AER(EP).DT-2020-026

MINISTERO DELLA DIFESA
Segretariato Generale della Difesa e Direzione Nazionale Armamenti
Direzione degli Armamenti Aeronautici e per l'Aeronavigabilità

CYBER SECURITY

FOR

AIR SYSTEMS:

PRINCIPLES AND GUIDELINES

FOR

AIRWORTHINESS CERTIFICATION,

PERFOMANCE ASSESSMENT

AND

MISSION ASSURANCE

Edition 02 July 2020

LIST OF VALID PAGES

NOTICE: This Technical Directive is validi if composed by the following updated pages. A copy of this Technical Directive is available at:

http://www.difesa.it/SGD-DNA/Staff/DT/ARMAEREO/Biblioteca/Pagine/default_.aspx

Date of Issue of Original pages and Updated pages:

Original…….. 0……..Date 02/07/2020

This Technical Directive is composed by N. 57 pages including the first page and N° 01 annex as specified below:

Page. n°	Issue n°
Front page……..	0
A……	0
I-II……..	0
i-ii……..	0
1-44……...	0
Annex A 1-7…….	0

INDEX

ATTACHMENT:

Annex “A”: Cyber Risk Index

INDEX OF FIGURES

INDEX OF TABLES

DEFINITIONS AND ACRONIMS

Acronyms	Definition	Description
AMC	Acceptable Means of Compliance	Acceptable evidence to show a compliance to a requirement.
AP	Air Platform	The airborne system as system of systems.
AS	Air System	Air Platform and Applicable Ground Support System.
ASP	Assessed Security Perimeter	It is the interface between the Target of Evaluation and the Environment which a Cyber threat could come from.
AW	Airworthiness	The ability of an aircraft, or other airborne equipment or system, to operate in flight and on ground without significant hazard to aircrew, ground-crew, passengers (where relevant) or to other third parties.
CCE	Cyber Contested Environment	The environment in which operates an Air Systems that includes possible Cyber Threats.
CCIA	Cyber Change Impact Analysis	It is the process needed to assess the impact of a change to the Air System configuration from a cyber prospective.
CEMA	Cyber Electromagnetic Activity	An electromagnetic activity that, when coupled with an Air System equipment, is able to modify the expected system behavior inducing malfunctions.
Cd AW	Continued Airworthiness	All tasks to be carried-out to verify that the conditions under which a type-certificate has been granted continue to be fulfilled at any time during its period of validity.
Cg AW	Continuing Airworthiness	All of the processes ensuring that, at any time in its operating life, the aircraft complies with the airworthiness requirements in force and is in a condition for safe operation.
CKPIs	Cyber Key Performance Indicators	They are the indicators that need to be defined in order to be able to evaluate the performance of an air system against Cyber Threats.
CIMP	Cyber Incident Management Process	It is the process needed to deal with Cyber incidents.
CS	Cyber Scenario	It includes the entire threat scenario in a given Cyber Contested Environment.
CSAP	Cyber Security Analysis Process	The process which require to identify the Security context identify the target object and interface which the Cyber Contested environment in order to achieve to a definition of the Assurance level of each component to provide sufficient protection by design against cyber threats.
CT	Cyber Threat	In this document, IEUI and IEMI are considered as Cyber Threat.
GM	Guidance Material	Material that can be used as guidance to show compliance to requirements.
IAW	Initial Airworthiness	All of the processes ensuring that new aircraft are airworthy.
IEMI	Intentional Electro - Magnetic Interference	Intentional malicious generation of electromagnetic energy introducing noise or signals into electric and electronic systems, thus disrupting, confusing or damaging these systems for terrorist or criminal purposes (IEC International Electro technical Committee).
IUEI	Intentional Unauthorized Electronic Interaction	A circumstance or event with the potential to affect the aircraft due to human action resulting from unauthorized access, use, disclosure, denial, disruption, modification, or destruction of information and/or aircraft system interfaces. Note that this includes malware and the effects of external systems on aircraft

Acronyms	Definition	Description
		systems, but does not include physical attacks or electromagnetic jamming. (Ed: see also Information Security Threat) (ED-202A).
LGSS	Linked Ground Support System	The ground part of the air system that is in some way connected to the Air Platform and consequently, when compromised by a cyber threat, may have an adverse impact on the safety of the Air Platform. It is a peculiar 1st level AGE that should be include in the Target Object for the Cyber Security Analysis Process.
PT	Penetration Testing	It is the practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit.
RP	Recommended Process	Process that are usable to support the compliance to requirements.
SC	Security Scope	It includes the security perimeter, the list of all the items of an air systems, and characteristics of the environment in which the security shall be ensured.
ST	Security Target	According to Common Criteria, it is a complete and rigorous description of a security problem in terms of Target of Evaluation description, threats, assumptions, security objectives, security functional requirements (SFRs), security assurance requirements (SARs), and rationales. For the CSAS, it is related to the security objectives that need to be achieved in the design phase for a given Cyber Threat Scenario.
TC	Threat Condition	It is similar to the failure condition, with the difference that the threat condition is the outcome of a cyber threat; it is the effect of the threat on a system.
TIA	Threat Impact Analysis	It is the process to assess the impact of a given threat on an Air Systems.
TO	Target Object	It is the final objective of a cyber-attack.
TS	Threat Scenario	It includes the all the conditions, the vulnerabilities and the usable means through which a cyber threat could create threat condition, in other words, it define how a cyber threat could effectively cause a damage on a system.
V	Vulnerability	Vulnerability is a cyber-security term that refers to a flaw in a system that can leave it open to attack and affect the system's confidentiality, integrity or availability. A vulnerability may also refer to any type of weakness in an Air System itself, in a set of procedures, or in anything that leaves the system information and functionalities exposed to a threat.
VA	Vulnerability Assessment	A vulnerability assessment is the process of defining, identifying, classifying and prioritizing vulnerabilities in Air System, and providing the organization doing the assessment with the necessary knowledge, awareness and risk background to understand the threats to its environment and react appropriately.
VT	Vulnerability Testing	It is test specifically designed to identify the weakness on an Air System with respect to its cyber security posture.

1. INTRODUCTION

1.1 SCOPE

The Cyber Security for Air Systems (CSAS) is nowadays a trend topic in the aviation community. The aim of this document is to provide an overall overview on the main Principles and Guidelines identified by the IT Military Technical Airworthiness Authority – DAAA (Direzione Armamenti Aeronautici e per l'Aeronavigabilità) to ensure that an Air System is designed and maintained to face the arising cyber threats fulfilling its mission objectives.

The document is divided in three sections:

- Airworthiness (Initial, Continuing and Continued Airworthiness);
- Performance Assessment;
- Mission Assurance.

The Initial Certification paragraph of the Airworthiness section is written on the basis of Annexes G and H of the AER(EP).P-516 Ed. 13/05/2019. These Annexes, available in Italian only, have been defined to expand the Airworthiness Certification Criteria in order to cope with the Cyber Security for Air System in relation to Intentional Unauthorized Electronic Interaction (IUEI) and Intentional ElectroMagnetic Interference (IEMI).

The main principles and guidelines reported in this document may be considered fully comprehensive of all certification criteria and processes proposed in the AER(EP).P-516 Ed. 13/05/2019 as Acceptable Means of Compliance (AMC) or Recommended Process (RP). They have been streamlined to be more effective and direct.

The paragraphs related to continued and continuing airworthiness describe the new basic concepts that will be incorporated in the new edition of AER(EP).00-00-05 when considered necessary, which means once the first Air System designed in accordance with the Cyber Security process defined for the Initial Airworthiness is going to be available.

The Performance section has the aim of providing a methodology to define, implement and verify cyber-security requirements in order to provide assurance that the intended cyber-security objectives have been met. These objectives are to be agreed by the relevant stakeholders and could be related to cyber-resilience and cyber-resistance of non-safety-critical functions, anti-tamper, authentication, cyber-forensics, cyber-monitoring and other areas not related to the airworthiness of the air system.

The Mission Assurance section outlines the methodologies to test and evaluate the suitability of an Air System to perform the intended mission in an operationally representative cyber-contested environment.

The first two sections are mainly related to the Design& Development Phases (apart from Continuing/Continued Airworthiness) and, in accordance with the standard airworthiness process, are preliminary to the release of a Military Type Certificate (MTC). Therefore, they may be considered as new guidance material on the Cyber Security domain for the certification activities of new Air Systems.

The third section is not specifically linked to the development lifecycle of an Air System, but it can be seen as set of concepts/processes and tools that, based on what it is envisaged for the certification phase, may be used to assess operational

aspects and the capability to perform the assigned mission. Therefore, with the aim to achieve an harmonized approach for the CSAS, this section has been developed in conjunction with the Italian Official Test Centre (RSV - Reparto Sperimentale di Volo) to provide guidelines and methodologies for conducting the IT Air Force Cyber Operational Test And Evaluation in line with the RSV role defined in the SMA PIANI 239. The RSV is recognized, for the purpose of this document and in line with the SMA policy, as the Cyber Test Organization for Air Systems.

1.2 References

In order to develop this document, the following are considered as ground basis:

- AER(EP).P-516, which endorses and expand the EMACC Issue 3.0;
- RTCA-DO-326A Airworthiness Security Process Specification (EUROCAE ED202A);
- RTCA-DO-356 Airworthiness Security Methods and Considerations (EUROCAE ED203);
- EASA - Notice of Proposed Amendment 2019-01 - Aircraft Cybersecurity;
- US National Institute of Standards and Technology - Special Publication 800-115;
- US National Institute of Standards and Technology – Special Publication 800-160;
- Italian Joint Integrating Concept 012 – Cyber Warfare.

1.3 Relation with other Regulations

The Notice of Proposed Amendment (NPA) 2019-01 from EASA proposes amendment to “CS-23, CS-25, CS-27, CS-29, CS-E, CS-ETSO, CS-P, and, as applicable to their related Acceptable Means of Compliance (AMC)/Guidance Material (GM), together with AMC-20. The amendments would introduce cybersecurity provisions into the relevant Certification Specifications (CSs), taking into account the existing Special Conditions (SCs) and the recommendations of the Aviation Rulemaking Advisory Committee (ARAC) regarding Aircraft Systems Information Security/Protection (ASISP). The object is “to mitigate the potential effects of cybersecurity threats on safety. Such threats could be the consequences of intentional unauthorized acts of interference with aircraft on-board electronic networks and systems.” In general, this NPA states that AMC 20-42 – “Airworthiness Information Security Risk Assessment” may be considered as a means of complying with these new requirements.

With respect to the AMC/GM provided by EASA, this document aims to provide the basic steps and criteria that need to be followed to define an alternative compliance process against cyber threats. IEMI are also considered. Moreover, this document establishes basic concepts to be followed for the analysis of the classification of information, Performance Assessment and Mission Assurance, typical aspects of the military domain, not covered by EASA documentation.

1.4 WHAT IS CSAS

To understand the limitation and applicability of this document, a basic definition for Cyber Security for Air Systems is provided.
CSAS is needed to ensure that an Air System (Air Platform + Applicable Ground Support Systems) is airworthy, resilient and secure in a defined or supposed/envisaged Cyber Contested Environment where:

- airworthy means that it is safe for flight;
- resilient means that it is capable of operating and completing the assigned mission preventing, detecting or responding to a cyberattack, notwithstanding the breach of the security perimeter and/or the degradation of system components;
- secure means that it is free from those threat conditions that could impact its operations with unwanted consequences. System security is related to Information Security (INFOSEC), which is the "preservation of confidentiality, integrity and availability of information. Note: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved." (ISO/IEC 27000:2009). In this context, confidentiality is a set of rules that protect and restrict access to information to authorized users, integrity is the assurance that the information is trustworthy and accurate and availability is a guarantee that the information can be accessed when required.

The INFOSEC processes, methodologies and requirements are regulated by other organizations, as mandated by law and/or by internal policies and in accordance with the security classification of the information to protect. These aspects are outside the scope of this document, which is solely focused on attaining safe-for-flight and mission-suitable air system, regardless of the INFOSEC aspects. While the INFOSEC is focused on avoiding the disclosure of information, the CSAS is focused on avoiding that such a disclosure could harm the safety or the performance of the air system. Therefore, alongside the mandatory INFOSEC measures, other additional measures could be deemed necessary in order to satisfy the CSAS requirements, regardless of the security classification of the target system.

S1. SECTION 1 - AIRWORTHINESS

S1.1. Initial Airworthiness

Initial Airworthiness Certification for CSAS means to ensure Security for Safety: the effects of a cyber threat may lead to safety issues and therefore they should be considered in the safety analysis. Hence, System Safety Programme (par. 14 – EMACC Issue 3.0) which aims to “identify any associate system hazard risks, and to eliminate them where possible, or to mitigate the risks such that the residual risks are at acceptable levels” should be augmented to include the system hazard risks due to the effects of cyber threats.

The natural environment in which an Air System has to be certified should be expanded in consideration of cyber threats; therefore, the certification should be achieved in a defined or supposed/envisaged Cyber Contested Environment.

