EASA
European Union Aviation Safety Agency

Cybersecurity in Aviation and ATM insights

Davide Martini,
Senior Expert - Cybersecurity in Aviation

3 December 2024

Your safety is our mission.

An Agency of the European Union

Objectives of Day 1

Gain an understanding of:

- → Information security concepts applied to aviation (framing the problem)
- → Aviation as a system of systems
- → Building blocks for a resilient air-transport system
- → Elements of safety/security risk management in aviation
- → Regulatory framework – our experience in EU

General Concepts

Security Objectives and Attributes

Principles of Information Security

Information Security

The protection of information and information systems

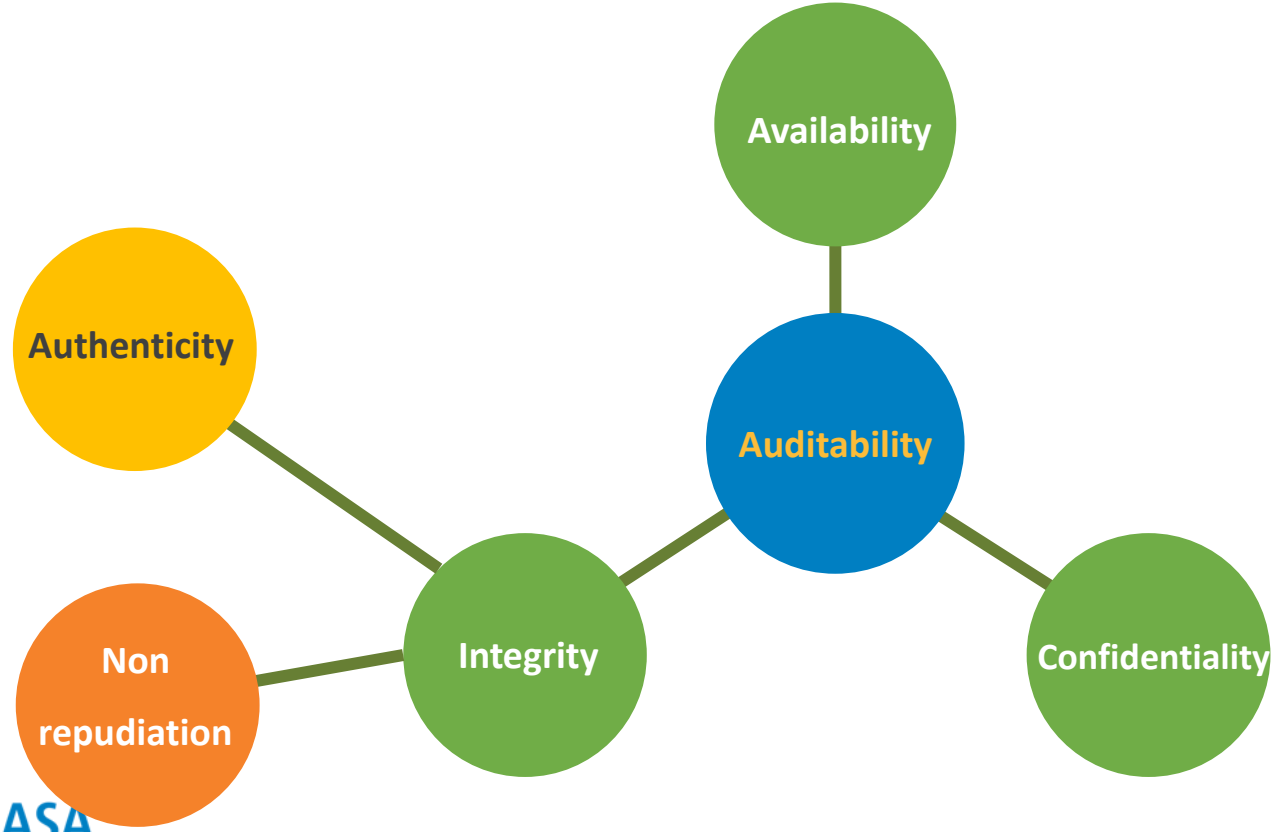
from unauthorized access, disclosure, disruption, modification, destruction.

Principles of Information Security

EASA

Principles of Information Security

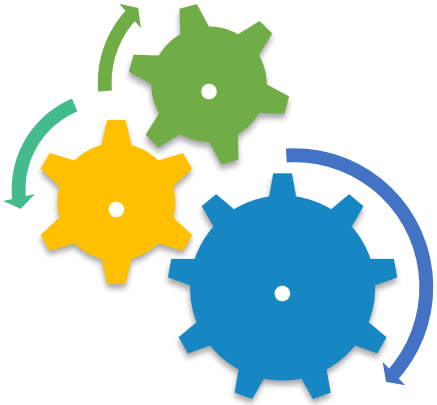
Additional pillars of Information Security



Security Concepts Summary

Threat Agent → Give rises to → **Threat** → Exploits a → **Vulnerability**

Directly affects



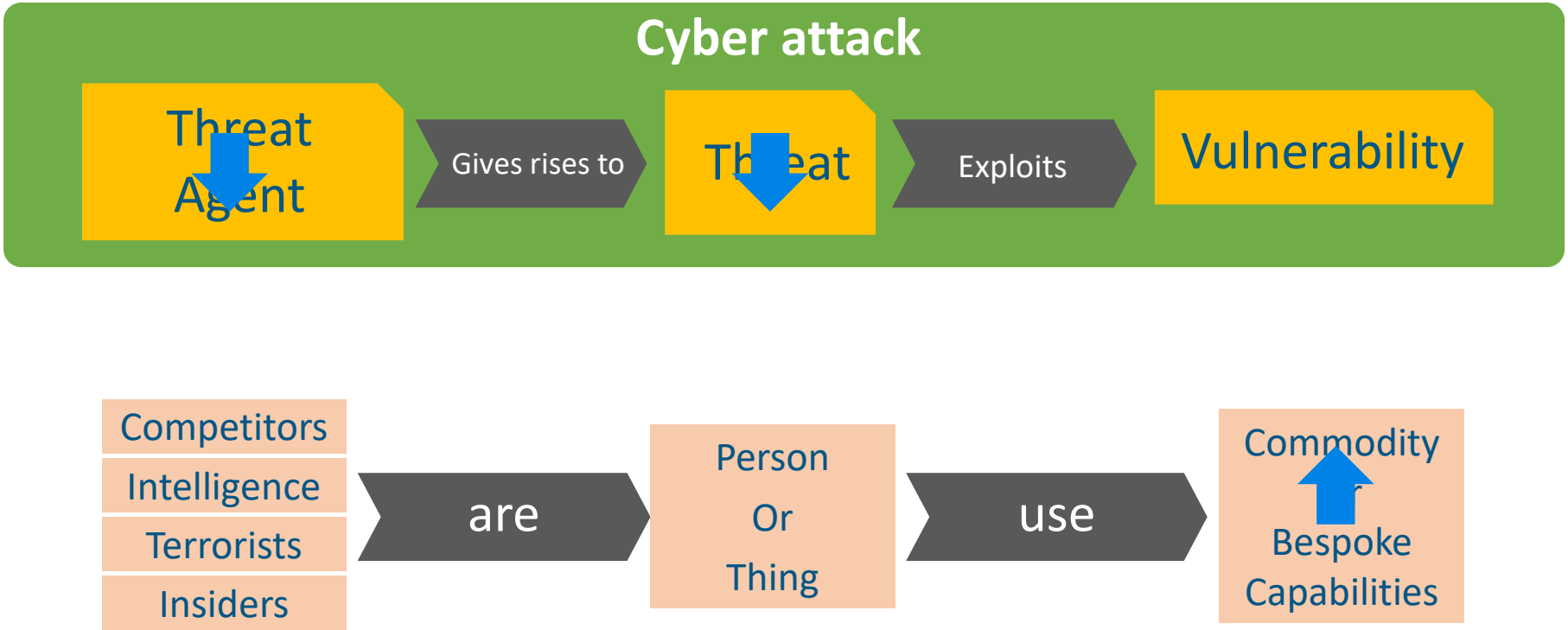
Leads to a

Risk

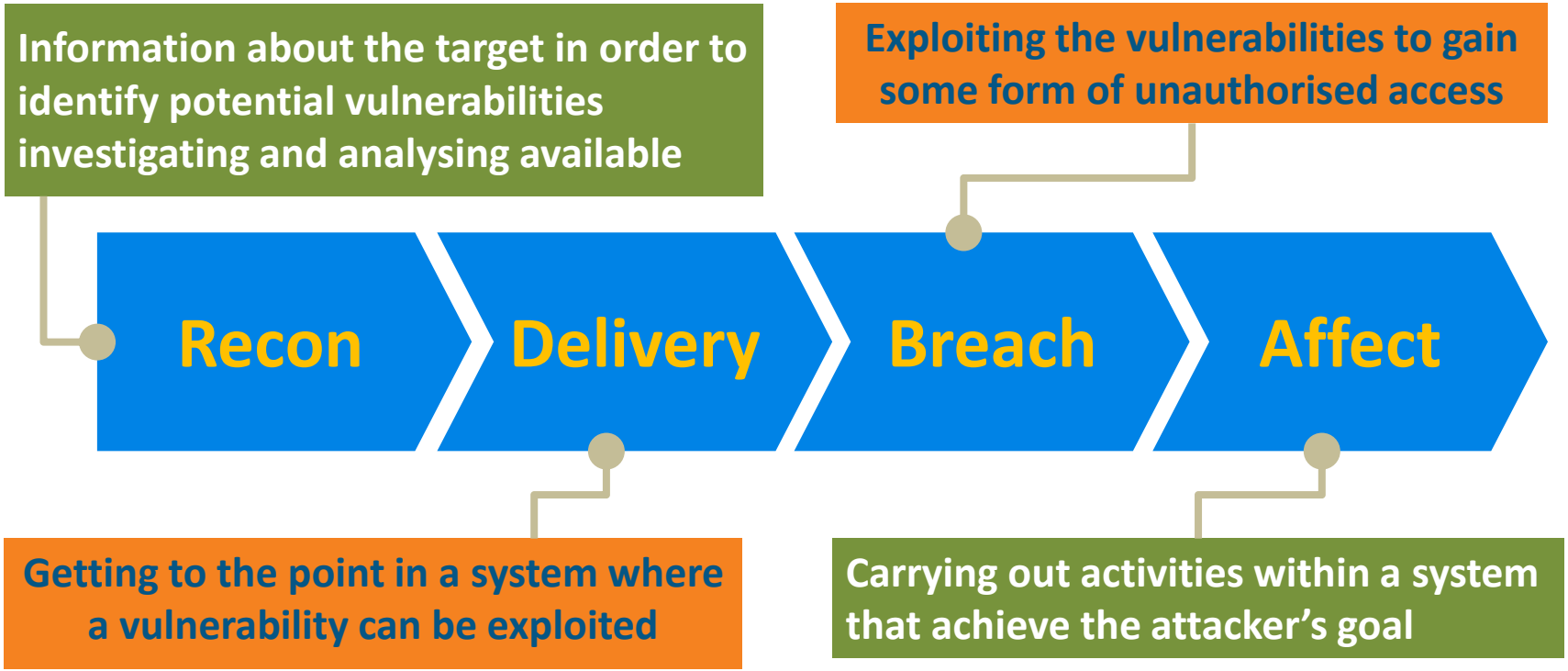
Can damage

Countermeasure → Can be safeguarded → Impact → Causing an → Assets

Cyber attack is targeted or untargeted



Cyber attacks stages



Cybersecuity – the Aviation Perspective

Security for Safety

EASA

A key to reading Security and Safety approaches

Security — System-of-Systems — *Safety*

Causes

Reduce the Likelihood of Occurrences in Aviation caused by Intentional Acts by Threat Actors

Effects

Reduce the Severity and Probability of Safety Effects on Aviation Systems

The boundary is blurring

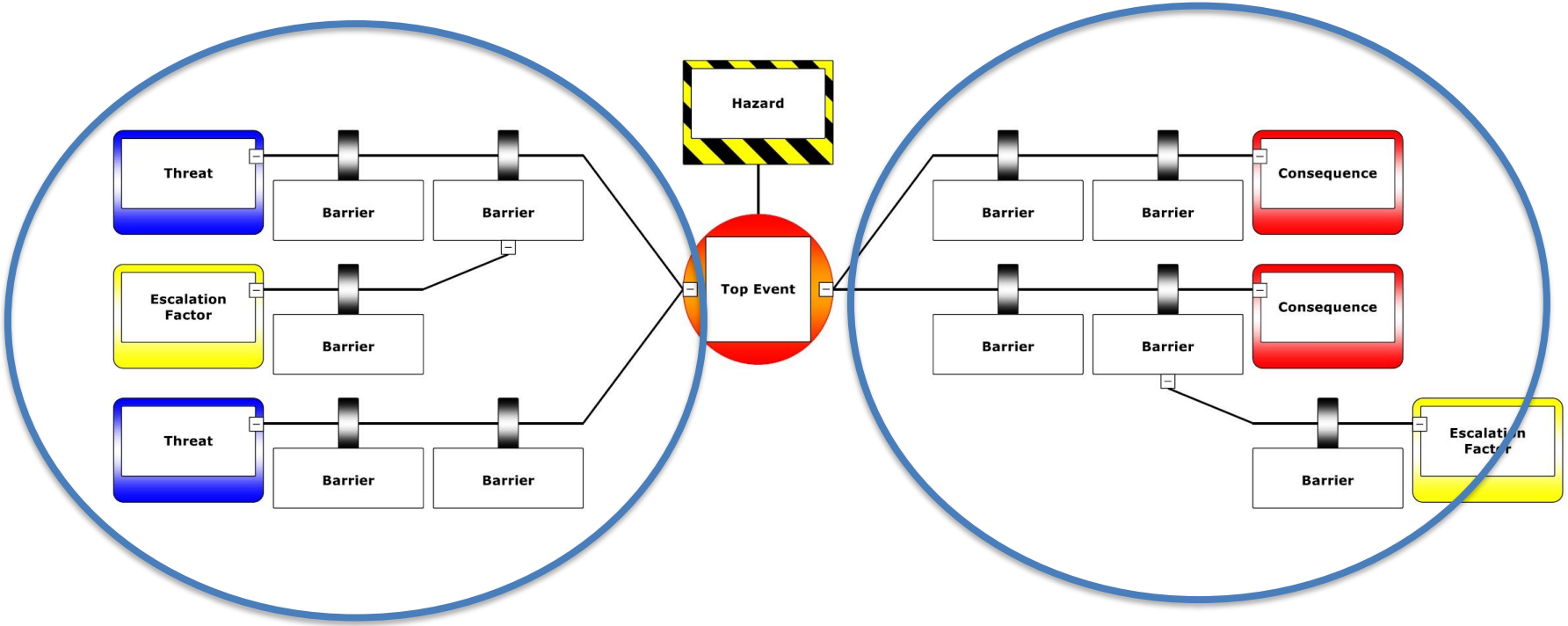
“Today’s security threats, including cybersecurity, blur the traditional divide between the two approaches.”

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

The reduction of the causes alone is not the best option

We need to bridge aviation security and aviation safety



AVIATION SECURITY MEASURES

AVIATION SAFETY MEASURES

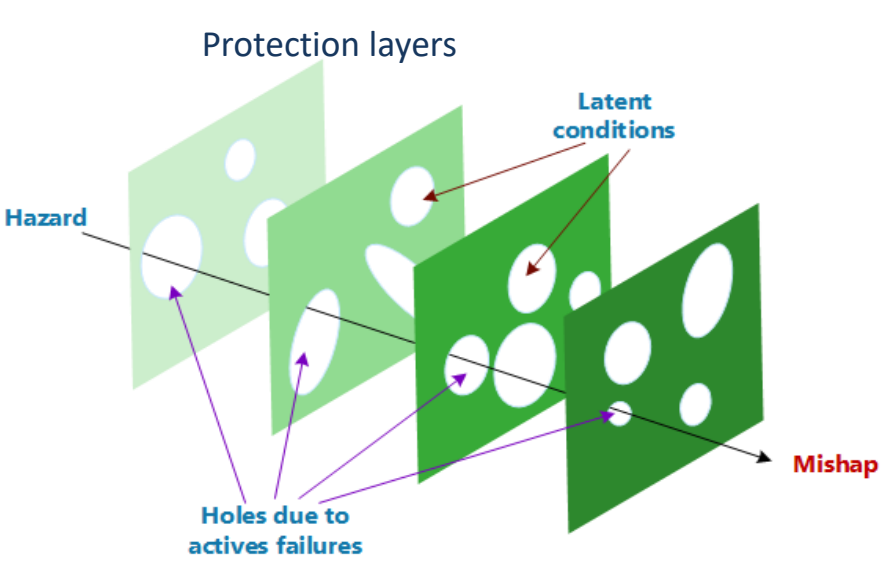
Initial considerations on the cybersecurity scope

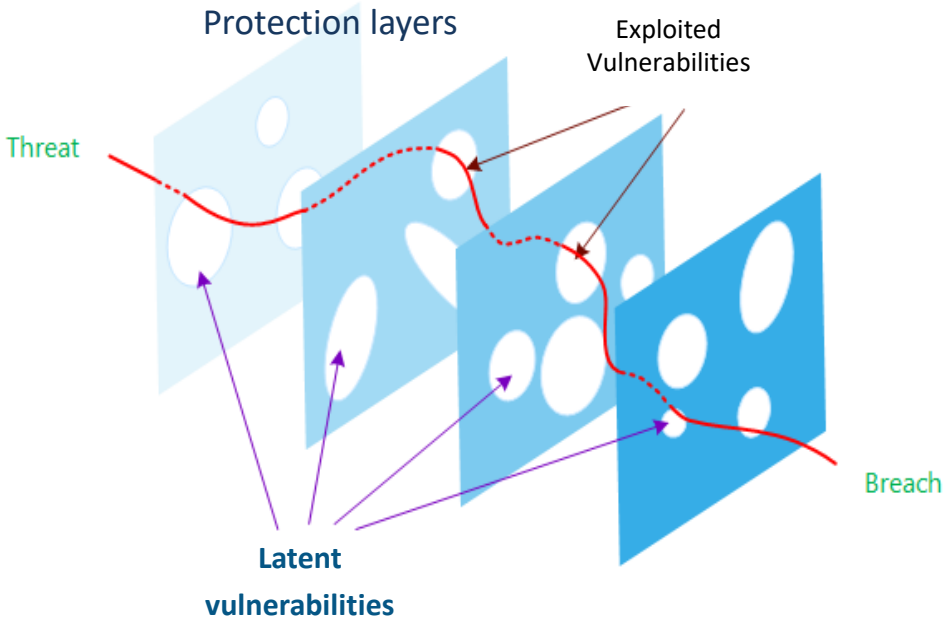
- Main focus is on **aviation safety**, regardless of whether this comes from a direct effect on the aircraft or as an indirect effect due to malfunctioning of e.g. air navigation.

- From an organisation's perspective, business implications and non-safety related impacts also have to be considered

There is often overlap.

The cultural bias in aviation





Safety **vs.** **Security**

Framing the cybersecurity problem

Cyberattack targeting an aircraft ≡ Sabotage

It requires attention, however cybersecurity has two other more concerning implications:

Remote execution and **Scalability** (propagation and growth) of an attack

The Aviation community effort should be focused on threat scenario that can jeopardise the aviation functional chains, impairing their functionalities.

Information Security – Adopting ER013 definition

ER-013 - Aeronautical Information System Security Glossary, published by EUROCAE

Information security, sometimes shortened to InfoSec, is the practice of defending information from **unauthorized** access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (electronic, physical, etc.)

Exercise

Reflect on the definition, in particular:

- How do you interpret unauthorised?

- Does the definition entails **accidental circumstances**, e.g. malfunctions or natural disasters?

Exercise - Considerations

Reflect on the definition, in particular:

- How do you interpret unauthorised?

unauthorized ≠ unlawful

- Does the definition entails **accidental circumstances**, e.g. malfunctions or natural disasters?

Scope is the so called “Airworthiness Security”
Focusing on intentional unauthorised interactions

Airworthiness Security – refining the scope

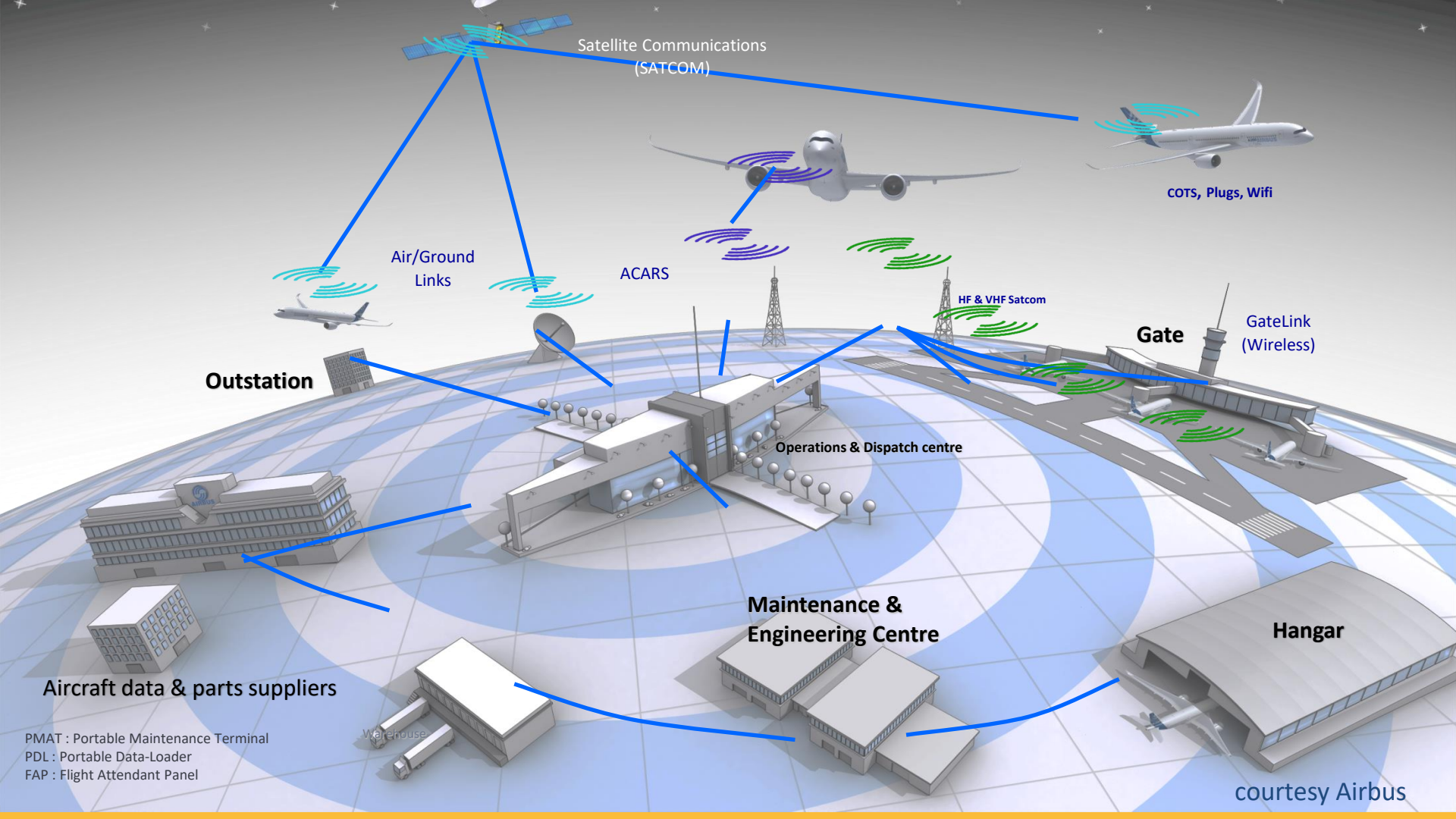
ER-013 - Aeronautical Information System Security Glossary, published by EUROCAE (actually defined in ED-202A)

