

Air Traffic Management Security in the Digital Age: A Proactive Risk Management Strategy

Tim H. Stelkens-Kobsch
Institute of Flight Guidance
German Aerospace Center (DLR)
Braunschweig, Germany
<https://orcid.org/0000-0002-8485-6628>

Maria Hagl
Institute of Flight Guidance
German Aerospace Center (DLR)
Braunschweig, Germany
maria.hagl@dlr.de

Per Håkon Meland
Department of Software Engineering,
Safety and Security
SINTEF Digital
Trondheim, Norway
<https://orcid.org/0000-0002-5509-0184>

Gurjot Singh Gaba
Department of Computer and
Information Science (IDA)
Linköping University, Sweden
Linköping, Sweden
gurjot.singh@liu.se

Karin Bernsmed
Department of Software Engineering,
Safety and Security
SINTEF Digital
Trondheim, Norway
<https://orcid.org/0000-0001-9109-5401>

Carlo Dambra
ZenaByte s.r.l.
Genova, Italy
carlo.dambra@zenabyte.com

Vladimíra Čanádiová
Secure Societies Area
Deep Blue S.r.l.
Rome, Italy
<https://orcid.org/0009-0001-3962-3366>

Gencer Erdogan
Sustainable Communication
Technologies
SINTEF Digital
Oslo, Norway
<https://orcid.org/0000-0001-9407-5748>

Marius Simionescu
Technical Directorate
Skyway Air Navigation Services, S.A.
Madrid, Spain
msimionescu@skyway-ans.com

Bhavesh Sharma
Secure Societies Area
Deep Blue S.r.l.
Rome, Italy
bhavesh.sharma@dblue.it

Andrei Gurtov
Department of Computer and
Information Science (IDA)
Linköping University, Sweden
Linköping, Sweden
andrei.gurtov@liu.se

Abstract— The security risk management discipline has historically been less developed than safety management systems, but the rapid digitalization of industries creates an urgent need for more proactive approaches. Current methods often rely on outdated lists and paper-based processes, leading to overlooked vulnerabilities and delayed responses to emerging threats. This paper presents a possible enhancement of the existing cyber and physical Security Risk Assessment Methodology (SecRAM). The enhanced SecRAM is currently validated through dedicated exercises and expert input. The approach considers cascading effects for attack and impact propagation, and is embedded within a system framework that recognizes interconnections and dependencies between services, systems, procedures, roles, and functions. With its web-based tool and user-friendly interface, the enhanced SecRAM proves its general applicability and shows potential for broader adoption across sectors, particularly aviation. Future work will focus on integrating automation and AI to improve efficiency and accuracy in risk assessments.

Keywords—cyber, security, risk assessment, risk management, tool support

I. INTRODUCTION

Unlike safety management systems, security risk management systems are a relatively new discipline that has gained attention in recent years. While safety management systems have been extensively developed with the first systems emerging even before the Industrial Revolution, security risk management was first explored in the second half of the last century. The rapid digitalization of the aviation industry and the rise of emerging risks, such as cyberattacks,

emphasize the urgent need for more proactive, dynamic, and adaptive approaches to security risk management. Security risk management is still commonly relying on static checklists that quickly become outdated. For example, the underlying catalogs of assets, threats, vulnerabilities, and controls are tedious to keep updated. Furthermore, relying on outdated lists and paper-based processes can lead to overlooked vulnerabilities and hence delayed responses to emerging threats. In some cases, security checklists remain unchanged for years, failing to reflect the latest regulatory requirements or threat landscape. This is not only inefficient but also increases the likelihood of human error in risk assessment. Nonetheless, keeping the informational content adjusted to the increasing speed of technology development requires a fundamental change in the underlying methodology. There are just a few tools available which provide automated assessment and maintenance of security risks [1], and especially when physical security needs to be considered, the common cybersecurity-optimized tools reach their limits.

The technologies driving the world are experiencing an increasing number of cyber-attacks. While this can harm individuals, it becomes even more devastating for the general public when targeting critical infrastructures. Air Traffic Management (ATM), being one of these safety-critical infrastructures, is no exception. In fact, ATM is a very vulnerable target, especially due to its interconnection with multiple systems, the increased use of commercial-off-the-shelf software and services and the involvement of operational and safety-critical personnel. ATM security does not rely solely on its own protection but also on the cybersecurity of

Author version.

Published version available at: <https://doi.org/10.1109/DASC66011.2025.11257275>

Copyright 2025 IEEE

airports, airlines, and digital service providers. A breach in any of these elements can compromise the integrity of the entire system, increasing the risk of coordinated attacks and operational failures. Furthermore, the continuous development of adversaries' technological equipment and knowledge necessitates adaptation on the defender's side. To stay ahead of the attackers, it is essential to rethink legacy approaches, methodologies, and habits, while the analysis of cascading effects may reveal hidden vulnerabilities, costs and a need for additional mitigations measures.

This paper addresses the development of an enhanced cyber and physical security management capability, for the existing SecRAM [2], which was developed specifically for the aviation and ATM environment. As a part of the SEC-AIRSPACE project¹, the methodology has been revised and upgraded with additional modules, user-friendly interfaces, and web-based interaction. These enhancements better reflect the increased interconnectivity of services, systems, procedures, roles, and functions in ATM, while also easing the arduous work that security experts typically have to perform. In addition, the updated approach also considers cascading effects for both attack and impact propagation. The modernization of the methodology not only responds to the increasing interconnectivity but also to the need for a more dynamic and adaptable management approach to emerging threats. This updated approach is currently being validated through dedicated exercises and with the involvement of knowledge experts and stakeholders to achieve proof of concept. This paper will provide the first insights into the results.

The work involved updating and expanding the existing taxonomy of primary and supporting assets, as well as the attack vectors targeting them. Furthermore, the system in question is not viewed in isolation but is recognized as a system embedded within other systems. Therefore, new interconnections, such as cyber, physical and logical connections, are considered as potential pathways for cascading effects to dependent systems. These connections may function as propagation pathways and potential causes or intensifiers of vulnerabilities in the interconnected infrastructure, possibly amplifying the impact of cascading effects.

The exercises aim to test the general feasibility of the enhanced security risk assessment methodology and its initial implementation as a web-based tool called SecRAM Navigator. The paper will report on how the validation findings support the further implementation of the methodology.

As cyber threats evolve, the approach must be able to adapt to remain effective. Continuous updates and improvements are crucial to ensure SecRAM stays relevant across various sectors, but particularly ATM. Amongst others, this ability needs to be validated.

The main research question addressed in this paper is "How can the cybersecurity risk assessment of existing and future ATM systems be improved?". This paper summarizes the research activities that have been undertaken to address this overall question, and it will explain how validation activities were used to validate key results (KRs).

