EASA
European Union Aviation Safety Agency

Cybersecurity Aspects Related to STCs

Cyrille Rosay
Senior Expert Avionics - Cybersecurity

Angeliki Karakoliou
Junior Aviation Professional

STC WORKSHOP

May 16th/17th 2019

Your safety is our mission.

An Agency of the European Union

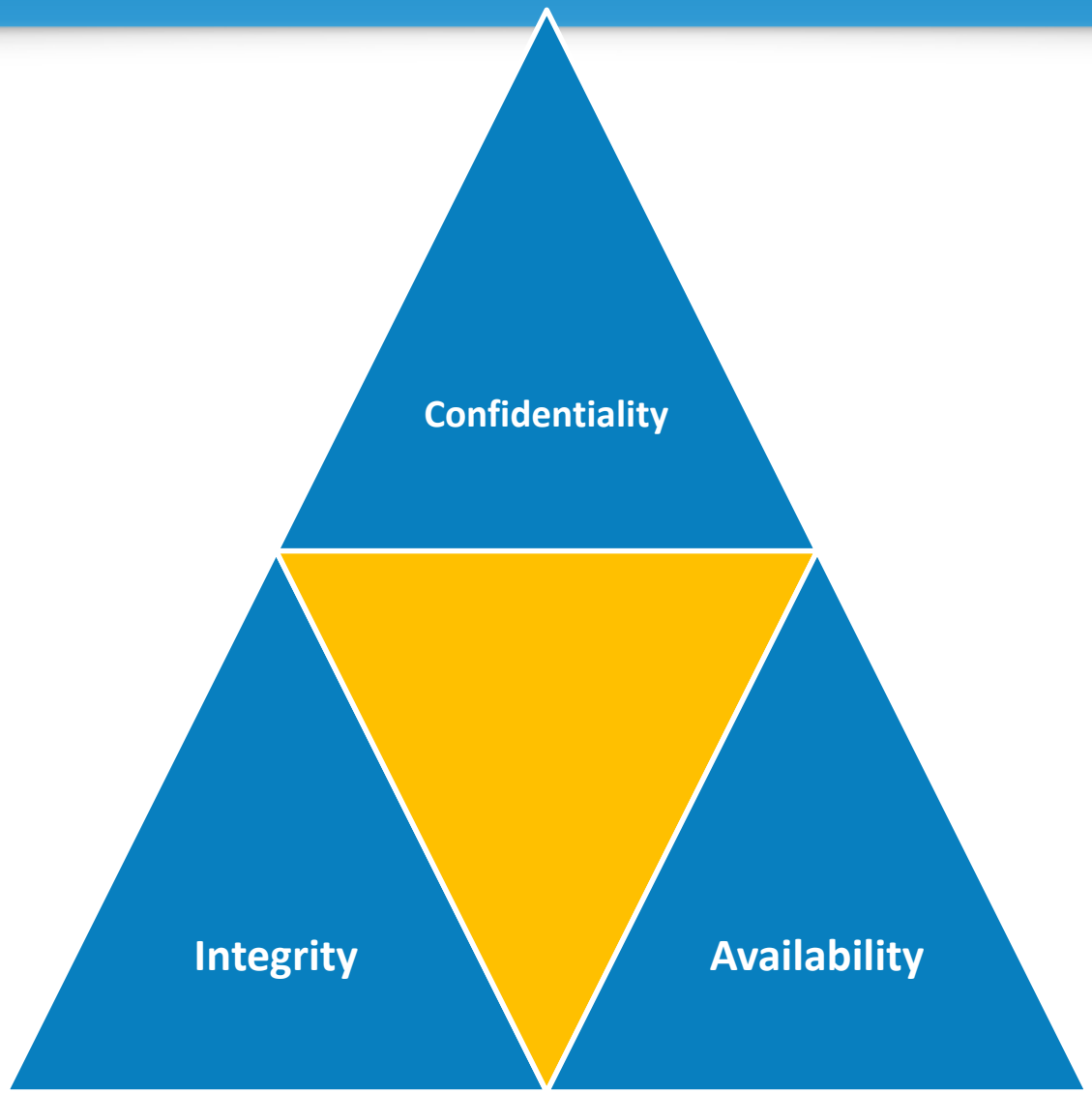
Table of Contents

- Common Language Framework
- Current Situation for Airworthiness
- Tomorrow for Products
- Security Risk Assessment
- Specifics for STCs
- The day after tomorrow for Organisations
- Reality Check

Common Language Framework

credit Markus Spiske on Unsplash

Common Language Framework: the ***CIA***!



