EASA
European Union Aviation Safety Agency

Cybersecurity in Aviation

An Introduction

Hamburg Aerospace Lecture Series

RAeS Annual Gerhard Sedlmayr Lecture
Lecture organised by RAeS Hamburg
in cooperation with the DGLR, VDI, ZAL & HAW Hamburg
11.9.2023

Jean-Paul Moreaux
Principal, Cybersecurity in Aviation

Picture credits: Adobe Stock / Pixabay (inspiredimages, emslichter)

Your safety is our mission.

https://doi.org/10.5281/zenodo.8396741

An Agency of the European Union

Agenda

- Why are we talking about “Cyber”?
- A few more reasons to talk!
- What drives us to talk “Cyber”?
- Where Do we want to go?
- What about Risk?
- And Risk Management?
- What is covered by Part-IS?

Why are we talking about “Cyber”?

Attacks on Aviation already started (already before 2017)!

POLICY + POLITICS

FAA Hack Attack Did Not Hit Air-Traffic Control…Yet

By Aliya Sternstein, Next Gov
April 6, 2015

Hackers earlier this year attacked a Federal Aviation Administration network with malicious software, agency officials said Monday.

In early February, FAA discovered "a known virus" spread via email on "its administrative computer system," agency spokeswoman Laura Brown told *Nextgov*. "After a thorough review, the FAA did not identify any damage to agency systems," she added.

An upcoming competition among
center might be altered as a result
award notice that casually mentio

Related: Congress Enraged by

HOME / POLICY / CYBERSECURITY

Airlines under siege from hackers

Getty Images

By Cory Bennett - 05/10/15 06:00 AM EDT

The airline industry is under siege from cyberattackers, and lawmakers are struggling to help.

In recent months, hackers have infiltrated the U.S. air traffic control system, forced airlines to ground planes and potentially stolen detailed travel records on millions of people.

Yet the industry lacks strict requirements to report these incidents or even adhere to specific cybersecurity standards.

"There should be a requirement for immediate reporting to the federal government," Sen. Susan Collins (R-Maine), who chairs the Appropriations subcommittee that oversees the Federal Aviation Administration (FAA), told The Hill.

"We need to address that," agreed Sen. Bill Nelson (Fla.), the top Democrat on the Senate Commerce Committee.

#TECHNOLOGY NEWS NOVEMBER 30, 2017 / 3:30 PM / A DAY AGO

'Bomb on board' wi-fi network causes Turkish Airlines flight to be diverted

Reuters Staff 1 MIN READ

ANKARA (Reuters) - A Turkish Airlines flight from Nairobi to Istanbul was diverted after the detection of a wi-fi network called "bomb on board" that alarmed the passengers, the airline said on Thursday.

In a statement, Turkish Airlines said the flight made an emergency landing at the Khartoum airport in Sudan, but the flight was safely resumed after security inspections on all passengers and the aircraft.

"Experts said the wi-fi network in question wa
irregularities were seen after security procedu
passengers were brought back on the plane on
Turkish Airlines said.

Individuals can create personal wi-fi networks
phones and name them what they want.

The airline said all 100 passengers were broug
did not say whether authorities had identified
the wi-fi network.

World Algeria

Air France cyberattack: Who is the Moujahidin Team and why are they waging cyber-jihad?

By Vara Staff
April 2, 2015 18:18 BST

El Moujahidin calling card (Vara Cyber Security)

On 30 March 2015, a little-known hacking group calling itself the 'Moujahidin Team' (aka El Moujahidin) claimed credit for a cyberattack on Air France. The defacement on the website showed the group's logo and contained the message:

> "I promise you O my homeland that I will remain the faithful soldier that defends your border with the blood... and to protect the trust, to deliver the message, and to keep going on the method of 'Let Algeria live, freely independent, with blood and work of its sons, Allah permitting'"

CYBER ATTACK

Hackers break into Lufthansa customer database

Cyber-attackers have obtained info on a number of passengers using the Lufthansa website. The hackers used frequent-flyers miles to obtain vouchers and redeem rewards.

o gain access to individual passenger accounts on company's website LH.com,
nsa confirmed Friday.
mpt countermeasures, but it "had not been able to prevent illicit access to
cording to company's representatives.
undred customer pages," a Lufthansa spokesman told DPA news agency after
gazine Der Spiegel broke the story.

UNITED

Reservations Travel information Deals & offers MileagePl

Home > Contact us > Bug Bounty Program

United Airlines bug bounty program

At United, we take your safety, security and privacy seriously. We utilize best practices and are confident that our systems are secure. We are committed to protecting our customers' privacy and the personal data we receive from them, which is why we are offering a bug bounty program — the first of its kind within the airline industry. We believe that this program will further bolster our security and allow us to continue to provide excellent service. If you think you have discovered a potential security bug that affects our websites, apps and/or online portals, please let us know. If the submission meets our requirements, we'll gladly reward you for your time and effort.

Before reporting a security bug, please review the "United Terms." By participating in the bug bounty program, you agree to comply with these terms.

What is a bug bounty program?

A bug bounty program permits independent researchers to discover and report security issues that affect the confidentiality, integrity and/or availability of customer or company information and rewards them for being the first to discover a bug.

Eligibility requirements

To ensure that submissions and payouts are fair and relevant, the following eligibility requirements and guidelines apply to all researchers submitting bug reports:

- All bugs must be new discoveries. Award miles will be provided only to the first researcher who submits a particular security bug.
- The researcher must be a MileagePlus member in good standing. If you're not yet a member, join the MileagePlus program now.
- The researcher must not reside in a country currently on a United States sanctions list.
- The researcher submitting the bug must not be an employee of United Airlines, any Star Alliance™ member airline or any other partner airline, or a family member or household member of an employee of United Airlines or any partner airline.
- The researcher submitting the bug must not be the author of the vulnerable code.

Mail Online WIRES

Home | News | U.S. | Sport | TV&Showbiz | Australia | Femail | Health | Science | Money |
Wires Home

Major technical trouble disrupts traffic at Amsterdam airport

By REUTERS
PUBLISHED: 12:20 GMT, 21 November 2017 | UPDATED: 16:35 GMT, 21 November 2017

Share

AMSTERDAM, Nov 21 (Reuters) - Malfunctioning air traffic control systems at Amsterdam's Schiphol airport on Tuesday led to dozens of cancelled flights and long delays at one of Europe's busiest transportation hubs.

The problems were resolved around 1600 GMT, but it would still take hours for operations to return to normal, a spokeswoman for Air Traffic Control the Netherlands said. She said it was still unclear what caused the problems, but excluded the possibility of a cyber attack.

Air France-KLM, the national Dutch carrier, said it had scrapped 50 flights. Delays ran up to more than four hours on other flights, a KLM spokesman said.

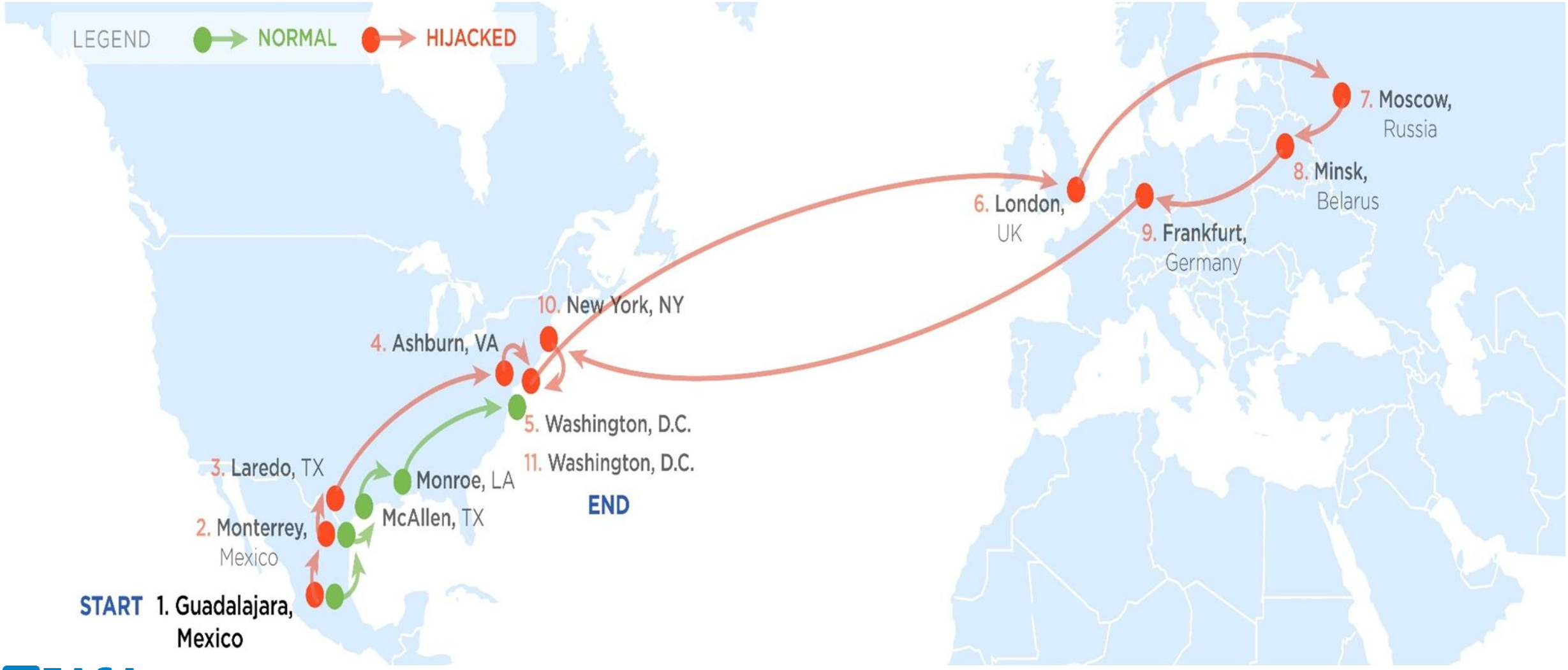
A spokesman for Schiphol could not give an exact number of cancellations and delays, but the airport's website showed problems with almost all incoming and outgoing afternoon flights.

