Towards cybersecurity risk assessment for future ATM – first steps

Tim H. Stelkens-Kobsch*, Frank Morlang*, Karin Bernsmed†, Per Håkon Meland†, Hilke Boumann*, Davide Martintoni‡, Valerio Senni‡, Vladimíra Čanádyová§ and Bhavesh Sharma§
Email: {tim.stelkens-kobsch, frank.morlang, hilke.boumann}@dlr.de, {karin.bernsmed, per.h.meland}@sintef.no, {davide.martintoni, valerio.senni}@collins.com, {vladimira.canadyova, bhavesh.sharma}@dblue.it
*Institute of Flight Guidance, German Aerospace Center (DLR), Braunschweig, Germany
†SINTEF Digital, Trondheim, Norway.
‡Collins Aerospace, Rome, Italy
§Deep Blue srl, Rome, Italy

***Abstract*— Cybersecurity risk assessment in air traffic management (ATM) is indispensable for maintaining and enhancing the safety and efficiency of air navigation services. It supports informed decision-making, helps in adapting to changing operational conditions, ensures compliance with safety regulations, and prepares the system for disturbances, thereby contributing to the overall integrity and reliability of the air traffic management system. However, there are practical challenges when risk analysts conduct such assessments, and there is a need for better support tools and materials. The European exploratory research project SEC-AIRSPACE is developing an improved cybersecurity risk assessment methodology for ATM. The novelty here is to improve existing approaches and provide an up-to-date taxonomy of primary and supporting assets that should be considered when developing new ATM solutions. This will make it easier for stakeholders to identify new assets and threats that arise with emerging technologies and services. The constructive research approach will make use of validation through two different use cases, where the first is related to the establishment of the future communications infrastructure and multilink and the second to virtual centers that provides ATM services independently of physical locations.**

Keywords—cybersecurity, air traffic management, future air traffic management, dynamic security risk assessment

I. INTRODUCTION

The importance of cybersecurity for air traffic management (ATM) can be traced back to its historical evolution and increasing reliance on digital technologies. Initially, ATM depended on manual systems and direct radio communications, which posed minimal cyber risks due to the isolated nature of these systems. Even telephone systems and communication networks were established for exclusive use by aviation entities, allowing ground-ground communication and provision of services, as well as air-ground communication between the respective actors. The isolated existence of aviation systems assured a secure perimeter and kept a very high cybersecurity standard. However, with the transition to digital systems in the late 20th century, the reliance on data networks, radar, and satellite-based navigation grew, introducing new vulnerabilities [1] [2]. Aviation has to turn to a more proactive security approach, especially because existing legacy systems were never designed to "be in the wild" and are therefore specifically prone to cybersecurity attacks. Increased connectivity between systems poses a new working environment in which the systems must operate. New systems and services need to be designed with emerging, more interconnected environments in mind in order to meet current and future security requirements. It is of special importance that they can be adapted to new threats on the horizon, ensuring a long lifecycle and future-proof security measures.

Whereas aviation has suffered early and repeatedly from physical/kinetic security incidents, security incidents related to information technology (IT) and operational technology (OT) started to endanger aviation and jeopardize the smooth and safe flow of passengers and goods only some years ago. Since the Internet of Things (IoT) has started to conquer aviation [3], IT/OT security has to be treated with at least the same priority as physical security. Recent scientific research, such as [4] [5] [6] [7] [8], has highlighted the risks of cyberattacks like GPS spoofing and signal interference, which can mislead aircraft or disrupt air traffic control (ATC). Today, modern ATM integrates digital networks, data links, and automated control systems, making it vulnerable to cyberattacks that could disrupt operations, manipulate data, or create unsafe conditions.

Cybersecurity measures are essential to protect sensitive information, support operational continuity, and ensure safety. As ATM has evolved technologically, it is crucial to protect it against cyber threats. Cybersecurity in ATM assures efficient movement of aircrafts, and supports national security by preventing unauthorized access or interference. Ultimately, strong cybersecurity measures protect the safety of passengers and crew, maintain trust in the aviation industry, and preserve the reputation and reliability of air traffic management.

Although one could think cybersecurity risk assessment is already an established and widely used procedure in the ATM domain, this is not completely true [9]. There are several methods to assess the different kinds of security risks [10] like e.g., the security risk assessment methodology (SecRAM) [11], which was developed by the Single European Sky ATM Research (SESAR). SecRAM indeed provides a comprehensive and detailed security risk assessment methodology for ATM, but it is not fully equipped for assessing cybersecurity risks of emerging systems. For example, when systems have to be assessed which currently are in transit to a virtualized setup (i.e., the entire ATM system), and in parallel an increased data sharing has to be considered (and assessed), SecRAM needs to be enabled to provide the functionalities.

Emerging technologies are nowadays included in more and more systems and products which ease our lives. The same will become true for systems building the backbone of

ATM in the near future, as ATM will receive a game-changing shift in its setup. Around the world, aviation stakeholders are working to transform the originally separate and isolated ATM system into a virtualized system that takes advantage of the new technologies and enhanced information exchange available today. As such, the established cybersecurity risk assessment methodologies have to be restructured and enhanced to reflect and cover these changes.

