Improving Cyber Security in ATM Systems

The system landscape of Air Traffic Management (ATM) is transforming. The systems used to be homogenous isolated environments with limited information exchange between systems and users. In modern ATM the systems are adapted and developed to more current system design principles (Based on SWIM, CDM and other principles as SOA (Service-Oriented Architecture), IT/OT (Integration of information technology systems used for data-centric computing with operational technology OT systems) and 'The Internet of Things').

These developments are raising concerns in the ATSEP community regarding the cyber security of the systems in this new role. Entry Point North explored the challenges and solutions regarding modern-day cyber security in ATM during this year's edition of our annual ATSEP Workshop: an event for ATSEP professionals to share and discussed the latest news, regulation updates, developments and best practices.

IFATSEA presented and pinpointed some new areas of challenges for the ATSEP community:

- Data link complementary technologies.
- Integration of RPAs (UAV/UAS/Drones, etc.) in ATM
- "Digitalisation/Automation of ATM"
- Enhanced Reality, remote towers and virtual towers
- Networking services and SOA-Service oriented architecture

During the workshop, speaker Patrik Solsten from Combitech presented several measures an organisation can undertake in order to broaden and deepen the scope of cyber security in the design of systems and the organisations:

- Security by design: constructing a system from start to finish with security in mind, the base of which is a hardened platform.
- System Hardening: providing various layers of protection in a computer system ('defence in depth'). Protecting in layers means to protect through a unique method of security for each level: the host level, the application level, the operating system level, the user level, the physical level and all the sublevels in between.
- Penetration tests /white hat hackers: final testing of the system implementation and the integration to verify the functioning of the security measures put in place.
- Enhance security at the interface points with packet inspection gateways as a complement to the ordinary firewalls to be able to have a view of the data that is transported over the interfaces.

Additionally, it should be kept in mind that the cyber security is not only an issue for the IT department or a matter of implementation of technical solutions. There is a large portion of social skills and employee awareness to reach a full coverage of cyber security implementation.

Entry Point North integrates cyber security topics in our ATSEP courses and are continuously developing them to ensure their relevancy to the latest industry knowledge. View the ATSEP course overview here, if you have questions please do not hesitate to contact us at sales@entrypointnorth.com.