SEC-AIRSPACE: Addressing Cyber Security Challenges in Future Air Traffic Management

Karin Bernsmed and Per Håkon Meland
Dep. of software engineering, safety and security
SINTEF
Trondheim, Norway
{karin.bernsmed,per.h.meland}@sintef.no

Tim H. Stelkens-Kobsch
Dep. of ATM Simulation
German Aerospace Center (DLR)
Braunschweig, Germany
tim.stelkens-kobsch@dlr.de

Alessandra Tedeschi
Research and Innovation
Deep Blue srl
Rome, Italy
alessandra.tedeschi@dblue.it

Carlo Dambra and Irene Buselli
ZenaByte s.r.l.
Genova, Italy
{carlo.dambra,irene.buselli}@zenabyte.com

Enrico Frumento
Cybersecurity Research Lead
Cefriel - polytechnic of Milano
Milan, Italy
enrico.frumento@cefriel.com

Davide Martintoni and Valerio Senni
Dept. of Applied Research & Technology
Collins Aerospace
Trento and Rome, Italy
{davide.martintoni,valerio.senni}@collins.com

Andrei Gurtov and Gurjot Singh Gaba
Dep. of Computer and Information Science
Linköping University
Linköping, Sweden
{andrei.gurtov,gurjot.singh}@liu.se

Alejandro Sastre García
Technical Directorate
Skyway Air Navigation Services, S.A.
Madrid, Spain
asastre@skyway-ans.com

Supathida Boonsong
Research and Innovation
Air Navigation Services of Sweden
Norrköping, Sweden
supathida.boonsong@lfv.se

***Abstract*—Digitalisation offers many benefits to Air Traffic Management (ATM). Yet, with technological innovations come challenges in managing new cyber security threats and risks. This paper presents a comprehensive review over challenges faced in ATM when protecting critical assets, and outlines how the newly established exploratory research project SEC-AIRSPACE will address these challenges.**

Keywords-cyber security; threats; vulnerabilities; security risk assessment; Learning Analytics; Air Traffic Management; SESAR.

I. Introduction

Air Traffic Management (ATM) is a complex global infrastructure that enables a safe and efficient flow of air traffic. However, as the ATM systems become more interconnected and complex, the risks towards these systems are increasing. Emerging technologies are including a future data-sharing service delivery model, the deployment of infrastructure through a service-oriented architecture, and increased sharing of data between different actors. The new technologies required for achieving a more dynamic airspace management and ATM service provision will expose the ATM systems to new cyber security threats. In the worst-case, this can have catastrophic consequences if not properly addressed. To address these challenges, this paper briefly describes the approach of the recently established Horizon Europe project SEC-AIRSPACE [1], which aims to enable a more resilient ATM, by focusing on reducing the cyber security risks of the ATM systems and increase the awareness of the ATM stakeholders of such risks.

Section II of this paper provides a comprehensive review and discussion of challenges to cyber security in current and future ATM systems. In Section III, we present the SEC-AIRSPACE approach, which aim to address these challenges. Finally, Section IV concludes the paper.

II. Challenges

This section outlines a set of distinct challenges that the project will address.

A. Cyber security risk assessment of ATM systems

Cyber security risk assessment is nowadays *the* established approach to identify, assess, and mitigate cyber security threats in any sector that relies on digital information, data-sharing and service-oriented architectures, including critical infrastructure. Aviation, and more specifically the dynamic, integrated management of air traffic and airspace, known as ATM, is no exception. In Europe, a significant part of the Research & Development (R&D) activities in the ATM sector is performed as part of the SESAR Joint Undertaking [2]. Their cyber security strategy [3] recognises that the key to deliver secure and cyber-resilient solutions for ATM is to focus the efforts where they are most effective, and points out that security risk assessment needs to be performed already under the R&D phase, in particular when technologically complex architectures and new technologies are being introduced. The state of the art for applied risk assessment in ATM is still scattered though, as there is no "one-size-fits-all" solution for its various systems. The majority of the ATM (R&D) projects in Europe follow the Security Risk Assessment Methodology (SecRAM) [4], which has been developed and is being maintained by SESAR for many years. Similar approaches are being used in other sectors and in different contexts;

two widely used standards are ISO/IEC 27005 [5] and NIST SP 800-30 [6]. Regardless of which methodology is being applied, it is necessary to fully understand the architecture of the system and its intended operation and to understand which are the critical assets that needs protection. This is a prerequisite for a correct understanding of the cyber risks and for identifying suitable countermeasures for reducing the risk to an acceptable level. However, a recent published interview study of SecRAM practitioners [7], identified that many of them struggle in the process, in particular when trying to identify critical assets and when trying to understand what will be the relevant threats and risks for the technologies and processes that they will deliver.

