

AI IN AVIATION CYBERSECURITY RISK ASSESSMENT: OPPORTUNITIES AND CHALLENGES

Raffaele Elia[1], Pierre Bieber[2], Domenico Pascarella[3], Massimiliano Rak[4] & Carsten Döll[2]

[1]University of Campania Luigi Vanvitelli
[2]ONERA, Université de Toulouse, 31000, Toulouse, France
[3]CIRA (Italian Aerospace Research Centre)
[4]University of Naples Federico II

Abstract

A literature survey about the use of AI to support cybersecurity risk assessment was conducted within GARTEUR Aviation Security group. The paper reports the main findings, it identifies opportunities where it was already established that AI can efficiently support risk assessment and challenges where research activities are still needed.

Keywords: Cybersecurity, Safety, Risk Assessment

1. Introduction

The pervasive integration of Information Technologies in aircraft, air traffic management, maintenance, airport and airline systems is making the aeronautical domain increasingly automated. But this integration significantly extends the attack surface available for malicious agents, thus paving the way for exploiting existing and emerging threats in order to attack the aeronautical domain. Recent events [1] confirmed that cyber-attacks can compromise the integrity and availability of the aviation transport system, causing disruptions that can lead to economic and financial losses, as well as threats to citizen safety and privacy. Consequently, aviation authorities such as EASA have mandated [2] the application of security risk assessment during the early stages of the development of aeronautical systems. Indeed, adopting a security-by-design approach should ensure proactive, efficient, and effective risk management, thereby safeguarding citizens, the environment, and critical infrastructures.

However, traditional assessment approaches are typically manually performed, which makes them impractical in this highly automated, interconnected, and distributed domain. In addition, such assessments are time-consuming, prone to errors, and susceptible to subjective interpretation. As a result, GARTEUR [3] Aviation Security group launched an exploratory project in order to investigate methods that automate risk assessment. The first step of this project was to conduct a comprehensive systematic literature review in order to answer to the Research Question: *Can Artificial Intelligence (AI) support the automation of cybersecurity risk assessment within the aeronautical domain?* The main contribution of this paper is a rather positive answer to this question.

The remainder of this paper is organized as follows. Section 2. introduces the main steps of cybersecurity risk assessment. Section 3. summarizes the methodology of the systematic literature search. Section 4. presents areas where AI can efficiently support risk assessment as well as research challenges.

2. Security Risk Assessment within Aeronautical Domain

Cybersecurity aims to safeguard hardware and software resources, as well as data, against intentional and malicious attacks that may compromise one or more CIA (Confidentiality, Integrity, and Availability) properties that a system should satisfy.

The ED-203A [4] standard defines the main steps of a security risk assessment that would comply with EASA regulations. The first step defines the security perimeter to be protected, this perimeter includes primary assets (e.g. applications and communications) and supporting assets (e.g. software and hardware implementing applications and communications) that are the target of attacks. The following step evaluates the impact of a threat condition, e.g. the compromise of CIA properties of an asset, on safety and other aspects such as operation success. Then, vulnerabilities affecting supporting assets are identified, thereby establishing the complete set of threat scenarios leading to threat conditions. Finally, the security risk level for each threat scenario must be assessed as the combination of its impact and its likelihood. ED-203A defines acceptable risk levels with respect to safety impacts. For all non-acceptable risks, the implementation of security controls is required to mitigate the risks, this triggers a new iteration of the risk assessment process leading to calculation of a residual risk level.

Security risk assessment is mostly performed manually. Shared data resources can alleviate the security analyst workload. The SecRAM [5] helps the security analyst by providing catalogs of predefined assets, vulnerabilities and security controls relevant in the ATM (Air Traffic Management) domain. Other general purpose databases such as CVE that collects vulnerabilities, Common Vulnerability Scoring System (CVSS) that propose an automated impact assessment and MITRE ATT&CK that collects attack patterns can also assist the security analyst. But today security risk assessment is still far from being automated.In the recent years, AI has proved to be very useful to assist software coding activities. Similarly, we thought that AI could play a key role in supporting the various stages of the assessment process. Following this direction, we conducted a comprehensive systematic literature review to identify existing AI-powered security assessment methodologies applicable to the aeronautical domain.

