Journal of Air Transport Management 102 (2022) 102223

Contents lists available at ScienceDirect

Journal of Air Transport Management

journal homepage: www.elsevier.com/locate/jairtraman

An evaluation of practitioners' perceptions of a security risk assessment methodology in air traffic management projects ☆

Karin Bernsmed [a,*], Guillaume Bour [a], Martin Lundgren [b], Erik Bergström [c]

[a] SINTEF Digital, Trondheim, Norway
[b] Luleå University of Technology, Luleå, Sweden
[c] Jönköping University, Jönköping, Sweden

ARTICLE INFO

Keywords:
Information security
Cyber security
Security risk assessment
Air Traffic Management
SESAR
SecRAM

ABSTRACT

Cyber security is a key enabler for safe Air Traffic Management (ATM). This paper presents results from an empirical study, in which we have investigated and evaluated the use of the Security Risk Assessment Methodology for SESAR (SecRAM) in European ATM research and development projects. The study was performed with the intention to find and document common issues and aspects that could be improved in the methodology. The results from the study reveal that while most of the practitioners had a positive perception of the methodology itself, they were less satisfied with the process of applying it in their projects. Based on the results, we provide a number of recommendations, which aim to improve the security risk assessment process in the ATM domain.

1. Introduction

Cyber security risk management is about reducing the risk of organizations' operation and use of information systems to an acceptable level (Whitman and Mattord, 2014). However, as information systems become increasingly more interconnected and complex, risks towards these systems are likewise becoming more complex (Chivers et al., 2009). Perhaps even more so in the evolving nature of aviation security, which has traditionally focused on aircraft security and non-dependent ground infrastructure security (Asgari et al., 2017). However, increased dependencies in the development of e.g., on-board platforms for integrated aircraft communication, electricity, energy, positioning and satellite systems have created complexities that, similarly, could open up Air Traffic Management (ATM) systems to new types of security related challenges and risks (Asgari et al., 2016; Bergomi et al., 2013).

ATM systems are crucial to aviation safety, and serves to ensure adequate separation of aircraft from each another and from objects on the ground (Nie et al., 2009). The infrastructure of and the ATM systems themselves must therefore undergo several validation cycles to ensure technical readiness levels and safety requirements (Stelkens-Kobsch et al., 2017). While such safety procedures for the design, implementation, and operation of ATM systems are well established, there has long been an absent of an equivalent cyber security focused procedure (Stelkens-Kobsch et al., 2017).

Wrongfully blocking, intercepting, or manipulating information related to ATM systems, or accessing them without proper authorization to do so, could pose severe risks to flight safety. As such, security requirements to ensure confidentiality and prevent unauthorized disclosure, to ensure integrity and prevent improper or malicious modification, and to ensure availability of information when needed, becomes relevant to ensure not only ATM systems security, but also safety of human lives (Asgari et al., 2016, 2018). The identification and management of cyber security risks towards ATM systems is therefore not only necessary to maintain over time, but also to include already during the overall design, implementation, and operation of the individual ATM systems (Stelkens-Kobsch et al., 2017).

Methodologically sound assessments of cyber security related risks are therefore crucial to ensure systems security, and that possible implications thereof are planned and prepared for (Baskerville et al., 2018). Cyber security risk management is commonly described as the systematic process to identify and protect the confidentiality, integrity, and availability of information assets to reach an acceptable level of risk (Chivers et al., 2009; Whitman and Mattord, 2014). Different

☆ This project has received funding from the SESAR JU under the EU H2020 research and innovation programme under grant agreement 731765. The work has also been supported by the Science of Security in Agile Software Development (SoS-Agile) project, funded by the Research Council of Norway (grant number 247678).

* Corresponding author.
E-mail addresses: karin.bernsmed@sintef.no (K. Bernsmed), guillaume.bour@sintef.no (G. Bour), martin.lundgren@ltu.se (M. Lundgren), erik.bergstrom@ju.se (E. Bergström).

https://doi.org/10.1016/j.jairtraman.2022.102223
Received 6 August 2020; Received in revised form 1 December 2021; Accepted 24 April 2022
Available online 20 May 2022

approaches to cyber security risk management have been proposed for different industries and contexts. Cyber security risk management processes such as ISO/IEC 27005 (ISO/IEC 27005, 2018a), NIST SP 800-30 (NIST SP 800-30, 2012), or OCTAVE-Allegro (Caralli et al., 2007) are but a few examples of industry standards, each developed to meets its own particular needs and objectives (Silva and Jacob, 2018). For example, in response to the criticality of cyber security in ATM systems, efforts towards establishing ATM specific cyber security risk management processes have been made, such as the Security Risk Assessment Methodology for SESAR (SecRAM) (Asgari et al., 2017; Bergomi et al., 2013).

Although there exist a lot of literature on different cyber security risk management processes, there is, however, a noticeable absence of empirical studies on the actual establishment and implementation of cyber security risk management practices within cyber security (Cram et al., 2019; Hsu, 2009; Kotulic and Clark, 2004; Webb et al., 2014), and ATM security in particular (Asgari et al., 2017). But there are studies that suggest such empirical insights are needed. For example, earlier studies have focused on the applicability of existing cyber security risk management approaches within the context of aviation and ATM systems (Bergomi et al., 2013), and how there is a need to establish new adaptations and procedures in ATM to better bridge security and operations (Asgari et al., 2017), whereas others have suggested the need for using cyber security risk management experts' knowledge to validate the effectiveness of security controls in reducing the risks in ATM systems (Asgari et al., 2016).

In this study, therefore, we further this research stream by investigating practical implications and lessons learned from studying how ATM specific cyber security risk management approaches (i.e., SecRAM) have been implemented in practice, thereby addressing the research question: *What issues are there inhibiting the adoption of security risk assessment methodologies in ATM*? To shed some light upon this matter, we decided to perform a qualitative study based on semi-structured interviews. In total 21 in-depth interviews were performed in the fall of 2019 and the resulting interview data was coded and analyzed during the winter and spring of 2019–2020. As will be shown in this paper, the results from the study propose areas of practical recommendations.

This paper is organized as follows. Section 2 describes the background of our study, including related work. Section 3 outlines the research approach that has been used in the study. In Section 4, 5 and 6 we present the results. Our proposed improvements, which are based on the results, are presented in Section 7. Finally, Sections 8 and 9 include a discussion and the conclusions of our work.

2. Background

2.1. The digital transformation of ATM

In Europe, the digital transformation of ATM services and technologies is driven by the Single European Sky ATM Research Joint Undertaking (SESAR JU) (Anon, 2020b), which is a public–private partnership that aims to modernize European ATM through defining, developing and delivering new or improved technologies and procedures. The vision of SESAR builds of the concept of trajectory-based operations, which will revolutionize ATM by allowing aircraft to fly their preferred trajectories without being constrained by today's sector-based airspace configurations. The vision will be enabled by an increase in the level of information sharing and automation, the implementation of virtualization technologies and the use of standardized and interoperable technologies. The changes will be implemented across the entire ATM ecosystem, offering improvements to every stage of the flight; from planning, pre-departure, taxi-out and take-off, through the climb, cruise and descent, to landing, taxi-in and post-flight operations.

In SESAR, the ATM research and development activities is being executed by the so-called SESAR solutions (Anon, 2017b), which are projects that work on new or improved operational procedures or technologies. The SESAR solutions are categorized according to four thematic areas: Airports, Network, Air Traffic Services and Technology Enablers, spanning through all the phases of the flight as mentioned above. The solutions are, however, of different maturity levels; some are more mature and have already been implemented and deployed locally in Europe and/or world-wide, while others are still in their research and/or validation phase. A common factor of the solutions though is that they are all being developed by consortiums consisting of a wide variety of European ATM industry partners and research organizations.

To monitor and ensure progress, the SESAR solutions go through different development phases. Each phase ends with a gate, in which the maturity of the solution is assessed. The gate needs to be approved before the solution is allowed to move into the next phase. The phases that have been defined are (Anon, 2018):

- V0–V1 validation, which includes topics that are investigated in the SESAR Exploratory Research projects. These projects are working on solutions with low maturity levels, typically TRL1–TRL2,[1]
- V1 validation, which includes solutions with TRL2-3,
- V2 validation, which includes solutions with TRL4-5,
- V3 validation, which includes solutions with TRL6, and
- Very Large Demonstration (VLD), which includes solutions aiming towards TRL7 and above.

2.2. ATM and cyber security

Safety is, and has always been, a top priority of ATM. During the last few years, cyber security has also been gaining increased interest in the aviation community. The vision of the future ATM implies an increased connectivity and integration of systems and services, enabling actors such as Air Navigation Service Providers (ANSPs), airlines, airports and aircraft 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 the use of proprietary standards and a lack of network connectivity. Further, interoperability implies 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, in particular when COTS software is integrated with other software products to create new composite services or systems-of-system (Ellison and Woody, 2010).

In recent years, we have also seen an increased interest in ATM security from the hacker community. For example, "white-hat" security researchers have on several occasions demonstrated that it is both easy and inexpensive to manipulate existing air-to-ground safety-related data transmission protocols, such as ADS-B (Costin and Francillon, 2012; Kelly, 2012; The International Federation of Air Line Pilots, 2013). In 2014, IOActive (Santamarta, 2014) conducted tests on Satellite Communication (SATCOM) firmware from a number of different vendors and found multiple vulnerabilities including hardcoded credentials, undocumented protocols, insecure protocols, backdoors, and weak password reset mechanisms. 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

While safety and security have historically been considered as separate disciplines by the ATM community, it is now generally accepted that security risks can also have safety implications (see e.g., Sampigethaya et al., 2011 and Chivers and Hird, 2013). Cyber security has therefore been a key concern in the SESAR programme (Johnson, 2015; Casado et al., 2016) and is currently being managed through a risk-based approach, which we will describe in the next subsection.

[1] TRL: Technology Readiness Levels.

Table 1
The main steps of SecRAM. Column 2–4 show which steps that are mandatory for the different maturity levels of the prioritized solutions. Column 5 shows the security classification of the produced results from the different steps.

SecRAM step	V1	V2	V3 & VLD	Confidentiality level
Scoping and assumptions	Initialize	Update	Update	Low
Identification of primary assets	Initialize	Update	Update	Low
Impact assessment of primary assets	Initialize	Update	Update	Medium
Identification and valuation of supporting assets		Initialize	Update	Medium
Identification of vulnerabilities and threats		Initialize	Update	High
Identification of likely threat combinations		Initialize	Update	High
Identification of controls		Initialize	Update	Medium
Impact on Primary Assets after implementation of Controls		Initialize	Update	Medium
Likelihood of impact on Primary Assets after implementation of Controls		Initialize	Update	Medium
Residual risk after implementation of controls		Initialize	Update	Medium
Capturing controls as security requirements		Initialize	Update	Low

2.3. The SecRAM methodology

SecRAM (Anon, 2017a) is a methodology for assessing cyber security risks and deriving security requirements for ATM projects. In Europe, the method provides the means for the SESAR solutions to demonstrate that they have adequately addressed cyber security in their research and development phases, hence ensuring that the outcome will be sufficiently secure to address the relevant cyber security threats. SecRAM is based on ISO/IEC 27005 (ISO/IEC 27005, 2018b), which is an international standard for information security risk management, but has been specifically adapted to fit the context of ATM. SecRAM includes detailed guidelines for the application of the methodology, templates for documenting and sharing the results and pre-populated catalogs with lists of assets, threats and vulnerabilities and security controls that are relevant for ATM solutions.

In SESAR, performing a security risk assessment in accordance to SecRAM has, until just recently, been mandatory for those solutions that have been categorized as "security prioritized",[2] however, the maturity level of the solution dictates which of the steps in SecRAM should be completed and when. An overview over what needs to be done at which maturity level is provided in Table 1. For example, as can be seen from the table, a prioritized solution that is in a V1 development phase should perform a first version of the three first steps (Scoping and assumptions, Identification of primary assets, and Impact assessment of primary assets), while a prioritized SESAR solution that is in a V2 development phase must produce a new version of those first three steps, (that they initialized in V1) and perform a first version of all the remaining steps.

In SESAR, the results of SecRAM are documented using three different templates, with different security classifications. Three different risk levels for classified material have been defined: green (low risk) for material that can be shared but not published or posted on the Internet, amber (medium risk) for material that has a limited distribution, on a need to know basis, and red (high risk) for material that is restricted to those present at the meeting where the material was produced, or to named recipients, only. The rightmost column in Table 1 indicates what security classification the material produced in the different steps will have. An important implication of this is that, from a legal perspective, management of the restricted material has to comply with national regulation of all of our involved members and/or international law, as well as with H2020 rules (we will refer to this as the "information sharing issue" in this paper). Another, more practical, implication is that the results that are documented using these three different templates will not necessarily appear in "chronological order". For example, a recipient of a "green" report, which is part of a full SecRAM analysis, will only be able to read the results from the first two steps and the last step.

[2] SecRAM is also recommended for non-prioritized SESAR solutions, however, most of the steps are then stated to be optional.

