ICAO EUR/NAT DGCA 2022

Cyber-Resilience for Operators

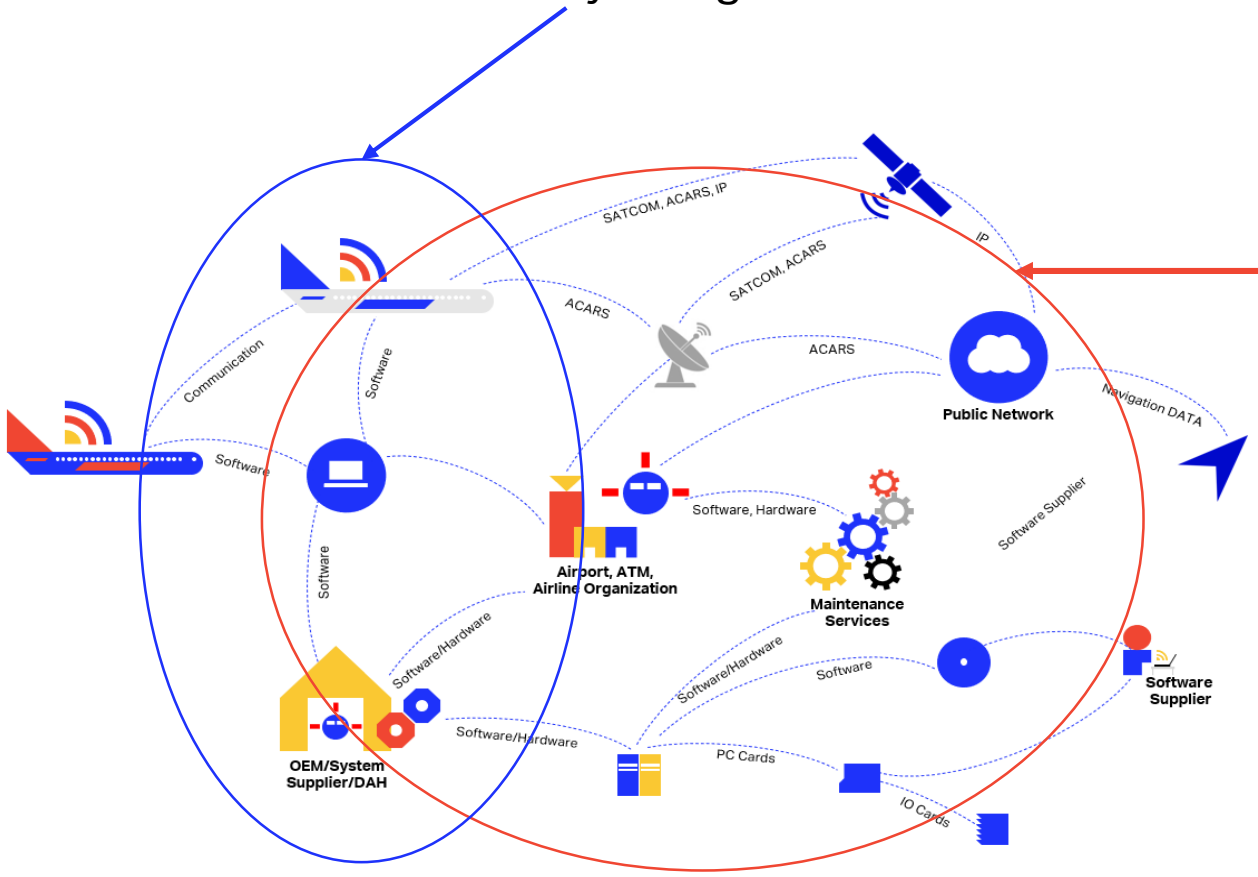
IATA's international support

Manon Gaudet, CISSP, GCED
Assistant Director Aviation Cyber Security

Angeles Pozo Romero
Assistant Director Airport, Passenger, Cargo and Security, Europe

Current Scope of the Civil Aviation

Safety of flight



Aviation Cyber Resilience

We are moving to a new massively interconnected system environment

Critical Information and Systems which

- connect to, maintain and/or operate the aircraft or its critical airline functions
- are used to support the critical airline operations
- are connected, maintained and/or operated by a supply chain party for critical aircraft or airline functions

need to be cyber protected, updated and monitored!