The Cyber Contested Environment is:

- defined when the cyber threats and possible attack patterns are well identified by Security Agencies and/or specified in the Development Contract (Intelligence Driven Approach – par. S1.1.3.1);
- supposed/envisaged when possible attack patterns and hypothetic cyber threats are considered in the assessment the Air Systems (Engineering Judgment Approach – par. S1.1.3.2).

S1.1.1. Methodologies

The methodology used for the Initial Airworthiness Certification is based on the combination of concepts specified in the RTCA-DO-326A - Airworthiness Security Process Specification (EUROCAE ED202A) and in the Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408).

The aim is to define a pragmatic simplified approach focused on:

- defining the Security Scope and the Security Object of an Air System;
- overcoming the issue of the availability of a defined threat scenario against which the Security for Safety shall be ensured;
- providing a methodology for assessing the impact of IUEI and IEMI augmenting the standard safety analysis with the security analysis normally performed by the Information Communication Technology (ICT) community;
- providing common criteria for the Initial Airworthiness Certification.

S1.1.2. Security Scope

For the Initial Certification, is it mandatory to define the Security Scope, which is the Security Perimeter, including the involved items (Air Platform and its subsystems, Ground Support System and its subsystems) and the Security Environment characteristic in which to ensure the Security for Safety of the Air System.

The picture below shows a typical representation of the Security Environment for an Air System. To ensure the Security for Safety of an Air System for the initial certification, the Security Object needs to be defined. It is made of all the equipment/procedures that should be included in the assessment for ensuring the

Security for Safety; it represents the Target of Evaluation as normally defined in the ITSEC Common Criteria.
For instance, the Security Object could not consider the supply chain management or the physical security, but it could be only related to the Air Platform and its subsystems, including data loading equipment (in some way connected to the Air Platform). Once the Target Object for the assessment is selected, the Security Perimeter for the assessment is defined and, on these items, the Cyber Security Analysis Process should be conducted.
Interfaces between the Target Object perimeter and the Cyber Contested Environment should be analyzed, and any connection/link carefully assessed.
Those that are considered reliable can be excluded from the Cyber Security Analysis Process (CSAP). Interfaces that are outside the Development contract but could generate a cyber risk, should be addressed or the customer should be informed of the possible risks.
When the Target Object does not contain physical and/or personal security, the user of the system shall be considered part of the cyber kill chain (a possible example of Cyber Kill Chain is depicted in Figure 2), which means he/she can be considered an element of the attack.
Once the Target Object is well known, in order to conduct the Cyber Security Analysis Process, a definition and/or characterization of the Threat Scenario is mandatory. It could be, as said, defined or supposed/envisaged as described in the following paragraphs.

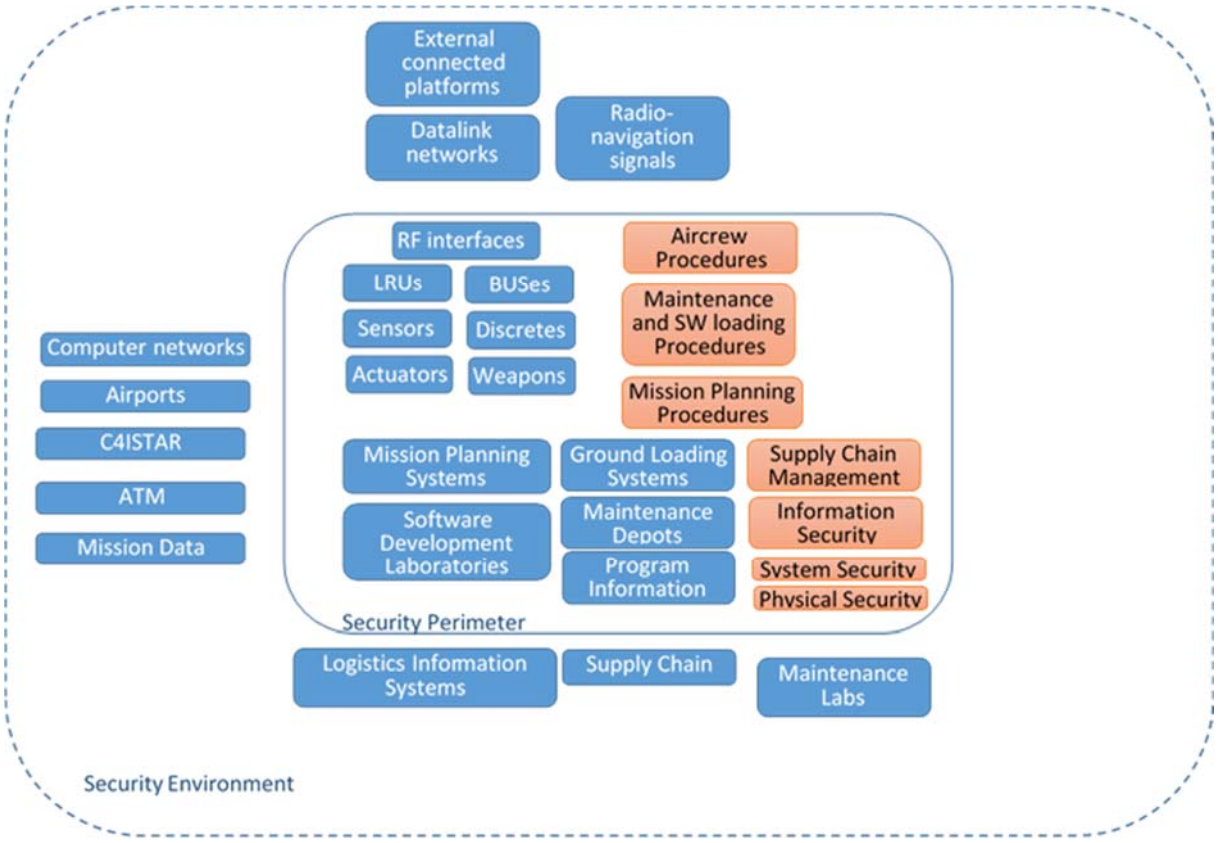

Figure 1: Security Environment and Security Perimeter

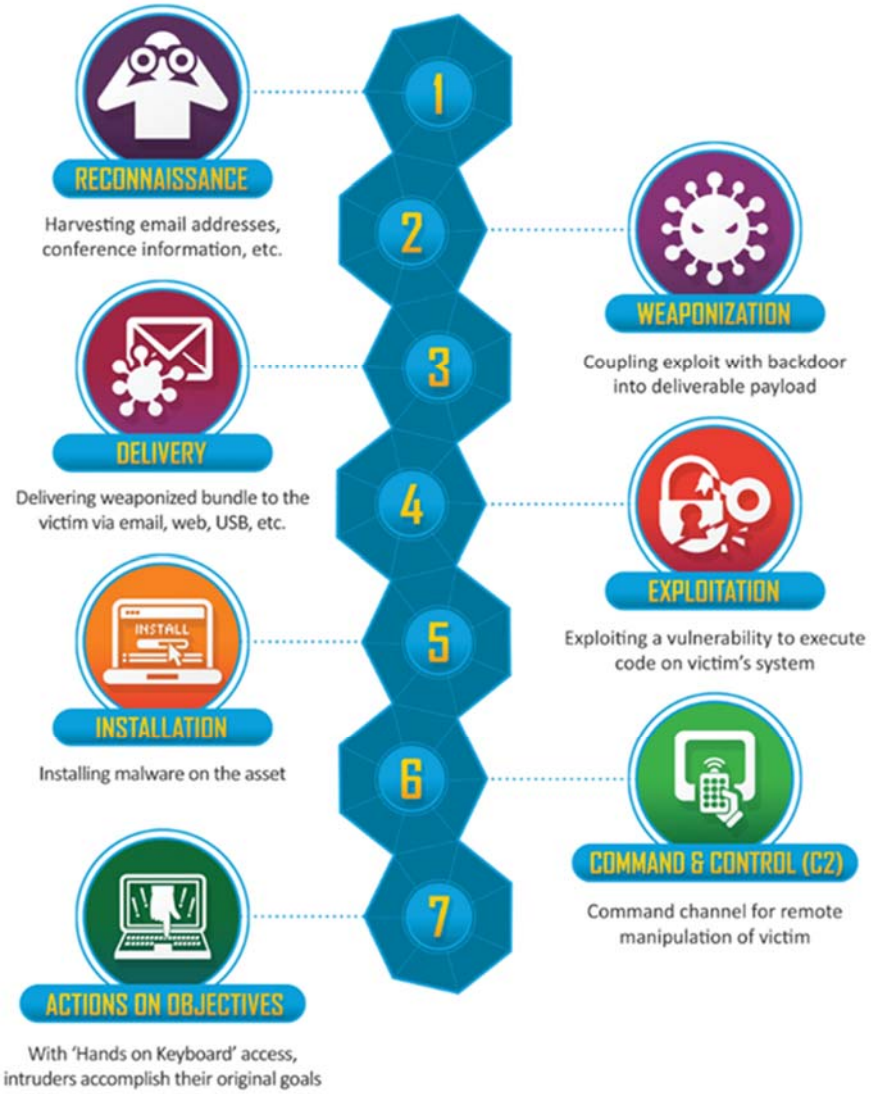

Figure 2: Cyber Kill Chain® (Lockheed Martin)

S1.1.3. Cyber Security Analysis Process

The Cyber Security Analysis Process is defined to take into account the IUEI. The IEMI are addressed as new EM interference in addition to the interference usually considered in the A/C certification, especially in relation to High Intensity Radiated Field (HIRF).

The main concept on which is based the Cyber Security Analysis Process is that an IUEI can change the condition (threat condition) of the system under attack implying an impact on the Safety of the Air System (airworthiness) or on the performance just like a failure. The safety analysis should be expanded to include also the threat condition and not only the failure condition. The failure condition is due to unwanted physical/logical condition, the threat condition is due to the IUEI. In Figure 3, the parallelism between a threat condition and a failure condition is shown.

The existence of a vulnerability could be used by a cyber agent to create a threat mode equivalent to a failure that it is able to generate an effect on the system. The

effect could cause a consequence that can be categorized in accordance with its level of severity.
The threat condition is the effect of the threat on the system; the failure condition is the effect of a bug/failure on the system.
Even if the effect could be the same, the probability may change and depends on the Threat Scenario.
In the standard process of the safety analysis, in order to understand the level of risk associated to a given failure, it is usually defined a Hazardous Risk Index, which provide the criticality of a failure based on probability of occurrence and severity. In the same way, a Cyber Risk Index could be defined to identify the criticality of a threat looking at probability of occurrence of and the severity.
The criticality of the threat condition in the airworthiness process is judged in isolation, while in the Performance Assessment and Mission Assurance Process has to be matched respectively with the general intended performance of the system and with the criticality for the success of the mission of the system under attack.

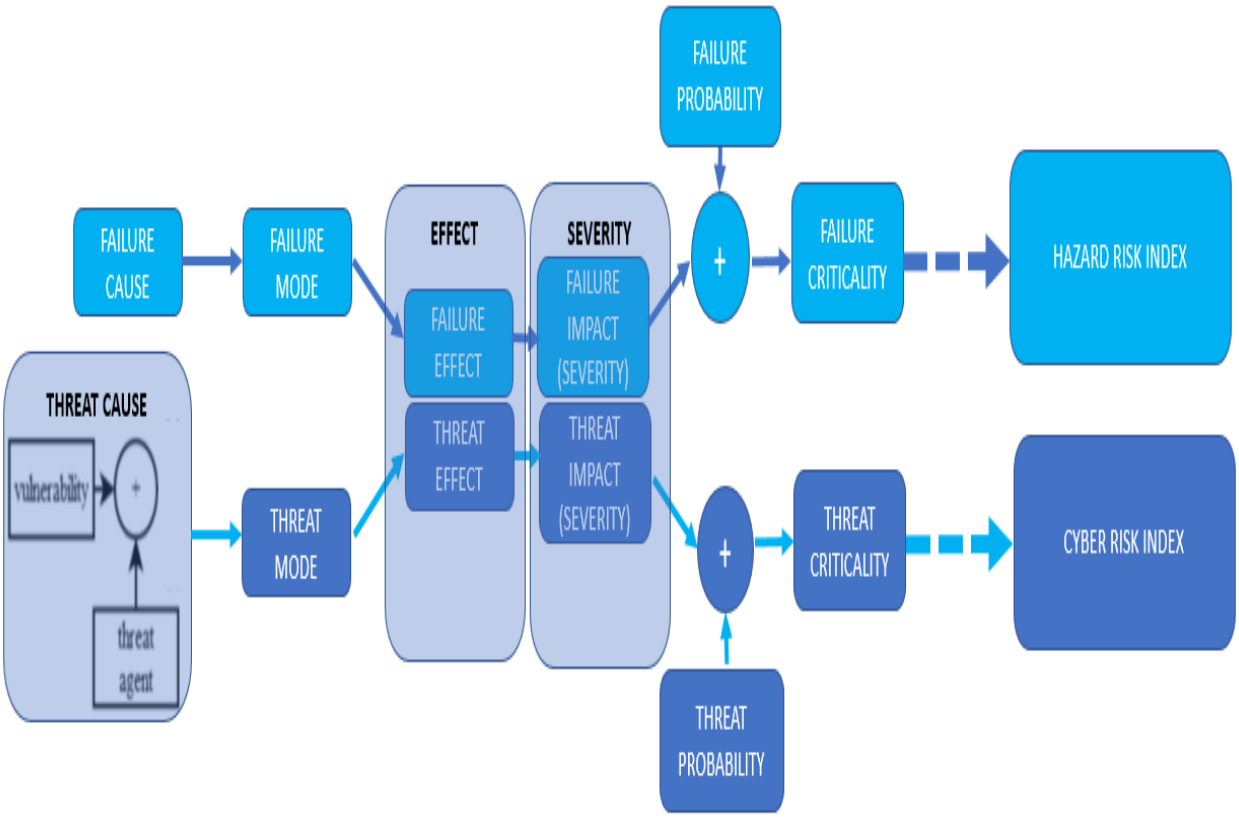

Figure 3: FMECA + Threat – Cyber FMECA

The implementation of a risk management process is mandatory to identify, analyze and evaluate risks linked to cyber threats. For the ICT system, a process is defined in the ISO 27005 - Information Technology - Security Techniques - Information Security Risk Management (see Figure 4 and Figure 5), while the RTCA-DO-326A provides the Airworthiness Security Process (Figure 6).