Terminology: The notion of “intent”

SAFETY

Fate

SECURITY

Intent

Current Situation for Airworthiness

✈ ***Special Condition:***

Information Security Protection of Aircraft Systems and Networks

Requires the manufacturer to define and assess the cyber risk on the A/C design, when needed, to mitigate and to maintain the risk to an acceptable level during operation!

What the future entails…

- RMT.0648 : PRODUCTS!
- RMT.0720: ORGANISATIONS!

Tomorrow for Products

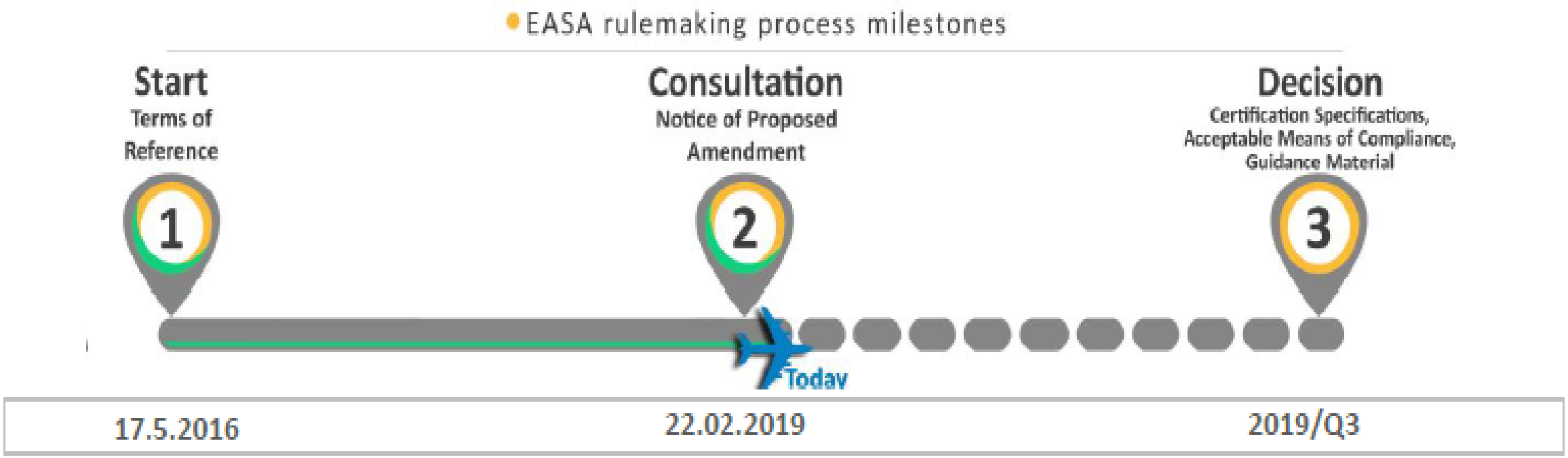
RMT. 0648: is aiming at

- including generic cybersecurity requirements in CS 23, CS 25, CS 27, CS 29, CS E, CS ETSO, CS P, amending AMC 20 and adding AMC 20-42
- Taking into account the interdependencies between aviation safety and security

Note:

- Existing special condition and recommendations from the ASISP ARAC group have been taken into consideration.

Milestones with respect to RMT. 0648



NPA under public consultation

When???

Deadline for comments: **Wednesday 22nd of May 2019**

Where???

http://hub.easa.europa.eu/crt/

To the point….