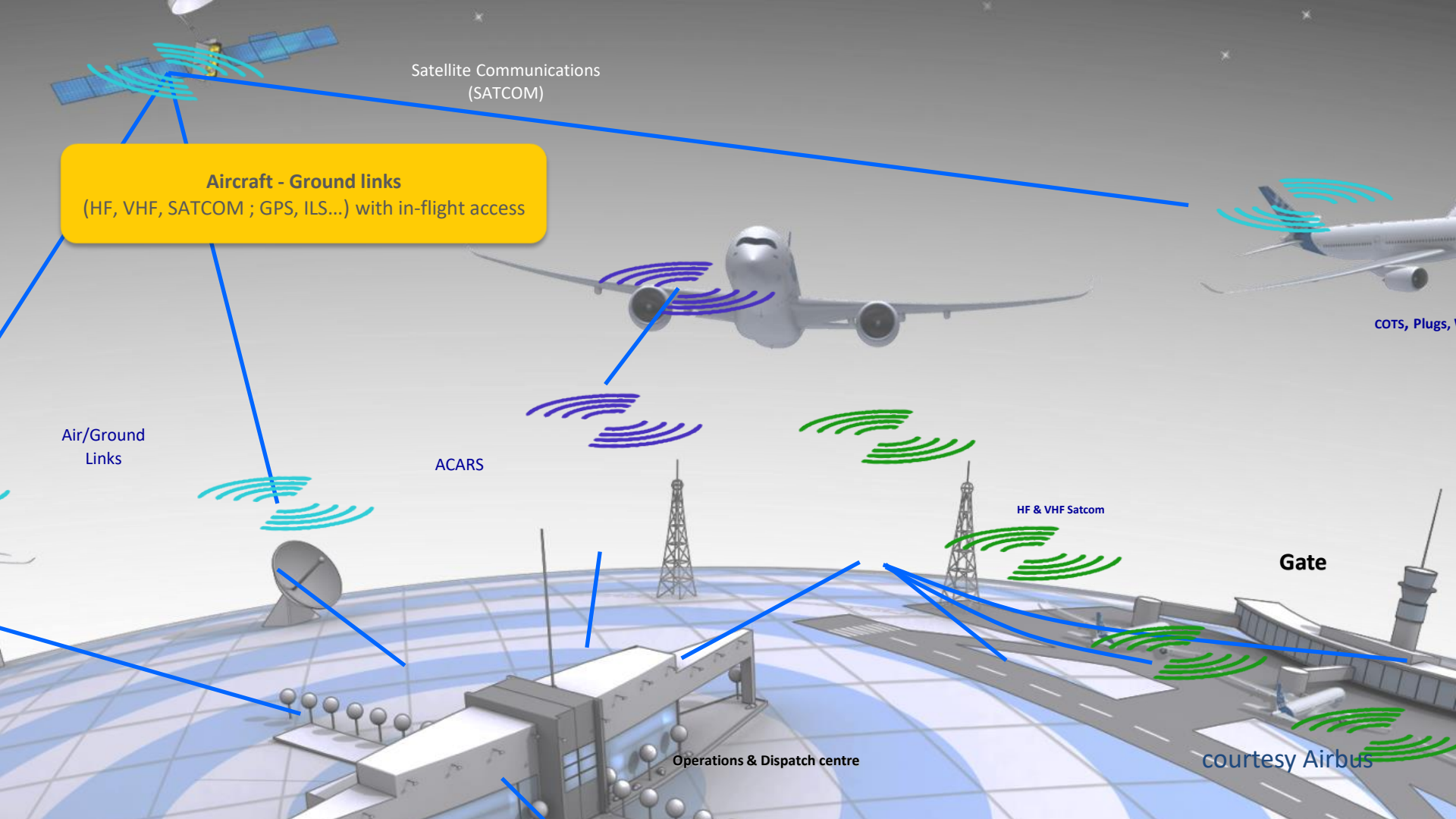
Airworthiness Security is **"**The protection of the airworthiness of an aircraft from **intentional** **unauthorized electronic interaction**: harm due to human action (intentional or unintentional) using access, use, disclosure, disruption, modification, or destruction of data and/or data interfaces. This also includes the consequences of malware and forged data and of access of other systems to aircraft systems."

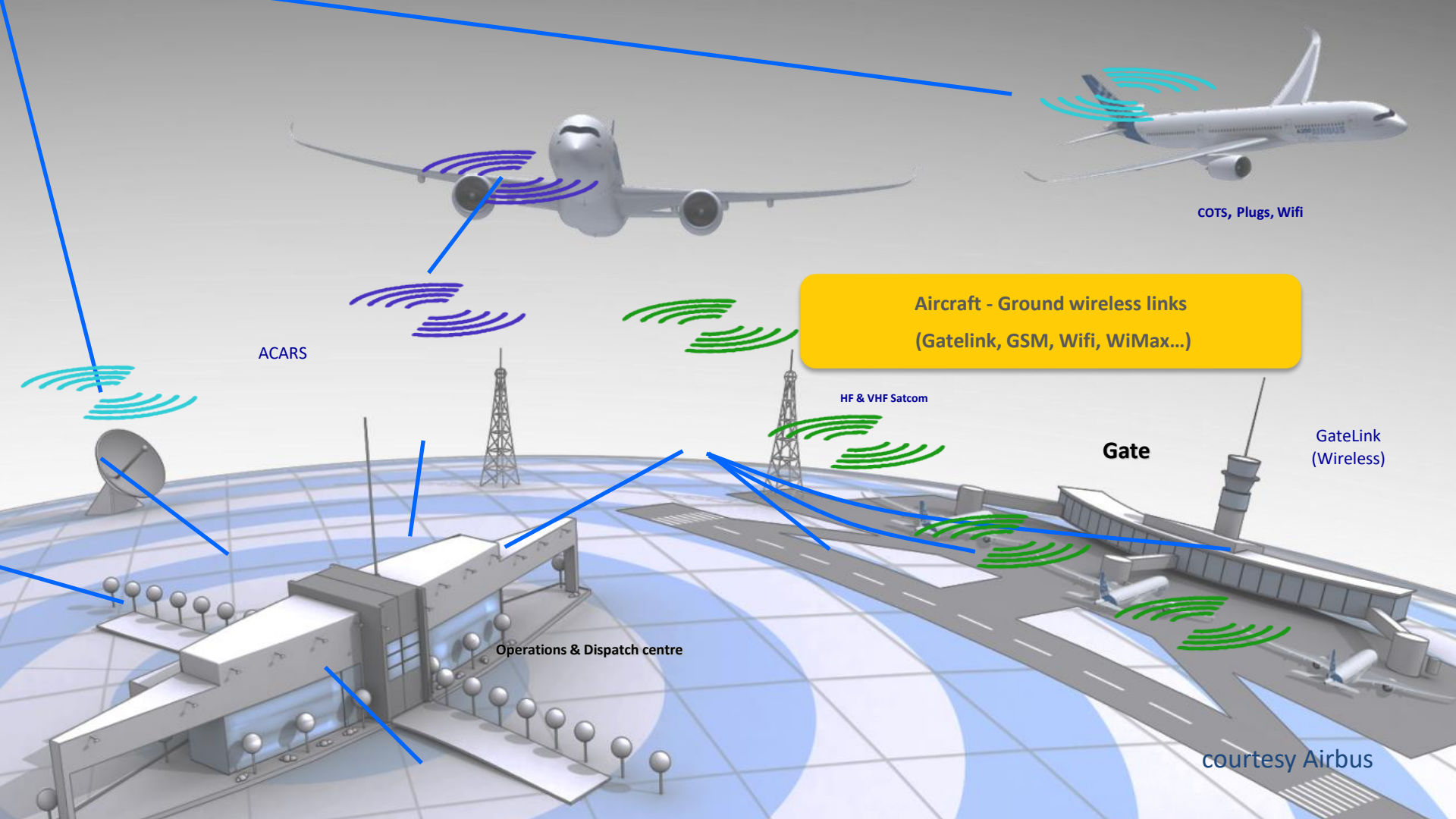
Cybersecuity – the Aviation Perspective

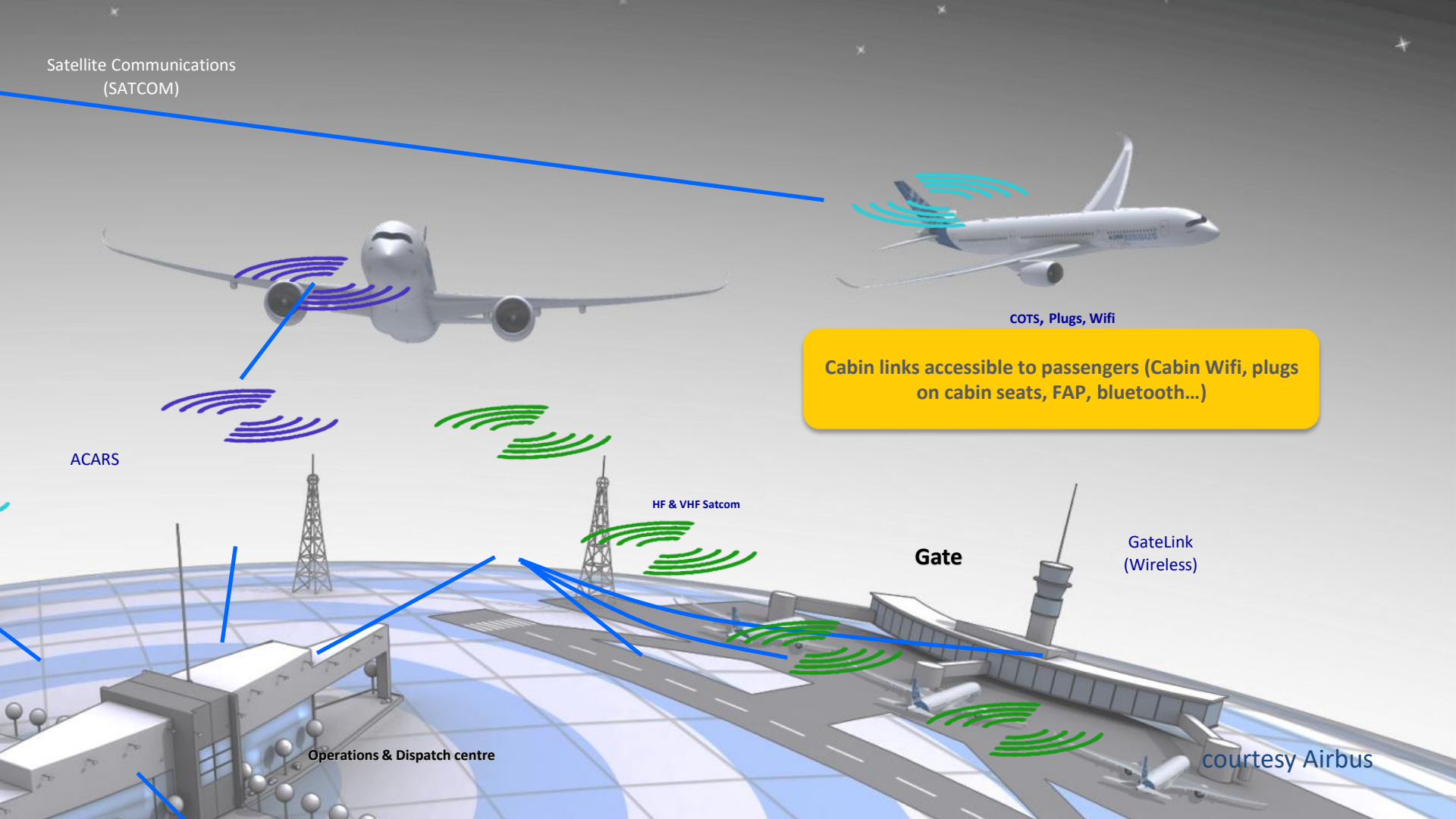
Aviation is a System-of-Systems

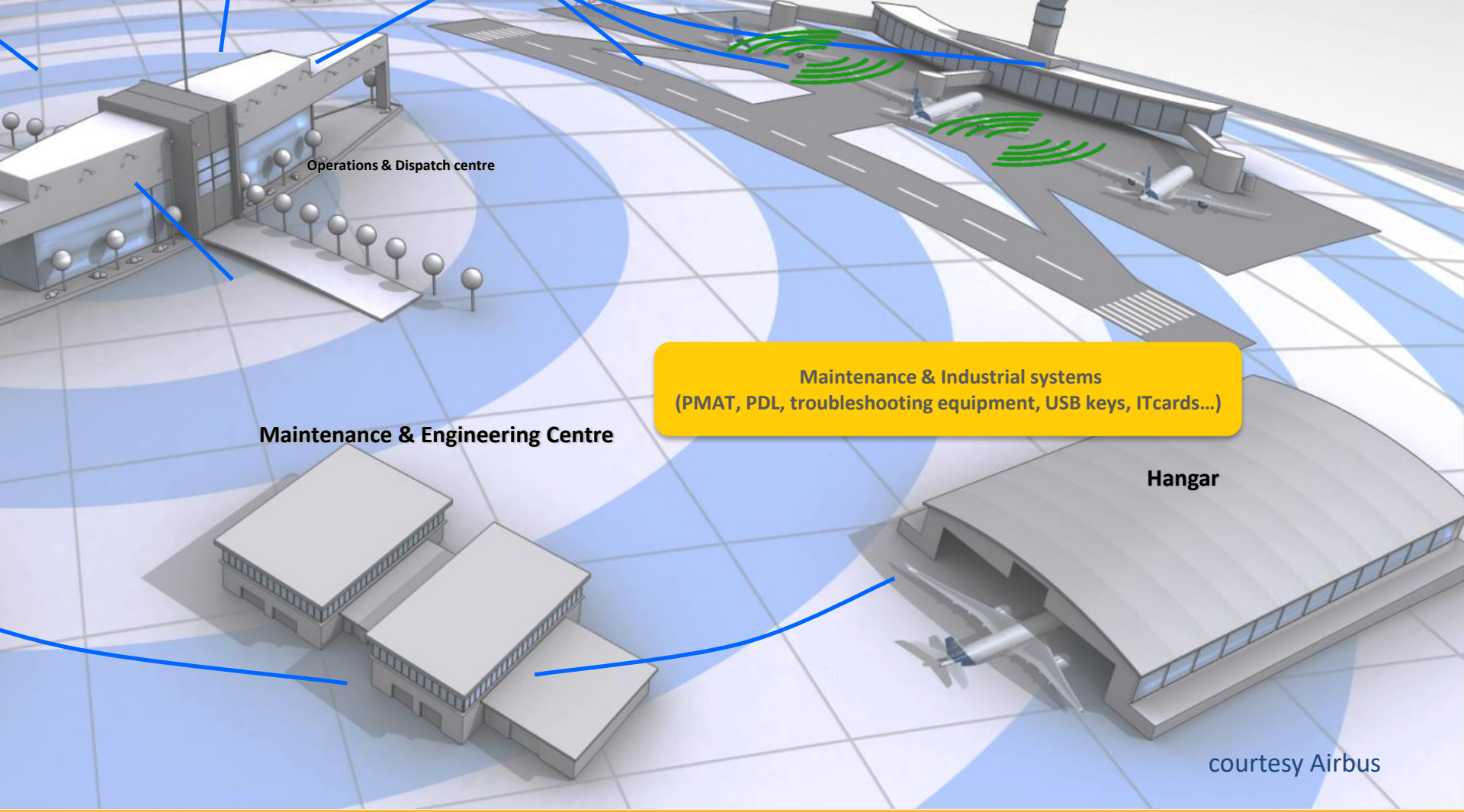
EASA


Satellite Communications
(SATCOM)
COTS, Plugs, Wifi
Air/Ground
Links
ACARS
HF & VHF Satcom
Gate
GateLink
(Wireless)
Outstation
Operations & Dispatch centre
Maintenance &
Engineering Centre
Hangar
Aircraft data & parts suppliers
Warehouse
PMAT : Portable Maintenance Terminal
PDL : Portable Data-Loader
FAP : Flight Attendant Panel
courtesy Airbus

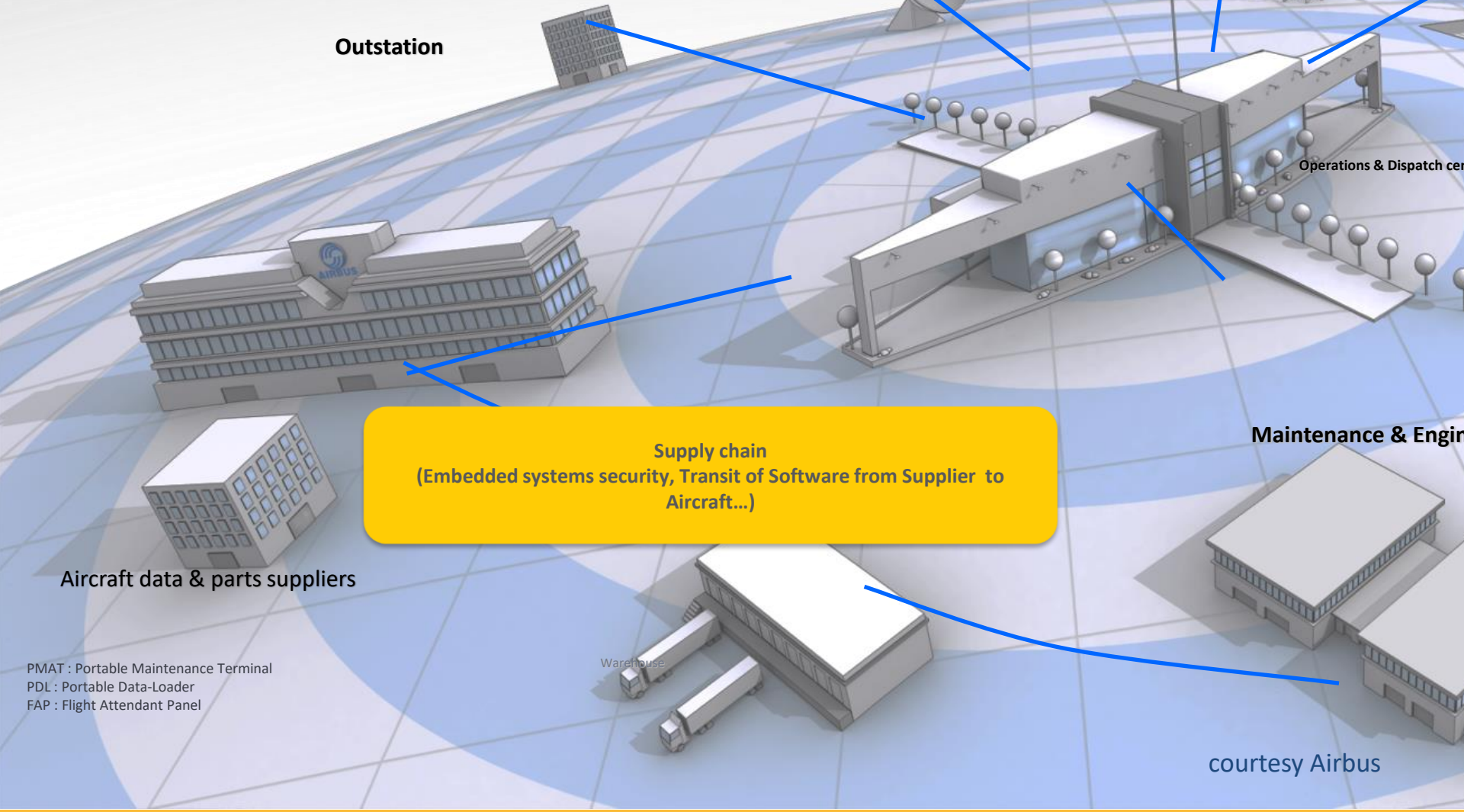

Satellite Communications
(SATCOM)
Aircraft - Ground links
(HF, VHF, SATCOM ; GPS, ILS…) with in-flight access
Air/Ground
Links
ACARS
HF & VHF Satcom
Gate
Operations & Dispatch centre
courtesy Airbus

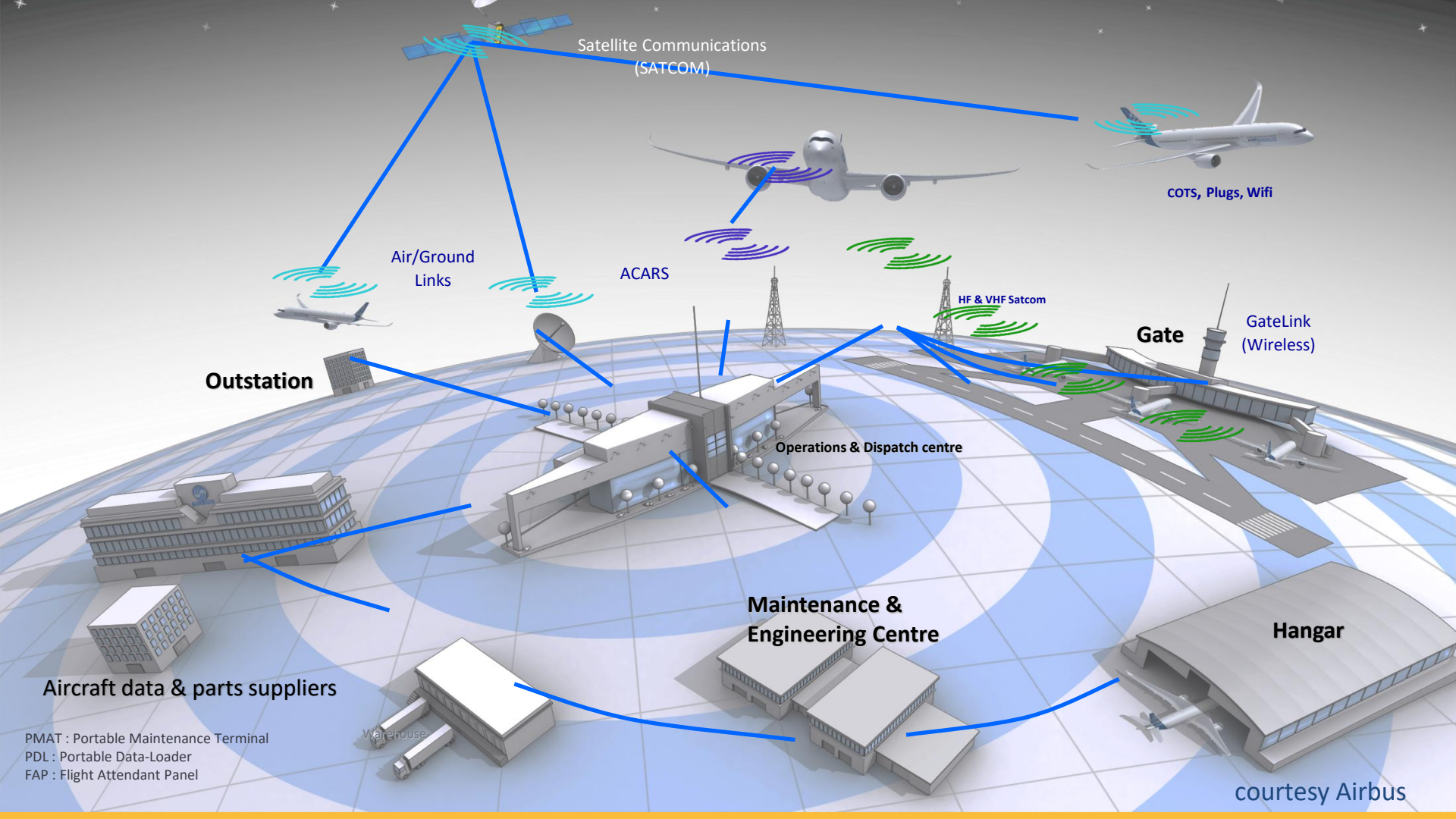

COTS, Plugs, Wifi
Aircraft - Ground wireless links
(Gatelink, GSM, Wifi, WiMax…)
ACARS
HF & VHF Satcom
Gate
GateLink
(Wireless)
Operations & Dispatch centre
courtesy Airbus


