EASA
European Union Aviation Safety Agency

Introduction to the Sharing of Information

Davide Martini

Senior Expert - Cybersecurity in Aviation

5th – 7th February 2020

Colombo – Sri Lanka

Your safety is our mission.

An Agency of the European Union

Why Sharing is so important in Cybersecurity

We may have some clue about the threat agents, vulnerabilities and exploits to perform a reasonable assessment as of today.

However, new threats may appear without notice and it is a fact that its practically impossible to know all the vulnerabilities of a system.

It is essential to be aware of the existence of elements of Knowledge that will emerge in the future and may change the risk picture.

The practical scheme is provided by the Johari Window that introduces the notion of "unknown unknowns".

Johari Window

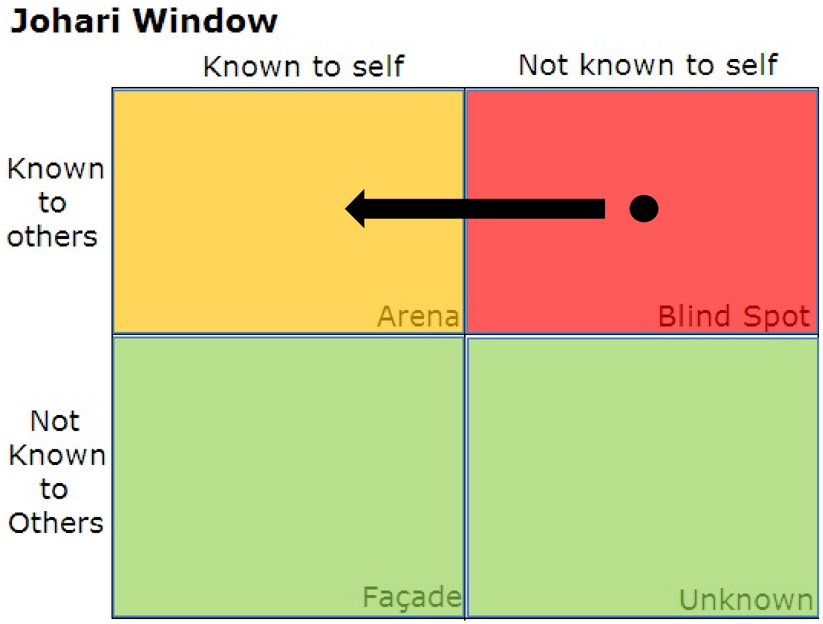
	Known to self	Not known to self
Known to others	Arena	Blind Spot
Not Known to Others	Façade	Unknown

Your (the defender) perspective

- The "Self" is your organisation

The "unknown unknown" is safe until it becomes know to a threat source than turns into a "blind spot" for you

If "others" with knowledge are "allies" there should be means in place to get to the Arena state



Johari Window

	Known to self	Not known to self
Known to others	Arena	Blind Spot
Not Known to Others	Façade	Unknown

The opponent perspective

What if "others" is a Threat Source?

The Blind Spot is a Zero Days quadrant

Vulnerabilities privately known, unpatched and exploitable!

Johari Window

	Known to self	Not known to self
Known to others	Arena	● Blind Spot
Not Known to Others	Façade	Unknown

How to maintain security – Reality Check

NIST - NVD

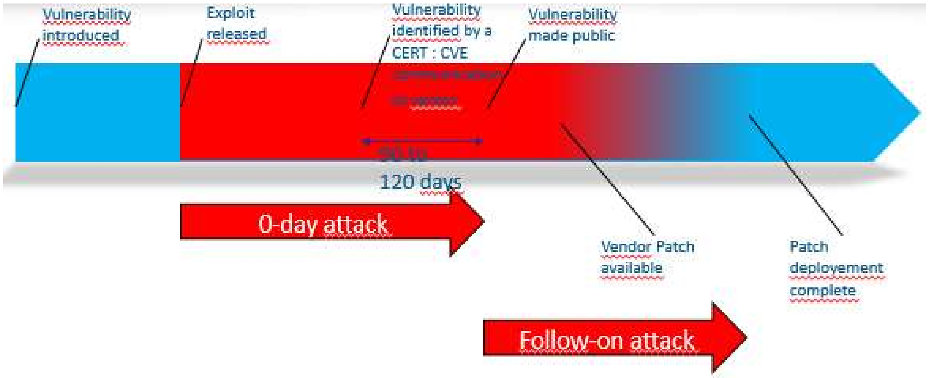
Common Vulnerabilities and Exposures is a list of entries for **publicly** known cybersecurity vulnerabilities.