On its web site, Eurocontrol, Europe's organization for air traffic control coordination and planning, showed a large number of flights to Schiphol were delayed more than 30 minutes. In a notice, it said airplanes could opt to divert to other airports.

A major computer malfunction in February crippled traffic at Schiphol for hours, causing delays or cancellations on more than 100 flights.

EASA

Example: Internet Infrastructure/Traffic Diversion



Example: Well Known Vulnerabilities -„Heartbleed“

Flaw in **OpenSSL Libary**

a widely used implementation of the Transport Layer Security protocol

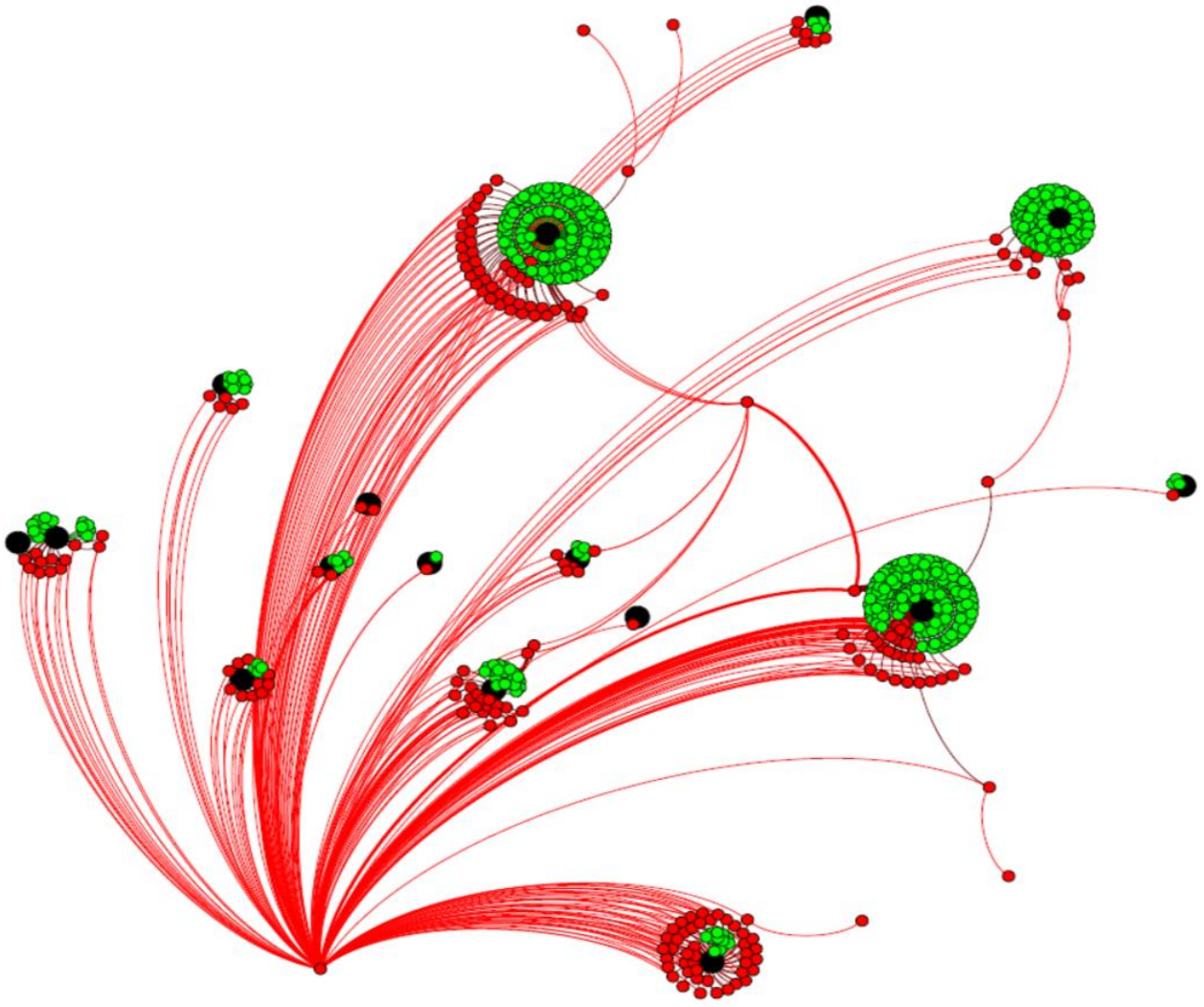
Allows for **access of credentials** of previous communication session

Disclosed in **April 2014**

Registered in a public Database as CVE-2014-0160

2014 … that’s more than 8 years ago!

How many systems still vulnerable?



A few more reasons to talk!

And in Reality: The Notion of Intent!

SAFETY

SECURITY

FORTUITY

INTENT

And in Reality: The Notion of Intent!

SAFETY

SECURITY

The notion of

INTENT

Transition of Notions

From a **Safety Notion** to a **Security-for-Safety Notion**

Reliable System

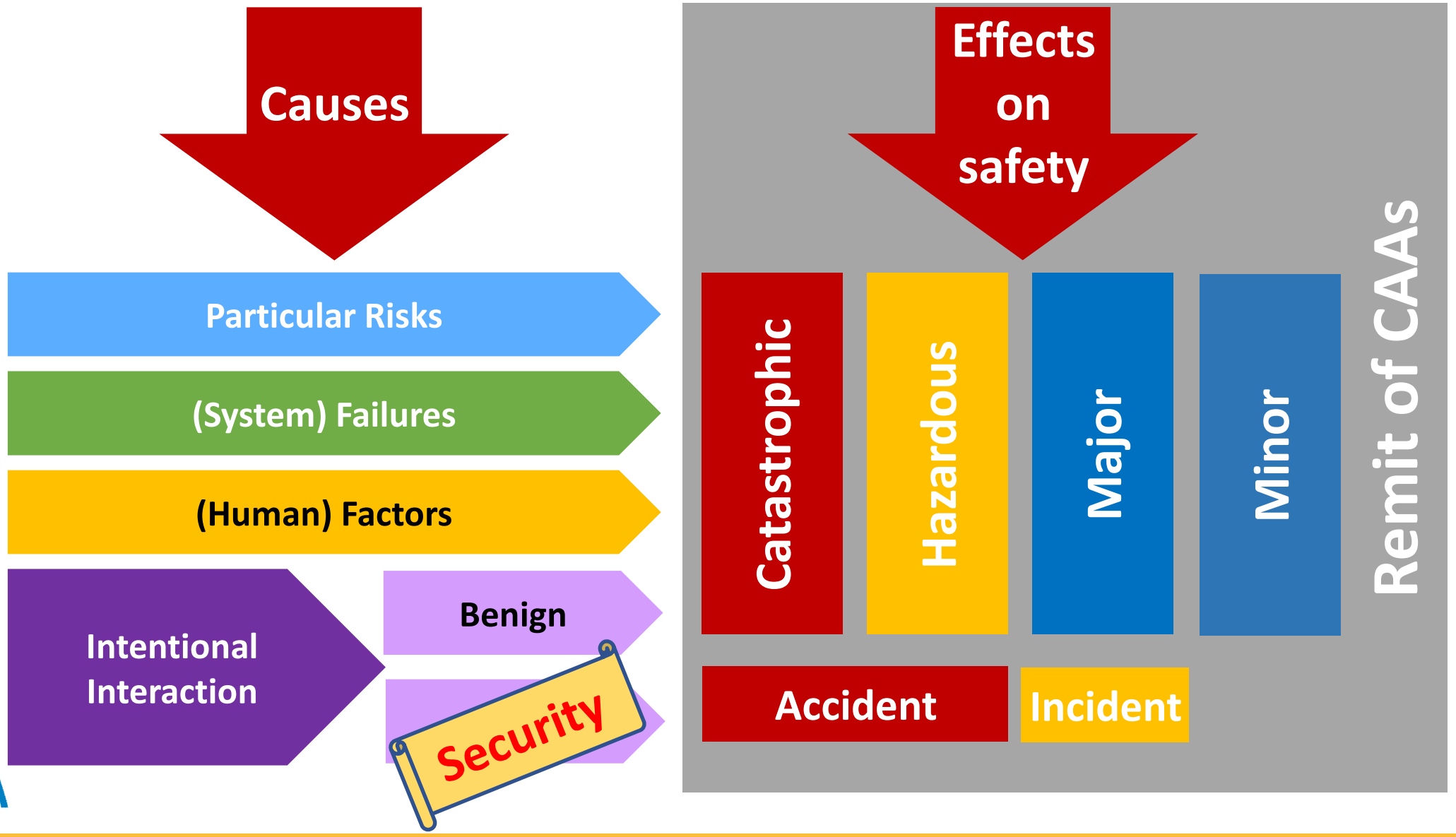
A **Reliable System** does, what it is supposed to do.