Satellite Communications
(SATCOM)
COTS, Plugs, Wifi
Cabin links accessible to passengers (Cabin Wifi, plugs on cabin seats, FAP, bluetooth…)
ACARS
HF & VHF Satcom
Gate
GateLink
(Wireless)
Operations & Dispatch centre
courtesy Airbus



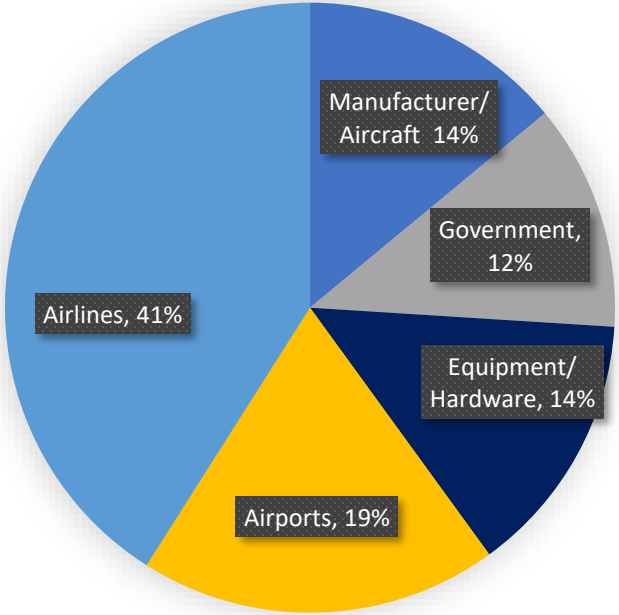
courtesy Airbus


Outstation
Operations & Dispatch cer
Maintenance & Engir
Supply chain
(Embedded systems security, Transit of Software from Supplier to Aircraft…)
Aircraft data & parts suppliers
Warehouse
PMAT : Portable Maintenance Terminal
PDL : Portable Data-Loader
FAP : Flight Attendant Panel
courtesy Airbus

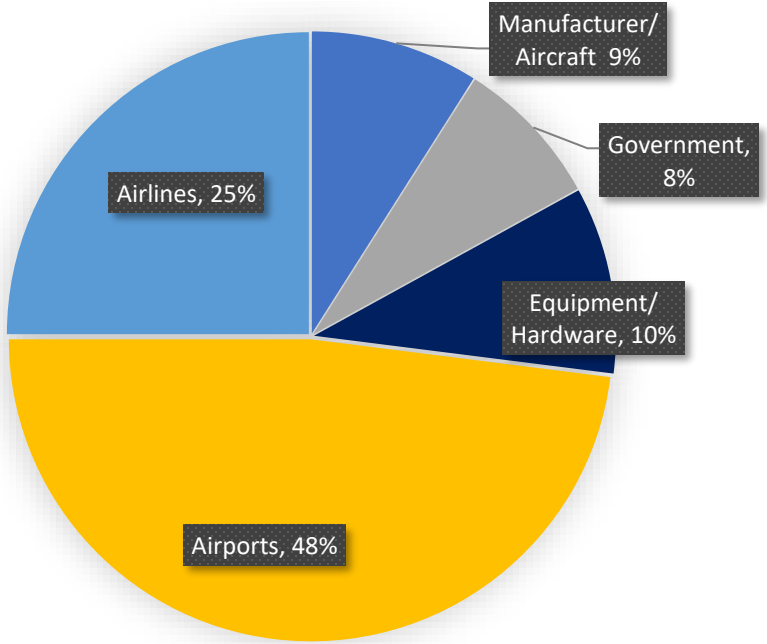

Satellite Communications
(SATCOM)
COTS, Plugs, Wifi
Air/Ground
Links
ACARS
HF & VHF Satcom
Gate
GateLink
(Wireless)
Outstation
Operations & Dispatch centre
Maintenance &
Engineering Centre
Hangar
Aircraft data & parts suppliers
Warehouse
PMAT : Portable Maintenance Terminal
PDL : Portable Data-Loader
FAP : Flight Attendant Panel
courtesy Airbus

Cybersecurity risks matter to you – EU data

116 attacks by target organisation in 2022



175 attacks by target organisation in 2023



Questions?

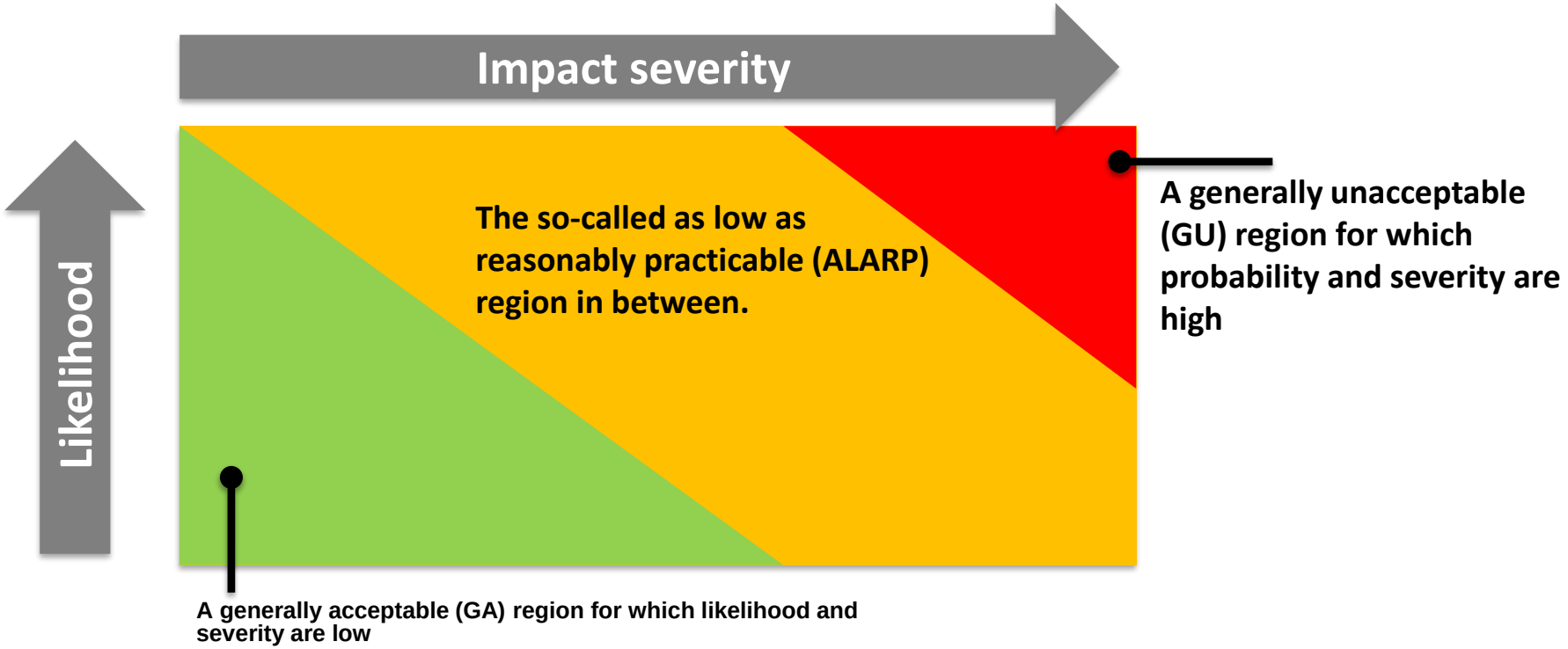
Cybersecuity – the Aviation Perspective

A safety driven Risk Management

What is Risk?


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

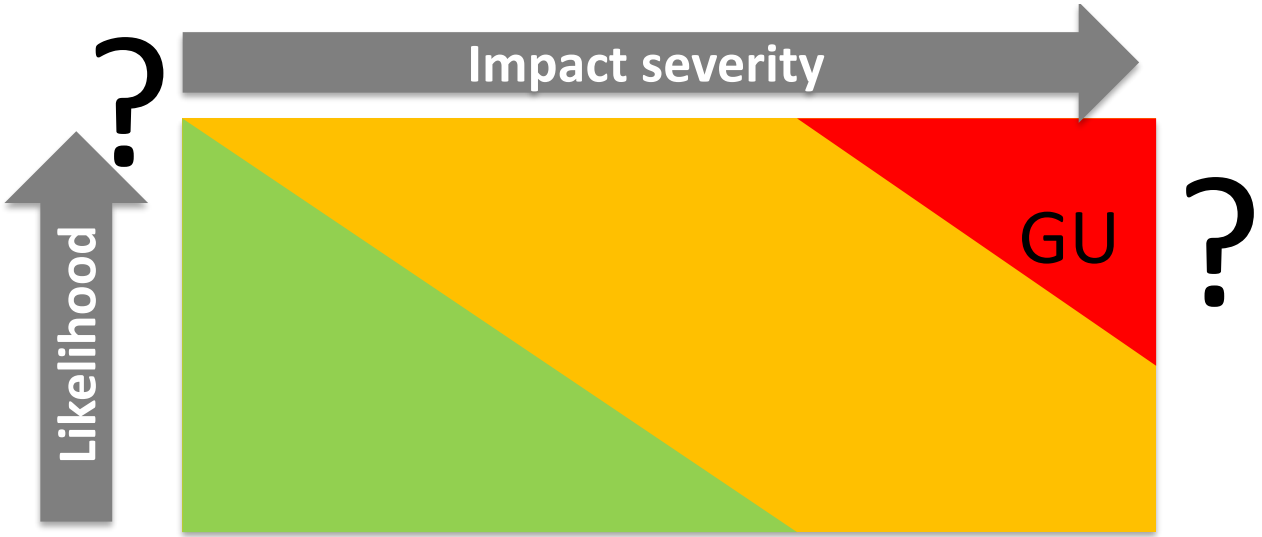
Common risk management tool – Risk Matrix



Establishing the “system of reference”

How do we measure Likelihood and Impact Severity ?

How do we establish the GU zone?



Defining likelihood in a Security Risk Assessment

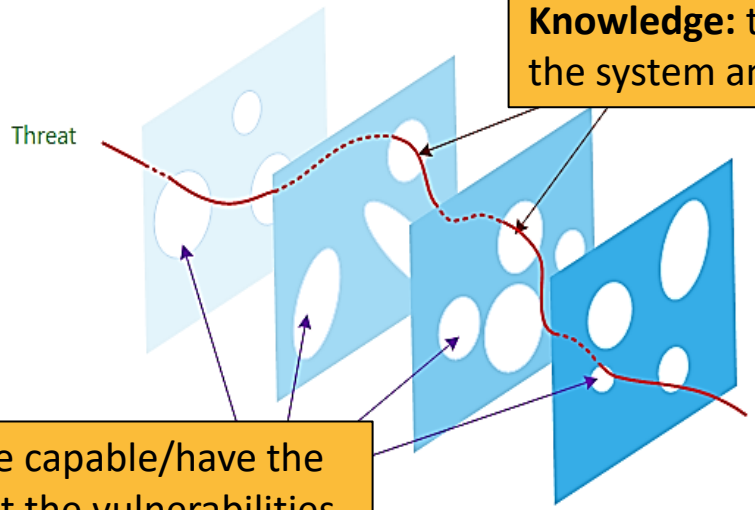
Likelihood is the chance of something happening and is adequate to describe the probability of occurrence of accidental events, e.g. in a safety risk assessment.

A security risks assessment (SRA) instead shall evaluate how likely is the materialisation of deliberate acts.

Likelihood in SRA is to be intended as a “score” and not the strict statistical sense of the term.

A different approach to risk assessment

Risk assessment in cybersecurity is based on capability, knowledge and access



Knowledge: to be informed about the system and its vulnerabilities

Capability: to be capable/have the means to exploit the vulnerabilities and perform “lateral movements”

Access: to have the window of opportunity and the possibility to interact with the systems as needed

Defining likelihood in a Security Risk Assessment

SRA Likelihood = Level of Threat

The higher the level of threat, the higher the likelihood

The magnitude of the scale shall reflect the increase of effort to perform and attack.

The scale is relative and contextual, i.e. not absolute

Interpretation is required for comparisons

Defininig the impact severity in SRA for aviation

The Severity of the Impact can be classified in a number of ways, such as the impact on:

- Air transport system **Safety**
- Air transport system **Capacity**
- Organisation’s performance and mission
- Non-compliancy to regulations (e.g. GDPR)
- Intellectual property rights (IPR)

Defininig the impact severity in SRA for aviation

The conventional impact severity scale of the “safety risk assessment” is adopted.

Similarly, for capacity a conventional impact scale can be used

No Effect	Minor	Major	Hazardous	Catastrophic
No damage or injury	Minor discomfort and/or less than minor system damage	Increased workload, serious incident, injury to persons	Physical distress, serious or fatal injuries to a number of persons, major equipment damage	Multiple fatalities, loss of the system
No capacity loss	Reduction of 10% of airspace capacity	Reduction between 10% to 30% of airspace capacity	Reduction between 30% to 60% of airspace capacity	Reduction between 60% to 100% of airspace capacity

Severity of other impacts – example

Domain / Severity	Operational missions	Economic	Branding / Image	Reg. non-compliancy	Legal (IPR,…)
No effect	No impact	No effect	No impact	No impact	No impact
Minor	Activity trouble	Minor loss of income	Minor complaints	Minor regulatory infraction	Mutual Agreement
Major	Disturbance of one mission	Large loss of income	Complaints and local attention	Multiple minor regulatory infractions	Liability company engaged in the courts
Hazardous	Disturbance of all missions	Serious loss of income	National attention Press campaign	Major regulatory infraction	Individual criminal responsibility of individual
Catastrophic	Total disruption	Bankruptcy or loss of all income	Government & international attention	Multiple major regulatory infractions	Individual criminal responsibility of corporation

Exercise – definition of the GU zone

Consider the below domains and reflect on which entity should be responsible for defining risk acceptability and unacceptability criteria.

- Air transport system **Safety**
- Air transport system **Capacity**
- Non-compliancy to regulations (e.g. GDPR)
- Intellectual property rights (IPR)
- Organisation’s performance and mission

Exercise- definition of the GU zone

Consider the below domains and reflect on how to define the risk acceptability and unacceptability area.

- Air transport system **Safety**
- Air transport system **Capacity**

Aviation Regulation and/or National Regulation

- Non-compliancy to regulations (e.g. GDPR)
- Intellectual property rights (IPR)

National Laws (also stemming from EU reg.)

- Organisation's performance and mission

Organisation's Policies

Example of risk acceptability matrix for aviation products

Risk assessment matrix

security risk

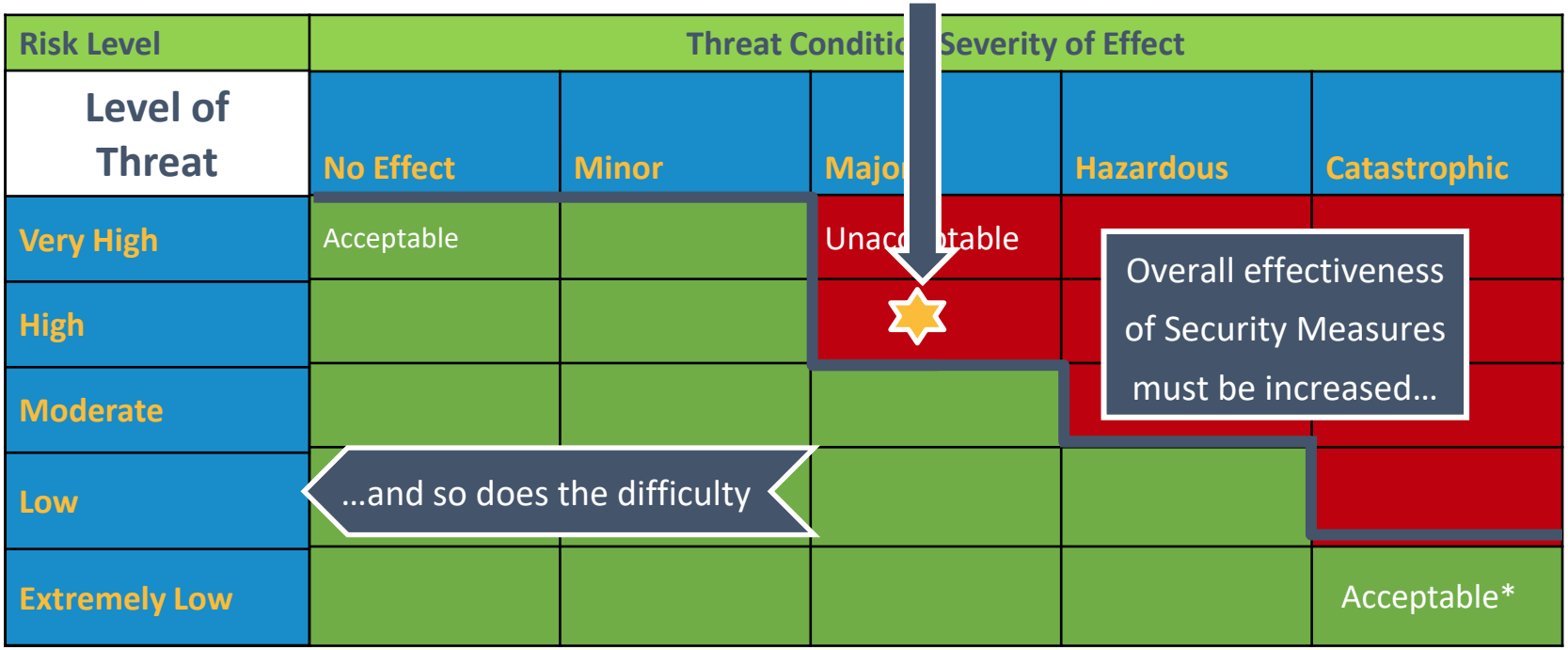
vs

Airworthiness

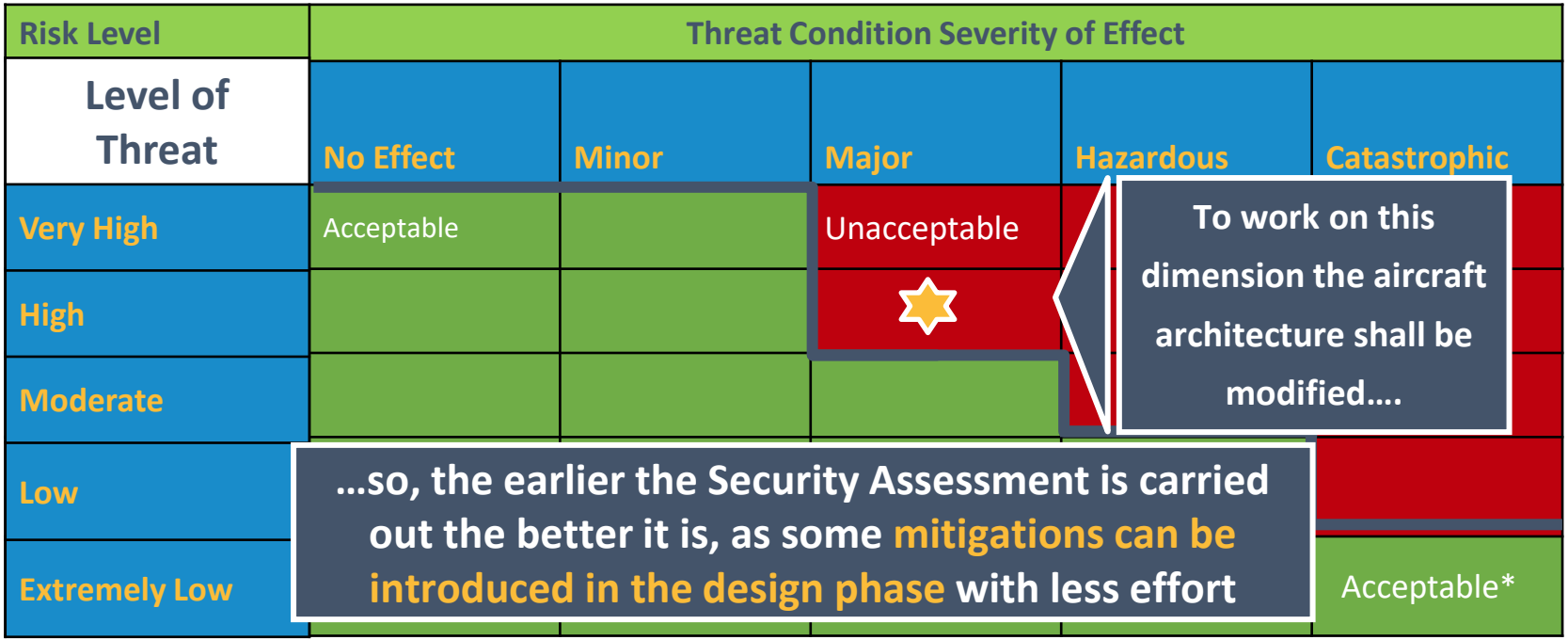
from **EUROCAE ED-203A**

	Severity of the Threat Condition				
Likelihood/ Level of Threat	None	Minor	Major	Hazardous	Catastrophic
Very High	Acceptable	Acceptable	Not acceptable	Not acceptable	Not acceptable
High	Acceptable	Acceptable	Not acceptable	Not acceptable	Not acceptable
Moderate	Acceptable	Acceptable	Acceptable	Not acceptable	Not acceptable
Low	Acceptable	Acceptable	Acceptable	Acceptable	Not acceptable
Extremely Low	Acceptable	Acceptable	Acceptable	Acceptable	Acceptable

Security Risk Acceptability Matrix



Security Risk Acceptability Matrix



Effectiveness of protections

- → Preparation Means
- → Window of opportunity
- → Execution Means

Knowledge / Equipment	None/Public Information and no preparation time	Uncontrolled Information and no significant preparation time	Insider Knowledge or Significant preparation time

Effect	Description
0	The attack can be carried out at any time.
1	The attack can be carried out during regular cruise flight.
2	The attack vector is available while the aircraft is on the ground.
3	Maximum effectiveness for mandatory operational procedures limiting the window of opportunity.
6	The attack vector is only available in a restricted time phase, e.g. on the ground in maintenance mode.
8	The attack can only be carried out during a very restricted time slot independent from the flight phase (e.g. during system reboot).

points	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
effectiveness	None							Basic						Moderate						High						Very High					
level of threat	Very High							High						Moderate						Low						Very Low					

Exercise – reflection on the time dimension

For the Information Security Risk Assessment a two-dimensional approach, i.e. likelihood/probability vs severity of the effect is adopted.

What if we introduce the **time** as a third dimension?

Threat actors motivations may change in time and so does the “knowledge” (capabilities of the sources and defenders).

Security Risk Acceptability Matrix

Risk Level	Threat Condition Severity of Effect				
Level of Threat	No Effect	Minor	Major	Hazardous	Catastrophic
Very High	Acceptable		Unacceptable		
High					
Moderate					
Low					
Extremely Low					Acceptable*

Security Risk Assessment is not Stable

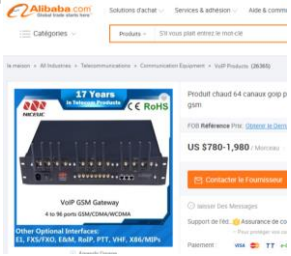
Knowledge / Equipment	None/Public Information and no preparation time	Uncontrolled Information and no significant preparation time	Insider Knowledge or Significant preparation time
None/Standard	0	2	6
Special COTS	0	2	6
Special	n/a		6
Bespoke	n/a	5	6

Special equipment which requires a substantial amount of resources to assemble (time above half a year or money above $100.000).

