



**EASA**  
European Aviation Safety Agency

# **Product Certification and Design Organisation Approval Workshop**

**22<sup>nd</sup> -23<sup>rd</sup> November 2016**

**Your safety is our mission.**

An agency of the European Union 

TE.GEN.00409-001



**EASA**  
European Aviation Safety Agency

# Cyber Security

**Cyrille Rosay**  
**Senior Expert Cyber Security**

**23rd November 2016**

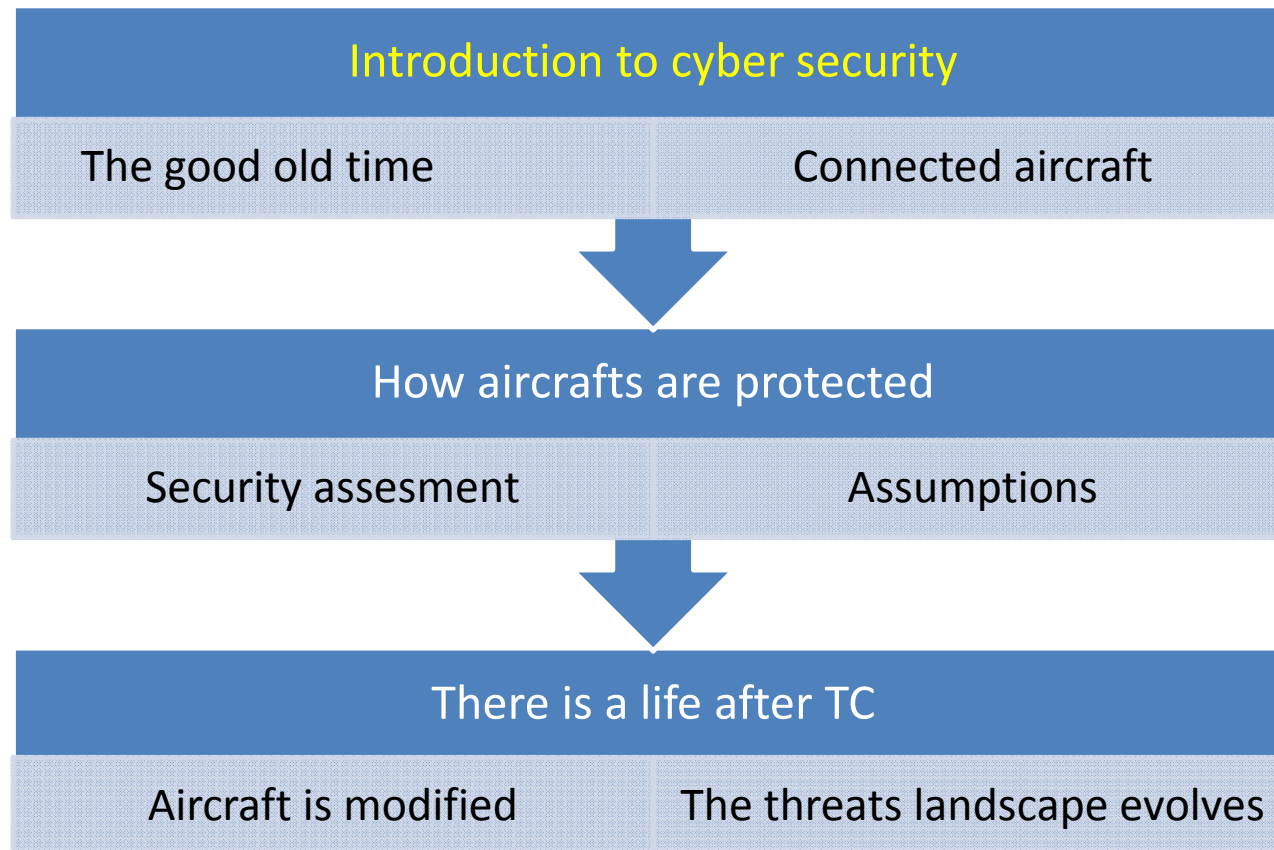
**Your safety is our mission.**

An agency of the European Union 

TE.GEN.00409-001



# Presentation Overview





# Introduction to Cyber Security



## Cyberspace

## Cyber security

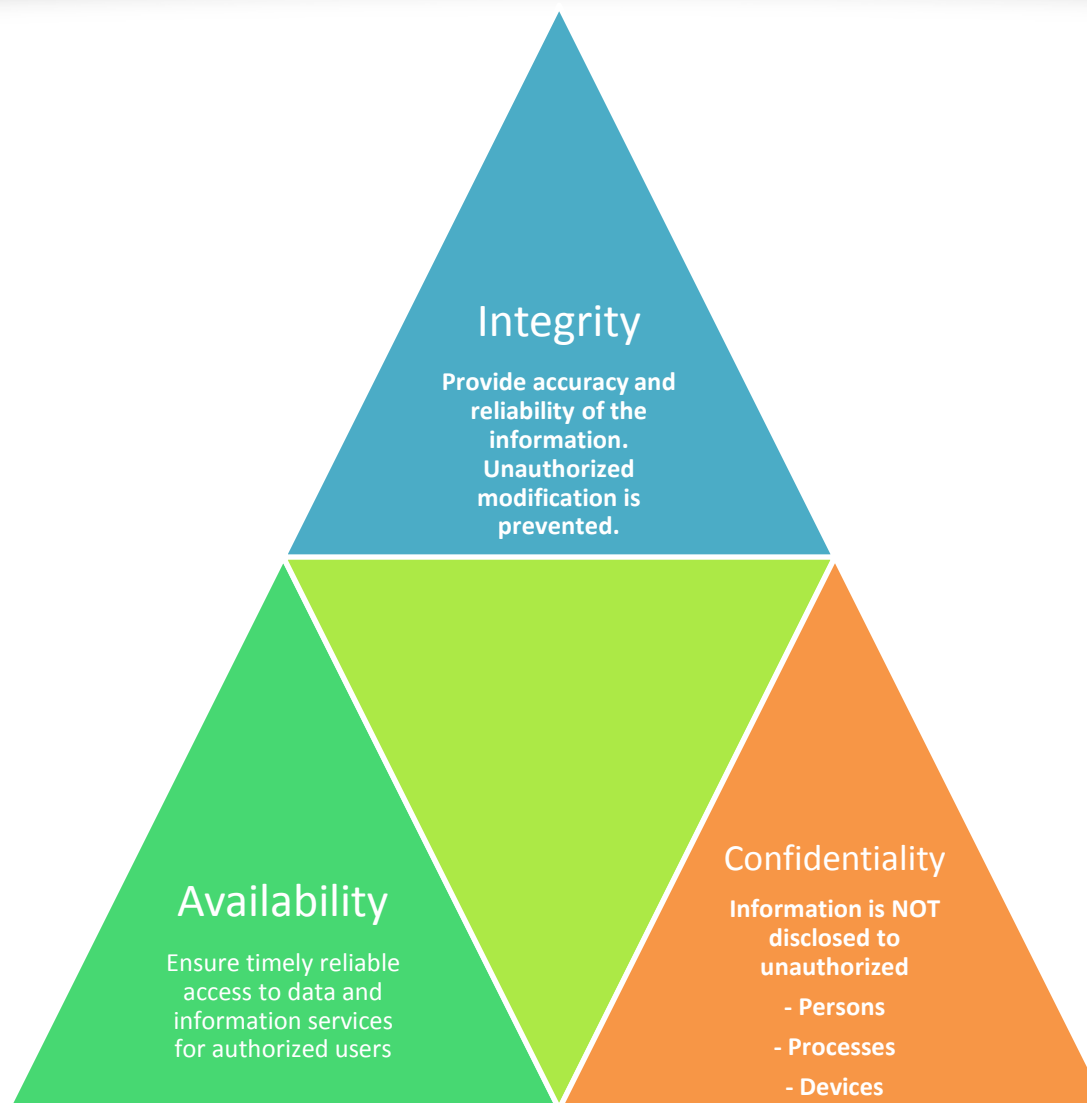
The ability to protect or defend the use of cyberspace from cyber attacks