3. Literature Survey Method

We adopted a keyword-based approach to select relevant articles needed to answer the research question *RQ: In what ways can Artificial Intelligence (AI) support the automation of safety and security risk assessment in cyber-physical systems within aeronautical domain? RQ*. A search query SQ *SQ: (artificial intelligence) AND (cybersecurity assessment) AND (aeronautics)* was applied to search engines (e.g., Scopus) to gather articles that can help to address the *RQ*. SQ is structured so that the first part covers the various AI techniques that may be employed to support the assessment, while the last part targets the aeronautical domain. Applying SQ in Scopus returned only 79 articles with very limited contributions suitable to address *RQ*. Therefore, although our main focus lies in the aeronautical domain, we had to broaden the research query by replacing the target domain by the more general term: Cyber-Physical Systems (CPS). This was motivated by the consideration that AI-powered assessment techniques developed for CPS such as autonomous cars, medical systems or electrical power systems should also be applicable in the aeronautical sector.

Applying the revised SQ allowed to gather 248 articles, which were then reduced to 41 after the analysis of their abstracts. A vast majority of discarded articles deal with AI-powered intrusion detection and management. They describe runtime threat assessment techniques that are applicable only when the system is fully developed and deployed. Intrusion detection is clearly an area where AI can contribute to secure systems yet these approaches do not help the risk assessment tasks to be performed at early stages of the design of a system so we discarded them.

We analyzed the 41 identified papers and assessed several questions:

- Which step(s) of the risk assessment process is covered: Perimeter and Asset Definition, Threat Condition Impact Evaluation, Threat Scenario Likelihood Computation, Security Control Selection ?
- What type of AI is used: Supervised Learning, Unsupervised Learning, Reinforcement Learning, Self-Supervised Learning (Large Language Models) ?

- What type of data is used: unstructured text, database records, system models, ... ?
- How is the approach validated: numerical criteria, expert judgement ?
- To what extent the approach is automated: very partially, partially, fully ?

4. Opportunities and Challenges

Analyzing the outcomes of the literature survey, this section provides a list of opportunities and challenges related with the use of AI in order to support cybersecurity risk assessment in aviation. The papers we have reviewed report several successful application of AI to support risk assessment. We identified three main opportunities:

1. **Use Reinforcement Learning to Evaluate Threat Scenario Likelihood**. The most popular topic we found in the reviewed literature is AI-powered computation of threat scenarios. Several papers, including [6, 7], propose to use Reinforcement Learning (RL) approach to train an agent to use system model simulations in order to find optimal threat scenarios that maximize the impact and minimize the attacker effort.

2. **Use Supervised Learning to Classify Threat Condition Impact**. Another topic that is well covered by the literature is the use of AI in order to evaluate the impact of a Threat Condition. Several papers including [8, 9] propose to use Supervised Learning in order to automatically classify a threat condition and assess its impact by computing its Common Vulnerability Scoring System (CVSS) score.

3. **Use Large Language Models to Generate Threat Assessment**. A strong trend in the most recent papers is the use of LLM to support risk assessment. Papers such as [10, 11, 12, 13], have explored approaches where the analyst writes a prompt asking the LLM to perform the main steps of risk assessment with references to the available resources and descriptions of the system under study. LLMs successfully supported multiple stages of the assessment process (mainly Threat Condition Identification and Impact evaluation). Furthermore, LLMs are very good at generating documents (generally tables) in the form expected by regulations.

Although representing a step toward automation, the analyzed papers are characterized by several substantial drawbacks. We identified three main challenges related with the use of AI:

1. **Develop AI Techniques that Support the Full Scope of Threat Assessment**. The reviewed literature shows a strong imbalance in the AI support provided across the different risk assessment steps. The definition of the security perimeter, asset identification and security function selection were seldom covered by the literature. Approaches such as [12] rely on conventional system models to define the perimeter and identify assets. But, as design are quickly evolving during the early stages of design, it should be valuable to investigate AI techniques that could cope with these design evolutions.