SecRAM was initially developed by Eurocontrol and released in 2008 (Eurocontrol, 2018). Since then, it has been used to assess cyber security risks in a number of ATM projects, including the prototypes developed in the GAMMA project (Anon, 2020a) in 2013–2017 and the SESAR Wave 1 solutions in 2016–2019. In 2012 the methodology was updated and refined (SESAR Project 16.02.03, 2012), and in 2013 it was extended with the Minimum Set of Security Controls (MSSC) (SESAR Project 16.02.03, 2013a), which consists of a set of baseline security measures that each ATM organization should consider for implementation. In 2017, the methodology was completed with a supplementary guidance material (SESAR Project 16.02.03, 2013b), including what we in this paper will refer to as "the catalogs", which is an inventory of commonly used primary and supporting assets in ATM, relevant threats and vulnerabilities as well as the MSSC mentioned above, documented in an MS Excel file (Anon, 2017b). The current version of the methodology is SecRAM 2.0 (Anon, 2017a). An overview over SecRAM 2.0 is provide in Fig. 1.

2.4. Related work

The introduction of SecRAM as a framework for addressing security in ATM is described in Hawley et al. (2014). Even though this framework is the recommended approach to identify and manage cyber security risks in European ATM projects, it is not the only methodology that is available for ATM projects. For example, the EUROCAE ED-203 standard (Anon, 2015b) is commonly used by, for example Airbus, to assess risks in airborne systems. Further, ISO/IEC 27005 (ISO/IEC 27005, 2018b), on which SecRAM is based, is both well-known and appreciated by cyber security experts in the European ATM domain. Finally, the Spanish methodology MARGERIT (Anon, 2020c) is well-known and commonly applied in the ATM organizations located in southern Europe. The European Union Agency for Cybersecurity (ENISA) has compiled an inventory of risk management/risk assessment methods commonly applied in Europe (see ENISA, 2020), however, as far as we are aware, very few of these have been applied in the ATM domain.

In 2014, for example, the EMFASE project created and validated an empirical framework for the evaluation, comparison and ranking of security risk assessment methodologies for the ATM domain Massacci et al. (2014). The methodology delivered by this project can be used to quantitatively evaluate the efficacy of the methodology. An initial evaluation of the proposed framework showed that participants better perceive graphical methods for security risk assessment. In addition, the use of domain-specific catalogues of threats and security controls seems to have a significant effect on the perceived usefulness of the methods (Labunets et al., 2014). To the best of our knowledge there is no previous study that investigates, in a systematic manner, how cyber security risk is being managed in ATM projects. The exception is an experience report from a single project, which was published by the GAMMA consortium in 2013 (see Anon (0000a)), but this paper focused on the quality of the results from applying the process, rather than on the process itself.

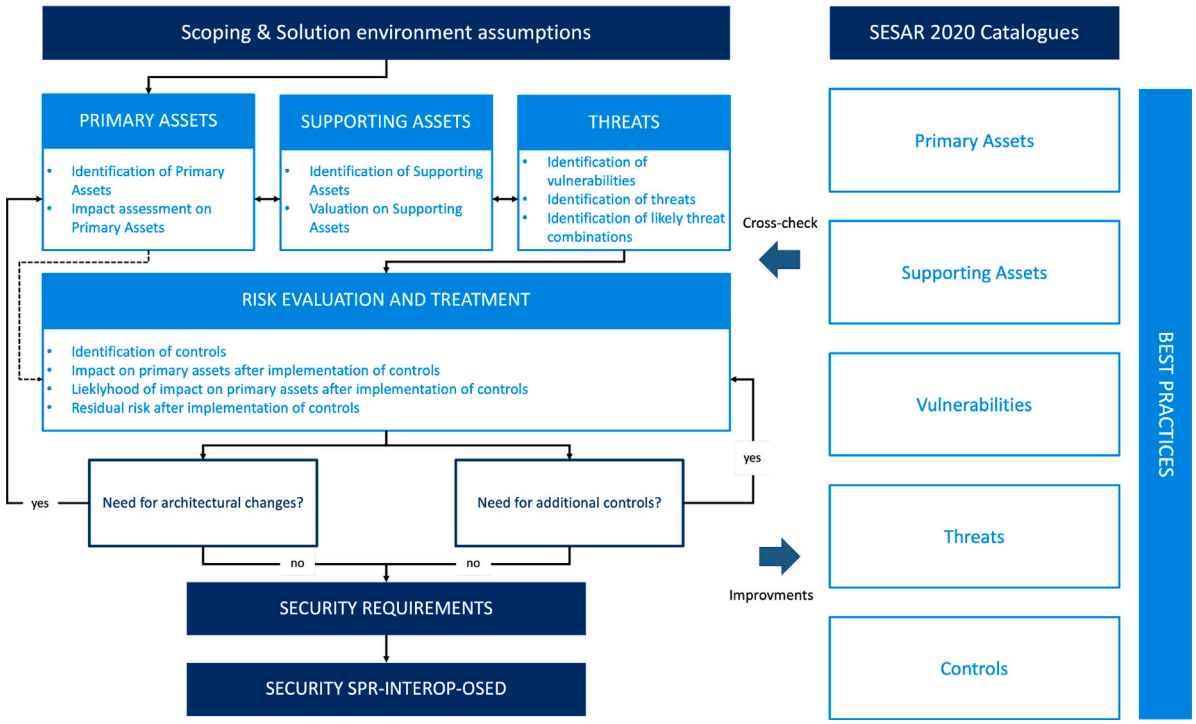

Fig. 1. An overview over SecRAM 2.0.
Source: Adapted from Anon (2017a).

However, relevant research can be found in other areas of cyber security similar to ATM, in the sense of operational technology and the potential hazardous impact of threats. Cyber security related to railway control-, automotive-, and healthcare systems are but a few examples. While information systems and related operational technology becomes increasingly interconnected, safety analysis and assessment frequently remain with people (e.g., software developers and system owners) who are not necessarily professional safety analysts (Stålhane and Sindre, 2014). While there exist safety standards that outline specific criteria that must be fulfilled, these criteria must however be understood and met in order to reach compliance. In a study on to better the understanding of safety compliance needs, de la Vara et al. (2020) was able to show that the use of models could improve the understanding of relationships between different concepts of safety standards. Human factors and abilities therefore play an important role in interpreting the inherent complexity of cyber security, but could be enhanced with the help of tools, e.g., models, to better clarify risks, concretize threats and security controls, or provide context to aid the overall assessment.

For example, Stålhane and Sindre's (Stålhane and Sindre, 2014) study compared the use of system diagrams against textual use cases in finding potential hazards and concluded that textual use cases could be beneficial as it often include not just system parts but system actions as well, thereby providing additional context. However, too detailed context could become inefficient. The level of granularity in different areas of cyber security risk assessment has been the topic of some discussion. Some scholars have suggested that high of a granularity of assets, although giving a more precise view of what to protect, often becomes too complex to manage over time, and that a system level granularity could make it easier to manage (Shameli-Sendi et al., 2016). Whereas others, such as Tuma and Scandariato Tuma and Scandariato (2018), have illustrated the opposite with regard to threat modeling. Tuma and Scandariato Tuma and Scandariato (2018) studied the effectiveness—in terms of the difference between benefits (number of threats) and cost (performance of analysis)—in using Microsoft's threat modeling tool, STRIDE, per system or per system component. The study observed better result when STRIDE was applied on a per system component level, suggesting that the per system level created larger and more complex models.

Other areas within cyber security risk management that have long been described as a complex and time consuming process is the identification of possible threats and selection of security controls (Montesino and Fenz, 2011; Roy et al., 2021). This has led to the development of various tools in the form of e.g., checklist and catalogues that list possible threats and security controls to aid the identification. On the other hand, such approaches have received scholarly criticism for limiting the perspectives of possible threats (Shedden et al., 2010), as some of which might only occur in practice and specific contexts (McEvoy and Kowalski, 2019). Furthermore, de Gramatica et al. (2015) and Labunets et al. (2015) found in their studies little difference in actual efficiency when conducting security risk assessment armed with catalogues of physical, information and procedural threats and preventative as well as responsive security controls to mitigate each threat. de Gramatica et al. (2015) studied the use of catalogues to identify cyber security threats and controls within the ATM context and found that people with the help of catalogues together with some prior security knowledge could identify threats and controls of the same quality as did security experts without the aid of such catalogues. Labunets et al. (2015) study found supporting results in their study that focused solely on security novices. However, de Gramatica et al. (2015) result did suggest that using catalogues could be beneficial in other aspects, like lowering the potential language barrier that can occur in cyber security (Bergström et al., 2019; Bergström and Lundgren, 2019), by providing a shared vocabulary. Other scholars, such as Labunets et al. (2017), have addressed additional aspects that could be perceived as barriers to risk assessment, such as the difference in efficiency between graphical or tabular methods. In their study, Labunets et al. (2017) found no evidence of superiority over any of the two cyber security risk management methods.

3. Research method

In our study, we sought to extract in-depth information on how the practitioners had perceived the application of SecRAM in their

projects. We, therefore, chose a qualitative research method based on a selected set of informants, which enabled us to perform a rich and detailed analysis of the gathered data. Further, since we wanted to derive patterns from our observations rather than evaluating existing hypotheses, we used an inductive research approach (Oates, 2005a).

3.1. Research approach

The focus of this paper is to investigate practical implications and lessons learned from studying how ATM-specific cyber security risk management approaches such as SecRAM have been implemented in practice. When practice is to be investigated, are there multiple qualitative approaches to how data collection can be performed, such as interviews or ethnographic studies. A qualitative approach implies that statistical generalizations are not sought after, and hence we opted for saturation of the chosen topic, which is a viable approach in such cases (Mason, 2002). In this study, interviews and document collection have been selected as data collection techniques. Interviews are a well-known and powerful instrument for gathering data in qualitative research (Oates, 2005b).

The interviews were performed as in-depth semi-structured interviews, which are interviews that are driven by open questions, have a limited degree of structure, and tend to focus on specific situations and experiences made by the respondents (Cassell and Symon, 2004). To be able elicit more in-depth knowledge on the respondents' experiences of applying SecRAM, the laddering technique was used (Reynolds and Gutman, 1988). In laddering, an interview guide with a set of open-ended questions is prepared, and the respondent is repeatedly asked "why" questions based on the respondents' answers. Doing so makes it possible *"to get below the respondent's surface reasons and rationalizations to discover the more fundamental reasons underlying the respondent's perceptions and behavior."* (Reynolds and Gutman, 1988, pp. 14). Another critical component in laddering is setting up an interviewing environment so that the respondents do not feel threatened and are thus willing to be introspective and look for the underlying motivations behind their perceptions (Reynolds and Gutman, 1988). In order to do so, one of the researchers had the leading role in all of the interviews, asking most of the questions while the other researchers were mostly only listening in. Questions that arose during the interviews were, for instance, sent electronically to the leading interviewer not to interrupt and remind the respondent of their presence. This was possible due to the use of the GoToMeeting tool (The International Federation of Air Line Pilots, 2013). The use of an online tool for performing the interviews also enabled electronic data collection from all over Europe and participation from the whole research team.

3.2. Data collection

Document collection of SecRAM was initiated as the first data collection activity. A total of 7 documents (Anon, 2017c,a,b; SESAR Project 16.02.03, 2013a; Anon, 0000b,c,d), containing in total of 120 pages, were collected in this effort. These documents describe how the methodology is supposed to be applied and hence crucial for being able to develop an interview guide. The interviews, on the other hand, inform on how the methodology is applied and perceived in practice. In addition, the current ISO/IEC 27005 (ISO/IEC 27005, 2018b) standard was used as a central reference, as SecRAM is based on it. An interview guide consisting of three parts was constructed. The first part of the interview guide was about demographics to better understand the respondent's background, the experience of working with cyber security in general, and the experience of working with SecRAM. Questions asked in this part were, for example, *"Have you been working with other methodologies?"* and *"How does the security-related work you do fit into your day-to-day work?"*

The next part focused on SecRAM as a methodology and the tasks it consists of. Here broader questions such as *"What would you say your work entail?"* and *"What could have been made more efficient?"* were asked to capture how the respondent works with the methodology in practice. The aim was to broadly capture if the steps as described in SecRAM were followed, such as the identification of primary and secondary assets, identification of threats, vulnerabilities, the risk evaluation and treatment, and the specification of security requirements and security controls. There are several indications that the rational and sequential relation between the activities described in the literature is not as rational and sequential in practice. For example, Parker (2007) describes that the activities can be performed in a different order or in parallel, and Coles-Kemp (2009) questions how the activities interact in practice.

The third part of the interview guide was based on the answers provided, and by using the laddering technique, it was possible to penetrate different tasks in SecRAM depending on the respondent's background. In this part, the questions were, for example, formulated as *"How did you perceive using the catalogs?"* and *"How did you perceive the division of assets into primary and secondary assets?"* Here, several literature streams contributed to the interview guide's development as several activities were in focus. For the questions on assets, we drew from many of the well-described issues, such as the difficulty in performing the valuation (Fenz et al., 2014; Wangen et al., 2018), and deciding on the granularity of assets (Shedden et al., 2016; Fibikova and Müller, 2011). For the questions on the usage of the catalogs, we drew from literature discussing the impact of catalog usage (de Gramatica et al., 2015; Labunets et al., 2015).

