EASA
European Union Aviation Safety Agency

Cologne, 19th June 2019

Cybersecurity impact on DOA Processes

Cyrille Rosay
Senior Expert – Cybersecurity
Davide Martini
Senior Expert – Cybersecurity
Angeliki Karakoliou
Junior Aviation Professional

Your safety is our mission.

An Agency of the European Union

FS 4.4 Cybersecurity & Emerging Risks

Davide Martini

Cyrille Rosay

Angeliki Karakoliou

Jean-Paul Moreaux

New Addition Start Date: 01/01/2020

Matthew Hilscher

Gerry Ngu

Juan Anton Bernalte

New Vacancy Notice EASA/AD/2019/012

Table of Contents

- Terminology
- Case study
- Regulatory (R)Evolution

ICAO

"…safety…"

EASA

"…between aviation safety, cybersecurity and…"

EUROCAE

"…safety…"

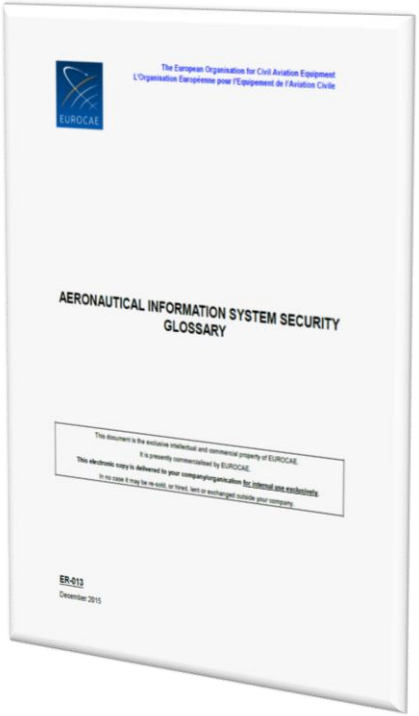
SAFETY

Fate

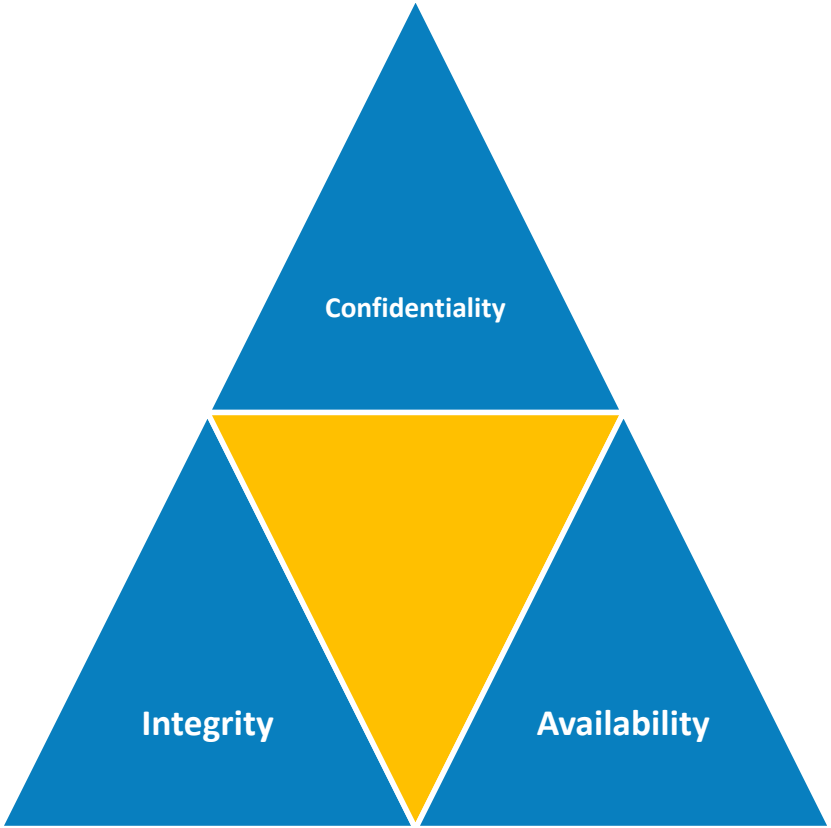
SECURITY

Intent

Terminology



Terminology: The CIA!



