CYBER-SECURITY MANAGEMENT OF ATM SERVICES: ARE WE READY FOR THE FUTURE?

Air traffic management is undergoing fundamental cross-border transformation, requiring increased collaboration and service-oriented interaction between its stakeholders. In addition to the anticipated benefits, new ways of working introduce cyber-security risks that need to be well managed. However, it remains to be seen whether risk management frameworks developed for other domains can maintain the cyber-security of future air traffic management services. Mariken Everdij, Bart Gijsen, Andre Smulders, Theo Verhoogt, and René Wiegers investigate state-of-the-art cyber-security practices for air traffic management services, and explore options for the future.

Air Traffic Management (ATM) is currently undergoing a fundamental transformation, implemented by programmes such as Single European Sky ATM Research (SESAR) in Europe and the Next Generation Air Transportation programme (NextGen) in the U.S.A. The transformation is driven by the need to improve the performance of ATM in terms of safety, capacity, environment and economy, leading to the requirement for new developments in operational concepts and deployment of technological enablers. In the context of the Single European Sky (SES) ambition, this transformation takes form in increased collaboration, and a more open and service-oriented interaction between ATM stakeholders.

© NLR

As part of this transformation, the ATM Information and Communication Technology (ICT) landscape is also gradually changing in terms of the ICT infrastructure, as well as the way ICT-based ATM functions are developed and controlled. In order to accommodate next generation ATM functions, service-oriented architectures are being explored. Within SESAR, a system-wide information management (SWIM) environment is being developed to facilitate the sharing of essential information between all ATM stakeholders. SWIM will introduce new communication methods and technologies, including commercial internet-based solutions.

This development shows that while the SES evolution brings a wide range of business and societal opportunities within reach, the new way of working also introduces cyber-security risks. The openness between collaborating stakeholders is a vulnerability in itself, and a service-oriented way of working increases interdependencies. The ATM sector faces the challenge of successfully achieving the benefits of the SES evolution, while safeguarding the cyber-resilience of the pan-European ATM systems.

Cyber-security requires a structured approach in the form of a management system consisting of a combination of organisational, procedural and technological elements. However, it remains an open question whether cyber-security of future ATM services can be achieved and managed by applying traditional cyber-security and risk management frameworks, which are not specific for ATM. This article presents a view on cyber-security frameworks that are fit for a future with collaborating, interdependent ATM stakeholders. It identifies state-of-the-art and current cyber-security practices for ATM, and illustrates directions for cyber-security methodologies for the future service-oriented SES.

STATE-OF-THE-ART CYBER-SECURITY METHODS

One of the challenges in addressing ATM cyber-security is to identify relevant and applicable cyber-security methods (including techniques, processes, and approaches). Therefore, a literature search was performed, aiming to collect methods that can be used in support of cyber-security management and risk assessment in ATM.

The literature search was conducted in the public domain, complemented by a search in the SESAR domain and by background knowledge of the research team. Methods found were organised in a list, and details were collected including a brief description of, and references to, source material used.

Some methods were referred to under different names or had become obsolete. Therefore, the list was reduced to 82 distinct and relevant methods. The resulting list was used as a starting point for further study and analysis. It should be highlighted that the result is not exhaustive and that many other methods may be available to support cyber-security analysis.

The objective of the study was to find a practical cyber-security framework, supported by guidelines and methods that can be used to assess 'cyber-security maturity' in ATM solutions/systems. Based on this objective, a set of indicators was defined for the key aspects: 'framework', 'practice', and 'basic elements of a Security Management System (SecMS)'. This last key aspect was based on the ISO28000 standard, which consists of 18 elements grouped into 5 key activities. Eurocontrol, in support of SES regulation, developed a nonmandatory Security Management Handbook describing these elements as part of an ATM-specific SecMS. Also, CANSO, in their Cyber-Security position paper, mentioned this standard as one of the key points of their ATM-specific cyber-security strategy.

