At the core of the Engage KTN is the definition of various thematic challenges: new ideas suggested by the research community, not already included within the scope of an existing SESAR project. They are developed along with the ATM concepts roadmap and complementarily with some of the network's PhDs and theses.

Thematic challenge 1

Vulnerabilities and global security of the CNS/ATM system

Edition 4.1, December 2019

This is an evolving document that summarises the key concepts (and, later, findings) for thematic challenge 1.

Abstract

CNS/ATM components (e.g., ADS-B, SWIM, datalink, Asterix) of the current and future air transport system present vulnerabilities that could be used to perform an 'attack'. Further investigations are necessary to mitigate these vulnerabilities, moving towards a cyber-resilient system, fully characterising ATM data, its confidentiality, integrity and availability requirements. A better understanding of the safety-security trade-off is required. Additional security assessments for legacy systems are also needed to identify possible mitigating controls in order to improve cyber-resilience without having to replace and refit. Future systems security by design is essential: a new generation of systems architectures and applications should be explored to ensure confidentiality, cyber-resilience, fault tolerance, scalability, efficiency, flexibility and trust among data owners. Collaborative, security-related information exchange is essential to all actors in aviation. This is specially challenging in a multi-stakeholder, multi-system environment such as ATM, where confidentiality and trust are key.

Description of challenge

Data science applications are revolutionising many industries, including aviation. The increasing availability of data, coming from an increasingly sensorised and communicating sector, is multiplying the opportunities of delivering data and information-based solutions to diverse challenges, including fuel efficiency, safety, predictability and crew training. However, this is also opening new vulnerabilities or hazards that need to be faced, as declared by the Industry Consultation Body (2017) in its information paper, noting that the increasing reliance on inter-connected ATM systems, services and technologies increases the risk of cyberattacks.

From the human and organisational perspective, the growing potential impact of the described cyber threats require the cooperation and adaptation of mental models within the sector. Stakeholders involved in aviation and air transportation, and especially those directly interacting with the systems and basing their operations on them, need to be trained and prepared to understand and face the threats. Aviation stakeholders, airlines, airports, and air navigation service providers all operate different information management systems for their operational purposes. This generates a complex, multi-stakeholder, multi-system environment where the global security of the system architecture needs to be ensured and its cyber-resilience needs to be further reinforced through a combination of organisational, procedural and technological elements (Everdij *et al*., 2016). The reliability of the information displayed and used by ATM/CNS components is crucial to ensure the safe operation of a flight. Different ATM systems (e.g. ADS-B, datalink, SWIM, Asterix) are vulnerable to certain attacks (some of which might still be unknown), such as: corrupting, through false instructions or information, aeronautical communications broadcast in known frequencies (Strohmeier *et al*., 2015); ADS-B false-aircraft transmissions – so-called false data injection attacks (FDIA; e.g. see Cretin *et al*., 2018); and, attacking key infrastructure elements such as SWIM (system wide information management; e.g. see Everdij *et al*., 2016).

From the technological perspective, the complex, multi-stakeholder, multi-system environment that is developed for CNS/ATM, requires updates of software and firmware of IT components in order to resolve security vulnerabilities of any critical infrastructure. The problem of ensuring that vendors will indeed guarantee development and delivery of security upgrades and security patches for ten years or more will soon become of crucial importance. This is currently unsolved and involves several difficult issues: technical, economic and legal. These difficulties include either how to upgrade each component, while ensuring capability with all other elements, or how to guarantee that this activity is economically sustainable over a long period. Taking into consideration the risks involved in the IT supply chain is an extremely challenging problem.

Considering the growing importance of communications, information and data sharing among ATM stakeholders, systems and components, it is necessary to ensure adequate protection against these and future potential attacks. Considering current global threats, it is pertinent to perform an initial security assessment of the elements supporting air navigation as well as their relationships, in order to identify its vulnerabilities. The collaboration of the different stakeholders plays a crucial role in achieving this objective, as highlighted by the ICB in its information paper (Industry Consultation Body, 2017), where sharing information about previous attacks and effective mitigations are considered a necessary step to protect the industry from future attacks. A European holistic, coherent, affordable and adaptable response that first understands the risks and then establishes mitigation measures is needed. The risk assessment should consider the potential impact of additional security measures to avoid unwanted effects regarding safety (e.g. TCAS encryption). On the other hand, it is necessary to apply controls to existing aviation and air traffic systems to detect exposure to attacks and make them cyber secure without having to replace and refit.