What is a vulnerability?

Threat or Failure Condition?

```
void receiveACARS(string msg) {
  char localCopy[128];
  strcpy(localCopy, msg);
  ...
}
```

STACK

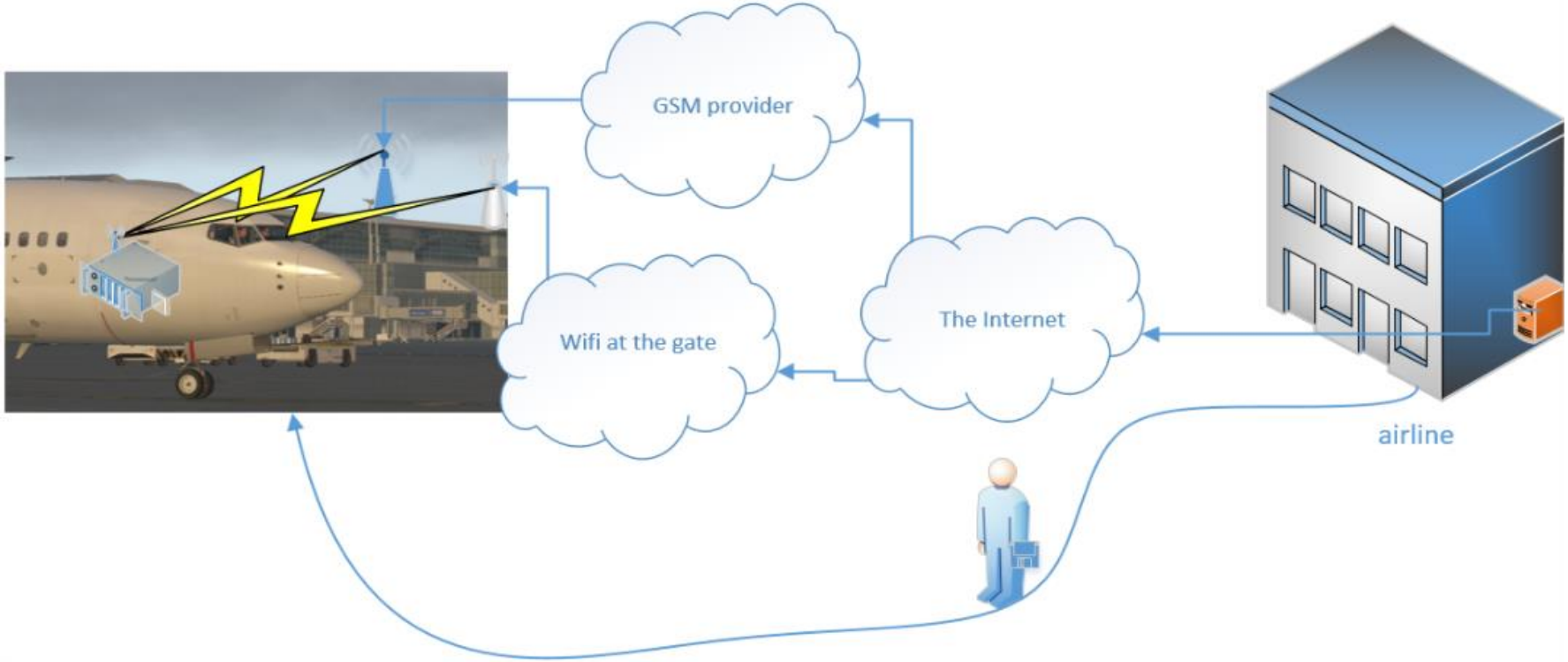
128 o space for message

OxACCARS_MESSAGE_THAT_COULD_ALSO_BE_EXECUTABLE_CODE+NOP+NOP+_

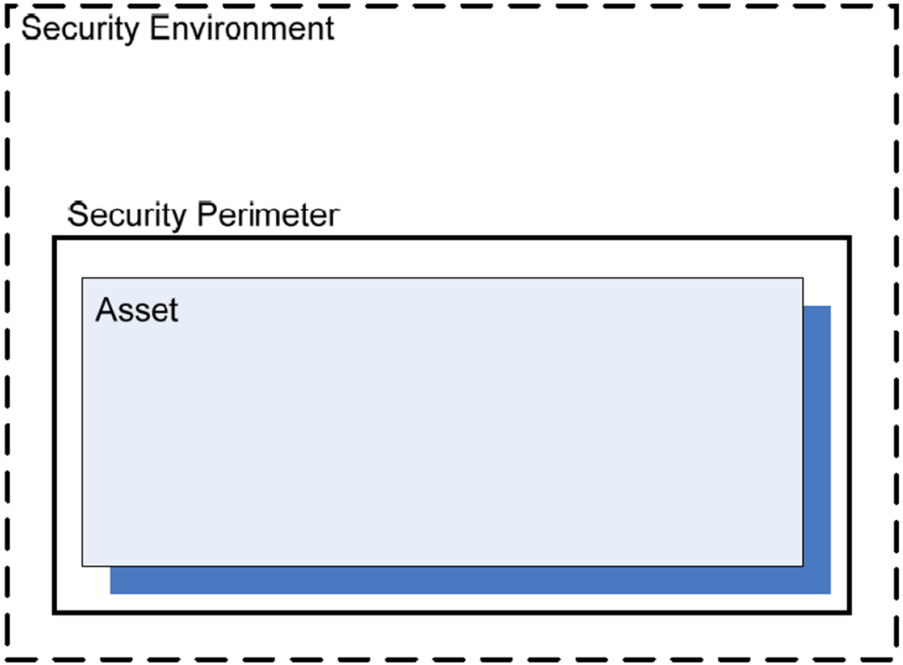
Return address

@_TO_START

Case Study: Remote Data Loader



Security Scope



Case study: Remote Data Loader

Security scope

Functions

- Acquisition and Transmission of FDAU Data
- FLS Upload
- Core SW Maintenance

Assets

- Dataloader
- FLS
- .....

Interfaces

- WiFI
- GSM
- SD Cards

Failure conditions

	Failures	Attribute	Flight Phase	Hazard Classification
F1	Loss of Acquisition	Availability	All	Minor
F2	Undetected Erroneous Activation	Integrity	Airborne	Major
F3	Undetected Errors in FDAU Data	Integrity	On Ground	Minor
F4	Loss of FLS Upload	Availability	On Ground	No safety effect
F5	Undetected Errors in installed FLS	Integrity	Airborne	Hazardous
F6	Loss of Maintenance	Availability	All	No Safety Effect

Threat conditions

	Threat Condition	Path	Attribute	Flight Phase	Failure	Hazard Classification
TC1	DOS	Wireless Communication	Availability	All	F1,F4	Minor
TC2	Remote Activation	Wireless Communication	Integrity	Airborne	F2	Major
TC3	Upload of an unauthorized FLS	Maintenance Laptop	Integrity	Airborne	F5	Hazardous
TC4	Upload of an unauthorized FLS	Wireless Communication	Integrity	Airborne	F5	Hazardous