Let’s have a look…

https://nvd.nist.gov

>100.000 entries ☹

Zero Day – Rand Corporation



7 years average ☹

ICAO Assembly Resolution 39-19

- Encourage government/industry coordination with regard to aviation cybersecurity strategies, policies, and plans, as well as **sharing of information to help identify critical vulnerabilities that need to be addressed**;

- Develop and participate in government/industry partnerships and mechanisms, nationally and internationally, for the systematic sharing of information on cyber threats, incidents, trends and mitigation efforts.

Main Sectorial Initiatives

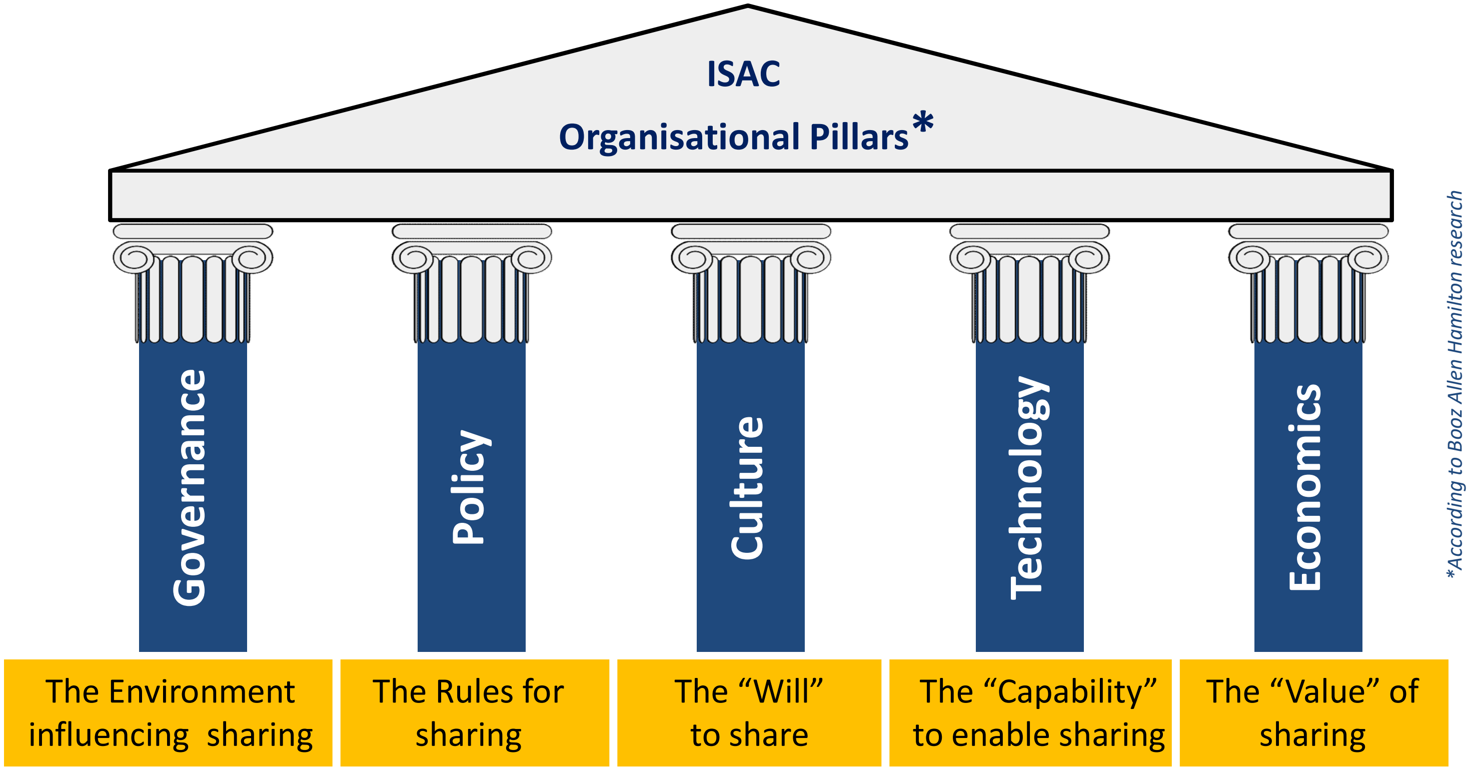
Information Sharing and Analysis Centres (ISACs) and Computer Emergency Response Teams (CERTs)