The laddering questions used throughout the interviews were, for example, *"Could you describe more?"*, *"Could you give an example?"*, *"Could you elaborate a bit more on how you mean?"*and *"Why do you think that?"*

It is generally considered extremely difficult to collect data in the security risk assessment field (Baskerville et al., 2018; Cram et al., 2019; Kotulic and Clark, 2004). In an area where critical infrastructure such as ATM is in focus, it is arguably even more difficult. Despite this, 21 interviews were performed. All the interviewees had hands-on experience applying SecRAM to assess the security risks of European ATM research and development projects. A majority of the interviewees had several years of experience in applying the methodology. The interviewees came from organizations all across Europe and were selected for participation mainly through recommendations from the cyber security experts in the SESAR transversal project PJ19 CI ("Content Integration") (Anon, 2020e).

All the interviews lasted approximately one hour. The audio files from the interviews were transcribed by a research assistant. The transcriptions were then reviewed and cross-checked against the original audio file by one of the researchers.

3.3. Data coding and analysis

The analysis followed the coding recommendations provided by Saldaña (2015), who advocates that data should be coded in at least two cycles. For the first cycle, a structural coding approach was applied. According to Saldaña (2015), it is an appropriate approach when having data from multiple semi-structured interview transcripts. During the first cycle, one of the researchers coded all the 21 transcriptions and made an initial categorization of the data to examine comparable segments' commonalities, differences, and relationships. In the second cycle, another researcher from the core team re-applied and refined the structural coding approach from the first cycle. Finally, the coding from the second cycle was reviewed by the first researcher to ensure that there was consistency in the coded data. All coding in the first and the second cycle were done using the software Nvivo (Anon, 2020d). The result of the coding cycles was a 3-level code-book. We were then able to use the analysis tool embedded in Nvivo to query our data.

When coding the interview data, it quickly became clear that there was a distinction between the interviewees' perceptions of the methodology itself, and their perceptions of *the process of applying it* in their

Table 2
Interviewees participating in our study (ATM project).

Type of ATM project	Number of interviewees
SESAR Wave 1	15
GAMMA	4
SESAR-1	1
Other	1

Table 3
Interviewees participating in our study (security experience).

Previous security experience	Number of interviewees
No prior experience	8
Some experience (1–3 years)	7
Experienced (more than 3 years)	6

projects. Thus, the codebook we obtained from the coding was divided in two main sections: "Perceptions of the methodology" and "Perceptions of the process". Each of these two sections were divided in four categories, where the first two represented the perceived positive and negative aspects. We also added a third node for representing what they considered to be a problem induced by one or more of the negative aspects, and a fourth node to represent what were their suggested improvements. Finally, we added a fifth node to the "Perceptions of the process" section, to represent how the interviewees had organized their work when they applied the methodology.

- Perceptions of the methodology
  - Positive aspects
  - Negative aspects
  - Problems induced by the negative aspects
  - Proposed improvements
- Perceptions of the process
  - Positive aspects
  - Negative aspects
  - Problems induced by the negative aspects
  - Proposed improvements
  - Work organization

The resulting code book hence consisted of these two layers, plus an additional sub-layer with a much more detailed coding representing more specific statements that we found in the interview data.

In addition to the 3-level code book, we also tagged all the transcribed interview data files with information about the type of ATM project that the interviewee had worked in when applying SecRAM and the previous security experience of the interviewee at the time of performing SecRAM. An overview over these data is provided in Tables 2 and 3.

As can be seen from Table 2, 15 of the 21 interviewees had experience with SecRAM from the SESAR Wave 1 programme (which run between 2016–2019). We also interviewed four persons who had applied it as part of the GAMMA project (2013–2017), one person from SESAR-1 (2012–2013), and finally one person whose work had been funded by another, non-identified, source.

As can be seen from Table 3, eight of the interviewees claimed they had no prior experience with cyber security at all when they started to work with SecRAM. Seven of the interviewees had "some experience", meaning up to three years, and six of the interviews were considered to be "very experienced" in security, some of them having up to 20 years of previous relevant experience.

3.4. Ethics statement

All research projects need to address and consider ethical issues. This is especially true when research is performed in a domain where much potential harm can be caused and where the study is driven by human and organizational participation. Ethical considerations have traditionally not been a central issue in interpretative research such as interview studies (Walsham, 2006), but it has become increasingly important. This study has followed a strict protocol to consider ethical aspects throughout the research process to protect the participants and their respective organizations. There are several alternatives to ethical protocols, and in this work, Thornhill et al. (2016) have been used as a guide since they offer advice for all research stages, from planning to publication. Some of the more central ethical issues are relating to the privacy rights of the interviewees. Such rights include the right not to participate, the right to withdraw, the right to give informed consent, and the right to confidentiality and anonymity (Oates, 2005a; Thornhill et al., 2016). In this study the interviewees were informed about their rights via e-mail already at first contact. Each interview started with a reminder of their rights, including asking explicitly for consent to record the interview session. Regarding the collected data, all the interview transcripts have been anonymized and all the recorded audio files have been deleted.[3]

Table 4
The interviewees' overall perceptions of the methodology.

Node	Discussed by
Positive aspects of the methodology	90%
Negative aspects of the methodology	95%
Problems induced by the negative aspects	24%
Proposed improvements	76%

3.5. How to interpret the results

In this paper, the results from the analysis of the interview data in our study is to a large extent presented in the form of tables. To avoid misunderstandings, a further explanation on how to interpret the numbers in these tables is needed.

In all of the tables in Section 4–5, the first column "Node" is consistently used to indicate what category in the codebook that has been queried. The subsequent columns are then used to indicate how many of the interviewees (in percent) discussed this particular topic during their interview. Hence, the tables do not tell how many times, or how much, an interviewee spoke about a particular topic, but they indicate how many of the interviewees who had opinions about, or said something that would confirm, this particular topic.

In the three next sections, we will present the results that we obtained when we coded and analyzed the interview data.

4. Results from the interviews: Perceptions of the methodology

This section presents the interviewees' perceptions of the different aspects of the SecRAM methodology itself.

4.1. General overview

Table 4 provides a general overview over the interviewees' overall contribution to the interview data that represents their perceptions of the methodology. As can be seen from the table, 90% of the interviewees spoke about positive aspects of the methodology and 95% spoke about negative aspects of the methodology. 24% also highlighted problems that were induced by the negative aspects that they had mentioned. Finally, 76% of the interviewees gave at least one suggestion on how to improve the methodology.

[3] The processing of personal data in this project has been registered at and approved by the Norwegian Center for Research Data (NSD). See https://nsd.no/nsd/english/index.html.

Table 5
The interviewees' overall contribution to each subcategory, given their experience working with security.

Node	Experienced (6)	Some experience (7)	No prior experience (8)
Positive aspects of the methodology	100%	100%	75%
Negative aspects of the methodology	100%	100%	88%
Problems induced by the negative aspects	50%	14%	13%
Proposed improvements	100%	86%	50%

Table 5 is a refinement of the interviewees' overall contribution to their perceptions of the methodology, taking their previous experience in security into account. Looking at the table, we note that the more experience the interviewees had, the more they contributed to each subcategory. It is also interesting to see that 50% of the interviewees who were "experienced", also discussed problems that could be induced by the negative aspects of the methodology. In addition, all of the experienced interviewees proposed improvements to the methodology. This indicates that people with more experience are more willing to take a step back and have a critical mind on the methodology and the quality of the results that they have produced. However, we can also see that the people with less experience still raised a lot of points related to the methodology, however these were mainly related to its positive and negative sides.

From the interview data, it seems that the interviewees did appreciate SecRAM. As shown in Tables 4 and 5, even though most of them said something negative about the methodology, they almost always also said something positive, regardless of their background. Also, as a general feeling when discussing with the interviewees, it was clear that even though they had experienced some pitfalls that they wanted to highlight, they really did appreciate the methodology in itself.

4.2. Positive aspects of the methodology

As shown in Table 6, 76% of the interviewees said that they appreciated the guidance material of the SecRAM. They considered the guidance to be clear and logic, thereby providing a good starting point for working with security for people who do not have any prior experience in this field. For instance, one interviewee explained that he "*find[s] the methodology has a quite nice description of what has to be done and how to do it.*" Some of them also highlighted that the guidance material made it easier to come up with relevant countermeasures for their systems: "*I think the easiest part must have been to actually be coming up with countermeasures after having defined the threats.*" Further, 71% of the interviewees considered the catalogs to be a positive aspect of SecRAM. They explained that they are rich and that they ease the process of doing risk assessment. Another positive aspect of the methodology, which was mentioned by several of the interviewees, were the compliance with the ISO/IEC 27005 standard. Especially, the interviewees appreciated the fact that SecRAM is a lighter version and an ATM-focused adaptation of the ISO standard, which they said makes it easier to evaluate the risks: "*I think that the main advantage of the SecRAM methodology is that it is not so huge like the ISO 27005, because the other methodologies are really a lot of topic to be be addressed on the managerial part, the work to be done is very, very huge. The SecRAM methodology will give us the same results in an easiest way.*" Finally, some of the interviewees highlighted the fact that the scope of SecRAM is broader than other methodologies when it comes to the impact areas as a positive aspect. They also appreciated that it is high-level and will thus fit solutions with different technology readiness levels (TRLs).

4.3. Positive aspects of the methodology, given the interviewees' previous experience working with security

When digging deeper into the interview data, it became clear that the interviewees had different perceptions of the methodology, based on their previous experience working with security. As shown in Table 7, the interviewees with "some experience" were the ones who had the most positive perceptions of SecRAM. In this table, it can also be observed that it was only the "experienced" and the interviewees with "some experience" in security who highlighted the scope of the methodology, and the fact that it is compliant with the ISO/IEC 27005 standard, as positive aspects. Another result, which was more surprising, is that interviewees who had "no prior experience" working with security were also the ones who spoke the least about the advantages of the catalogs. Only 50% of them perceived these as a positive aspect, versus 67% and 100% for the "experienced" and "some experience" groups, respectively. This was unexpected, because the catalogs are intended to ease the application of the methodology, especially for people who have no prior experience with security. Please note that, since the number of interviewees contribution to the data in each column of Table 7 is relatively small (6, 7 and 8, respectively), it is not possible to generalize from these results.

Table 6
What the interviewees liked the most about the methodology.

Node	Discussed by
The guidance material	76%
The catalogs	71%
ISO/IEC 27005 compliance	38%
Scope of the methodology	19%

4.4. Negative aspects of the methodology

As can be seen in Table 8, what the interviewees perceived as negative with the methodology varied a lot. As shown in this table, the most commonly mentioned aspect was that they thought SecRAM contains (at least one) hard step (57%). They also said that the methodology contains unnecessary steps (52%), they were unhappy with the lack of a tool (48%), they disliked things about the catalogs (43%) and they had a hard time understanding the methodology overall (38%). Other perceived negative aspects were that SecRAM lacks one or more steps (33%) and that it is difficult to trust the results from the process (33%). Some also claimed that the methodology is not suited for all solutions (19%).

When looking at what the interviewees perceived to be negative aspects, taking their experience working with security into account, the results differed a lot. From Table 9, one can see that most of the interviewees who had experience working with security claimed that SecRAM contains unnecessary steps (83%). At the same time, this group of interviewees also pointed out that there are steps lacking in the methodology (68%). A majority of the experienced people also think that the SecRAM lacks a companion tool (68%).

Interviewees with some experience with security seemed to agree with the experienced people regarding the lack of a tool (71%) and that there are unnecessary steps in SecRAM (57%). However, the most important point for them, which was mentioned by 86% of the interviewees, was that there are hard steps in the methodology.

When it comes to people who had no prior experience with security at all, it seems that they struggled mostly with understanding the methodology (63%). They also thought that there are hard steps in the methodology (50%) and, to a smaller extent, that the catalogs were a problem (38%). Again, this was unexpected, because the catalogs are supposed to be of help. This point will be studied in more detail in Section 4.7.

Table 7
Positive aspects of the methodology, given the interviewees' previous experience working with security.

Node	Experienced (6)	Some experience (7)	No prior experience (8)
The guidance material	67%	86%	75%
The catalogs	67%	100%	50%
ISO/IEC 27005 compliance	50%	71%	0%
Scope of the methodology	33%	29%	0%

Table 8
Negative aspects of the methodology.

Node	Discussed by
Hard steps	57%
Unnecessary steps	52%
Lack of a tool	48%
The catalogs	43%
Understanding the methodology	38%
Missing steps	33%
Trustworthiness of results	33%
Not suited for all solutions	19%

4.5. Negative aspects, as perceived by the "experienced" group

In this section we analyze what problems were faced by the interviewees who were "experienced" working with security. As highlighted in Table 9, the experienced interviewees mostly criticized the presence of unnecessary steps and missing steps in SecRAM, and the lack of a tool. We will first have a look at what they are saying exactly, before outlining their proposed improvements. Note that the percentages that are discussed in the body text of the subsections below are marked with bold font in the table. Please note that, since there were only six interviewees in this group, it is not possible to generalize from their input.

4.5.1. Unnecessary steps

Of the interviewees in the "experienced" group, 83% said that there are steps in SecRAM that they considered to be unnecessary. One of the main points that they highlighted, was that they found SecRAM to be repetitive. They said that several different parts of the guidance material appear to be very similar and that it was hard not to repeat yourself when filing out the templates with the assessment results. According to them, they had to do a lot of copying and pasting of text between different parts of these documents, which made the job of working with SecRAM feel tedious.