The fabulous case of the IMSI Catcher

Before 2013
Around 100K€

2016
20.000€



2018
700€ on Ali baba
DIY for 10€

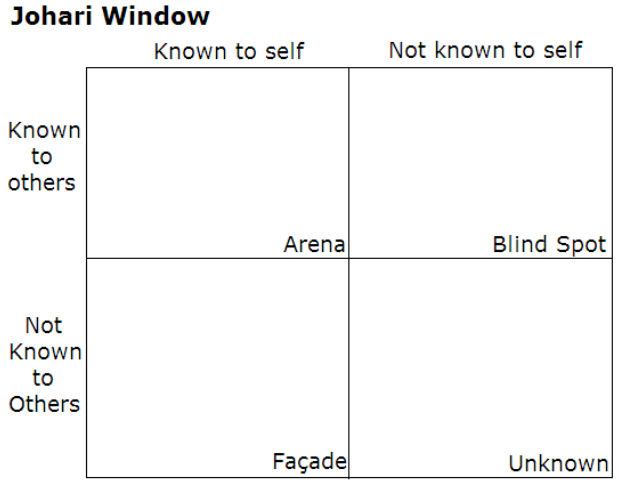
Uncertainty in cybersecurity risk assessment

We may have a 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.

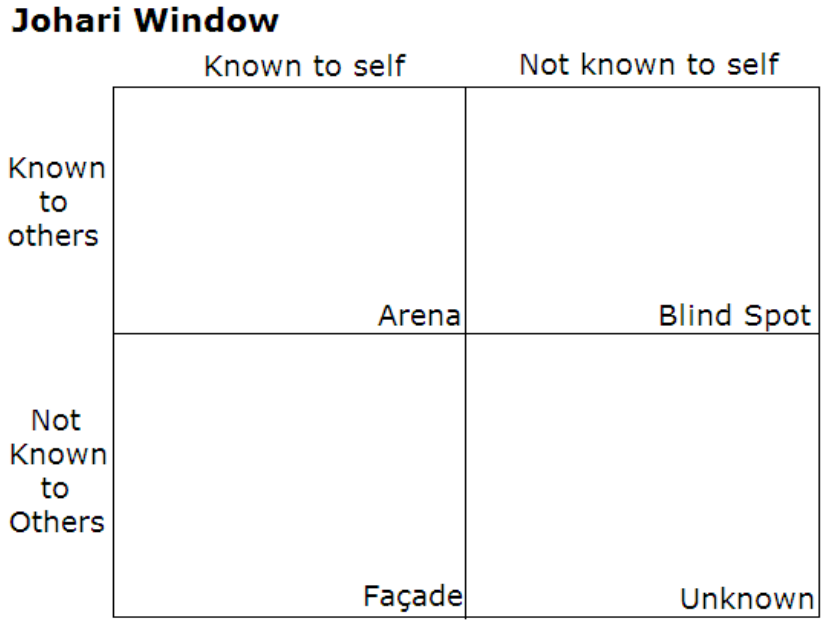
It is essential to be aware of the existence of elements of Knowledge that will emerge in the future and may change the risk picture.

The practical scheme is provided by the Johari Window that introduces the notion of “unknown unknowns”



Exercise – play with the roles

- The “Self” is your organisation

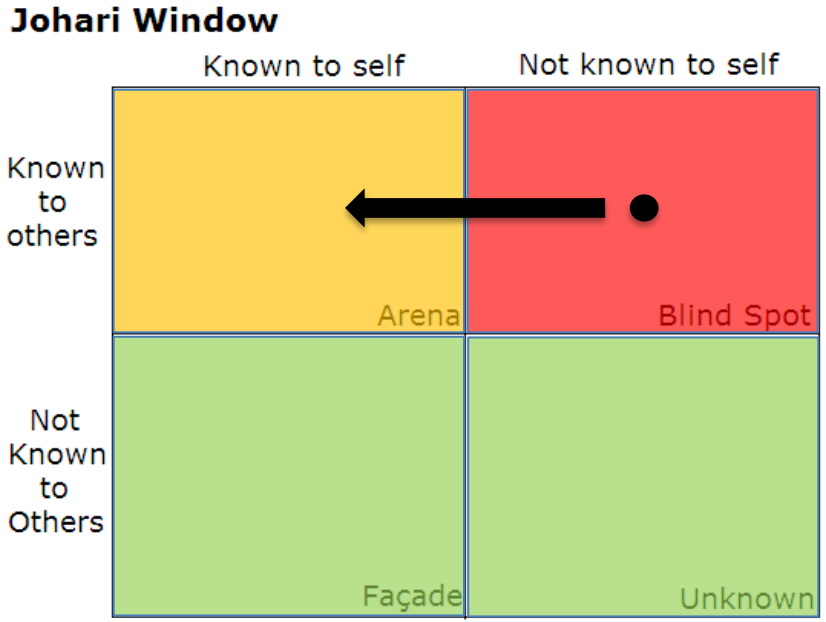


Exercise – play with the roles

- The “Self” is your organisation

The “unknown unknown” is safe until it becomes known to a threat source than turns into a “blind spot” for you

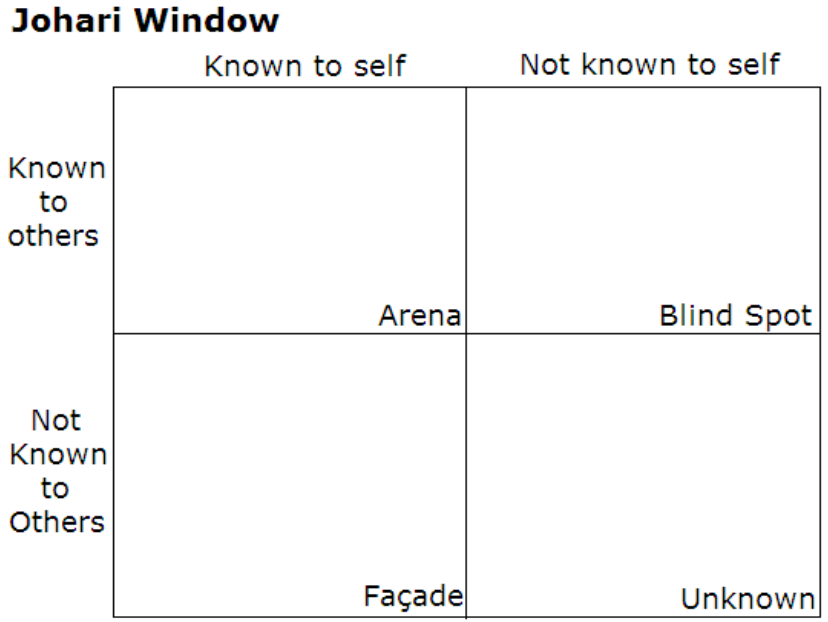
If “others” with knowledge are “allies” there should be means in place to get to the Arena state



Exercise – play with the roles

- The “Self” is a Threat Source

Where in the quadrant do you have the greatest advantages?

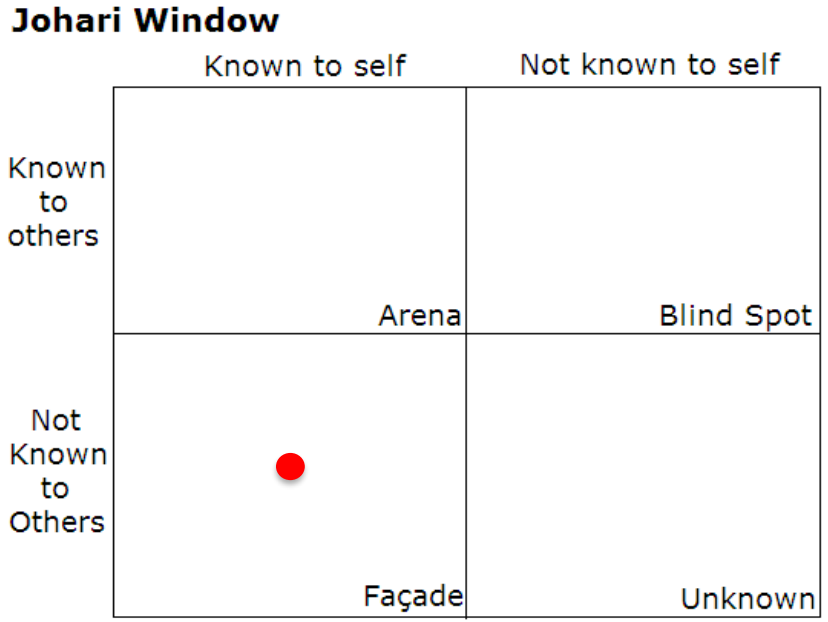


Exercise – play with the roles

- The “Self” is a Threat Source

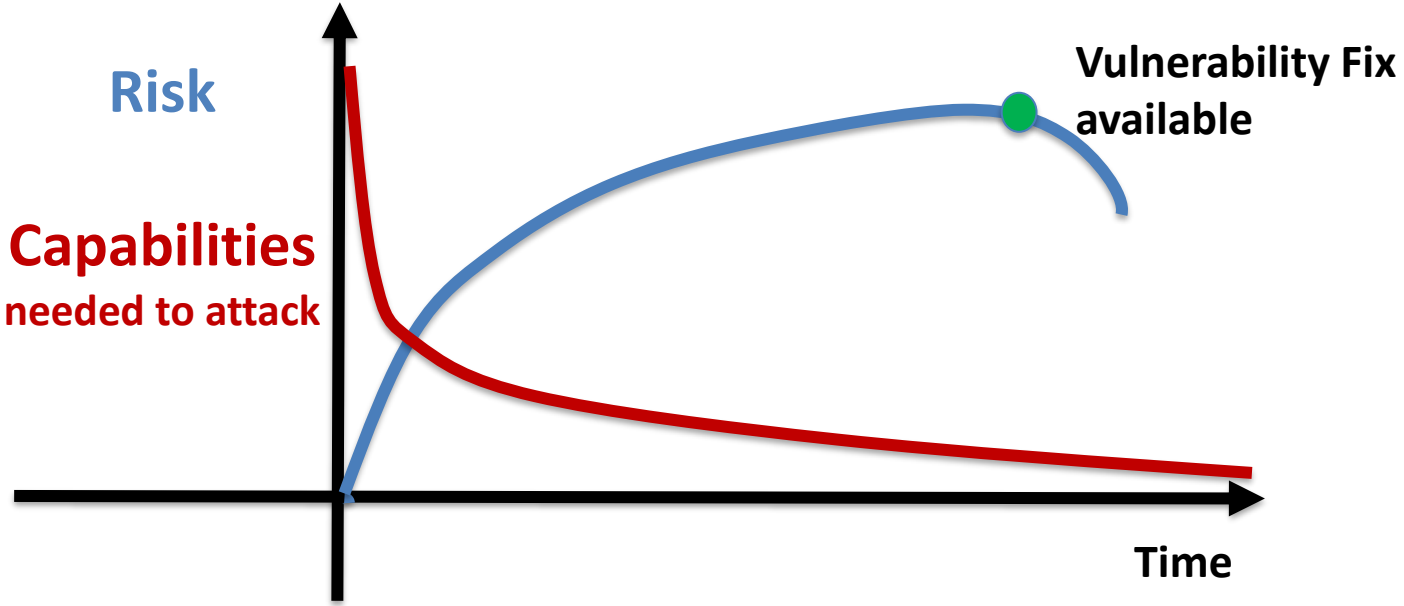
The façade is the Zero Days quadrant

Vulnerabilities privately known, unpatched and (maybe) exploitable!



Risk evolution – a graphical representation

Sooner or later a Vulnerability will be discovered and Exploits will be available



Elements driving the cybersecurity risks

Cybersecurity risks are driven by the notion of intent

vulnerabilities are exploited and an accident is not a fortuitous event

Traditional safety layers are not sufficient.

Aviation is a “System of Systems”

covering all aviation domains, and where products, services and organisations are increasingly interconnected.

Cybersecurity risks evolve very quickly

and incidents can spread very fast, which requires industry and authorities to do business differently.

Regulatory aspects

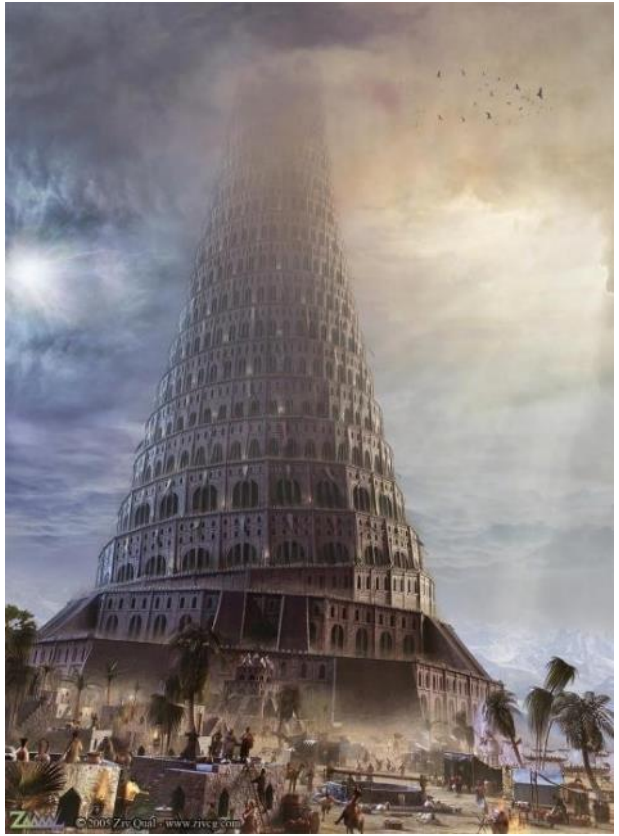
Managing Risk in a Multi-Stakeholder Environment

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



EASA

Regulation - from global to EU nation state level

Global Level – International Civil Aviation Organisation (ICAO)

European Union coordination

Basic Regulation and Implementing Regulations

Safety

Safety

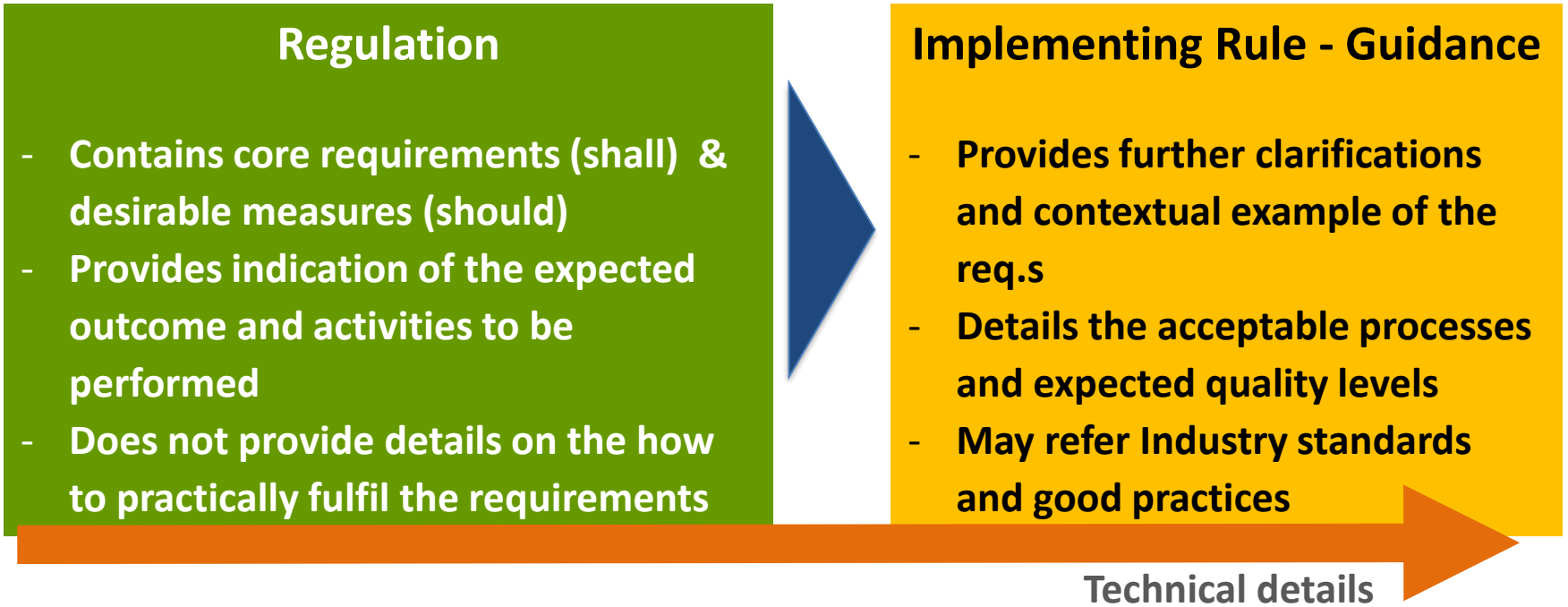
Security

Certification Specifications
Acceptable Means of Compliance
Guidance Material

EU Member States

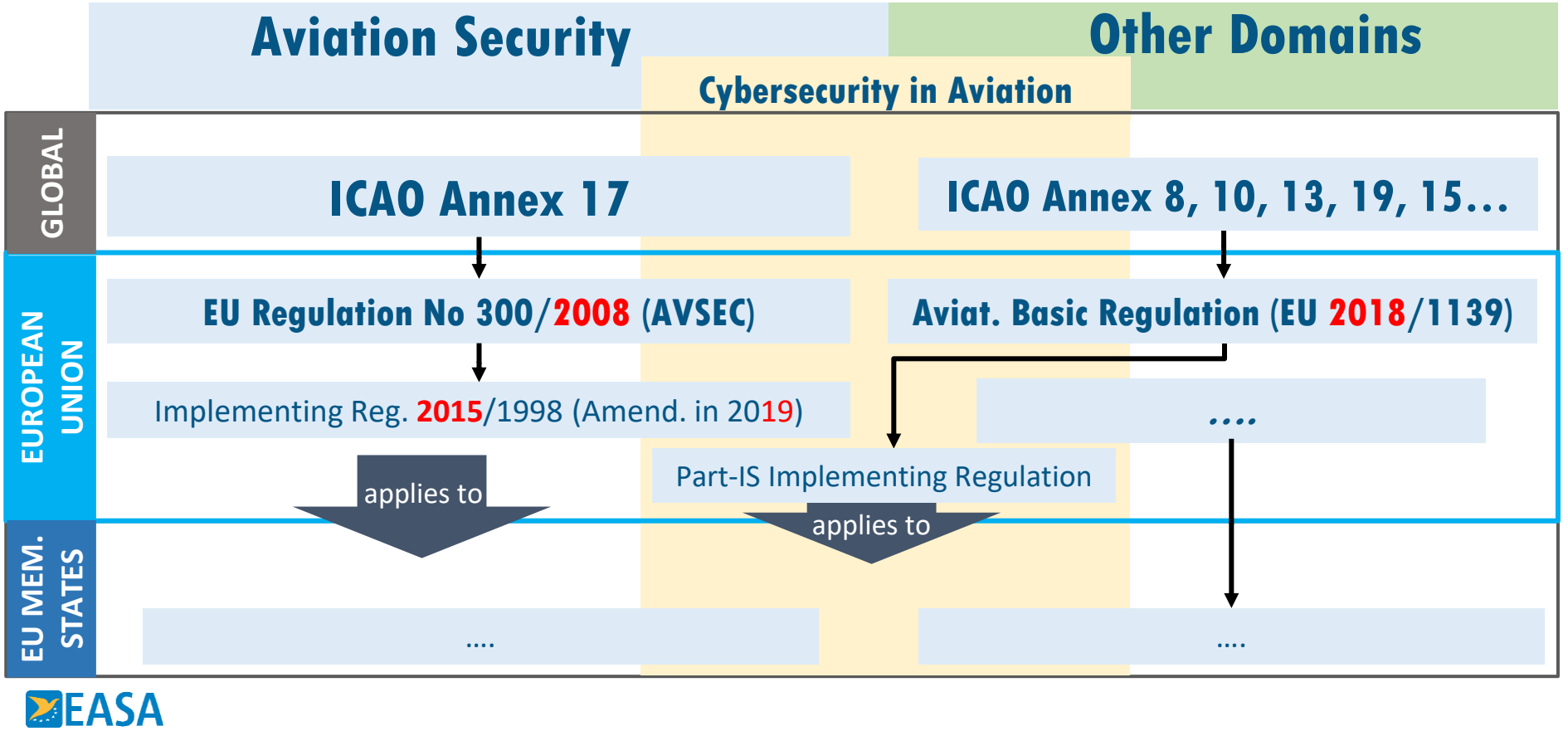
Binding regulatory requirements aligned with harmonised guidance

Typical aviation regulatory structure



This is a simplification - there may be further intermediate levels

Overview of the EU regulatory framework – cybersecurity in aviation



EASA

Making EU aviation cyber resilient

Regulations

Products

Cyber included in certification processes for all products

Aviation Organisations (People, Processes)

Part-IS regulatory package in force, applicable by 2026

Information Sharing - Collaborate to Reinforce the system

Sectorial ISAC to share knowledge

Network of National Experts to analysis events

Capacity building & Research

For a competent and well aware workforce

To understand the future Threat Landscape

Making EU aviation cyber resilient

Products

Cyber included in certification processes for all products

Aviation Organisations (People, Processes)

Part-IS regulatory package in force, applicable by 2026

Information Sharing - Collaborate to Reinforce the system

Sectorial ISAC to share knowledge

Network of National Experts to analysis events

Capacity building & Research

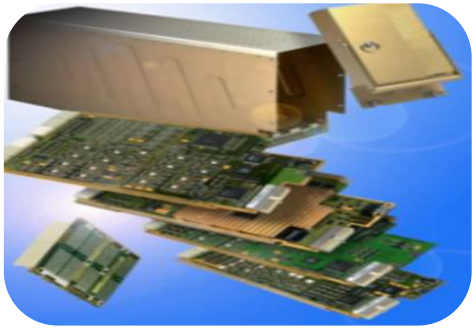
For a competent and well aware workforce

To understand the future Threat Landscape

EASA

Cybersecurity regulations for Products

Certification Specifications (CS) for different classes of products and equipment



All include similar requirements with the code CS NN.1319

Certification Specifications

CS 25.1319 Equipment, systems and network information protection

(a) Aeroplane equipment, systems and networks, considered separately and in relation to other systems, must be protected from intentional unauthorised electronic interactions (IUEIs) that may result in adverse effects on the safety of the aeroplane. Protection must be ensured by showing that the security risks have been identified, assessed and mitigated as necessary.

(b) When required by paragraph (a), the applicant must make procedures and Instructions for Continued Airworthiness (ICA) available that ensure that the security protections of the aeroplane's equipment, systems and networks are maintained.

[Amdt No: 25/25]

"Mitigated as necessary" means the manufacturer has the discretion to establish appropriate means of mitigation against information security risks

AMC 20-42 provides acceptable means of compliance, guidance and methods to perform security risk assessments and mitigations for aircraft information systems.

Threat Conditions in the Aviation Domain

Conditions resulting from exploitation of vulnerabilities having an adverse safety effect on the Aircraft and/or its occupants

…for example

The Vulnerability

The MFD software crashes if a malformed flight plan is loaded.

The Attacker Exploitation

An Attacker loads a maliciously formatted flight plan onto the MFD

The Safety Effect

The pilot activate the malformed flight plan on the MFD…

…that crashes, becoming unavailable!