Certification, legal and liability issues should also be taken into account. Identifying the vulnerabilities and anticipating potential risks should then be used to design adequate mitigation actions and procedures that may imply certain changes in the system. Moreover, the legal frameworks necessary for providing concrete operational guidelines suitable for these novel forms of dependence are often still excessively vague. Assessing and managing these hazards is rapidly becoming an inescapable necessity in safety critical systems.

In a growing environment of data-driven applications (machine learning, artificial intelligence, data science, etc.) likely capable of further improving aviation performance, we need innovative data-sharing architectures capable of connecting and providing access to distributed data while preserving data privacy. The optimal data-sharing framework for a multi-stakeholder, multi-systems system like ATM, should be built on data owners' trust, placing data privacy at the heart of its architecture. The application of innovative, secure, distributed architectures, needs to be explored in the aviation domain as a potential path to ensure trust from both the technical and data usage/protocol perspectives. Further studies should also analyse the use of advanced, secure computing functions for privacy-preserving applications built over distributed applications.

As a particular example, to move to the managed service provision of surveillance data, such as space-based ADS-B, introduces the need for service suppliers to provide adequate assurance that the data are secure. Models applied have to ensure data integrity while considering security quality for data sources from multiple parties. A greater degree of technical integration and sharing data is also introduced with the intention of rationalising traditional radar information and the utilisation of layers of newer surveillance technologies to advance capabilities. This leads to the requirement of tight security of the information, further leading to the difficulty of how to constrain data accessibility with the potential reduction of precision that this action involves.

The information and communication technologies sector has made significant progress in this respect and, in particular, in the cybersecurity domain, which could be transferred to the aviation industry where several initiatives have also been launched. This previous work should serve as a basis for future research in the field. The SESAR cybersecurity strategy and framework study (SESAR, 2015), in particular, provides a European framework enabling the application of an aviation security maturity model to define the roadmap towards fully secured aviation. Challenges covered therein are: bridging the gap between security risk management and the system-of-systems architecture (EATMA); strengthening cyber-resilience by linking with operational contingency; and, assessing different architectural options from a security perspective.

Focusing on the crucial security analysis and strategic protocols that are needed to mitigate the system's vulnerabilities, there is a necessity to analyse whether or not protocols contain weaknesses themselves or protocols scale to the new trust mechanisms required (i.e. do they contain the required security mechanisms, or have the ability to flexibly adopt new security mechanisms?). A deeper study of the security analysis of aviation-specific protocol implementations has to be carried out, especially for the case of a common software library used across vendors to implement a protocol specification, to know the security vulnerabilities content that these products could expose.

The CANSO *Cyber Security and Risk Assessment Guide* provides an overview of the threats and risks, including considerations for managing them and suggestions for a cybersecurity programme (CANSO, 2014). In addition, a number of workshops and research projects have been organised around this topic, helping to progress beyond the state of the art, foster the debate and promote the creation of an associated community. The following (non-exhaustive) list collects some of the most relevant activities.

- The EUROCONTROL ART workshop on cybersecurity (EUROCONTROL, 2016) focused on providing recommendations to foster progress in the field, covering regulatory, liability, validation, human and organisational aspects, including cooperation and harmonisation with other non-EU programmes.
- EASA and EUROCAE (2017) organised a workshop on technical standards to initiate the discussion about future rule-making and standardisation for cybersecurity in aviation.
- The GAMMA project (2017) developed a new vision, representing a concrete proposal for the day-to-day operation of air traffic management security. The ATM security solution proposed by GAMMA builds on the principles and concepts related to security management in a collaborative, multi-stakeholder environment, while maintaining a strong link with the current international and European legal frameworks, and the constraints imposed by national sovereignty issues.