Over-formalization was another issue that was pointed out by many of the interviewees in this group and as a result, they found the method to be cumbersome. As one interviewee explained it: *"85% of it [the methodology] is good, but maybe 15% which was added by the formalization of this method because it was done by people which did not actually use it in practice. So they did not have practical experience with it, and they over-formalized this method…"*

One step that seemed particularly "unnecessary" from the experienced interviewees' point of view was the identification of threats. For them, this task was too detailed and could be made much more straightforward. One of the interviewees had a particularly strong opinion on this, stating: *"There is a lot of effort wasted […] in describing threat agents and threat profiles. I told you already I was trained in the military and it really does not matter whether a journalist or a terrorist kicks me in the butt. The more I am kicked, the more I am kicked."* To him, what should be analyzed instead is what he referred to as the "threat path" in the system that is being assessed, rather than spending time and effort on describing the potential threat actors.

4.5.2. Missing steps

Of the interviewees in the "experienced" group, 68% thought that there were steps missing in SecRAM. As an example, one of the interviewees said that, even though he considered the methodology to be a quite complete and well-defined methodology, he thought it lacked a way to add a *"zone model with security functions"*, which he often used himself in security risk assessment activities as a way to model different domains ("private", "shared" and "public") and to model and visualize the interactions between the assets in each of these zones. Using such a model helped him to analyze threats and vulnerabilities on a much more detailed level. Mainly, he criticized the fact that SecRAM does not go enough into the details of the assessment.

Another interviewee also highlighted something that he saw as an advantage in another methodology, EBIOS (National Cybersecurity Agency of France (ANSSI), 2020), which is missing from SecRAM; a way to *"understand the risk from a global perspective"*. That means, not only being aware of the vulnerabilities in each component but also knowing what paths can be used by attackers along the whole chain of components.

Several other interviewees also said that *"SecRAM stops too early"*, meaning that it should go one step further and identify the security measures that will be necessary to mitigate the identified threats.[4] Several interviewees also claimed that the catalogs do not provide enough security measures, and that the work packages should have the opportunity to add their own security measures, which are more accurate regarding the context of the technologies that they assess.[5]

Another point that was raised by one of the interviewees, which applies not only to SecRAM but to all risk assessment methodologies, is the static nature of the assessment. He pointed out that, due to the rapid changing threat landscape and the dynamic nature of new technologies, any risk assessment will be outdated as soon as it is finished. To him, the re-assessment process is too long and does not fit the need anymore. He would therefore prefer to have a methodology for continuous monitoring and assessment of risks, which would help secure the system close to real-time.

4.5.3. Lack of a tool

Of the interviewees in the "experienced" group, 68% pointed out the lack of an accompanying tool as a major disadvantage in SecRAM. They explained that it is very difficult to keep track of all the assets when there are a lot in a solution. They also said that documenting the results manually using the three document templates was a tedious task, because of all the copying and pasting that has to be done. Some of them actually referred to this manual labor as a risk in itself, because important information could easily be forgotten or left out by mistake.

Further, they pointed out that it was hard to harmonize the information that they produced without a dedicated tool, in particular when several persons were working on the documents at the same time in different locations. Having to synchronize the documents afterwards lead not only to additional work load, but could also lead to mistakes and forgotten parts. One of them mentioned that *'it could have a lot of it software-based and not a bunch of Excel-sheets which you send around and… people are filling it in, and information is diverted and so on. So, it*

[4] It should be noted that these interviewees had only applied SecRAM to V1 solutions in the SESAR Wave 1 program, in which the last step "Capturing controls as security requirements" of the methodology was not required.

[5] It is worth noting that using other assets, vulnerabilities, threats, controls etc. than the ones that are pre-defined in the catalogs is already allowed in SecRAM. It is also possible to suggest changes and updates to the catalogs. This appeared, however, to be something that many of the interviewees in our study had misunderstood, or were not aware of.

Table 9
Negative aspects of the methodology, given the interviewees' previous experience working with security.

Node	Experienced (6)	Some experience (7)	No prior experience (8)
Hard steps	33%	**86%**	**50%**
Unnecessary steps	**83%**	**57%**	25%
Lack of a tool	**68%**	**71%**	13%
The catalogs	50%	43%	**38%**
Understanding the methodology	33%	14%	**63%**
Missing steps	**68%**	43%	0%
Trustworthiness of results	33%	43%	25%
Not suited for all solutions	50%	0%	13%

really would help if it's some kind of a software.[…] The problem is always the harmonization of the information." Some of the interviewees also mentioned that they did not feel confident with the results when they had to assign the numbers to likelihood and impact values manually; they wish they could have used a tool that would provide a more deterministic way of assessing the risks.

4.6. Negative aspects, as perceived by the "some experience" group

This section describes in more detail the three specific problems that were highlighted by the group of interviewees, who all had "some" prior experience working with security. As highlighted in Table 9, these were "Hard steps" (86%), "Lack of a tool" (71%) and "Unnecessary steps" (57%). We also outline their suggestions for improvements to the SecRAM methodology. Please note that, since there were only seven interviewees in this group, it is not possible to generalize from their input.

4.6.1. Hard steps

The group of interviewees with "Some experience" considered most of the steps in SecRAM to be difficult. One of the first problems they encountered was the definition of the assets, more specifically they were struggling to find the right granularity for the solution so that it would be understandable. In addition, defining the scope of the risk assessment has also been reported as being a difficult task by some.

Further, some interviewees found difficult to identify vulnerabilities in the systems they were assessing and to find relevant threat scenarios.

Risk evaluation, and residual risk evaluation, were two tasks seen as difficult, or at least subjective, by the interviewees with "some experience". They explained that the pre-defined scales used in SecRAM are not always a good fit. Impact assessment of the primary assets were pointed out as being particularly difficult by several of the interviewees in this group, especially for the impact areas where they felt that they did not have the required competence to make a correct judgment (assessing the regulatory impact was mentioned as an example by several of the interviewees). In addition to being difficult, some of the interviewees also stated that this task felt subjective, since "*there is no scientific way of assessing the impact*". Their feeling was that two people doing the same analysis could therefore easily end up with very different results.

4.6.2. Lack of a tool

Similarly to the "experienced" group, the interviewees with "some experience" also reported that the lack of a tool made it difficult to keep track of all the assets, threats scenarios, vulnerabilities, etc. when working with SecRAM. In addition to make the work more tedious, they also said that the lack of a tool can lead to accidental loss of data during the reporting process: "*working without a tool is difficult. It is difficult because you can miss some data.*" Some of the interviewees in this group made a comparison with another methodology called Magerit,[6] which they had good experience from. They explained that this methodology is similar to SecRAM, but that it has a accompanying tool (Pillar) that helps them keep track of the generated data. They also expressed dissatisfaction with the non-linearity way of documenting the results in the three different templates (low, medium and high risk material), an issue which they also attributed to the lack of a tool. During the interviews, some of the interviewees revealed that they had actually solved this problem themselves, by using their own version of an Excel based tool to document their results.

The interviewees with "some experience" also criticized the lack of an automatic way to link items from the catalogs, like primary and supporting assets, or even the countermeasures, through the different parts of the assessment. They felt like there was a lot of "mechanical operations" involved in doing the risk assessment, such as reporting values, which are also prone to errors. They also felt like this was an inefficient way of working, because they focused a lot on filling the templates, which takes the focus away from the actual security analysis: "*It [a tool] could automate some operations, and I could spend more effort on the analysis of the security aspects and not on the filling of the template.*" In addition, sometimes changing one value in the assessment would have a lot of impact on the rest of the analysis and they would therefore appreciate a tool to recompute everything automatically.

Finally, the interviewees with "some experience" also said that the lack of a tool prevented them from being able to easily reuse results that had already been produced in previous phases of SESAR, or in other projects who worked on similar solutions.

4.6.3. Unnecessary steps

Some of interviewees who had performed a full SecRAM analysis felt that the step of identification of likely threat combinations is not really useful, and the methodology should focus on more specific threats instead.

Several of the interviewees considered it unnecessary to apply the full methodology on all solutions, as some of them are still in an early stage of development and would only require a high level risk assessment. It also appeared that they felt like parts of the process are useless, since they already knew which assets are important and need protection. They felt that the resulting security controls and requirements are already known, and that they had to assess and report something that was already obvious. One interviewee reported for instance that "*in some cases this is quite obvious that there are some primary assets that are using some supporting assets. We know already that this is really important without doing any calculation and so on.*"

Finally, having to do an impact assessment for all of the assets in all of the seven impact areas felt very repetitive for some interviewees. Some of them even claimed that the impact assessment were not really useful at all.

4.7. Negative aspects, as perceived by the "no prior experience" group

In this section we present the three points interviewees from the group having "no prior experience working security" seem to have struggled the most with. According to Table 9, these points were "understanding the methodology" (63%), "hard steps" (50%) and "the catalogs" (38%). Please note that, since there were only eight interviewees in this group, it is not possible to generalize from their input.

[6] Magerit. Available at http://www.csi.map.es/csi/pg5m20.html.

4.7.1. Understanding the methodology

In general, it seemed like the interviewees who had no prior experience working with security struggled to understand the terminology used in SecRAM, at least in the beginning when they started to work with it. One point that was raised by several of the interviewees in this group was the difficulty of understanding the concept of an "asset", as this is a notion that is rarely used outside the security community. For instance one of the interviewee mentioned that "*the vocabulary was not so easy to understand. For example, a detail but… the term "asset" is not so used in other domains and there are many other examples where vocabulary and concepts are very specific, quite technical, and it was not so easy, coming from scratch in fact, to enter this domain.*" Many of them also struggled with the distinction between primary and supporting assets. Further, most of them had problems understanding what it meant to assess the impact of assets being compromised. According to them, the examples in the SecRAM documentation did not help, because they were too far away from the solutions that they were working on. Overall, they thought that getting started with the SecRAM was hard for people without prior experience or background in security.

Some of the interviewees in this group also raised the fact that, even though they had read the guidance documentation and believed they understood the methodology, they still struggled to understand what was asked from them in the different steps. More specifically, they would have preferred to have someone with experience in security to guide them through the process and ask them the right questions, especially when assessing the impact areas: "*I think it is in this activity, surely in every solution, we need to have some expert on the security aspect.*" They explained that afterwards, once they had completed the assessment, the SecRAM process is not that difficult, but that it can be quite frightening at the beginning when you do not have any experience.

Finally, it seemed like the interviewees in the "no prior experience" group struggled to understand the objectives of SecRAM and why it was important to do it in the first place. They say things like "*I worked for years in the research aspect in Air Traffic Control, and I never heard about security. So I'm not so sure it's really necessary, at least not in the research phase…*" This seemed to be particularly true for the interviewees who had applied it to operational solutions.

4.7.2. Hard steps

Even though it appeared like understanding the different steps of SecRAM and the examples in the guidance documentation was not that difficult for the interviewees in this group, applying it to their own solutions seemed to be more challenging. In particular, the interviewees had a hard time with the identification of vulnerabilities and threats, and to come up with relevant and realistic threat scenarios. Some of them also pointed out that doing a risk assessment of a single component only may be too restrictive, since you may then loose the overall picture. Further, according to the interviewees, impact assessment (in terms of legal, economic, branding, etc.) was a complex task and they did not feel confident that the values that they had selected were correct.

4.7.3. The catalogs

According to the interviewees in this group, the catalogs came out as being both messy and incomplete. They explained that there is a lot of redundancy in this very large inventory and it is not that simple to identify the assets that are part of their solutions. An interviewee explained that he "*felt there were not definitive documents at that time in fact. […] For example the tables that are in the SecRAM catalogues, there are some that are a bit fuzzy in fact, with some missing elements, with some elements that are strange in fact.*" Some interviewees also thought that, even though the catalogs could make it easier to choose assets, they can also be a constraint in case it is not possible to find an appropriate asset. [5]

Table 10
The interviewees' overall perceptions of the process.

Node	Discussed by
Positive aspects of the process	10%
Negative aspects of the process	71%
Problems induced by the negative aspects	48%
Proposed improvements	52%
Work organization	95%

4.8. Suggestions on improvements to the methodology

In addition to bringing up positive and negative aspects, the interviewees also contributed with proposals on how the methodology could be improved. The "top of the list"suggestion, which was highlighted by many of the interviewees, was to improve the SecRAM documentation (Anon, 2017a). Many of the interviewees wanted to have more examples in the guidance documentation, both real-life examples from the ATM domain and more simple examples, to better illustrate the concepts. As one of the interviewees pointed out: "*To help to understand, I made an exercise for myself, for my home-system. […] I tried to do SecRAM according to the guidance for my system at home. And that was very interesting […] after I did this exercise, I think I could say, I understood what is meant by the SecRAM.*"

Many of the interviewees also mentioned that some of the terminology could be better explained. They also requested better guidance on how much they were expected to do, considering the varying maturity levels (TRL) and special characteristics of their individual solutions.

More advanced suggestions on how the methodology could be improved were brought up by the interviewees from the "experienced" group. Several of them wanted to extend the guidance material with Excel sheets, which could include short scripts that would help assessing likelihood and impact values when analyzing risks. One of them even proposed "*an automatic mapping, from supporting assets to vulnerabilities and from vulnerabilities to threats and controls*", which he proposed could be re-used across solutions in order to improve consistency between different assessments.

