

EASA cybersecurity activities and research

Davide Martini

Senior Expert – Cybersecurity in Aviation

EU Aviation Safety Agency

Your safety is our mission.

Facts and figures

Established
2002

800

aviation experts
& administrators



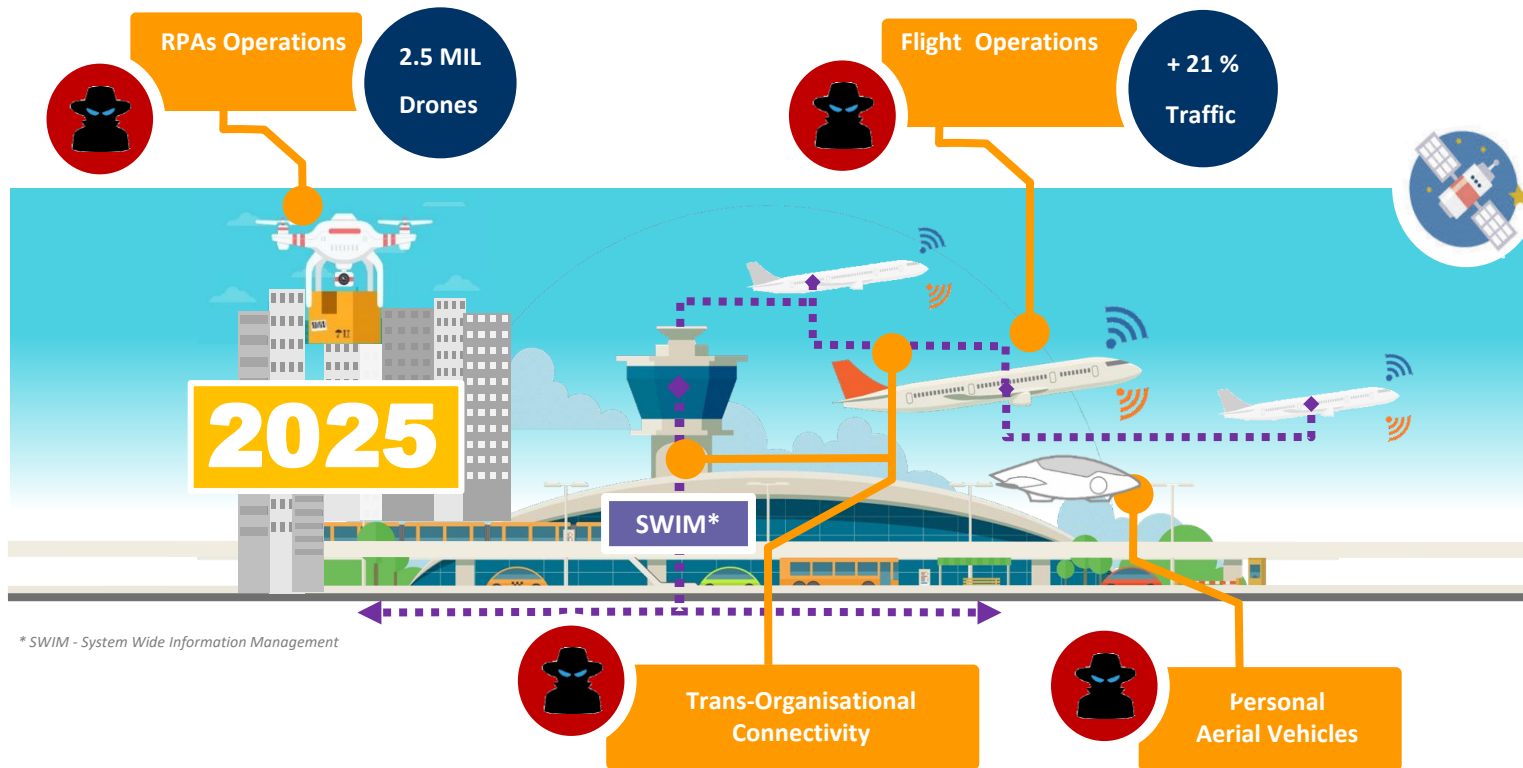
Headquarters in
Cologne
Office in
Brussels

32 EASA member states
 $= 28^* + 4$
EU + Switzerland, Norway
Iceland, Liechtenstein

Tasks

- Draft implementing rules in all fields pertinent to the EASA mission
- Certify & approve products and organisations, in fields where EASA has exclusive competence (e.g. airworthiness)
- Provide oversight and support to Member States in fields where EASA has shared competence (e.g. Air Operations , Air Traffic Management)
- Promote the use of European and worldwide standards
- Cooperate with international actors in order to achieve the highest safety level for EU citizens globally (e.g. EU safety list, Third Country Operators authorisations)

Aviation changes and so does the Risk



A key to reading Security and Safety approaches



The boundary is blurring

“Today’s security threats, including cybersecurity, blur the traditional divide between the two approaches.”

Why?