Secure System

A **Secure** System does, what it is supposed to do.

And nothing else!

Relationship between Example Causes & Effects



What drives us to talk “Cyber”?

Also in Security, the environment drives what we do

Threat Landscape will change, so the security process must evolve with the perceived level of risk

The Tools for adversaries change rapidly, with constantly enhanced functionality, at a fraction of the original cost

The required Skill level of adversaries deteriorates, as tools are becoming more and more automated and fully comprehensive

The actual Skills of adversaries evolve, as they practice on other targets

And: **There are services out there to perform cyber attacks for you!**

Security is an evolutionary Process, not a Product

As the **security environment** evolves, protections will have to be adapted

Technologies will change, so the security process must evolve with the perceived level of risk

Societal expectations of aviation will change, so the security process must evolve with the perceived level of safety risk

Business Direction of Aviation Industry will change, so the security process must evolve with the perceived level of risk

The whole is more than the sum of its parts

Architecture

- ✓ Each system shall protect itself against it's individual risks
- ✓ All interacting measures contribute to the individual Level of Protection
- ✓ **Functional Architecture ≠ Security Architecture**

Composability

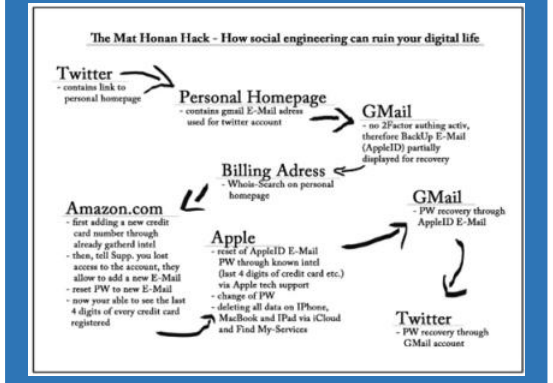
- ✓ Functional System Integration requires compatible interfaces, Security System Integration requires coherent and consistent behaviour
- ✓ Understanding aviation as a **System-of-Systems** is the prerequisite to an integrated and global cybersecurity approach by all stakeholders

Everything is linked with everything else

Individual systems with **aligned protections** are collectively creating a secure environment for the whole aviation system

Evolving technical and operational risks of individual systems require adjusted System-of-Systems risk assessments

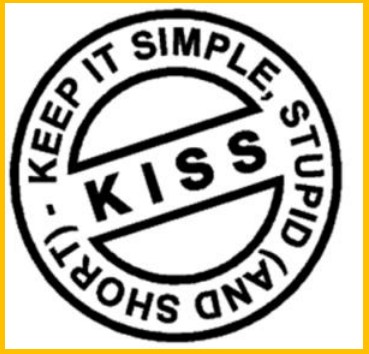
Evolutionary risk aware system-of-systems are capable of interaction, to enhance mutual levels of protection



Self-healing architecture concepts actively 'manage' individually protected systems in securing an enhanced environment

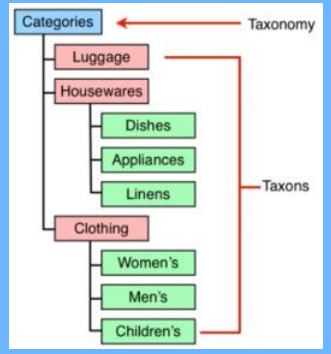
Complexity is the Enemy of Security

"Keep It Simple, and Stupid": A key goal in Design, Implementation, Operation and Upgrade, making security a naturally evolving process



Linking the **security process** to identified (safety) **risks** helps understanding, why the process is necessary

Developing agreed **coherent methodologies** for risk assessments and threat taxonomy supports a uniform view of the System-of-Systems



Simple security message: **<u>Safety & Security</u> in all aspects of aviation!**

EASA

Where Do we want to go?

Resiliency as EU Objective

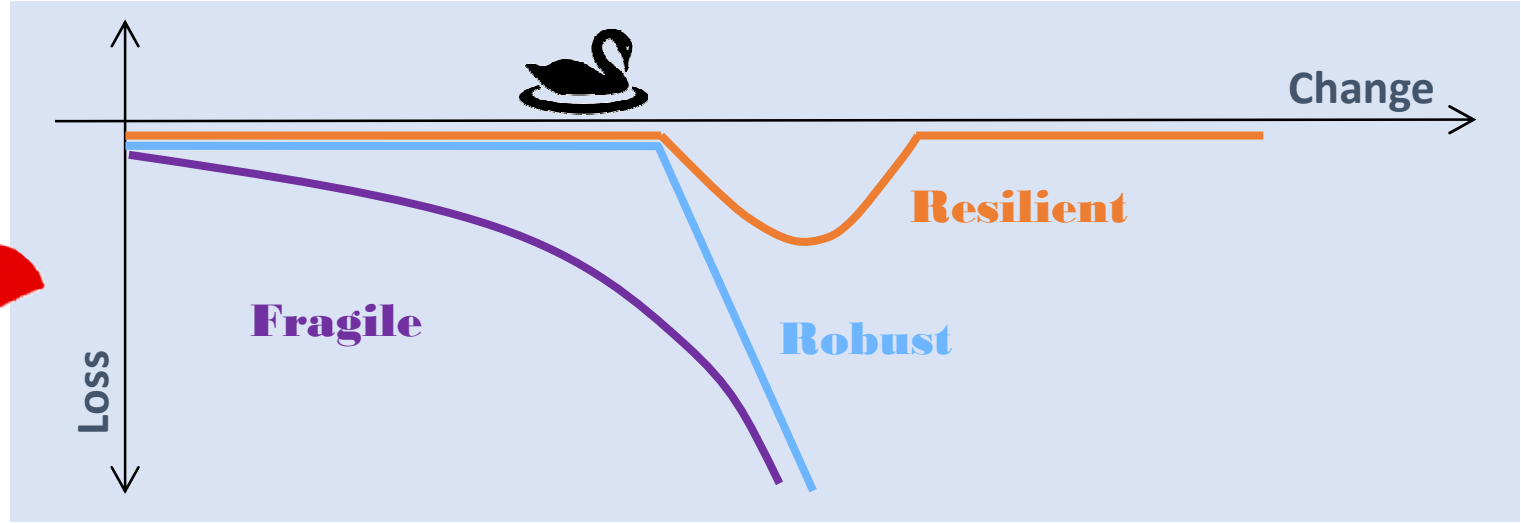
By 2025

European Aviation System is Resilient to Cyber Threats

How we define it

The ability to **prevent** disruptions, to **prepare** for and adapt to changing conditions and to **respond** and **recover** rapidly from disruptions ensuring the continuity of services.