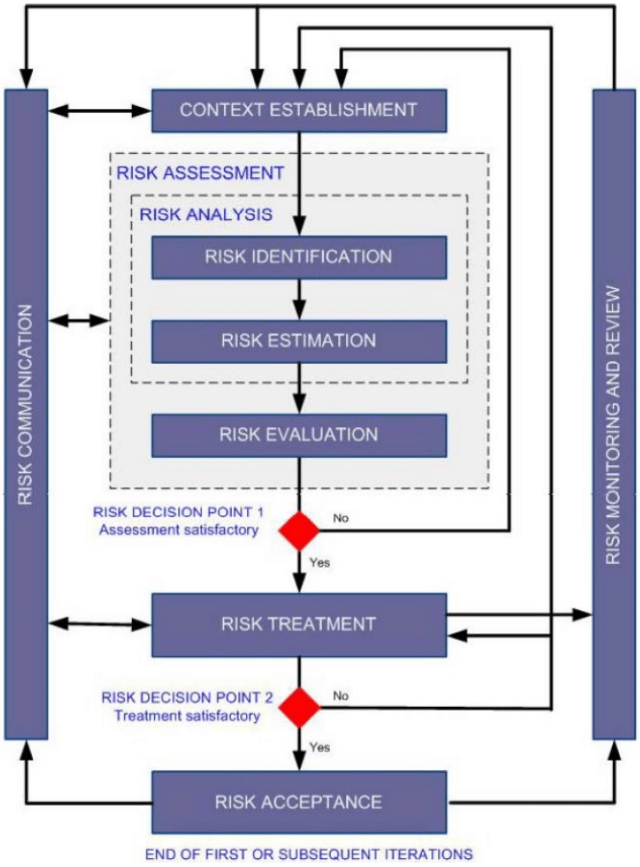

Figure 4: ISO 27005 - Risk Assessment Process

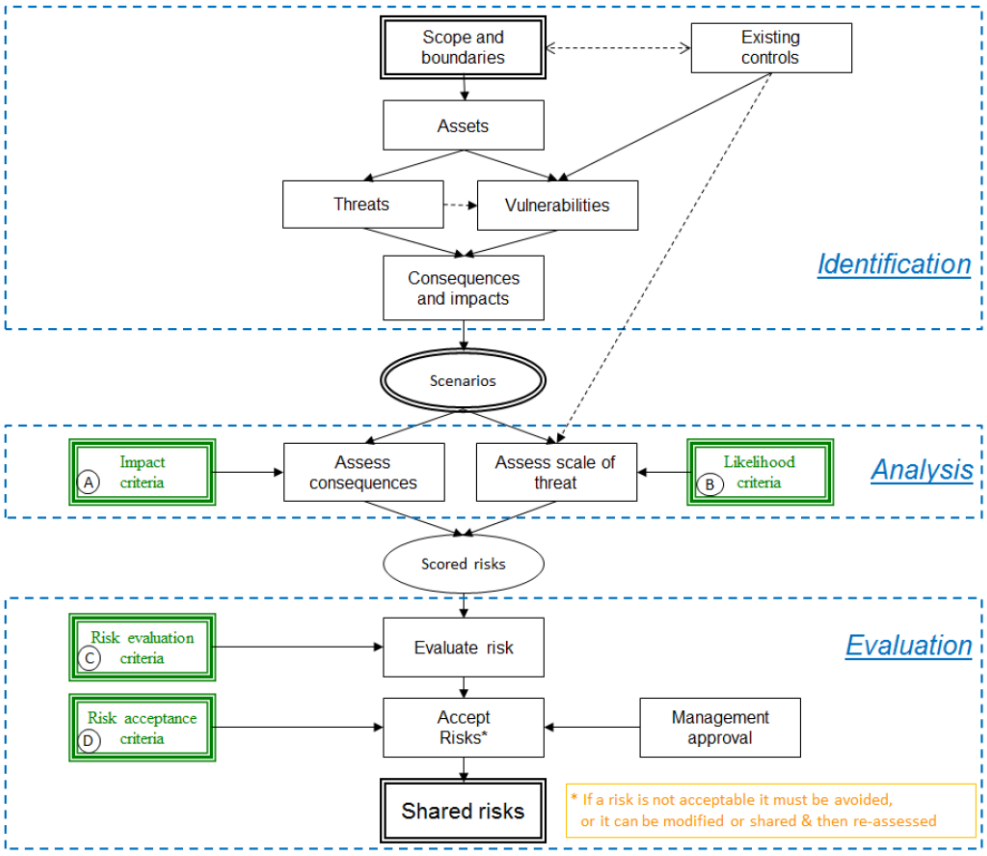

Figure 5: Common Steps for Risk Analysis

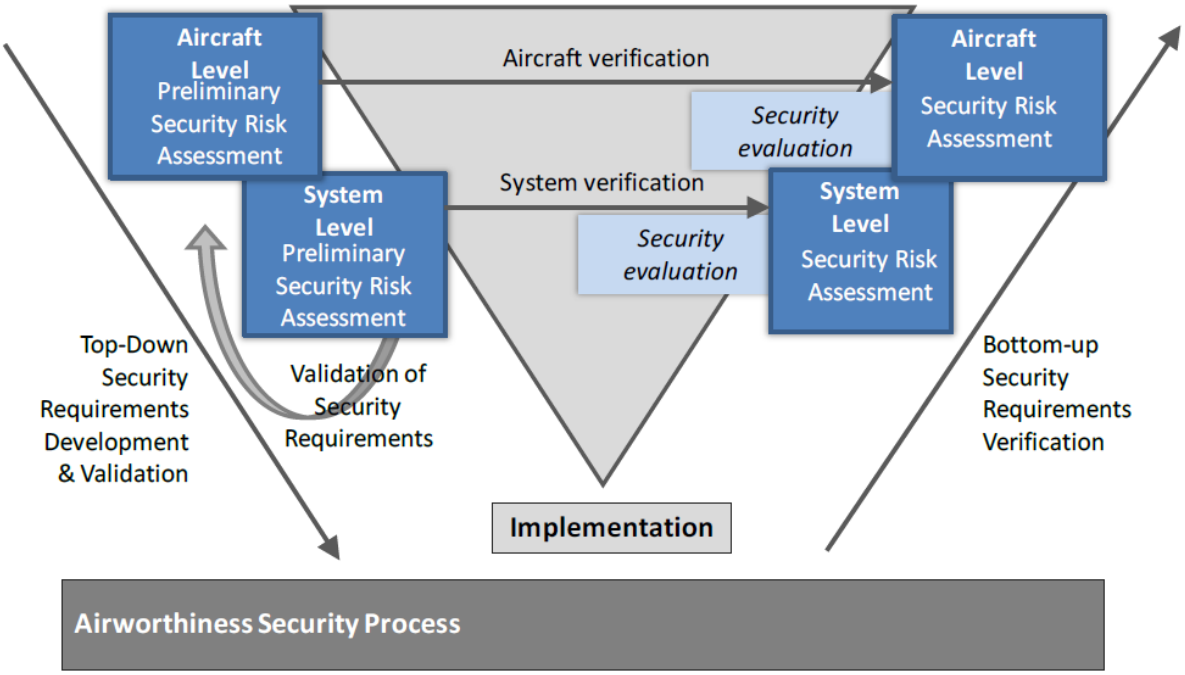

Figure 6: *Airworthiness Security Process* (DO-326A)

The Cyber Security Analysis Process allows assessing the risk associated to cyber threats and it is based on the understanding of the threat scenario, to:

- analyze the effect of the threat on the system (threat condition)
- discover/understand the vulnerabilities used for the attack;
- describing the enabling attack factors;
- identify the attack patterns, (i.e. the routes through which the cyber threat has been able to generate an effect on the system);
- assess the residual vulnerabilities and the role of the preventive security measures.

A successful attack is able to overcome the existing (if any) security measures, compromising the attack target and generating an effect on the system (threat condition). It can be analyzed assigning a severity level and trying to understand the level of occurrence probability. The level of occurrence probability is the real issue for a cyber threat, because a cyber attack is not the result of a random process, but an intentional act undertaken by an intelligent agent that can choose the time and the method to defeat the security measures in place. Therefore, estimating the level of occurrence probability for a cyber-threat could be problematic and not entirely correct from a strictly mathematical standpoint. However, in order to proceed with the analysis, it will be necessary to define a methodology to attain such estimation. The Cyber Security Analysis Process is based on the assumption that a threat could generate an effect (threat condition) that can have an impact to the safety of an Air Systems, as a failure could do, but with a different level of severity and occurrence (Figure 3). Therefore, for the airworthiness perspective, it is necessary to amend the

traditional safety analysis based on *Failure Mode, Effects, and Criticality Analysis* (FMECA) and *Fault Tree Analysis* (FTA) to take into account threat conditions.
The Threat Scenario definition/availability changes the way in which the safety analysis could be amended. As established in Annex G of AER(EP).P-516, two distinct approach are possible, which are: Intelligence Driven Approach and Engineering Judgement Approach.

S1.1.3.1. Intelligence Driven Approach

The Intelligence Driven Approach is applicable when the Threat Scenario is known or defined in a Development Contract. The characterization of the Cyber Contested Environment is fundamental for the evaluation of security risks and understating of the mitigation actions that could be implemented.
This approach is applicable for both airworthiness certification and performance assessment and it represents the traditional way to design and develop a system when the environment in which it needs to operate is known and the expected performance defined.
The knowledge of the Threat Scenario allows to perform the Security Risk Assessment in two standard phases:

- preliminary risk assessment: it is carried out during the design phase when an initial vulnerability assessment helps identifying additional Security Requirements to be developed.
- final risk assessment: it is carried out to verify and test security requirements and assess the effectiveness of the security measures identified in the design phase.

The Vulnerability Assessment is the overarching process that is used to identify and test additional security requirements, which are additional SW or HW requirements that need to be developed and tested in accordance with the approved processes (i.e.RTCA-DO-254 for hardware, RTCA-DO-178C for software).
It is important to note that they are different from the security requirements that will be introduced later on in par. S1.1.3.6 when discussing about Cyber Risk Index, Assurance Level and Common Criteria, where the security requirements are intended more as security objects to be demonstrated rather than additional functional requirements.
DO-326A provides a clear explanation of the Airworthiness Security Process (Figure 6) and of the relationship between the standard processes (Safety Assessment Process and System Development Process) and the new process for Cyber Security (Security Risk Assessment - Figure 7).
In synthesis, in the design/development phase, following a top down approach, the threat conditions identified during the initial vulnerability assessment are scrutinised for defining new security requirements and valued to understand the impact on the safety of the Air System. In the verification phase (security evaluation), a bottom-up approach it is carried out to define other security requirements in an iterative process until an acceptable security level is reached.