Additional issues also arise when ATM systems become more complex. The SESAR 2020 cyber security strategy [3] explicitly states that security risks are to be managed by the individual R&D projects. This may be an appropriate strategy for today's ATM systems, but may become a risk in itself in the (not so distant) future, when the systems are expected to become more interconnected, with increased data sharing and realised through virtualised services where the boundaries between actors and systems become "blurred". This risk has already been recognised by key stakeholders in Europe, as documented in the report on ATM cyber security challenges published by EUROCOM [8]. A new proposal for rationalisation and harmonisation of the regulatory framework, issued by the European Union Aviation Safety Agency (EASA) and a number of aviation stakeholders in the European Strategic Coordination Platform (ESCP), therefore promotes international cooperation and harmonisation in risk management, risk information-sharing between organisations, and points out the need for more holistic risk assessment methods [9].

Charitoudi and Blyth [10] recognises that current cyber risk models need to be improved: (i) from the process point of view because the threats change very rapidly, they need efficiency to enable a continuous update of estimations, (ii) from the model point of view, consider that cyber threats are no longer limited to the IT systems, but they also include humans, and cyber-physical systems, and (iii) from the comprehensiveness point of view, failing to include both tangible and intangible assets along the entire supply chain. Systems can be attacked through the humans operating the systems, through the cyber-physical systems or through the suppliers. Further, as pointed out by the FP7 GAMMA project, "any security solution [for ATM] must consider the changes in security risk profiles due to the new security threats faced by the ATM system that can spread their negative effects; an attack to one particular node could compromise, in a very short time with domino effect, the functionality of the whole ATM system and the air transportation system" [11]. Such aspects are not sufficiently covered in SecRAM. For example, there is little or no support for identifying critical assets in virtualised environments, for analysing cascading effects of cyber-attacks, or for dynamic analysis of security risks.

Further, cyber security risk assessments are rarely performed; usually only once during the development of a system, and/or once a year when it has been deployed [12]. At the same time, the need to perform risk assessments more frequently, or ideally to be able to monitor risks dynamically has been recognised, not only in the ATM domain but also in other domains where the threat picture is constantly changing [13]. Erdogan et al. have recently published a systematic mapping study [14] providing an overview of security risk assessment approaches that use automatic support, including Artificial Intelligence (AI), to identify, estimate, and/or evaluate cyber risks. The study shows that on average, the number of papers on AI-supported security risk assessment has increased with the growth rate of 133% between 2010 and 2020. The approaches reported have mainly addressed cyber-risks related to intrusion detection, malware detection, and industrial systems. They focus mostly on identifying and/or estimating security risks and use primarily Bayesian networks and neural networks for the AI part. Nevertheless, the usage of AI for cyber-risk assessment is relatively new, particularly in the ATM community, where this research topic is still at its infancy.

B. Vulnerabilities and threats to ATM systems

The vision of the future ATM implies an increased connectivity and integration of systems and services, enabling Air Navigation Service Providers (ANSPs), airlines, airports, and future ATM data service providers to share information and access to services in new and innovative manners. This will inevitably increase the potential attack surface to the ATM systems, which have previously been "shielded" from attacks through their use of proprietary standards and isolated systems. Further, the need to increase interoperability while reducing costs imply an increased use of Commercial-Off-The-Shelf (COTS) components. It is well known that the use of COTS poses a serious risk to security when such software is integrated with other software products to create new composite services or systems-of-systems [8]. A well-known example for ATM is the introduction of the IP protocol suite in the Future Communication Infrastructure (FCI). Another issue that may increase risk in future ATM systems is the integration between different civil and military actors, and ground and space-based communication, navigation, and surveillance systems [8].