Two of the interviewees in the "experienced" group, who had the role as security experts in several SESAR Wave 1 projects also wanted to change the scale for impact assessment, by extending it to 1–10 (instead of 1–5), in order to add more granularity to the different assessments.

Finally, a few of the interviewees also wanted more flexibility in the methodology, so that they could add the assets, vulnerabilities, threats etc, that are relevant for the contexts that they are working in. [5]

5. Results from the interviews: Perceptions of the process

In the previous section, we reported the interviewees perceptions of the SecRAM methodology itself. Now we will look at what they think about *the process of applying the methodology*. In this section, we will first study how the different projects organized themselves to work with SecRAM. Then we investigate which problems they encountered and what were the results of those problems. Finally, we report how they think the process can be improved.

5.1. General overview

Table 10 provides a general overview over the interviewees' overall contribution to the interview data that represents their feedback on the process. As can be seen table, 71% of the interviewees highlighted negative aspects of the process of applying SecRAM, and 48% of all the interviewees reported a problem resulting from the negative aspects of the process. However, 52% of the interviewees also suggested improvements to the process. Finally, 95% of the interviewees provided information on the way they had organized their work with SecRAM.

Table 11
Work organization across the different type of projects.

Node	SESAR Wave 1 (15)	GAMMA (4)	Other (1)	SESAR-1 (1)
Team with different skills	67%	100%	N/A	N/A
Asking someone else to double check	27%	25%	N/A	N/A
External security expert involved	7%	0%	N/A	N/A
No security expert involved	27%	0%	N/A	N/A
One person doing the assessment	33%	0%	N/A	N/A

Table 12
Process-related problems raised by interviewees from the SESAR Wave 1 project.

Node	SESAR Wave 1 (15)
Lack of guidance on security classification	40%
Lack of guidance on expected results	40%
Lack of necessary skills	40%
Prioritization issues	40%
Insufficient time and budget	27%

As shown in Table 10, only 10% of the interviewees commented about on the positive aspects of the process. We have therefore chosen not to go into more details of this particular aspect in our analysis.[7]

5.2. Work organization

Looking at Table 11, one can see that all the four interviewees from the GAMMA project reported that they had been working in groups when doing the security risk assessment, while the interviewees from SESAR Wave 1 worked either in groups or alone. It is surprising to see that 27% of the respondents from SESAR Wave 1 said that there was no security expert involved at all in doing the assessment. Further, in 33% of the cases it was a single person who did all the work. It should be noted that these two numbers are not independent; in some cases the interviewee revealed that there was a single person, without any security background, who performed all the work by himself.

However, in the majority of the cases (100% in GAMMA, 67% in SESAR Wave 1), the security risk assessment was conducted by a group constituted of experts in several domains; security experts, technical experts and/or operational experts. In addition, many of these groups also had a "moderator", meaning a person who guided the team through the assessment, asked the right questions and encouraged them to participate in, for example, brainstorm activities.

5.3. Process-related problems and consequences

Table 12 outlines the process-related problems raised by the 15 interviewees from SESAR Wave 1.[8] As can be observed from the table, five different problems were highlighted, We will discuss these in more detail below.

5.3.1. Lack of guidance on security classification

An issue that was highlighted by 40% of the interviewees was the lack of guidance on how the results of the security risk assessment should be classified, which apparently had led to a lot of confusion. They all seemed to be aware of the three different risk levels for classified material (red/amber/green, as outlined in Table 1), and the accompanying three different templates for documenting their results (Anon, 0000b,c,d), but they were still confused over whether and how they were allowed to share information with their partners. Also, many of them complained that they did not get any feedback or help from the SJU on this. This lack of guidance resulted in several problems:

- Some of the interviewees claimed that, since they did not know how to share information with their partners, they were forced to do SecRAM alone: "*The plan was to work together with a colleague, yes. But then we noticed that there are different colors, the green, yellow and red documents. Then we said, "ok to be on the safe side, I will do the work alone.""*"
- Some of the interviewees claimed that they had to pause their risk assessment activities and that they would not continue until SJU had clarified how they were allowed to communicate the results. A few of them had even stopped all their ongoing security activities and, to be on the safe side, they even deleted everything that had been produced so far: "*all activities on security issues have stopped. Because it was not clear who is allowed to read, to provide input and so on.*"
- Some of the interviewees also complained that they had completed the assessment, but it had never been read by anyone. Their therefore questioned whether it was meaningful in the first place: "*No one will read a document that cannot be shared.*"

5.3.2. Lack of guidance on expected results

Of the interviewees, 40% also complained they had a hard time understanding what was expected from them. They explained that they had problems understanding the scope (what should be included in the analysis and what could be left out), and they did not know what levels of details that was expected in the analysis. The lack of guidance on expected results also had consequences in terms of different results from different solutions. As one of interviewees explained it: "*It [SecRAM] is not precise enough and there may be large differences among the different risk analysis that are done within one project. Because one project is divided in different work packages and so on. So, each work package does... its own risk analysis, but they may differ in their contents and methodology may not be enough precise on some aspects.*"

5.3.3. Lack of necessary skills

Another important point that was brought up by 40% of the participants was the lack of necessary skills to perform the assessment. They mentioned not only the lack of team members with specific competence in the different areas for the impact assessment (economic, legal, branding, etc.), but also a general lack of security competence in their teams. For instance, an interviewee mentioned that "*[his] main concern [...] was that [he] was not trained or sufficiently aware of all the security aspects.*" Finally, they highlighted the lack of security training in SESAR in general as a problem.

According to the interviewees, the lack of necessary skills had two major consequences. First, they did not prioritize security and the security risk assessment thus often ended up in the bottom of the "to do-list". Second, many of the interviewees were in addition unsure about the quality of the results that they had produced.

[7] The lack of data on the positive aspects of the process does not necessarily mean that the interviewees think that the process was bad, it rather indicates that this is not a topic that the interviewees felt like they needed to discuss.

[8] The reason for not including the interviewees from the GAMMA project in this particular analysis is that the way people have been working with SecRAM has changed over the years (see Section 2.3). Most of the identified problems in Table 12 were therefore not relevant for the interviewees from the GAMMA project.

5.3.4. Prioritization issues

Of the interviewees, 40% also complained about the prioritization of their solutions; in most cases because they had been "security prioritized" (see Section 2.3). One interviewee said that he " *think[s] that the security, that spending time on the security for [their] solution and in V2.. was not really necessary.*", and when we asked whether this meant that he did not agree with the prioritization of your project, his reply was: "*Yeah, that's the conclusion yeah.*"

5.3.5. Insufficient time and budget

Several of the interviewees (27%) also claimed that the budget allocated for security was not enough, and that they therefore had no time to do it properly. Also, they said there were too few security experts in SESAR, which makes it difficult in general to work with security. For instance, an interviewee pointed out that "*by the end of your day you don't have enough resources. And you certainly do not have enough security trained staff that is able to perform everything in an ideal setup.*" Furthermore, many of them pointed out that the reason they did not have any security experts in their teams was because when they had planned their projects they were not aware that had to do the security risk assessment; to many it came as a surprise after their projects had already started.

5.4. Suggestions on improvements to the process

In addition to bringing up problems, the interviewees also contributed with proposals on how the process of applying SecRAM could be improved. The "top of the list" suggestion, which was highlighted by many of the interviewees, was "*the risk assessment should be be performed by a team*", which they said should include people with security skills, technical skills and operational skills. The need to involve security experts were particularly emphasized by one of the interviewees from the "no experience group", who also pointed out that "*having help from security experts, who are involved in several different solutions, will create more homogeneous results*". Some interviewees also pointed out the need for team members with knowledge in the different impact areas (legal, economic, branding).

Further, several of the interviewees requested security training to be offered to novice users, for example by arranging a workshop to help them get started with SecRAM.

To solve the problem associated with sharing security classified material (using the three templates (Anon, 0000b,c,d)), one interviewee suggested that "*SecRAM should be performed on prototype level, rather than on the solution level*", meaning that each partner should assess their own technology only, hence avoiding the need to involve and share security classified material with the other partners in the solution consortium.

Finally, one of the interviewees, who had a long experience in security, was concerned that, in many solutions, the security risk assessment was only done once, as a preparation for the solution's maturity gate. He therefore suggested that the methodology should include a trigger for updating the identified risks whenever there were relevant changes in the security threat landscape, which could affect the ATM domain.

5.5. Links between work organization and process related problems

In this section, we study the links between how the interviewees had organized their work and the potential impact on the way they perceived working with SecRAM.

In Section 4, we discussed what the interviewees disliked about the methodology. To better understand *why* they struggled with these issues, we cross-checked the numbers in Table 8 with the data representing how the interviewees had organized their work. The results are presented in Table 13. As can be seen in the table, interesting results appeared: 60% of the interviewees who worked alone also struggled with understanding the methodology, whereas only 31% who worked in a team had the same problem. Similarly, 40% of the interviewees who worked alone also claimed that the methodology was not suitable for all solutions, whereas this was only the case for 13% of the interviewees who had worked in a team. On the contrary, the people who worked in a team, seemed to be more concerned about missing steps in SecRAM and the trustworthiness of their results (both 38%), than the people who had worked alone (both 20%). Similarly, 50% of the interviewees who had worked in a team also had problems with the catalogs, while this was only the case for 20% of the people who had worked alone. Regarding the other process-related problems, how the interviewees had organized their work did not seem to have any significant impact on the problems that they associated with the methodology.

Looking more closely into what the interviewees struggle with, given how they had organized their work (Table 14), it became clear that people who worked alone had a hard time understanding the concept of assets (60%). They also found it very difficult to get started with the methodology (60%).

Please note that since the number of participants in each group in Tables 13 and 14 is rather small (in particular, there were only five of the interviewees who had worked alone), it is not possible to generalize from their input.

6. Results from the interviews: two "hot topics"

When analyzing the interview data, it quickly became clear that two topics were of particular interest to the interviewees, which they also had very diverse opinions about: the use of the catalogs and the lack of a tool. We therefore decided to dig deeper into these two topics.

6.1. The interviewees' position on tooling

In Table 15, we take a closer look at the interviewees' position on tooling, given their previous experience working with security. Please note that since the number of interviewees in each group is relatively small (6, 7 and 8, respectively), it is not possible to generalize from these results.

As can be seen in Table 15, almost half of the interviewees think that a tool is missing with the SecRAM methodology (48%). Looking closer at the number in the table, we notice that it was mainly the interviewees from the "experienced" and "some experienced" groups who were mostly concerned about the lack of a tool (67% and 71%, respectively). Naturally, these two groups of interviewees were also the ones who to a larger degree requested functionality for such a tool (50% and 57%, respectively).

The reasons *why* the interviewees wanted a tool were quite similar among the participants. Most of them said it would help them keep track of the assets. They also said it would reduce the "mechanical" and tedious work currently required by the methodology, like copying and pasting values between the three different templates. They also explained that having a tool that would do the computations and update all the values automatically would: 1) reduce the amount of administrative work (i.e. filling the templates), thus allowing to spend more time on the security analysis itself, and 2) prevent mistakes and inconsistencies when reporting the same values in different documents. A tool would also help people understand the methodology better, as it would guide them through the process, hence avoiding some of the confusion that they associated with the "non-linear" use of the three different templates for documenting the results. Further, they pointed out that a tool could also help in the synchronization and harmonization of information, not only among partners working in the same solution but also between different solutions, by storing the information in one single place and making it available for reuse. Some mapping could be done automatically as well, thus helping the solutions to identify vulnerabilities typically associated with particular assets and so on, and also helping gain time. Finally, they said that a tool could make easier to understand what needed to be done on

Table 13
Negative aspects of the methodology, given how the interviewees had organized their work.

Node	Worked alone (5)	Worked in a team (16)	Total (21)
Hard steps	60%	56%	57%
Unnecessary steps	60%	50%	52%
Lack of a tool	40%	50%	48%
The catalogs	20%	50%	43%
Understanding the methodology	60%	31%	38%
Missing steps	20%	38%	33%
Trustworthiness of results	20%	38%	33%
Not suited for all solutions	40%	13%	19%

Table 14
What the interviewees struggled with, given how they had organized their work.

Node	Worked alone (5)	Worked in a team (16)	Total (21)
The concept of assets	60%	13%	24%
Getting started with the methodology	60%	25%	33%

Table 15
The interviewees' position on tooling, given their experience working with security.

Node	Experienced (6)	Some experience (7)	No prior experience (8)	Total (21)
Lack of a tool	67%	71%	13%	48%
Requests for functionality	50%	57%	13%	38%

a per-solution basis, thus making it easier to adapt the security risk assessment to the maturity level (TRL) of the solution.

When discussing what kind of tool they would like to see, the interviewees' opinions varied. Some said they would prefer to have a software-based tool, while others were strongly in favor of Excel. One of the interviewees in favor of software said "*… there were tons of Excel-sheets flying around […] people are filling it in, and information is diverted and so on. So, it really would help [to have] some kind of software*". On the contrary, another interviewee detailed why he thinks a software-based tool would be a bad idea: "*There is no business model behind it, and it needs to have support*".