A **global domain** within the **information environment** consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.





# Introduction to cyber security





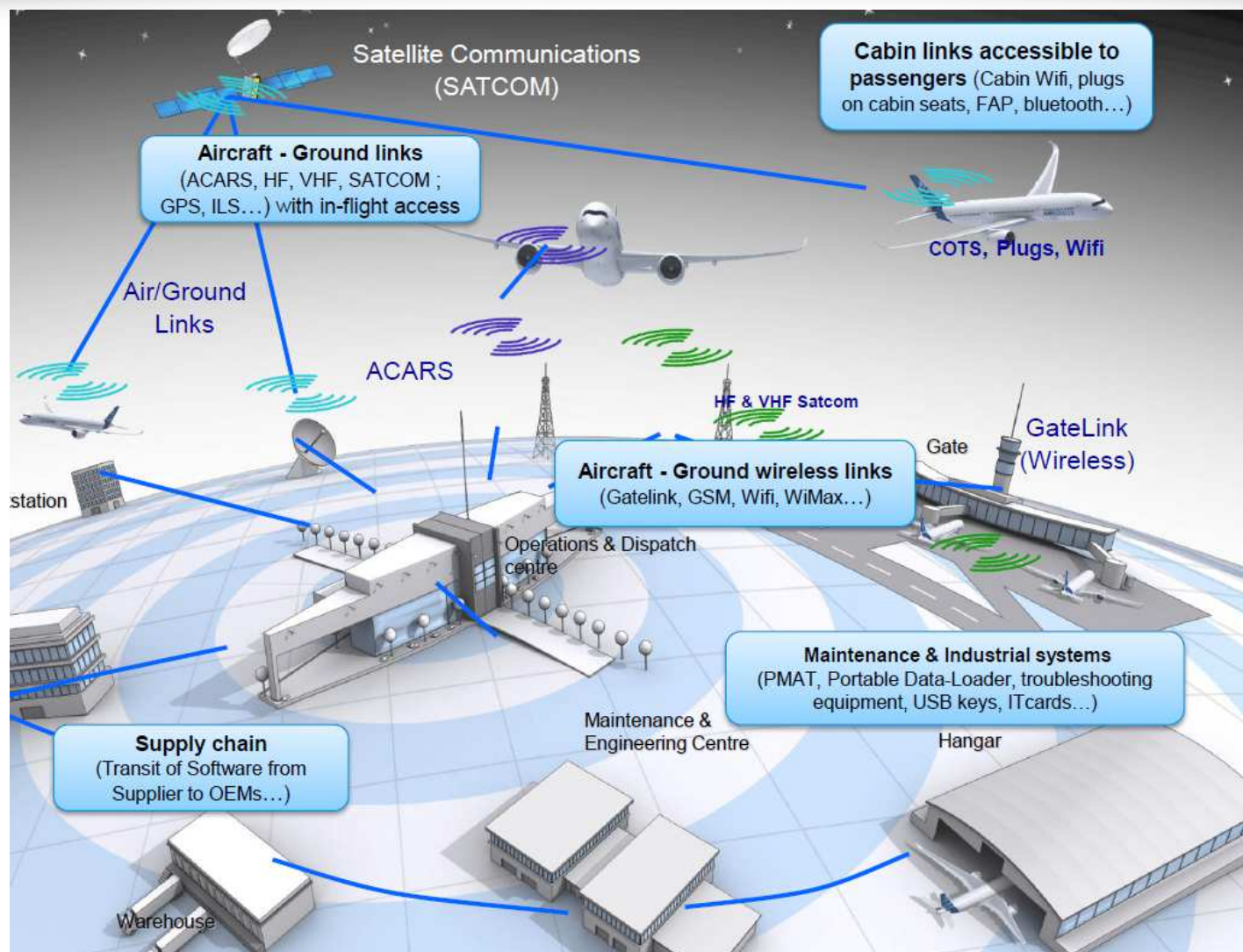
# The good old days







# Today



courtesy Airbus



# (bad) Example

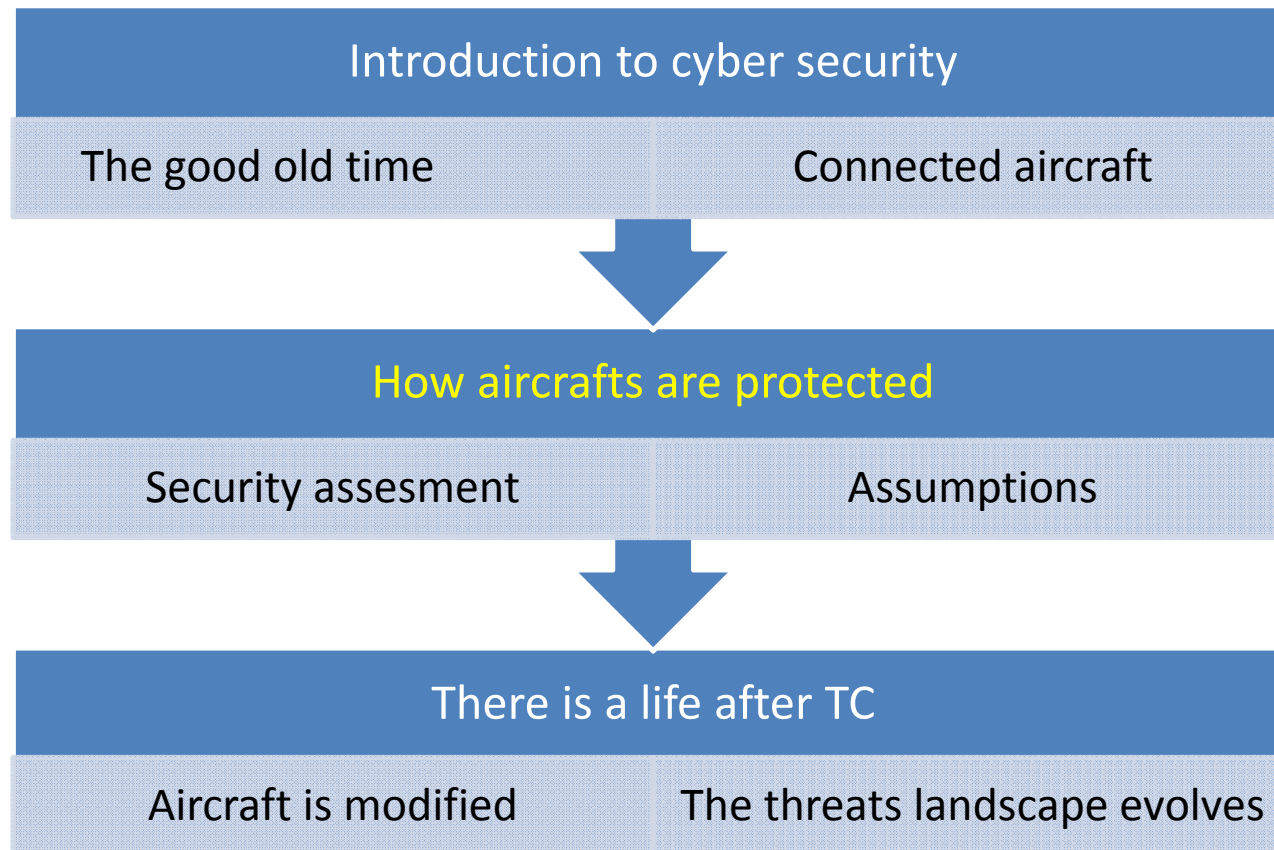
- It can take 5 min for a hacker to steal operator password (X-script on portal)
- Social engineering also possible
- With it he get access to the whole airline fleet anywhere in the world, on the ground or airborne.
- He can send data directly to the plane (AOC)







# Presentation Overview





# Initial Airworthiness

## Large A/C

Today, Special condition

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.

Tomorrow in CS-25