This paper explains the first steps to improve such a methodology and how and what has to be reviewed in each and every step. After a short overview of the project (section II) and a review of existing approaches for cybersecurity risk assessment in ATM (section III), the reflection starts with explaining the method applied to set up the new taxonomy (section IV), continues with the application of the taxonomy to achieve a structured risk assessment (section V) and provides a discussion on the actions taken (section VI). The final section VII provides a conclusion. This paper will explain how SEC-AIRSPACE achieved the first two steps of the renewed risk assessment methodology, while the reporting on the remaining steps (evaluation of risk in terms of impact and cascading effects, and mitigating security controls) has to be tackled in future dissemination. The latter is still under development and will be conducted in the remaining time of the project.

II. Description of the Project

The work presented in this project has been performed in the Exploratory Research project SEC-AIRSPACE [1]. The project aims to enable a more resilient ATM by focusing on reducing the risks of virtualization and increased data-sharing between all components of the ATM infrastructure and the relevant stakeholders. The project will enhance the state-of-the-art security risk assessment methodology(ies) currently adopted in ATM with relevant cyber security components. Further, the project will investigate the potential of applying the concept of People Analytics [12] to increase cyber security awareness in ATM organizations.

In order to achieve the updated risk assessment, the project develops a taxonomy for ATM from different sources while existing threat and vulnerability handling approaches are updated. Furthermore, the effect of cascading effects within the surveyed systems is considered and the entire approach is exemplarily tailored to two project use cases.

The first use case is about establishing the future communication infrastructure (FCI) in ATM. Nowadays the communication infrastructure in ATM consists of three main elements [13]:

- The air traffic services (ATS) such as the aeronautical telecommunications network (ATN), which support ATM operations and key stakeholders in their collaboration and day-to-day work, and the datalink applications they rely on like, e.g., controller-pilot datalink communications (CPDLC) and automatic dependent surveillance - contract (ADS-C).
- Networks, which support transportation of application data through routing functions to ensure delivery.
- Physical links (radio and terrestrial), which support the connection of two or more locations for the purpose of transmitting and receiving information.

In the near future, the ATN network system is subject to a significant reorganization in several areas to support greater efficiency and upscaling of transportation needs [14]. Fig. 1 provides an overview of the current and future ATM operations layered architecture.

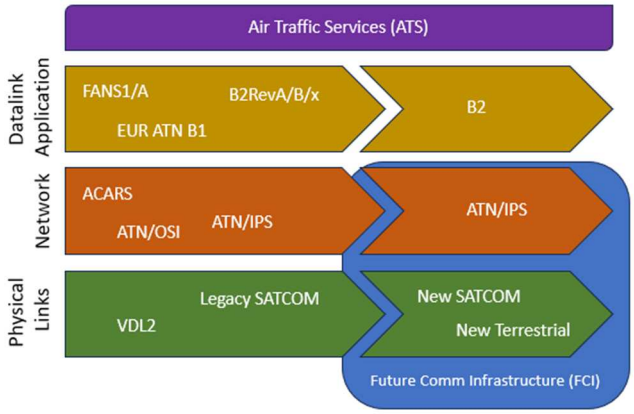

Fig. 1. ATM operations layered architecture, adapted from [13].
FANS: Future Air Navigation System; ACARS: Aircraft Communications Addressing and Reporting System; OSI: Open Systems Interconnection; IPS: Internet protocol suite VDL: Very High Frequency Datalink, ATN BX: Aeronautical Telecommunications Network Baseline X.

The second use case is about the virtualization of air traffic services (ATS) with the help of virtual centers (VC).

The concept of a Virtual Centre (VC) is illustrated in Fig. 2. It intends to decouple Air Traffic Management (ATM) data services, such as flight data, radar, and weather information, from the physical Controller Working Position (CWP). The aim is to enable greater flexibility when it comes to organizing ATC operations and, in doing so, seamless and more cost-efficient service provision to airlines and other airspace users. The new approach shall bring advantages in terms of increased flexibility in organizing ATC operations in and between the air traffic service units (ATSUs), as well as enabling multiple ATSUs to perform services seamlessly from an airspace user's perspective.

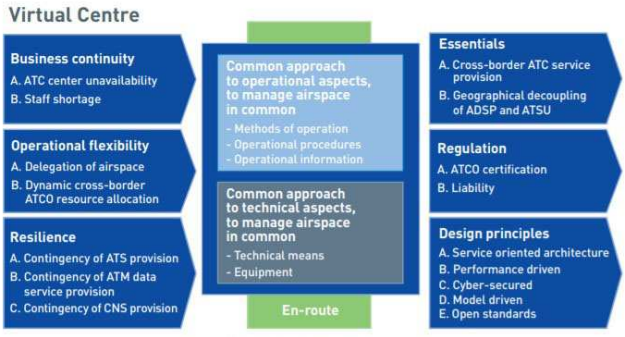

Fig. 2. Overview of Virtual Centres [15].

In this paper, the focus is kept on the development of the taxonomy and the assessment of the threat landscape and vulnerabilities, as the following steps (cascading effects, inclusion of People Analytics and subsequent validations) still

[1] https://www.sesarju.eu/projects/sec-airspace

need to be facilitated in the remaining project period and are work in progress.