How we see it



EASA

Practical elements of Resilience

KEY ELEMENTS

Identify critical services and scenarios that could be affected

Build layered systems and allow partial and recoverable failures

Stay networked to predict new threats and be prepared

Protect Crown Jewels

Avoid Domino effect

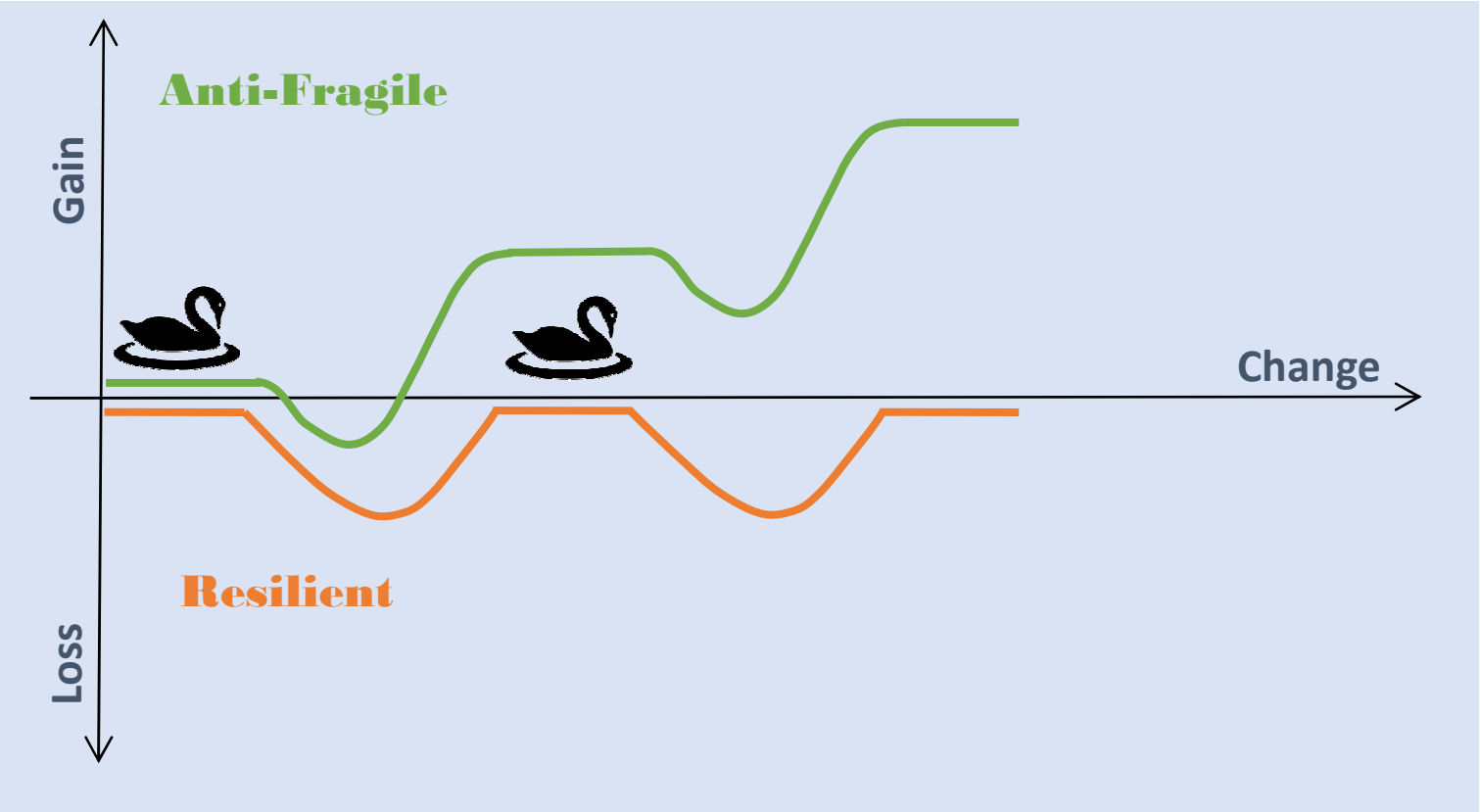
Collaborative Intelligence

EASA

We have a dream…

By 2035

European Aviation System on its way to Security



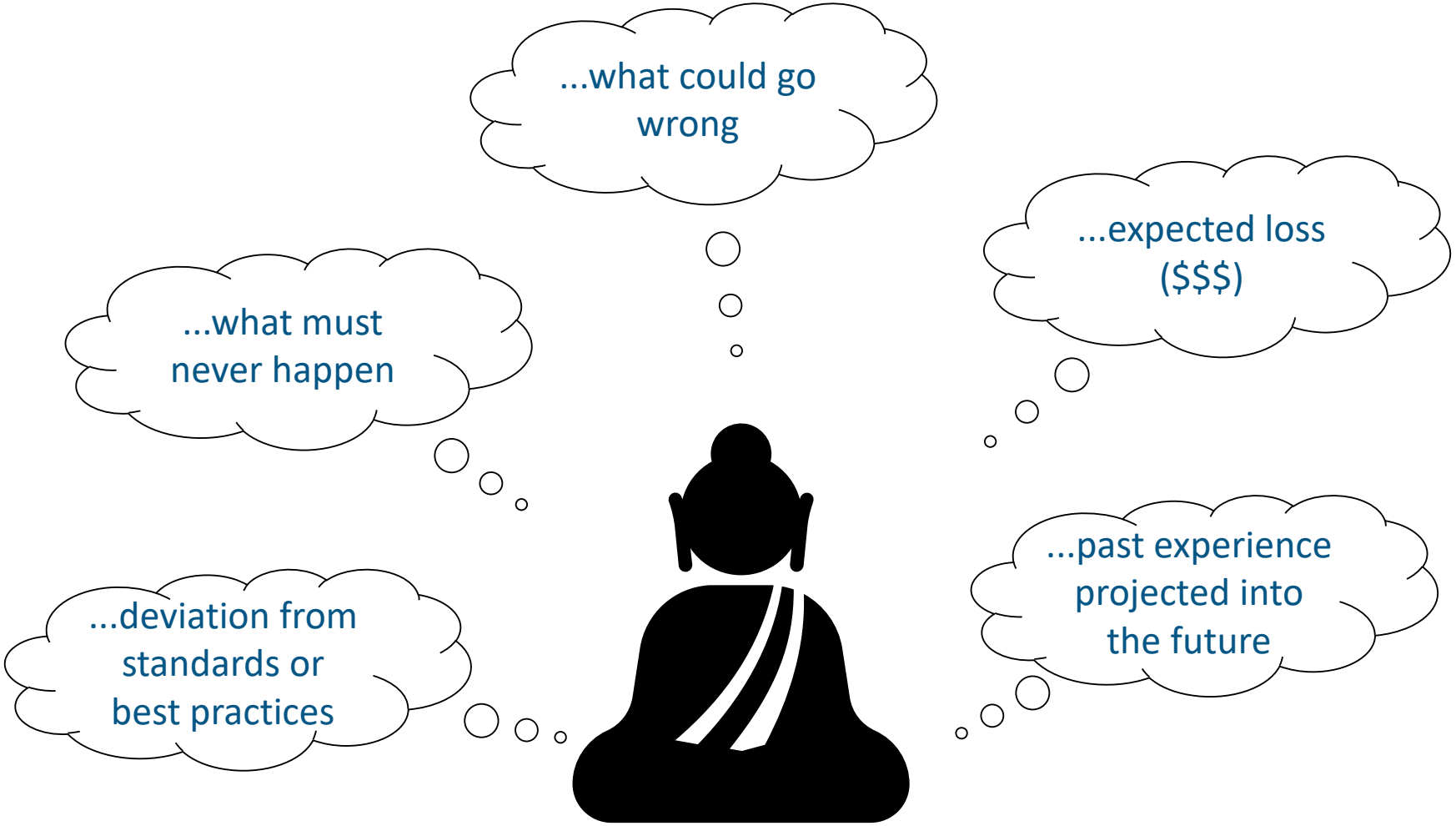
What about Risk?

Where we are without Risk Management!

A few thoughts…

- → What is Risk?
  - → A few perspectives and reflections
- → Dimensions of Multi-Stakeholder Risk Management
  - → System-of-System (aviation is highly interconnected)
  - → End-to-End Security (communication, mission, life-cycle)
  - → Trustworthiness (reliance upon other stakeholders)
- → How to approach Shared Trans-Organisational Risk Management

What is Risk?


