



# Briefing ENGAGE TC1: Scientific committee recommendation paper on cyber

Ruben Flohr  
ATM expert

Brussels, 15 September 2021



Founding Members



# S2020 Scientific Committee Security Task Force 2020-2021



The TF was asked to:

1. Provide guidance on how to organize the security activities in the future SESAR programme; possibly by suggesting best practice from other international research and development (R&D) programmes.
2. Focus on the multi-member international collaborative development and programme requirements drawing on the quality and quantity of security expertise.
3. Consider any necessary means of ensuring the security and thereby encouraging the exchange of cyber security requirements/best practices between partners under Single European Sky (SES).

# Workshop series

- 21<sup>st</sup> January 2021
- 28<sup>th</sup> January 2021
- 04<sup>th</sup> February 2021

Chistopher Johson (University of Belfast)

“Machine Learning in the Cyber Security of ATM Infrastructures”

Nicole Keeley (UK CAA)

“The UK CAA’s cyber vision”

Andreas Gerstinger (Frequentis)

“Safety & Security from an ATM supplier’s view”

Patrick Mana (ECTL)

“Complexity of Securing the Aviation Ecosystem”

Martin Strohmeier (Cyber-Defence Swiss/Uni Oxford)

“How (not) to do Wireless Security”

Tony Licu (ECTRL)

“Cyber Security Maturity Model and EATM\_CERT”

# Recommendations

- As the scope and reach of SJU is limited to R&D activities, the TF divides the recommendations into:
  - **Programme level recommendations** can be tackled by the SJU as they lie within the SJU remit
  - **Strategic recommendations** that indicate a path the SJU can follow to play an active role in promoting the uptake of these issues through the collaboration with the appropriate, external organisations

# Programme level recommendations

- **Recommendation 1:**
- **Every SJU project should be required to conduct a formal cyber security risk assessment, ideally using the SecRam approach.** The output of this may be to argue that the project does not raise any explicit cyber concerns but such an argument should be reviewed by the project manager early in the project lifecycle. The SecRAM methodology does not specify the exact vulnerabilities but lists security requirements and the underlying security risk assessment. Note that these requirements can be addressed in different ways in the final, deployable system. Furthermore, in the R&D V1-V3 phases the security requirements and risk assessments are in sufficiently high level form that it should not preclude the information sharing between project members and the SJU.

# Programme level recommendations

- **Recommendation 2:**
- In order to ensure that cyber security is sufficiently considered within all future proposals and to protect the future of SES, we recommend that a **high-level maturity risk assessment be provided by applicants** as an eligibility criteria for entities answering the calls for proposals in the next SESAR work programme. Another possibility would be to present the evidence that **project members have security training.**

# Programme level recommendations

- **Recommendation 3:**
- We recommend that the SJU explore the costs and benefits of deploying a **specific infrastructure for security information exchange**, in view of increased number of attacks on research institutions. The authors of this report can provide links to relevant agencies within our member states that now place this expectation on our domestic research programmes – in the light of recent attacks on Universities from nation states outside Europe.

# Programme level recommendations

- **Recommendation 4:**
- The safety and security objectives often compete, but as they are equally important to ensure safe and secure air transport, they should be addressed jointly. For instance, existing intrusion detection tools have not been designed to meeting the requirements of ED-143 . **Thus, we recommend the development of a joint safety/security approach.** SecRAM only partially satisfies this requirement, as evidenced by the OPTICS2 work and GAMMA. The SJU should fund extensions to the existing approach that align with the safety management systems of partner organisations.



# Programme level recommendations

- **Recommendation 5:**
- Many cybersecurity issues are not unique for the air transport industry, and **the existing knowledge can be re-used**. We need a strategy in investing in issues that best can be addressed **through collaboration**.
- **Recommendation 6:**
- Build on the success of the workshops in identifying a **community of experts in cybersecurity in air transportation**. In SESAR1 the security community existed and formulated the first SecRAM methodology. Such a community is useful as it enables the sharing of best practices, and can strengthen the quality of security risk assessments and security of the final ATM solutions.



# Programme level recommendations

- **Recommendation 7:**
- **Novel technologies** (e.g. artificial intelligence, drones) offer promising opportunities in improving ATM. However, their introduction will also enlarge the **attack surface with unknown vulnerabilities**. To learn understanding these novel vulnerabilities during the design process, SecRAM has to be complemented by novel methods, such as **computer-simulation based cybersecurity penetration testing and the use of more sophisticated digital twins** which are in development by a number of ECAC states.

# Strategic recommendations

- **Strategic Recommendation 1:**
- There is the need for closer links with other sectors institutes and other national and European agencies to stop developing research in niche areas and to ensure better communication and cooperation between science, industry and policy makers across different domains. SJU should **identify potential areas of cybersecurity research that overlap with other domains**, and coordinate with **EUROCONTROL, EASA and EU cyber-security research plans**.
- **Strategic Recommendation 2**
- There is a need for an improvement of regulatory and organisational processes **for the exchange of security information across national borders**. SJU can play an instrumental role in promoting the development of such regulation and organisational processes within Europe.

# Strategic recommendations

- **Strategic Recommendation 3:**
- There is a shortage of cybersecurity expertise, e.g., in looking at the socio-technical system as a whole. Investment in education is essential for growing cybersecurity maturity. Through the Digital Academy SJU can stimulate the identification and further development of **the necessary adjustments of cybersecurity courses for ATM sector**, in Europe.

# Status



- Recommendation paper has been handed over to the ED
- Recommendations are being assessed internally for adoption in the new Programme



Briefing ENGAGE TC1:

Scientific committee recommendation paper on cyber

---

Thank you very much  
for your attention!



Founding Members