Risk acceptability

- Contained in the Standards
- Can be tailored by products

TABLE 2-2: AIRWORTHINESS RISK ACCEPTABILITY MATRIX

	Severity of the Threat Condition Effect				
Level of Threat	No Safety Effect	Minor	Major	Hazardous	Catastrophic
Very High	Acceptable	Acceptable	Unacceptable	Unacceptable	Unacceptable
High	Acceptable	Acceptable	Unacceptable	Unacceptable	Unacceptable
Moderate	Acceptable	Acceptable	Acceptable	Unacceptable	Unacceptable
Low	Acceptable	Acceptable	Acceptable	Acceptable	Unacceptable
Extremely Low	Acceptable	Acceptable	Acceptable	Acceptable	Acceptable*

Source: ED-203A

Mitigations

- → Are they commensurate with the threat?
- → Are they efficient?
- → Which assurance do I have that the system is protected?

TABLE 4-4: SECURITY ASSURANCE RELATION TO THREAT CONDITION SEVERITY

Threat Condition Effect Severity	Minimum Security Assurance
Catastrophic	SAL 3 + SAL 2
Hazardous	SAL 3
Major	SAL 2
Minor	SAL 0
No Safety Effect	SAL 0

TABLE A-1: SECURITY SPECIFIC ASSURANCE OBJECTIVES ALLOCATION TABLE

Ref.	Objective	Scope	SAL 3	SAL 2	SAL 1	SAL 0	Security specific	Document sections
Security Risk Assessment Objectives								
O1.1	The security scope is established and validated.	AC, S	R	R	R	R	yes	4.1.1, B.2.1
O1.2	The Threat Condition Identification and Evaluation is complete and validated.	AC, S	R*	R	R	R	yes	4.1.1, B.2.1
O1.3	The Preliminary Aircraft/System Security Risk Assessments and Aircraft/System Security Risk Assessments are performed and consistent with related aircraft/system safety assessments.	AC, S	R*	R	A	N	yes	4.1.1, B.2.1
O1.4	Preliminary Aircraft/System Security Risk Assessment results have been processed to define aircraft/system security architecture and identify the need for security measures.	AC, S	R*	R	A	N	yes	4.1.1, B.2.1
O1.5	Aircraft/System Security Risk Assessment is consistent and complete with respect to security scope, security guidance, security requirements, security verification, security refutation and vulnerability identification.	AC, S	R*	R	A	N	yes	4.1.1, B.2.1

Source: ED-203A

Making EU aviation cyber resilient

Products

Cyber included in certification processes for all products

Aviation Organisations (People, Processes)

Part-IS regulatory package in force, applicable by 2026

Information Sharing - Collaborate to Reinforce the system

Sectorial ISAC to share knowledge

Network of National Experts to analysis events

Capacity building & Research

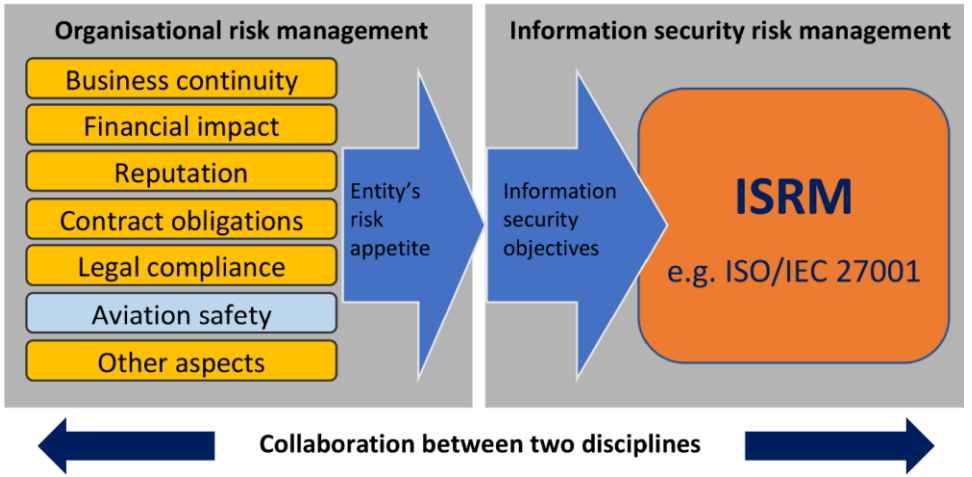
For a competent and well aware workforce

To understand the future Threat Landscape

EASA

Cybersecurity regulations for Organisations

- Evaluate risk **across the whole aviation system**
- 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**



EASA

Part-Information Security (IS)

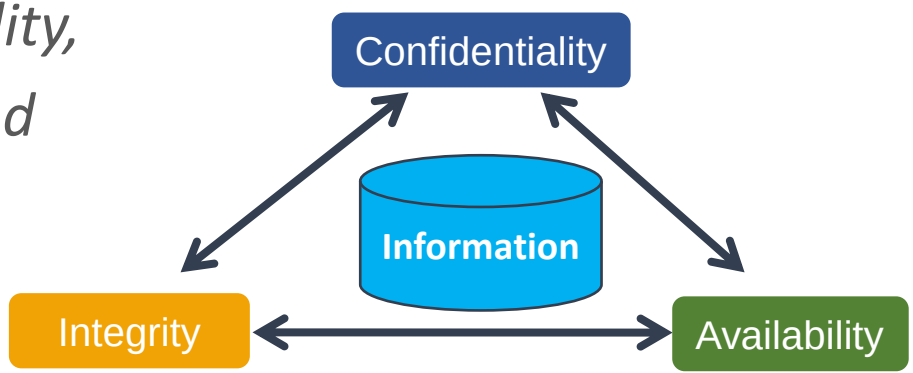
Objective	Protect the aviation system from information security risks **with potential impact on aviation safety**
Scope	Information and communication technology systems and data used by Approved Organisations and Authorities for civil aviation purposes
Activity	- **identify and manage** information security risks related to information and communication technology systems and data used for civil aviation purposes; - **detect** information security events, identifying those which are considered information security incidents; and - **respond** to, and **recover** from, those information security incidents

Proportionate to the impact on aviation safety

What is an ISMS?

What is Information Security Management?

- ISO 27000 states that ***Information Security Management*** *is a top-down, business driven approach to the management of an organization's physical and electronic information assets in order to preserve their*
  - *Confidentiality,*
  - *Integrity, and*
  - *Availability.*



Definition of ISMS

ISO 27001

An ISMS is the means by which management monitors and controls information security, minimizing the residual **business risk** and ensuring that information security continues to fulfill corporate, customer and legal requirements.

business risk

Part-IS

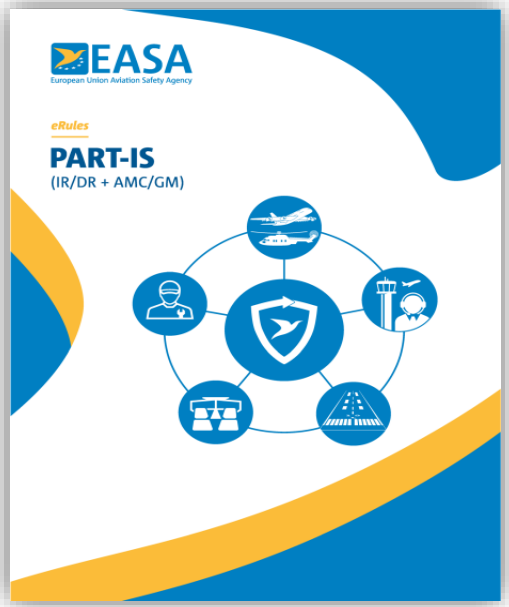
An ISMS is the means by which management monitors and controls information security, minimizing the residual business safety risk and ensuring that information security continues to fulfill ~~corporate, customer and~~ legal requirements and societal expectations.

safety risk

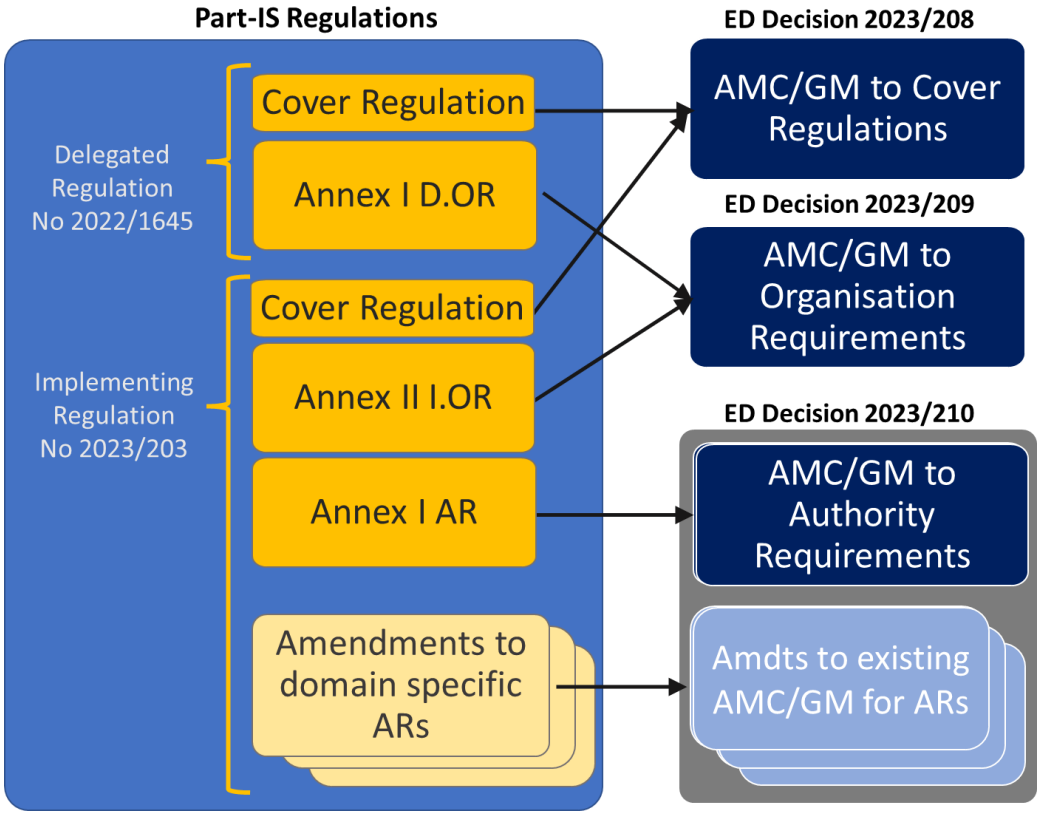
Overview of Part IS requirements: Organisation vs Authority

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

Rules and AMC/GM structure



Easy Access Rules available here



Aircraft cybersecurity

Security domains principles

EASA

ARINC - 811

- Standard for aircraft security
  - ARINC - 811 is
    - Commercial Aircraft Information Security Concepts of Operation and Process Framework
  - In particular its attachment nr 3
    - Provides typical security needs for each information type

Aircraft domain	Security categorisation		
	Confidentiality	Integrity	Availability
ACD information	Low	High	High
Airline Ops information	High	Medium	Medium
Airline administrative info.	High	Medium	Medium
Airline passenger info.	High	High	Medium

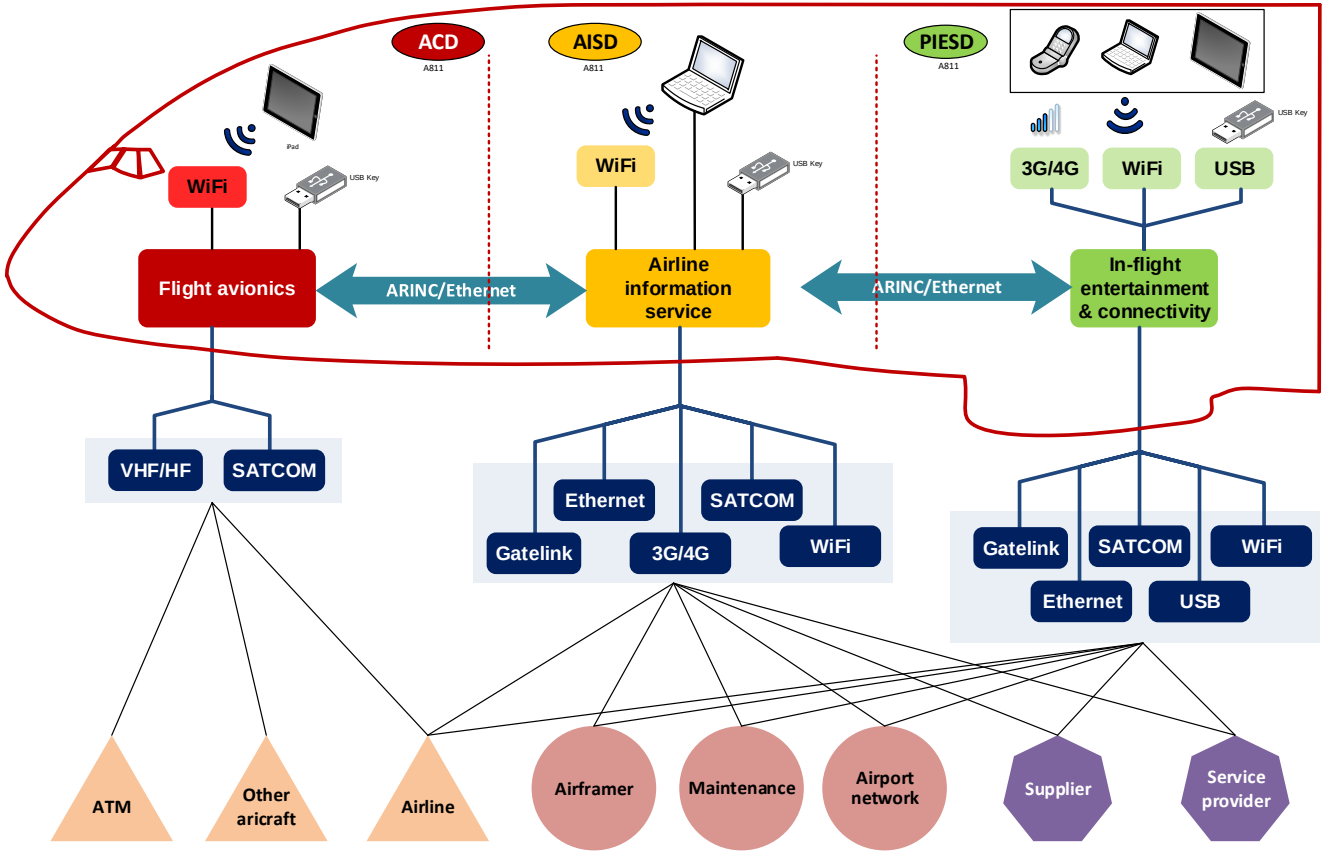
Aircraft security domains

Information within an aircraft have different “sensitivity”

Sensitivity has to be measured against C.I.A

- Military sensitivity is the confidentiality level
- Military aircraft sensitivity is
  - Integrity level for flight data
  - Confidentiality level for air operations
- Commercial Aircraft sensitivity is
  - Integrity level for flight data
  - Confidentiality and integrity level for airlines data