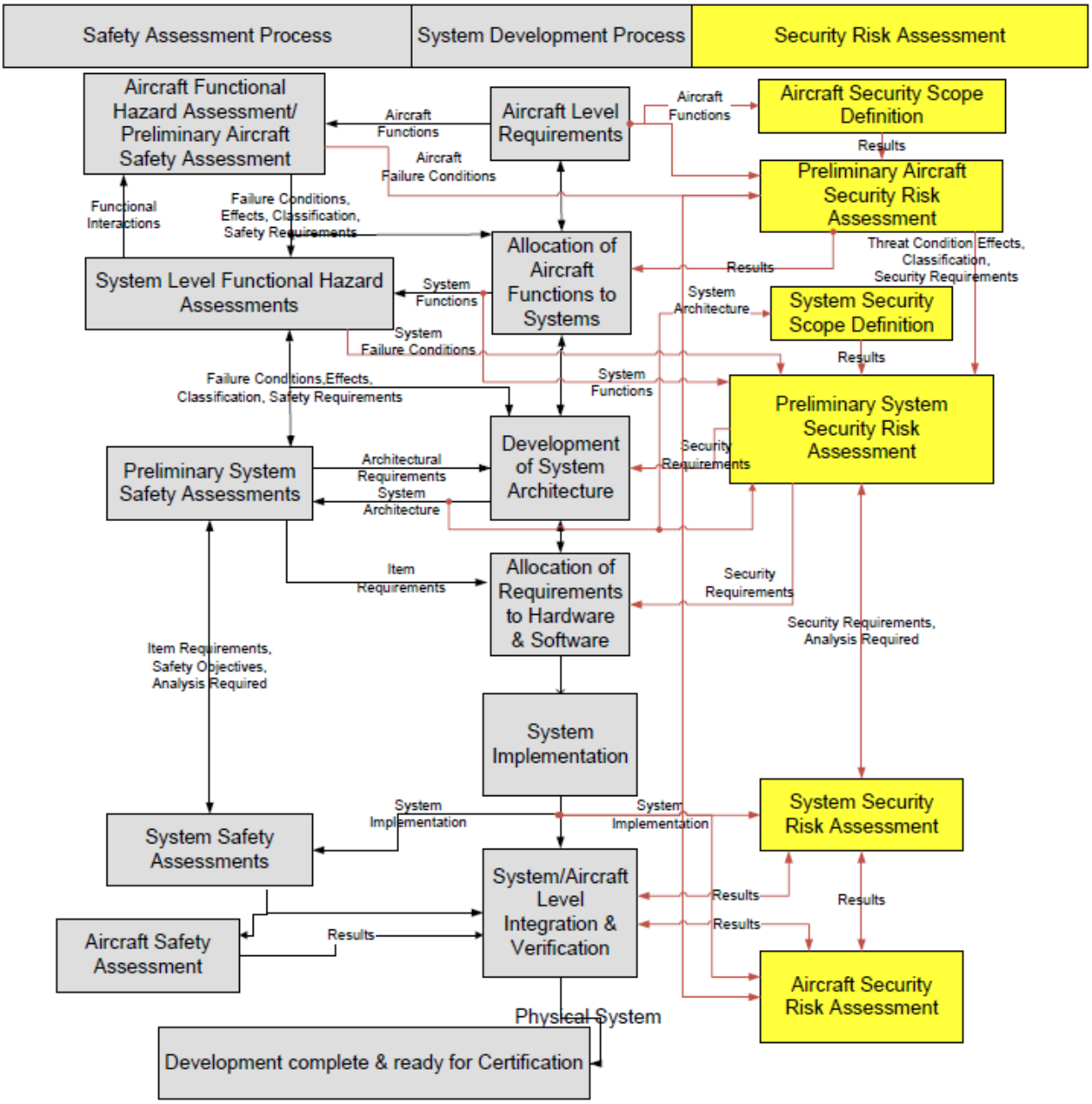

Figure 7: Processes interrelation in (RTCA-DO-326A)

S1.1.3.2. Engineering Judgment Approach

The Engineering Judgement Approach is applicable when the Threat Scenario is not known or defined in a Development Contract. The absence of characterization of the Cyber Contested Environment in theory does not allow the evaluation of security risks and the definition of proved countermeasures. In order to overcome this issue, in this approach, the Cyber Contested Environment is supposed/envisaged and the process of evaluating cyber risks does not start from the cyber threat, but from the definition of what has to be protected first in the Weapon System.

A deduction methodology is applied, where the final unwanted event and its associated effect on the system is supposed to be true and the chain of event that may cause the final unwanted effect are gathered and evaluated.
All the possible attack patterns that may lead to unwanted effects should be explored considering the existing vulnerabilities and security measures, in a process that could be defined as Cyber Risk Assessment.
This approach is applicable for both airworthiness certification and performance assessment and it represents a way to overcome the uncertainty on the Threat Scenario definition.
Once the security object is established, the items that may constitute an access point for the cyber threat and are “more exposed” (e.g. communication equipment, interface towards external loading equipment, etc.) should be included in a target list and all attack patterns should be evaluated. The target list should be regularly updated by intelligence Services to include equipment, functions and areas of the systems more exposed and to associate possible entry points for each supposed threat. Each attack pattern should be evaluated and weighted starting from entry points. The weights for each attack pattern could be given considering the following parameters:

- the presence of known vulnerabilities;
- the role and the effectiveness of the existing countermeasures (if any);
- availability of security checks;
- heterogeneity of the architecture;
- functional and architectural redundancy;
- used communication protocol for the access points;
- level of exposition of access point;
- usage of sensible functionalities or process;
- distributed functional allocation;
- time to prepare the attack;
- effort to action a given vulnerability (to understand the level of threat);
- value of the specific security object to be attacked (to assess the level of occurrence of an attack).

The last three bullets evaluate the skills and the know-how necessary for a cyber agent to partially or completely compromise the Air System and the resource necessary to conduct the supposed attack.
For augmenting the Safety Analysis, at minimum, the following types of attack should be considered when intelligence data are not available:

- supply chain attack;
- malware infection/code injection:
- data injection;
- firmware attacks/modification;
- barrage attack/sleep deprivation;
- communication links misusage;

- network attacks (Command Injection, Denial of Service, Fuzzing, Network Isolation, Packet Sniffing, Password Cracking, etc).

S1.1.3.3. Augmented Safety Analysis for IUEI

Independently from the followed approach, which is discriminated by the availability of intelligence information, the output of the Cyber Security Analysis Process is:

- additional security requirements to be developed in accordance with available standards (i.e. RTCA-DO-254 for hardware, RTAC-DO-178C for software) or “security for safety procedures” to set up additional security measures against the known vulnerabilities and the identified attack patterns for the specific security objects;
- threat conditions to be considered in the Safety Analysis for Airworthiness Certification.

To analyze risks associated to cyber threats is nowadays mandatory: it could be based on AMC 20-42 – “Airworthiness Information Security Risk Assessment” as defined in AMC 20-42 or on other processes as the Cyber Risk Assessment process defined by NAVAIR, which also links Cyber Risk activities with traditional FMECA (Figure 8).

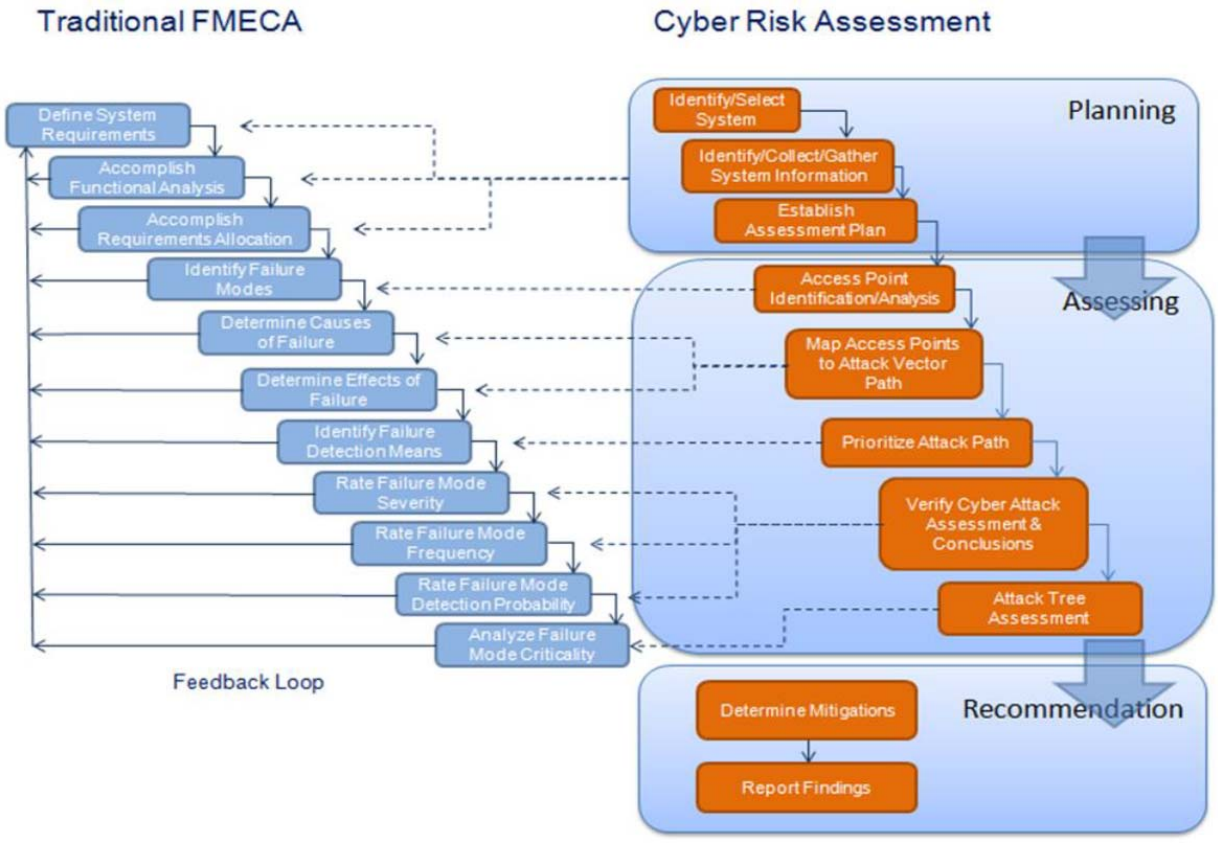

Figure 8: *Cyber Risk Assessment*/Traditional FMECA
(NAVAIR – MP-SCI-300-12P)

For the safety analysis, it is fundamental to categorize the threat conditions to identify those catastrophic. To address the severity of the effect, the Failure Mode Effect Cause Analysis (FMECA) should be integrated with the Fault Tree Analysis (FTA).
RTCA-DO-356 introduces an approach defined as Threat Tree Analysis that allows identifying cutsets for each Treat Scenario. This is similar to the Attack Tree Analysis (ATA - par. S1.1.3.4), commonly used in the software development to integrate FTA and FMECA, which is becoming typical in the software development of modern communication equipment. For example, Figure 9 shows an integration between FMECA and FTA called Backward Integrated Analysis.
The unwanted effect supposed in the Engineering Judgment Approach is considered and the attack pattern is examined to verify if there are arising failure modes and threat modes to be included in the safety analysis as additional failure modes.

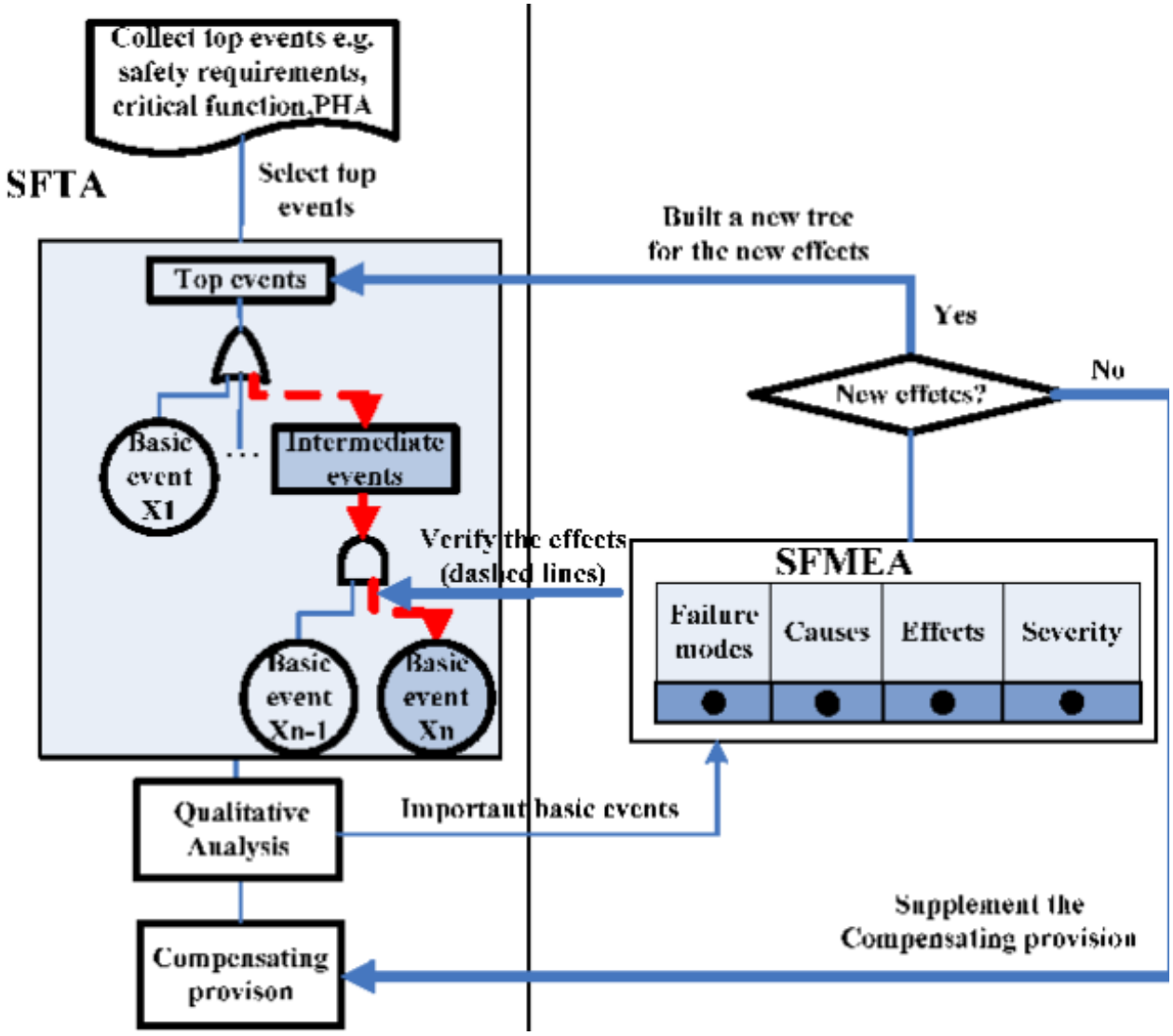

Figure 9: Backward Integrated analysis FMEA – FTA – Software

S1.1.3.4. Attack Tree Analysis (ATA) for threat conditions

In the Attack Tree Analysis adapted to include Cyber threat assessment, the Fault Tree Analysis is modified to add to the failure event also the threat event, in order to show the effect of the threat on the system. The failure event, which is normally on top of the FTA graph, is substituted by the security object to attack (for instance, compromising the Airborne Operational Software) or, from the system designer point of view, from what has to be protected (for instance, the integrity of the Airborne Operational Software).