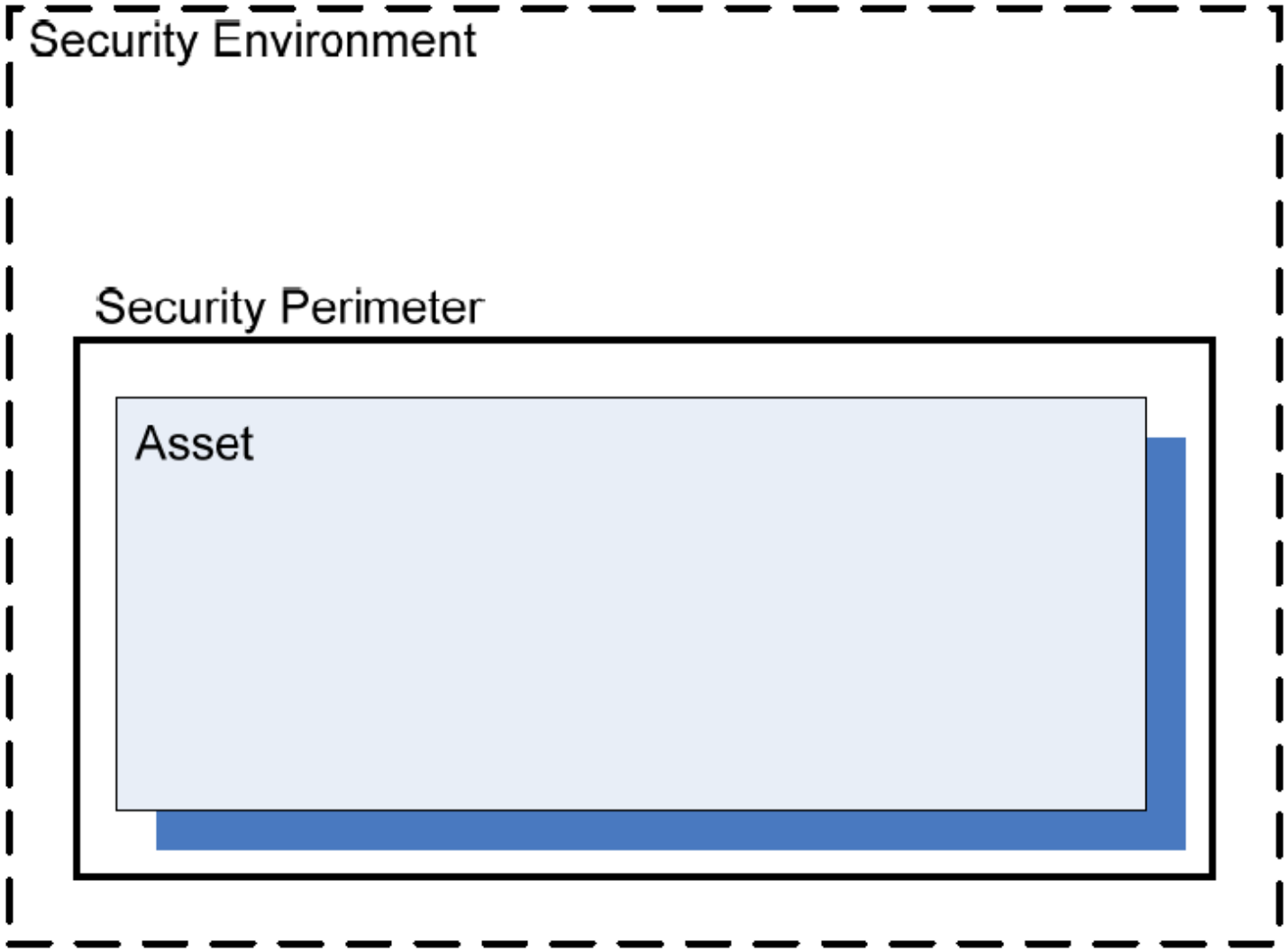
- The provisions require that an applicant shows that he/she **has <u>identified, assessed and mitigated</u>** the possible security risks as necessary.
- The provisions require that the applicant makes procedures and instructions for continued airworthiness (ICA) available to ensure that the security protections of the
  - aeroplane equipment, systems and networks
  - rotorcraft equipment, systems and networks
  - engine controls
  - propeller control systems

  <u>are maintained.</u>

AMC 20-42

- New material just for cybersecurity explaining how to comply with CSs above.
- The applicant may consider AMC 20-42, which provides acceptable means, guidance and methods to perform security risk assessments and mitigation for aircraft information systems.
- EUROCAE & RTCA Standards are recognised and integrated.
- PISRA : Product information Security Risk Assessment

Security Scope



Cyber Security Risk Assessment

Purpose is to evaluate the security risk of an aircraft or system subject to unauthorized interference with its systems

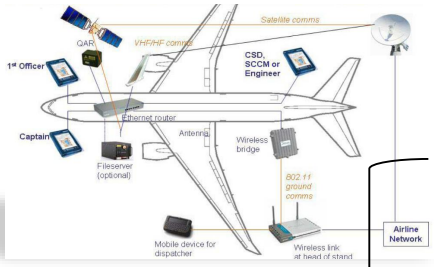
Risk is defined by

1. **Severity of the Threat Condition**
2. **Level of Threat**

Risk = Severity *Level of Threat

Src ED 202A

Case study: Air Mgt. Syst.