During the last decade, we have seen an increased interest in ATM security from the hacker community. For example, "white-hat" security researchers have demonstrated on several occasions that it is both easy and inexpensive to manipulate existing air-to-ground safety-related data transmission protocols [15], [16]. Already in 2014, IOActive revealed that SATCOM firmware from several different vendors contain multiple vulnerabilities, including hard-coded credentials, undocumented protocols, insecure protocols, back doors, and weak password reset mechanisms [17]. According to IOActive, these vulnerabilities may allow an attacker to take control of the air-to-ground SATCOM link, thus posing a direct threat to flight safety due to the lack of cyber security. Similar experiments have since been performed at Linköping University (LiU) in Sweden, where researchers have found weaknesses and demonstrated potential attack scenarios to both

the surveillance technology Automatic Dependent Surveillance–Broadcast (ADS-B) and to the communication protocol Controller Pilot Data Link Communications (CPDLC) [18]. To add to this, the increased occurrence of jamming of GPS-based navigation systems is having an increasingly serious effect on air traffic, in particular in the Baltic area [19]. All in all, the cyber risks and threats towards ATM systems are expected to increase.

C. Cascading effects of cyber-attacks in ATM systems

Many systems for airport and airspace management have grown historically and were never designed to be connected to complex global systems. The growing passenger and freight volumes require new systems that enable more effective operations. Furthermore, exponentially growing amounts of data provide opportunities for new business models, which can only be utilised efficiently by increasing the connections to other sectors. To advance the optimisation of airport management for the growing challenges, data and isolated systems will require more interconnection.

The progressive transition from traditional air traffic control systems to improved monitoring and communication systems in modern data networks will significantly change the safety assessment of the aviation environment [20]. However, this makes legacy systems that were rarely considered and developed from a security but rather from a safety perspective vulnerable and could provide a gateway to malicious actors. This system integration will lead to expanded supply chains in which each party is dependent on the services of their counterparts and on the interaction between ATM stakeholders, their industrial partners and the related supply chains.

In summary, as reported by Wynsma and Sulliva [21], "*The security of the supply chain within aviation poses a great risk as it allows multiple points for malicious actors to subvert the activities of an organisation or its products. Attacks can impact both electronic components as well as data and non-electronic components such as structural items. Thus, supply chain security can appear to be an indistinct problem in comparison to securing systems in operation – whether these are enterprise systems, servers or electronic components installed on aircraft. The view of supply chain should consider more than just the operational systems but instead include all systems that are used to support the products and operations*". As highlighted by Haan [11], two challenges have received insufficient attention: ATM architectures and their supply chains. Therefore, by assessing and understanding the ATM architecture, its components and the related vendors, ATM supply chain security can become a crucial part of a cyber risk assessment, allowing practitioners to identify possible cascading effects, implement appropriate measures and build trust.

D. Security controls for mitigating threats to ATM systems

Cyber security in aviation is explicitly addressed in the ICAO Standards and Recommended Practices Annex 17 [22], which in Europe has been implemented in the Common Requirements Regulation in the form of requirements for ANSPs. Since the ANSPs are considered to be "providers of essential services", they also need to comply with the NIS2 Directive [23] and the Cybersecurity Act [24]. The regulatory framework is complex, but, as explained in EUROCONTROL's report on ATM cyber security, it "forces operators to adopt a broad-based, holistic approach to security, addressing people, processes, and technology" [8].

For the ATM organisations that apply SecRAM to manage their security-related risks, the mitigation strategies for managing high- and medium level risks are usually selected from the SESAR Minimum Set of Security Controls (MSSC) [25]. As discovered in the study by Bernsmed et al. [7], this approach is problematic, since the MSSC is based on the ISO/IEC 27002 standard, which implies that it contains high-level security controls for *information systems*, which in turn could cause conflicts with *safety* if proper care is not taken when the security controls are implemented and deployed in the ATM systems. Further, as shown in the paper by Bernsmed, Jaatun and Meland [26], there is no guidance material available on how to ensure that subcontractors implement the necessary security controls. This is particularly concerning in the aviation domain where there are few, if any, obligations on 3rd party software providers to deliver secure software, not even when their software is integrated into safety-critical systems.

E. Personalised cyber security training and awareness for ATM organisations

Resilience requires a holistic approach to cyber security, which includes not only reducing risk through technical security controls, but to also include the social, human and organisation factors when protecting the systems. It is well known that humans can be a significant source of cyber risk. A newly released report by the World Economic Forum shows that 95% of cyber security incidents occur due to human errors [27]. Similarly, a recent study performed by the Boston Consultancy showed that of 50 major data breaches, only 23% were caused by inadequate security technology and that in most cases (77%) the breach was the result of an organizational failure, a process failure, or a human error [28]. These findings are relevant for all IT-enabled sectors, including ATM, because, as shown by Frumento et al. [29], humans are a significance source of cyber risk in any business context they operate. Many cyber security attacks therefore target humans, by exploiting their lack of training or awareness. Hence, human interventions with technology is a crucial element in both attack and defence strategies. Inducted errors (e.g., convincing people to do something they should not do using social engineering tactics) or mistakes (e.g., underestimating a threat or not blocking a website) are common examples. No IT-enabled sector is safe. For this reason, cyber security technology nowadays utilizes automation, AI systems, and logic to assist or even remove humans from the loop. However, there is one category of security defence where this is not possible and which is at the same time not evolving at a similar pace compared to other cyber security areas: training. With an unprecedented number