- The European Strategic Coordination Platform (2017) on cybersecurity in aviation, organised by EASA, accepted a declaration which "called upon the European Commission and the European Aviation Safety Agency to develop and adopt Implementing Regulations addressing Cybersecurity in Aviation with harmonised common objectives but tailored requirements for subjects and sub-sectors, assuring commensurate responses to risks, called on airports, ground handling operators, maintenance organisations, air navigation service providers to develop information security management systems in accordance with specific procedures and appropriate standards, recommended to harmonise the security risk assessment methodologies, recognised that cybersecurity is an interdisciplinary problem in transport that has its challenges in aviation, but also in shipping, rail and road transport, called upon a stronger partnership between regulators, operators, service providers, and manufacturing industry, in particular within the ESCP, where EASA welcomes and supports the Industry to come with standards."
- In 2018, DGAC France and EASA hosted the European Strategic Coordination Platform (ESCP) High Level Meeting. The purpose was to bring together States, industry, partners and other key players to raise awareness of cyber threats and attacks that could damage or disrupt critical infrastructures endangering airlines, airports and air traffic management. Potential actions, sustainable policies, approaches and measures to protect against them and mitigate their impact were also discussed and developed. See: DGAC and EASA (2018).
- In April 2019, IATA held, for the first time, an Aviation Cyber Security Roundtable (ACSR) in Singapore. This aimed to better understand and manage cybersecurity risks in civil aviation by sharing knowledge and experience, as well as developing tangible actions for the aviation industry. See: IATA (2019).
- In November 2019, the Israel Airports Authority (IAA) and EUROCONTROL conducted a joint cybersecurity exercise on aviation systems. The exercise consisted of various challenges in different fields related to cybersecurity. The objective was to help train cybersecurity experts of both organisations in order to maintain their skills in a fast-evolving domain. The IAA hopes to host similar annual events involving stakeholders from other EUROCONTROL Member States. See: Israel Airport Authority and EUROCONTROL (2019).
- 2019 also saw the launch of two Engage catalyst fund projects aligned with thematic challenge 1: "Authentication and integrity for ADS-B" (project coordinator: TU Kaiserslautern, Germany), and "The drone identity – investigating forensic-readiness of U-Space services" (project coordinator: The Open University, UK). Please refer to the link in the next section for further details.

Making the most of the latest progress achieved in previous and on-going activities, this thematic challenge aims to pave the way towards a privacy-preserving, cyber-resilient, fault-tolerant and trustworthy system of systems, with all layers ensuring the integrity and availability of aeronautical data.

Workshop conclusions

This section consolidates conclusions from the first workshop. See the Engage website for the presentations. Readers are also invited to refer to abstracts of on-going research by projects funded through the first catalyst funding wave.

Progress in security risk assessment is required (including the development of indicators for key risks) as a first step in understanding, controlling and preventing the vulnerabilities of the systems. In correctly addressing this need, the role of the operator needs to be considered as the end user of the system to be assessed and secured. Adequate training for operators should be provided in order to increase the awareness and develop operational procedures for risks identification and reaction.

To maintain safety levels, current ATM/CNS systems are subject to rigorous change-management procedures to ensure that required system updates do not have an adverse impact on the reliability of the system. However, if new security vulnerabilities are identified in an ATM/CNS system, there is pressure to update the system as quickly as possible to prevent it from being subject to attack. New approaches are required to develop systems that are capable of addressing these conflicting demands while maintaining resilience. As an example, the application of AI algorithms could be explored to proactively detect patterns and mitigate attacks.

Assuring the security of CNS/ATM systems requires shorter implementation times and updates/upgrades. Safety regulations are therefore challenged to face cybersecurity needs (e.g. patch management). The ability to rapidly patch vulnerabilities will be necessary when aircraft become more connected, which implies further development in certification processes of certified software (ED12-C). The requirements for certification of safety-critical systems should also include best practices from the security community.

While security information is usually protected as part of the security policies themselves, cooperation among security stakeholders is required in order to learn from previous security issues and attacks. The secure sharing of this information between ATM/CNS stakeholders is required at many levels. Examples include: post-incident forensics; real-time alerting of security incidents to connected partners; threats and vulnerabilities; lessons learned, for example detection, response and recovery methods.

New open models to enhance security should be developed in addition to the more traditional approach of security by obscurity. Aviation could learn from other sectors (e.g. banking) in order to overcome national sensitivities and confidentialities, to the benefit of a collaborative security culture.

When considering new security procedures and technologies, it is important to consider the social dimension. New developments in screening, monitoring, and tracking may potentially breach accepted norms for ethics, privacy, societal acceptance, and could be in breach of the regulatory framework. Consideration of such non-technical potential issues in advance of embarking on such programmes would be prudent. Engaging the whole society would help building cyber-resilient culture. Security governance framework needed to establish the common policies, legal aspects and procedures for all stakeholders to collaborate as a resilient ecosystem.