→ Aviation ISAC (A-ISAC) – US Industry initiative, activities started in 2014, more than 70 members

→ European Centre for Cyber Security in Aviation (ECCSA) – EU cross cutting initiative supported by EASA, activities started in 2019, 26 members and growing

→ EATM- CERT –EUROCONTROL initiative aimed at to providing proactive cyber-security services, within EUROCONTROL, and, on a voluntary basis, to EUROCONTROL stakeholders

Organisational Pillars for Information Sharing



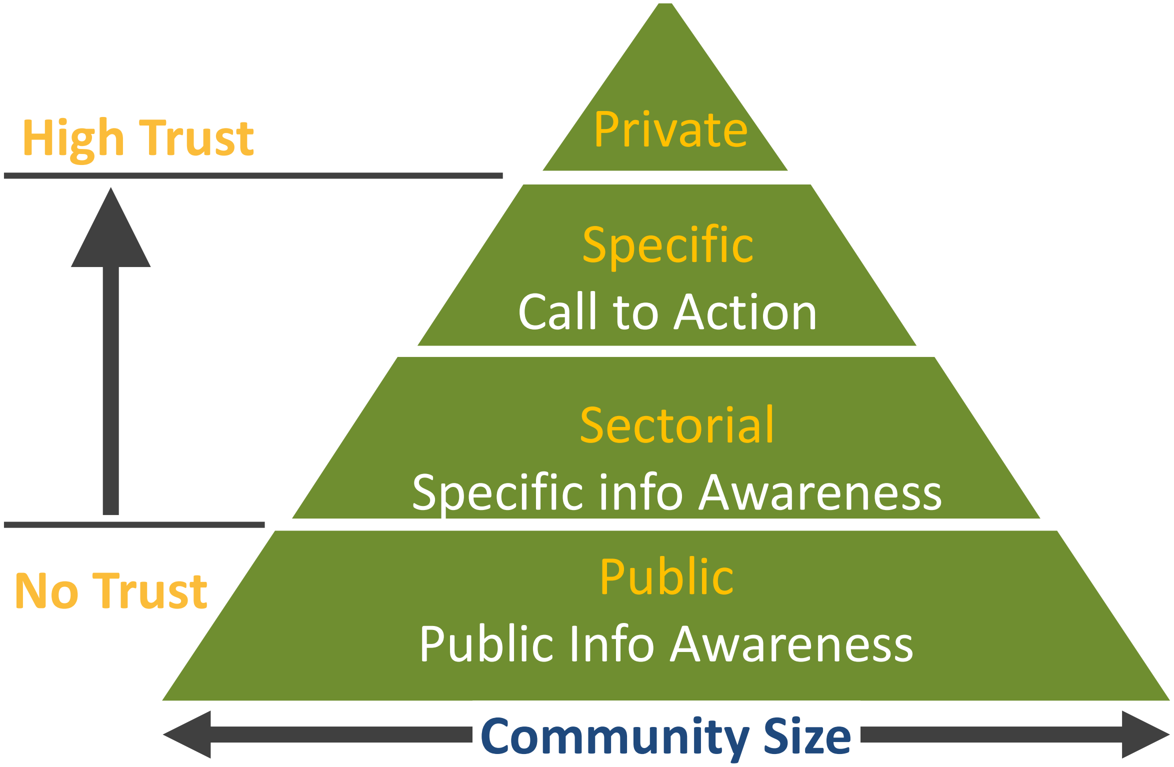
ISAC

Organisational Pillars*

Governance	Policy	Culture	Technology	Economics
The Environment influencing sharing	The Rules for sharing	The "Will" to share	The "Capability" to enable sharing	The "Value" of sharing