of employees working in hybrid or fully remote environments, such as in virtualised centres [30], there has never been a more critical time to effectively create and maintain a cyber-secure ATM workforce and an engaged security culture. Today, training and awareness campaigns are already performed with the purpose to reduce severe cyber risk. However, the evolution of training methodologies is not proceeding as desired. Often, the best option is still to train people in traditional ways, through courses, classes, and training tracks. This approach has two problems: first, the lessons are often loosely tied to current cyber risk and the critical assets at stake: second, the tangible impact on risk reduction is hard to measure and the Return of Training Investment (ROTI) is uncertain. In other words, the problem is to monitor how people's skills and awareness evolve and to measure the impact on ROTI and the corresponding cyber risk reduction. At professional level, there is a lack of accessible tools for continuous awareness, training, and skills development on cyber security aspects [31].

In ATM, simulation of real air traffic scenarios is part of the practical training for both pilots and air traffic controllers. However, it is very rare that cyber security threats are included in the exercises. As shown by Strohmeier et al. [32], neither pilot nor air traffic controllers are prepared to handle cyber-attacks, and many of them are not even aware that commonly used communication protocols, such as CPDLC, lack integrity and authenticity protection. Similar results have been shown by researchers at LiU, who have developed a tool for simulating ADS-B and CPDLC attacks and used it to demonstrate and evaluate how air traffic controllers react to such attacks [33].

III. The way forward: The SEC-AIRSPACE approach

To address the challenges identified in the previous section, the SEC-AIRSPACE project has formulated the following objectives: 1) improving the cyber security risk management of existing and future ATM systems, and 2) increasing the cyber security awareness and maturity amongst the ATM stakeholders. The overall ambition and long-term vision is to enable a more cyber-resilient ATM, focusing on reducing the risks of virtualisation and increased data-sharing between all components of the ATM infrastructure and the relevant stakeholders.

A. Improving ATM cyber security risk management

SEC-AIRSPACE will enhance the existing methodologies and the good practices currently adopted in ATM with prominent building blocks for cyber security risk management. Our baseline will be the typical steps that one may find in most cyber security risk assessment methodologies, including but not limited to ISO/IEC 27005 and SecRAM. The intention is 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.

First, SEC-AIRSPACE will deliver a taxonomy for modelling the elements of future ATM systems. The taxonomy will be based on a holistic vocabulary that facilitates the representation of the complete ATM supply chain, including

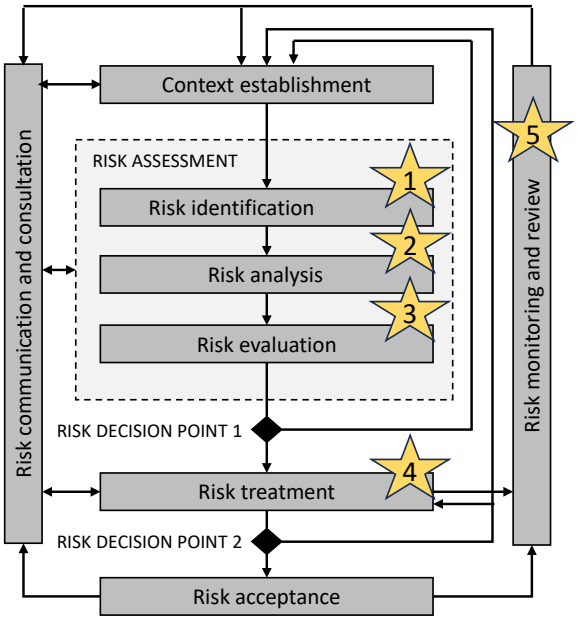

Figure 1. Overview over the key contributions for improving established security risk management processes (figure adapted from ISO/IEC 27005 [5]).

tangible and intangible assets and human, procedural and organisational aspects. It will also support the representation of risks related to complex systems-of-systems and service-oriented architectures, the use of virtualized elements, and interfaces for data sharing between ATM actors. The ambition is to facilitate better and more accurate cyber risk assessment of complex ATM systems and, in a later step, also help analysing the potential impacts of cyber-attacks with cascading effects. As illustrated by the first golden star in Figure 1, the taxonomy will support the context establishment phase of the security risk assessment, where the identification of critical assets at risk is one of the main outputs.