...what could go wrong
...expected loss ($$$)
...what must never happen
...past experience projected into the future
...deviation from standards or best practices

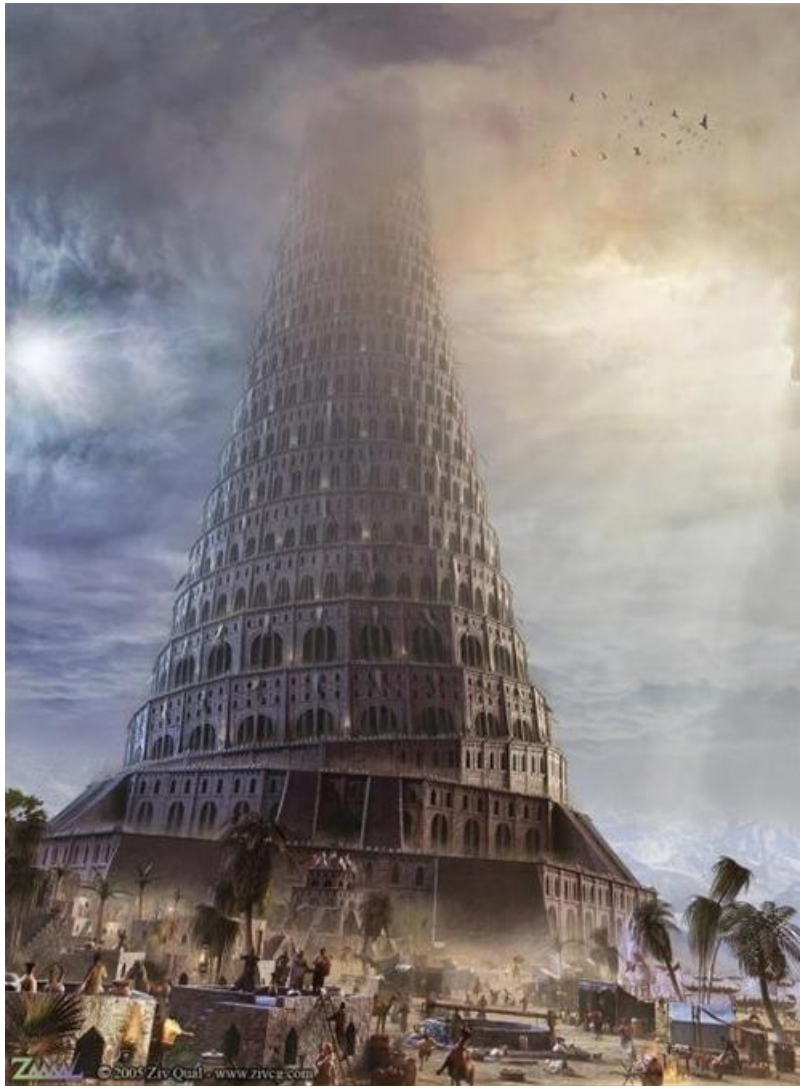
Managing Risk in a Multi-Stakeholder Environment

Civil Aviation, a highly regulated business

- Risks are ultimately related to lives of crew, passengers and individuals on ground
- Implicitly, society expects states to protect its members against such risks
- Risk Acceptability is largely a matter of regulatory approval and oversight

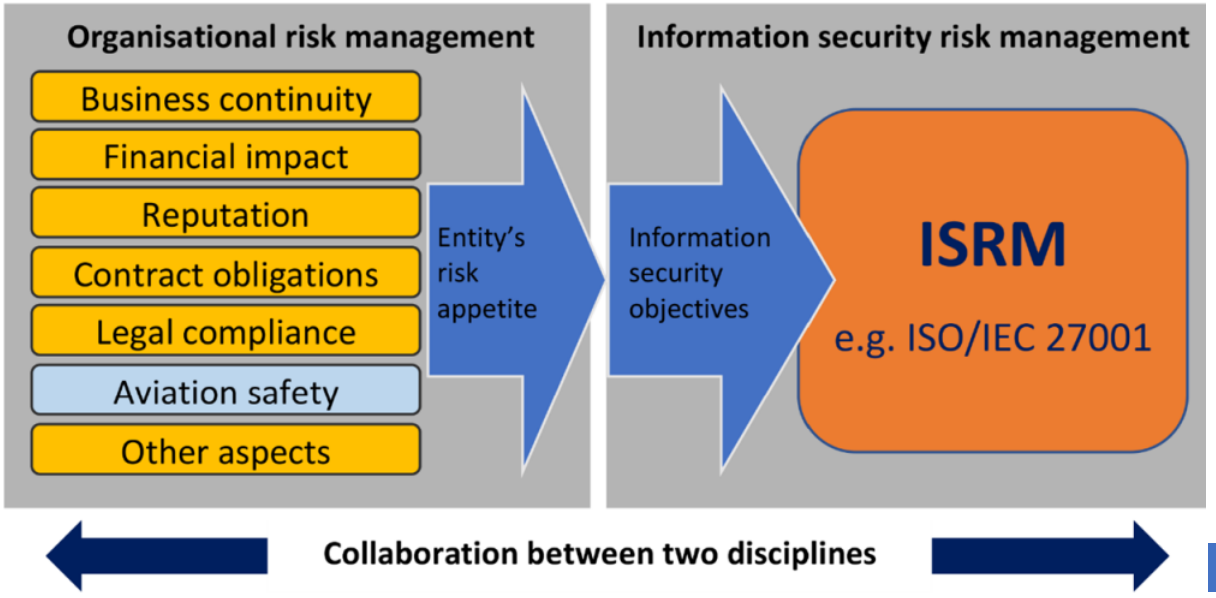
Civil Aviation, an international business

- ICAO has 193 States Contracting States from diverse regions & continents
- Each having developed its own culture, including perception of Risk

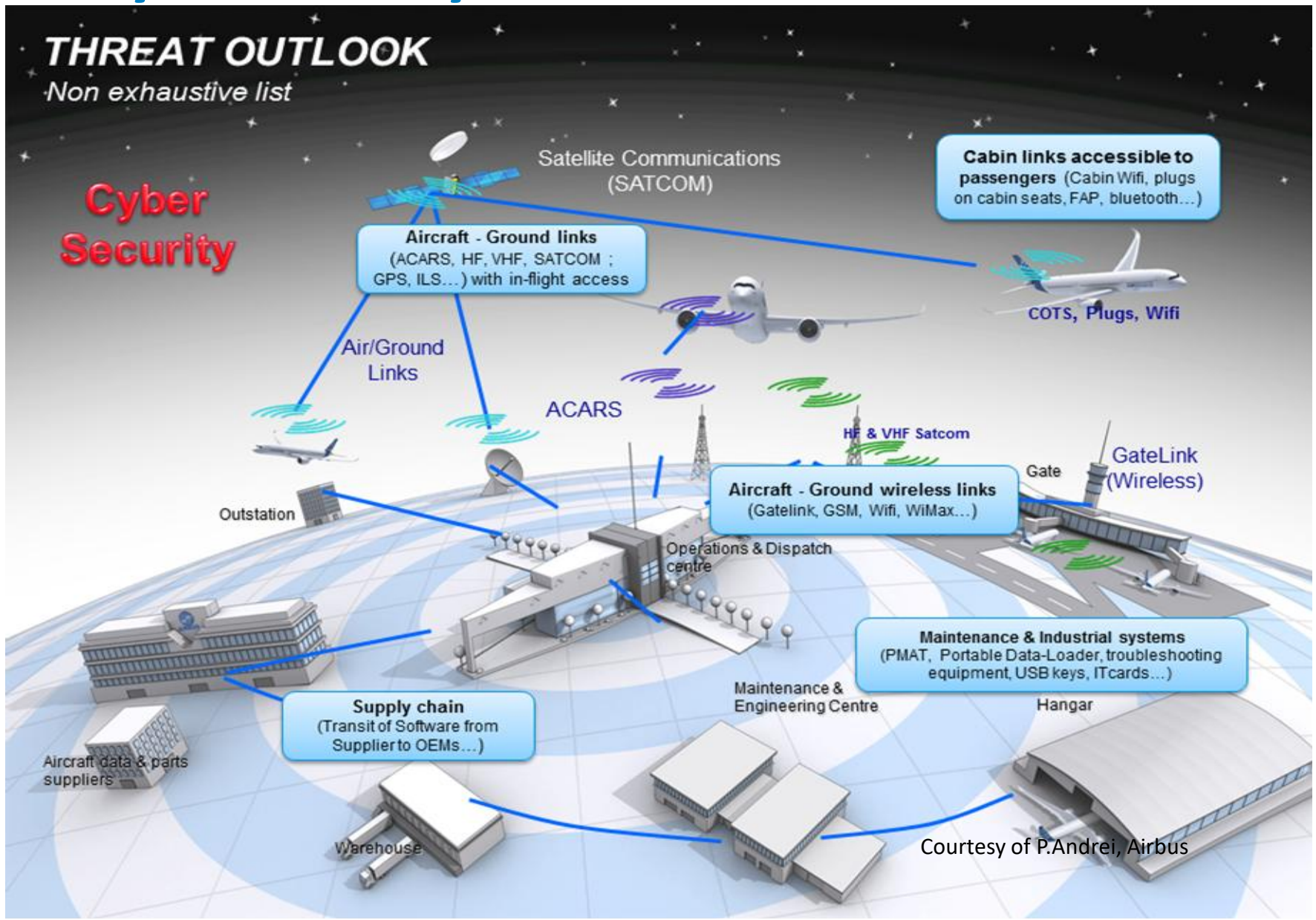


What are we trying to achieve?

- Evaluate risk **across the whole aviation system** to include
  - ANSPs, ACSPs, Aircrafts, Airlines
- Enable **effective risk management** considering variable risk appetite
- Coordinate risk treatment
  - The security level of a system is the one of its weakest sub-system
  - Preserve critical functions globally
  - Maintain operational capability
  - Develop resilience
- Be able to sustain **crisis periods**
- Achieve **maturity**



Aviation is a System-of-Systems!