Starting from the target object, every possible attack pattern is analyzed taking into consideration existing vulnerabilities, those discovered during the evaluation, the existing security measures and their effectiveness in order to understand in which way a threat condition could be generated. An example is provided in Figure 10.

It helps defining additional security measures during the design/implementation phase and verifying the effectiveness of the implemented security measures in the verification phase, as well as the Security Risk Assessment does when the Threat Scenario is defined.

The outcome is also in this case to identify additional security requirements (to be developed in accordance with RTCA-DO-254 for *hardware*, RTCA-DO-178C for s*oftware),* assessing the residual Cyber Risk Index once all the mitigation actions are implemented.

The definition of the Cyber Risk Index does not provide only a classification of the risk due to cyber threat, but it is the key criteria to understand which is the Assurance Level (AL) required to ensure the Security for Safety of an Air System (par. S1.1.3.6).

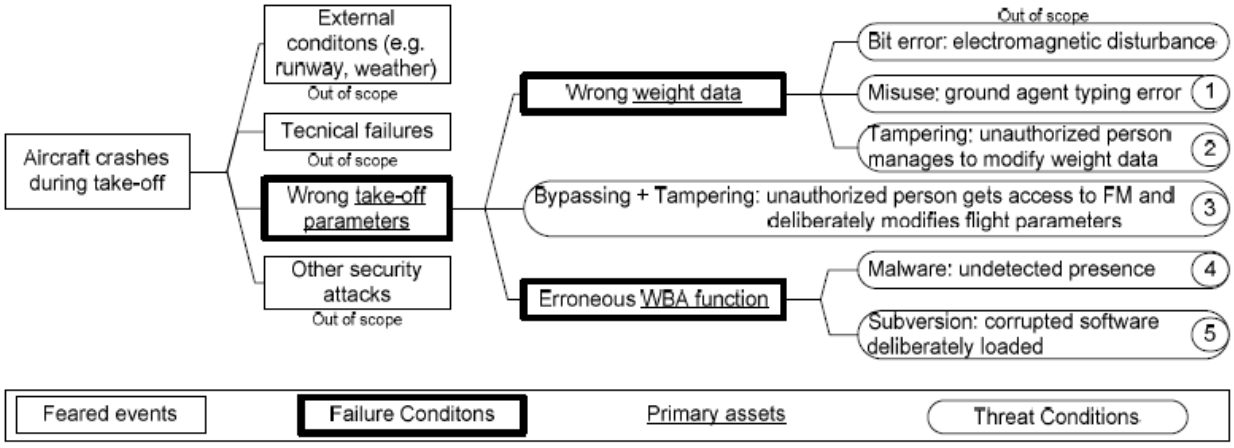

Figure 10: *Attack Tree Analysis example – Weight and Balance parameters*

S1.1.3.5. Protection against IEMI

IEMI should be intended as an extension of cyber threats into the ElectroMagnetic domain. For the scope of Initial Airworthiness Certification, the cyber activities into the EM domain should be taken into account limiting the analysis at what it is applicable in reality with the current technology. Looking at Figure 11, the IEMI can be seen as a particular type of High Intensity Radiated Field (HIRF), already considered in the certification process. Nowadays, it is not difficult to generate Electromagnetic Pulse (EMP) with a high peak value and at higher band using commercial equipment (see Figure 13).

There are many analyses on the effects on software, cryptographic algorithms and so on of such EMP; through an electromagnetic signal, it is possible to induce an effect on the software changing, for instance, the clock frequency of a processor, the fetch phase of a program, the value of the instance of a variable.

However, for the time being, this kind of scenario is not considered applicable due to the precision needed to carry out these types of attacks and the power needed to attack a flying Air Platform. It is believed that these phenomena are feasible more in a laboratory than in a real environment.

For this reason, even if it considered important to augment the safety analysis taking into account the IEMI, the only criteria that it suggested is the amendment of the System Safety Assessment for the HIRF (for instance in Figure 14 the process for system B and C is reported as an example).

The additional activities consist in defining protection not only against the HIRF, but also against the IEMI in case the new waveform/signal (generated by a Cyber EM Activity - CEMA) are defined by the intelligence or specified in the Development Contract.

The Certification of Aircraft Electrical and Electronic Systems for Operation in the High-intensity Radiated Fields (HIRF) Environment has been updated by AC 20-158 to include the latest revision of SAE ARP 5583A (and EUROCAE document ED-107A), “Guide to Certification of Aircraft in a High Intensity Radiated Field (HIRF) Environment”, June 2010. Apart from the definition of new waveforms, the new values are assumed to be sufficient also for IEMI.

Regarding the ground segment of an Air System and its installation in a dedicated building, the IEC 61000-4-36 ed. 1.0 EMC - Part 4-36: “Testing and measurement techniques IEMI immunity test methods for equipment and systems” could be considered applicable.