Second, to be able to combat cyber threats, modern cyber security risk management life-cycles must be holistic, meaning they need to consider all the possible sources of risks, including those arising from the integration of IT systems with cyber-physical and control systems, and from humans. Indeed, some security issues are generated by human malicious intents or errors and should therefore be modelled considering the interactions among people, organizations, and the technologies they use [34]. Moreover, a comprehensive cyber risk assessment should include any type of asset at risk. For example, the recent EU project HERMENEUT [35] demonstrated that intangible assets, e.g., brand, reputation and human capital are crucial elements. Another recent EU project DOGANA [36] studied a cyber risk estimation methodology for human-related risks derived from social engineering. However, integrated and holistic cyber risk models and life-cycle are still rarely used, and SecRAM is no exception. SEC-AIRSPACE will deliver guidelines to identify vulnerabilities and weaknesses of the considered ATM systems, including human, procedural and organisational factors. This will enable the ATM security risk

assessment practitioners to create a holistic picture of the cyber threat landscape and identify and analyse relevant risks (second golden star in Figure 1).

Third, in the highly interconnected ATM world, virtualisation among the systems within this world, cascading effects, i.e., secondary consequences of an attack on other organizations and/or sectors become an emerging issue. SEC-AIRSPACE will review established approaches to prevent such events and provide a novel analysis of identification, correlation, and mitigation mechanisms. The main contribution will be a model for analysing dependencies between different ATM system components, and between ATM systems and other (critical) infrastructures. As illustrated by the third golden star in Figure 1, the output will support the risk analysis and evaluation phases of the security risk assessment process.

Fourth, once cyber security risks are identified, specific security controls must be applied to reduce the risks to an acceptable level. SEC-AIRSPACE will provide a new set of "recommended security controls" for ATM, to mitigate the threats identified in the earlier steps (fourth golden star in Figure 1). These security controls will be based on existing best practices, such as the ISO/IEC 27002 standard [37] and the SESAR Minimum Set of Security Controls (MSSC) [25], but adapted to the needs of the future ATM systems. SEC-AIRSPACE will also analyse the cyber-related human factors and organisational aspects in the ATM supply chain to identify key areas where mitigations, such as training and awareness, redesign of tools and procedures, and increasing engagement of operators can be more effective. The recommended security controls will be tagged with cost indicators to help the risk analyst prioritise different mitigation strategies. Special care will be taken to avoid conflicts between safety and security, which otherwise tend to occur when IT security specialists formulate requirements on safety critical systems [38].

Finally, SEC-AIRSPACE will improve the reviewing and monitoring of the risks, by providing a method for dynamic monitoring and assessment of risks, which will be specially crafted for ATM (fifth golden star in Figure 1). The method will use the data models of the ATM systems as input and schematically translate these into risk assessment algorithms, which will be connected to risk indicators to dynamically measure and visualize the current level of risk.

B. Increasing cyber security awareness and maturity

To increase the cyber security awareness and maturity amongst the ATM stakeholders, the SEC-AIRSPACE project will utilize a cutting-edge application of the general concept of People Analytics (PA) [39], [40], applied to cyber risk mitigation. PA is originally a human resources analytics approach for managing people at work, which has been successfully used in many different settings to develop data-driven insights to improve workforce processes and promote employee experiences. The hypothesis in SEC-AIRSPACE is that PA can also be successfully used to increase cyber security awareness while keeping training costs at a minimum. The intention is to deliver contextualised and personalised cyber security training, by integrating analytics and visualization techniques to support the reduction of human-related cyber risks. The project will first apply the core concepts of PA to Learning Analytics [41], and then take the results further to generate Learning Analytics for cyber security. This means generating the most appropriate cyber security awareness recipe, i.e., *what to teach, to whom and how*, with the goal of developing and growing the ATM organisations' cyber security culture based on their current exposure to cyber risk. Awareness and training will then become a tool to reduce human-related cyber risks. An overview of the key elements in the application of PA in the SEC-AIRSPACE project is provided in Figure 2. As can be seen, the output of this research activity will be training suggestions for groups of employees, such as air traffic controllers, selected from the available catalogue of courses in the ATM organisation and specifically targeted for protecting the organisation's assets at risk. These can then be delivered as recommendations to (other) organisations providing the training.