II. HISTORY OF SECURITY RISK ASSESSMENT METHODOLOGIES IN ATM

In the early years of aviation, security concerns were quite limited, as the industry was relatively small, and its systems were isolated from the outside world. As air traffic grew, basic security measures were developed due to an increased number of malicious attacks on ATM which reached an impact that could no longer be neglected. In the 1960s and 1970s aviation administrations and other regulatory bodies began to develop initial security guidelines for ATM as a reaction to recurring terrorist attacks. These were, however, mostly applicable for physical security measures at airports to avoid passengers bringing explosives, inflammables or weapons on board. The measures helped to counter the threat and the number of successful physical attacks (specifically hijacking) has since decreased [3] [4]. However, the attacks could never be completely avoided, and a fundamental feeling of insecurity grew among those involved in air traffic management. This confirmed the need for a comprehensive and structured approach to counter adversaries in aviation and led to the development of specific security risk assessment methodologies.

Existing risk assessment frameworks, such as the ICAO Safety Management Manual (SMM) [5], FAA Safety Risk Management (SRM) [6], EU/EASA Safety Management System (SMS) Framework [7], and ISO/IEC 27005 [8], may fall short in addressing the distinct challenges of modern aviation systems. While all these frameworks provide structured approaches to identifying, analyzing, and mitigating risks – essential for protecting systems, reducing vulnerabilities, and supporting decision-making – they were developed primarily for aviation safety or general IT environments. As a result, they lack the specialized context, cyber-physical integration, and operational complexity needed to effectively secure today's highly interconnected aviation environment.

In Europe, the development of ATM security was led by EUROCONTROL and NATO in the aftermath of the 9/11 attacks. This can be seen as a trigger point for the development of today's approaches in security. The two organizations established the NEASCOG (NATO EUROCONTROL ATM Security Coordinating group). At this inter-organizational forum, representatives from both civil and military sectors converge to exchange intelligence, discuss emerging threats, and collaborate on implementing countermeasures to safeguard ATM systems. The original concept for ATM security was adopted by e.g.,

- SESAR (Single European Sky ATM Research) during its definition phase in 2005 [9].
- ICAO: Annex 17 (Security) [10] included a SARP (Standard And Recommended Practice) for ATM security (12th amendment); the Aviation Security Manual (Doc 8973) [11] was further updated; the Circular 330 on Civil Military Cooperation in ATM (published in 2011) [12], included a chapter on ATM security; and finally, at the beginning of 2013 the Air Traffic Security Manual [13] was published, including the agreed global definition of ATM security.

¹ <https://www.sesarju.eu/projects/sec-airspace>

- ECAC, the European Civil Aviation Conference, which included ATM security as Chapter 13 within its Doc 30 (guidance for aviation security) [14].
- Last but not least, in 2013 CANSO set up the ATM Security Working Group.

The purpose of a security risk assessment methodology is to evaluate the security risks of an organization facing intentional unauthorized interactions. Process steps and methodologies for security risk assessment vary depending on the specific assessment process adopted. The following sections outline various approaches to conducting security risk assessments for ATM.

The implementation of the risk assessment approaches may vary depending on the national authority. In airspaces, such as those in the United States (FAA, NextGEN) and Europe (EUROCONTROL, SESAR), standardized security risk assessment methodologies have been established. Their application is recommended, if not mandatory. Supported by the European Union, SESAR Joint Undertaking (SESAR JU) has developed SecRAM, which is now a widely accepted framework for European aviation stakeholders to assess risks. Due to the collaboration of SESAR JU and NextGEN, their security risk assessment methodologies are being harmonized to ensure consistency and alignment across the initiatives [15].

A. Reference risk management frameworks

It can be stated that in principle, all security risk assessment methodology frameworks have the following characteristics:

- Methodology: A structured framework that assesses the likelihood and potential consequences of various security threats.
- Strengths: Comprehensive, widely adopted, and providing a standardized approach.
- Weaknesses: Requires significant resources, expertise, and time to implement. Difficult to adapt.

When facing the need to perform a security risk assessment, it has to be decided which of the frameworks is the best choice for the problem at hand. This is often driven by work experience of the responsible person or group. However, some of the frameworks became more and more popular and adopted. A synopsis of the most prevalent ones is given in the sub-sections below, which does not claim to give an exhaustive overview.

1) ISO/IEC 27005

The ISO/IEC 27005 [8] standard aims to provide guidance on management of information risks, threats or vulnerabilities that could impact an organization's confidentiality, integrity, availability, and security. Its key elements provide systematic processes for risk assessment and risk management. Fig. 1 shows the typical management lifecycle in assessing cybersecurity risks in the context of ISO/IEC 27005.

In addition to its regulatory effect as an international standard, ISO/IEC 27005 gained importance for security risk assessment as it provides a structured approach to the management of information risks, which is essential for organizations that handle sensitive data. Implementing the standard or other frameworks which are aligned to or based on is a pre-requisite for satisfying many regulations such as the General Data Protection Regulation (GDPR), the Health

Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI-DSS).

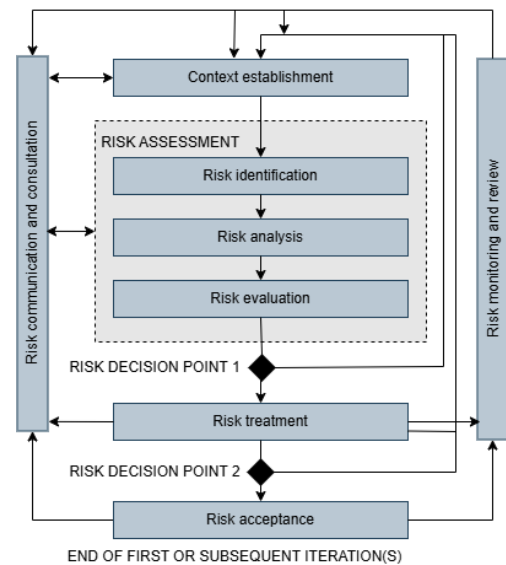


Fig. 1. Activities in a typical cybersecurity risk management lifecycle (figure adapted from ISO/IEC 27005 [8]).

The lifecycle begins with context establishment, where the organizational environment is understood, the requirements of interested parties are identified, and risk criteria are set.

Next, central assets needing protection are named and cataloged in the risk assessment phase. Potential threats and vulnerabilities are then identified, followed by a risk analysis to understand their impact and likelihood. This leads to risk evaluation, prioritizing risks according to the set criteria.