6.2. The interviewees position on the catalogs

The second topic, which was frequently brought up by the interviewees, was the catalogs (Anon, 2017b). This topic was however more controversial than the tool, as some interviewee were clearly against them, while others found them extremely useful. However, when analyzing the interview data, it quickly became clear that many of the interviewees had misunderstood the intention behind the catalogs; in SESAR the catalogs are there to help (by providing relevant examples, representing best practices, etc.) but there is no obligation to use them; the solutions are free to define their own assets, identify other vulnerabilities/threats than the ones in the catalogs, etc. This was apparently something that many of the interviewees had misunderstood and should hence be kept in mind when reading this section.

Looking at the rightmost column of Table 16, we can see that 71% of the interviewees said something positive about the catalogs and 43% of them said something negative. 38% proposed improvements (to either the catalogs themselves or to the way that they are used). When looking at the interviewees' position of the catalogs, given their experience working with security, we notice that all of the interviewees with "some experience" had positive things to say about the catalogs (100%). Further, we notice that even though the "experienced" interviewees frequently brought up the disadvantages (50%), they also are the ones who proposed the most improvements (84%). Finally, only 50% of the interviewees with no prior experience had positive things to say about the catalogs. Please note that since the number of interviewees in each group is relatively small (6, 7 and 8, respectively), it is not possible to generalize from these results.

In particular the interviewees from the "experienced" group were unanimous in their opinions of the catalogs. Some of them claimed that the catalogs should be removed altogether, because "*the brainstorming is brain-storm-free activity. Where you really can start with the approach "If I were an attacker. What would be the weakest link? Where would I start to invest less money and have the biggest impact?". You cannot do it with a list. If you start to study a list, you are lost*". On the other hand, others wanted to keep them, but suggested that it should be clarified that they should only be used as a starting point: " *I think it is a good departure point and it is reliable in that sense that from an ATC*[9]*-perspective we do have a fairly good understanding of our engineering architecture. And ultimately I do believe you could derive a primary asset list from that. It is also helpful for individuals who have not yet been thinking in security terms to tune in their minds in what is actually when we are speaking about security. And I do believe that on an abstract level that is high enough to support the argument that it is complete*".

To summarize, the interviewees highlighted the following advantages with the catalogs:

- The catalogs can help to identify assets and to get started with the security risk assessment.
- The catalogs will ensure consistency in the naming of components (assets) across different solutions.
- The catalogs can help in reusing results from other projects or previous assessments.
- The catalogs can help mapping assets to well-known vulnerabilities, vulnerabilities to relevant risks, etc.

To summarize, the interviewees highlighted the following disadvantages with the catalogues:

- The catalogs do not include everything that will relevant for all solutions and they are rarely updated. Therefore they will always be outdated and/or incomplete.
- The catalogs may limit people's ability to "think outside the box". Relying on the predefined assets, vulnerabilities and threats may restrict their ability to think freely, hence there is a risk they are missing out on other important elements.

Again, it appeared like this last aspect raised the strongest reactions from the interviewees with whom the topic was discussed. For example, one of them said: "*I do not need them [the catalogs], because then people get stuck looking at the pre-defined list and they stop to think.*"

[9] Air Traffic Controller (ATC).

Table 16
The interviewees' position on the catalogs, given the experience working with security.

Node	Experienced (6)	Some experience (7)	No prior experience (8)	Total (21)
Advantages	67%	100%	50%	71%
Disadvantages	50%	43%	38%	43%
Proposed improvements	84%	29%	13%	38%

Table 17
An overview over our recommendations, mapped to the supporting interview data and relevant identified literature ("best practice").

Recommendation	Supporting interview data	References
Offer tool support.	Interviewees think a tool is lacking (Sections 4.5.3 and 4.6.2). Interviewees ask for Excel-based support (Sections 4.8 and 6).	Cherdantseva et al. (2016), Landoll and Landoll (2005) and Baca and Petersen (2013)
Encourage working in teams.	Interviewees lacks necessary skills (Section 5.3.3). Interviewees ask for help from security experts (Section 5.4).	Hawley et al. (2014) and Landoll and Landoll (2005)
Clarify the use of the catalogs	Interviewees are confused about the catalogs (Sections 6.2 and 4.7.3)	Massacci et al. (2014) and de Gramatica et al. (2015)
Define running example.	Interviewees do not understand what is expected (Section 5.3.2). Interviewees struggle to understand the methodology (Section 4.7.1). Interviewees ask for better guidance, including more examples (Section 4.8).	–
Simplify the impact assessment.	Interviewees lacks necessary skills (Section 5.3.3). Interviewees ask for more flexibility (Section 4.8)	Anon (2015a) and Anon (0000e)
Launch a light-weight version of SecRAM.	Interviewees think SecRAM contains hard steps (Sections 4.6.1 and 4.7.2). Interviewees are confused about the rules (Section 5.3.1). Interviewees have insufficient time and budget (Section 5.3.5). Interviewees think SecRAM contains unnecessary steps (Sections 4.5.1 and 4.6.3).	Schmitz and Pape (2020) and Czech (2019)
Clarify the rules for information classification and sharing.	Interviewees are confused about the rules (Section 5.3.1).	–
Organize security training.	Interviewees lacks necessary skills (Section 5.3.3). Interviewees ask for security training (Section 5.4)	Costin and Francillon (2012), Kelly (2012), Santamarta (2014), Strohmeier et al. (2016) and Johnson (2015)

7. Recommendations

In this section we present our recommendations. These are derived from the results from the interviews (as presented in Section 4–6), and supported by existing literature and/or "best practice" adopted by the security community outside the ATM domain. An overview is provided in Table 17.

Recommendation: Offer tool support

First and foremost, we propose that SecRAM is extended with tool support. Not only did many of the interviewees in our study request it (see Sections 4.5.3 and 4.6.2), but it is also recommended by the academics (Cherdantseva et al., 2016; Landoll and Landoll, 2005; Baca and Petersen, 2013). As pointed out by Cherdantseva et al. (2016), "tools may facilitate data input for risk assessment in an intuitive user-friendly manner, automatically generate and analyze risk models, recommend security countermeasures or even trigger them as a response to undesired events".

Our recommendations for a tool is to start by providing basic functionality, preferably implemented in Excel (as suggested by the interviewees in Sections 6 and 4.8), which could be tested by a selected number of solutions in order to gain their feedback and opinions.

Recommendation: Encourage working in teams

Many of the interviewees claimed they lacked the necessary competence and skills to do a security risk assessment (see Section 5.3.3) and many of them specifically requested help from security experts (Section 5.4). This is in line with the findings in the study by Hawley et al. (2014), who recommended that security risk assessment should be led by security experts working closely with operational and technical experts, or those with significant related competence such as safety experts. We therefore recommend that the security risk assessment always is performed by a team, led by a person with security background who preferably also have previous experience of applying SecRAM. The teams should also have access to individuals with competence in the legal, economic and branding aspects of ATM, in order to help with the impact assessment part of SecRAM.

Recommendation: Clarify the use of the catalogs

The use of the catalogs needs to be clarified. Many of the interviewees were confused about them (see Sections 6.2 and 4.7.3), and some of them had even misunderstood the intention behind them (Section 6.2). It must therefore be clearly communicated that the catalogs are there to serve as an inspiration, but that the users are free to identify and analyze other assets, vulnerabilities, threats, controls, etc. than the ones that are included in the catalogs. Also, to keep the catalogs up to date, the users should be encouraged to propose updates whenever they discover that something is missing. The catalogs could also preferably be integrated into an Excel-based tool, which was proposed above.

Some of the "expert users" did not want to use the catalogs at all, however, our opinion is that they should be kept, in order to make it easier for users with less experience to get started. Similar conclusions can also been found in previous studies. de Gramatica et al. (2015), for example, found that security novices express catalogs as useful

especially if there is a lack of previous experience in the field. The use of domain specific catalogs has also been recommended in previous studies, such as Massacci et al. (2014), and could serve as inspiration for brainstorming activities for experts and novices alike de Gramatica et al. (2015).

Recommendation: Define running example

Many of the interviewees struggled to understand the methodology (Section 4.7.1) and the results that was expected from them (Section 5.3.2). Further, many of them asked better guidance documentation, including more examples (Section 4.8). We therefore recommend that the guidance document is updated to include a running example, which demonstrates all the steps of SecRAM. There exist some publicly available examples, e.g., Marotta et al. (2013) and Asgari et al. (2016), which could be used for this purpose.

Recommendation: Simply the impact assessment

The impact assessment should be simplified. As has been shown in this paper, many of the interviewees struggled with it (see Section 5.3.3), which in our opinion is understandable because this particular step requires knowledge in domains, such as legal, economic, branding etc., which in most cases is very far away from what the users of the methodology work with on a daily basis. Some of the interviewees also requested more flexibility in this step, for example by adjusting the granularity of the scales that are being used (Section 4.8).

The literature gives little advice on how to simplify this particular step in a security risk assessment process, and to the best of our knowledge there is no unified approach in the security community, however, there exist guidance documents from other domains that could serve as inspiration (see for example Anon (2015a) from the smartgrid domain and Anon (0000e) from the maritime domain.

The impact assessment could also be simplified to some extent if integrated in a tool, as proposed above.

Recommendation: Launch a "light weight" version of SecRAM

Many of the interviewees claimed they did not manage to complete a full security risk assessment. Their reasons varied, but common complaints were that some of the steps were very hard to perform (see Sections 4.5.1 and 4.7.2), they struggled to share information with their partners (Section 5.3.1) or they did not have sufficient time or budget (Section 5.3.5). Some of the interviewees also claimed that SecRAM contains unnecessary steps (Sections 4.5.1 and 4.6.3). This is a well-known problem from industry in general, in particular for small and medium size enterprises (Schmitz and Pape, 2020; Czech, 2019). We therefore propose that SESAR JU launches a "lightweight" version of SecRAM. The intention would be to allow solutions to get a quick overview over what needs to be protected, to identify relevant threats and associated risks, and to come up with a basic set of security requirements. The lightweight version could then be applied both by immature solutions (in their early design stage) and by solutions that runs on a low budget. To design an approach that will be suitable in the ATM context more research will be needed, but existing methods, such as LiSRA: Lightweight Security Risk Assessment for Decision Support in Information Security (Schmitz and Pape, 2020), can be used as a starting point.

Recommendation: Clarify the information classification and sharing rules

To be able to work efficiently with SecRAM, in particular in solutions where different partners cooperate to deliver technology, the users need to have both guidance and tools, to help them collaborate during the process and to share their results afterwards. Correct information classification and sharing of data using the three different templates (Anon, 0000b,c,d) was been reported as a challenge by many of the interviewees, and in some cases even as a show stopper (see Section 5.3.1). While the "information sharing issue" (see Section 2.3) is the root cause of this issue, it is still of uttermost importance that this process is clarified, and preferably also simplified.

Recommendation: Organize security training

Finally, we strongly recommend that a security training is organized and offered to the ATM community; not only to help with the security risk assessment (see Sections 5.4 and 5.3.3), but also to raise awareness of relevant threats (see, for example, Costin and Francillon (2012), Kelly (2012), Santamarta (2014) and Strohmeier et al. (2016)) and of the need to consider cyber security as an integral part of software and systems development, deployment and operation in the ATM domain in general (see Johnson (2015) and Casado et al. (2016)).

8. Discussion

8.1. The findings and recommendations

The main goal of this paper was to identify issues that may inhibit the adoption of security risk assessment methodologies in ATM. We have also suggested a number of recommendations that aim to address these issues. We expect our results to be a useful input for the SESAR JU when reviewing and updating their cyber security strategy, and ultimately for the SESAR solutions when addressing security in their research and development activities.

In our study, we saw several indications that the risk assessment played a different role than traditionally described in standards and literature. In particular, a more direct relationship between asset valuation and security requirements was described in several of the interviews. That activities in risk management are not always performed as described in standards is a commonly described phenomenon (Alaskar et al., 2015; Taylor, 2015; Niemimaa and Niemimaa, 2017; Njenga and Brown, 2012) and there may be many different underlying reasons to why. Some argue that risk assessments can be seen as static as the same risks keep recurring (Lundgren and Bergström, 2019), some believe that risk assessment is not fine-grained enough (Park and Huh, 2020), while others see a decreased focus due to legal requirements, i.e., that certain assets require particular security requirements by law (Diamantopoulou et al., 2020). The role of risk assessments and how to perform them are well-discussed (Slayton, 2015), and these aspects could benefit from further studies investigating the role of risk assessment and the direct relationship between, for example, asset valuation and security requirements.

Also, the "information sharing issue" (see Section 2.3) appears to have been a major issue for many of the practitioners. While information classification is essential for several reasons, it often creates a challenge for organizations, especially when organizations are increasingly dependent on other organizations for value creation (Partanen and Möller, 2012), which also is the case here. While we in Section 7

have recommended that the information classification and sharing rules should be simplified, this is easier said than done. While previous research has argued for consensus use of classification schemes (Cherdantseva and Hilton, 2013), they have also acknowledged the difficulties in achieving it. In SESAR, potential non-compliance with rules and regulations may make any of the involved organizations, and in worst case even their employees, liable in case of a security breach. As a consequence, the SESAR JU has not been able to provide the necessary infrastructure for ensuring that the documentation from the security risk assessments is protected in compliance with all its members national regulations (i.e. storage requirements and any staff security clearance). This issue has discussed in length at the level of both SESAR Programme Committee (PC) as Development Management Sub Committee (DMSC) and some of the practitioners' negative perceptions on the process is likely to be a consequence of this.