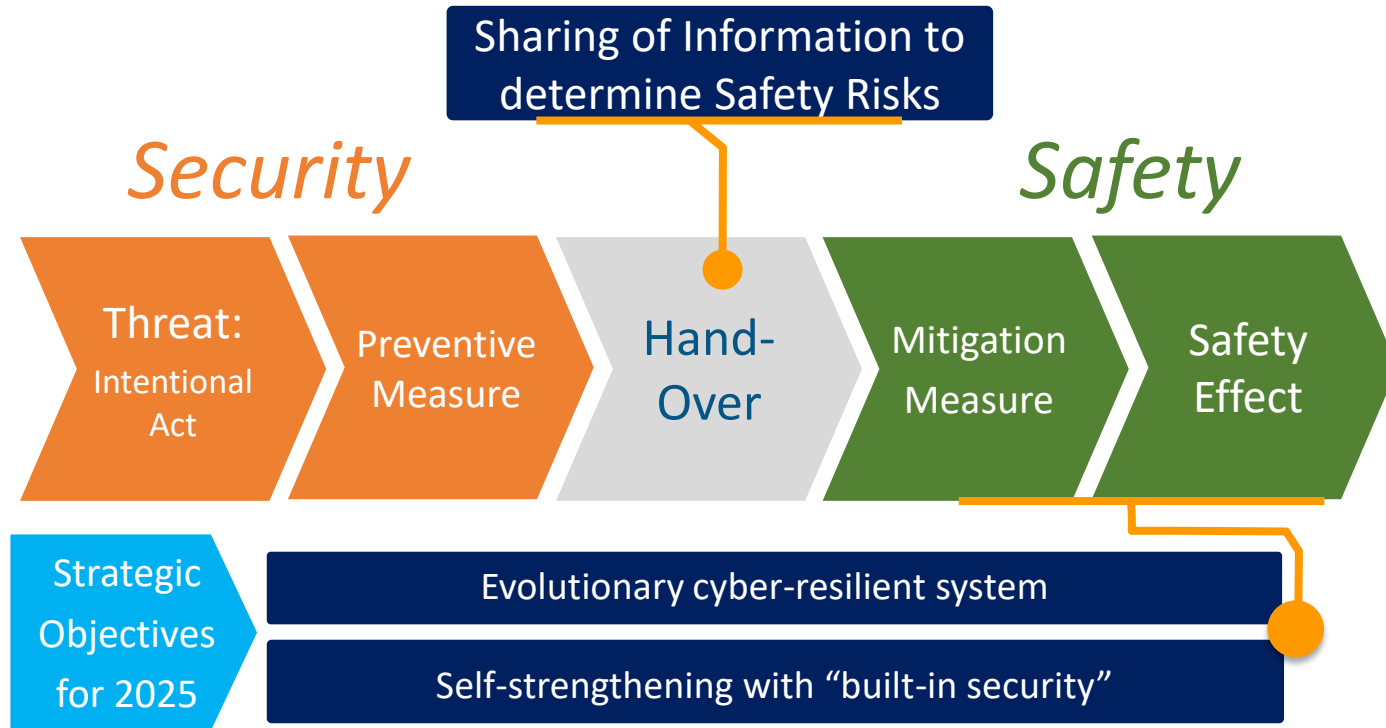
Cyber Threat Actors have no physical borders

Cybersecurity attacks per year is a six figures number...

Threat Actors have an easy access to resources + costs decrease

A reduction of the causes, left alone, is not the best option

Collaborative Aviation Security and Safety



Cybersecurity for Products

RMT. 0648 aimed at

- ➔ **including generic cybersecurity requirements in CS 23, CS 25, CS 27, CS 29, CS E, CS ETSO, CS P and amending AMC-20 and adding AMC-20-42**
- ➔ **Taking into account the interdependencies between aviation safety and security**

Tomorrow Cybersecurity for Organisations

RMT. 0720 is aiming at

- ➔ Introducing provisions for the management of information security in all the aviation domains, including design, production, continuing airworthiness management etc.
- ➔ These provisions include high-level performance-based requirements.

To the point....

Organisation Requirements

- ➔ Personnel requirements
- ➔ Information Security Management System
- ➔ Establishment of internal inf. security reporting scheme
- ➔ Establishment of external inf. security reporting scheme
- ➔ Contracted Activities
- ➔ Record-keeping

EASA Research Needs and Priorities

European Plan for Aviation Safety (EPAS)

Strategic document for required actions at EU level in the fields of safety, security and environment

EASA Research Agenda

- Agency's expert input for new research as well as from externals
- Integrated into EPAS
- Priorities set EASA Research Committee, revisited annually



Develop knowledge on system's security properties

Evolutionary cyber-resilient system

A Cyber Resilient system fails gracefully and manages to keep alive, to an acceptable extent, those functions deemed critical.

R&I - How the “security properties” of connected systems **interrelate** and how get **degraded**?

How should vulnerabilities be managed in complex systems?

The diagram consists of three colored boxes connected by orange lines. At the bottom is a light gray box containing the text 'What kind of system results from the composition (or de-composition) of secure systems?'. Above it and to the right is a light green box containing the text 'How should vulnerabilities be managed in complex systems?'. At the top is a yellow box containing the text 'R&I - How the “security properties” of connected systems interrelate and how get degraded?'. An orange line starts from a dot on the left side of the gray box, goes up and right to a dot on the left side of the green box. Another orange line starts from a dot on the top side of the green box, goes up and right to a dot on the left side of the yellow box. A third orange line starts from a dot on the right side of the yellow box, goes down and left to a dot on the top side of the green box.

What kind of system results from the composition (or de-composition) of secure systems?

Develop knowledge on system's security properties

Self-strengthening with “built-in security”

Security is built-in to face new threats is a more automated way –
The concept of Antifragility.

R&I - How and till which extent can security be automated and dealt with AI/ML approaches?

How an embedded system (used in transport means) can be analysed by an AI/ML to discover vulnerabilities?

How can these vulnerabilities be autonomously patched by preserving at the same time the safety features?

Thank you for your attention

cybersec@easa.europa.eu

Your safety is our mission.

cybersec@easa.europa.eu

An Agency of the European Union 