In the risk treatment phase, measures are selected and implemented to mitigate, transfer, accept, or avoid the risks. Risk communication and consultation involve sharing information about risks and management activities with stakeholders. Finally, the process includes continuous risk monitoring and review to ensure the effectiveness of the risk treatment measures.

2) NIST Cybersecurity Framework (NIST)

The Cybersecurity Framework (CSF) was developed by the National Institute of Standards and Technology (NIST). It was first published in 2013 as a voluntary consensus standard.

The framework consists of five main functions: Identify, Protect, Detect, Respond, and Recover (Fig. 2). Each function has several categories that provide more specific guidance on implementing the functions, and each category has a set of security control templates.

The CSF allows for a risk-based approach to cybersecurity management. Its approach is adaptive and iterative, and promotes proactive and responsive security practices by providing a common language and set of best practices to follow. It is commonly used by small and medium-sized businesses, large enterprises, government agencies, and non-profit organizations.



Fig. 2. Steps for creating/using a CSF Organizational Profile (from [16]).

The framework was updated to version 2.0 in the beginning of 2024 [16]. The steps shown in Fig. 2 illustrate the way how an organization can use it to achieve continuous improvement of cybersecurity.

3) Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)

This risk management framework was developed by the Carnegie Mellon Software Engineering Institute [17] and frequently used in different application areas. It is utilized e.g., by financial institutions, in the energy sector, by government agencies, for healthcare and pharmaceuticals, in the manufacturing and process industry, by transportation and logistics, and by critical infrastructures.

OCTAVE has proven to be particularly useful in industries where: (i) Human performance and decision-making are critical to operational success, (ii) Complex systems and processes are involved, and (iii) Risk management is a high priority, but may not be as well defined or quantifiable as, e.g., the static treatment and consideration of risks.

4) Open Web Application Security Project (OWASP)

The OWASP risk assessment framework is an application to perform static security testing. It provides risk assessment tools, and DAST (Dynamic Application Security Testing) scanner tools. Many tools are available for testers, but compatibility is not always given and the environment setup process is complex. However, by correctly applying the OWASP risk assessment framework's static application security testing tool, testers are able to analyze and review software code quality and vulnerabilities without any additional setup. The OWASP risk assessment framework can be integrated in the DevSecOps (Development, Security, and Operations) toolchain to help developers to write and produce secure code.

This risk assessment method uses a straightforward framework that assigns each potential risk a likelihood of occurring (Low, Medium, or High) and an impact score (also Low, Medium, or High). A 3x3 matrix then calculates the Overall Risk Severity, as illustrated in Fig. 3. While easy to apply, this approach might not offer sufficient detail for informed prioritization decisions. For instance, one may need to differentiate between risk severities that fall within the OWASP medium rating category, where more nuanced distinctions are required [18].

OWASP was introduced for software development, but its methodology can also be transferred, tailored and applied to other areas, where risk assessment is needed [19].

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

Fig. 3. OWASP Risk Assessment Matrix.

5) ISA/IEC 62443 series

ISA/IEC 62443 is a family of standards that set best practices for cybersecurity [20]. ISA/IEC 62443-3-2 outlines a structured approach to managing cybersecurity risks in Industrial Automation and Control Systems (IACS). It starts with an initial risk assessment to define scope, establish zones and conduits, and identify high-risk areas. A detailed risk assessment follows, focusing on critical assets and potential risks, creating logical zones and conduits to protect these assets. As with ISO/IEC 27005, risk treatment involves implementing measures to mitigate, transfer, accept, or avoid risks. Continuous monitoring and review ensure the effectiveness of these measures, adapting to emerging threats and vulnerabilities.

III. SECARAM OVERVIEW

SecRAM, developed under the SESAR program, is a structured framework for assessing and managing cybersecurity risks in ATM systems. Initial developments began shortly after the 9/11 attacks. SESAR decided to provide a tailored security risk assessment methodology for ATM and subsequent EU funding of the first SESAR wave allowed the initial version of SecRAM to be developed. This was concluded in the SESAR project 16.02.03, which ended 2016 [21]. Participants of the SecRAM development team were also contributing to the standardization activities leading to the well-known Airworthiness Security Process Specifications DO-326A/ED-202A and DO-356A/ED-203A from RTCA and EUROCAE.

Relevant ATM stakeholders decided in 2017 for an update of the methodology in order to make it more easy applicable, future- and cybersecurity-proof [22]. A group of European security experts (i.e., end-users, regulatory bodies, researchers) was nominated to gather lessons learnt from applying the methodology, identifying weak points and any need for improvement to establish the SecRAM 2.0 [2].

Since 2020, SecRAM 2.0 guides stakeholders – system designers, regulatory bodies, and security experts – through threat identification, vulnerability assessment, and risk evaluation tailored to the aviation sector. It promotes a systematic, operationally aligned approach to standardize collaborative cybersecurity assessments and ensure compliance with EU regulations. However, a study published in 2022 [23] revealed that while most of the practitioners from the ATM community had a positive perception of the methodology itself, they were less satisfied with the process of applying it in their projects. As aviation technologies evolve rapidly and cyber threats grow increasingly sophisticated, the SEC-AIRSPACE project now aims to evaluate and enhance SecRAM's relevance for modern cyber-physical ATM environments by identifying gaps and proposing improvements to its catalog.