Rulemaking task 0648 started. ToR published (17/05/2016)

Standards and AMCs

Objective is to recognize and reference the industry standards (EUROCAE).

Issue to be solve by the industry on difference between RTCA and EUROCAE

## General Aviation

Low end: nothing asked.  
Industry voluntary basis

GAMA GA initiative to address cyber security in GA is well perceived by EASA.

Candidate for an ASTM standard in F44?

PAX > 19

Today case by case basis. Asking usually via a CAI (Certification Action Item) to review the design with the cyber security scope. Sometime followed by a SC.



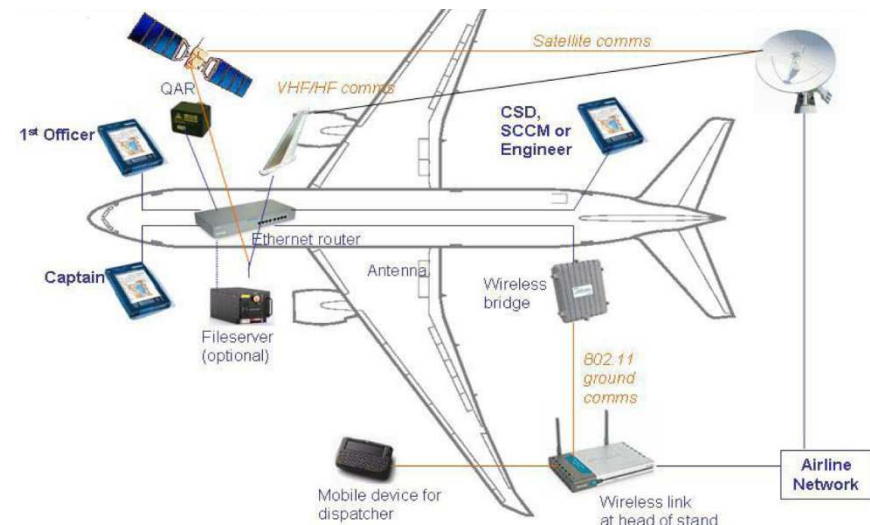
# Cyber Security Risk Assessment

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 effect of the Threat Condition**
2. **Difficulty to attack**