*According to Booz Allen Hamilton research

Info Sharing and Trust levels



High Trust

Private

Specific

Call to Action

Sectorial

Specific info Awareness

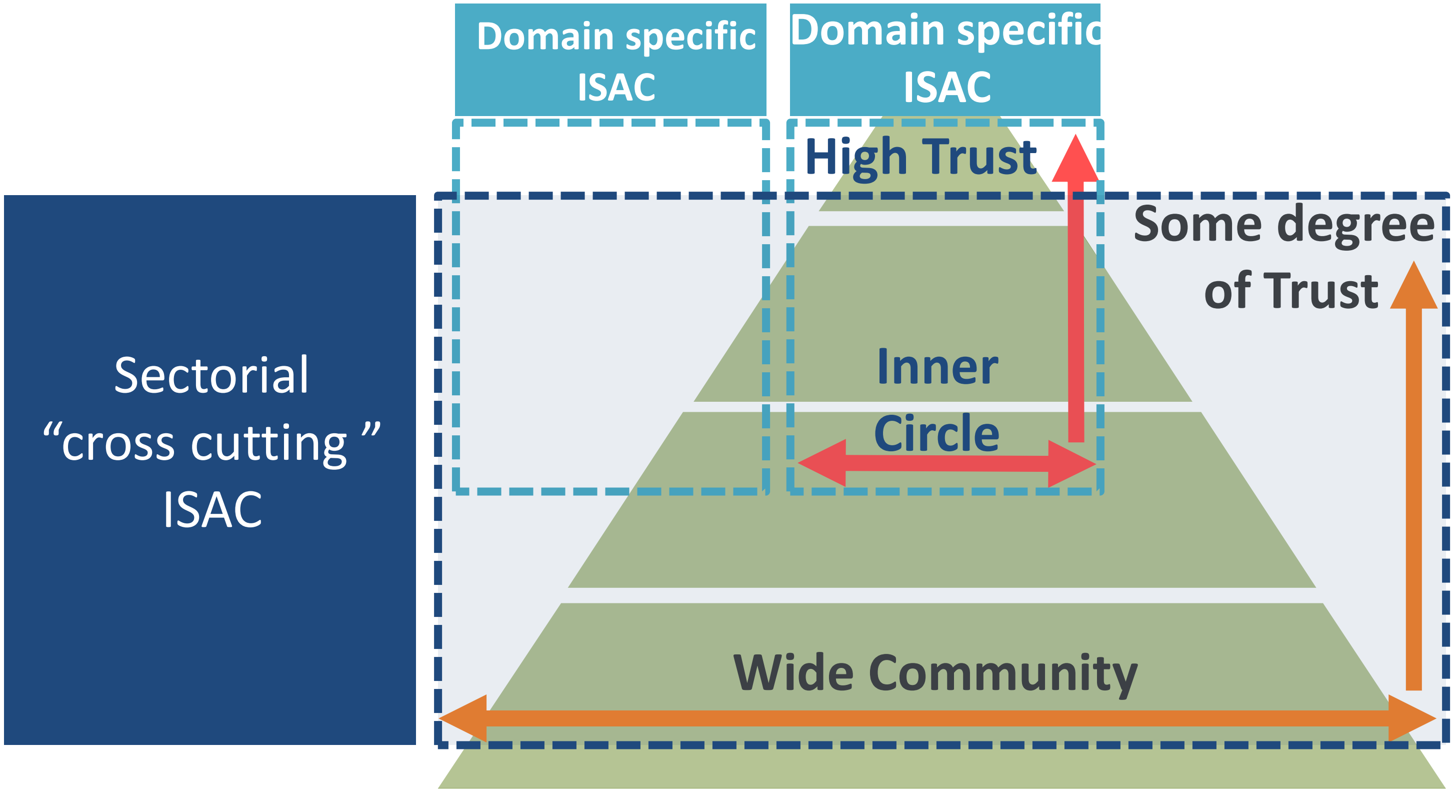
No Trust

Public

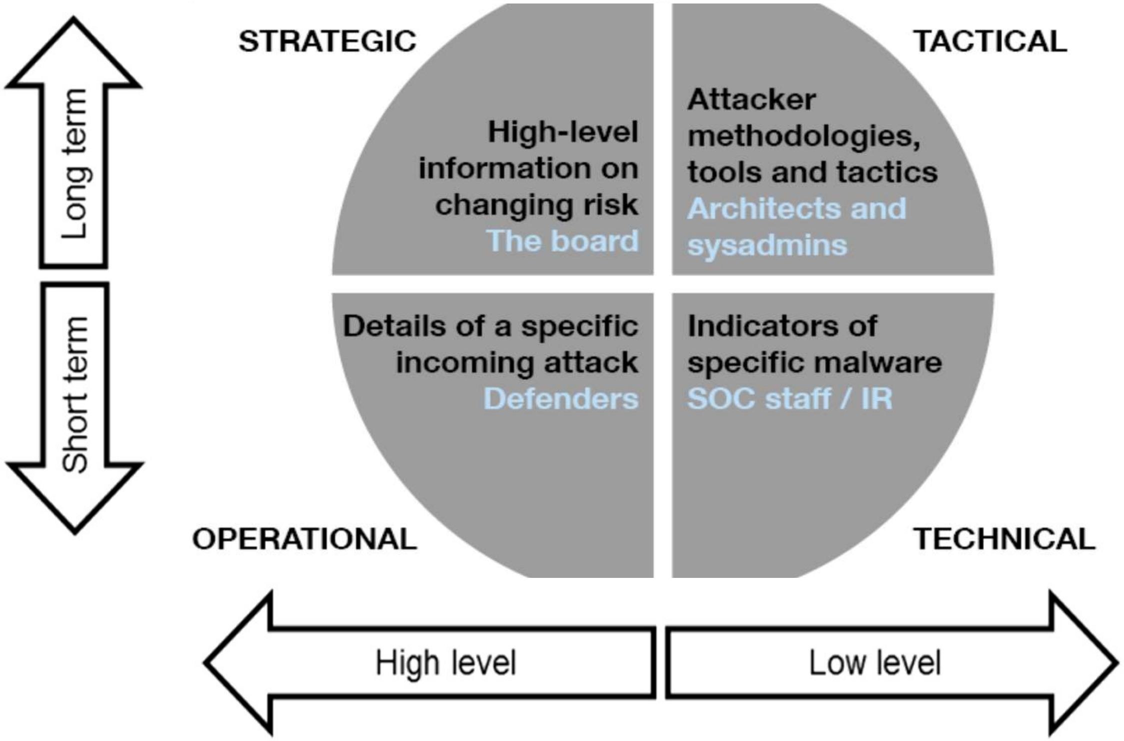
Public Info Awareness

Community Size

Cross cutting vs targeted initiatives



What to Share


STRATEGIC
TACTICAL
High-level information on changing risk
The board
Attacker methodologies, tools and tactics
