

FLASH TALK: Human Factors in Cybersecurity Protecting Aviation Systems from Digital Threats

Jean-Paul Moreaux

Principal – Cybersecurity in Aviation

EASA Annual Safety Conference

30 - 31 October 2024

Your safety is our mission.

An Agency of the European Union 

Some Expectation Management

→ I do not plan to waste your time talking about

- Social Engineering (e.g. Phishing) Attacks
- Viruses, Trojans or Other Malware
- MS Office Macro Attacks

→ What should not be underestimated, though, are

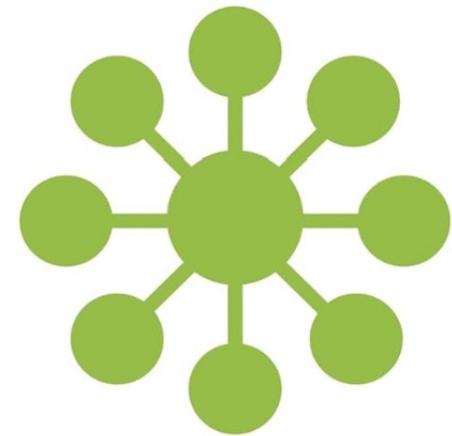
- Uninformed people, taking inadequate, sometimes careless decisions
- Disloyal people, acting irresponsibly
- Malicious people, carrying out Insider Attacks
- People getting tired of repetitive tasks, leading to compliance fatigue
- Random instructions with eroding acceptance, causing fading awareness

Everything is Connected to Everything Else

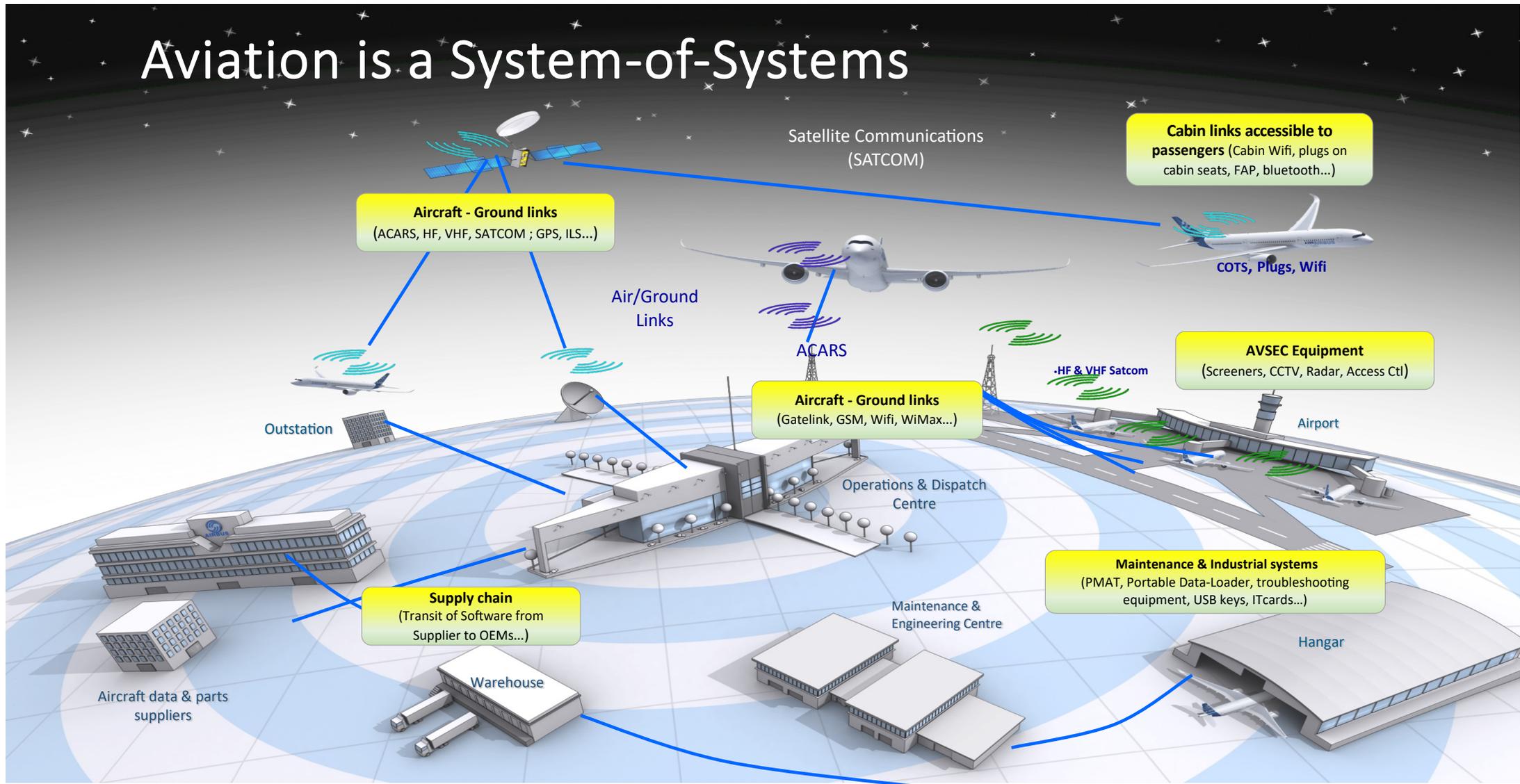
- Albert-László Barabási
 - Romanian-born Hungarian-American physicist, best known for his discoveries in **network science** and **network medicine**
- Notion of “Everything’s a Network”
 - Technological
 - Societal
 - Biological
 - Physiological
 - Psychological

