Cybersecurity in Aviation

New versus “classic” concerns

5. September 2017
Agenda

What sets „Cybersecurity“ apart from „traditional“ concerns?

„Also in Security, the environment drives what we do“
„Security is an evolutionary Process, not a Product“
„Everything is linked with everything else“
„The whole is more than the sum of its parts“
„Complexity is the Enemy of Security“

Euro... What?

European Strategic Coordination Platform for Cybersecurity in Aviation

And what about ICAO?
Threat Landscape will change, so the security process must evolve with the perceived level of risk.

The Tools for adversaries change rapidly, with constantly enhanced functionality, at a fraction of the original cost.

The required Skill level of adversaries deteriorates, as tools are becoming more and more automated and fully comprehensive.

The actual Skills of adversaries evolve, as they practice on other targets.

And: There are services out there to perform cyber attacks for you!
Security is an evolutionary Process, not a Product

As the **security environment** evolves, protections will have to be adapted

**Technologies** will change, so the security process must evolve with the perceived level of risk

**Societal expectations** of aviation will change, so the security process must evolve with the perceived level of safety risk

**Business Direction** of Aviation Industry will change, so the security process must evolve with the perceived level of risk
The whole is more than the sum of its parts

**Architecture**

- Each system shall protect itself against its individual risks
- All interacting measures contribute to the individual Level of Protection
- Functional Architecture ≠ Security Architecture

**Composability**

- Functional System Integration requires compatible interfaces, Security System Integration requires coherent and consistent behaviour
- Understanding aviation as a System-of-Systems is the prerequisite to an integrated and global cybersecurity approach by all stakeholders
Individual systems with aligned protections are collectively creating a secure environment for the whole aviation system.

Evolving technical and operational risks of individual systems require adjusted System-of-Systems risk assessments.

Evolutionary risk aware system-of-systems are capable of interaction, to enhance mutual levels of protection.

Self-healing architecture concepts actively ‘manage’ individually protected systems in securing an enhanced environment.
Complexity is the Enemy of Security

“Keep It Simple, and Stupid”: A key goal in Design, Implementation, Operation and Upgrade, making security a naturally evolving process.

Linking the security process to identified (safety) risks helps understanding, why the process is necessary.

Developing an agreed common methodology of risk assessment and taxonomy of threat helps a uniform new for our System-of-Systems.

Simple security message: Safety & Security in all aspects of aviation!
European Strategic Coordination Platform (ESCP) for Cybersecurity in Aviation

EASA Member States, EU Organisations and European Aviation Industry

Facilitate

Participate

Policy Papers for EC Institutions and Member States
Coordination Papers for International Collaboration
Tasking Papers for European Industry Organisations
And what about ICAO?

- **Composition**
  - ICCAIA, IATA, ACI, CANSO, ICAO
- **Objective**
  - Position the Aviation Industry wrt Cybersecurity
- **Origin & Results**
  - Produced a Working paper for the AVSEC Panel, based upon an AIAA Decision Paper

**Industry High Level Group (IHLG)**

- **Composition**
  - ICCAIA, IATA, ACI, CANSO, FAA/TSA, EASA, ECTRL, ICAO
- **Objective**
  - Informally discuss how Cybersecurity should be addressed on ICAO level
- **Results**
  - Informal understanding how to proceed

**Cyberfriends Meetings**

- **Composition**
  - ICCAIA, IATA, ACI, CANSO, FAA, EASA, ECTRL, ICAO
- **Objective**
  - Discuss base requirements for a secure „Aviation Internet“ (ATN IPS)
- **Results**
  - In progress

**Cybersafety / INNOVA**

- **Composition**
  - ICCAIA, IATA, ACI, CANSO, FAA, EASA, ECTRL, ICAO
- **Objective**
  - The SSGC will coordinate cyber work to be developed in a harmonised and coordinated fashion
- **Results**
  - Launching

**Secretariat Study Group on Cyber**

- **Composition**
  - ICCAIA, IATA, ACI, CANSO, FAA, EASA, ECTRL, SESAR, ECAC, ICAO
Proposed Regulatory Concept: Key Framework Aspects

A single “horizontal” Cyber-Security Rule

Includes only high-level, performance-based requirements (details in AMC/GM, Certification Specifications and Industry Standards)

Common requirements to all fields
   (design, production, maintenance, operations, aircrew, ATM/ANS, aerodromes, ...)

Specific requirements for each field
   (could follow a phased approach)

Content to be coordinated with rulemaking activities linked to Safety Management System (SMS)

A single “horizontal” Cyber-Security Certification Specification (CSCS, or CS²)
Taking into account the regulatory concept plus any feedback obtained in the workshop and in other meetings with stakeholders, authorities and institutions.

Taking into account comments received during the Public Consultation.

Industry Standards should be ready before the rules are adopted.
Thank you for your attention.

Your safety is our mission.