Architects and sysadmins
Details of a specific incoming attack
Defenders
Indicators of specific malware
SOC staff / IR
OPERATIONAL
TECHNICAL
Long term
Short term
High level
Low level

EASA
European Union Aviation Safety Agency

Sharing of Operational Information

Davide Martini

Senior Expert - Cybersecurity in Aviation

5th – 7th February 2020

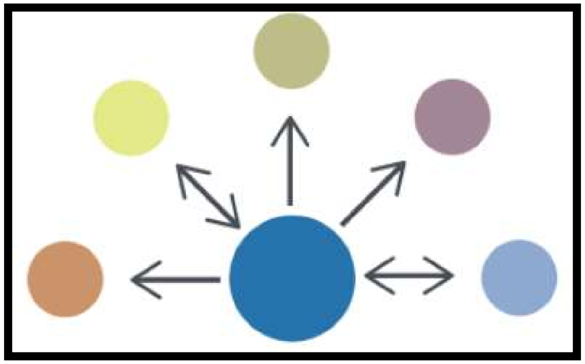
Colombo – Sri Lanka

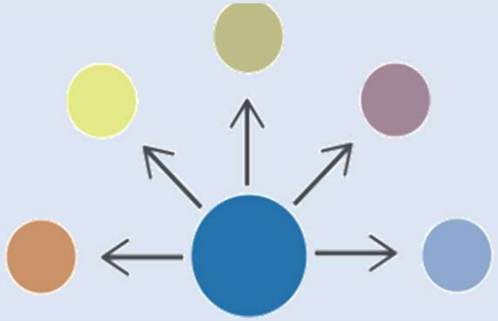
Your safety is our mission.