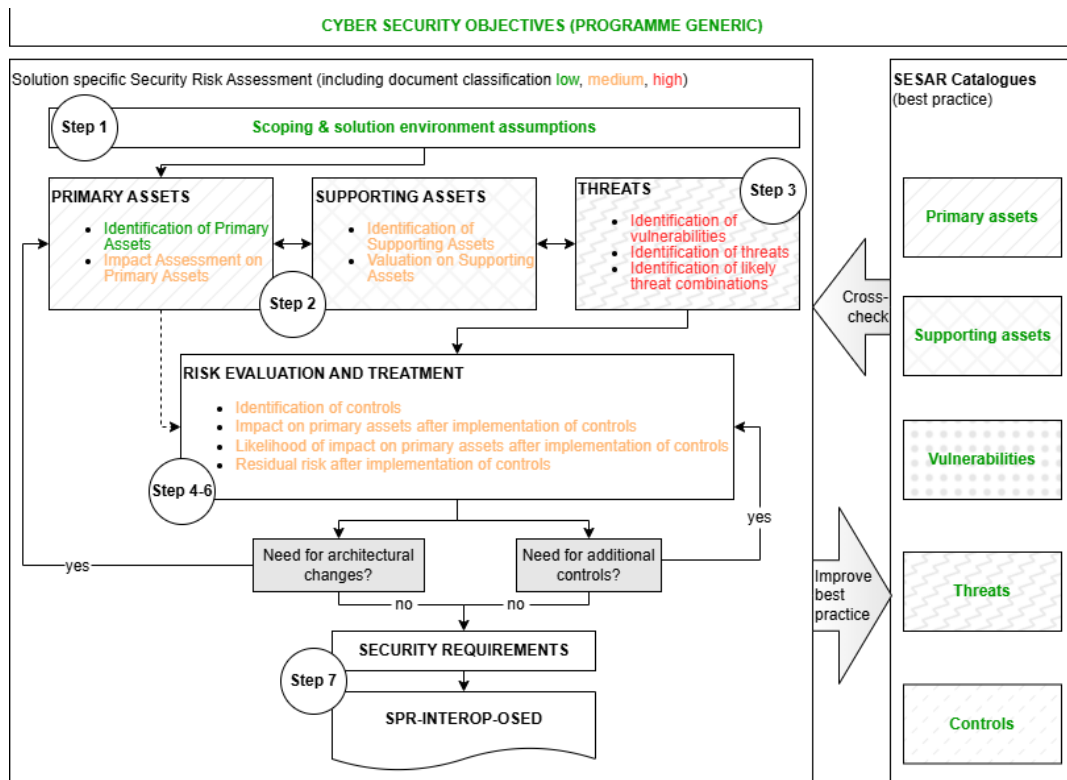


Fig. 4. The SecRAM methodology (figure adapted from SecRAM 2.0 [2]).

IV. UPDATE OF THE METHODOLOGY – KEY RESULTS

To achieve an improved methodology, SEC-AIRSPACE revisited existing ones and evaluated best-practices currently adopted in ATM. These were subsequently included as prominent building blocks for cybersecurity risk assessment. The baseline were the typical steps that one usually finds in most cybersecurity risk assessment methodologies, including but not limited to ISO/IEC 27005 [8] and SecRAM 2.0 [2]. However, the intention was not to propose a new methodology, but rather to provide the necessary extensions that will be needed to provide better estimations of the cyber risks in future ATM scenarios.

SEC-AIRSPACE formulated a set of KRs which target the identified areas of SecRAM that need improvement or further development.

The KRs which the project aims to achieve are:

- KR 1.1: An updated taxonomy for representing the elements at risk (assets) in the ATM supply chain is established.
- KR 1.2: Guidelines for identifying emerging cyber threats and vulnerabilities in ATM systems are formulated.
- KR 1.3: An analysis of potential cascading effects of cyber-attacks on ATM system is performed.
- KR 1.4: A set of recommended security controls, specifically adapted to ATM systems, including human, procedural, and organizational mitigation measures, is defined.
- KR 1.5: A method for dynamically assessing security risks in the ATM systems is developed.

- KR 1.6: A web-based interface supporting the usage of the above “building blocks” for cybersecurity risk assessment is built.
- KR 1.7: Validation and demonstration of KR related to cybersecurity risks are conducted.

All formulated key results received at least two key performance indicators (KPI) to assess their achievement.

A seven-step methodology is applied in SecRAM. This systematic approach (illustrated in Fig. 4) involves to clearly define the scope, step 1; identify relevant Primary (PA) and Supporting Assets (SA), step 2; find the threats targeting the SA, step 3; perform a risk evaluation and thereafter a treatment of unacceptable risks, step 4-6; and identify the security requirements to achieve a balanced tolerance for uncertainty and an acceptable risk landscape, step 7.

A. Research Methodology

The project employs a constructive research approach that combines theoretical analysis with practical testing. This follows pragmatism as a research paradigm, where real-life problems are solved through subjective and objective methods [24]. Researchers collaborated with practitioners to design a problem-solving solution, create a taxonomy of PA and SA, conducted literature surveys and investigated actual incidents. This led to revisiting and updating the existing catalogs of threats, vulnerabilities, and security controls, as well as describing how to close additional future gaps. The possibility of adding more steps to the SecRAM methodology was evaluated and the extensions and improvements through use cases from emerging ATM services were validated. This approach aimed to bridge theory and practice in the field of risk management in air traffic management. The validation took place in May 2025 through a series of validation exercises with ATM stakeholders.

B. Primary and Supporting Assets

The first KR from the SEC-AIRSPACE project is the updated taxonomy for representing the elements at risk (assets) in the ATM supply chain. To create this taxonomy, a structured approach was used to collect and align all the assets that were identified as being relevant to include. Several tools to set up the taxonomy were reviewed, and finally, one of them was chosen. In fact, the tool, Protégé, is open source, and provides the necessary functionalities [25].

The updated taxonomy that created in Protégé contains content from several different sources of information. Entities from the European ATM Architecture (EATMA) [26] as well as from the NASA Air Traffic Management Ontology (atmonto) [27] and the ATM Information Reference Model Ontology (AIRM) [28] were imported, including virtualization concepts and data sharing capabilities. This built upon previous research projects on remote tower and multi-remote tower centers. The currently existing taxonomy of assets in the SecRAM catalogs was also integrated to facilitate seamless transition [29].

As stated in [29], existing taxonomies for risk assessment in ATM had limitations due to heterogeneity. No “super” taxonomy existed that combined all content from individual ones.

C. Threats and Vulnerabilities

The second KR from the SEC-AIRSPACE project is the guidelines for identifying emerging cyber threats and vulnerabilities in ATM systems. To compile these, the team of aerospace security professionals involved in SEC-AIRSPACE conducted a threat analysis based on two specific use cases. The resulting data was utilized to perform a comprehensive gap analysis of the existing SecRAM threat and vulnerability catalogs. Each identified threat from the scenarios was then aligned with the most closely related threat in the SecRAM catalog, a process that required considerable adaptation and interpretive flexibility. Additionally, the analysis included a vulnerability analysis, identifying vulnerabilities susceptible to these threats and mapping them to corresponding entries in the catalog.

Of the 64 threats listed in the current version of the SecRAM catalog, only 33 were relevant to the scenarios analyzed by the project. This discrepancy primarily stems from many threats in SecRAM focusing on physical security, which did not align with the cyber-focused scenarios analyzed. The findings revealed that the existing threats in SecRAM are predominantly tailored to IT systems and do not adequately address the complexity of cyber-physical systems prevalent in the aerospace sector. The insights and recommendations in TABLE I. aim to refine the SecRAM threat and vulnerability catalogs.

To ensure the relevance and accuracy of this ATM-specific resource, it is recommended that the SecRAM catalogs align with publicly maintained catalogs, which are regularly updated by a broad community of security experts. This strategy minimizes maintenance efforts and ensure that the catalog stays aligned with current security practices, thereby enhancing its applicability and effectiveness in aviation.