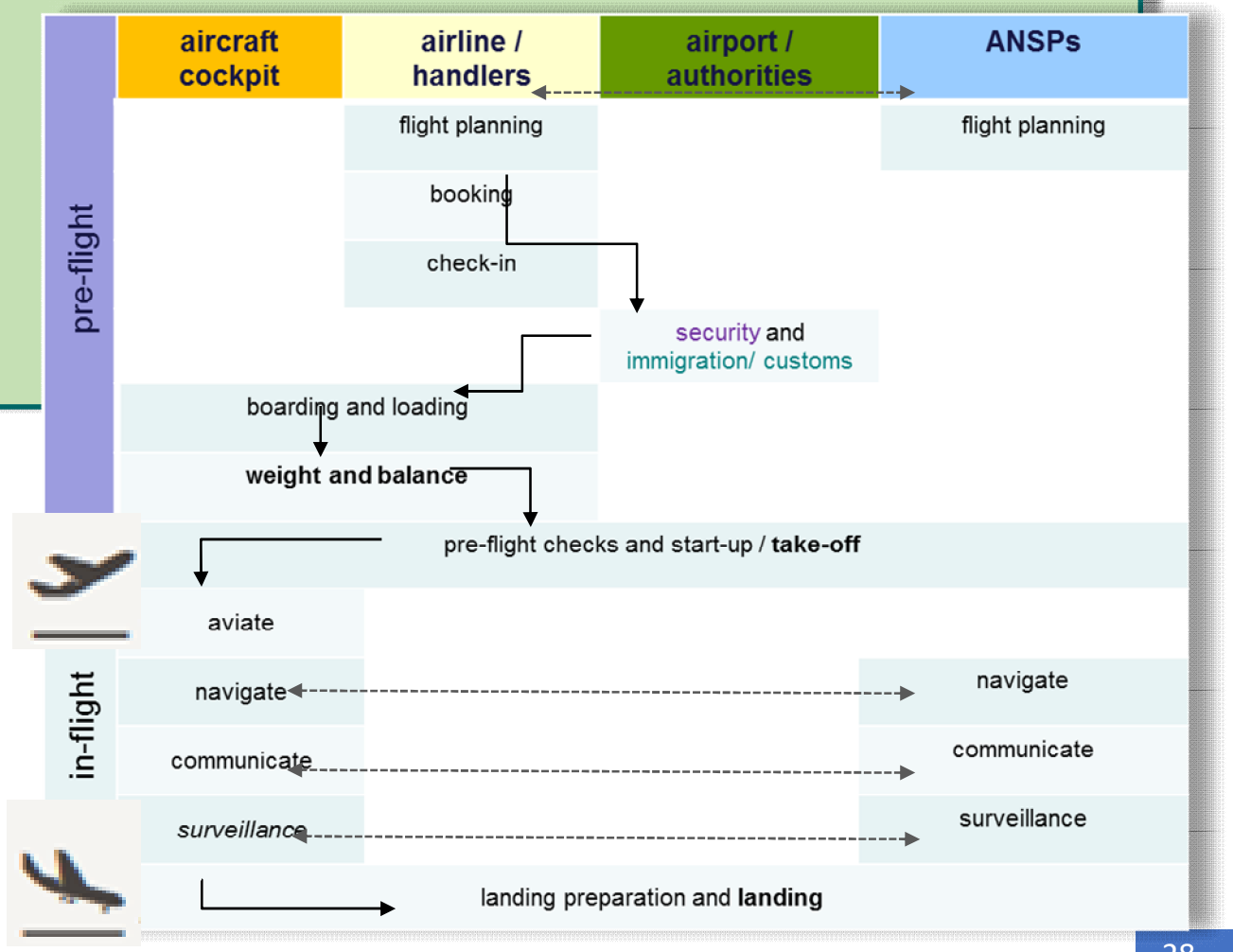
Courtesy of P.Andrei, Airbus

Avoid the stove pipe risk management

- Identify security needs across the system
  - Identifying your critical assets (crown jewels) and less critical ones
- Standardise risk appetite
  - To know what it costs you to lose them - the jewels
- Develop Risk assessment baseline
  - Not egocentric
  - Not only business oriented – favouring availability
  - Make it reproducible – same system, different stakeholder
- Agree on risk treatment

Focus on the End-to-End Perspective

Mission: Flying Safely



Life-cycle: From Cradle to Grave

Communication: From the originator to the consumer

EASA

Civil Aviation continues to face a challenge

1 The **Coherence** of Risk Assessments

2 The **Comparability** of Risk Evaluation

3 The **Commonality** of Risk Acceptability

EASA

The Risk Assessment Stages (ISO 27005)