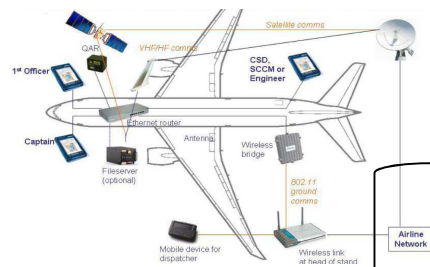
**Risk = Severity / Difficulty**



Src ED 202A



# Case study: Air Mgt. Syst. (src ED 203)



Security scope

## Functions

Provide Cabin Pressurization

Provide Aircraft Structural Integrity

Provide Aircraft status

Troubleshooting Support

## Assets

Press. Contr.  
Field Loadable S/W

Press. Contr. Configuration files

## Interfaces

Physical I/F to Maintenance GSE

Logical I/F to Bleed System

## Failure conditions

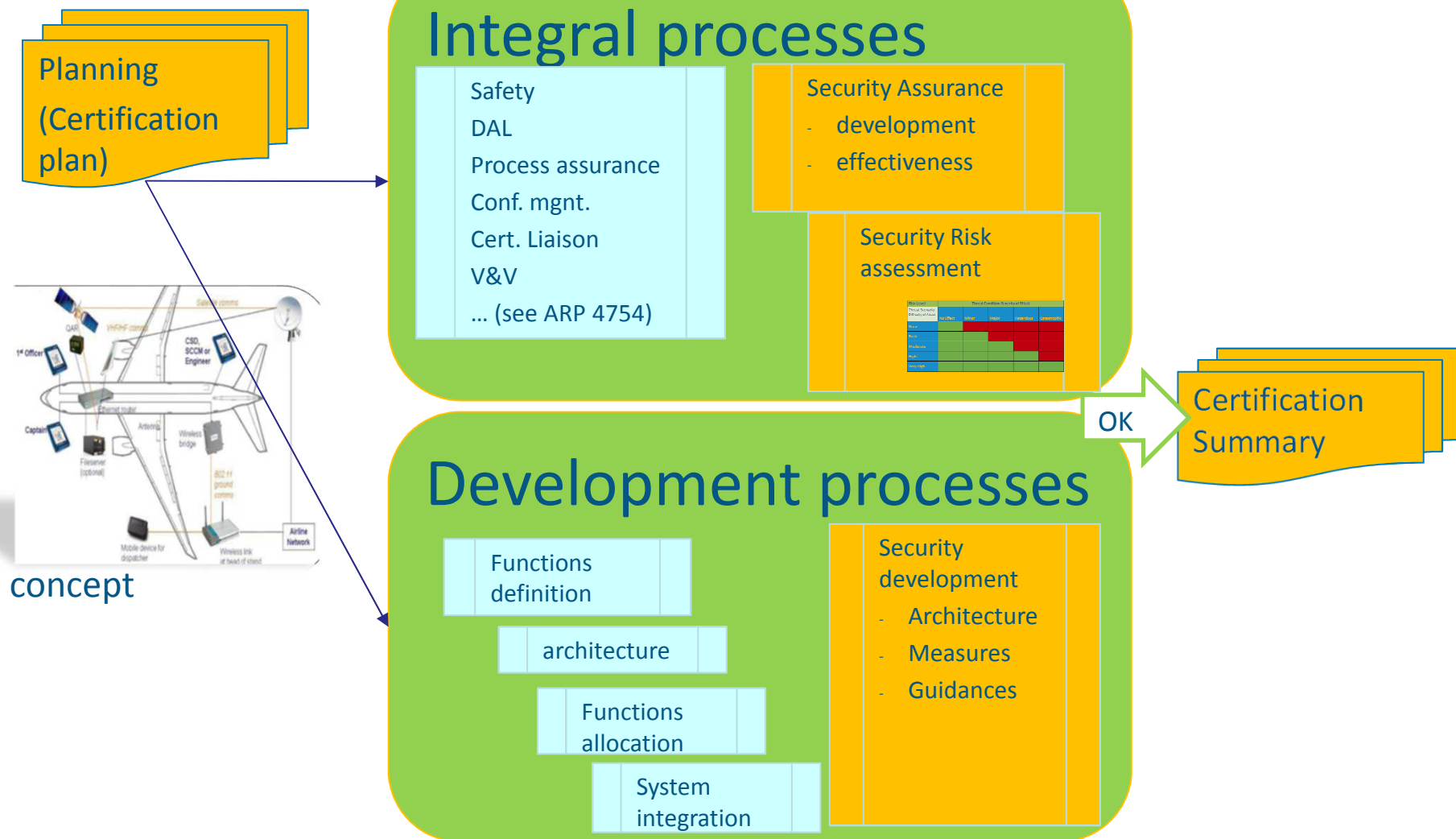
|    | Failures                        | Attribute    | Flight Phase | Hazzard Classification |
|----|---------------------------------|--------------|--------------|------------------------|
| F1 | Loss of Pressurization          | Availability | Airborne     | Catastrophic           |
| F2 | Loss of 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 | Communication interrupted due to malware infection | Availability | Airborne     | F1      | Catastrophic           |
| TC2 | 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           |



# General process (ED 202)





# Risk Acceptability Matrix

## safety

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

## security

Needs to modify the architecture to reduce the safety impact  
So better think security from start!

| Risk Level                           | Threat Condition Severity of Effect |       |       |           |              |
|--------------------------------------|-------------------------------------|-------|-------|-----------|--------------|
| Threat Scenario Difficulty of Attack | No Effect                           | Minor | Major | Hazardous | Catastrophic |
| None                                 |                                     |       |       |           |              |
| Basic                                |                                     |       |       |           |              |
| Moderate                             |                                     |       |       |           |              |
| High                                 |                                     |       |       |           |              |