Moreover, the project proposes to categorize all the threats in the catalog into distinct groups such as type of supporting

assets affected, cyber vs non-cyber vectors, asset locations (whether ground or airspace), lifecycle stages of assets (e.g., production, deployment, etc.), and the level of sophistication or complexity of the threats. This type of categorization provides security professionals with the ability to navigate the threats in the catalog and filter them based on different properties. Furthermore, this analysis supports aviation stakeholders in the creation of tailored policies, awareness programs, and robust security measures to safeguard the aviation ecosystem.

D. Security Controls

The third KR from the SEC-AIRSPACE project is a set of recommended security controls, specifically adapted to ATM systems, which include human, procedural and organizational mitigation measures. These security controls are based on best practices, including the revised 2022 version of ISO/IEC 27002, the Center for Internet Security (CIS) Top 18 Critical Security Controls, the National Institute of Standards and Technology (NIST) guidelines [19], ISO/IEC 27400 [20], and the existing SESAR Minimum Set of Security Controls (MSSC) [9]. The existing controls from these sources have been collected and then extensively updated and expanded by the SEC-AIRSPACE project as follows.

TABLE I. SUMMARY OF PROPOSED CHANGES TO SECARAM 2.0 THREATS AND VULNERABILITIES CATALOGS

Category	Description
Title	Revisions or enhancements proposed for the titles of 3 threats.
Description	Extensions and improvements suggested for the descriptions of 23 threats
Deletion	Recommended deletion of 3 duplicate threats and merging of 2 threats into a single entity.
New Threat	Identified 4 new threats not previously included in the SecRAM catalog.
Sub-threat	Proposed further specialization of generic threats into more precise sub-threats for 9 of the SecRAM threats. This approach defines several sub-threats under a high-level threat to represent specific types of attacks.
Categorization	Categorized identified threats according to attributes like software, hardware, network, complexity, STRIDE, etc.
Public Catalog Mapping	Each threat was aligned with the closest match in the CAPEC and ATT&CK catalogs.
New Vulnerability	15 new vulnerabilities were identified that are not currently present in the catalog.
Vulnerability Description	The mapping process matched 33 vulnerabilities from the SecRAM catalog, which were previously listed only by title without descriptions. Precise descriptions were proposed for each of these vulnerabilities.
Public Vulnerability Mapping	All identified vulnerabilities were mapped to the closest match in the CWE catalog maintained by MITRE.

First, additional security controls that were missing from the sources were identified through extensive research review and detailed analysis of selected risk assessment scenarios, explicitly addressing needs of ATM systems. Then, each control was categorized based on its operational impact: preventive (stop attacks before they occur), detective (identify threats quickly), reactive (respond to attacks effectively), and deterrent (discourage adversaries). Finally, cost indicators for many of the security controls were included, based on the CIS Top 18 Critical Security Controls framework. These cost indicators offer a comprehensive view.

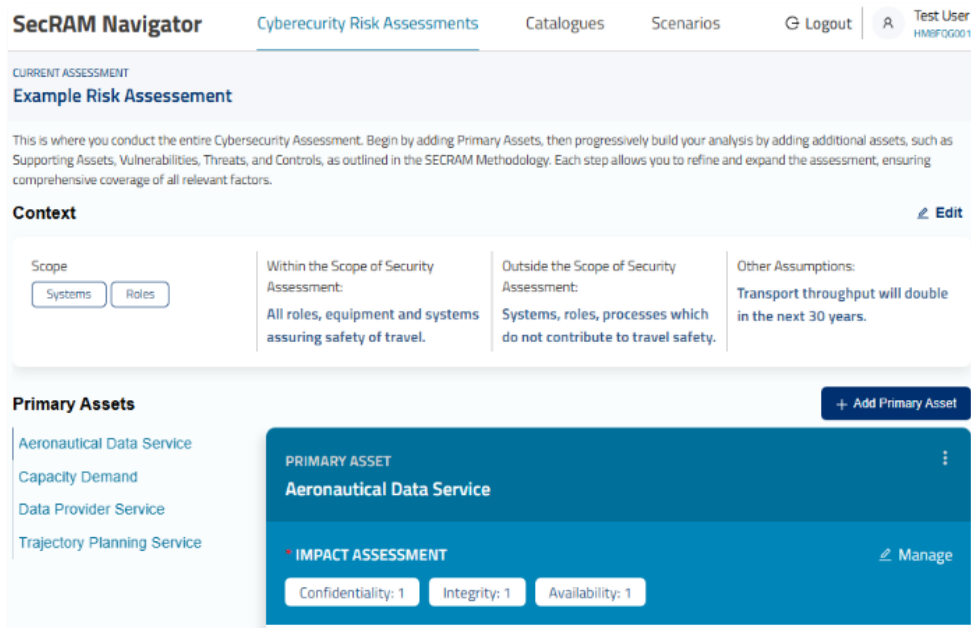


Fig. 5. SecRAM Navigator - Primary Asset overview.

tailored to different organizational scales (small, medium, large), thereby helping security analysts to prioritize and balance cybersecurity effectiveness with budgetary constraints.

The resulting set of recommended security controls from the project aim to ensure a robust and comprehensive cybersecurity posture in the ATM organizations, thereby significantly enhancing operational resilience and risk mitigation capabilities for aviation stakeholders

E. Cascading Effects

The fourth KR from the SEC-AIRSPACE project is a method for analyzing cascading effects of cyber-attacks on ATM systems. A cascading effect is a phenomenon where a security threat propagates within a component, and/or to nearby components, either sequentially or concurrently, triggering one or more additional incidents, resulting in an overall consequence that is more severe than the consequence of the first security threat alone.

Risk assessments for ATM systems often overlook the potential consequences of cascading attacks on services operated by linked infrastructures. SEC-AIRSPACE has proposed a new methodology step for SecRAM (inspired from the work of Kotzanikolaou et al. on critical infrastructures [30]), which addresses this gap by introducing the concept of “Dependency Risk of Attack” (DRoA). The DRoA value assesses the risk of cascading effects and determines their impact on SAs and connected PAs. The introduction of the DRoA metric allows for a more nuanced assessment of risks, revealing that traditional risk management approaches may underestimate the true extent of vulnerabilities.

As soon as the DRoA on each PA is assessed, it will be possible to define:

- The value associated to the direct and indirect consequences on the organisation’s PAs and SAs.
- The attack-related costs associated to the fact of being a victim of a successful cyberattack.

The proposed approach allows stakeholders to broaden the scope and awareness of their risk assessment to other areas outside their control (and potentially with contrasting interests) and discover hidden costs and liabilities.