Determining the level of threat

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

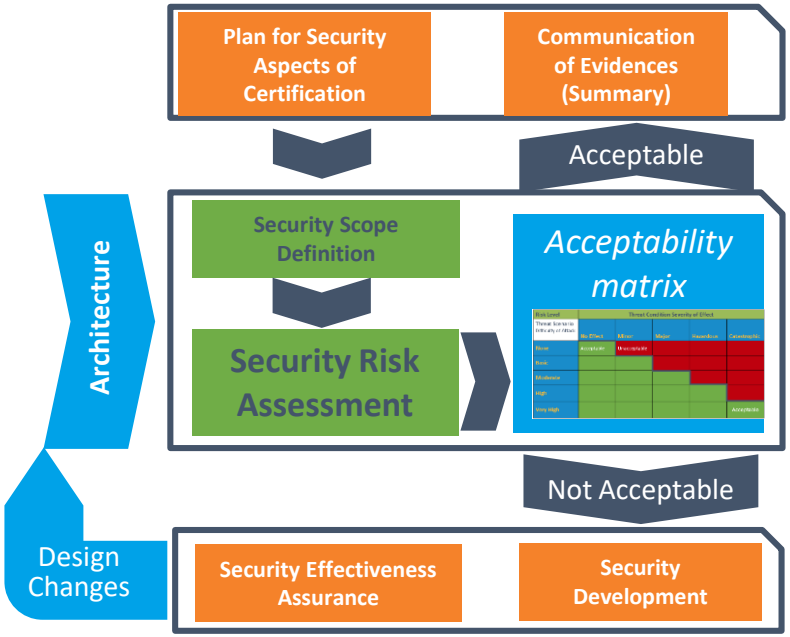
Safety

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

Security

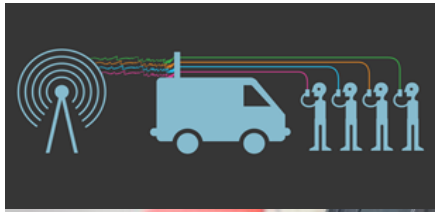
Severity / Level of Threat	No effect	Minor	Major	Hazardous	Catastrophic
Very High					
High					
Moderate					
Low					
Extremely Low					

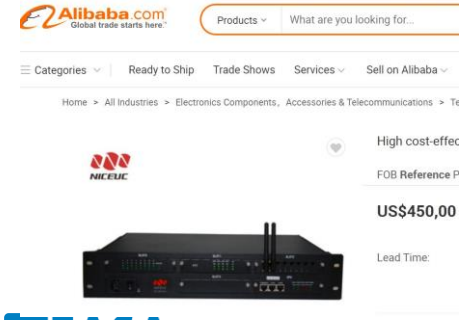
Risk Acceptability Procees



How long does it stay secure?

→ The fabulous case of the IMSI catcher





Before 2013
100K$

In 2016
20000$

2019
450$ on Ali Baba

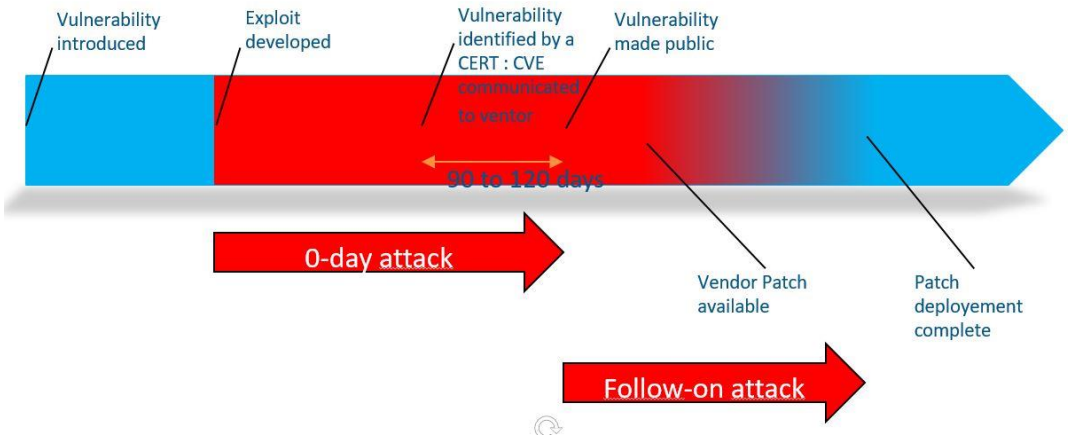
Knowledge / Equipment	None/Public Information and no preparation time	Uncontrolled Information and no significant preparation time	Insider Knowledge or Significant preparation time
None/Standard	0	2	6
Special COTS	0	2	6
Special	n/a	4	6
Bespoke	n/a	5	6

Expertise / Equipment	Layman	Proficient	Expert	Multiple Expert
None/Standard	0	4	6	10
Special COTS	4	4	6	10
Special	n/a	6	8	12
Bespoke	n/a	n/a	10	12