III. Existing aproaches for ATM Cybersecurity Risk Assessment

The state of the art for applied risk assessment in ATM is scattered. Most of the aviation related projects in Europe follow the SecRAM, which has been developed and maintained by the SESAR Joint Undertaking for many years. Some other work bases on the risk analysis initially provided by a European research project called CORAS [16] [17]. Similar approaches are being used in other sectors and in different contexts, e.g., ISO/IEC 27005 [18], NIST SP 800-30 [19] and EBIOS [20]. These standards are sector-independent and are occasionally applied in ATM as well. Some solutions also utilize standards and guidelines issued by their own governments, for example Margerit [21], which was developed by the Spanish Ministry of Public Administrations.

Regardless of which methodology is being applied, to achieve a correct understanding of the main risks and how to manage them, it is necessary to fully understand the architecture of the system being assessed and its intended operation and relevant procedures and tools. To this end, an understanding of the *main assets that need protection* and the *relevant threats and vulnerabilities* is needed. In SecRAM, the identification of assets, threats and vulnerabilities is supported by the so-called "catalogues". The catalogues are in a spreadsheet file. It lists typical examples of information and services that the SESAR solutions utilize, the supporting software, hardware, and network components that the ATM systems are constructed upon, and a set of accompanying threats and vulnerabilities that are typically seen in (IT) systems. SecRAM not only covers information systems but also other aspects such as operations/procedures (human related), physical security, and natural hazards, which, however, are not of concern for the presented work. These catalogues are currently maintained by the SESAR transversal project PEARL[2]. However, a recent study performed by Bernsmed et al. [9] showed that many of the SESAR solutions struggle to identify relevant assets and threats when using these catalogues. In addition, or as an alternative to the catalogues, many solutions therefore choose to rely on models in the European Air Traffic Management (eATM) portal[3] to identify assets at risks. A problem with both approaches is that their content is rarely updated, and they tend to focus on the technical parts of the ATM systems only. While additional taxonomies have been created, including the NASA Air Traffic Management Ontology [22] and the ATM Information Reference Model Ontology [23] these do not seem to have been incorporated into any guidance material so far that would help the security risk assessment practitioners utilize them. Further, the inability of current cyber risk models to include socio-technical factors along the entire supply chain in addition to technical components has also been recognized in literature [24]. Hence, there is an urgent need to support the practitioners in their efforts of identifying, evaluating, and protecting assets at risk in future ATM scenarios that utilize more advanced technologies and tools.

The static nature of current risk assessment methodologies, which are based on catalogues and spreadsheets, is a shortcoming for further development and upgrade of cyber (and also physical) security risk assessments. It is obvious that a more flexible approach has to be taken, which allows to assess the core data more quickly and easily.

The basis of each risk assessment is the knowledge about the elements at risk. The European ATM research and industry currently relies on SecRAM, which utilizes the idea of primary (PA) and supporting assets (SA).

The developed taxonomy follows the SecRAM definitions of primary and supporting assets, where a primary asset is an "Intangible function, service, process or information that are part of the ATM system within the scope of the project and has value to the system. They are information and services that are valuable in the sense that a successful attack impairing them will mean harm to the ATM system in terms of personnel, capacity, performance, etc." [11]. On the other hand, a supporting asset is "a tangible element that supports the existence of the primary assets. Entities involved in storing, processing and/or transmitting primary information assets are classified as supporting assets. Examples are hardware, software and people." [11]

IV. Method

The project follows a constructive research approach [25], where a problem faced in the real world is solved, and this solution also contributes to the theory of this field by analyzing what works (or does not work) in practice. The solutions, that is, constructs, can be processes, practices, tools or organization charts. Through a close collaboration between researchers and practitioners, SEC-AIRSPACE provided a construct (here: a taxonomy) which was then tested internally for practical applicability through use cases.

The realized taxonomy contains content from the following sources of information related to assets:

- NASA Air Traffic Management Ontology (atmonto) [22].
- ATM Information Reference Model Ontology (AIRM) [23].
- Approved content from finished and ongoing SESAR projects handling Remote Tower (RT), Multiple Remote Tower (MRT) [26] and Future Communication Infrastructure (FCI) [27] [28].
- The SecRAM catalogues [29].
- The eATM portal.

Several tools to set up a taxonomy were reviewed and finally Protégé was chosen to collect and align the different lists of assets [30]. In fact, the tool is open source, and provides the necessary functionalities.

At first, the ATM Information Reference Model Ontology and the NASA Air Traffic Management Ontology were imported as Resource Description Framework (RDF) files and merged in the ontology tool. Secondly, the relationship specifications were deleted to transform the merged ontologies to a taxonomy template. After that, the entities were sorted by editing adaptations into PAs and SAs according to the structure in Fig. 3.