To support this statement with an example, as described in [31], a cyberattack that degrades the Controller-pilot data link communications (CPDLC) service can generate all types of SecRAM impacts (except safety) on various stakeholders (sometimes with contrasting interests):

- ANSPs – Air Navigation Service Providers, e.g. *capacity* (revert to voice communication that implies increased separation in specific circumstances), *regulatory* (liability/accountability due to capacity reduction) and *economic* impact (increased insurance premiums according to ATM/ANS.OR.D.020 of EU Reg. 2017/373).
- Airlines, e.g. *capacity* (delayed/cancelled flights), *economic* impact (delayed/cancelled flights can generate extra airport costs, night ban breach costs, extra crew costs, passengers’ compensation).
- Airports, e.g. *capacity* (airport congestion) and *economic* impact (airport congestion costs).
- Passengers, e.g. *economic* impact (business losses and extra personal costs).

F. Dynamic risk assessment

The fifth KR from the SEC-AIRSPACE project is a method for dynamically assessing security risks in ATM systems. The method uses threat models representing the ATM scenarios and translates these into multi-attribute decision tree algorithms. The method takes the SAs and their associated vulnerabilities and threats identified in the security risk assessment as a starting point. These are then used to create models of the relationships between threat sources, threat scenarios, vulnerabilities, unwanted incidents, and impacted assets. This modelling phase will capture both the logical flow of attack paths and the cascading nature of incidents within the ATM infrastructure.

TABLE II. VALIDATION OBJECTIVES AND SUCCESS CRITERIA

Title	Validation objective	Success Criterion		
		#1	#2	#3
Validation of the taxonomy.	Taxonomy represents relevant elements at risk in the ATM supply chain and can be applied in a structured CRA ² .	Stakeholders confirm that taxonomy represents relevant elements at risk in the ATM supply chain.	Stakeholders confirm that taxonomy can be applied in a structured CRA.	N/A
Identification of emerging cyber threats and vulnerabilities.	Updated RAM ³ allows to identify emerging cyber threats and vulnerabilities in ATM systems.	Stakeholders confirm that updated RAM allows to identify relevant emerging cyber threats in their ATM systems.	Stakeholders confirm that updated RAM allows to identify relevant emerging cyber vulnerabilities in their ATM systems.	N/A
Detection of cascading effects.	Updated RAM allows to detect potential cascading effects in ATM systems.	Stakeholders confirm that updated RAM allows to detect potential cascading effects in their ATM systems.	N/A	N/A
Consideration of human, procedural and organizational aspects for recommended security controls.	Recommended security controls consider human, procedural and organizational aspects.	Stakeholders confirm that recommended security controls consider human aspects.	Stakeholders confirm that recommended security controls consider procedural aspects.	Stakeholders confirm that recommended security controls consider organizational aspects.
Usefulness of the web-based tool for CRA.	Web-based tool is a useful tool for CRA	Stakeholders perceive web-based tool as useful tool for CRA.	N/A	N/A
Usability of the web-based tool for CRA.	Web-based tool is a usable tool for CRA.	Stakeholders perceive web-based tool as usable tool for CRA.	N/A	N/A
Trust in the web-based tool for CRA.	Stakeholders trust in web-based tool process and results for CRA.	Stakeholders trust the web-based tool process for CRA.	Stakeholders trust the web-based tool results for CRA.	N/A

For each threat scenario, risk indicators are identified that provide measurable input for risk evaluation. These indicators can come from expert knowledge, test results, and network/application layer monitoring. They are connected to the threat model to represent real-time or contextual evidence influencing likelihood or consequence of each threat scenario. The threat models and risk indicators are translated into multi-attribute decision tree algorithms, where each leaf node represents a risk indicator, and internal nodes model conditional logic for assessing the likelihood or consequence of a threat path. As indicator values change (e.g., from expert input or through the monitoring systems), the model propagates updated values throughout the decision tree. This results in a recalculated risk level for each threat scenario or impacted asset. This results in a dynamic output, supporting operational awareness and proactive mitigation planning.

This method aims to enhance the capacity of ATM operators and stakeholders to monitor and react to evolving cyber threats in a context-aware and evidence-based manner. The method is described in more detail in the project deliverable D1.2 [32], which also includes examples of how it can be applied.

G. Web-based tool SecRAM Navigator

SecRAM Navigator is a tool (KR 1.6), designed to utilize the improved SecRAM. The web-based interface simplifies the processes of identifying, analyzing, and evaluating potential cybersecurity threats and vulnerabilities (Fig. 5).

Key functionalities of the SecRAM Navigator include:

- Structured risk assessment workflow: Seamless guidance through the risk assessment process – from scope definition and asset identification to

vulnerability assessment, threat evaluation, security controls implementation, and residual risk analysis.

- Comprehensive asset catalogs: Access to centralized and carefully curated catalogs of PA and SA, Controls, Threats, and Vulnerabilities. Users can quickly locate and integrate these pre-defined elements into their assessments, streamlining the overall process. If needed, new items can be defined.
- Integration of human factors: The embedded Human Aspects of Information Security Questionnaire (HAIS-Q) [33], [34] feature enhances risk assessments by incorporating crucial insights on organizational behavior and employee perceptions related to cybersecurity, allowing for a more holistic and effective management strategy.
- Multi-tenant architecture with data isolation: Ensuring data security and confidentiality, each user or organization accessing the tool benefits from a dedicated isolated database. This supports secure storage and handling of sensitive data.
- User-friendly interface (Fig. 5): SecRAM Navigator features an intuitive interface, enabling users to conduct assessments efficiently and effectively. Visualization of risk assessment steps and outcomes facilitates informed decision-making and strategic planning, including strategies for risk mitigations.
- Cascading effects analysis: This capability allows users to determine potential chain reactions and broader impacts of cyber threats across interconnected organizational assets.

² Cybersecurity Risk Assessment

³ Risk Assessment Methodology

V. VALIDATIONS

Following the European Operational Concept Validation Methodology (E-OCVM) [35], a “*validation is an iterative process by which the fitness for purpose of a new system or operational concept being developed is established. The E-OCVM focuses on providing evidence that the concept is ‘fit for purpose’ and answers the question, ‘Are we building the right system?’*”. SEC-AIRSPACE implemented two specific use cases to validate the research question. These were utilized to validate the improved methodology, while the SecRAM Navigator was used as the platform to validate the updated catalogs and all project KRs implemented as tool’s functionalities.

The first use case involves an ATM scenario including Trajectory-Based Operations (TBO) with a focus on the end-to-end data flow between aircraft and ground systems. The second use case encompasses the concept of virtualization (e.g., Virtual Centers; VC) and dynamization of air traffic services by decoupling ATM data services, such as flight data, radar, and weather information, from the physical Controller Working Position (CWP).