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





•SAFETY



•VS

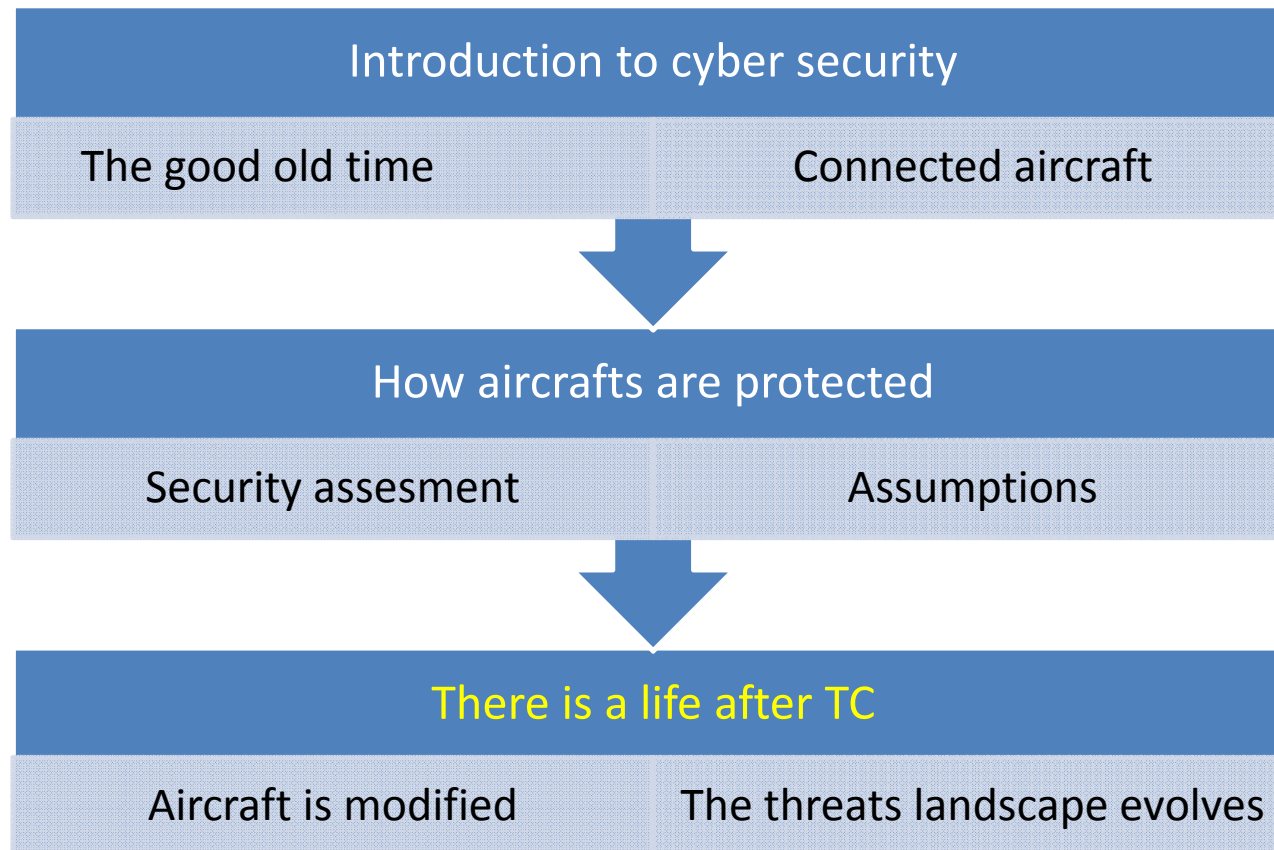
•SECURITY



•The notion of  
**INTENT**



# Presentation Overview

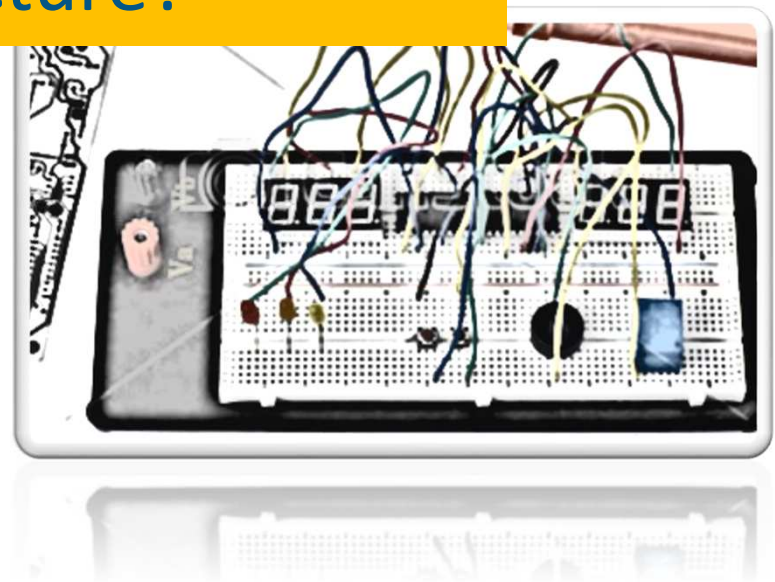




# Aircraft modification

Issue:

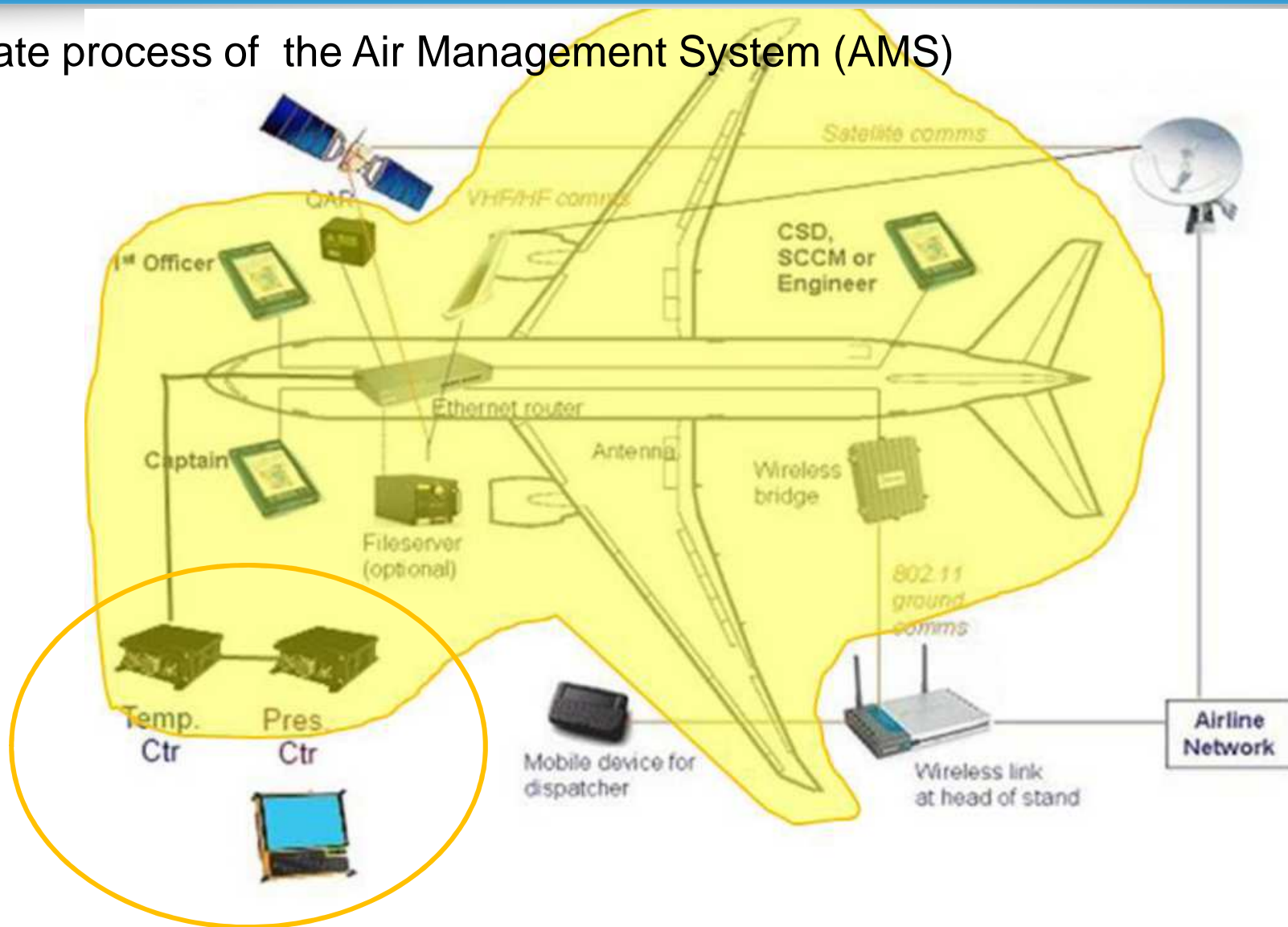
How can we maintain the security effectiveness when modification are made on existing architecture?





