Electric & Hybrid Aviation Project

Session: Flight Standards

Topic 7: Cybersecurity

Presenter : Juan Anton

Questions and Answers

30 minutes!

Scope:

- EU Cyber strategy and regulatory activities.

“A Comprehensive EU Cybersecurity Strategy for Aviation”

Elements driving the cybersecurity risks

Aviation is a "System of Systems", covering all aviation domains, and where products, services and organisations are increasingly interconnected.

Cybersecurity risks have no borders and are driven by the notion of malicious intent, where vulnerabilities are exploited and an accident is not a fortuitous event **(as opposed to "classic safety")**.

Cybersecurity risks evolve very quickly, which requires industry and authorities to do business differently.

A comprehensive EU cyber strategy

Take due account of interdependencies between safety and security (both at aircraft and ground levels)

Facilitate the view on the full cybersecurity risk landscape

Facilitate the identification and sharing of new risks

Promote international cooperation and harmonization

Create a strong and flexible regulatory framework supplemented by Industry Standards

Ensure a high level of cybersecurity knowledge and competence

“Regulatory activities”

RMT.0648 (for aircraft, engines, propellers)

Rulemaking Task RMT.0648 "Aircraft Cybersecurity": ***Introduce cybersecurity provisions in the product Certification Specifications.***

Next Deliverable: Notice of Proposed Amendment (NPA) expected 2019Q1

Key aspects:

- **Introduces provisions for the certification of aircraft, engines and propellers (and certain equipment)**
- **The objective is to ensure a robust design to avoid cybersecurity risks.**
- **Harmonised with the FAA. Takes into account the recommendations to the FAA of the ASISP (Aviation Systems Information Security/Protection) ARAC (Aviation Rulemaking Advisory Committee) group, where EASA participated.**
- **Include amendments to the Certification Specifications and Acceptable Means of Compliance (AMC).**
- **There will be references to Industry Standards (ED-202A and ED-203A).**

RMT.0720 (for organisations)

Rulemaking Task RMT.0720: ***Requirements for the management of cybersecurity risks for organizations in all aviation domains (design, production, maintenance, operations, aircrew, ATM/ANS, aerodromes).***

Next Deliverable: ***Notice of Proposed Amendment (NPA) expected first half 2019.***

Key aspects:

- **The objective is to ensure that organisations are able to manage cybersecurity risks, including the need for an Information Security Management System (ISMS) and occurrence reporting.**
- **For organizations in all aviation domains, and for competent authorities (with some exceptions to ensure proportionallity to the risks).**
- **Including high-level, risk and performance-based requirements (flexibility, no frequent amendments).**
- **Complemented by AMC, Guidance Material and Industry Standards.**
- **The structure should facilitate to the organisations the future integration of ISMS with existing Safety Management Systems (SMS) and Security Management Systems (SeMS).**
- **Coordination between National Aviation Authorities and National Security Agencies.**

Concept of Operations

- Comments and questions welcome