[2] https://sesar.eu/projects/pearl

[3] https://www.eurocontrol.int/portal/european-atm-master-plan-portal

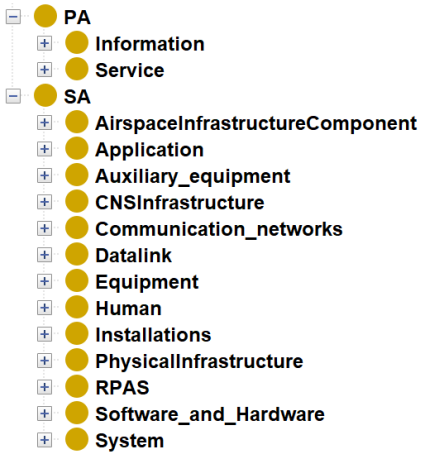

Fig. 3. The SEC-AIRSPACE taxonomy structure.

In the next step, specific entities with a focus on virtualization and increased data sharing (the main focus of SEC-AIRSPACE) were imported, which already exist in the European ATM Architecture (EATMA) and have been used by previous European research projects on remote tower (RT), multi remote tower (MRT) centers and future communication infrastructure (FCI). Then, the currently existing taxonomy utilized by SecRAM was imported into the new one. The import was facilitated with a combination of MappingMaster domain-specific language (DSL) rule development [31] and successive editing adaptations. The MappingMaster DSL defines mappings from spreadsheet content to Web Ontology Language (OWL) ontologies and is a subset of the Manchester OWL Syntax [32].

In order to add content from eATM, a tailored software needed to be developed. eATM allows to download specific sub-architectures in the form of spreadsheets. These spreadsheets, however, differ significantly in their arrangement and shape from the ones previously imported to the SEC-AIRSPACE taxonomy. Therefore, a taxonomy analyzer software was developed in the Tool Command Language (Tcl) [33] to compare the content against the existing taxonomy entities. Tcl is a scripting language that was introduced in the late 1980s. It has become a popular choice for scripting tasks in a wide range of industries, including software development, network administration, and scientific research. One of the key strengths of Tcl is its extensibility. The language includes a powerful extension mechanism that allows developers to add new commands and functions to the language, enabling them to customize and extend Tcl to suit their specific needs. This extensibility has made Tcl a popular choice for building custom scripting environments and domain-specific languages. The two extension packages used for the taxonomy analyzer development were the "COM Automation With Tcl package" (CAWT [34]) and the tdom package [35]. CAWT provides users with a powerful tool for integrating and interacting with external applications and data sources through the Component Object Model (COM) interface, streamlining data processing workflows, enhancing data integration, and facilitating cross-platform communication for improved research outcomes. CAWT itself uses the Tcl Windows API (TWAPI) extension for scripting Microsoft Windows applications with Tcl. This was used for the connectivity to the spreadsheets. The tdom package is a tool for working with the Extensible Markup Language (XML) and Hypertext Markup Language (HTML) data in the Tcl. It provides a set of commands and functions that allow users to parse, manipulate, and generate XML and HTML documents. One of the key features of tdom is its ability to handle large XML and HTML files efficiently. The package uses a lightweight streaming parser that can process documents of any size without consuming excessive memory or causing performance issues. This makes tdom ideal for working with complex data sets or processing large amounts of information in real time. It was used for the connectivity to the taxonomy file in the XML-based RDF format. The taxonomy analyzer runs through all cells of a defined region in a spreadsheet and compares the cell content with each entity in an RDF file. With each cell content, it runs the comparison with each substring of the cell, always allowing the abortion of the cell content check. As a result, the software generates an information file describing if spreadsheet content was found in the RDF file or not, and if yes, where. This information streamlines further editing adaptation needs of the taxonomy under consideration.

The steps needed to include data from the eATM spreadsheets are summarized in TABLE I.

TABLE I. STEPS FOR IMPORTING EATM DATA TO THE SEC-AIRSPACE TAXONOMY.

No.	Description
1	Check for duplicates in downloaded eATM spreadsheets (apply to column *description*).
2	Reformat corrupt entries in column *description* (some formatting may have got lost during data transfers).
3	Check again for duplicates (apply to entire row).
4	Identify most up-to-date entries to solve persisting ambiguities. e.g. *Attention Guidance* vs *Attention Guidance (PJ.05-W2-97.1)*. Then move PJ reference from column *title* to column *description*.
5	Swap *C01*, *C02*, etc., within title of some assets to allow proper comparison with existing taxonomy. (e.g. *C01 Radar Composite* swapped to *Radar Composite (C01)*).
6	When duplicate entries are given from different phases of SESAR, keep content of latest phase.
7	Delete spaces in column *title* to achieve comparable structure of asset names.
8	Use taxonomy analyzer to identify already existing and non-existing entries in the taxonomy.
9	Import identified assets which are new to the taxonomy

When looking at the available taxonomies and ontologies for risk assessment in ATM it was clear that they could not be easily merged due to their heterogeneity. The existing methodologies have grown historically and have also been designed by different interest groups and stakeholders. There exists no "super" taxonomy gathering all the content of the single ones. While developing the updated taxonomy in SEC-AIRSPACE and applying it to identify PAs and SAs for the underlying use case studies, the following challenges were experienced and overcome:

- Semantic heterogeneity: Different source ontologies used somewhat varying terminology and conceptualizations, even within the same ATM domain. This required to semantically map corresponding concepts and choose which terms to keep.
- Syntactic differences: Not all sources used a standardized format, such as OWL or RDF. These syntactic differences necessitated conversion mechanisms, which introduced complexity and errors

in the merging process. A manual cleanup was therefore needed.