A. Validation Exercise

The KRs outlined in section IV were validated during a final validation activity in May 2025. The entire validation exercise consisted of three validation activities. The first two activities collected feedback from SESAR security champions and the project consortium. These were used to enhance the methodology and the tool further. The third and last activity was an online session, attended by 19 external stakeholders from the ATM domain. To prepare for the validation exercise, the first four KRs were integrated into the tool (the sixth KR). This tool was used to gather qualitative feedback from the stakeholders on both the tool itself, as well as on the updated methodology that is implemented in the tool. To validate the KRs, some validation objectives were defined (TABLE II.).

The participants were split into three groups in separate breakout rooms. In each group there was a one user actively assessing the tool, while others were observers. Based on the involvement these users can therefore be further sub-divided (*direct*, as a main assessor or *indirect*, providing specific expertise to the main assessor) and the type of their role within ATM (operational or non-operational staff). Primary users are cybersecurity experts and aviation safety professionals. The latter were expected to provide insights into the effects of cybersecurity risk impacts on safety, especially for the critical operational environment. Secondary users, such as air traffic controllers, airline and airport operators, and external stakeholders, were expected to provide further insights into the operational impacts, passenger safety and overall operational resilience. The participants followed the guided risk assessment process of SEC-AIRSPACE in the validation activity. The users were instructed to apply the seven-step methodology (Fig. 4) to the previously described scenarios.

A structured questionnaire was provided to assess participants' experience with the improved security risk assessment methodology aided by the SecRAM Navigator tool. The evaluation of the validation allowed detection of the achievement of the success criteria (TABLE II.). The results will be the input for further developments of the enhanced SecRAM and the used tool.

Validation outcomes confirm the feasibility, usability and usefulness of the SecRAM 2.0 methodology and its steps, to

be applied to realistic ATM cybersecurity assessments, as reported by stakeholders. The tool and implemented methodology allow for scoping of systems, identification of primary and supporting assets, impact assessment, mapping of threats, vulnerabilities and controls. While the cascading effect part remains only partially implemented, its baseline concept was validated. The step-by-step workflow and overall design were well received and considered user-friendly.

Following these results, the tool can be rated as technically feasible but not yet mature for deployment. It was confirmed by the end-users, that the degree of development exceeds the expectations for the initially aimed low maturity level.

VI. DISCUSSION OF PROPOSED ENHANCEMENTS

A. The Aviation Organisation Employee’s view

The update to SecRAM brings several benefits to aviation organizations. The availability of the methodology through the SecRAM Navigator eases the assessment fundamentally. The changes allow employees to stay informed about the current security posture and they enable quick and efficient updates of risk assessments. Furthermore, the employees can be provided with specific training targeting the identified risks while they already can collaborate more efficiently with colleagues to counter the specific risks. The improved methodology provides a more comprehensive approach to security risk assessment and by adopting the improved methodology, the organization's supply chain security can be improved as well. This, in turn, increases opportunities for automation and innovation and furthermore contribute to an improved culture of cyber- as well as physical security.

B. Threats to validity

However, in the underlying study, several validity threats were identified. Internally, selection bias and recent events, which the validation stakeholders may have experienced could have influenced feedback. Externally, small sample size and specific scope of the use cases may limit the possibility to generalize the findings. Additionally, stakeholders might have altered their behavior based on expectations inherited from colleagues, and researchers could unintentionally have influenced responses. The developed and tested prototype for security risk assessment in ATM adds another layer of complexity to the project work. The same validity threats, such as selection bias and external events might have influenced the prototype’s performance.

VII. CONCLUSIONS

The SecRAM assessment methodology has been significantly improved with integrated and expandable databases, simplifying the entire process, while maintaining its effectiveness. A new intuitive web-based tool enhances transparency, taking the proven methodology for security risk assessment (SecRAM) to the next level. Validation was conducted by a carefully selected group of experienced security experts.

With the applied changes to the methodology SecRAM is now enabled to consider cascading effects, which allows to project the risk assessment along a chain of connected assets. Furthermore, the first steps have been taken to establish a dynamic risk evaluation within the SecRAM.

Future work will prioritize integrating automation and Artificial Intelligence (AI) into the risk assessment to enhance efficiency and accuracy. With proven feasibility and

effectiveness, SecRAM will likely gain broader adoption, and its adaptation will be key to addressing new threats.

ACKNOWLEDGMENT

This project has received funding from the SESAR Joint Undertaking under the European Union’s Horizon Europe research and innovation programme under grant agreement No 101114635. The authors would like to thank all SEC-AIRSPACE consortium members that contributed to this paper through stimulating discussions around the concepts presented.

This work was partly conducted using Protégé [25].