C. Project use cases

The SEC-AIRSPACE use cases serve multiple purposes. First, they will be used to establish the context and the baseline for the research activities outlined in Section III-A and III-B. Then, they will be used to validate the key results from this research. Finally, the use cases will be utilized in the demonstration, exploitation, and communication of the project results.

In the first use case, we will investigate the end-to-end data flow between air traffic controllers and pilots in a future scenario of 4D trajectory-based operations [42], where voice instructions are replaced by digital messaging utilizing existing, publicly available, IP-based communication infrastructures. Here, CPDLC clearances will be sent in advance of horizontal, vertical and longitudinal trajectory changes, thereby enabling an optimal path for the airborne aircraft. In the second use case, we will analyse a conceptual architecture of a virtual centre. The virtual centre will be built upon a number of elements, including System-Wide Information Management (SWIM) principles of data exchange protocols and open service-oriented architectures.

The two use cases have been carefully selected; they are both scenarios that illustrate evolving ATM scenarios with digital infrastructures and services provisioning, with associated cyber security threats and risks, and they are both in line with the vision of the development of ATM in the coming decade, as outlined in the SESAR Strategic Research and Innovation Agenda for the Digital European Sky [3]. Needless to say, cyber security is a hot topic of interest in both these use cases.

IV. Conclusion

The ATM world is becoming more complex. As outlined in this paper, the introduction of new actors, new services, integrated technologies, virtualization, and increased data sharing will expose ATM systems and their critical assets to new cyber threats and risks. To efficiently protect aviation

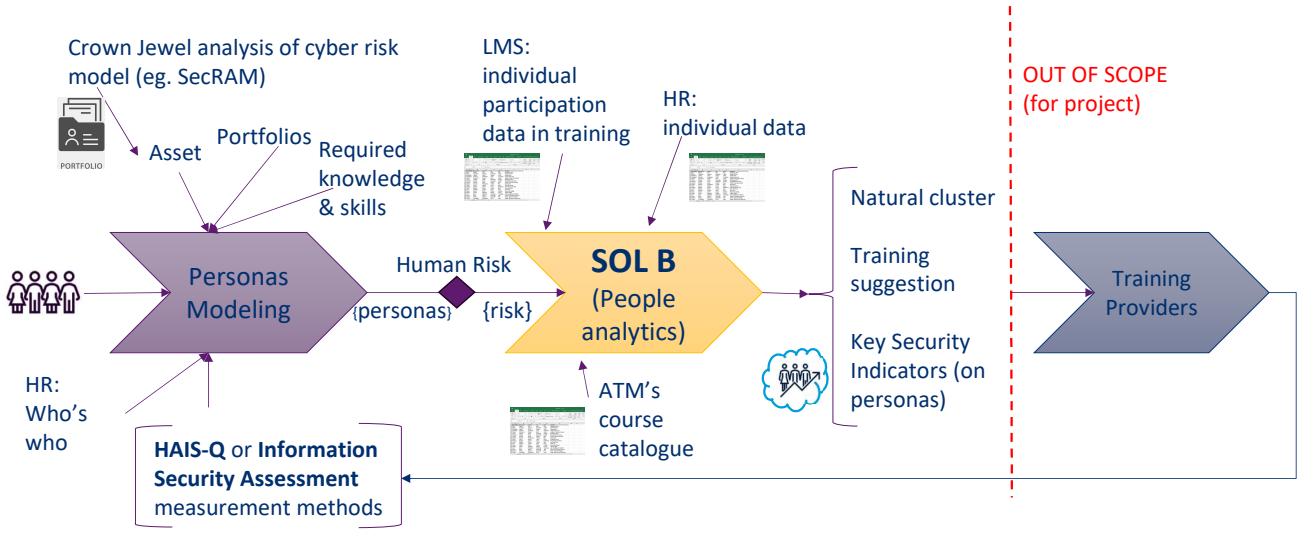

Figure 2. Overview over the key elements in the application of People Analytics.

systems, operators must perform security risk assessments and implement security controls to mitigate the identified risks. However, technology, in the form of security controls will not be enough to combat the threats. When defences are compromised, operators must detect these breaches, alert personnel, contain the effects of the breaches, and identify recovery and mitigation actions based on contingency plans. Cyber resilience hence requires a holistic view of security risk assessment, which also includes increased focus on awareness and training for the humans operating these systems.