- Granularity: The sources differed in the level of detail they provided. One source might describe a concept in great detail, while another might treat it more generally. Aligning these varying levels of granularity without losing important information or overcomplicating the new taxonomy required delicate balancing.
- Completeness: Different ontologies have been designed with different purposes in mind, even within the same domain. Therefore, concepts with less relevance for risk assessment were ignored. The overall size of the taxonomy also needed to be considered, keeping it manageable and user-friendly.
- Gaps: Despite having several source ontologies, there were gaps that none of them covered. This especially concerned concepts related to new services, roles and technologies within the ATM domain. The applied research strategy was to fill in these gaps based on assessments already performed on SESAR solutions and assets from the use cases developed in this project. Here, it has to be noted, that a clear limitation in the completeness of the assessment is the limited set of solutions and use cases which was used. Hence, the taxonomy should not be considered complete and exhaustive for all possible solutions.

In order to assess the applicability of the developed taxonomy the first two steps of the risk assessment were conducted on the two use cases. Some insights of this process are given in Section V.

V. Enabling of a Structured Risk Assessment

The structured taxonomy of primary and supporting assets, resulting from Section IV, serves as the foundational framework to facilitate a high-level understanding of the core components and their interrelation in the complex system of systems presented by a modern ATM use case scenario. The taxonomy delineates the assets using a hierarchy that enables a security professional to effectively identify and map the core components of the use case scenario to the taxonomy. The SecRAM approach proposes the identification of assets that represent the most important components and concepts in the system under analysis as a first step. A structured taxonomy enables the stakeholders to abstract the functional architecture not only as a list but also as a structured asset diagram representation that can be used to orchestrate a detailed threat and vulnerability assessment. This is efficient to extract the multiple relationships between different components which would not be easily inferred by a general system architecture. By using a structured asset diagram, it is possible to capture assets and relationships that are not highlighted in a standard functional architecture.

Fig. 4 shows a simple example of how an asset diagram (right side) can help representing and extending the core components from a security point of view in a functional architecture (left side). The asset diagram shall be produced by a security professional using the proposed taxonomy as a guideline. This asset model is not formal: it is a support tool for security professionals and thus provides them with high degrees of freedom on what is possible to represent. Given the ability to represent different concepts and relationships, the asset model should, at least, always carry as a minimum of information a set of assets and a representation of how they relate to each other. The example asset diagram on the right shows a set of SAs for a high-level airborne communication infrastructure (green boxes) that are all coordinated to realize the intangible PA concepts (violet boxes). Notice that not all assets identified can be directly mapped to the functional architecture on the left, e.g., high level concepts such as “PA - Flight Information” are captured only in the asset diagram. Another example is the fact, that the asset diagram includes a “SA Human - Maintainer” box which interacts with the system and thus might introduce some security risks: this type of asset can be easily identified by browsing the proposed taxonomy that reminds the stakeholder to analyze also the humans involved in the scenario.

On top of a pure asset list, the asset diagram carries a set of informal relationships that support the reasoning process for a threat and vulnerability analysis. A first type of relationship is the encapsulation which derives directly from the taxonomy: this type of structure represents elements that belong to a superordinate unit and represent a specification (e.g., a maintainer is a specific type of human) or a functional containment (e.g., an ATN/IPS host will have a CPDLC service running in it). A generic relationship can be depicted using arrows and specifying how one asset interacts with or affects another asset (e.g. physical datalinks support the IP/ATN airborne infrastructure). Notice that most of the standards and methods for security risk assessments are asset-driven [11] [16], meaning that the assets are used as attacker goals. However, an asset diagram representation as proposed here does not only model the assets and their hierarchy but also introduces the concept of asset dependencies. This captures information coming from the functional architecture (i.e. data flows) and on top of it also highlights asset dependencies which are not easily identified directly in the functional architecture. By looking at the functional architecture it is possible to deduce, that an attack on the “ATN/IPS router” could lead to an impact on the “Trajectory Based Operations (TBO)”. With the support of the asset diagram, on top of direct outcome, it is also possible to presume that this type of attack would also impact the overall “PA Info - Flight Information“ and possibly the safety of the respective flight.

Using the asset diagram representation, a security professional can systematically assess the threat landscape for each supporting asset identified and pinpoint potential adversaries and how they could attack the system. The developed taxonomy is also the driver for vulnerability assessments which scrutinize all the assets in the diagram and identify possible weak points which facilitate or enable threats inside the system.