An Agency of the European Union

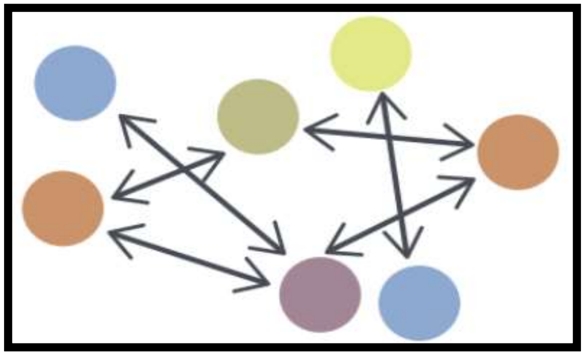
How - Information Sharing Models

Hub and Spoke - one organization acts as a clearinghouse (the hub) for all sharing participants (the spokes). A spoke shares information with the hub, which then re-shares this information with all other spokes. The hub may perform analytics or filtering before re-sharing information. In this architecture, information may flow from spoke to hub and from hub to spoke.





Source/Subscriber - one organization acts as a single source of information for all subscribers. In this architecture, information flows from the source to a subscriber.



Peer to Peer - any number of organizations act as both producers and consumers of information. In this architecture, information flows from one peer to another peer.

How - Sensitive Information sharing Rules

Two main widely adopted rules:

→Traffic Light protocol

→Chatham House Rule

Traffic Light Protocol (TLP)

A way to ***commonly understand*** the exchange of (more or less) sensitive information among a group of organisations

A fundamental concept ***for the originator to signal*** how widely they want their information to be circulated beyond the immediate recipient.

What does the TLP NOT mean to be?

It is **NOT** a way to ***classify information*** according to sensitivity, based upon „harm to the organisation“!

It does NOT imply that those handling this information are „security cleared“

It does **NOT** prescribe a way ***to handle*** the information exchanged

The TLP Tags in Detail: TLP:RED

TLP:RED = Not for disclosure, restricted to participants only.

- Sources may use **TLP:RED** when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's *privacy, reputation, or operations* if misused.
- Recipients may not share **TLP:RED** information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed.
- In the context of a meeting, for example, **TLP:RED** information is limited to those present at the meeting.
- In most circumstances, **TLP:RED** should be exchanged verbally or in person.

(source: FIRST - Forum of Incident Response and Security Teams)

The TLP Tags in Detail: TLP:AMBER

TLP:AMBER = Limited disclosure, restricted to participants' organizations.

- Sources may use **TLP:AMBER** when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
- Recipients may only share **TLP:AMBER** information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.
- Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.

(source: FIRST – Forum of Incident Response and Security Teams)

The TLP Tags in Detail: TLP:GREEN

TLP:GREEN = Limited disclosure, restricted to the community.

- Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.
- Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.
- Information in this category can be circulated widely within a particular community. TLP:GREEN information may not released outside of the community.

(source: FIRST - Forum of Incident Response and Security Teams)

The TLP Tags in Detail: TLP:WHITE

TLP:WHITE = Disclosure is not limited.

- Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.
- Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

(source: FIRST - Forum of Incident Response and Security Teams)

The Chatham House Rule

When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.

The Missing Link - Attribution

→ Some legal frameworks restrict Sharing of full Information

- National Security Considerations

→ Organisations have contractual obligations

- Foreign National Customers
- State Customers

→ Trans-Organisational Information Sharing Facilities need to protect the interests of their constituencies

- Intellectual property, Privacy, Competitive Information

EASA

European Union Aviation Safety Agency

Thank you for your attention!

Questions?

easa.europa.eu/connect

Your safety is our mission.

An Agency of the European Union