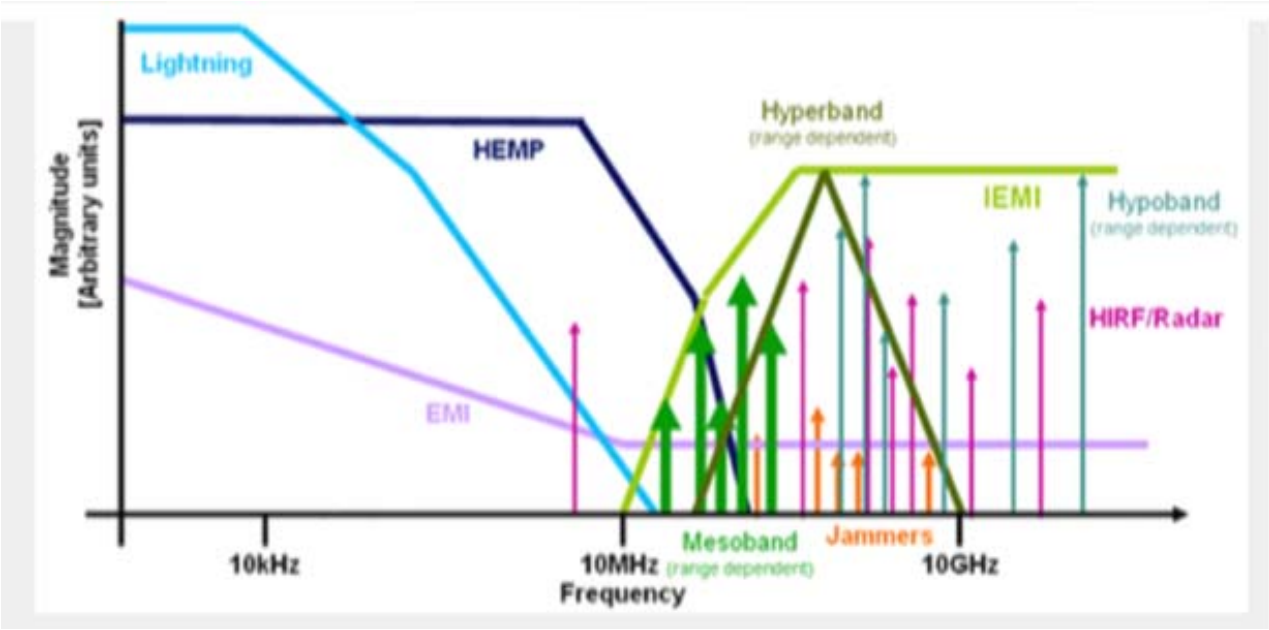

Figure 11: IEMI

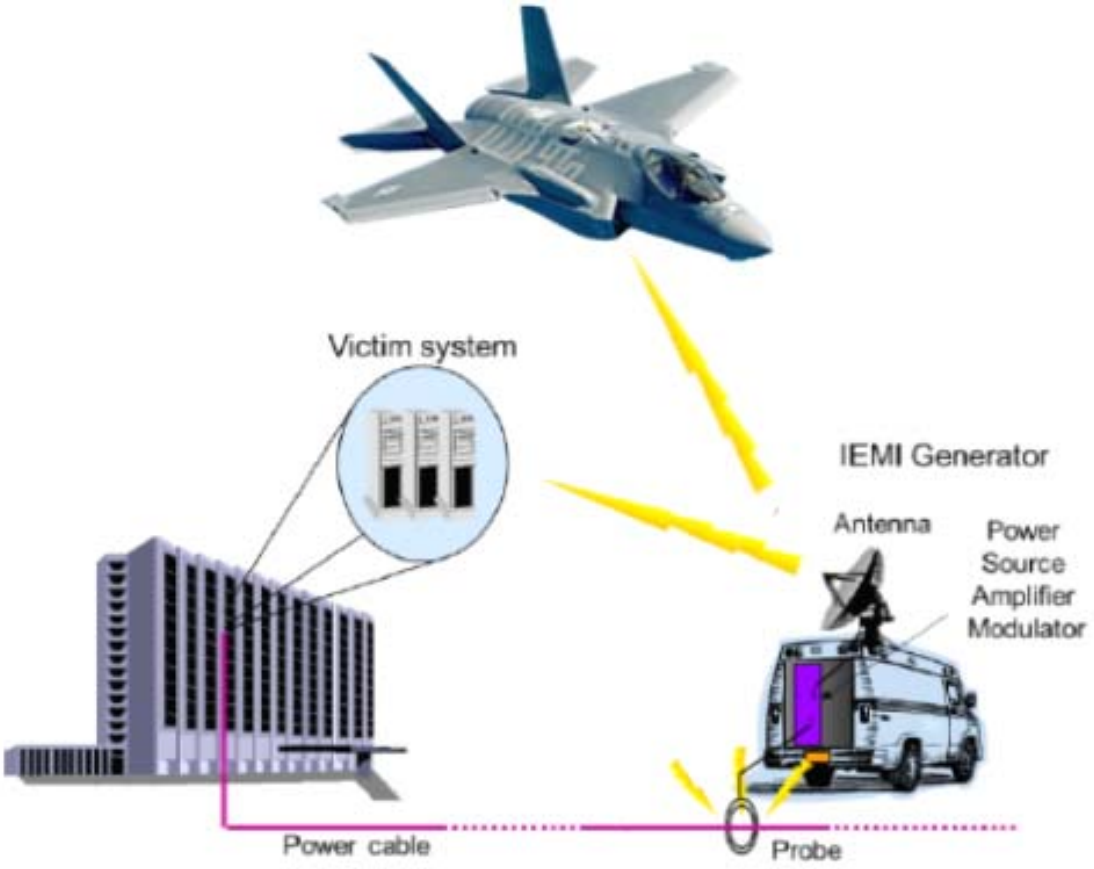

Figure 12: An Electromagnetic Cyber Scenario

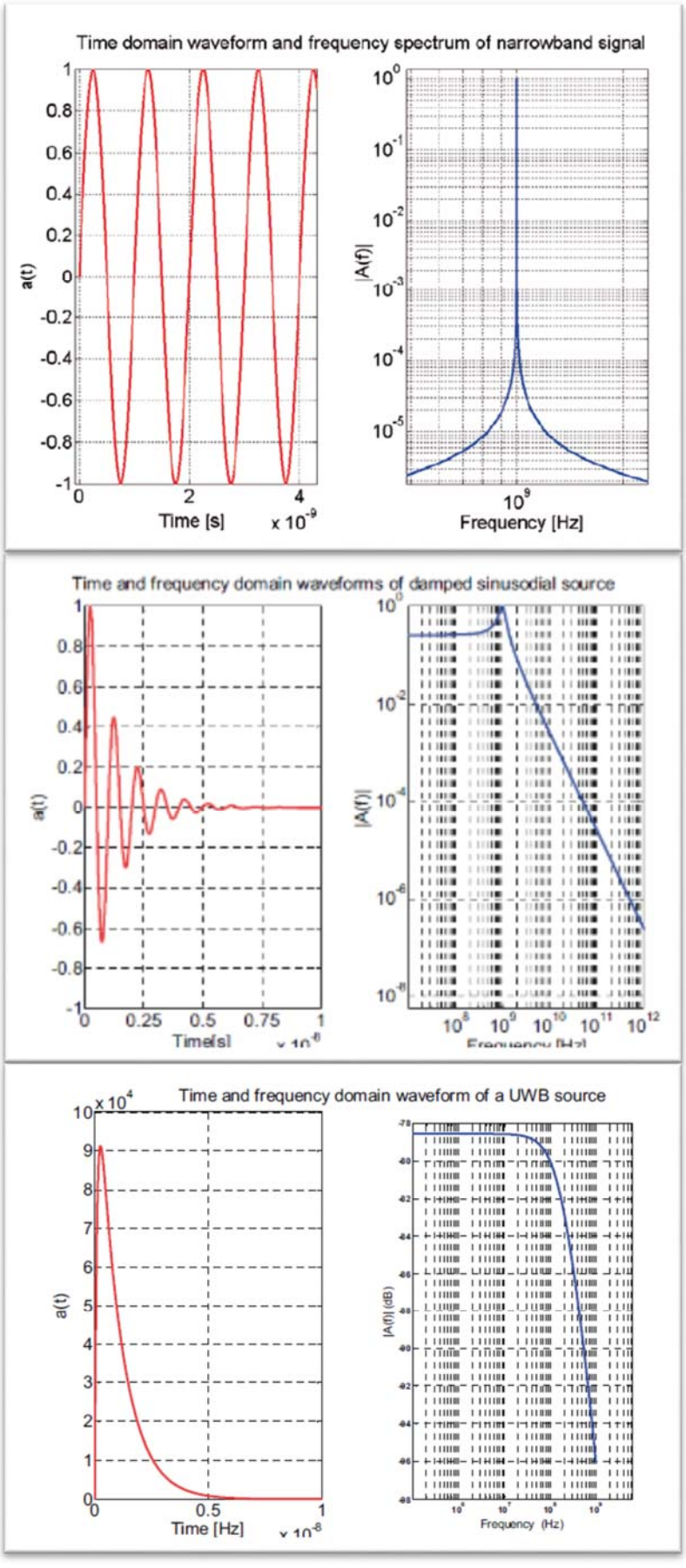

Figure 13: Potential IEMI signal generated by simple commercial tools

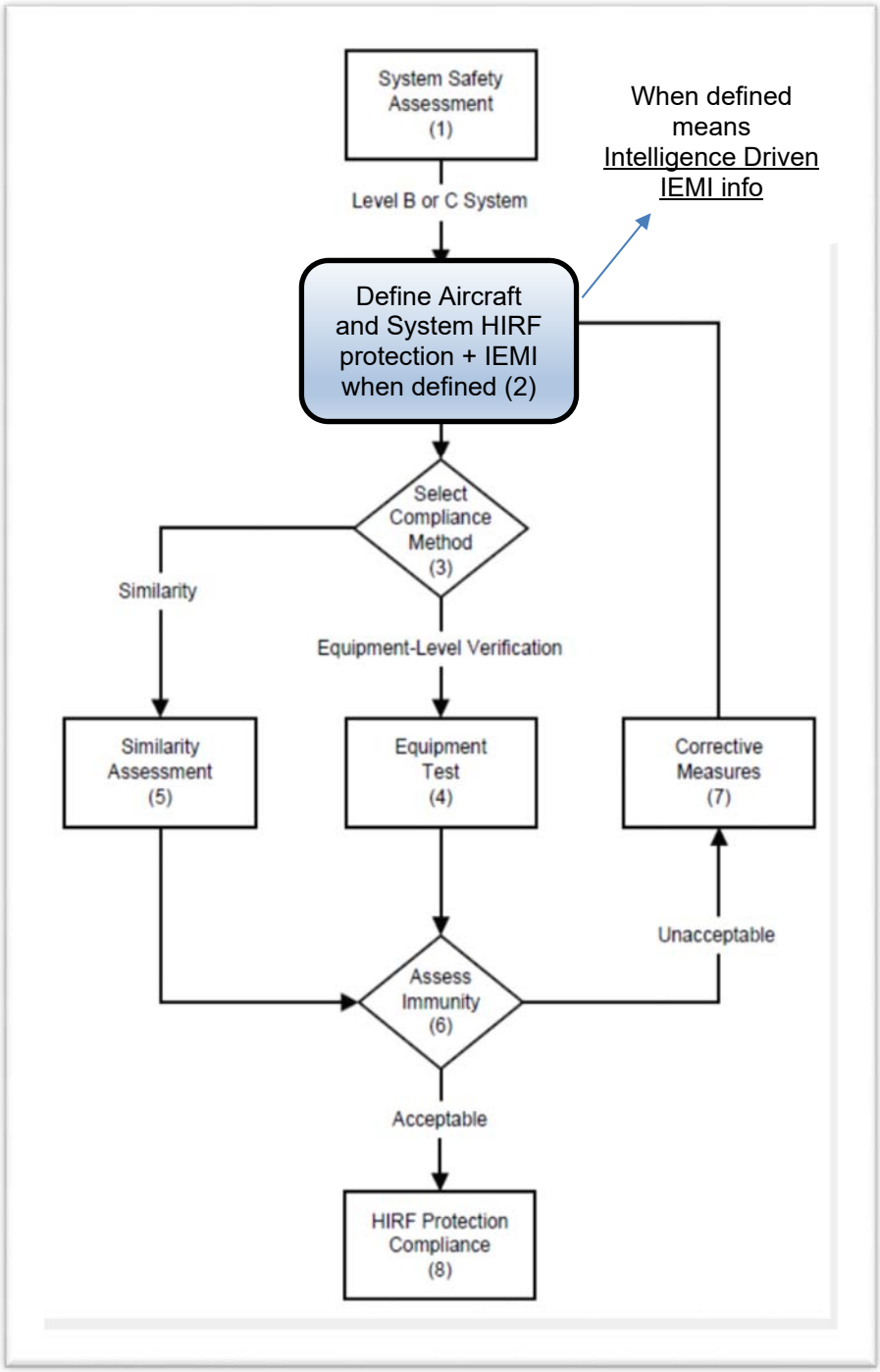

Figure 14: Augmented System Safety Assessment for IEMI

S1.1.3.6. Cyber Risk Index and Assurance Level

As shown in Figure 7, to ensure the Security for Safety against IUEI, three interdependent processes are carried out: Safety Assessment Process, System Development Process and Security Risk Assessment Process. The high-level security requirements are defined in the design/development phase following a top down approach, while during the verification phase a bottom up approach is followed to identify additional low-level security requirements.

The risk estimation, which is to assess the safety impact of a threat condition considering the level of severity and the associated level of concurrency, is a fundamental step to achieve a consolidated Cyber Risk Index for the defined or supposed/envisaged Threat Scenario.
The assessment of the level of severity of a threat condition does not change with respect to a failure condition, while for cyber threats it is difficult to estimate a probability of occurrence.
In annex A, a possible approach is proposed to evaluate the Cyber Risk Index considering the level of occurrence of a threat condition based upon the exposition level of an Air System and the cyber agent capabilities/characteristics.
The method is generally applicable and a different characterization of the parameters may also be proposed when applying for an Military Type Certificate.
However, the Security Risk Assessment process aims to identify proper corrective actions in the design/development phase to reach an acceptable level of cyber risk due to IUEI for a given/supposed/envisaged Threat Scenario. In accordance with the Hazardous Risk Index reported in the AER(EP).P-6 the following Cyber Risk Index Matrix can be used.

Cyber Risk Index (CRI)	(1) CATASTROPHIC	(2) CRITICAL	(3) MAJOR	(4) MINOR	NO SAFETY IMPACT
(A) FREQUENT	1A	2A	3A	4A	No Security for Safety Impact
(B) PROBABLE	1B	2B	3B	4B	
(C) OCCASIONAL	1C	2C	3C	4C	
(D) REMOTE	1D	2D	3D	4D	
(E) IMPROBABLE	1E	2E	3E	4E	

Figure 15: Cyber Risk Index Matrix

In the risk estimation phase of the risk assessment (Figure 4), the risk of a given cyber threat is estimated in accordance with the system design/behavior and the threat scenario. In case the risk is estimated as not acceptable, additional security measures can be implemented to reduce or the level of severity or the level of occurrence. In the model in Annex A, the level of severity is assumed unchanged, while the level of occurrence may change. The scope of the risk assessment is to define the level of assurance required in the development/verification process to reduce the risk to an acceptable level. In order to reduce the level of occurrence, actions are usually taken to reduce the level of exposition of the Air System through additional security requirements. In accordance with how much the risk should be reduced, an Assurance Level (AL) may be defined for a given item or function of the Air System as well as the Design Assurance Level is defined for a given Software/ hardware Item or Function in accordance with ARP4754 – “Aerospace recommended practice Development of civil aircraft and systems”

The Assurance Level represents:

- the robustness/effectiveness of the security measures introduced, to demonstrate that they absolve their function without adding adverse effects;
- The level of confidence in the process during the development phase, to provide evidence that the security measures are well implemented and verified.

The Assurance Level may be defined as in Table 1.

ASSURANCE LEVEL	CLASSIFICATION
E	No effects
D	Sufficient protection against Minor Safety Effect due to IUEI
C	Sufficient protection against Major Safety Effect due to IUEI
B	Sufficient protection against Hazardous Safety Effect due to IUEI
A	Sufficient protection against Catastrophic Safety Effect due to IUEI

Table 1: Assurance Level Classification (RTCA-DO-326A)

Sufficient protection in the above table means that no single vulnerability capable of overcoming the security measures in place leading to catastrophic events is expected. This condition could be defined as Threat Safe System.

The Assurance Level to which a system has to be developed should be used to complement the standard software and hardware development processes adding security objectives not identified in RTCA-DO-178C and RTCA-DO-254 (which are, for instance the Security Functional Requirement of Common Criteria) and ensuring that they are developed and verified properly (through for instance the Security Assurance Requirement of the Common Criteria).

The analysis to assign DAL and AL are not directly linked, because the first is dealing with the safety of a system and the second with the security. However, in this approach, which is defined to ensure Security for Safety in Air Systems, in case for a given item or function of the Air System after the security risk assessment an AL A is assigned, the corresponding Function/Item DAL should not be less than A.

For instance, in the design process, an Item DAL A may be assigned to a Flight Control Computer, while an Item DAL C could be assigned to a Communication Computer. In case the Cyber Security Analysis Process herein described is carried out on this avionic architecture, it could be assessed that the communication system is more exposed to cyber threat that a Flight Control Computer (FCC) which is well segregated in the avionic architecture. For instance, the Cyber Risk Index is assessed as 2C (see Figure 15) for the communication equipment, while the FCC

is judged not sensible to cyber threats. To bring the system in the green area of the Cyber Risk Index Matrix, the AL should be raised of one level to AL B. Since the DAL cannot be less than the AL, also the DAL of the communication equipment should be B. In order to include in the development process specific security objects, the formal methodology of Security Functional Requirement and Security Assurance Requirement defined in ISO/IEC 15408 – "Common Criteria for Information Technology Security Evaluation Part 2/3" could be used, bearing in mind that they are not defined for Air Systems but for ITC system.
The final output of the Cyber Security Analysis Process (CSAP) is to reach a complete allocation, up at least to subsystem level (Item or Functional), of AL, DAL and CC EAL. To do so, an association between AL, DAL and CC EAL should be established as in Table 2. For each AL A, a proper EAL should be defined to include the applicable venerability assessment as defined in the Common Criteria. Figure 16 shows how the Assurance Level introduced applying customized Common Criteria can be seen as an additional layer of protection to functions and/or development items of Air Systems.

Item or Function	AL	DAL*	EAL **
#	X	Y	CC EAL Z

* DAL applicable for Item directly involved in the Cyber Security Analysis
** Common Criteria Evaluation Assurance Level

Table 2: Example of Equivalence AL, DAL, CC EAL

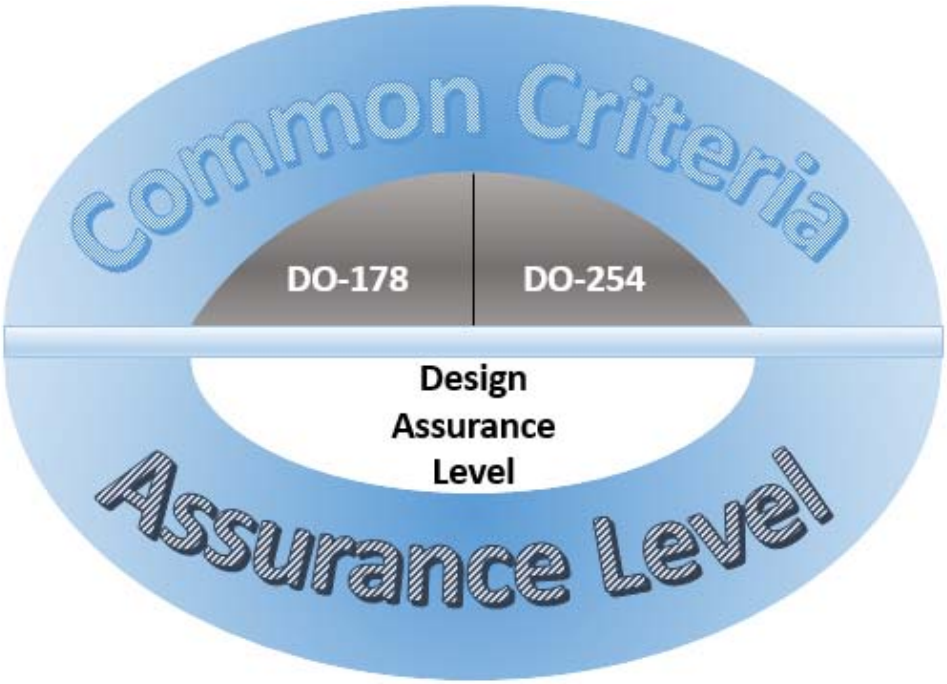

Figure 16: The Assurance Level as an additional security shield

S1.1.4. Common Criteria for Initial Airworthiness

The Common Criteria for Initial Airworthiness are defined below.