8.2. Threats to validity

The majority of the data collected in this study consisted of interview transcripts. While there is no rule of thumb for determining the appropriate sample size for a qualitative study (Baker et al., 2012), it has been showed that basic elements for meta-themes can be present as early as six interviews and that saturation within the data occur already within the first twelve interviews (Guest et al., 2006). The number of participants in our study was 21 and their background profiles can be considered relatively homogeneous; they have all worked in European ATM projects and they have all hands-on experience from applying SecRAM to such projects. In our case, applying the method to assess thematic saturation in qualitative research proposed by Guest et al. (2020), we reached saturation already after six interviews (using a base size of 4, a run length of 2 and an information threshold of ≤5%). We can therefore, to a certain degree, generalize from their answers. Still, the numbers in the tables presented in this paper should be read with care; they give an indication of aspects that were considered important by the interviewees, but these may not necessarily be representative for users of SecRAM in general. In particular, all the reported data that classifies data in two different ways (i.e., Tables 7, 9 and 13–16) should be read with care; the statistical significance of the values in these tables are much too small to be able to generalize from these results.

While semi-structured interviews is an efficient way to obtain data from the interview subjects (Oates, 2005b), interviewing a stranger, who does not know or trust you, about a potentially very sensitive subject, such as cyber security, can be challenging, since the lack of trust may cause the interviewee to withhold information that could be of value to the study (Myers and Newman, 2007). To mitigate potential trust issues we therefore highlighted the anonymization of all the data collected during our study during all of the interviews.

The data in our study was extracted from interview subjects whose previous security experience varied a lot. As discussed in Section 3.2, some of the interviewees had never worked with security before, while others had up to 20 years of relevant experience. This was reflected in the conversations, for example regarding their perceptions of tooling, where it was mainly the users with previous experience who mentioned on the lack of a accompanying tool in SecRAM (see Table 15). We have striven to mitigate the identified concerns from the different types of interview subjects when compiling our recommendations.

There is also a risk of bias in the results, on several levels. Some interviewees talked much more, and therefore they also contributed with more interview data. To ensure that all participants were equally heard, we therefore counted the number of interviews where an aspects was discussed, rather than counting how many times the aspect was discussed, when generating the numbers that we presented in our tables. Further, bias may also be introduced both by the researcher who was questioning the interviewees and by the researchers who transcribed, analyzed and coded the interview files. We have tried to minimize all such bias by always working in teams. There was always at least an additional researcher participating in all of the interviews, who was listening in and adding additional questions and asking for clarifications whenever needed. In addition, all the transcriptions and all the coded data was reviewed and double-checked by another member from the core research team.

The language barrier was an additional concern in our study. Most of the interviewees were non-native English speakers and some of them struggled with expressing their opinions during the interviews. The quality of the recorded audio files were also not always the best, which occasionally made it very hard to reproduce the conversations when transcribing the interviews. As described above, we mitigated this issue the best we could by re-playing all the audio files and reviewing the transcriptions at least once.

Finally, relying solely on interview data makes it impossible to validate the results. For example, we cannot know whether the interviewees' opinions on what they considered to be "easy" (and on the contrary, what they struggled with) in the methodology corresponds to the quality of the results that they ultimately managed to produce.

9. Conclusions

In this paper we have studied the practitioners' perceptions of SecRAM and how they have applied it in their ATM research & development projects. As outlined in Section 7, our analysis ended up on eight concrete recommendations for improvement. As can be seen, our position is that there is no need to make significant changes to SecRAM itself. The methodology is based on ISO/IEC 27005 (ISO/IEC 27005, 2018b), which is a well-known internationally accepted standard for security risk assessments. Using the ISO standard as a baseline, and adapting it to the context where it should be used (as has been done with SecRAM), is an approach that has been successfully applied to an immense number of cases from a wide variety of domains, such as the energy sector (Anon, 2015a; Langer et al., 2015) and maritime communication (Anon, 0000f,e; Jones and Tam, 2019). We found, however, some aspects of both the methodology, and the process of applying it, which we think would make life easier for the people in the ATM community.

Even though we did not have sufficient interview data to generalize the interviewees' position on SecRAM, given the type of or maturity level of their projects, we have not received any indications that the methodology did not fit any of their solutions. It appeared like, even though we cannot show any data that supports it, the methodology worked very well, regardless of the type of solution and the maturity level of the technology.

The proposed recommendations could benefit from future research. For example, the recommendation to encourage working in teams could pose challenges in determining who to include in the team or what competencies are needed to perform the risk assessment activities. Even though there are frameworks for describing risk management competencies (e.g., CEN EN 16234-1 (EN 16234-1:2019, 2019) and ISO/IEC 27021 (ISO/IEC 27021, 2017)), it is not always clear what competences and skills are required in risk management in general and SecRAM specifically. For example, ISO/IEC 27021 (ISO/IEC 27021, 2017) mentions asset valuation as part of the competence "documentation" rather than actually outlining what competence is needed for valuation. Hence, not much practical advice is given to managers trying to compose risk management teams. Another area for additional research, as mentioned in the discussion, is a "lightweight" version of SecRAM; more specifically, which activities should be included and why. Finally, there are many more avenues worth exploring; each of the eight recommendations presented herein provide some ideas for research streams towards a better understanding of best-practices for risk management and how these should be applied in ATM projects.

CRediT authorship contribution statement

Karin Bernsmed: Conceptualization, Methodology, Validation, Formal analysis, Resources, Data curation, Writing – original draft, Writing – review & editing, Visualization, Supervision, Project administration, Funding acquisition. **Guillaume Bour:** Conceptualization, Methodology, Validation, Resources, Data curation, Writing – original draft, Writing – review & editing, Visualization. **Martin Lundgren:** Conceptualization, Methodology, Validation, Resources, Writing – original draft, Writing – review & editing, Visualization. **Erik Bergström:** Conceptualization, Methodology, Validation, Resources, Writing – original draft, Writing – review & editing, Visualization.

References

Alaskar, M., Vodanovich, S., Shen, K.N., 2015. Evolvement of information security research on employees' behavior: A systematic review and future direction. In: Proceedings of the 48th Hawaii International Conference on System Sciences. HICSS, pp. 4241–4250. http://dx.doi.org/10.1109/HICSS.2015.508.

Anon, 0000a.Advances in the provision of Security in ATM. Gamma project handbook.

Anon, 0000b.Document template: [SESAR Solution XX SPR-INTEROP/OSED Template - Part IIIA - Security Assessment Report], 02.00.01.

Anon, 0000c.Document template: [SESAR Solution XX TS-IRS Annex IIB Security Assessment Report], 02.00.01.

Anon, 0000d.Document template: [SESAR Solution XX TS-IRS Annex IIC Security Assessment Report], 02.00.01.

Anon, 0000e.Recommended practice: Cyber security resilience management. DNVGL-RP-0496.

Anon, 0000f.The Guidelines on Cyber Security Onboard Ships, Version 4. Issued by BIMCO et.al., https://www.ics-shipping.org/.

Anon, 2015a. D2.2 threat and risk assessment methodology - smart grid protection aginst cyber attacks (SPARKS) project deliverable..

Anon, 2015b. EUROCAE ED-203. Airworthiness Security methods and considerations.

Anon, 2017a. SecRAM 2.0. Security risk assessment methodology for SESAR 2020, 02.00.00.

Anon, 2017b. SecRAM catalogues 02-00-00(1-0).xlsx (MS excel file). SESAR wave 1 project internal deliverable.

Anon, 2017c. SESAR 2020 Cyber security strategy, 01.00.00.

Anon, 2018. SESAR Joint undertaking. Introduction to SESAR maturity criteria, 01.01.03.

Anon, 2020a. Global ATM security management project (GAMMA). URL http://www.gamma-project.eu/ (Accessed May 2020).

Anon, 2020b. SESAR JU. URL https://www.sesarju.eu/ ((Accessed May 2020).

Anon, 2020c. MAGERIT V.3: methodology of analysis and risk management information systems. URL https://tinyurl.com/y9hs2al9 (Accessed May, 2020).

Anon, 2020d. Nvivo tool. URL https://www.qsrinternational.com/nvivo/ (Accessed May, 2020).

Anon, 2020e. SESAR JU - Content integration. URL https://www.sesarju.eu/projects/ci (Accessed May, 2020).

Asgari, H., Haines, S., Rysavy, O., 2018. Identification of threats and security risk assessments for recursive internet architecture. IEEE Syst. J. 12 (3), 2437–2448. http://dx.doi.org/10.1109/JSYST.2017.2765178, URL https://ieeexplore.ieee.org/document/8105791/.

Asgari, H., Haines, S., Waller, A., 2016. Security risk assessment and risk treatment for integrated modular communication. In: 2016 11th International Conference on Availability, Reliability and Security (ARES). IEEE, Salzburg, Austria, pp. 503–509. http://dx.doi.org/10.1109/ARES.2016.6, URL http://ieeexplore.ieee.org/document/7784612/.

Asgari, H., Haines, S., Waller, A., 2016. Security risk assessment and risk treatment for integrated modular communication. In: 2016 11th International Conference on Availability, Reliability and Security. ARES, pp. 503–509. http://dx.doi.org/10.1109/ARES.2016.6.

Asgari, H., Stelkens-Kobsch, T.H., Montefusco, P., Abhaya, L., Koelle, R., Markarian, G., D'Auria, G., 2017. Provisioning for a distributed ATM security management: The GAMMA approach. IEEE Aerosp. Electron. Syst. Mag. 32 (11), 5–21. http://dx.doi.org/10.1109/MAES.2017.170037, URL http://ieeexplore.ieee.org/document/8171268/.

Baca, D., Petersen, K., 2013. Countermeasure graphs for software security risk assessment: An action research. J. Syst. Softw. 86 (9), 2411–2428. http://dx.doi.org/10.1016/j.jss.2013.04.023, URL http://www.sciencedirect.com/science/article/pii/S0164121213001027.

Baker, S.E., Edwards, R., Doidge, M., 2012. How many qualitative interviews is enough?: Expert voices and early career reflections on sampling and cases in qualitative research. National Centre for Research Methods, Southampton.

Baskerville, R., Rowe, F., Wolff, F.-C., 2018. Integration of information systems and cybersecurity countermeasures: An exposure to risk perspective. SIGMIS Database 49 (1), 33–52. http://dx.doi.org/10.1145/3184444.3184448.

Bergomi, F., Paul, S., Solhaug, B., Vignon-Davillier, R., 2013. Beyond traceability: Compared approaches to consistent security risk assessments. In: 2013 International Conference on Availability, Reliability and Security. IEEE, Regensburg, Germany, pp. 814–820. http://dx.doi.org/10.1109/ARES.2013.109, URL http://ieeexplore.ieee.org/document/6657325/.

Bergström, E., Lundgren, M., 2019. Stress amongst novice information security risk management practitioners. Int. J. Cyber Situat. Aware. 4 (1), 128–154.

Bergström, E., Lundgren, M., Ericson, Å., 2019. Revisiting information security risk management challenges: a practice perspective. Inf. Comput. Secur..

Caralli, R., Stevens, J., Young, L., Wilson, W., 2007. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Tech. Rep. CMU/SEI-2007-TR-012, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, URL http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=8419.

Casado, E., Rodríguez, R., Taboso, P., García, J., 2016. Information security in future air traffic management systems. J. Aerosp. Inf. Syst. 13 (3), 101–112.

Cassell, C., Symon, G., 2004. Essential Guide to Qualitative Methods in Organizational Research. Sage.

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., Stoddart, K., 2016. A review of cyber security risk assessment methods for SCADA systems. Comput. Secur. 56, 1–27. http://dx.doi.org/10.1016/j.cose.2015.09.009, URL http://www.sciencedirect.com/science/article/pii/S0167404815001388.

Cherdantseva, Y., Hilton, J., 2013. A reference model of information assurance & security. In: 2013 International Conference on Availability, Reliability and Security. IEEE, pp. 546–555.

Chivers, H., Clark, J.A., Cheng, P.-C., 2009. Risk profiles and distributed risk assessment. Comput. Secur. 28 (7), 521–535. http://dx.doi.org/10.1016/j.cose.2009.04.005, URL https://linkinghub.elsevier.com/retrieve/pii/S0167404809000455.

Chivers, H., Hird, J., 2013. Security blind spots in the atm safety culture. In: 2013 International Conference on Availability, Reliability and Security. IEEE, pp. 774–779.

Coles-Kemp, L., 2009. Information security management: An entangled research challenge. Inform. Secur. Tech. Rep. 14 (4), 181–185. http://dx.doi.org/10.1016/j.istr.2010.04.005, URL http://www.sciencedirect.com/science/article/pii/S1363412710000063.

Costin, A., Francillon, A., 2012. Ghost in the air (traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices. In: Black Hat USA. pp. 1–12.

Cram, W.A., D'Arcy, J., Proudfoot, J.G., 2019. Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. MIS Q. 43 (2), 525–554. http://dx.doi.org/10.25300/MISQ/2019/15117.