The main impact of the SEC-AIRSPACE project will be increased cyber resilience; our system-wide holistic approach to cyber security risk management means that cyber-attacks will be more likely to be identified (and mitigated) at an early stage. In the longer term, the project results will contribute to a continued safe delivery of ATM services, despite eventual cyber-attacks and unwanted variations in the digital information chain. This will ensure that air transportation remains the safest way to travel, also in the future.

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 and 101114676.

References

[1] *Exploratory research project. SEC-AIRSPACE - Cyber Security Risk Assessment in virtualized AIRSPACE scenarios and stakeholders' awareness of building resilient ATM*, https://www.sesarju.eu/projects/sec-airspace, [retrieved: 09, 2024].

[2] *The Single European Sky ATM Research Joint Undertaking (SESAR-JU)*, https://sesar.eu/, [retrieved: 09, 2024].

[3] SESAR Joint Undertaking, *SESAR 2020 cybersecurity strategy*, Oct. 2017.

[4] *SecRAM 2.0. Security Risk Assessment Methodology for SESAR 2020*, Sep. 2017.

[5] *ISO/IEC 27005:2018 — Information technology — Security techniques — Information security risk management (third edition)*.

[6] NIST SP 800-30, "Guide for conducting risk assessments," en, National Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep. NIST SP 800-30r1, 2012. DOI: 10.6028/NIST.SP.800-30r1.

[7] 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. 102 223, 2022, ISSN: 0969-6997. DOI: https://doi.org/10.1016/j.jairtraman.2022.102223.

[8] EUROCONTROL, *Air traffic management - a cybersecurity challenge*, https://www.eurocontrol.int/sites/default/files/2021-12/eurocontrol-atm-cybersecurity-report.pdf, [retrieved: 09, 2024].

[9] European Union Aviation Safety Agency, *Opinion no 03/2021. management of information security risks*, https://www.easa.europa.eu/en/document-library/opinions/opinion-032021, [retrieved: 10, 2024].

[10] K. Charitoudi and A. Blyth, "A socio-technical approach to cyber risk management and impact assessment," 2013. DOI: 10.4236/jis.2013.41005.

[11] J. de Haan, "Specific air traffic management cybersecurity challenges: Architecture and supply chain," in *Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops*, ser. ICSEW'20, Seoul, Republic of Korea: Association for Computing Machinery, 2020, pp. 245–249, ISBN: 9781450379632. DOI: 10.1145/3387940.3392223.

[12] G. Falco and E. Rosenbach, "Why is cyber risk an issue?" In *Confronting Cyber Risk: An Embedded Endurance Strategy for Cybersecurity*. Oxford university press, Jan. 2022, pp. 1–15, ISBN: 9780197526545. DOI: 10.1093/oso/9780197526545.003.0001.

[13] M. S. K. Awan, P. Burnap, O. Rana, and A. Javed, "Continuous monitoring and assessment of cybersecurity risks in large computing infrastructures," in *2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems*,

2015, pp. 1442–1447. DOI: 10.1109/HPCC-CSS-ICESS.2015.224.

[14] G. Erdogan, E. Garcia-Ceja, Å. Hugo, P. H. Nguyen, and S. Sen, "A systematic mapping study on approaches for al-supported security risk assessment," in *2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC)*, 2021, pp. 755–760. DOI: 10.1109/COMPSAC51774.2021.00107.

[15] A. Costin and A. Francillon, "Ghost in the air (traffic): On insecurity of ads-b protocol and practical attacks on ads-b devices," *Black Hat USA*, pp. 1–12, 2012.

[16] H. Kelly, "Researcher: New air traffic control system is hackable," *Cable News Network (CNN), Jul*, 2012.

[17] R. Santamarta, *A Wake-up Call for SATCOM Security*, https://ioactive.com/wp-content/uploads/2018/05/IOActive_SATCOM_Security_WhitePaper.pdf, [retrieved: 09, 2024].

[18] S. Eskilsson, H. Gustafsson, S. Khan, and A. Gurtov, "Demonstrating ads-b and cpdlc attacks with software-defined radio," in *2020 Integrated Communications Navigation and Surveillance Conference (ICNS)*, 2020, 1B2-1-1B2–9. DOI: 10.1109/ICNS50378.2020.9222945.

