

Collaborative cyber security management framework

Summary

The aim of this project is to address a fundamental factor that will considerably support cyber security in the ATM Industry and in the work of SESAR. This factor is the end to end *management of cyber security*, from R&D to industrialisation, deployment and decommissioning.

At present, cyber security is a patchwork of efforts, mostly done in siloes with limited collaboration. EUROCONTROL is now leading in this area on the operational side and SESAR has built in risk assessment in R&D, but the challenge demands a much greater level of support and integration.

Cyber security efforts can be contrasted with safety, where safety management systems have been constantly researched and developed through practical experience and extensive collaboration. Importantly, safety recognises that ATM is a complex socio-technical system, where management systems and methods are key.

Our proposal is about ‘zooming out’ to gain a greater situational awareness of cyber security. To do this we aim to progress a concept of ‘collaborative cyber security management’ by connecting some different strands of work: risk, architecture and collaboration and making room for more in the future. We are focusing on ‘joining the dots’ in cyber security management. To validate the concept, we will develop a prototype, taking our initial work from TRL2 to TRL3/4.

An underlying concept is to introduce a much higher degree of information sharing so that work in cyber security is leveraged between different actors at different stages of the ATM lifecycle. The proposed research is also in direct response to industry needs, recently articulated by the Industry Consultation Body (ICB). This includes the need to improve links between cyber-security and architecture, legacy system integration, the perils of selective risk assessments, safety-security, coordinating software changes etc. These and other concerns are fundamentally about cyber security management.

Security experts have become wary of new technologies that promise to be ‘silver bullets’, so we shift the focus from specialist solutions to the overall management framework. To build the management framework we have identified three priority themes to connect: collaboration, architecture and risk management. When applied in combination these themes will reduce risk and increase resilience in the adoption of digital technologies.

The aim of this research proposal is to build an operating framework for cyber security management and deliver:

- A CONOPS for a framework for collaborative cyber security management.
- A prototype for collaborative exchange of cyber security design, including architecture.
- Evolution of risk assessment capability within the CONOPS and prototype, including quantified risk.

The results of our R&D will advance the state of the art as well as contributing more generally to the enduring challenges of cyber security: to improve collaboration, simplicity and certainty.



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.