Going forward with the security risk assessment, the structured asset diagram can provide strong insight to empower security professionals for a cascading effect analysis. The threats identified might have an overall low risk if taken as single entities. However, the combination of events exploiting threats and vulnerabilities by an expert attacker might lead to a drastic change in the overall risk estimation of

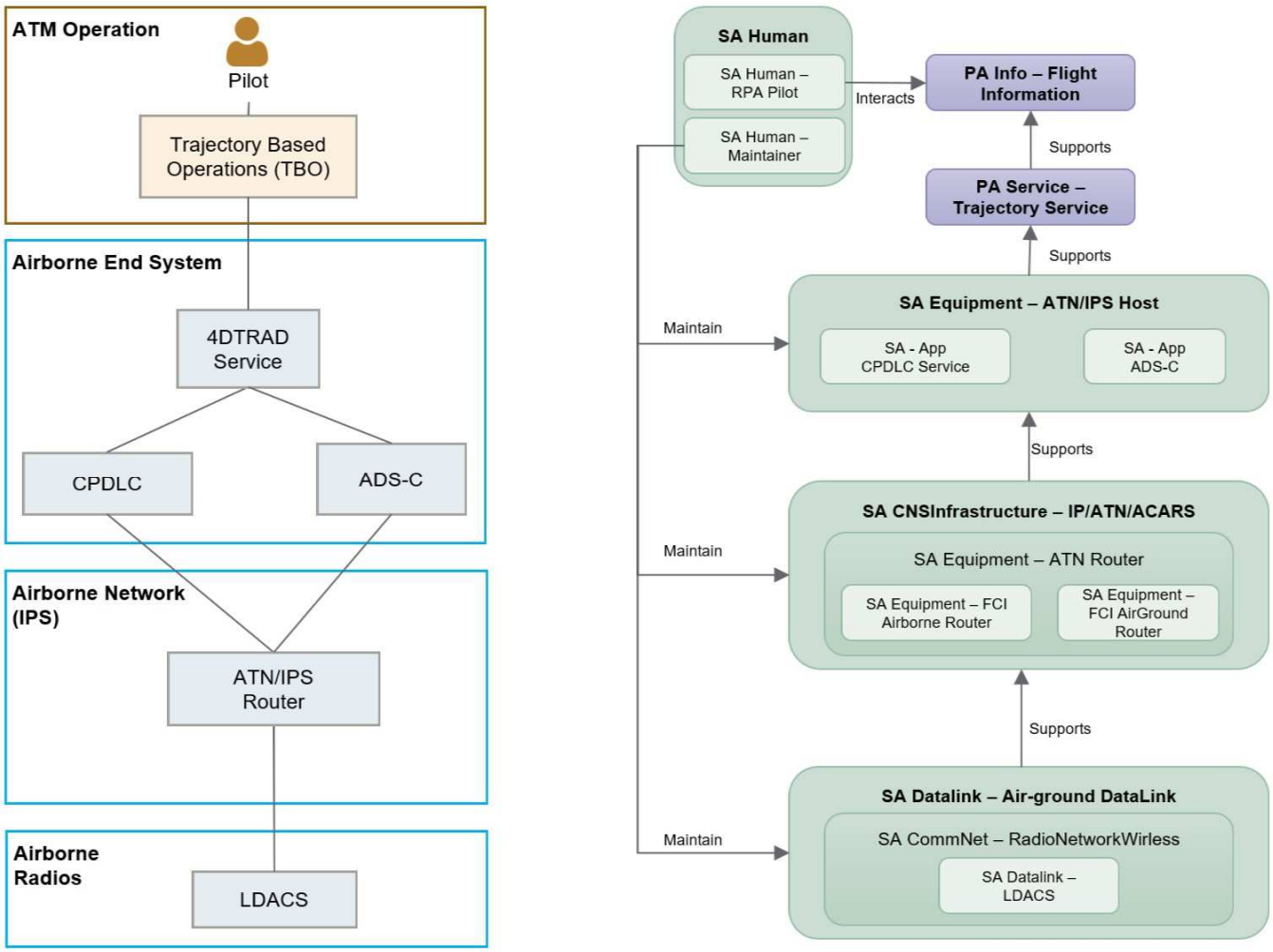

Fig. 4. High-level diagrams for airborne Trajectory Based Operation. Left: Functional Architecture. Right: Asset Diagram; PA: Primary Asset; SA: Supporting Asset; 4DTRAD: 4-Dimension TRAjectory Data link; LDACS: L-band Digital Aeronautical Communications System.

the scenario by introducing highly relevant attack combinations. Finally, the asset diagram empowers the stakeholder organization to formulate a structured and targeted mitigation strategy aiming at providing resilience and robustness to the assets identified as core security points by the threat and vulnerability analysis.

Such a structured hierarchy of assets is a powerful tool to represent the information required by and produced throughout risk assessments which are usually performed in a general risk assessment methodology such as SecRAM. The proposed taxonomy therefore is an enabler mechanism for navigating the complexities of modern ATM environments and pursuing the cyber-resilience posture that those systems demand.