Functions

- Provide Cabin Pressurization
- Provide Aircraft Structural Integrity
- Provide Aircraft status
- Troubleshooting Support

Assets

- Field Loadable S/W
  ...
- Configuration files
  ...

Interfaces

- Physical I/F
- Logical I/F

Security scope

Failure conditions

	Failures	Attribute	Flight Phase	Hazzard Classification
F1	Loss of Pressurization	Availability	Airborne	Catastrophic
F2	Loss of Structural Integrity	Availability	Airborne	Catastrophic
F3	Loss of Aircraft status	Availability	Airborne	Major
F4	Loss of Troubleshooting Support	Availability	On Ground	No safety effect

Threat conditions

	Threat Condition	Attribute	Flight Phase	Failure	Hazzard Classification
TC1	Air Management System unresponsive due to malware infection	Availability	Airborne	F1	Catastrophic
TC2	Inter-system Communication interrupted due to malware infection	Availability	On Ground	F1	No safety effect
TC3	Counterfeit LRU installation	Integrity	Airborne	F1	Catastrophic
TC4	Misleading commands to bleed due to S/W corruption	Integrity	Airborne	F1	Catastrophic

Determining the level of threat

- effectiveness of the security protection
  - The more difficult it is, the less likely
    - Preparation means
    - Execution means
    - Window of opportunity

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					

Risk acceptability

safety

Risk Level	SEVERITY				
PROBABILITY (Likelihood)	No Effect	Minor	Major	Hazardous	Catastrophic
Frequent					
Probable					
Remote					
Extremely Remote					
Extremely Improbable					

security

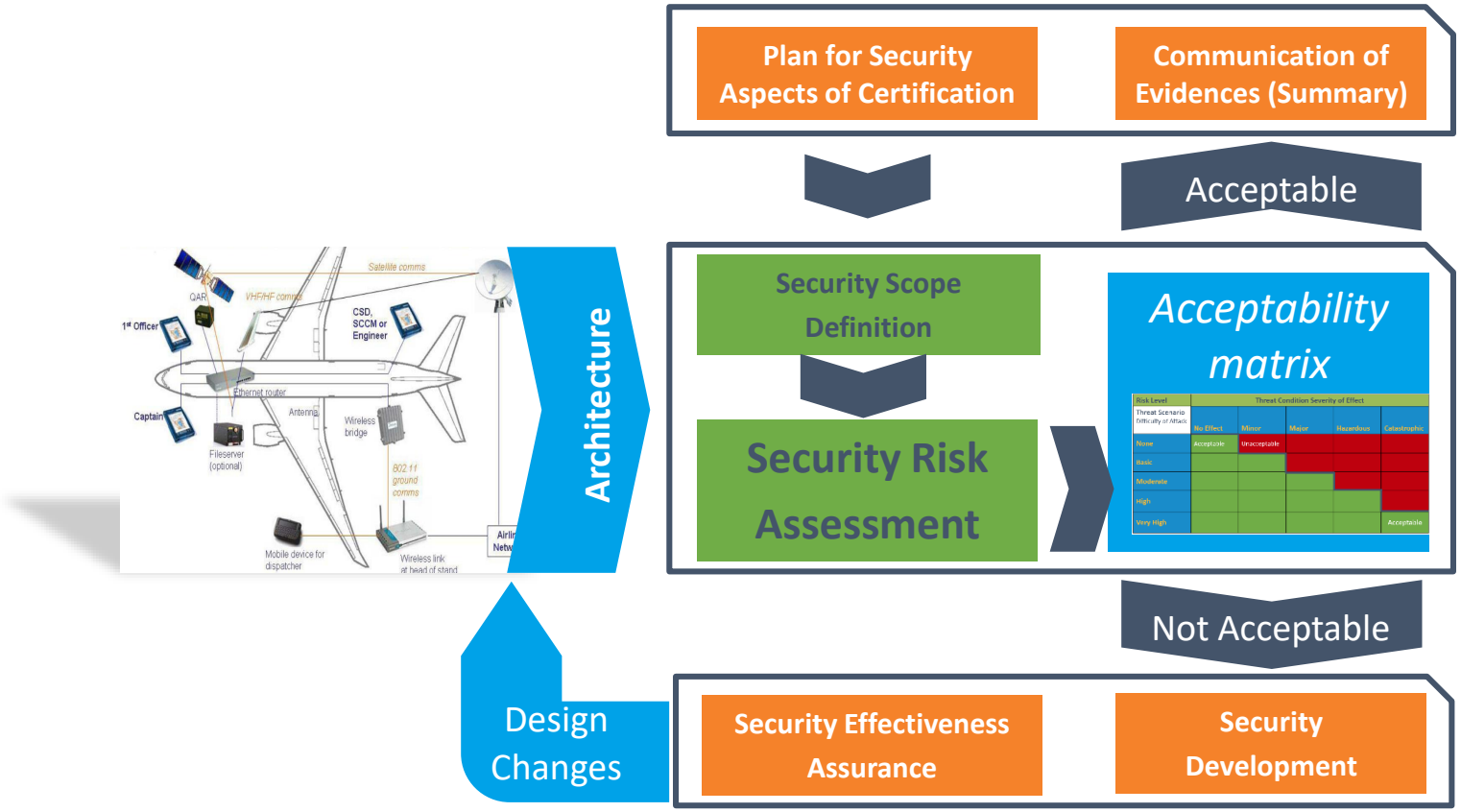
Severity / hreat	No effect	Minor	Major	Hazardous	Catastrophic
ery High					
High					
oderate					
Low					