How Everything Is Connected to Everything Else and What It Means for Business, Science, and Everyday Life

Linked

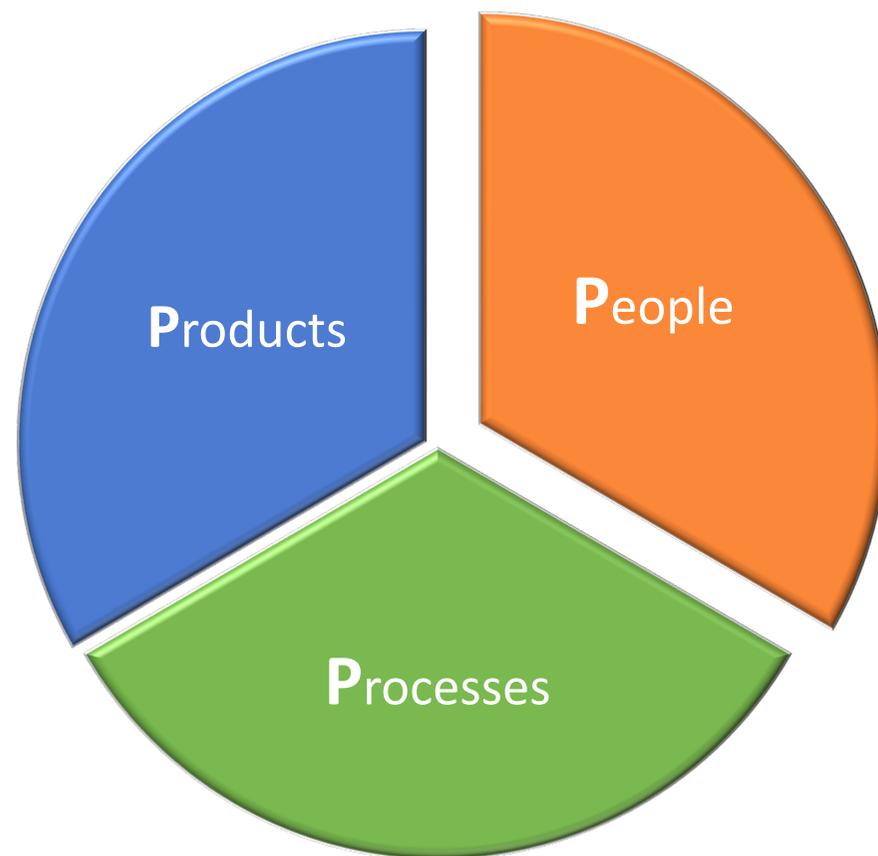


Aviation is a System-of-Systems



A System is

- Composed of
 - People, Processes, Products
- Functionally structured
 - As a System of Systems
- Connected to Other Systems
 - Horizontally, Vertically, or Both



The EASA Approach: Address **All** Pillars



Products

Cyber objectives included in certification processes for all products



People and Processes (i.e. Aviation Organisations)

Part-IS regulatory package in force, applicable by 2026



Information Sharing - Collaborate to Reinforce the system

ECCSA to share knowledge
NoCA to analysis events



Capacity building & Research

For a competent and well aware workforce
To understand the future Threat Landscape



Key System Asset: People

→ Decision-Making in Crisis:

- During security incidents, human judgment is crucial for making real-time decisions that automated systems may not be programmed to handle effectively.

→ First Line of Defense:

- People often serve as the first point of contact for attacks, making them critical in detecting and preventing breaches early on.

→ Adaptability to New Threats:

- Unlike machines, people can adapt quickly to evolving cybersecurity threats, using critical thinking and creativity to devise new defense strategies.

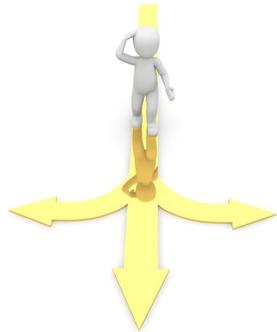
→ Human Awareness and Vigilance:

- Employees can recognize and respond to potential threats, such as phishing attacks or suspicious behavior, better than automated systems alone.

→ Access Control and Enforcement:

- Employees are responsible for managing and enforcing access controls, safeguarding sensitive information, and ensuring compliance with security protocols.

The People Focus: Types



Uninformed People

- Make them aware of the risks for the organisation and the different disciplines to involve.
- Encourage them to create internal networks of specialists to address challenges as transversal as Information Security
- Messages from experts need to be clear and concise to empower decision makers to implement measures adequately protecting against organizational risks



Disloyal People

- It may be too late to bring them back into the group of loyal employees, but worth any attempt
- Educate them about the importance of adherence to rules and processes
- Obtain their explicit minimum buy-in
- Nevertheless, as they may not intentionally act maliciously, measures need to be in place to limit the effects of neglect or unwillingness



Malicious People

- They misuse legitimate permissions for malicious acts
- Treat them as any unacceptable risk:



- They intentionally act maliciously, so measures need to be in place to limit the effects of those acts

The People Focus: Operating Conditions



Compliance Fatigue

- Complex processes & procedures sometimes contain loopholes, which may lead to people using shortcuts
- Operational incentives may also lead to the inclination for using shortcuts
- Maintaining awareness is supported by a sense of purpose that people need to keep intrinsic motivation for compliance high



Fading Awareness

- Complex and rarely used information or rarely encountered situations are easily misinterpreted, overlooked or simply forgotten
- Rules which are not perceived as obviously important or just random are often assessed being expendable
- Extra efforts are needed to keep risk awareness levels high and the importance of own contribution well understood

Remove Silos! Example: Safety/Info Sec Risk Assessment