Information to be shared

Scope and Boundaries

Scenarios

Impact Criteria

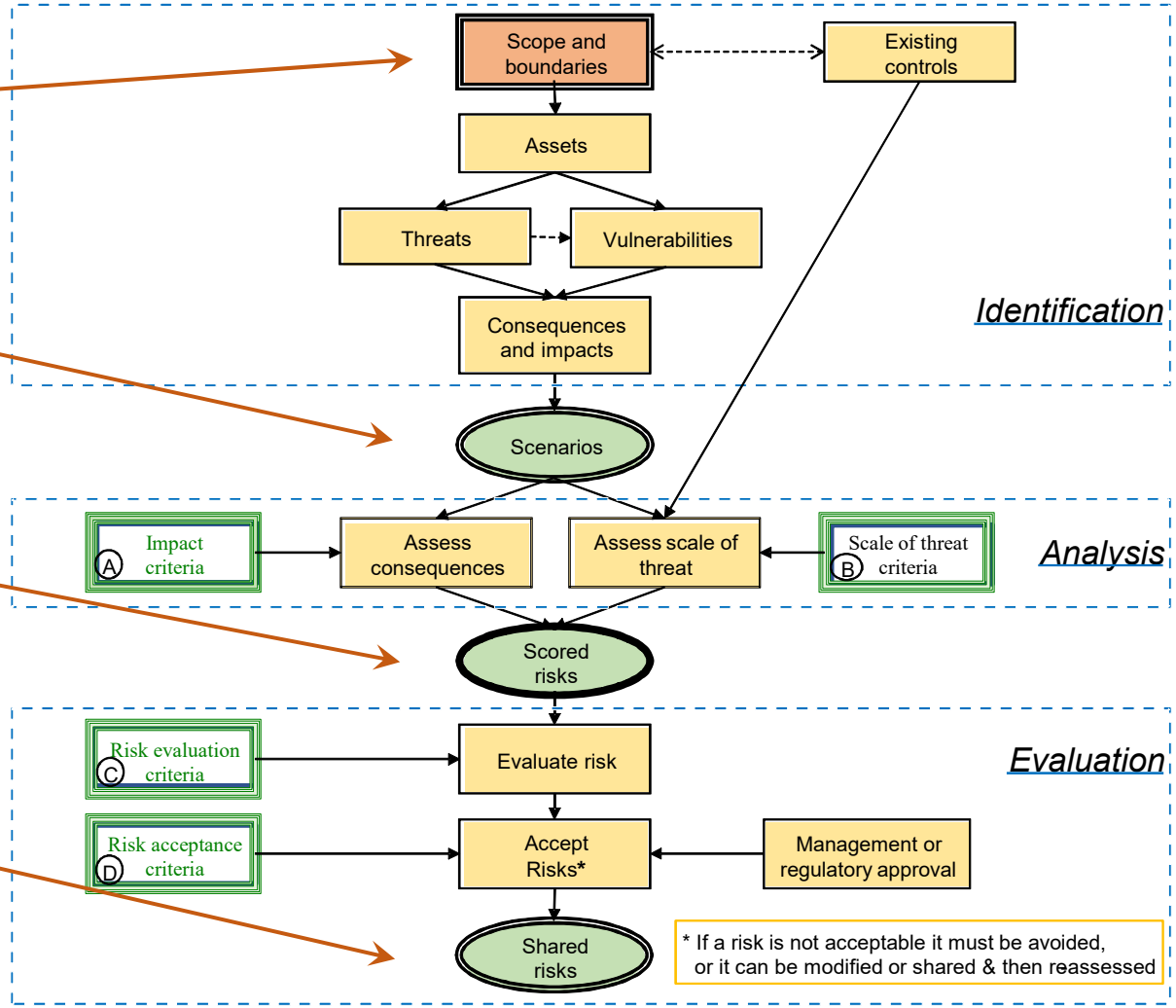
Scale of Threat Criteria

Scored Risk

Risk Evaluation Criteria

Risk Acceptance Criteria

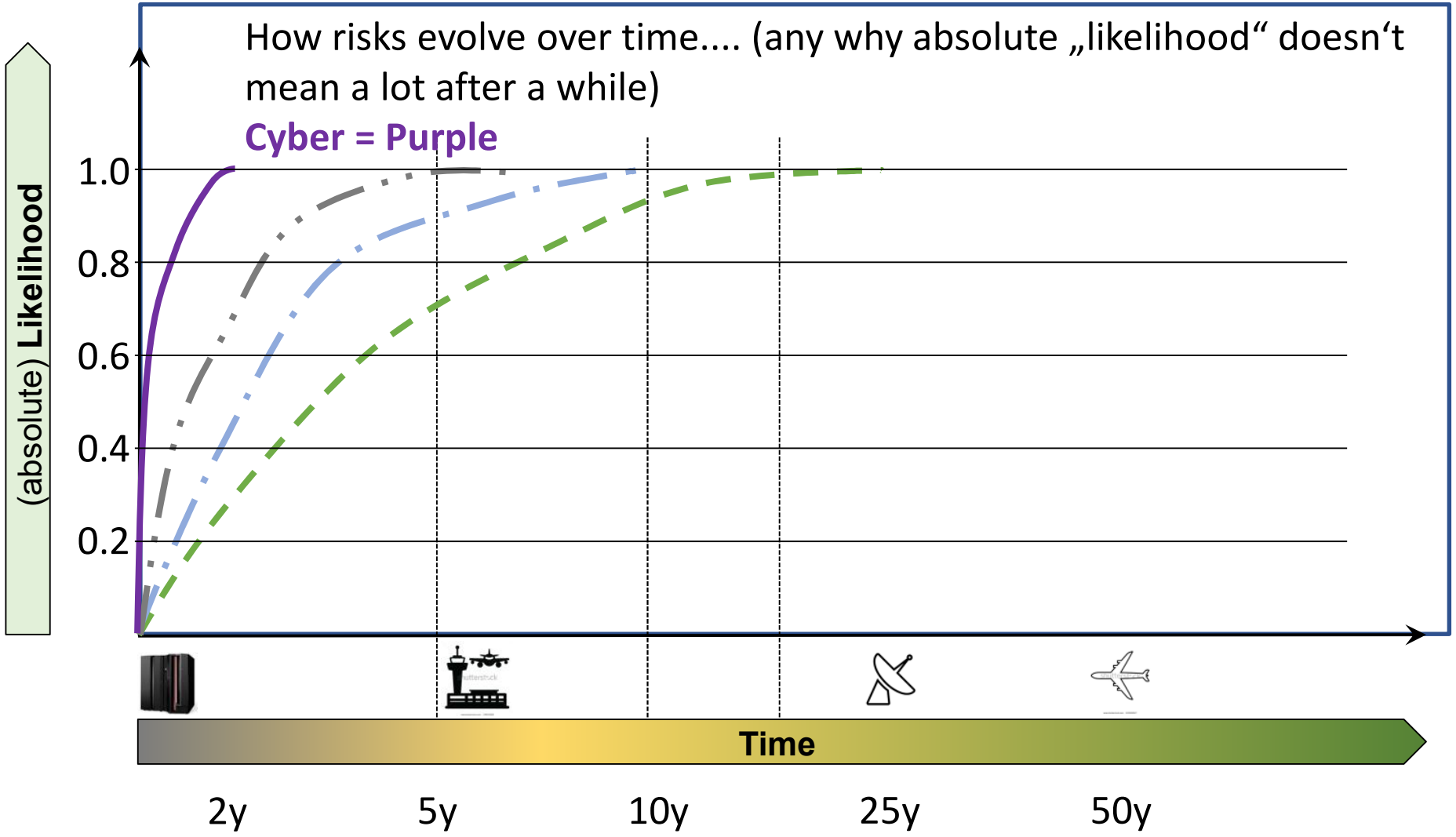
Shared Risks



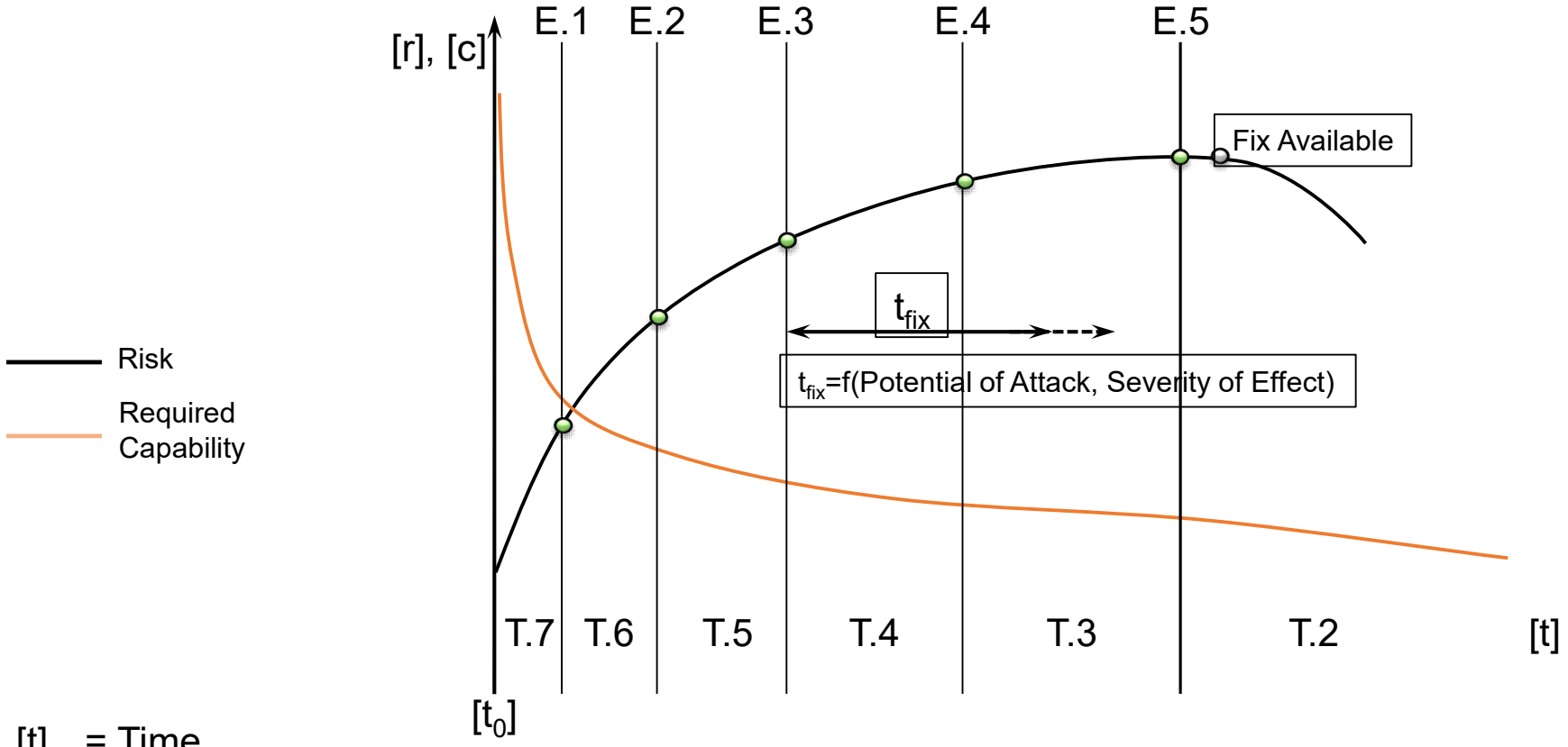
How Risk Assessment Methods Proliferate...

And Risk Management?