Needs to modify the architecture to reduce the severity

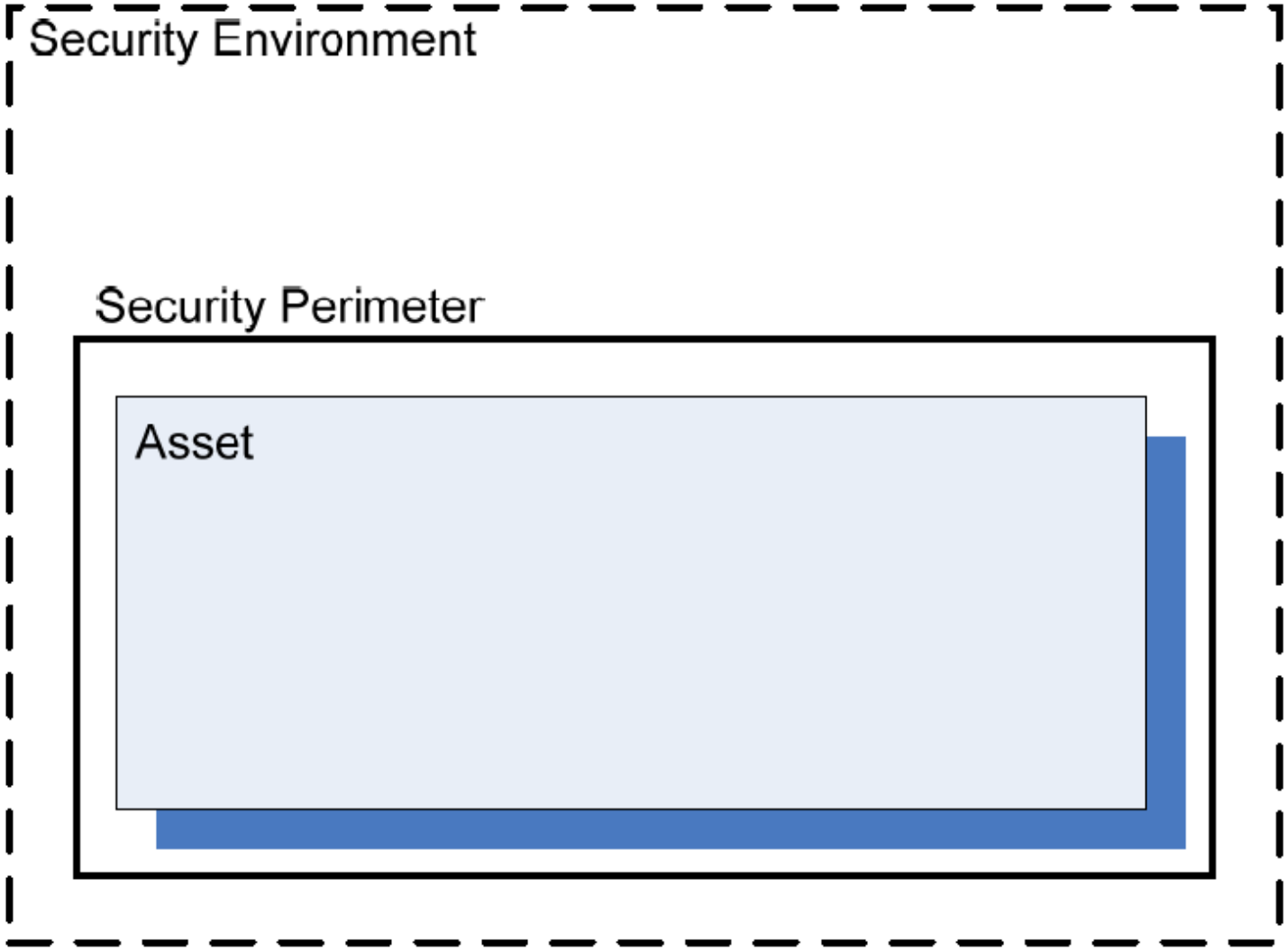
So better think security from start!