VI. Discussion

So far in the SEC-AIRSPACE project, the initial insights show that using the updated taxonomy of primary and supporting assets in complex systems like ATM offers numerous benefits. The applied structured approach aids in organizing and analyzing the plenitude of elements that constitute such systems, facilitating more effective and comprehensive risk management. A taxonomy helps to organize assets into clear categories, making it easier for risk analysts to understand the structure and functions of the system. This classification simplifies identifying which assets are critical (primary) and which ones support those critical assets (supporting). While constructing this first version of the taxonomy, it turned out that it already allowed better communication between the participating persons and organizations (here: consortium partners in the project) by creating a common understanding of terms and definitions. Having the same basis facilitated better co-operation among team members and stakeholders and ensured that everyone understood which assets are under discussion and their roles within the system. A common taxonomy also accelerated the start of the next steps in the enhancement of the methodology (threat analysis and evaluation of cascading effects; out of scope for this paper), as all contributors share the same understanding. Applying the same taxonomy in assessments of different ATM solutions is thought to achieve better knowledge transfer and enhance efficiency, e.g., by reducing redundant analysis. Though several challenges were experienced when developing the taxonomy, these were overcome in a satisfactory way and the result is a construct that has proven to be of good use in a practical setting (i.e., the first part and subsequent steps of the risk assessment conducted on the project use cases), which is the goal of a constructive research approach.

There are several potential threats to validity that could affect the outcomes and generalizability of the research. Understanding these threats is crucial for interpreting the results accurately and for guiding future research and application in the field. The taxonomy has been applied to a security analysis in a European ATM context. The findings may not be directly applicable to other sectors or even to all aspects of ATM worldwide. Similarly, the use cases selected for validation cover only limited scenarios and emerging technologies in ATM. If the use cases are too narrow or not sufficiently representative of broader ATM operations, the results might not be broadly applicable. Related to the completeness of the taxonomy, the primary and supporting assets should comprehensively cover relevant elements. Any gaps or omissions could lead to incomplete assessments and potentially overlook critical risks. In terms of consistency, methods used to perform risk assessments must be reliable, meaning they should produce consistent results under similar conditions. Variability in how risk assessments are conducted or interpreted can lead to inconsistencies in the findings.

Looking ahead, the next step of the risk assessment approach will need to address the evaluation of risks in terms of impact and cascading effects, as well as the development of targeted security controls. This future work will be crucial in ensuring that the solutions being developed are adaptable and robust enough to meet the challenges posed by an increasingly complex and technologically advanced aviation industry. In addition, the analysts involved in the development of ATM solutions need to be trained so that they can really take advantage of the taxonomy in conjunction with their risk assessment methodology. In future project activities, the improved risk assessment approach will be validated with the help of relevant stakeholders in order to evaluate its foreseen benefits and its operational feasibility.

VII. Conclusion

In this paper some of the prevalent shortcomings of current ATM risk assessment methods are highlighted, which often struggle to keep pace with technological advancements and the evolving nature of cyber threats. The reliance on outdated catalogues and the lack of integration of socio-technical factors in risk assessments are significant gaps that the SEC-AIRSPACE project aims to fill. By developing an updated taxonomy of assets, the project seeks to create a more responsive and comprehensive framework that can better identify and mitigate potential threats.

The work conducted so far shows that established (though static) processes like security risk assessment can be enhanced to keep pace with the rapidly growing surface of attack vectors resulting from the increasing interconnectedness of ATM. The work presented in this paper shows that e.g., SecRAM can be enabled to assess the changing risk landscape of future ATM. This will allow to utilize increased data sharing and virtualization as requested by the SESAR Strategic Research and Innovation Agenda [36]. However, methodologies like SecRAM still need to be fully enabled to dynamically adapt to emerging changes identified and, even more important, not yet identified. SEC-AIRSPACE, which provided the basis and carried out the first steps for further development of an established risk assessment, will continue to upgrade the methodology for the subsequent steps like: evaluation of risk in terms of impact and cascading effects, and mitigating security controls.

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 conducted using Protégé [30].

References

[1] 'Air traffic management: evolution with technology', *IEEE Control Syst.*, vol. 16, no. 4, pp. 12–21, Aug. 1996, doi: 10.1109/37.526911.

[2] 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. doi: 10.1007/978-3-030-00024-0_13.

[3] M. S. Rahman, S. Manickam, and S. Ul Rehman, 'Role of Internet of Things in Aviation Industry: Applications, Challenges, and Possible Solutions', in *2022 International Conference on Informatics Electrical and Electronics (ICIEE)*, Oct. 2022, pp. 1–6. doi: 10.1109/ICIEE55596.2022.10010233.

[4] 'View of Spoofing in aviation: security threats on GPS and ADS-B systems'. Accessed: Apr. 19, 2024. [Online]. Available: https://aseestant.ceon.rs/index.php/vtg/article/view/30119/17261

[5] N. Mäurer, T. Guggemos, T. Ewert, T. Gräupl, C. Schmitt, and S. Grundner-Culemann, 'Security in Digital Aeronautical Communications A Comprehensive Gap Analysis', *Int. J. Crit. Infrastruct. Prot.*, vol. 38, p. 100549, Sep. 2022, doi: 10.1016/j.ijcip.2022.100549.

[6] G. Dave, G. Choudhary, V. Sihag, I. You, and K.-K. R. Choo, 'Cyber security challenges in aviation communication, navigation, and surveillance', *Comput. Secur.*, vol. 112, p. 102516, Jan. 2022, doi: 10.1016/j.cose.2021.102516.

[7] E. Habler, R. Bitton, and A. Shabtai, 'Evaluating the Security of Aircraft Systems', 2022, doi: 10.48550/ARXIV.2209.04028.