CCIA 1. Threat Safe

The equipment of an Air System shall be such that no single vulnerability, in case of attack, may lead to a catastrophic event.

CCIA 2. Airworthiness Security Process (ASP)

IUEI shall be considered in the design and development of Air Systems. RTCA-DO-326A and RTCA-DO-356 are the reference documents for the Airworthiness Security Process.

Any other proposed process to be used instead of the above documents shall be based on the following elements:

- Security Scope Definition
  The Air System and the interfaces to be analyzed shall be defined. All the interfaces shall be considered in the analysis, but some could be excluded from the security assessment providing the appropriate rationale. Any device that exchanges data with the avionic system shall be included in the analysis.

- Preliminary & Final Security Risk Assessment
  Once the Security Scope is identified, starting from the Threat Scenario (Intelligence Driven Approach) or from the Target Object (Engineering Judgement Approach), the preliminary security risk assessment aims to check for vulnerabilities and defining additional security requirements (to be developed in accordance with RTCA-DO-254 for hardware and RTCA-DO-178C for software) for all involved subsystems, whose effectiveness will be evaluate in the verification phase. Threat conditions should be taken into account in the safety analysis and in all phases of the system development process.

At minimum, the following security objects should be met:

- system security architecture is defined and explained;
- security requirements are defined, allocated to the different subsystems and traceable;
- vulnerability/penetration testing are defined and executed or, in alternative, formal requirements verification methods are used.

The above list may be expanded depending on the Air System characteristics. Moreover, specific security objects that can be addressed are:

- the Assurance Level for functional areas or items are defined;

- security objects have been mapped to Security Functional Requirements formally defined (the Common Criteria for Information Technology Security Evaluation Part 2 can be a reference).

In any case, during the Air System lifecycle, the Cyber Security Analysis Process should be considered as a standing process as well as the safety assessment process and the system development process.

CCIA 3. <u>Air System Architectural Design</u>

The Air System Architectural Design should take into account the IUEI and the IEMI. For the IUEI, a possible approach could be to design the avionic architecture using different layers of security in order to protect/segregate the safety critical areas. In Figure 17, the principle of security layers in an avionic architecture is depicted and summarized below:

- the safety critical equipment (especially Item DAL A and B) should be allocated in the most internal layer of the Air System;
- data bus with different scopes should be separated;
- in case a link between safety critical items and more security exposed/critical items could not be avoided, protection measures, where feasible, should be included such as:
  - data bus monitoring actions should be implemented to detect anomalies on the data bus transactions;
  - safety critical equipment should be protected even if it implies a reduction in the available functionalities (logically disconnecting equipment with anomalous behavior, providing information in the cockpit and so on);
  - security logs should be implemented for real time or post flight forensic analysis.

In any case, the Avionic Architectural Design should be assessed during the Cyber Security Analysis Process to prevent as much as possible by design the impacts of cyber threats on the safety of an Air System.

CCIA 4. <u>Criteria for Linked Ground Support Systems</u>

In case from the Cyber Security Analysis applied to the Air System, it is assessed that cyber threats (IUEI) may have effects on the Linked Ground Support Systems with potential impacts on Safety, the following criteria are applicable:

- the application software of the Ground Support Systems that may have direct impact on the safety of the Air Platform should be segregated; a dedicated Assurance Level should be assigned to the software component and it should be developed in accordance with RTCA-DO-278A “Guidelines For Communication, Navigation, Surveillance, and Air

Traffic Management (CNS/ATM) Systems Software Integrity Assurance" or equivalent.

- the following guidelines should be followed:
  - NIST SP800-53 – "Security and Privacy Controls for Federal Information Systems and Organizations";
  - ISO 15408 – "Information technology -- Security techniques -- Evaluation criteria for IT security";
  - ISO 27002 – "Information technology -- Security techniques -- Code of practice for information security controls".

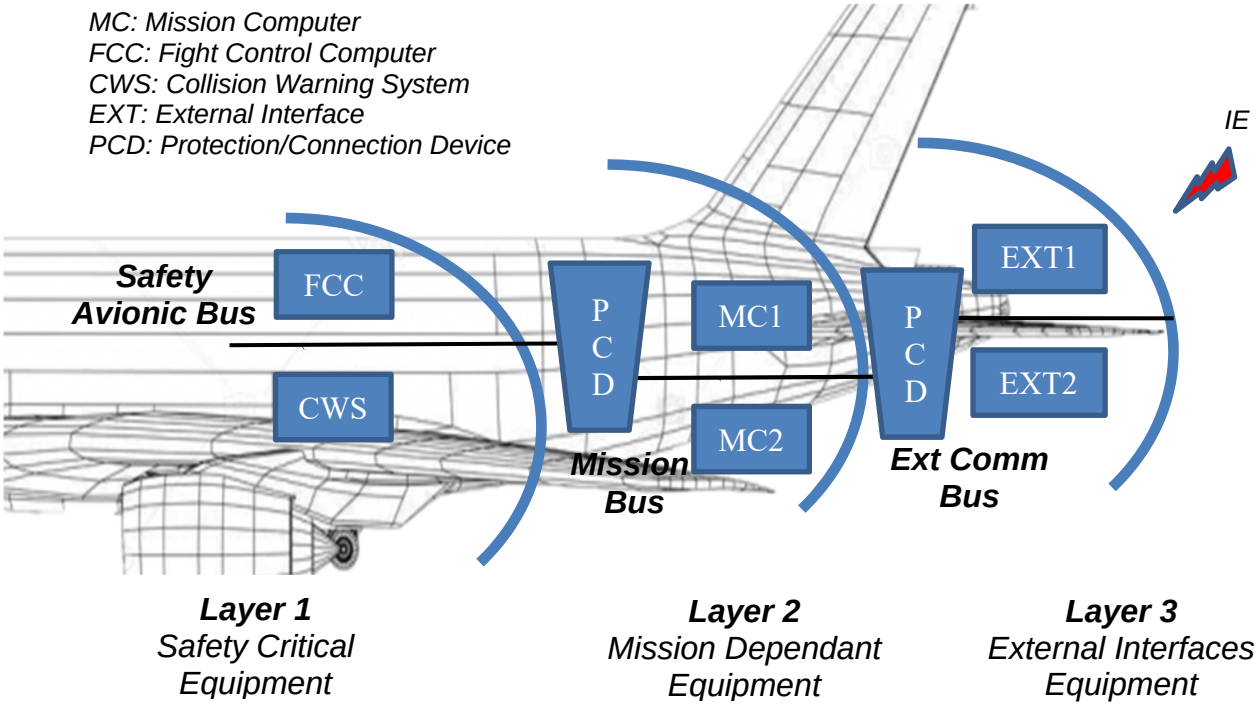

Figure 17: Security Layers in Avionic Architecture

CCIA 5. Additional Software Criteria

Additional criteria for the software are defined as follow:

- formal methods for the verification of the software are recommended depending on AL;
- software safety related requirements should be defined taking into consideration the IUEI; in particular, the security objects of the Common Criteria, there defined as Security Functional Requirements, for a given Assurance Level associated to a CC EAL as for Table 2 should be translated in software security requirements to be developed in accordance with RTCA-DO-178C;
- attention should be given in the verification process of dead code, deactivated code, derived requirements, field loadable software, user-

modifiable software, interface handler, specifically for the commercial one;

- the tools used in the development and verification phase should be qualified in accordance with RTCA-DO-330 “Software Tool Qualification Considerations”. The tools eventually used in the vulnerability assessment to be qualified should be listed in the Development Contract.
- Methodologies for formal development and verification should follow the recommendation provided in RTCA-DO-331 “Model-based Development and Certification”, RTCA-DO-332 – “Object-oriented Technology and Related Technique” e RTCA-DO-333 “Formal Methods”;
- Mechanisms to ensure the software integrity of each component of an Air System should be established to prevent that a system with compromised software may be active after the power up, reducing the issue due to a unsecure supply chain;
- For the field loadable data which include *Field Loadable Software e Software Parameter Data Items, Aeronautical Databases, User Modifiable Software (o Data), User Modifiable Security Data,* the following considerations apply:
  - Implication on Security for Safety should be considered;
  - Preventing security measures should be introduced in the loading phase;
  - Security Aspects included in RTCA-DO-356 related to software impairment, tool qualification and configuration management should be taken into account;
  - field loadable data such as Aeronautical database should be developed in accordance with RTCA-DO-202 - *Report Of Special Committee 159 on Minimum Aviation System Performance Standards (Masps) for Global Positioning System (GPS) and the data integrity checked.*

CCIA 6. <u>Additional Hardware/Firmware Criteria</u>

For the development of Field Programmable Gate Arrays (FPGAs), Programmable Logic Devices (PLDs) and Application Specific Integrated Circuits (ASICs), in addition to RTCA-DO-254, the following documents could be used:

- Simple Electronic Hardware and RTCA Document DO-254 and EUROCAE Document ED-80;
- Design Assurance Guidance for Airborne Electronic Hardware from Certification Authorities Software Team (CAST);

- As AMC the AC 20-152A “Development Assurance for Airborne Electronic Hardware (AEH)” defined in accordance with Notice of Proposed Amendment (NPA) 2018-09.

CCIA 7. Special conditions

Special conditions such as PS-AIR-21.16-02 – “Establishment of Special Conditions for Cyber Security” could be used to assess an external interface of an Air System.

CCIA 8. Solutions derived from Civil Aviation

For a MTC release, the certification of Civil Authority is usually endorsed. Concerning the Cyber Security for Air Systems, in order to harmonize the analysis of IP based communication solutions, the following document could be used:

- ARINC 882-1 “Aircraft/Ground IP Communication”;
- ARINC 822A “On-Ground Aircraft Wireless Communication”;
- ARINC Report 852 “Guidance for Security Event Logging in an IP Environment”.

S1.2. Continued Airworthiness

In order to ensure that an Air System is maintained cyber secure in its evolution, the Cyber Security Analysis Process (CSAP) or the Airworthiness Security Process (ASP) defined in RTCA-DO-326A shall be followed during the evolution of the Military Type Certification.
The chosen process shall be considered as an iterative cycle to be followed during the evolution of the Air System for the full lifecycle. Two main elements lead to the reinitiation of the security process after the MTC release:

- a change in the Air System that leads to an update of the MTC or an update of the configuration;
- a significant change in the Threat Scenario which modifies the security posture of the Air System.

In the first case, changes should be classified as defined in Table 3. In case of new equipment or significant modifications to the Air System Avionic Architecture, the Cyber Risk Index shall be updated and the Assurance Level for the new or modified items reassessed.
A Cyber Change Impact Analysis (CCIA) should be conducted. The analysis should be focused on understanding if the changes may introduce additional risks in order to assess the impact of the change on the security posture and to tailor, with respect to the modification, the part of the CSAP that should be redone.

Type of Change	Description
ΔCS	Change in Air Systems due to new equipment than may introduce additional vulnerabilities or jeopardize the security measures in place.
ØCS	Update of the Air System configuration without the introduction of new equipment that may require the need for a new vulnerability assessment.
0CS	Changes that do not affect the Security for Safety of the Air System.

Table 3: Security Changes Classification

In the second case, an analysis of the protection measures against the new threat defined by an updated Threat Scenario shall be carried out. A Threat Impact Analysis (TIA) should be conducted to evaluate the security posture of the Air System in the modified Threat Scenario. The TIA aims to understand the impacts of the new threats on the Security for Safety of the Air System. Once the new threat is well defined, a dedicated Penetration Test (PT) could be conducted to assess whether the system is secure enough or new security measures should be implemented.

Usually, a new threat does not change the defined Assurance Level, but may requires additional Security Requirements to be implemented and tested in accordance with the CSAP.

In case the introduction of additional security measures to face the updated threat scenario requires a change of the Air System, the classification and processes defined for the first case apply.

A balanced process is necessary to reach the optimum trade-off between the implementation of Updated Security Patches and the need to maintain the software/hardware assurance.

S1.3. Continuing Airworthiness

The RTCA-DO-355 “Information Security Guidance for Continuing Airworthiness” provides guidance for the operation, support, maintenance, administration and deconstruction of an Air System during its in-service lifecycle.

They are considered applicable security instructions to continuously ensure the Security for Safety of an Air System.