# Case study

update process of the Air Management System (AMS)





# What does the rule say?

## **21.A.113 Application for a supplemental type-certificate**

(a) An application for a supplemental type-certificate shall be made in a form and manner established by the Agency.

(b) An application for a supplemental type-certificate shall include the descriptions and identification, and changes to the operational suitability data required by point 21.A.93. In addition, such an application shall include a justification that the information on which those identifications are based is adequate either from the applicant's own resources, or through an arrangement with the type-certificate holder.



# How?

- security boundaries are available
  - Should allow modification without jeopardizing existing A/C security efficiency
- STC applicant get from OEM the necessary security information to perform the change, including operational security handbook and ICA
  - Implies some binding constraints between OEM and STC applicant





# Potential Issues

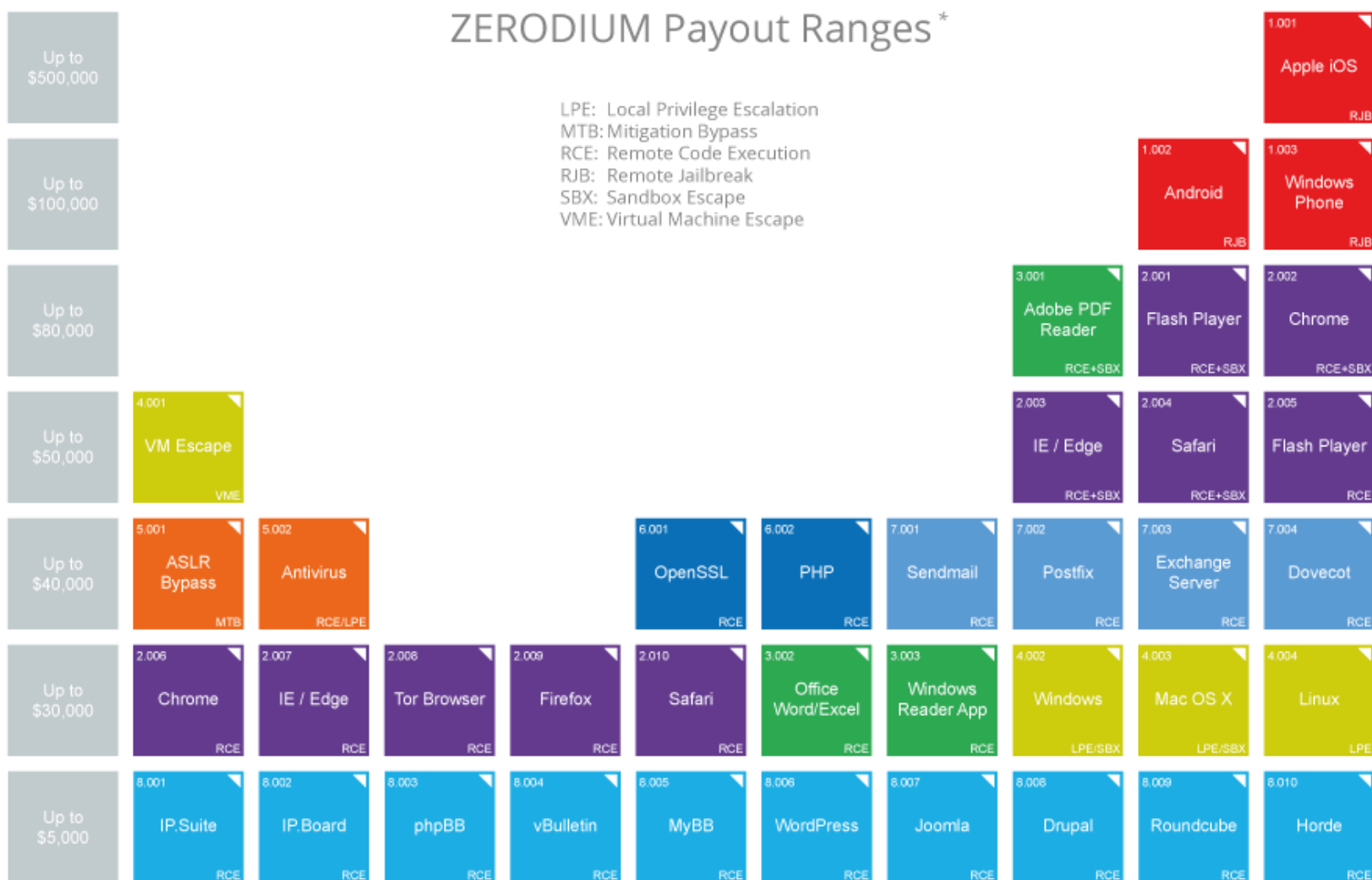
- DOA experienced CVEs and experts
- Capacity to tackle risk evolution
- Control of the supply chain



# Risk evolution

## ZERODIUM Payout Ranges\*

LPE: Local Privilege Escalation  
MTB: Mitigation Bypass  
RCE: Remote Code Execution  
RJB: Remote Jailbreak  
SBX: Sandbox Escape  
VME: Virtual Machine Escape



\* All payout amounts are chosen at the discretion of ZERODIUM and are subject to change or cancellation without notice.