[8] T. H. Stelkens-Kobsch and A.-V. Predescu, 'Contribution to a secure urban air mobility', in *2022 IEEE/AIAA 41st Digital Avionics Systems Conference (DASC)*, Sep. 2022, pp. 1–5. doi: 10.1109/DASC55683.2022.9925845.

[9] 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', *J. Air Transp. Manag.*, vol. 102, p. 102223, Jul. 2022, doi: 10.1016/j.jairtraman.2022.102223.

[10] A. A. Elmarady and K. Rahouma, 'Studying Cybersecurity in Civil Aviation, Including Developing and Applying Aviation Cybersecurity Risk Assessment', *IEEE Access*, vol. 9, pp. 143997–144016, 2021, doi: 10.1109/ACCESS.2021.3121230.

[11] M. Le Fevre, B. Gölz, 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

[12] A. Tursunbayeva, S. Di Lauro, and C. Pagliari, 'People analytics—A scoping review of conceptual boundaries and value propositions', *Int. J. Inf. Manag.*, vol. 43, pp. 224–247, Dec. 2018, doi: 10.1016/j.ijinfomgt.2018.08.002.

[13] G. T. Saccone, R. D. Hale, M. E. Matyas, and M. L. Olive, 'Preparing for transition: Accommodation of mixed data communication equipage for a harmonized future', in *2018 Integrated Communications, Navigation, Surveillance Conference (ICNS)*, Apr. 2018, pp. 4B2-1-4B2-10. doi: 10.1109/ICNSURV.2018.8384883.

[14] EASA, FAA, Airbus, and Boeing, 'Future Connectivity for Aviation - White Paper'. 2022.

[15] ‘SESAR Joint Undertaking | Virtual Centres’. Accessed: Feb. 27, 2024. [Online]. Available: https://www.sesarju.eu/virtual-centres

[16] ‘The CORAS Method’. Accessed: May 07, 2024. [Online]. Available: https://www.coras.tools/#/

[17] ‘A Platform for Risk Analysis of Security Critical Systems | CORAS Project | Fact Sheet | FP5’, CORDIS | European Commission. Accessed: May 07, 2024. [Online]. Available: https://cordis.europa.eu/project/id/IST-2000-25031

[18] ISO/IEC JTC 1/SC 27, ‘ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks’, ISO. Accessed: Feb. 27, 2024. [Online]. Available: https://www.iso.org/standard/80585.html

[19] Joint Task Force Transformation Initiative, ‘Guide for conducting risk assessments’, National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-30r1, 2012. doi: 10.6028/NIST.SP.800-30r1.

[20] ‘EBIOS Risk Manager – The method | ANSSI’. Accessed: May 03, 2024. [Online]. Available: https://cyber.gouv.fr/publications/ebios-risk-manager-method

[21] ‘Magerit’, ENISA. Accessed: May 03, 2024. [Online]. Available: https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_magerit.html

[22] 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/

[23] ‘Home | AIRM.aero’. Accessed: May 06, 2024. [Online]. Available: https://airm.aero/

[24] K. Charitoudi and A. Blyth, ‘A Socio-Technical Approach to Cyber Risk Management and Impact Assessment’, *J. Inf. Secur.*, vol. 04, no. 01, pp. 33–41, 2013, doi: 10.4236/jis.2013.41005.

[25] K. Lukka, ‘The Constructive Research Approach’, in *Case Study Research in Logistics*, 2003, pp. 83–101.

[26] ‘SESAR Joint Undertaking | Remote tower for multiple airports’. Accessed: May 07, 2024. [Online]. Available: https://www.sesarju.eu/projects/remotetower

[27] ‘SESAR Joint Undertaking | Essential and efficient communication, navigation and surveillance integrated system’. Accessed: May 07, 2024. [Online]. Available: https://www.sesarju.eu/projects/eecns

[28] ‘SESAR Joint Undertaking | FCDI- Future Connectivity and Digital Infrastructure’. Accessed: Feb. 27, 2024. [Online]. Available: https://www.sesarju.eu/projects/FCDI

[29] B. Goelz, M. le Fevre, and R. Flohr, ‘SecRAM catalogues 02_00_00 (1_0)’. Oct. 27, 2017.

[30] 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.

[31] ‘protegeproject/mapping-master’. Protégé Project, Apr. 04, 2024. Accessed: May 06, 2024. [Online]. Available: https://github.com/protegeproject/mapping-master

[32] ‘OWL 2 Web Ontology Language Manchester Syntax (Second Edition)’. Accessed: May 06, 2024. [Online]. Available: https://www.w3.org/TR/owl2-manchester-syntax/

[33] ‘Tcl/Tk Language’. Accessed: May 07, 2024. [Online]. Available: https://www.tcl.tk/about/language.html

[34] ‘CAWT’. Accessed: May 07, 2024. [Online]. Available: https://wiki.tcl-lang.org/page/CAWT

[35] ‘tDOM’. Accessed: May 07, 2024. [Online]. Available: https://wiki.tcl-lang.org/page/tDOM

[36] ‘Strategic Research and Innovation Agenda : Digital European Sky’.