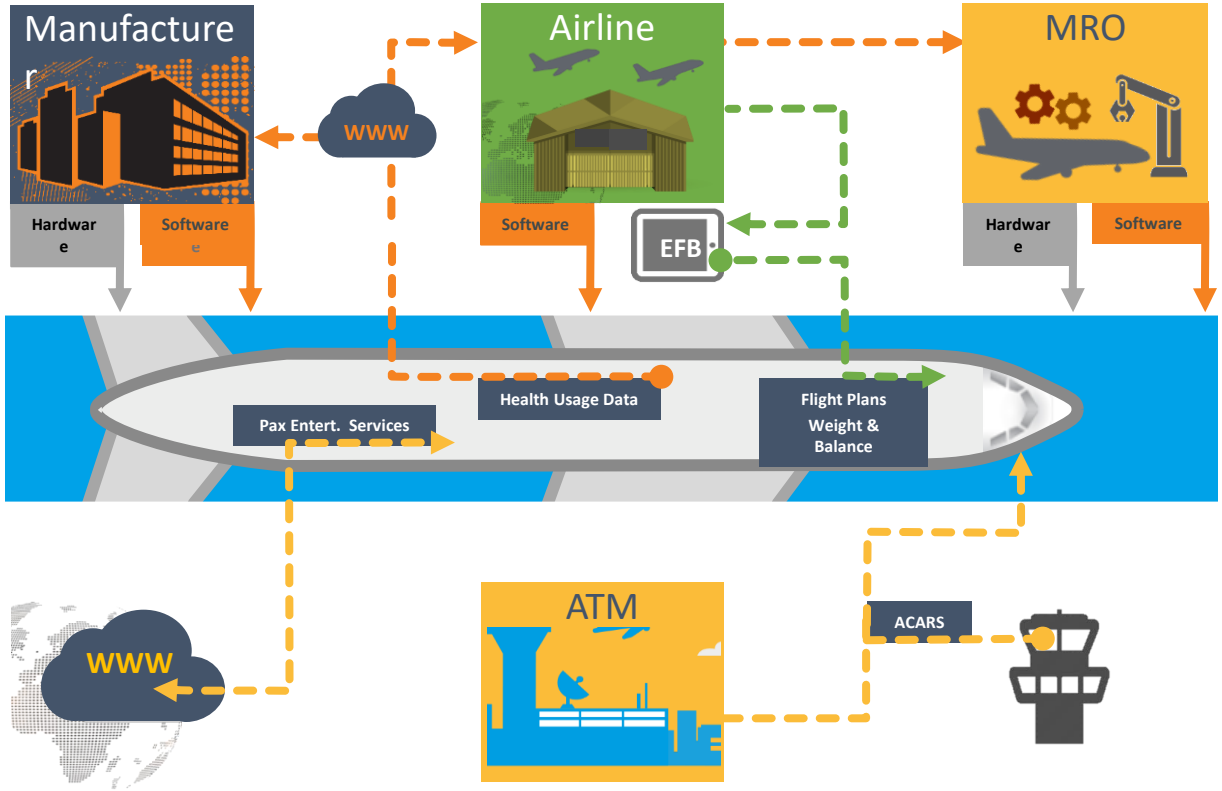
Aircraft Security Domains



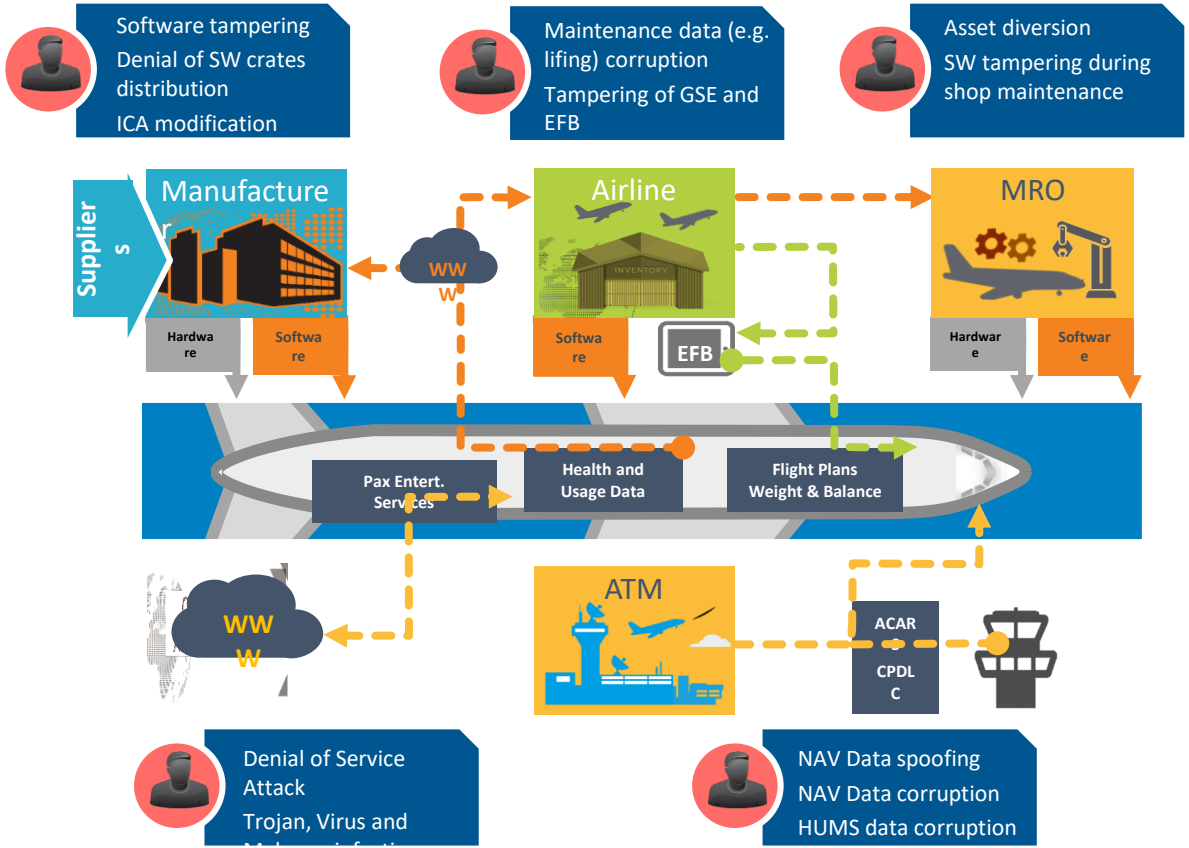
Continuing Airworthiness Insights

Security in the Maintenance Environment

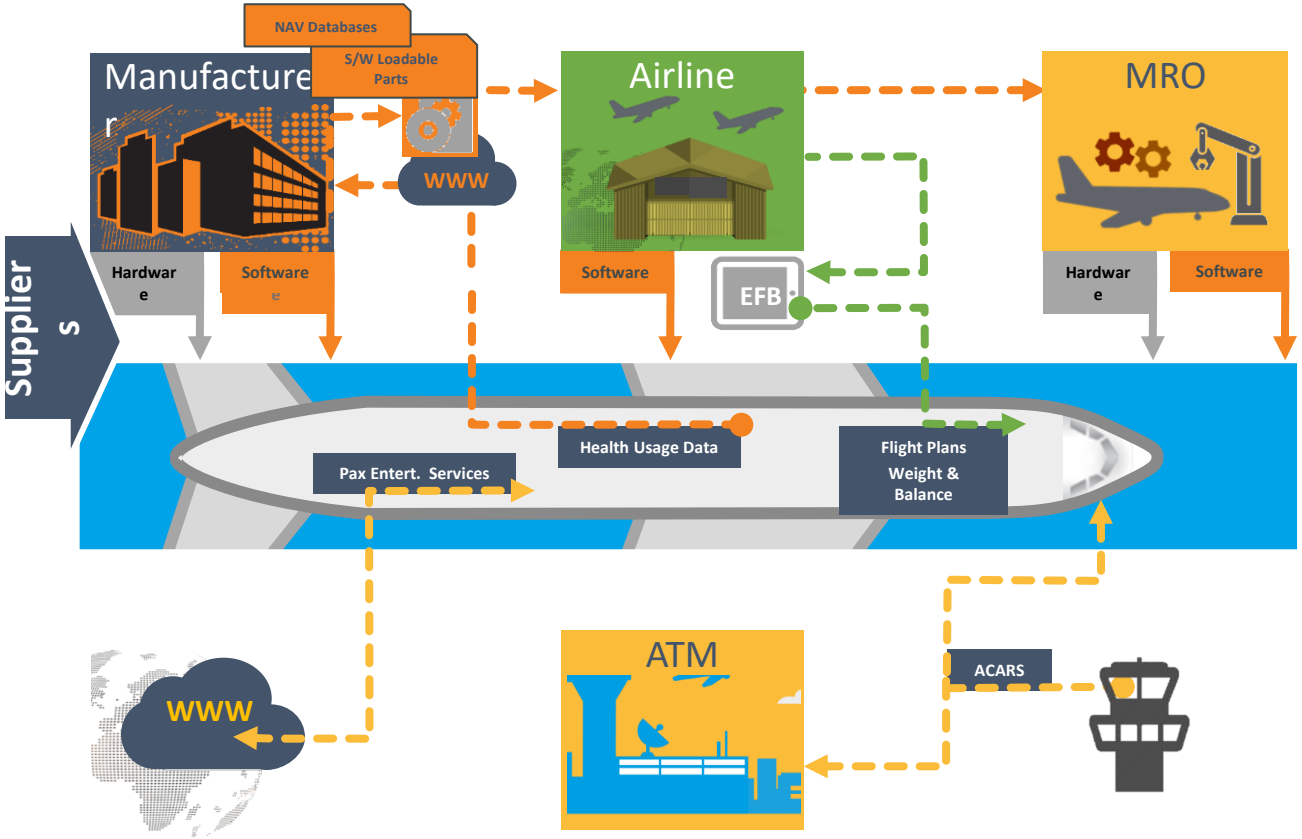
Aviation Security Environment- Overview



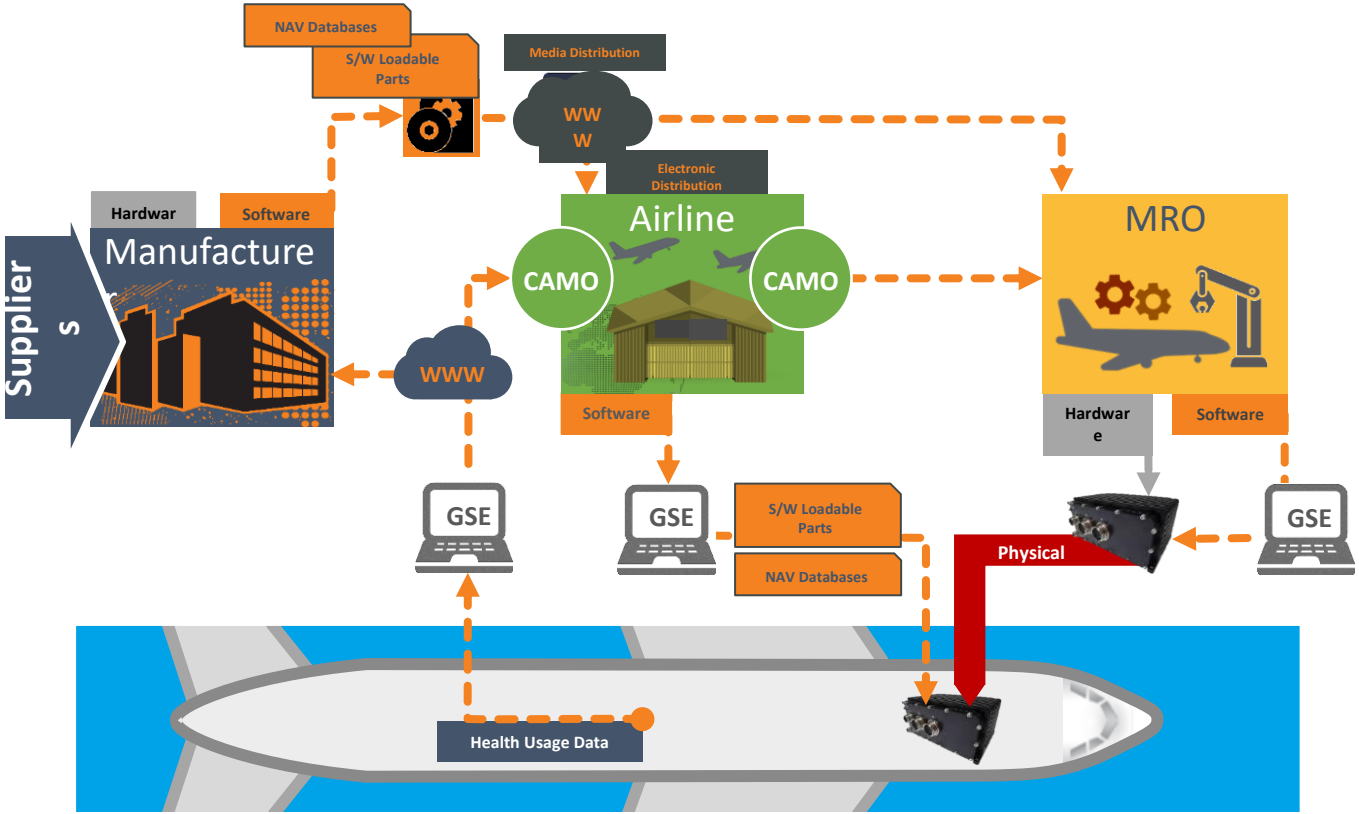
Threat Scenarios – What may happen



A/C Maintenance - Security Environment

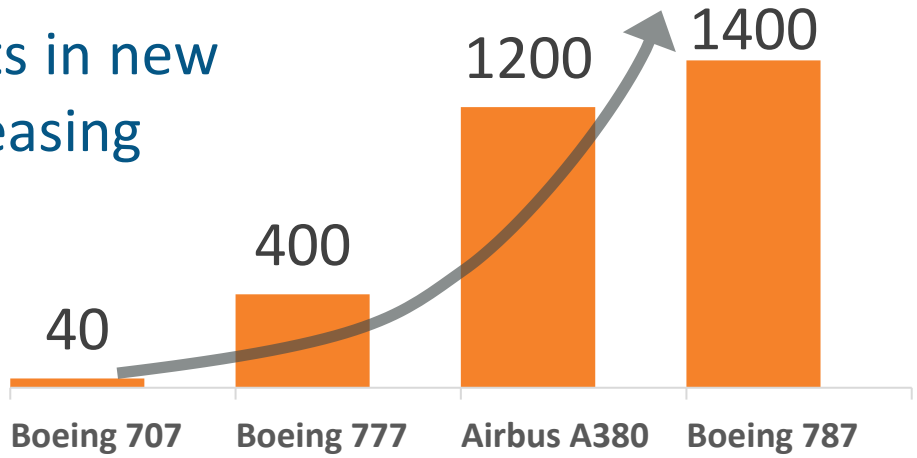


A/C Maintenance - Security Environment



Aggravating Factors

- Number of S/W loadable parts in new aircrafts is exponentially increasing



- Increase of Internet connected Services for Remote Maintenance via COTS devices with COTS Operating Systems

Aircraft maintenance – Data/SW loading

Based on outdated threat model

- Insider problem

Aircraft don’t always provide protected interfaces

- Maintenance access terminal (some Windows based)
- Easy access to connectors (A429, USB,…)

Though solution exist for recent aircraft

- ARINC 835 for signed Field Loadable Software parts

Continuing Airworthiness Guidance

Security of Field Load. S/W

Digital certificates

Copying

Storage & Distribution

Disposal of hardware

Network access points

Training

Access control methods

Incident response

Other Standards for Operations

ARINC

- Guidance for Security Event Logging in an IP Environment - A852
- Guidance for Security of Loadable SW Parts Using Digital Signatures - A835

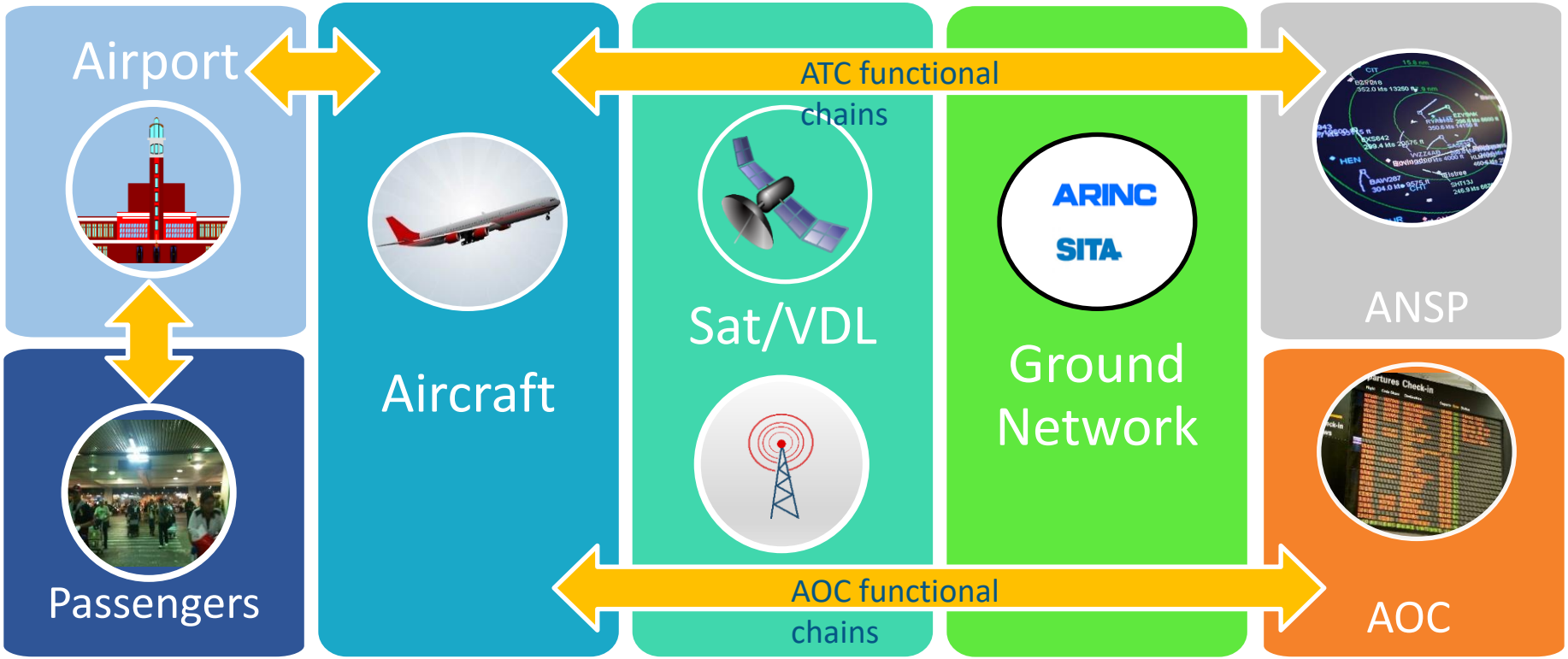
ATA

- Recommendations on standardized methods to achieve the appropriate level of security for an application primarily relying on digital identities – Spec 42

Risks in a system of systems

The functional chain

The global landscape – Combined perspective



The global landscape – Ground Operations

Aircraft

Airport Gatelink

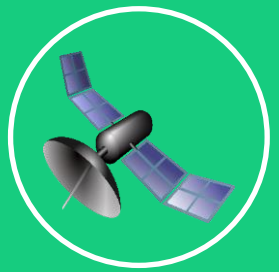
Internet

Airline

Functional chains (Monitoring, Weight& Balance, Maintenance,…)

The global landscape – Air Operations

Aircraft



Satellite or VHF

ARINC

SITA

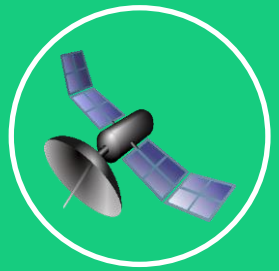
Ground Network

Airline

Functional chains (MET, FPL, Voice,..)

The global landscape – Safety perspective

Aircraft



Satellite

ARINC

SITA

Ground Network

ANSP

Functional chains (CPDLC, ADS-B, ACARS)

Functional chain & security objectives

- Functional chain operational objectives
  - Transferring ATC data between ANSP and aircraft
- Functional chain high-level security objectives
  - Integrity
    - Messages (CPDLC, ACARS, voice,..) origin is legitimate
    - Messages content is not modified end to end
  - Availability
    - Loss is major (backup exists)
    - Is cared of by safety analysis

Responsibilities on functional chain

- ANSP
  - Generates and delivers data to NSP
  - Is able to guarantee message authenticity
- Network Service Provider
  - Receives data from ANSP and routes messages to Satcom provider
  - Is NOT able to guarantee message authenticity
- Satellite Service provider
  - Receives messages from NSP and routes them to aircraft
  - Is NOT able to guarantee message authenticity
- Aircraft
  - Receives messages from SatCom provider
  - Is able to verify message authenticity

The need for trans-organisational risk management

Evaluate risk across the whole aviation system to include

- ANSPs, ACSPs, Aircrafts, Airlines, Aerodromes & safety relevant ground services

Enable efficient 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

- Communication plan with stakeholders to develop

Achieve maturity

- Anticipation and recovery

Comparability of risk assessments

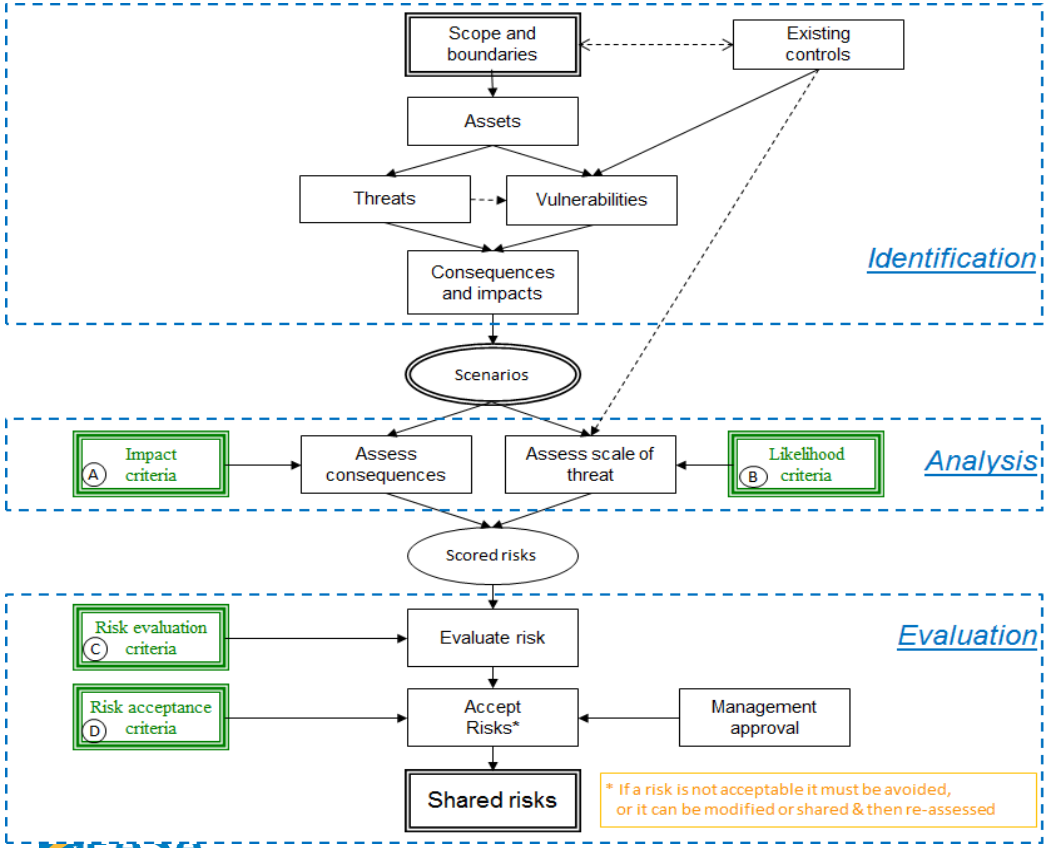


Diagram represents SRA standard as presented in ISO 27005 and ED-201

Identification phase carries all commonalities to SRAs

Analysis and Evaluation methods vary

Likelihood significance and usage is in aviation

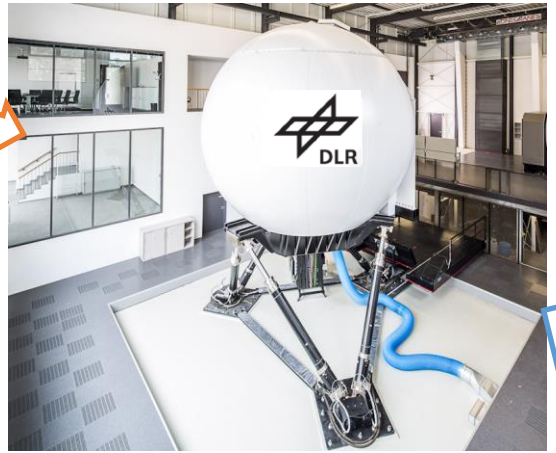
Aircraft cybersecurity

EASA research

IACT Research - report published in 2018

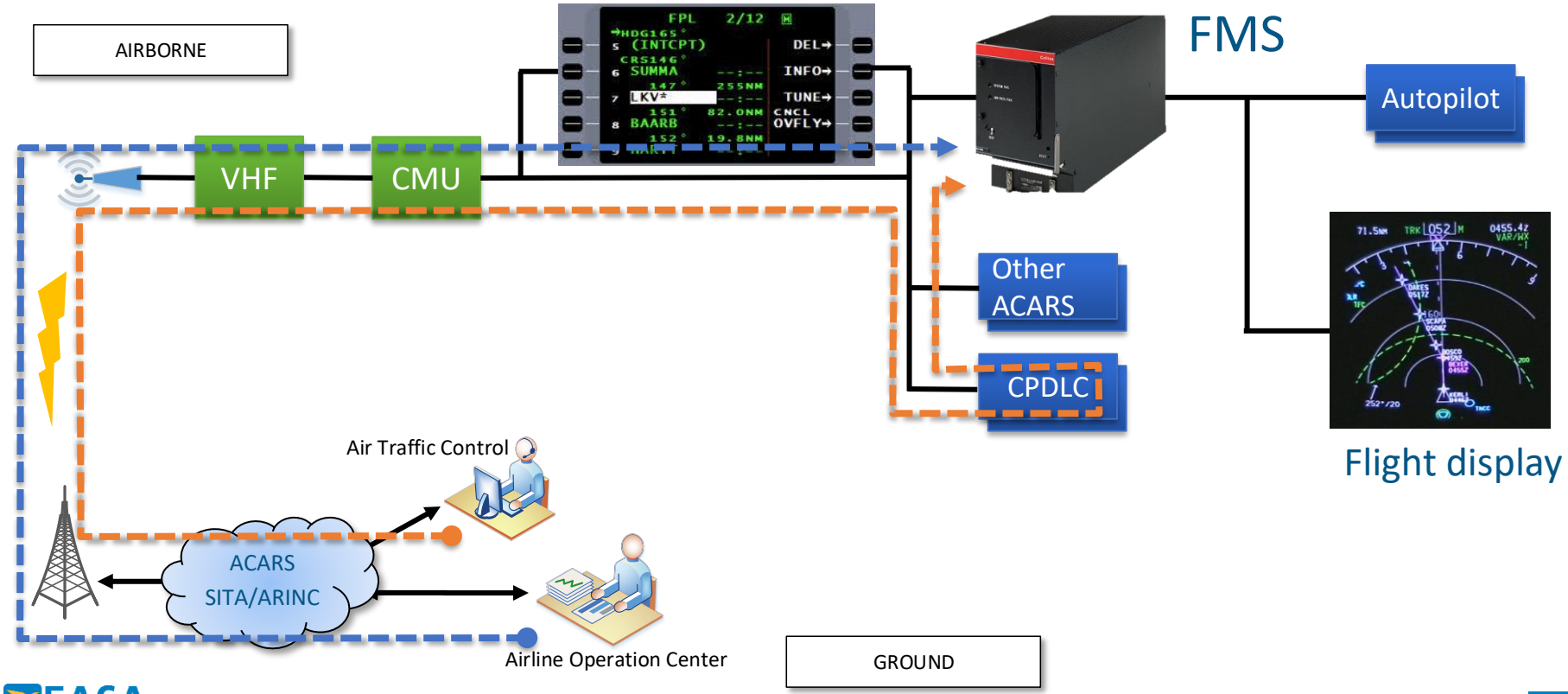
Impact Assessment of Cybersecurity Threats

Qascom
Trust is Nice, Control is Better.



enav

Datalink vulnerability analysis (Airborne)



420 USD and some effort

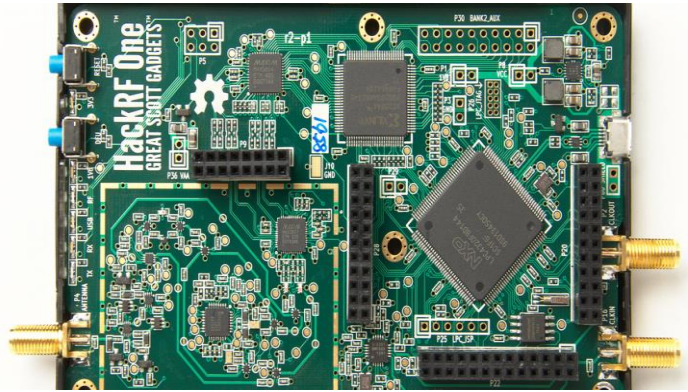
osqzss / gps-sdr-sim

Code | Issues 4 | Pull requests 0

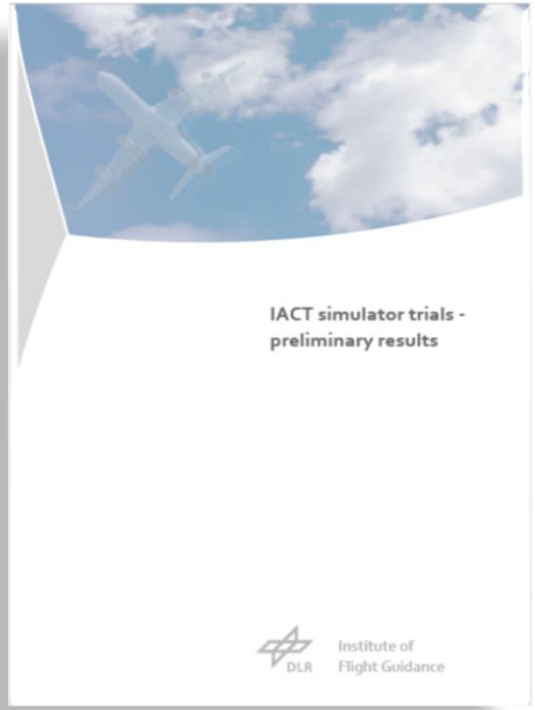
Software-Defined GPS Signal Simulator

GPS-SDR-SIM

GPS-SDR-SIM generates GPS baseband signal data streams, which can be converted to RF using software-defined radio (SDR) platforms, such as ADALM-Pluto, bladeRF, HackRF, and USRP.