REFERENCES

- [1] P. S. Evangelist Product, “Top 10 Automated Risk Assessment Tools in 2025.” Accessed: May 05, 2025. [Online]. Available: <https://www.flowforma.com/blog/automated-risk-assessment-tools>
- [2] M. Le Fevre, B. Gözl, R. Flohr, T. Stelkens-Kobsch, and T. Verhoogt, “SecRAM 2.0 Security Risk Assessment Methodology for SESAR 2020; 02.00. 00 SESAR Joint Undertaking: Brussels.” SESAR JU, Sep. 25, 2017. [Online]. Available: <https://www.sesarju.eu/sites/default/files/documents/transversal/SESAR%202020%20-%20Security%20Reference%20Material%20Guidance.pdf>
- [3] “Airliner hijackings and deaths in them,” Our World in Data. Accessed: Apr. 15, 2025. [Online]. Available: <https://ourworldindata.org/grapher/airliner-hijackings-and-fatalities-from-them>
- [4] B. A. Jackson, D. R. Frelinger, T. LaTourrette, E. W. Chan, R. Lundberg, and A. R. Morral, “The Problem to Be Solved: Aviation Terrorism Risk Past, Present, and Future,” in *Efficient Aviation Security*, in Strengthening the Analytic Foundation for Making Air Transportation Security Decisions. , RAND Corporation, 2012, pp. 11–42. Accessed: Apr. 15, 2025. [Online]. Available: <https://www.jstor.org/stable/10.7249/j.ctt3fgzr.10>
- [5] International Civil Aviation Organization, *Safety management manual (SMM)*, 3. ed. in Doc [Englische Ausgabe], no. 9859,3. Montreal: ICAO, 2013.
- [6] “FAA_Order_8040.4C.” Accessed: Apr. 30, 2025. [Online]. Available: https://www.faa.gov/documentLibrary/media/Order/FAA_Order_8040.4C.pdf
- [7] “Safety Management System and Management System — the integrated approach | EASA.” Accessed: Apr. 30, 2025. [Online]. Available: <https://www.easa.europa.eu/en/domains/safety-management/safety-management-system-sms>
- [8] “ISO/IEC 27005:2022,” ISO. Accessed: Apr. 15, 2025. [Online]. Available: <https://www.iso.org/standard/80585.html>
- [9] “SESAR Joint Undertaking | Delivering the Digital European Sky.” Accessed: Apr. 15, 2025. [Online]. Available: <https://www.sesarju.eu/>
- [10] “Annex 17 - Aviation Security.” Accessed: Apr. 15, 2025. [Online]. Available: <https://www.icao.int/security/sfp/pages/annex17.aspx>
- [11] “Aviation Security Manual (Doc 8973 – Restricted).” Accessed: Apr. 15, 2025. [Online]. Available: <https://www.icao.int/security/sfp/pages/securitymanual.aspx>
- [12] *Civil/military cooperation in air traffic management*. in ICAO cir, no. 330-AN/189. Montréal: International Civil Aviation Organization, 2011.
- [13] “Air Traffic Management Security Manual (Doc 9985 - Restricted),” ICAO. Accessed: Apr. 15, 2025. [Online]. Available: <https://store.icao.int/en/air-traffic-management-security-manual-doc-9985-restricted>
- [14] “ECAC-Doc 30_Part I Facilitation 13th edition 13 Dec 2023.” Accessed: Apr. 15, 2025. [Online]. Available: https://www.ecac-ceac.org/images/activities/facilitation/ECAC-Doc_30_Part_I_Facilitation_13th_edition_13_Dec_2023.pdf
- [15] SESAR Joint Undertaking and United States, Eds., *NextGen - SESAR: state of harmonisation*, Third edition. Luxembourg: Publications Office, 2018. doi: 10.2829/90536.
- [16] National Institute of Standards and Technology, “The NIST Cybersecurity Framework (CSF) 2.0,” National Institute of Standards and Technology, Gaithersburg, MD, NIST CSWP 29, Feb. 2024. doi: 10.6028/NIST.CSWP.29.
- [17] C. J. Alberts, S. G. Behrens, R. D. Pethia, and W. R. Wilson, “Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework, Version 1.0.,” Defense Technical Information Center, Fort Belvoir, VA, Jun. 1999. doi: 10.21236/ADA367718.
- [18] “OWASP Risk Assessment Framework | OWASP Foundation.” Accessed: Apr. 15, 2025. [Online]. Available: <https://owasp.org/www-project-risk-assessment-framework/>
- [19] K. Freeman and S. W. Garcia, “Implementing the Infosec Color Wheel into an Urban Air Mobility Software and System Development Lifecycle”.
- [20] “Cybersecurity Risk Assessment According to ISA/IEC 62443-3-2.” Accessed: May 05, 2025. [Online]. Available: <https://gca.isa.org/blog/cybersecurity-risk-assessment-according-to-isa-iec-62443-3-2>
- [21] “16.02-D04-011_ATM_Security_Final+Project+Report_00.01.00.” Accessed: Apr. 23, 2025. [Online]. Available: https://innaxis-comm.s3.eu-central-1.amazonaws.com/ENGAGE/WIKI/DELIVERABLES/SESAR1/16.02-D04-011_ATM_Security_Final+Project+Report_00.01.00.pdf
- [22] “PJ19_D1.2_Final_Project_Report.” Accessed: Apr. 23, 2025. [Online]. Available: https://www.sesarju.eu/sites/default/files/documents/projects/FPR/PJ19_D1.2_Final_Project_Report.pdf
- [23] K. Bernsmed, G. Bour, M. Lundgren, and E. Bergström, “An evaluation of practitioners’ perceptions of a security risk assessment methodology in air traffic management projects,” *Journal of Air Transport Management*, vol. 102, p. 102223, Jul. 2022, doi: 10.1016/j.jairtraman.2022.102223.
- [24] K. Weaver, “Pragmatic Paradigm,” in *The SAGE Encyclopedia of Educational Research, Measurement, and Evaluation*, SAGE Publications, Inc., 2018, pp. 1287–1288. doi: 10.4135/9781506326139.
- [25] M. A. Musen, “The Protégé Project: A Look Back and a Look Forward,” *AI Matters*, vol. 1, no. 4, pp. 4–12, Jun. 2015, doi: 10.1145/2757001.2757003.
- [26] “European ATM Master Plan portal (eATM Portal) | EUROCONTROL.” Accessed: Apr. 29, 2025. [Online]. Available: <https://www.eurocontrol.int/portal/european-atm-master-plan-portal>
- [27] R. Keller, “The NASA Air Traffic Management Ontology,” The NASA Air Traffic Management Ontology (atmonto). Accessed: May 02, 2024. [Online]. Available: <https://data.nasa.gov/ontologies/atmonto/>
- [28] “Home | AIRM.aero.” Accessed: Apr. 29, 2025. [Online]. Available: <https://airm.aero/>
- [29] Stelkens-Kobsch Tim H. *et al.*, “Towards Cybersecurity Risk Assessment for Future ATM – First Steps,” in *2024 AIAA DATC/IEEE 43rd Digital Avionics Systems Conference (DASC)*, Sep. 2024, pp. 1–8. doi: 10.1109/DASC62030.2024.10748983.
- [30] P. Kotzanikolaou, M. Theoharidou, and D. Gritzalis, “Cascading Effects of Common-Cause Failures in Critical Infrastructures,” in *Critical Infrastructure Protection VII*, vol. 417, J. Butts and S. Sheno, Eds., in IFIP Advances in Information and Communication Technology, vol. 417. , Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 171–182. doi: 10.1007/978-3-642-45330-4_12.
- [31] C. Dambra, S. Boonsong, K. Bernsmed, P. H. Meland, and T. H. Stelkens-Kobsch, “Modelling and analysing cascading effects of cyberattacks to ATM Systems,” presented at the 25th Integrated Communications Navigation and Surveillance Conference (ICNS), Brussels, Belgium, in press.
- [32] SEC-AIRSPACE consortium, “D1.2 - Concept Outline Holistic and dynamic security risk assessment for the ATM domain.” in press.
- [33] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, “Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q),” *Computers & Security*, vol. 42, pp. 165–176, May 2014, doi: 10.1016/j.cose.2013.12.003.
- [34] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, “The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies,” *Computers & Security*, vol. 66, pp. 40–51, May 2017, doi: 10.1016/j.cose.2017.01.004.
- [35] “European Operational Concept Validation Methodology (EOCVM) | EUROCONTROL.” Accessed: Apr. 24, 2025. [Online]. Available: <https://www.eurocontrol.int/publication/european-operational-concept-validation-methodology-eocvm>