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

EASA

How to maintain security – Reality Check

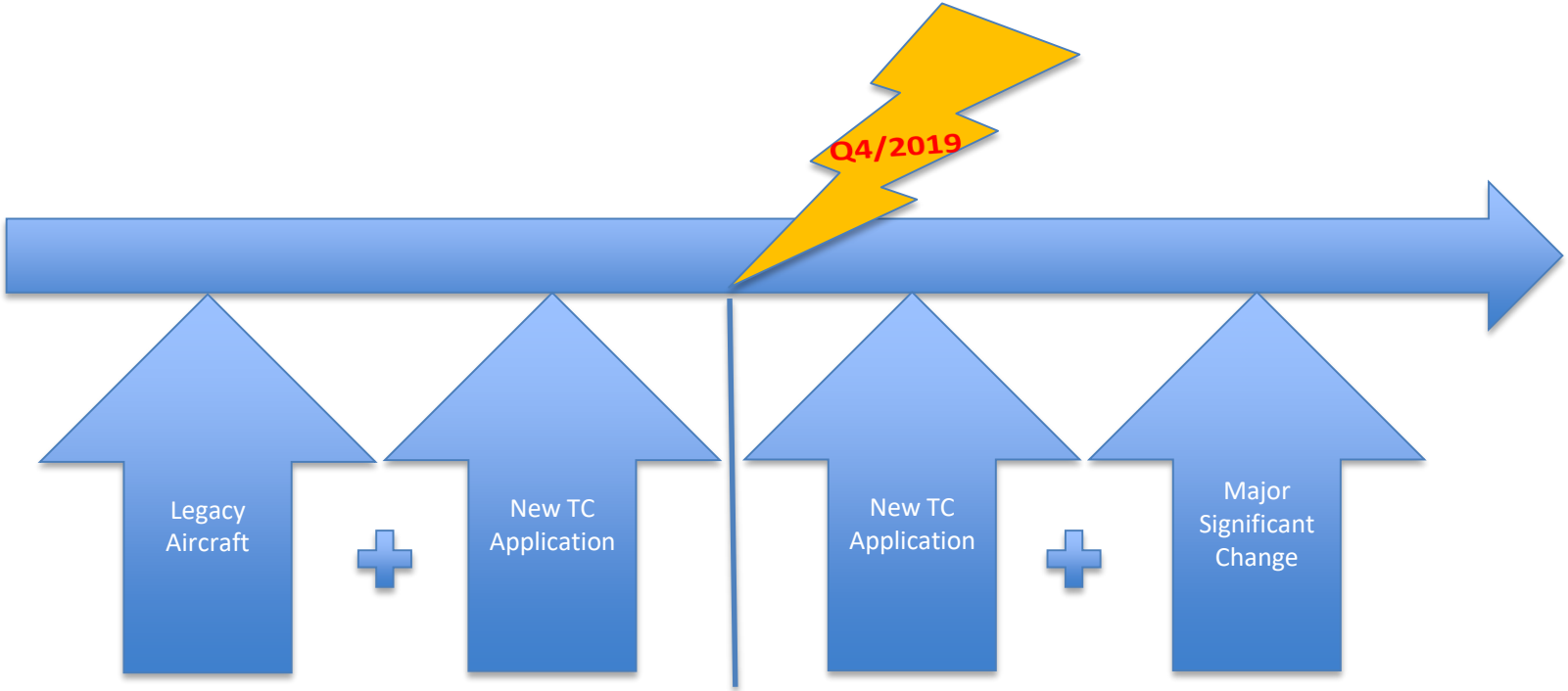


6,9 years average ☹

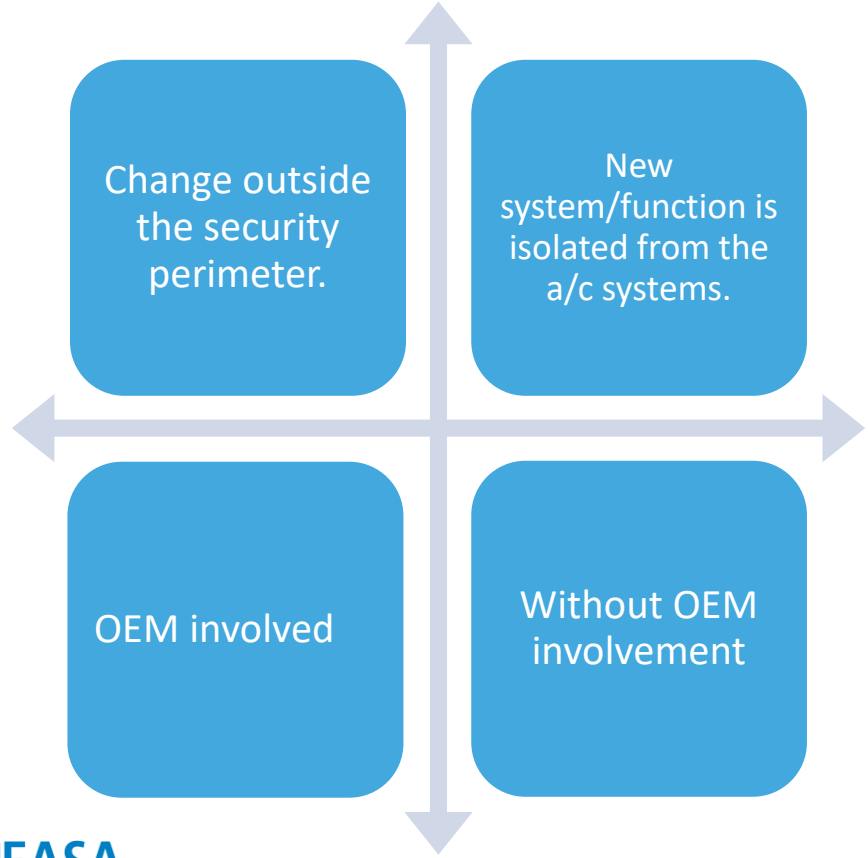
125.494 publicly known cybersecurity vulnerabilities