Risk Evolution over Time



Threat evolution



- Diagram shows evolution of level of risk with level of threat
- Diagram is IT centric
- Likelihood tends to evolve like the risk

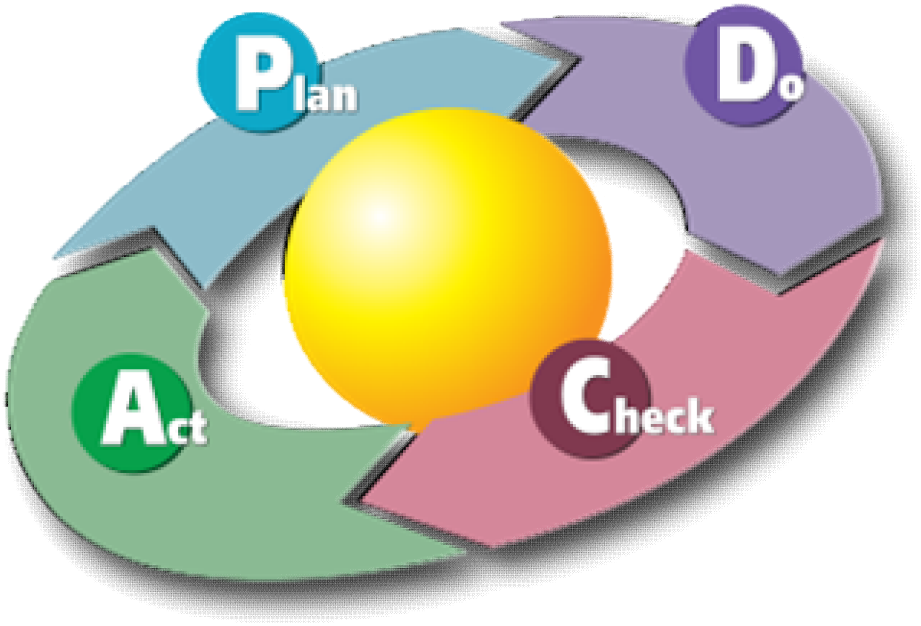
[t] = Time
[r] = Risk ; [c] = Relative Capability of an adversary
E.n = Event, where a transition between T.n and T.n-1 takes place
T.n = Example for adversary characteristic (source: IATF Release 3.1, 2002)

E.1= disclosure of detailed design
E.2= private discovery of vulnerability
E.3= Vulnerability public
E.4= Exploit Elements avail
E.5= Exploits avail

Information Security Management System

→ ISO 27001

Plan	Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.
Do	Implement and operate the ISMS policy, controls, processes and procedures.
Check	Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.
Act	Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

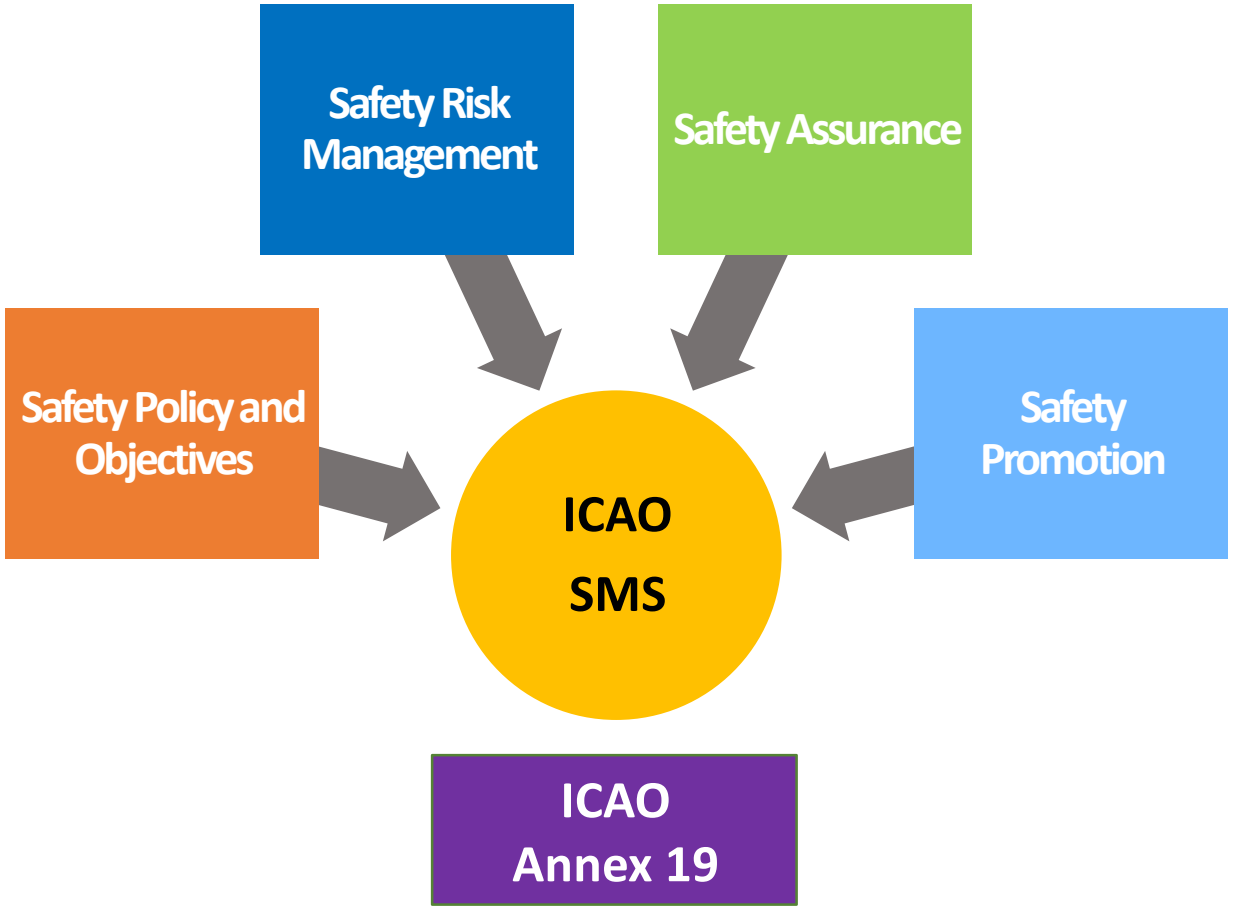


https://en.wikipedia.org/wiki/File:PDCA_Cycle.svg

Safety Management System (Annex 19)

ICAO Safety Management Manual

1. Safety policy and objectives
1.1 Management commitment and responsibility
1.2 Safety accountabilities
1.3 Appointment of key safety personnel
1.4 Coordination of emergency response planning
1.5 SMS documentation
2. Safety risk management
2.1 Hazard identification
2.2 Safety risk assessment and mitigation
3. Safety assurance
3.1 Safety performance monitoring and measurement
3.2 The management of change
3.3 Continuous improvement of SMS
4. Safety promotion
4.1 Training and education
4.2 Safety communication



Security Management System (ICAO Annex 17)

Key components of a SeMS

A SeMS should include the following key components applicable to all types and sizes of aviation Entity:

1. Management commitment
2. Threat and risk management
3. Accountability and responsibilities
4. Resources
5. Performance monitoring, assessment and reporting
6. Incident response
7. Management of change
8. Continuous improvement
9. Training and education
10. Communication

Framework for an Aviation Security Management System (SeMS), UK CAA

Peace of Mind

What is covered by Part-IS?

What are the Key Ingredients for Part-IS?

Basic Regulation

- Acceptable Safety Risks
- Record-keeping
- Personnel Requirements

ISO 2700x

- Information Security Management System (ISMS)
- Information Security Risk Assessment
- Continuous Improvement

NIST Cyber Security Framework

- Information Security Risk Treatment
- Information Security Incidents — Detection, Response, and Recovery

Reporting Regulation

- Information Security External Reporting Scheme

The ISMS in Part-IS

IS.OR.200
Policy on information security

IS.OR.205
IS Risk Assessment

IS.OR.210
Information Security Risk Treatment

IS.OR.220
Detection, Response, Recovery of Incidents

IS.OR.215
IS Internal Reporting Scheme

IS.OR.230
IS external reporting scheme

Implement authority measures as immediate reaction to Incidents or Vulnerabilities

IS.OR.225
Response to findings by the authority

IS.OR.235
Contracting of IS management activities

IS.OR.240
Personnel requirements

IS.OR.245
Record-keeping

IS.OR.200
Compliance monitoring

IS.OR.250 Information security management manual (ISMM)

IS.OR.255 Changes to the information security management system

IS.OR.260 Continuous improvement

Colour code: NIST Framework | Basic Reg. | Reporting Reg. | ISO 2700x

Overview of requirements: Organisation vs Authority

ORGANISATION	Description	AUTHORITY
IS.I.OR.100	Scope	IS.AR.100
IS.I.OR.200	Information security management system (ISMS)	IS.AR.200
IS.I.OR.205	Information security risk assessment	IS.AR.205
IS.I.OR.210	Information security risk treatment	IS.AR.210
IS.I.OR.215	Information security internal reporting scheme	
IS.I.OR.220	Information security incidents — detection, response, and recovery	IS.AR.215
IS.I.OR.225	Response to findings notified by the competent authority	
IS.I.OR.230	Information security external reporting scheme	✓
IS.I.OR.235	Contracting of information security management activities	IS.AR.220
IS.I.OR.240	Personnel requirements	IS.AR.225
IS.I.OR.245	Record-keeping	IS.AR.230
IS.I.OR.250	Information security management manual (ISMM)	
IS.I.OR.255	Changes to the information security management system	
IS.I.OR.260	Continuous improvement	IS.AR.235

The ultimate lesson

If You Want to Go Fast, Go Alone

If You Want to Go Far, Go Together

EASA
European Union Aviation Safety Agency

Thank you!

...for your attention

Join our Community:
https://www.easa.europa.eu/community/cybersecurity

easa.europa.eu/connect

Your safety is our mission.

An Agency of the European Union