2015/11 © zerodium.com



# DW marketplace

 How to buy exploit? Two ways to buy required exploit. Currency, that we accept.

1. Anonymous buying of exploits is the way to buy exploit without registration. You buy it directly and anonymous and get exploit on mail.

2. Another way to buy exploits is to became Oday.today 1337day user, get Oday.today 1337day Gold  and buy required exploit in our database.

We accept currencies: [\[contact admin to find more\]](#)




























[Extended search](#)

### Oday Today Exploit Market and Oday Exploits Database

[ private ]

| DATE       | DESCRIPTION  | TYPE    | HITS   | RISK  | GOLD  | AUTHOR          |
|------------|--|---------|--------|---|---|-----------------|
| 27-08-2016 | Twitter reset account Private Method Oday Exploit            | tricks  | 6 789  |  |  2 300 | Oday Today Team |
| 24-07-2015 | Instagram bypass Access Account Private Method Exploit       | tricks  | 6 591  |  |  2 000 | smokzz          |
| 24-11-2015 | SMF 2.1 Beta 2 Remote Code Execution Oday Exploit            | php     | 1 808  |  |  3 500 | Protocol.S      |
| 06-02-2015 | SMF 2.0.x Remote Code Execution Oday Exploit                 | php     | 11 919 |  |  5 000 | Protocol.S      |
| 20-10-2016 | WhatsApp Android text Crash Oday Exploit                     | Android | 1 241  |  |  2 000 | jackedbypapuh   |
| 27-08-2016 | Twitter reset account Private Method Oday Exploit            | tricks  | 6 789  |  |  2 300 | Oday Today Team |
| 29-11-2015 | Schoolbook purchased e-books on .pdf format Download Exploit | tricks  | 1 225  |  |  100   | MrUke           |
| 24-11-2015 | SMF 2.1 Beta 2 Remote Code Execution Oday Exploit            | php     | 1 808  |  |  3 500 | Protocol.S      |

[ remote exploits ]

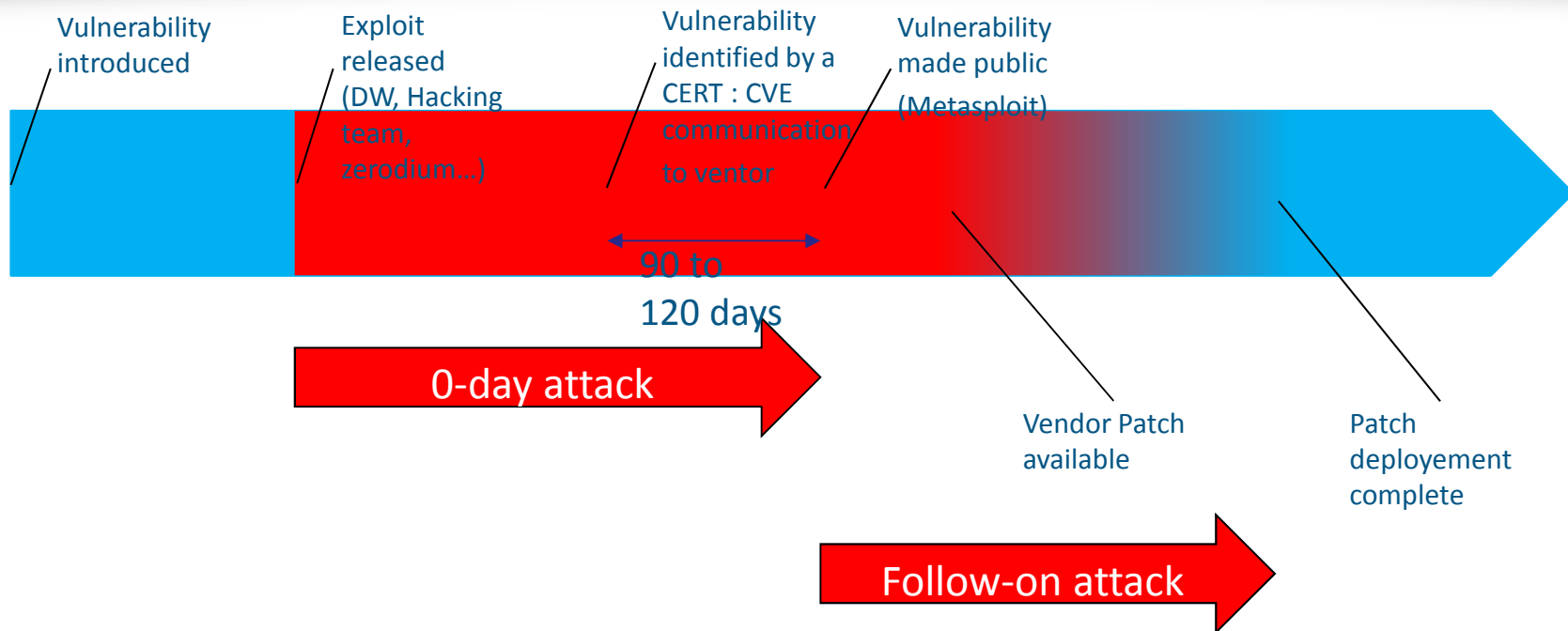
| DATE       | DESCRIPTION  | TYPE     | HITS  | RISK  | GOLD  | AUTHOR         |
|------------|--|----------|-------|---|---|----------------|
| 20-10-2016 | WhatsApp Android text Crash Oday Exploit                             | Android  | 1 241 |  |  2 000 | jackedbypapuh  |
| 20-10-2016 | WineBottler 1.8-rc4 Man-In-The-Middle / Code Execution Vulnerability | multiple | 393   |  | free  | Florian Begner |
| 19-10-2016 | Hak5 WiFi Pineapple Preconfiguration Command Injection 2             | hardware | 484   |  | free  | metasploit     |
| 19-10-2016 | Hak5 WiFi Pineapple Preconfiguration Command Injection Exploit       | hardware | 370   |  | free  | calatonicprime |
| 19-10-2016 | OpenNMS Java Object Unserialization Remote Code Execution            | java     | 312   |  | free  | metasploit     |
| 18-10-2016 | Metasploit Web UI Static secret_key_base Value Exploit               | multiple | 396   |  | free  | metasploit     |
| 18-10-2016 | PHP 5.6.26 and 7.0.11 Use After Free in unserialize() Vulnerability  | php      | 427   |  | free  | taoguangchen   |
| 15-10-2016 | Ruby on Rails Dynamic Render File Upload Remote Code Execution       | ruby     | 250   |  | free  | metasploit     |

