Cybersecurity; an EASA perspective on developments and challenges

Juan Anton
Cybersecurity in Aviation Section Manager

IATA Paperless Conference 2017
13/14 November 2017
Concerns and Objectives
Safety versus Security

SAFETY

VS

SECURITY

FORTUITY

INTENT
Safety versus Security

SAFETY

SECURITY

The notion of INTENT
Our Concern: Safety effects, caused by Cyber

- Software tampering
  - Denial of SW crates distribution
  - ICA modification

- Maintenance data (e.g. lifting) corruption
  - Tampering of GSE and EFB

- Asset diversion
  - SW tampering during shop maintenance

- Denial of Service Attack
- Trojan, Virus and Malware infection

- NAV Data spoofing
- NAV Data corruption
  - HUMS data corruption

- Pax Entert. Services
- Health and Usage Data
- Flight Plans Weight & Balance
Objectives: What do we want to achieve?

Create an environment under which the European Union is prepared to effectively address the aviation cybersecurity risks. In particular:

- Facilitate the development of a complete cybersecurity risk landscape
- Facilitate the identification and sharing of new risks and the rapid reaction by all parties
- Promote international cooperation and harmonization activities
- Create a strong and flexible regulatory framework supplemented by Industry Standards
- Ensure a high level of cybersecurity knowledge and competence of the different actors, promoting the competitiveness of EU Industry.
The pillars of the approach to Cybersecurity in Aviation

- Information Sharing
- Threat assessment & coordinated response
- Research & Studies
- Knowledge & Competence Building
- International Cooperation & Harmonization
- Industry Standards, Regulations and Oversight
Key initiatives

Establishment of ECCSA (European Centre for Cybersecurity In Aviation)
- To promote networking and knowledge sharing

EASA participation in related ICAO panels and groups

Coordination and collaboration with other EU institutions and agencies
(EU Commission and CERT-EU, ENISA)

On-going rulemaking activities for:
- Certification Specifications for product design (Task RMT.0648)
- Rules for risk management within organisations and service providers (Task RMT.0720)

Participation in the development of Industry Standards
Centralized discussion and coordination

The ESCP (European Strategic Coordination Platform), including:

- An Executive Committee (ESCP-EC) at the higher, political level
- A Technical Advisory Committee (ESCP-TAC) at the technical level
  - Includes several work-streams (groups): Charter, regulations....

The ESCP is composed of a representation of:

- EU Institutions, EU Member States and EU aviation industry associations.
- Observers: ICAO, FAA, AIA...
Regulatory Framework
Regulatory structure

A single “horizontal” Cyber-Security Rule (RMT.0720)

- 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 the SMS in the airworthiness domain (RMT.0252)
- Existing SMS in the other domains

A single “horizontal” Cyber-Security Certification Specification (CS-CS)
(incorporating the material from RMT.0648)
Estimated Calendar for RMT.0720

Before summer 2018
- Publish an NPA
  - Coordination with ESCP (European Strategic Coordination Platform):
    - ESCP TAC (Technical Advisory Committee) “Regulations” work stream (Oct. and Nov. 2017)
    - ESCP Executive Committee (Dec. 2017)

Before summer 2019
- Publish an Opinion

2020
- Rules adopted by EC and Decision issued by EASA
  - Industry Standards should be ready before the rules are adopted

Estimated Calendar for RMT.0720
Coordination with SMS:

• SMS is all about identifying, analysing and mitigating risks.

• Cybersecurity risks should be addressed in a similar manner, although we might need to consider the specificities created by the “notion of intent” of the cybersecurity attacks as well as the fact that these risks are both “safety-security” related.

• We should take an integrated approach to ensure consistency. However:
  • We still don’t have a complete SMS framework.
  • Introducing cybersecurity elements into each domain-specific SMS may lead to duplication and more complexity (and a more complicated Comitology Process).
  • In addition, certain aircraft categories/types of operations may not be required to have an SMS (such as General Aviation)

An “horizontal” cybersecurity rule may be a better option (with references into each domain-specific Implementing Rule)
Lyst of acronyms

- **AIA**: Aerospace Industries Association
- **AMC/GM**: Acceptable Means of Compliance / Guidance Material
- **ATM/ANS**: Air Traffic Management / Air Navigation Services
- **CERT-EU**: Computer Emergency Response Team – European Union
- **ECCSA**: European Centre for Cybersecurity in Aviation
- **ENISA**: European Network and Information Security Agency
- **EPAS**: European Plan for Aviation Safety
- **ESCP-EC**: European Strategic Coordination Platform – Executive Committee
- **ESCP-TAC**: European Strategic Coordination Platform – Technical Advisory Committee
- **FAA**: Federal Aviation Administration
- **ICAO**: International Civil Aviation Organisation
- **NPA**: Notice of Proposed Amendment
- **SMS**: Safety Management System
Thank You

Get in contact with us via email:

cybersec@easa.europa.eu