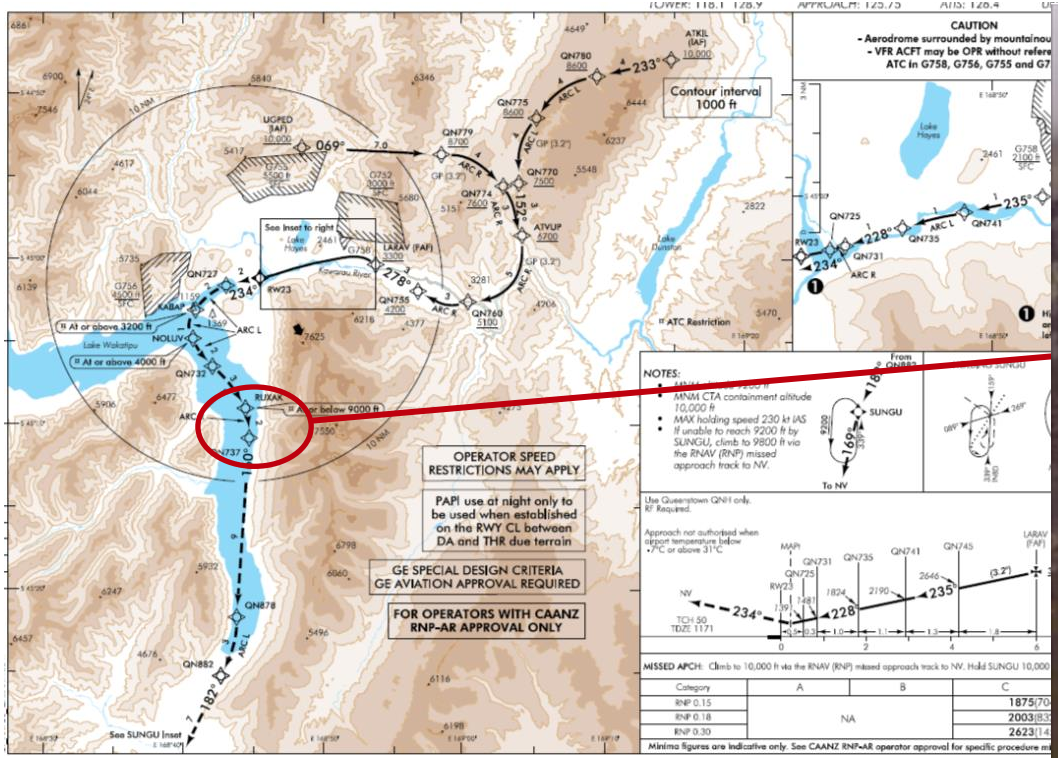
Research: IACT



Attack	Detection	Results / comments
ACARS load sheet update	1 out of 7 times	Aircraft rotated before V_r
ACARS flight plan update	2 out of 2 times	Flight plan change rejected, aircraft stayed on course
Hacked database during RNP 0.1 approach	5 out of 6 times	Go-around and missed approach detected during approach, once at the MDA
Denial of service attack FMS	2 out of 2 times	FMS/map functionality lost, aircraft still controllable, help from ATC requested, raw data available
En-route GNSS spoofing	0 out of 3 times	Diverging flight path not detected during event, except from ATC, slightly increased workload after event, reduction of confidence in navigation system
Approach GNSS spoofing	0 out of 1 time	Spoofing not detected during event. After event, due to the cross track error and the disengagement of auto pilot, the approach was discontinued

Research: IACT

RNP 0.15 approach



Mitigations for GPS spoofing

Use multiple satellite systems

- GLONASS
- Galileo

Cross reference with Inertial Reference System

- 0.6 Nautical Miles drift per hour and tenths of a degree per hour
  - Spoofing experiment was 0.6 NM within 5 mns
  - Detection capability of IRS?
- Resynced from GPS: when was the last trusted fix?

Detection capabilities in GPS equipment

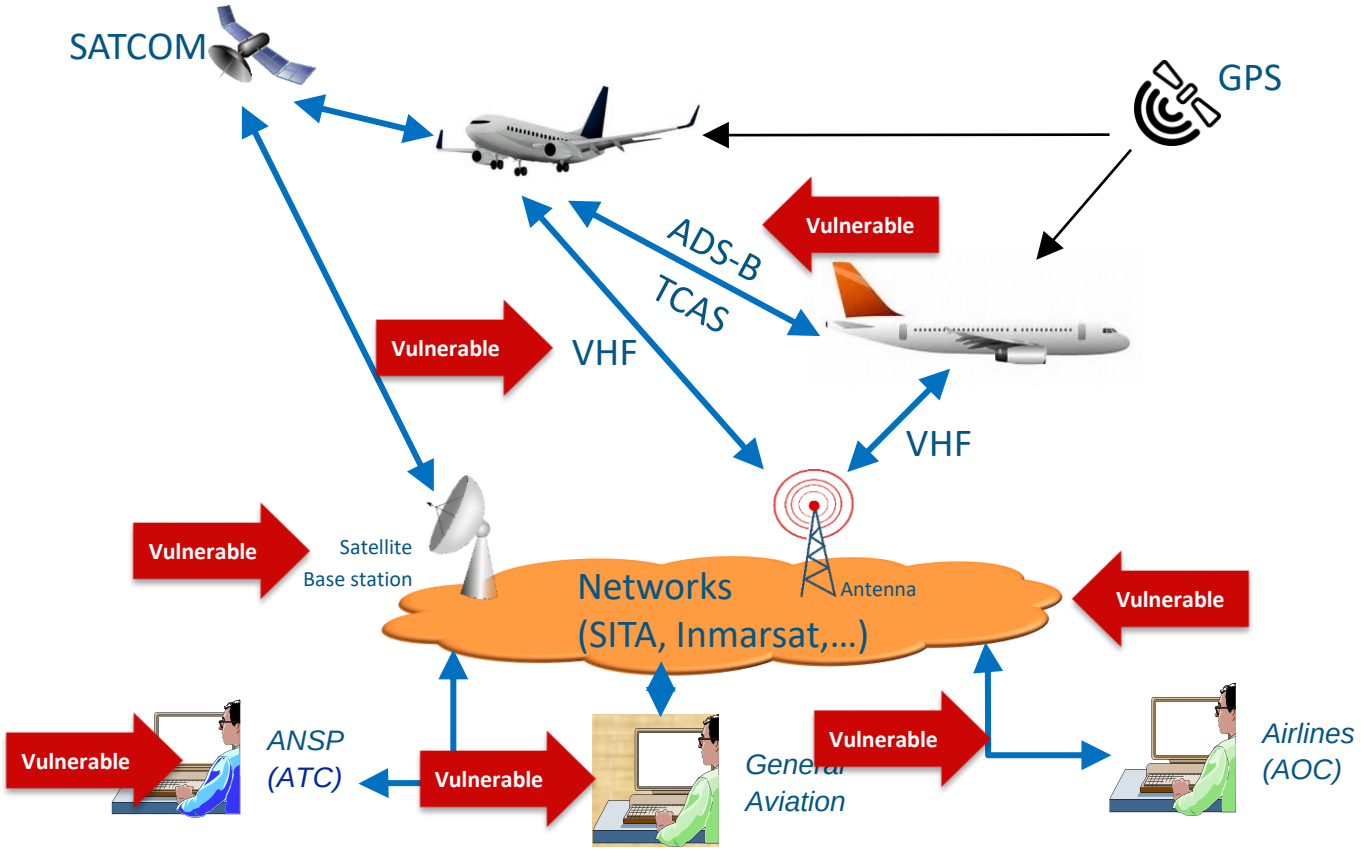
- Spoofed signal appears differently (spectrum, power and direction of radiation)

Cybersecurity in Aviation

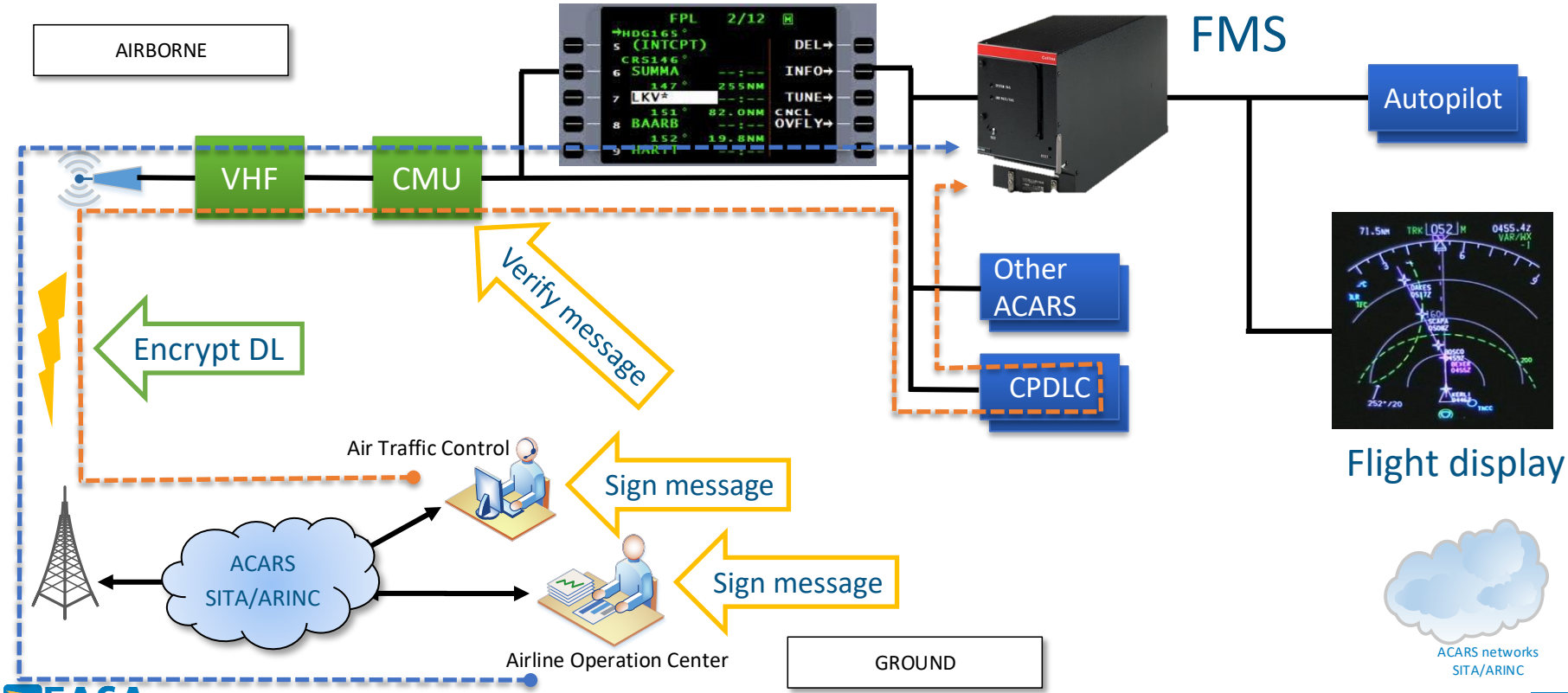
Global Environment

Vulnerabilities, threats and Solutions

The flying aircraft environment



Possible mitigations



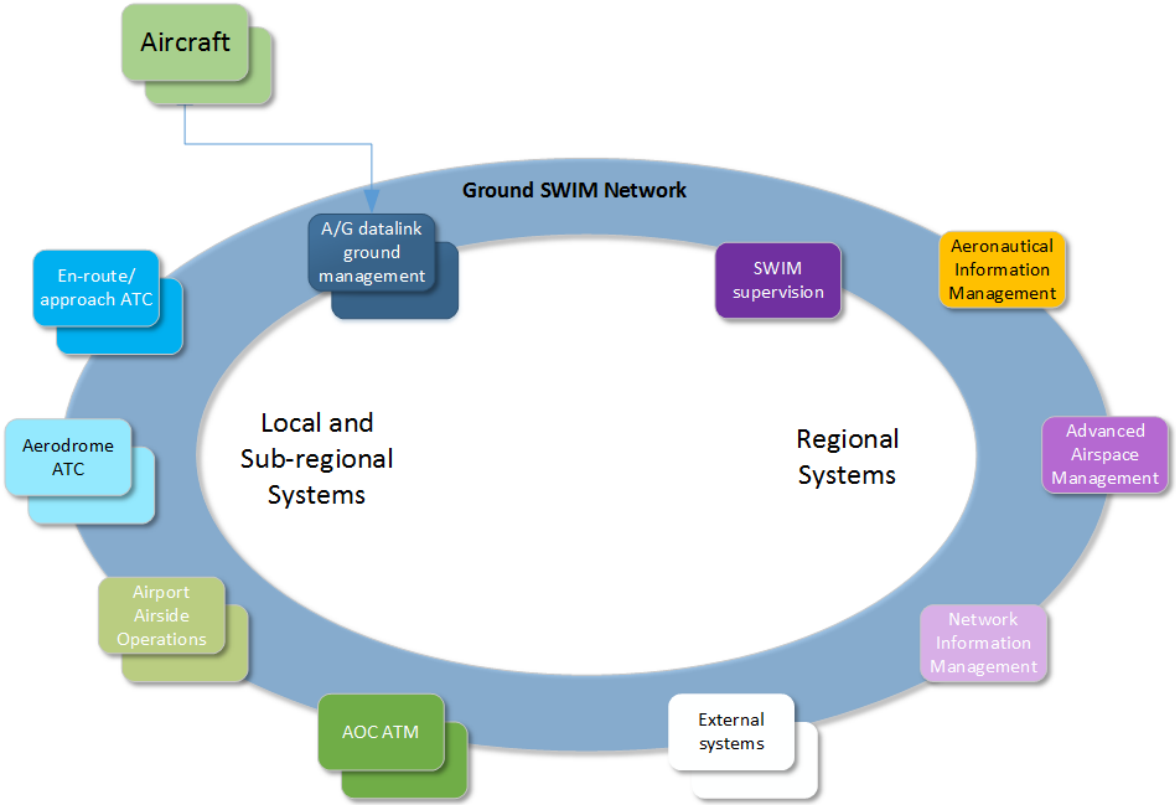
Other Datalink Vulnerability (Ground)

- Ground segment
  - ATM
  - AOC
- Communication segment
  - SITA, ARINC connection points and network
  - Radio segment (VHF, VDL)

ATM

Vulnerabilities, threats and Solutions

ATM – A system of system

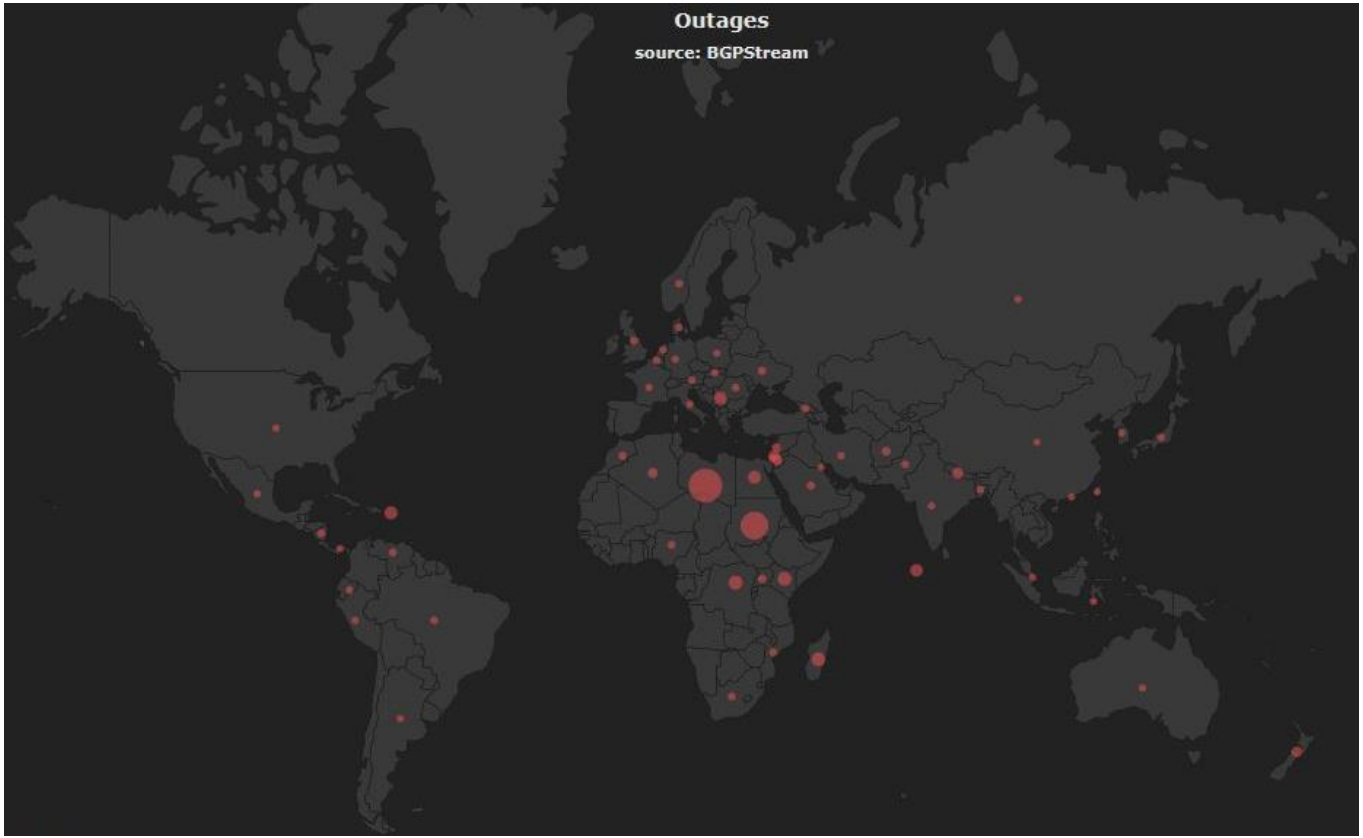


ATM ground segment vulnerability

- ATM infrastructure
  - Network centric operations concept
    - Real time information exchange
    - Rely on multiple sensors
  - Connected to external service providers
  - Use COTS components
  - Increased use of Internet as transport backbone
    - Cost reduction

Similar vulnerabilities as standard IT systems, plus…

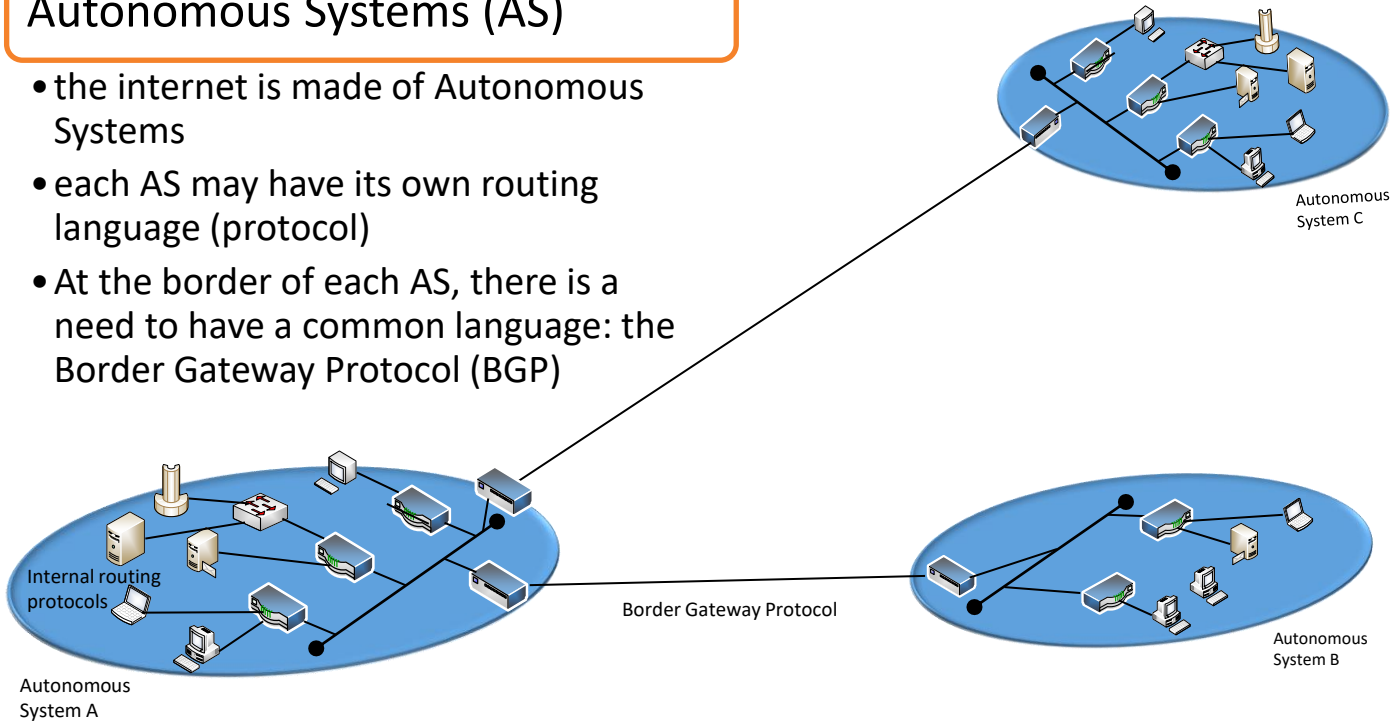
…risks induced by using Internet as backbone



A short introduction on the backbone

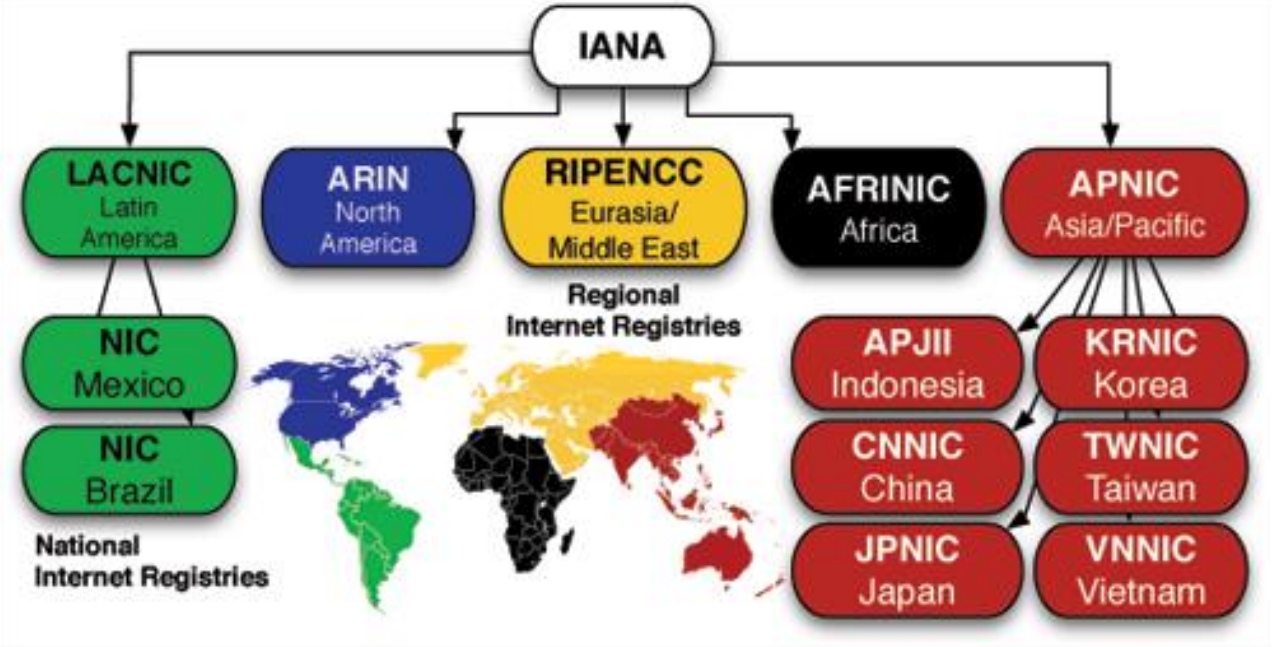
Autonomous Systems (AS)

- the internet is made of Autonomous Systems
- each AS may have its own routing language (protocol)
- At the border of each AS, there is a need to have a common language: the Border Gateway Protocol (BGP)



Governance

IP addresses distribution is hierarchical



What can go wrong

- By the Internet rule, any network can announce a route to any IP address (BGP protocol)
- If an AS decides to announce a bad route the consequences can be endured worldwide
  - Route announced are propagated to neighbours
  - Whole IP ranges can be unreachable
- Traffic can also be diverted (hijacked)
  - AS announces a route to a sub-range of address
  - AS announces a “best” route