Make the scenario more difficult to succeed: add protection (eg signing sw load), or operational constraints (eg. access to the aircraft vs remote loading)

Risk Acceptability Process



Security Scope …remember??



Specifically for STCs

STC applicant justifies that the change remains outside the security perimeter.

STC applicant needs to justify that the new system/function is completely isolated from the a/c systems.

OEM involved

The STC applicant should provide evidence using an acceptable process that the a/c security level is or remains acceptable when embodying the change,

Without OEM involvement

The STC applicant needs to justify the a/c systems are protected via a security risk assessment to be approved by the relevant airworthiness authority.

Part 21.A.113

(b) …information on which those identifications are based is adequate either from the applicant's own resources, or through an arrangement with the TC holder.

Part 21.A.115

1.the type-certificate holder has advised that it has no technical objection to the information submitted under point 21.A.93; and

2. the type-certificate holder has agreed to collaborate with the supplemental type certificate holder to ensure discharge of all obligations for continued airworthiness of the changed product

The day after tomorrow for Organisations

RMT. 0720: is aiming at

- Introducing provisions for the management of information security in all the aviation domains, including design, production, continuing airworthiness management etc.
- These provisions include high-level performance-based requirements.
- The NPA is the result of the cooperation with the ESCP.

Milestones with respect to RMT. 0720

To the point….

- Organisation Requirements
  - Personnel requirements
  - Information Security Management System
  - Establishment of internal information security reporting scheme
  - Establishment of external information security reporting scheme
  - Contracted Activities
  - Record-keeping

How to maintain security – Reality Check

NIST - NVD

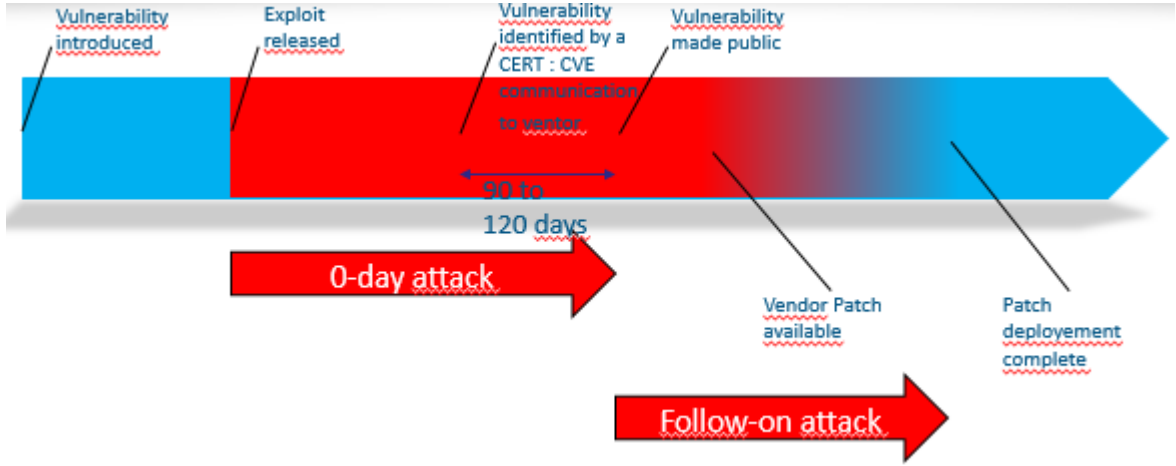
Common Vulnerabilities and Exposures is a list of entries for **publicly** known cybersecurity vulnerabilities.

Let's have a look…

https://nvd.nist.gov

116.158 entries ☹

Zero Day – Rand Corporation



6,9 years average ☹

EASA
European Union Aviation Safety Agency

Thank you for your attention!
Questions?

Contact:
cyrille.rosay@easa.europa.eu
angeliki.karakoliou@easa.europa.eu

Your safety is our mission.

An Agency of the European Union