Czech, D., 2019. How aligned are provider organizations with the health industry cybersecurity practices (HICP) guidelines? KLAS-CHIME white paper.

de Gramatica, M., Labunets, K., Massacci, F., Paci, F., Tedeschi, A., 2015. The role of catalogues of threats and security controls in security risk assessment: an empirical study with ATM professionals. In: International Working Conference on Requirements Engineering: Foundation for Software Quality. Springer, pp. 98–114.

de la Vara, J.L., Marín, B., Ayora, C., Giachetti, G., 2020. An empirical evaluation of the use of models to improve the understanding of safety compliance needs. Inf. Softw. Technol. 126, 106351.

Diamantopoulou, V., Tsohou, A., Karyda, M., 2020. From ISO/IEC 27002:2013 information security controls to personal data protection controls: Guidelines for GDPR compliance. In: Katsikas, S., Cuppens, F., Cuppens, N., Lambrinoudakis, C., Kalloniatis, C., Mylopoulos, J., Antón, A., Gritzalis, S., Pallas, F., Pohle, J., Sasse, A., Meng, W., Furnell, S., Garcia-Alfaro, J. (Eds.), Computer Security. CyberICPS 2019, SECPRE 2019, SPOSE 2019, ADIoT 2019. Lecture Notes in Computer Science, Vol 11980. In: Computer Security, Springer International Publishing, Cham, pp. 238–257.

Ellison, R.J., Woody, C., 2010. Supply-chain risk management: Incorporating security into software development. In: 2010 43rd Hawaii International Conference on System Sciences. IEEE, pp. 1–10.

EN 16234-1:2019, 2019. e-Competence Framework (e-CF) - A common European Framework for ICT Professionals in all industry sectors - Part 1: Framework. Standard.

ENISA, 2020. Inventory of risk management. URL https://tinyurl.com/jmwk3rx (Accessed May, 2020).

Eurocontrol, 2018. EUROCONTROL ATM security risk management toolkit, ATM security risk assessment methodology, 1.0.

Fenz, S., Heurix, J., Neubauer, T., Pechstein, F., 2014. Current challenges in information security risk management. Inf. Manag. Comput. Secur. 22 (5), 410–430. http://dx.doi.org/10.1108/IMCS-07-2013-0053, URL https://www.emeraldinsight.com/doi/abs/10.1108/IMCS-07-2013-0053.

Fibikova, L., Müller, R., 2011. A simplified approach for classifying applications. In: Pohlmann, N., Reimer, H., Schneider, W. (Eds.), ISSE 2010 Securing Electronic Business Processes. Vieweg+Teubner, pp. 39–49. http://dx.doi.org/10.1007/978-3-8348-9788-6_4.

Guest, G., Bunce, A., Johnson, L., 2006. How many interviews are enough? An experiment with data saturation and variability. Field Methods 18 (1), 59–82.

Guest, G., Namey, E., Chen, M., 2020. A simple method to assess and report thematic saturation in qualitative research. PLOS ONE 15, e0232076. http://dx.doi.org/10.1371/journal.pone.0232076.

Hawley, M., Gotz, K., Hird, J., Machin, C., 2014. Design-in security for air traffic control. In: 2014 Ninth International Conference on Availability, Reliability and Security. pp. 552–555. http://dx.doi.org/10.1109/ARES.2014.81.

Hsu, C.W., 2009. Frame misalignment: interpreting the implementation of information systems security certification in an organization. Eur. J. Inf. Syst. 18 (2), 140–150. http://dx.doi.org/10.1057/ejis.2009.7, URL http://link.springer.com/10.1057/ejis.2009.7.

ISO/IEC 27005, 2018a. ISO/IEC 27005: Information Technology-Security Techniques -Information Security Risk Management. ISO.

ISO/IEC 27005, 2018b. Information technology — Security techniques — Information security risk management, third edition.

ISO/IEC 27021, 2017. Information technology – Security techniques – Competence requirements for information security management systems professionals. Standard, ISO/IEC.

Johnson, C.W., 2015. 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. pp. 1–6. http://dx.doi.org/10.1049/cp.2015.0276.

Jones, K., Tam, K., 2019. MaCRA: A model-based framework for maritime cyber-risk assessment. WMU J. Marit. Aff. 18, http://dx.doi.org/10.1007/s13437-019-00162-2.

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

Kotulic, A.G., Clark, J.G., 2004. Why there aren't more information security research studies. Inf. Manag. 41 (5), 597–607. http://dx.doi.org/10.1016/j.im.2003.08.001, URL http://linkinghub.elsevier.com/retrieve/pii/S0378720603000995.

Labunets, K., Massacci, F., Paci, F., 2017. On the equivalence between graphical and tabular representations for security risk assessment. In: International Working Conference on Requirements Engineering: Foundation for Software Quality. Springer, pp. 191–208.

Labunets, K., Paci, F., Massacci, F., 2015. Which security catalogue is better for novices? In: 2015 IEEE Fifth International Workshop on Empirical Requirements Engineering. EmpiRE, IEEE, pp. 25–32.

Labunets, K., Paci, F., Massacci, F., Ragosta, M., Solhaug, B., 2014. A first empirical evaluation framework for security risk assessment methods in the ATM domain. SESAR Innov. Days.

Landoll, D.J., Landoll, D., 2005. The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments. CRC Press.

Langer, L., Smith, P., Hutle, M., 2015. Smart grid cybersecurity risk assessment. In: 2015 International Symposium on Smart Electric Distribution Systems and Technologies. EDST, IEEE, pp. 475–482.

Lundgren, M., Bergström, E., 2019. Dynamic interplay in the information security risk management process. Int. J. Risk Assess. Manag. 22 (2), 212–230.

Marotta, A., Carrozza, G., Battaglia, L., Montefusco, P., Manetti, V., 2013. Applying the SecRAM methodology in a cloud-based ATM environment. http://dx.doi.org/10.1109/ARES.2013.108.

Mason, J., 2002. Qualitative Researching, Second ed. SAGE Publications, London.

Massacci, F., Paci, F., Solhaug, B., Tedeschi, A., 2014. EMFASE–an empirical framework for security design and economic trade-off. In: 2014 Ninth International Conference on Availability, Reliability and Security. IEEE, pp. 537–543.

McEvoy, T.R., Kowalski, S.J., 2019. Deriving cyber security risks from human and organizational factors–A socio-technical approach. Complex Syst. Inform. Model. Q. (18), 47–64.

Montesino, R., Fenz, S., 2011. Automation possibilities in information security management. In: 2011 European Intelligence and Security Informatics Conference. IEEE, pp. 259–262.

Myers, M.D., Newman, M., 2007. The qualitative interview in IS research: Examining the craft. Inf. Organ. 17 (1), 2–26.

National Cybersecurity Agency of France (ANSSI), 2020. EBIOS Risk manager - the method (v1.0).. URL https://tinyurl.com/ydemtse8 (Accessed May, 2020).

Nie, R.-t., Zhao, Y., Dai, J.-h., 2009. Evaluation on safety performance of air traffic management based on fuzzy theory. In: 2009 International Conference on Measuring Technology and Mechatronics Automation. IEEE, Zhangjiajie, Hunan, China, pp. 554–557. http://dx.doi.org/10.1109/ICMTMA.2009.129, URL http://ieeexplore.ieee.org/document/5203494/.

Niemimaa, E., Niemimaa, M., 2017. Information systems security policy implementation in practice: from best practices to situated practices. Eur. J. Inf. Syst. 26 (1), 1–20. http://dx.doi.org/10.1057/s41303-016-0025-y.

NIST SP 800-30, 2012. Guide for conducting risk assessments. Tech. Rep. NIST SP 800-30r1, National Institute of Standards and Technology, Gaithersburg, MD, http://dx.doi.org/10.6028/NIST.SP.800-30r1, URL https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

Njenga, K., Brown, I., 2012. Conceptualising improvisation in information systems security. Eur. J. Inf. Syst. 21 (6), 592–607. http://dx.doi.org/10.1057/ejis.2012.3.

Oates, B.J., 2005a. Researching Information Systems and Computing. Sage.

Oates, B.J., 2005b. Researching Information Systems and Computing. Sage.

Park, J.-Y., Huh, E.-N., 2020. A cost-optimization scheme using security vulnerability measurement for efficient security enhancement. J. Inf. Process. Syst. 16 (1).

Parker, D.B., 2007. Comparison of risk-based and diligence-based idealized security reviews. EDPACS 36 (3–4), 1–12. http://dx.doi.org/10.1080/07366980701804805.

Partanen, J., Möller, K., 2012. How to build a strategic network: A practitioner-oriented process model for the ICT sector. Ind. Market. Manag. 41 (3), 481–494. http://dx.doi.org/10.1016/j.indmarman.2011.05.002, IMPASIA 2010, URL https://www.sciencedirect.com/science/article/pii/S001985011100054X.

Reynolds, T.J., Gutman, J., 1988. Laddering theory, method, analysis, and interpretation. J. Advert. Res. 28 (1), 11–31.

Roy, P., Sengupta, A., Mazumdar, C., 2021. A structured control selection methodology for insider threat mitigation. Procedia Comput. Sci. 181, 1187–1195.

Saldaña, J., 2015. The Coding Manual for Qualitative Researchers. Sage.

Sampigethaya, K., Poovendran, R., Shetty, S., Davis, T., Royalty, C., 2011. Future e-enabled aircraft communications and security: The next 20 years and beyond. Proc. IEEE 99 (11), 2040–2055.

Santamarta, R., 2014. A wake-up call for satcom security. Tech. White Pap..

Schmitz, C., Pape, S., 2020. LiSRA: Lightweight security risk assessment for decision support in information security. Comput. Secur. 90, 101656. http://dx.doi.org/10.1016/j.cose.2019.101656, URL http://www.sciencedirect.com/science/article/pii/S0167404819301993.

SESAR Project 16.02.03, 2012. SESAR ATM Security risk assessment methodology.

SESAR Project 16.02.03, 2013a. Minimum set of security controls.

SESAR Project 16.02.03, 2013b. SESAR ATM SecRAM Implementation guidance material.

Shameli-Sendi, A., Aghababaei-Barzegar, R., Cheriet, M., 2016. Taxonomy of information security risk assessment (ISRA). Comput. Secur. 57, 14–30.

Shedden, P., Ahmad, A., Smith, W., Tscherning, H., Scheepers, R., 2016. Asset identification in information security risk assessment: A business practice approach. Commun. Assoc. Inf. Syst. 39 (1), 297–320. http://dx.doi.org/10.17705/1CAIS.03915.

Shedden, P., Smith, W., Ahmad, A., 2010. Information security risk assessment: towards a business practice perspective. School of Computer and Information Science, Edith Cowan University, Perth.

Silva, F.R.L., Jacob, P., 2018. Mission-centric risk assessment to improve cyber situational awareness. In: Proceedings of the 13th International Conference on Availability, Reliability and Security - ARES 2018. ACM Press, Hamburg, Germany, pp. 1–8. http://dx.doi.org/10.1145/3230833.3233281, URL http://dl.acm.org/citation.cfm?doid=3230833.3233281.

Slayton, R., 2015. Measuring risk: Computer security metrics, automation, and learning. IEEE Ann. Hist. Comput. 37 (2), 32–45. http://dx.doi.org/10.1109/MAHC.2015.30.

Stålhane, T., Sindre, G., 2014. An experimental comparison of system diagrams and textual use cases for the identification of safety hazards. Int. J. Inf. Syst. Model. Des. (IJISMD) 5 (1), 1–24.

Stelkens-Kobsch, T.H., Finke, M., Carstengerdes, N., 2017. A comprehensive approach for validation of air traffic management security prototypes: A case study. In: 2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC). IEEE, St. Petersburg, FL, pp. 1–10. http://dx.doi.org/10.1109/DASC.2017.8102082, URL http://ieeexplore.ieee.org/document/8102082/.

Strohmeier, M., Schäfer, M., Pinheiro, R., Lenders, V., Martinovic, I., 2016. On perception and reality in wireless air traffic communication security. IEEE Trans. Intell. Transp. Syst. 18 (6), 1338–1357.

Taylor, R.G., 2015. Potential problems with information security risk assessments. Inf. Secur. J.: A Global Perspect. 24 (4–6), 177–184. http://dx.doi.org/10.1080/19393555.2015.1092620.

The International Federation of Air Line Pilots, 2013. Cyber threats: who controls your aircraft?.

Thornhill, A., Saunders, M., Lewis, P., 2016. Research Methods for Business Students. London, Prentice Hall.

Tuma, K., Scandariato, R., 2018. Two architectural threat analysis techniques compared. In: European Conference on Software Architecture. Springer, pp. 347–363.

Walsham, G., 2006. Doing interpretive research. Eur. J. Inf. Syst. 15 (3), 320–330.

Wangen, G., Hallstensen, C., Snekkenes, E., 2018. A framework for estimating information security risk assessment method completeness. Int. J. Inf. Secur. 17 (6), 681–699. http://dx.doi.org/10.1007/s10207-017-0382-0, URL.

Webb, J., Ahmad, A., Maynard, S.B., Shanks, G., 2014. A situation awareness model for information security risk management. Comput. Secur. 44, 1–15. http://dx.doi.org/10.1016/j.cose.2014.04.005, URL https://linkinghub.elsevier.com/retrieve/pii/S0167404814000571.

Whitman, M.E., Mattord, H.J., 2014. Management of information security, Fourth ed. Cengage Learning, Stamford, CT, USA.