The indicators are described below:

- **Framework:** In the literature, the term framework has various interpretations that include such terms as 'process', 'procedure', 'methodology', and 'tool'. Therefore, these terms were referred to as 'categories of methods' and used as indicators, as follows:
  - Framework – a number of processes to achieve a number of strongly related objectives;
  - Process – a sequence of steps focused on achieving a particular (overall) objective. It explains what needs to be done, but not necessarily how;
  - Technique – a dedicated sequence of precise steps explaining how to address a specific sub-objective;
  - Methodology – the combination of a process and at least two techniques;
  - Tool – software or hardware that aims to support a particular technique or methodology;
  - Language – a particular 'alphabet' and 'grammar' for specifying a model (symbolically, graphically or in combination).
- **Practice:** The indicators for this key aspect were:
  - Application – whether or not the method has been applied in industry, or in experimental setting;
  - Standardisation – whether or not the method has been standardised, or is compatible with a standardised approach;
  - Maturity – whether or not the method has been used a significant number of times;
  - Available – whether the method has documentation available in the public domain in English;
  - ATM – whether the method has been applied in ATM, or in another domain.
- **Basic elements of SecMS:** The indicators for this key aspect were:
  - The 5 key activities – number of key activities addressed (completely or partially);
  - The 18 elements – (a) number of elements addressed well, (b) the number of elements that are only partially addressed or are addressed at a high level, and (c) the number of elements not addressed.

Each of the collected methods has been assessed according to the indicators described above, and scores were assigned to the results of the indicators for key aspects Practice and Basic elements of SecMS. Weights were assigned to the indicators to differentiate their relative impact. The weighted scores were accumulated, and used for ordering the methods in each category. A sensitivity analysis was performed to test the dependency of weighted scores to the indicator weights. For the category of frameworks, the top three methods were independent of the weights; for the other categories, the results depended on whether there was more focus on practice or on the basic elements of SecMS.

The best scoring methods per category are listed below. For the categories 'Language' and 'Tool', the number of methods was small and therefore have been omitted.

Category Frameworks (20 methods)

The best scoring frameworks in our analysis were (in no particular order):

- ISO/IEC27k, which refers to the ISO27000 series on information security management, maintained by the International Organization for Standardization with the International Electrotechnical Commission;
- NIST Cyber-security Framework, which is an approach for organisations to manage cyber-security risk, maintained by the National Institute of Standards and Technology;
- ISF Methods, which provides a set of high-level principles and objectives for information security together with associated statements of good practice, maintained by Information Security Forum.

These three frameworks had the same score and were not ATM specific. An ATM-specific framework described in the Eurocontrol Security Management Handbook also scored high, but did not make the top three because it is relatively less mature than the above best scoring frameworks.

Category Methodologies (30 methods)

If the focus is on the key aspect of Practice then the following methodologies scored high: Microsoft Security Risk Management, UMLintr (UML for intrusion specifications), TARA (Threat Assessment and Remediation Analysis), CRAMM (CCTA Risk Analysis and Management Method), MORDA (Mission Oriented Risk and Design Analysis), SVDT (Security Verification and security solution Design Trade-off), and OSSTMM (Open Source Security Testing Methodology Manual). If the focus is on addressing the elements of a SecMS then other methodologies score high: SecST (Security Scanning Tool), ProSecO and SIREN (SImple REuse of software requiremeNts).

Category Process (14 methods):

None of the processes covered a significant number of elements of a SecMS, so key aspect Practice was discriminating. The highest scoring process is SESAR SecRAM (Security Risk Assessment Methodology), followed by CLASP (Comprehensive, Lightweight Application Security Process), IRIS (Integrating Requirements and Information Security), SKYDD (SaKerhets YttranDe Definition) Business Process Modelling, and SESAR Security Validation Process.

Category Technique (15 methods):

None of the techniques covered a significant number of elements of a SecMS, so the key aspect of Practice was discriminating. The highest scoring techniques were: Misuse Cases, Microsoft's Security Development Lifecycle (SDL) Threat Modelling, and Attack Graphs.

References to detailed documentation of these methods are available on the internet, or can be requested from the authors of this article.

ATM CYBER-SECURITY IN PRACTICE

To investigate current practices regarding cyber-security management of ATM operations, meetings were held with representatives from several (European) operational stakeholders. In addition, best practice publications were studied, such as those by CANSO.

For the interviewed operational stakeholders, using general security management frameworks, such as ISO/IEC27k, it is common practice and helpful to create an overview of risks, objectives and controls. However, these frameworks offer limited support for the more operational aspects of cyber-security management, such as security risk assessment and the implementation and operation of cyber-security intelligence, controls and response. The operational stakeholders indicate that one should be careful not to reduce operational cyber-security management to periodic checklist verification, and always keep an eye open to cyber-security aspects that slip through the framework's mazes.