[ local exploits ]

| DATE       | DESCRIPTION  | TYPE    | HITS | RISK  | GOLD | AUTHOR    |
|------------|--|---------|------|---|------|-----------|
| 20-10-2016 | Oracle Netbeans IDE 8.1 Directory Traversal Vulnerability                          | php     | 194  |  | free | hyp3rlinx |
| 20-10-2016 | Realtek High Definition Audio Driver 6.0.1.6730 Privilege Escalation Vulnerability | windows | 180  |  | free | Joey Lane |
| 20-10-2016 | PDF Complete 4.1.12 Corporate Edition Privilege Escalation Vulnerability           | windows | 144  |  | free | Joey Lane |
| 20-10-2016 | Vembu StoreGrid 4.0 Privilege Escalation Vulnerability                             | windows | 109  |  | free | Joey Lane |
| 20-10-2016 | BitComet 1.43 Privilege Escalation Vulnerability                                   | windows | 127  |  | free | Amir.ght  |
| 20-10-2016 | Wise Boot Assistant 4.28.416 Privilege Escalation Vulnerability                    | windows | 103  |  | free | Amir.ght  |
| 20-10-2016 | SpyHunter 4.23.2 Privilege Escalation Vulnerability                                | php     | 97   |  | free | Amir.ght  |
| 20-10-2016 | Lenovo Slim USB Keyboard 1.09 Privilege Escalation Vulnerability                   | windows | 95   |  | free | Joey Lane |



# 0-day timeline

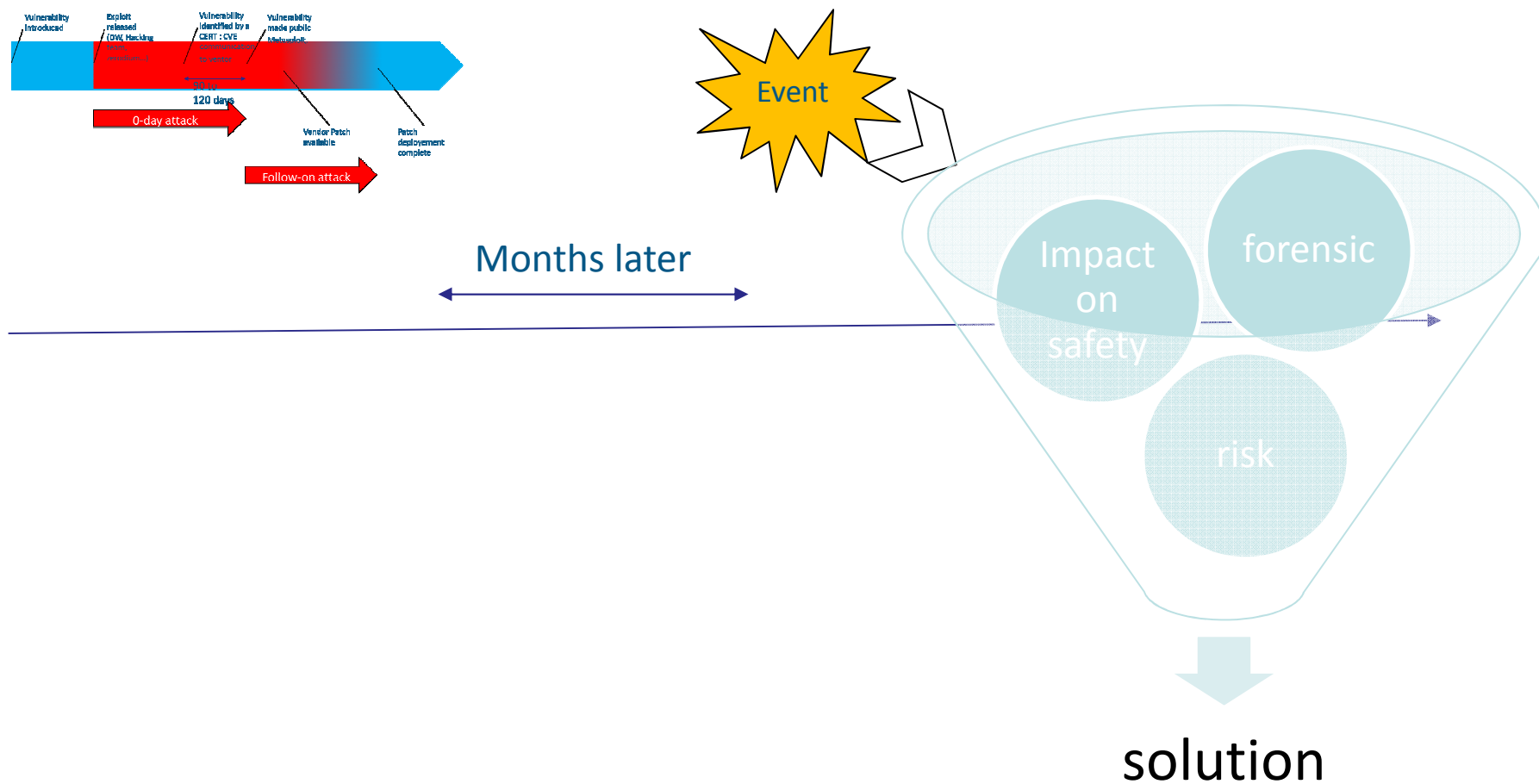


## Questions:

- who, in the aviation world is looking at vulnerabilities, CVEs, patches?
- Which vendors in the aviation world is developing security patch?
- What do you think of the timeline, in particular the follow-on attack window?



# 0-day timeline and the occurrence reporting





**EASA**  
European Aviation Safety Agency

# Questions?



**Your safety is our mission.**

An agency of the European Union 