One of the main barriers that needs to be overcome for enabling data sharing is the confidentiality of the data sources. Nevertheless, the relative importance of confidentiality, integrity, and availability depends on the information in question and on the application area. There are particular data (e.g. ANSP staff personal data or state flights) where confidentiality and data anonymisation are essential. To address this challenge, there are research opportunities for applying encryption methodologies without compromising safety. However, for ephemeral operational data (e.g. radar tracks) integrity and availability are probably more important and their assessment needs to be further investigated.

Collaboration will be required beyond the aviation stakeholders. Future research projects will require cooperation between multiple transport modes and other sectors to obtain funding. Reducing environmental impact will be a key requirement, as well as the provision of evidence that core components are close to industrialisation. Contributing to the streamlining of safe and secure transport is also key.

The following have been identified as *example* ideas for potential further exploration:

1. Perform an initial security assessment of the elements supporting air navigation as well as their relationships, in order to identify its vulnerabilities and to ensure adequate protection against future potential attacks and current global threats;
2. Apply controls to existing aviation and air traffic systems to detect exposure to attacks and make them cyber secure without having to replace and refit. Certification, legal and liability issues should be taken into account;
3. Innovate data-sharing architectures capable of connecting and providing access to distributed data while preserving privacy, including the use of advanced, secure computing functions;
4. Confidentiality, availability and integrity requirements for aeronautical data need to be assessed per dataset and particular application;
5. Adapt mental models within the sector to prepare operators to understand and manage cyber threats;
6. Requirement of updating software and firmware of IT components in order to fix security vulnerabilities of any critical infrastructure;
7. Further research into the security analysis of aviation-specific protocol implementations (vulnerabilities, trust, software library) is required;
8. Explore open models to enhance security, complementing traditional approaches towards protection, potentially drawing on lessons learned and best practice from other sectors.

References

CANSO, 2014. CANSO Cyber Security and Risk Assessment Guide.
https://www.canso.org/canso-cyber-security-and-risk-assessment-guide

Cretin A, Legeard B, Peureux F, Vernotte A, 2018. Increasing the Resilience of ATC systems against False Data Injection Attacks using DSL-based Testing. 8th International Conference for Research in Air Transportation – ICRAT 2018, Castelldefels, Spain.

DGAC and EASA, 2018.
https://www.easa.europa.eu/newsroom-and-events/events/escp-high-level-meeting-cybersecurity-civil-aviation

EASA, EUROCAE, 2017. Workshop on Cybersecurity in Aviation, 31 May 2017, Brussels.
https://www.easa.europa.eu/sites/default/files/dfu/Cybersecurity%20workshop%20Report%20-%20final.pdf

EUROCONTROL, 2016. Agency Research Team Workshop 'ATM Security and Cybersecurity' – 23rd March 2016, ENAC, Toulouse, France
https://www.eurocontrol.int/events/agency-research-team-workshop-atm-security-and-cybersecurity

European Strategic Coordination Platform, 2017.
https://www.easa.europa.eu/newsroom-and-events/news/high-level-conference-cybersecurity-civil-aviation-krakow-declaration

Everdij M, Gijsen B, Smulders A, Verhoogt T, Wiegers R, 2016. Cyber-security management of ATM services: are we ready for the future? Aviation security international, June, pp. 34-36.

GAMMA project, 2017. - Global ATM Security Management Project, European Union's Seventh research and innovation Framework Programme. http://www.gamma-project.eu.

IATA, 2019. Aviation Cyber Security Roundtable, April 11-12 2019, Singapore. https://www.iata.org/events/Documents/SIN_Roundtable_Readout.pdf

Industry Consultation Body, 2017. Information paper on Industry Developments in ATM CyberSecurity, 3 Nov 2017. http://www.icb-portal.eu/phocadownload/TSG_Positions/Industry%20Developments%20in%20ATM%20Cyber-Security%202017%20Issue.pdf

Israel Airport Authority and EUROCONTROL, 2019. https://www.eurocontrol.int/news/building-cyber-resilience-capture-flag-exercises

SESAR, 2015. SESAR Strategy and Management Framework Study for Information Cyber-Security, September 2015. https://www.sesarju.eu/sites/default/files/documents/news/SESAR_Strategy_and_Management_Framework_Study_for_Information_cybesecurity_FINAL.pdf

Strohmeier M, Lenders V, Martinovic I, 2015. On the Security of the Automatic Dependent Surveillance-Broadcast Protocol. IEEE Communications Surveys & Tutorials, 17(2), pp. 1066 – 1087.

This project has received funding from the SESAR Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement No 783287.