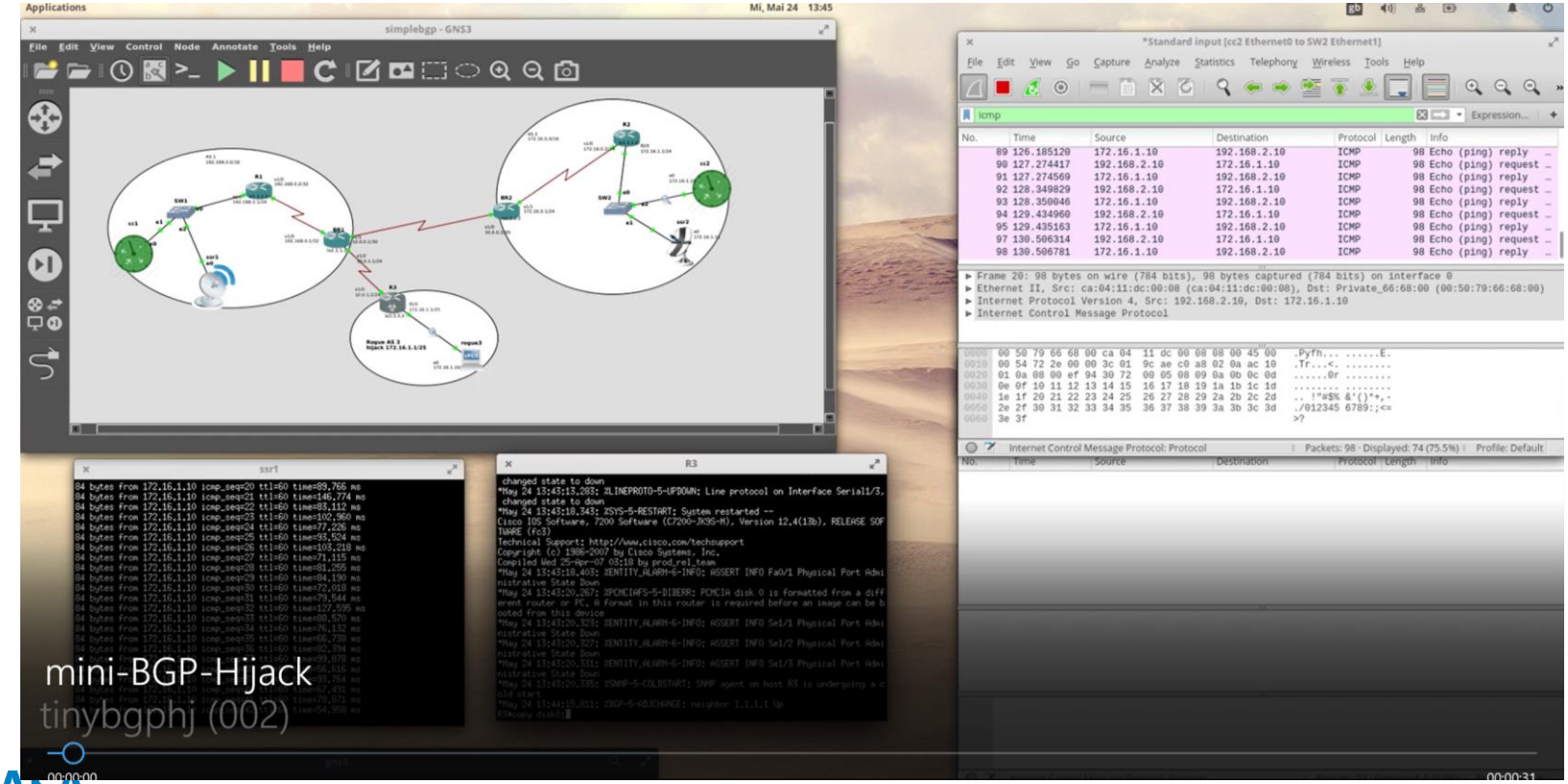
Motivations identified so far

- Censorship
  - Iran, Jan 2017
  - Pakistan, 2008
- Theft
  - May 2014, Bitcoins stealing
- Espionage
  - China, April 2010, diverted US military traffic for 18 minutes in claiming to provide the best routes to tens of thousands of networks worldwide.

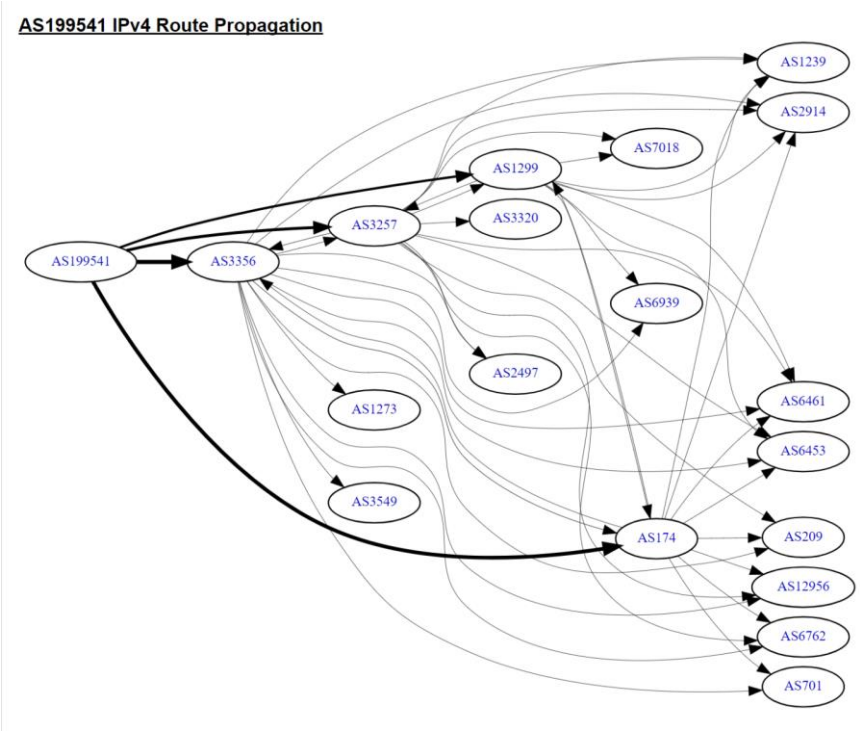
Attack frequency

Bgpstream capture 09/11/2017

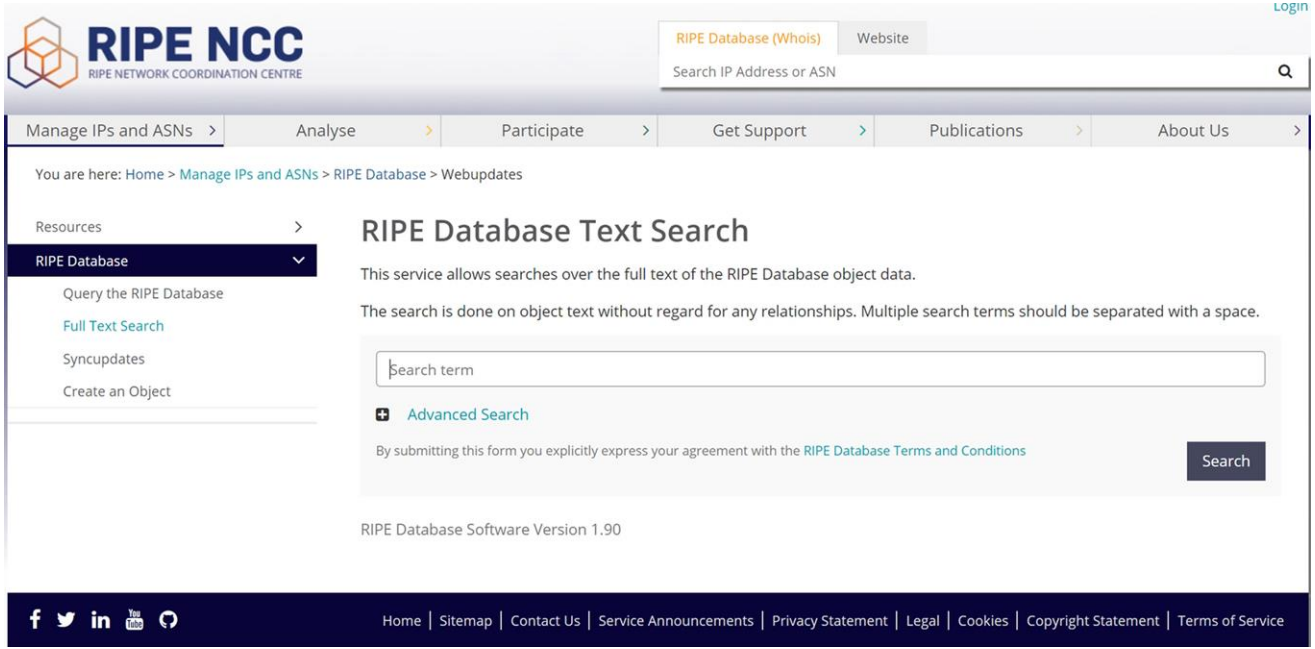
Difficulty



How addresses are made accessible worldwide?

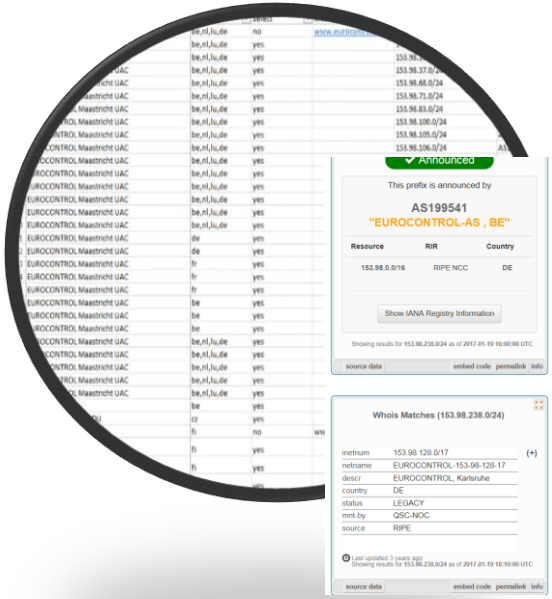



```
Frame 180: 107 bytes on wire (856 bits), 107 bytes captured (856 bits) on interface 0
Ethernet II, Src: c2:01:18:48:00:00 (c2:01:18:48:00:00), Dst: c2:02:1e:6c:00:00 (c2:02:1e:6c:00:00)
Internet Protocol Version 4, Src: 192.168.12.1 (192.168.12.1), Dst: 192.168.12.2 (192.168.12.2)
Transmission Control Protocol, Src Port: 42513 (42513), Dst Port: 179 (179), Seq: 236, Ack: 236, Len: 53
Border Gateway Protocol - UPDATE Message
    Marker: ffffffffffffffffffffffffffffffff
    Length: 53
    Type: UPDATE Message (2)
    Withdrawn Routes Length: 0
    Total Path Attribute Length: 25
  Path attributes
    Path Attribut - ORIGIN: IGP
      Flags: 0x40: Well-known, Transitive, Complete
        0... .... = Optional: Well-known
        .1.. .... = Transitive: Transitive
        ..0. .... = Partial: Complete
        ...0 .... = Length: Regular length
      Type Code: ORIGIN (1)
      Length: 1
      Origin: IGP (0)
    Path Attribut - AS_PATH: 1
      Flags: 0x40: Well-known, Transitive, Complete
        0... .... = Optional: Well-known
        .1.. .... = Transitive: Transitive
        ..0. .... = Partial: Complete
        ...0 .... = Length: Regular length
      Type Code: AS_PATH (2)
      Length: 4
      AS Path segment: 1
    Path Attribut - NEXT_HOP: 192.168.12.1
    Path Attribut - MULTI_EXIT_DISC: 0
      Flags: 0x80: Optional, Non-transitive, Complete
        1... .... = Optional: Optional
        .0.. .... = Transitive: Non-transitive
        ..0. .... = Partial: Complete
        ...0 .... = Length: Regular length
      Type Code: MULTI_EXIT_DISC (4)
      Length: 4
      Multiple exit discriminator: 0
  Network Layer Reachability Information (NLRI)
    1.1.1.1/32
      NLRI prefix length: 32
      NLRI prefix: 1.1.1.1 (1.1.1.1)
```


Login
RIPE NCC
RIPE NETWORK COORDINATION CENTRE
RIPE Database (Whois)
Website
Search IP Address or ASN
Manage IPs and ASNs
Analyse
Participate
Get Support
Publications
About Us
You are here: Home > Manage IPs and ASNs > RIPE Database > Webupdates
Resources
RIPE Database
Query the RIPE Database
Full Text Search
Syncupdates
Create an Object
RIPE Database Text Search
This service allows searches over the full text of the RIPE Database object data.
The search is done on object text without regard for any relationships. Multiple search terms should be separated with a space.
Search term
Advanced Search
By submitting this form you explicitly express your agreement with the RIPE Database Terms and Conditions
Search
RIPE Database Software Version 1.90
Home | Sitemap | Contact Us | Service Announcements | Privacy Statement | Legal | Cookies | Copyright Statement | Terms of Service

Implications for Aviation (EU examples)

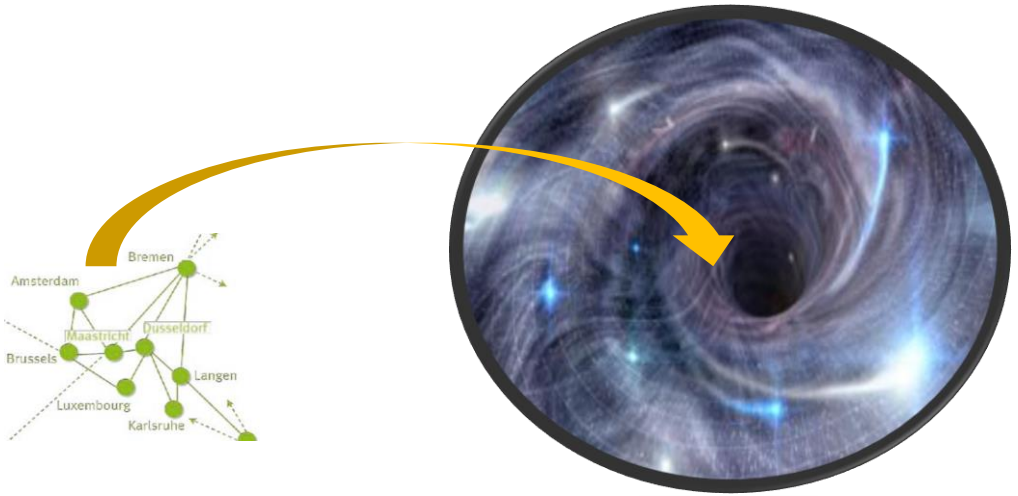
- EU ANSPs live in either
  - their own Autonomous System
    - DFS, SNA-F, Avinor, Austrocontrol…
  - The Eurocontrol Autonomous System
    - Be, Ne, Lux…
  - Commercial AS
    - ENAV (Telecom IT), Sweden ATM (TELIANET), …



It takes less of an hour to list all AS and prefixes of all European ANSPs. Just ask the RIPE

Weird idea 1

Reroute all or most of European ANSPs prefixes into a black hole for several hours.



Weird idea 2

Highjack routes from ANSP *XYZ*.

Try to figure out when radar surveillance UDP/ASTERIX messages are present and if found play with them…

Add/Remove/change plots?

WIRESHARK

```
ASTERIX Protocol
BLOCK Cat 1
    ASTERIX CATEGORY: Monoradar Target Reports (1)
    Block length: 47
  + RECORD : 1
  - RECORD : 2
      FSPEC Asterix: 0x0000f7a4
      System Area Code: 8
      System Identification code: 226
    + Target Report Descriptor: 0xa8
      Track number: 126
      Position in Polar Coordinates: 0x4c2bb35b rho= 76,00 NM, theta= 252,00 deg
      Calculated Track Velocity in Polar Representation: Ground speed= 358,16 kt
    + .... 1111 1000 1110 = Mode-3/A Code: 7616
    + ..00 0101 1100 1000 = Flight Level (*25ft): 1480 = 370 FL (x100ft)
    + 0000 010. = Radar Plot Characteristics: 2
```

EASA

BGP vulnerabilities mitigations

- Some solutions exist
  - prefix filtering
    - Reversed incentive (you protect the rest of the internet, not you)
  - RPKI (validation of the origin)
    - Centralized authority…
  - BGPSec (validation of the Path)
    - Online cryptography (need updated hardware)
    - Effective when all AS of a path implement BGPSec (who starts?)

    https://www.internetsociety.org/deploy360/start/

ATM wireless segment vulnerability

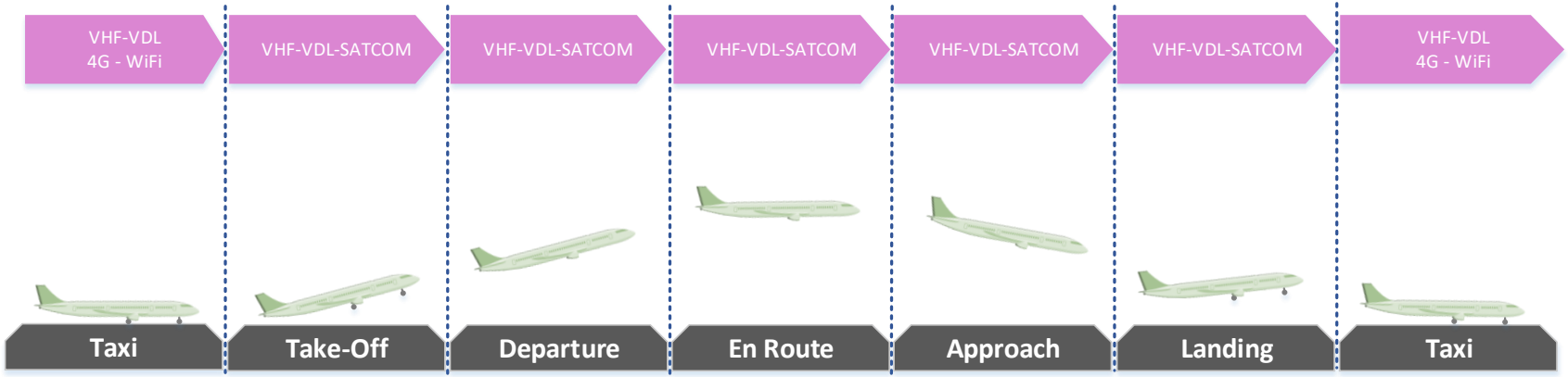
- Evolution from traditional threat model
  - Inferior technological, financial capabilities
  - Requirement of inside knowledge
  - Use of analog communications

Security by obscurity

- …to modern threat model
  - Increased digitisation and automation without considering possible attacks
  - Increased technological capabilities (SDR)
  - Aviation knowledge easily available

More on ATM vulnerabilities

- Controller Pilot Data Link Communications (CPDLC)
  - Replaces often voice for time-critical ATC clearances
  - End to end service used for various phases of flight
  - Impersonation is easily possible as not authenticated
  - Safety critical for messages related to FL changes

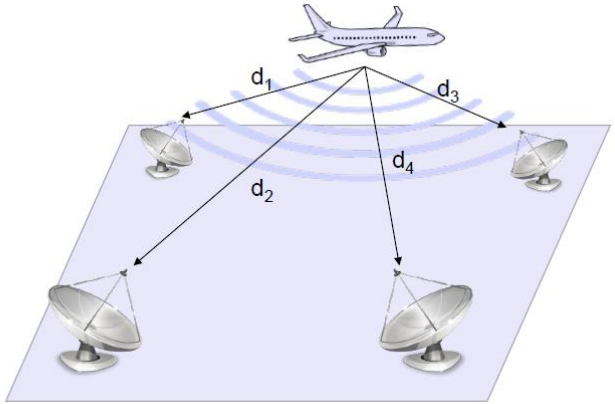


More on ATM vulnerabilities (Cont.)

- Primary surveillance radar (PSR)
  - Just to identify an object – no ID – no altitude
- Secondary Surveillance Radar (SSR)
  - Interrogation (1030MHz) – Reply (1090MHz)
  - Easy jamming, modifying, injection with SDR
    - https://github.com/antirez/dump1090
  - Mode S identifier is modifiable
  - Mode S is sensitive to DoS (via interrogation freq.)

More on ATM vulnerabilities (Cont.)

- ADS-B
  - Same vulnerabilities as Mode S
  - Injection of ghost aircrafts
    - Detectable on ground with multilateration
    - Non detectable on board
  - To become the main ATC protocol in the future



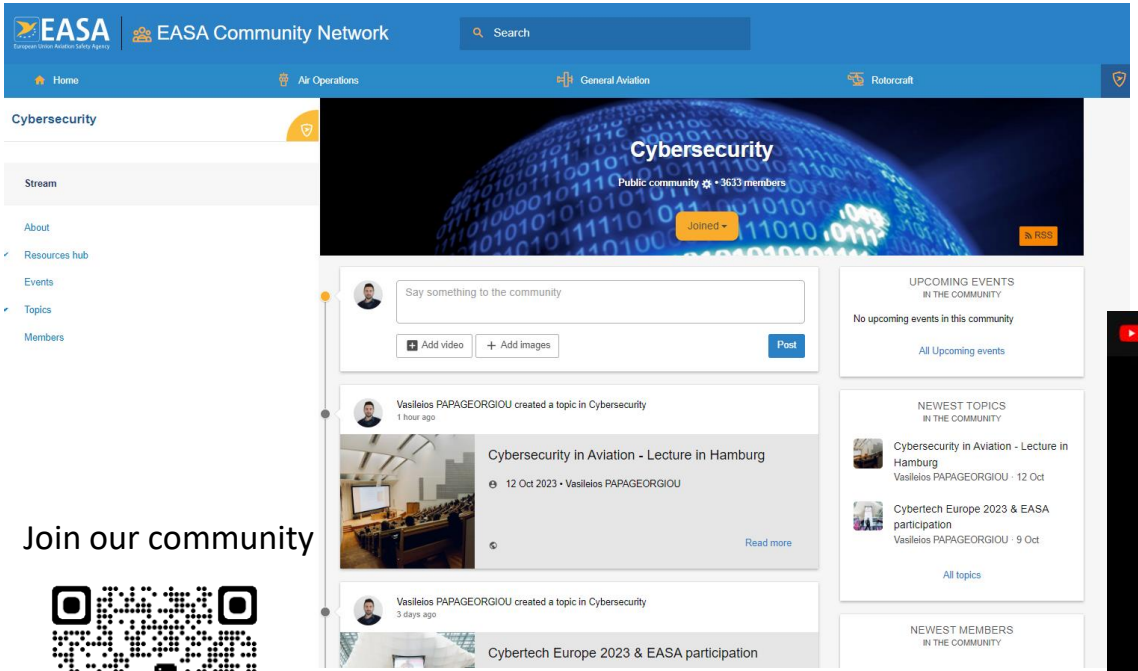
More on ATM vulnerabilities (Cont.)

- TCAS
  - Uses available ATC info such as Mode C and S
  - Interrogates all aircrafts in vicinity
  - Information received is not authenticated
  - Creating ghost aircraft is possible
- ACARS
  - Used for both ATC and AOC
  - Extremely vulnerable when sent via VHF or VDLm2
  - Secured ACARS (A823) was never implemented

Possible mitigations

- End-to-end authentication between aircraft and ATC
  - No short-term outcome
  - **ICAO Trust Framework Panel – use cases**
- Improvement of procedures
  - Simulate cyber-attacks to help on pilot/ATC reaction
  - Monitor to detect cyber-attacks
  - Include detection means in aircraft or equipment

EASA Cybersecurity Community



Join our community

SAFETY WEEK on YouTube