Milestones RMT.0648!

What happens after Publication?



Specifically for STCs DOAH



Part 21.A.113

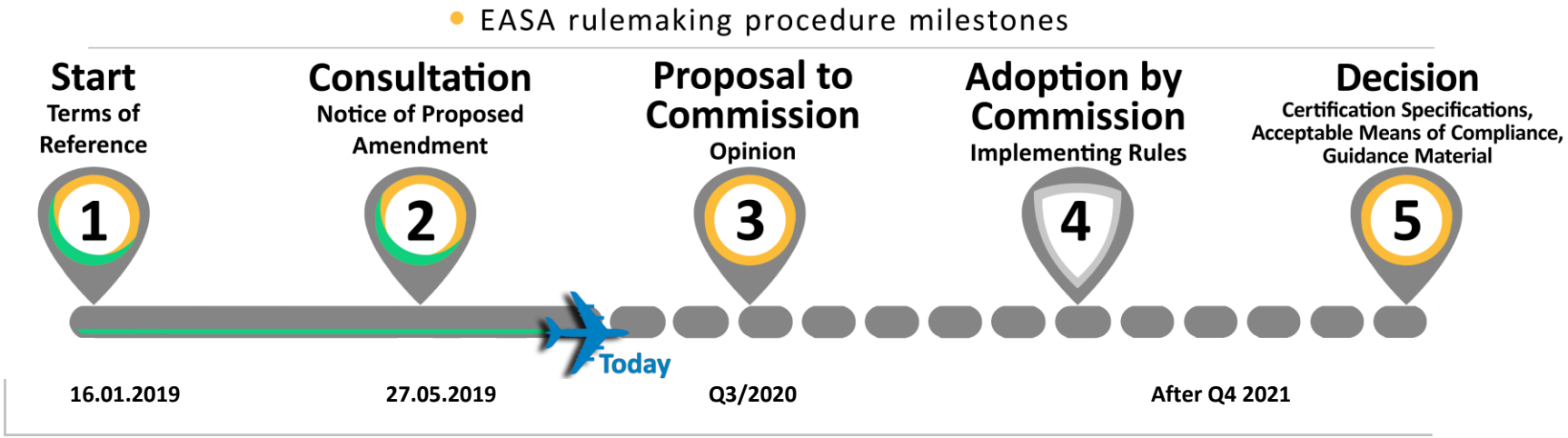
(b)(ii) specify whether the certification data has been or will be prepared completely by the applicant or on the basis of an arrangement with the owner of the type-certification data.

Part 21.A.115 (b)5.

(i) the type-certificate holder has indicated that it has no technical objection to the information submitted under point 21.A.93; and

(ii) 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

Milestones RMT.0720!



Part-AISS

- Common requirements for ISMS
- Reporting of incidents which may impact safety
- Possibility to integrate ISMS into existing SMS
- Possibility to be exempted

The picture is a courtesy of ENISA.

Wrap up!

EASA
European Union Aviation Safety Agency

Thank you
Any further question?

easa.europa.eu/connect

Your safety is our mission.

An agency of the European Union