	cd	acde	bd	abcde
9	cd	cd	cd	c	c	c	cd	acde	bd	abc
10	b	bd	b	b	bd	c	b	c	d	ae
11	abcd	ad	bde	ad	a	abcd	ad	abcd	e	-
12	b	b	a	b	b	cd	bd	b	d	bd
13	abcd	ab	e	ab	a	abcd	ab	abcd	e	abcd
14	b	bd	a	b	b	cd	bd	d	d	d
15	abcd	ad	e	ad	d	abcd	ad	abd	e	-
16	b	b	b	b	b	b	b	b	a	e
17	abcd	bd	bd	b	b	bc	ab	c	a	abcd
18	b	bd	abcd	b	b	ab	ab	c	a	abcd
19	b	a	c	b	b	b	b	a	b	b
20	bcde	bcdf	bc	bcd	cd	bcde	bcd	abdf	d	abcd
21	b	b	a	c	c	bd	bd	b	d	b
22	abcd	ab	e	b	a	abcd	ab	a	e	bc
23	abcd	ab	bc	a	a	bd	ab	abcd	ad	acd
24	b	b	ad	a	b	ac	b	abc	abd	abcd
25	c	c	d	c	c	b	c	a	c	c
26	acd	ac	ac	a	a	ad	a	abcd	ac	abd
27	a	ac	bc	a	a	abcd	abcd	bd	a	ab
28	bd	b	a	b	b	cd	bd	c	b	ae
29	abcd	ad	e	ab	a	abcd	abc	abcd	bc	-
30	3	3	4	4	3	1	3	2	-	4

Source: Prepared by the author.