Confluence of Cyber-Resilience for Operators

International regulation in time of Restart and Digital Transformation

Shaping the nature of the industry response to the cyber security challenge

- Aviation Cyber Security Legislation, Standards and AMCs/MoCs development
- Regional/local regulations over critical infrastructures requires adaptations for compliance

IATA has been part of different working groups, to support **harmonization** of the different frameworks for Aviation Cyber Security

Developing a strategic implementation roadmap including the supply chain

As new digital technologies are integrated into the aviation ecosystem, the overall life-cycle of aviation will be changed forever…

and so will the attack landscape.

Knowledge and information sharing as well as **understanding the shared risks** is essential for cyber resilience of the civil aviation ecosystem.

Increasing the overall aviation cyber awareness

The following needs to happen:

- Manage expectations from the management
- Lower the costs of cyber and hire people
- Report back, in a short time

Find the **right resources**!

ICAO Annex 17 | IOSA | EASA

	ICAO A17*	IOSA	EASA Part-IS
Identification of critical assets	✓	✓	⧗
Assess the risk	✓	✓	⧗
Treatment/transference of risks and acceptance of residual risks	✓	✓	⧗
Monitor and adjust according to threat landscape	✓	✓	⧗
Incident response & recover	✓	✓	⧗
Log & report		✓	⧗
Appoint responsible/accountable Senior Management Official		✓	⧗
Integrate in existing Safety Cyber Security Events in Management Systems		✓	⧗
Information Security Manual		✓	⧗
Have the right people, with the right training and right resources	✓	✓	⧗

* ICAO Standard 4.9.1 is introduced in the EU by way of Implementing Regulation (EU) 2019/1583

IATA

IOSA | Examples of systems and data

- Flight planning/dispatch systems and data to support it
- Load control systems and data
- Aircraft performance calculation systems and data
- Reservation/DCS systems
- Baggage reconciliation systems
- Electronic Flight Bag
- Aircraft Maintenance systems
- Training and Scheduling/rostering systems
- Communication systems/ACARS
- Navigation systems

IATA and International Regulations activities

Since 2018:

Secretariat Study Group on Cyber Security (SSGC)

Trust Framework Study Group (TFSG)

ICAO Cybersecurity Panel CYSECP

ICAO Trust Framework Panel TSP (TBC)

Since 2020 (earlier for SEC):

European Commission

EU Regulation 1583/2019 (Standard ICAO 4.9.1)

NIS Directive (business continuity)

EASA

Aircraft Cybersecurity

PART-IS - Information Security

ECAC

Different working groups support.

Since 2020:

- **ED-201A/DO-391** Aeronautical Information System Security (AISS) Framework Guidance
- **ED-205A/DO-393** Process Standard For Air Traffic Management/Air Navigation Services (ATM/ANS) Ground Systems Security Aspects For Certification/Declaration
- **ED-206/DO-392** Guidance on Information Security Event Management

Conclusions

- We are moving towards a massive **interconnected system** environment;
- Where critical information systems need to be **protected, updated and monitored**
- **Cyber-resilience of operators** focused on:
  - Shaping the nature of the industry response to the cyber security challenge
  - Developing a roadmap for new digital technologies (including supply chain)
  - Increasing aviation cyber awareness.
- Notwithstanding ongoing policy developments, **airline operators** already moving towards a **self protection and control** of their cyber risks.
- IATA urges **ICAO to lead the international debate on cybersecurity risks** in aviation with a view to having a harmonised framework (as oppose to a patchwork of measures) that guarantees cyber-resilience for the entire aviation sector.

ICAO EUR/NAT DGCA 2022

Cyber-Resilience for Operators

Mrs. Manon Gaudet, CISSP, GCED

IATA, Assistant-Director Aviation Cyber Security

gaudetm@iata.org

YMQ

Angeles Pozo Romero

IATA, Assistant Director Airport, Passenger Cargo and Security Europe

pozoa@iata.org

MAD