The operational stakeholders do see added value of using a standardised framework for improved information sharing within and between stakeholders. The advantages are that such frameworks support a common understanding of cyber-security management, and enable the use of uniform terminology. In current practice, there is ad-hoc exchange of information regarding cyber-security issues; a structural exchange is missing. Insights might be gained from other sectors, including telecommunications and finance, where cyber-security officers have adopted standards such as ISO/IEC27k and NIST as their 'language' for exchanging information.

More extensive information sharing could also address the challenge of realistic risk assessment based on a low number of cyber-security incidents in current internal operations. Increased information sharing, facilitated by a common cyber-security framework, could improve evidence-based policy-making in ATM cyber-security.

CYBER-SECURITY CHALLENGES OF NEXT GENERATION ATM

With the advent of future ATM services, the ICT landscape changes and new threats emerge. The interviewed operational stakeholders are involved in the initial steps of the gradual migration towards such future ATM services, including AMAN-EH (Arrival Manager Extended Horizon), Virtual Centres, and consolidation of radars. In AMAN-EH, aircraft under control of an en-route Air Traffic Service Unit (ATSU) can receive time or speed constraints from a destination ATSU to optimise the landing sequence. These future services are long term prospects, the details of their implementations are yet to be defined, and their impact on cyber-security management is unclear. Nevertheless, the current approach to cyber-security management may need to be updated. First, there is need for a methodology to gain insight into potential cyber-security issues with future ATM services in the early development stages. Secondly, there is need for a collaborative methodology to verify trust relations for future ATM services with increased degrees of interdependency.

For this purpose, the authors investigated two recent methods: Security Scanning Tool (SecST) and Networked Risk Management (NRM), both used at the authors' organisations. Both methods are typically applied in expert sessions with stakeholders. SecST aims at scanning a given operational concept against all security aspects, including Security Regulation, Security Management, Operational Security, and Security Architecture aspects. The NRM aims to enumerate expectations and obligations of individual actors and to match these by applying a set of matching rules. Both methods were applied to the AMAN-EH use case in two internal workshops, with promising results. More detailed information on both methods and on their application to AMAN-EH is available from the authors of this article.

CONCLUSION

For ATM stakeholders, cyber-security of current operations is considered one of the issues to be addressed in securing internal business operations. Beyond the current operation, it is becoming clear that future service-oriented ATM requires a multi-stakeholder, collaborative cyber-security management framework. The main purpose of such a framework is to provide a comprehensive overview and a common 'language' for exchanging information. Cyber-security frameworks such as ISO/IEC27k and NIST emerge as mature and widely adopted. They cover all the basic elements of an ATM security management system. However, due to their general nature, they do not offer ATM-specific guidelines. This omission is filled by Eurocontrol's Security Management Handbook. In Europe, this handbook enables the harmonisation of national ATM Security frameworks, which supports exchanging/sharing of information and knowledge, and can help standardise and execute national oversight. This will improve trust in each other's security frameworks, which is essential for sharing information.

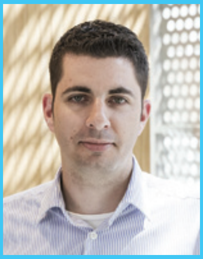
Regarding future ATM concepts, it is foreseen that methods and tools for assessing the maturity of a multi-stakeholder (eco-)system regarding the key elements defined in Eurocontrol's Security Management Handbook will be needed. Further, methods and tools will be needed to assess risks due to increased interdependency between ATM stakeholders for future ATM services. 🟩

Mariken Everdij *is a senior safety scientist at the Netherlands Aerospace Centre (NLR). Mariken is specialised in the development of methods for safety analysis of operations with multiple dynamically interacting agents. She can be contacted at mariken.everdij@nlr.nl.*

Bart Gijsen *is a consulting researcher at the Netherlands Organisation for Applied Scientific Research (TNO). Bart is specialised in cyber-security and robustness of mission critical ICT infrastructures. He can be contacted at: bart.gijsen@tno.nl.*

André Smulders *is senior business consultant cybersecurity at the Netherlands Organisation for Applied Scientific Research (TNO). André is specialised in risk management for multi stakeholder systems. He can be contacted at: andre.smulders@tno.nl.*

Theo Verhoogt *is a principal project engineer at the Netherlands Aerospace Centre (NLR). Theo is specialised in the development and validation of new ATM concepts. He can be contacted at theo.verhoogt@nlr.nl.*



René Wiegers *is senior R&D engineer at the Netherlands Aerospace Centre (NLR). René is specialised in aerospace data management and cyber-security. He can be contacted at rene.wiegers@nlr.nl.*