2. **Investigate the Validation of AI-powered Threat Assessment**. It well known that AI techniques are prone to hallucinations and provide statistically probable but incorrect answers. In order to avoid insecure designs it is very important to investigate means to validate AI-powered threat assessments. Some researchers [13] started to investigate this problem by comparing human produced vs AI produced threat assessments.

3. **Ensure Availability of Shared Data Resources Relevant for Aviation Cybersecurity**. AI/Machine Learning techniques need data to provide useful results. As mentioned earlier, in the cybersecurity risk assessment domain several useful data resources are available. Besides SecRAM, these resources are not Aviation-specific and their funding might be questioned in the future. So it should be valuable to build Aviation-specific data resources for instance by extending the scope of SecRAM in order to cover all the segments of Aviation.

5. Copyright Statement

The authors confirm that they, and/or their company or organization, hold copyright on all of the original material included in this paper. The authors also confirm that they have obtained permission, from the copyright holder of any third party material included in this paper, to publish it as part of their paper. The authors confirm that they give permission, or have obtained permission from the copyright holder of this paper, for the publication and distribution of this paper as part of the ICAS proceedings or as individual off-prints from the proceedings.

References

[1] J. Jolly. Disruption continues at heathrow, brussels and berlin airports after cyber-attack. https://www.theguardian.com/business/2025/sep/21/delays-continue-at-heathrow-brussels-and-berlin-airports-after-alleged-cyber_-attack, 2025. [Online]. Accessed: 2025-12-10.

[2] EASA. Easy Access Rules for Information Security. https://www.easa.europa.eu/en/downloads/138788/en, 2025. [Online]. Accessed: 2026-01-10.

[3] GARTEUR. Group for Aeronautical Research and Technology in Europe- Annual Report. https://www.garteur.org, 2023. [Online]. Accessed: 2026-01-10.

[4] EUROCAE. ED-203A - Airworthiness Security Methods and Considerations, 2018.

[5] Miriam le Fevre, Birgit Gölz, Ruben Flohr, Tim Stelkens-Kobsch, and Theo Verhoogt. SecRAM 2.0. Security Risk Assessment methodology for SESAR 2020. September 2017.

[6] Mariam Ibrahim and Ruba Elhafiz. Security assessment of industrial control system applying reinforcement learning. *Processes*, 12(4), 2024.

[7] Aolin Ding, Matthew Chan, Amin Hass, Nils Ole Tippenhauer, Shiqing Ma, and Saman Zonouz. Get your cyber-physical tests done! data-driven vulnerability assessment of robotic aerial vehicles. In *2023 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pages 67–80, 2023.

[8] Mohamed Sayed Farghaly, Heba Kamal Aslan, and Islam Tharwat Abdel Halim. A hybrid human-ai model for enhanced automated vulnerability scoring in modern vehicle sensor systems. *Future Internet*, 17(8), 2025.

[9] Halima Ibrahim Kure, Shareeful Islam, Mustansar Ghazanfar, Asad Raza, and Maruf Pasha. Asset criticality and risk prediction for an effective cybersecurity risk management of cyber-physical system. *Neural Comput. Appl.*, 34(1):493–514, January 2022.

[10] Stefan Stein, Michael Pilgermann, Simon B. Weber, and Martin Sedlmayr. Leveraging mds2 and sbom data for llm-assisted vulnerability analysis of medical devices. *Computational and Structural Biotechnology Journal*, 28:267 – 280, 2025.

[11] Mario Werthwein, Björn Annighöfer, and Zamira Daw. Towards continuous security assessment: Integrating model-based risk assessment and large language models. pages 1–12, 04 2025.

[12] M Sabbir Salek, Mashrur Chowdhury, Muhaimin Bin Munir, Yuchen Cai, Mohammad Imtiaz Hasan, Jean-Michel Tine, Latifur Khan, and Mizanur Rahman. A large language model-supported threat modeling framework for transportation cyber-physical systems. *IEEE Access*, 13:163046–163070, 2025.

[13] Fikret Gültekin, Oscar Lilja, Ranim Khojah, Rebekka Wohlrab, Marvin Damschen, and Mazen Mohamad. Leveraging large language models for cybersecurity risk assessment – a case from forestry cyber-physical systems. 10 2025.