[19] Financial Times, *Russian gps jamming threatens air disaster, warn baltic ministers*, https://www.ft.com/content/37776b16-0b92-4a23-9f90-199d45d955c3, [retrieved: 09, 2024].

[20] G. Lykou, G. Iakovakis, and D. Gritzalis, "Aviation cybersecurity and cyber-resilience: Assessing risk in air traffic management," in *Critical Infrastructure Security and Resilience: Theories, Methods, Tools and Technologies*, D. Gritzalis, M. Theocharidou, and G. Stergiopoulos, Eds. Cham: Springer International Publishing, 2019, pp. 245–260, ISBN: 978-3-030-00024-0. DOI: 10.1007/978-3-030-00024-0_13.

[21] H. Wynsma and S. Sullivan, "Civil aviation cybersecurity supply chain recommendations report," Civil Aviation Cybersecurity Subcommittee, Tech. Rep., 2020.

[22] International Standards and Recommended Practices, *ICAO Annex 17 to the Convention on International Civil Aviation, Safeguarding International Civil Aviation Against Acts of Unlawful Interference*, Jul. 2022.

[23] *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*.

[24] *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*.

[25] SESAR Project 16.02.03, *Minimum Set of Security Controls*, Aug. 2013.

[26] K. Bernsmed, M. G. Jaatun, and P. H. Meland, "Safety critical software and security - how low can you go?" In *2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC)*, 2018, pp. 1–6. DOI: 10.1109/DASC.2018.8569579.

[27] World Economic Forum, *The Global Risks Report 2022, 17th edition (insight report)*, https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf, [retrieved: 09, 2024].

[28] Boston Consultancy Group, *Building Cybersecurity Skills*, https://www.bcg.com/capabilities/digital-technology-data/building-cybersecurity-skills, [retrieved: 09, 2024].

[29] E. Frumento et al., *The role of Social Engineering in evolution of attacks*. 2016. DOI: 10.6084/m9.figshare.12369248.v1.

[30] *Smart ATM Virtual Centres*, https://www.sesarju.eu/virtual-centres, [retrieved: 09, 2024].

[31] European Cyber security Organisation, *Strategic Research and Innovation Agenda, WG6 SRIA*, https://ecs-org.eu/ecso-uploads/2022/10/59e615c9dd8f1.pdf, [retrieved: 10, 2024], Jun. 2017.

[32] M. Strohmeier, M. Schäfer, R. Pinheiro, V. Lenders, and I. Martinovic, "On perception and reality in wireless air traffic communication security," *IEEE transactions on intelligent transportation systems*, vol. 18, no. 6, pp. 1338–1357, 2016.

[33] A. Blåberg, G. Lindahl, A. Gurtov, and B. Josefsson, "Simulating ads-b attacks in air traffic management," in *2020 AIAA/IEEE 39th Digital Avionics Systems Conference (DASC)*, 2020, pp. 1–10. DOI: 10.1109/DASC50938.2020.9256438.

[34] PACAS deliverable D3.1, *Gap analysis of existing modelling methodologies for the ATM domain and requirements*, Nov. 2016.

[35] *Horizon 2020 project. Enterprises intangible Risk Management via Economic models based on simulation of modern cyber attacks (HERMENUT)*, https://www.hermeneut.eu/, [retrieved: 09, 2024].

[36] *Horizon 2020 project. aDvanced sOcial enGineering And vulNerability Assessment (DOGANA)*, https://www.dogana-project.eu/, [retrieved: 09, 2024].

[37] *ISO/IEC 27002:2022 — Information technology — cybersecurity and privacy protection — Information security controls*.

[38] C. W. Johnson, "Cyber security and the future of safety-critical air traffic management: identifying the challenges under NextGen and SESAR," in *10th IET System Safety and Cyber-Security Conference 2015*, IET, 2015, pp. 1–6.

[39] A. Tursunbayeva, S. Di Lauro, and C. Pagliari, "People analytics—a scoping review of conceptual boundaries and value propositions," *International journal of information management*, vol. 43, pp. 224–247, 2018.

[40] F. Pagnozzi, "People analytics and human resource management: How the use of smart data can improve the training processes," *puntOorg International Journal*, vol. 7, Aug. 2022. DOI: 10.19245/25.05.pij.7.2.2.

[41] T. Elias, *Learning analytics: Definitions, processes and potential*, 2011.

[42] SKYbrary, *4d trajectory concept*, https://skybrary.aero/articles/4d-trajectory-concept, [retrieved: 09, 2024].