Cybersecurity in Aviation

An Introduction

Jean-Paul Moreaux
Principal, Cybersecurity in Aviation

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

https://doi.org/10.5281/zenodo.8396741
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)!
Example: Internet Infrastructure/Traffic Diversion
Example: Well Known Vulnerabilities - „Heartbleed“

Flaw in **OpenSSL Library**
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

FORTUITY

SECURITY

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

Causes
- Particular Risks
- (System) Failures
- (Human) Factors
- Intentional Interaction
- Security

Effects on safety
- Catastrophic
- Hazardous
- Major
- Minor

Remit of CAAs
- Accident
- Incident
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 its 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.
“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: **Safety & Security** in all aspects of aviation!
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

<table>
<thead>
<tr>
<th>Loss</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fragile</td>
<td>Resilient</td>
</tr>
<tr>
<td>Robust</td>
<td></td>
</tr>
</tbody>
</table>
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
We have a dream...

By 2035

European Aviation System on its way to Security

Anti-Fragile

Resilient
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

...what must never happen

...deviation from standards or best practices

...expected loss ($$$)

...past experience projected into the future
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!
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
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
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

**Identification**
- Scope and boundaries
- Existing controls
- Assets
- Threats
- Vulnerabilities
- Consequences and impacts
- Scenarios

**Analysis**
- Assess consequences
- Assess scale of threat
- Scored risks
- Impact criteria
- Threats
- Scale of threat criteria
- Scored risk

**Evaluation**
- Evaluate risk
- Accept Risks*
- Shared risks
- Risk evaluation criteria
- Risk acceptance criteria
- Management or regulatory approval

*If a risk is not acceptable it must be avoided, or it can be modified or shared & then reassessed.
How Risk Assessment Methods Proliferate...

**Situation:**
There are 14 competing standards.

Assessment Methods

**Soon:**
There are 15 competing standards.

Assessment Methods

**How Standards Proliferate:**
(see: A/C chargers, character encodings, instant messaging, etc.)

14?! RIDICULOUS!
We need to develop one universal standard that covers everyone’s use cases.

YEAH!
And Risk Management?
Risk Evolution over Time

How risks evolve over time.... (any why absolute „likelihood“ doesn’t mean a lot after a while)

Cyber = Purple
Threat evolution

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

\[ E.n = \text{Event, where a transition between T.n and T.n-1 takes place} \]
\[ T.n = \text{Example for adversary characteristic (source: IATF Release 3.1, 2002)} \]
**Information Security Management System**

→ ISO 27001

<table>
<thead>
<tr>
<th>Plan</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do</td>
<td>Implement and operate the ISMS policy, controls, processes and procedures.</td>
</tr>
<tr>
<td>Check</td>
<td>Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.</td>
</tr>
<tr>
<td>Act</td>
<td>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.</td>
</tr>
</tbody>
</table>

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
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
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

<table>
<thead>
<tr>
<th>ORGANISATION</th>
<th>Description</th>
<th>AUTHORITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>IS.I.OR.100</td>
<td>Scope</td>
<td>IS.AR.100</td>
</tr>
<tr>
<td>IS.I.OR.200</td>
<td>Information security management system (ISMS)</td>
<td>IS.AR.200</td>
</tr>
<tr>
<td>IS.I.OR.205</td>
<td>Information security risk assessment</td>
<td>IS.AR.205</td>
</tr>
<tr>
<td>IS.I.OR.210</td>
<td>Information security risk treatment</td>
<td>IS.AR.210</td>
</tr>
<tr>
<td>IS.I.OR.215</td>
<td>Information security internal reporting scheme</td>
<td>IS.AR.215</td>
</tr>
<tr>
<td>IS.I.OR.220</td>
<td>Information security incidents — detection, response, and recovery</td>
<td>IS.AR.215</td>
</tr>
<tr>
<td>IS.I.OR.225</td>
<td>Response to findings notified by the competent authority</td>
<td>IS.AR.220</td>
</tr>
<tr>
<td>IS.I.OR.230</td>
<td>Information security external reporting scheme</td>
<td>✓</td>
</tr>
<tr>
<td>IS.I.OR.235</td>
<td>Contracting of information security management activities</td>
<td>IS.AR.220</td>
</tr>
<tr>
<td>IS.I.OR.240</td>
<td>Personnel requirements</td>
<td>IS.AR.225</td>
</tr>
<tr>
<td>IS.I.OR.245</td>
<td>Record-keeping</td>
<td>IS.AR.230</td>
</tr>
<tr>
<td>IS.I.OR.250</td>
<td>Information security management manual (ISMM)</td>
<td>IS.AR.235</td>
</tr>
<tr>
<td>IS.I.OR.255</td>
<td>Changes to the information security management system</td>
<td>IS.AR.235</td>
</tr>
<tr>
<td>IS.I.OR.260</td>
<td>Continuous improvement</td>
<td>IS.AR.235</td>
</tr>
</tbody>
</table>
The ultimate lesson
If You Want to Go Fast, Go Alone
If You Want to Go Far, Go Together
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