A Cyber Incident Management Process (CIMP) should be established to record and assess incidents due to a possible tentative of cyber intrusion as well as standard flight incidents are normally addressed in the DAAA regulation (see AER(EP).00_01_06 and peculiar Air System version). In case a cyber incident on an Air System has an impact on the Safety of Flight, the par 3.3 of AER(EP).P-2005 applies.

Cyber incidents due to new cyber threats or untested attack patterns should be considered as additional elements that activates the Cyber Security Analysis Process (CSAP) in a similar way as a significant change in the Threat Scenario does.

S2. SECTION 2 – PERFORMANCE ASSESSMENT

The performance of Air Systems is normally assessed in the Homologation Process to release the homologation certificate, so called COTAM (Certificato Omologazione Tipo Aeromobile Militare) or HMTC (Homologation Military Type Certificate). This document usually provides:

- an airworthiness statement that the system is Fit for Flight, within a proved envelope and with some limitations (if any);
- a performance assessment with respect to the requested functionalities defined in the Development Contract to state that the system is Fit for Purpose with a certain numbers of deviations (if any) that do not affect the Safety of Flight.

In Section 1, the Security for Safety aspects have been added to the airworthiness process to deal with IUEI and IEMI.
Consequently, the cyber threats are included in the certification process for the Safety for Flight of an Air System also in a Cyber Contested Environment, specified through the Threat Scenario.
In this section, a methodology is proposed to assess also the performance of an Air System with respect to the fulfillment of the cyber-security requirements in a Cyber Contested Environment. Being performance requirements usually defined in a Development Contract, the methodology could be applied in case they are properly defined.
In the AER(EP).P-6, on the basis of Joint Service Specification Guides (JSSG), the common requirement areas to be included in a Development Contract and in its specification parts are reported, but they do not include cyber aspects.
Therefore, this section provides:

- a proposal for possible cyber-security requirements to be included in a Development Contract;
- possible Cyber Key Performance Attributes (CKPA) and Cyber Key Performance Indicators (CKPI) to be used in the assessment;
- a resilience assessment methodology, which consists in evaluating the grade of performance achievable by a system and its intended functions when cyber threats are present.

S2.1. Cyber Performance Requirements

The Performance Assessment of an Air System against cyber threats may be performed in different ways. Two possible methodologies are defined in the following paragraphs:

- the first is based on the Lockheed Martin Cyber Kill Chain[1];
- the second is based on the Security Layer Protection approach.

[1] www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

These are only two of the possible solutions to define requirements for the different phases of a cyber attack.
It is important to differentiate requirements applicable for each phase of an attack looking at its role in the defensive chain. This approach helps in the definition of the Cyber Key Performance Indicator.

S2.1.1. Cyber Kill Chain approach

The methodology proposed in this section is based on the description of the cyber performance requirements against each phase of the Cyber Kill Chain defined in Figure 2.
The actions that an Air System may implement to face a cyber attack are divided in:

- preventive actions: they are based on detecting the threat, denying access to the system, disrupting any potential intrusion;
- responsive actions: they are usually taken once the threat has been delivered. They aim is to degrade to an acceptable level the possible effects of the threat, deceive the threat to protect the real target and destroy the threat where applicable.

Figure 18 shows the relation between possible actions to be taken in each phase of a cyber attack and the status of impairment of an Air System.
To assess the performance of an Air System, cyber requirements should be defined for each element of the matrix reported in Table 4 where considered necessary in accordance with the Threat Scenario.
General requirements that can be considered are:

- hardening of the attack surface (looking at the perimeter of the System defined in the Target Scope) enforcing encryption, authentication, security standards and so on;
- monitoring access points analyzing data traffic by means of intrusion detection system or other systems;
- logging data traffic for possible analysis (real time monitoring or post flight forensic analysis).

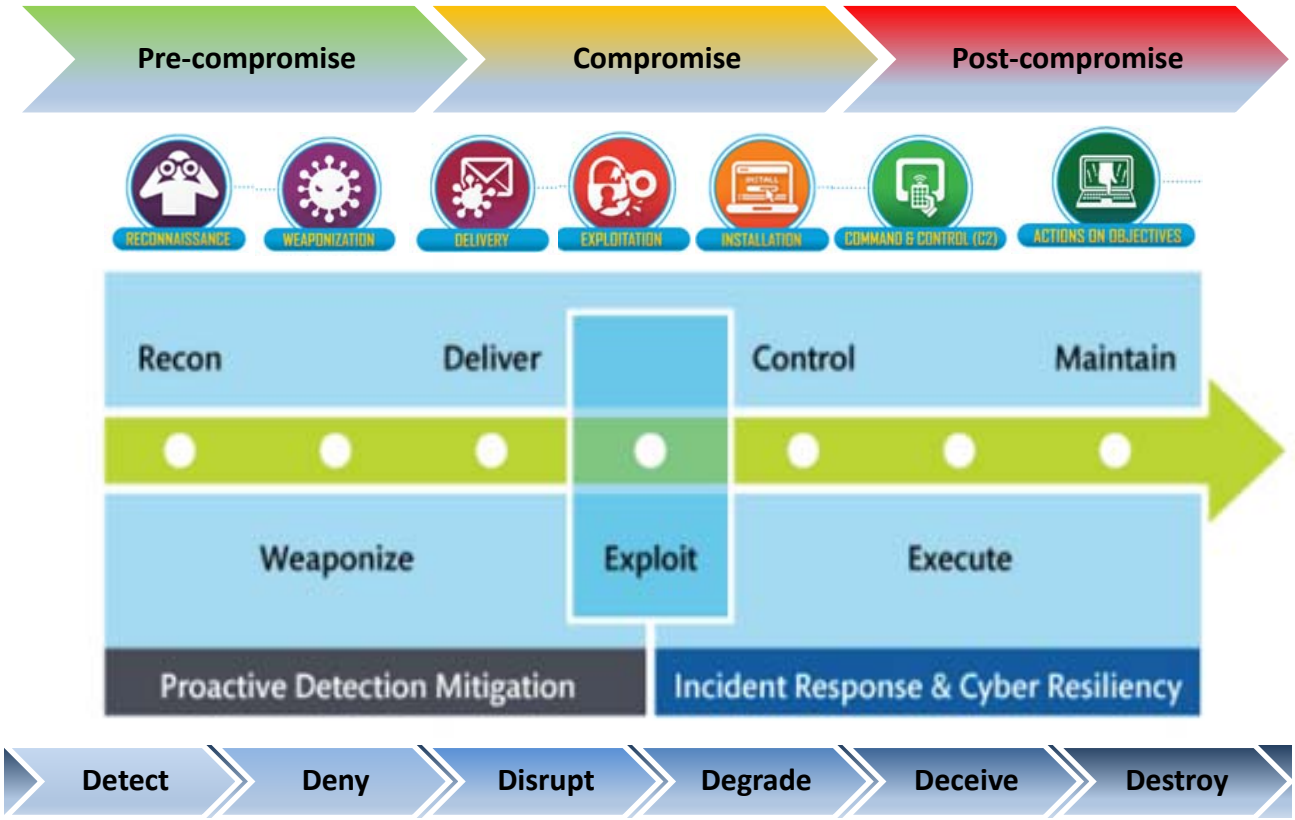

Figure 18: Air Systems actions for each Cyber Kill Chain Phase

Requirements may be allocated to functional areas or items that are considered more exposed on the basis of the Cyber Security Analysis Process defined in Section 1 and that have the higher Assurance Level. Potentially, the matrix shown in Table 4 should be filled for each system (equipment) that has been assessed as sensible from a security point of view.

Cyber Kill Chain Phases	Defenders Requirements					
	Preventive Actions			Responsive Actions		
	Detect	*Deny*	*Disrupt*	*Degrade*	*Deceive*	*Destroy*
						
						
						
						
						
						
						

Table 4: Defenders Process arrayed against Cyber Kill Chain

S2.1.2. Security Layer Protection approach

The second method aims to progressively develop and maintain a capability to defend the air system against the cyber threat by defining four layers of protections:

- Prepare: assess the air system cyber risk posture and design/develop the weapon system taking into account cyber management process to identify and remediate vulnerabilities;
- Protect: monitor the air system status and implement controls (security measures ad procedures) to prevent unauthorized access;
- Detect: capability to identify suspicious activity that can unveil a cyber threat, discovering that the system is infected and/or a cyber attack has been initiated;
- Defend: respond to a suspicious activity isolating the threat, mitigating the damage, blocking the attack and restore, where possible, the system standard behavior.

An alternative Cyber Kill Chain could be defined looking at the seven steps of successful cyber attack[2]:

[2] www.resources.infosecinstitute.com/the-seven-steps-of-a-successful-cyber-attack

1. Reconnaissance: Attackers first identify a vulnerable target (eg. interface or person) and explore the best ways to exploit it.
2. Scanning: Identify / scan for weak entry points that allow the attackers to gain access. This step can last months.
3. Access and Escalation: Attacker gains access through the weaknesses identified in the target and then escalates access privileges so that the attackers can move around freely.
4. Exfiltration: Attackers move around the network, access systems and gather /manipulate data at will.
5. Sustainment: Attackers secretly install malicious programs that enable attackers to return as frequently as they want with elevated privileges.
6. Assault: Attackers alter or disable the functionality of the victim's hardware. Attackers have already effectively taken control, so it's generally too late for the breached organization to defend itself.
7. Obfuscation: Attacker takes steps to confuse, disorientate and divert the forensic examination process.

7 Steps of Cyber Attack	**Defenders Requirements**			
	Prepare	***Protect***	***Detect***	***Defend***
Reconnaissance				
Scanning				
Access and Escalation				
Exfiltration				
Sustainment				
Assault				
Obfuscation				

Table 5: Defenders Phases arrayed against the 7 steps

S2.2. Cyber Key System Attributes and Cyber Key Performance Indicators (CKPI)

Once cyber requirements of an Air System are defined, in order to assess its performance in dealing with cyber threats, it is recommended to identify those key attributes and parameters that, when not attained, will be detrimental to the mission. The attributes are qualitative in nature while the performance indicators are quantitative, and could be expressed in terms of threshold and desired levels. They could be established for a given Threat Scenario and monitored to continuously evaluate the level of the security posture in an evolving Threat Scenario. Possible CKPIs are:

- Frequency of security updates;
- Number of known vulnerabilities;
- % of undetected attacks;

- % of effectiveness of preventive actions;
- Time for detecting an attack;
- Compromising level of the attack;
- Time to recover from an attack (i.e. to reach back the capability to perform intended function safely);
- Number of incident with Flight Safety implications;
- Capability to perform the intended function under attack.

In each Development Contract, CKPIs should be defined to be able to assess the system behavior with respect to cyber threats. Obviously, the performance assessment is related to the tested scenario and it may changes. However, it is the only available solution to assess the Cyber Resilience Performance.

S2.3. Cyber Performance Assessment

The definition of the cyber requirements and the CKPIs is fundamental for the Cyber Performance Assessment Process. In order to qualify the cyber performance of an Air Systems during the qualification process the agreement on an envisaged/ supposed or known Threat Scenario in required.

The Threat Scenario should be specified in terms of selected threats and attack patterns and the effectiveness of security measures should be evaluated. The requirements defined in the technical specification should be verified and the selected key performance indicators measured to assess the level of compliance.

Ideally, where the conditions allows and a dedicated team of cyber experts is available, a penetration testing should be carried out to finally assess the overall system cyber security posture and related performance.

S3. SECTION 3 – MISSION ASSURANCE

In line with SMA-PIANI-239, which is the Italian Air Force Policy for integrating the Cyber Domain in the Air Operations, the Italian Official Test Centre (IT-OTC) – Reparto Sperimentale di Volo has been identified as the Organization responsible for conducting “Cyber Operational Test and Evaluation for Air Systems” in order to support the Italian Air Force in the Cyber Avionics domain. For this reason, this section has been developed in conjunction with IT-OTC and aims to define the main principles and processes needed to conduct a mission assurance evaluation, which can be defined as the assessment of the suitability of an Air System to perform its mission in a Cyber Contested Environment.

S3.1. Cyber in the Operative Scenario

The evaluation of the mission assurance for a military Air System requires a different vocabulary with respect to the discussion related to the Security for Safety of the Airworthiness Section. In the Airworthiness section, cyber threats were distinguished in IUEI and IEMI, while this section will use the term Offensive Cyber Weapon (OCyW), defined in the Italian Joint Integrating Concept JIC-012 directive as the deliberate use of cyber weapons against military objectives within a military operations area.

The OCyW operations include enabling activities in the EM domain called Cyber EM Activities (CEMAs). There are many interpretations of what Cyber EM Activities (CEMAs) are. In this document, Cyber EM Activity (CEMA) could be defined as an electromagnetic activity that, when coupled with an Air System equipment, is able to modify the expected system behavior inducing malfunctions. IEMI is an extension in the air domain of the Offesive Cyber Weapon using the EW spectrum.

Considering the possible effects of the Cyber Operations on different domains (see Figure 19), the limitations of the approach provided in this section are:

- Cyber EM Activities (CEMAs) are not addressed;
- only effects the Physical and Digital domains are partially evaluated.

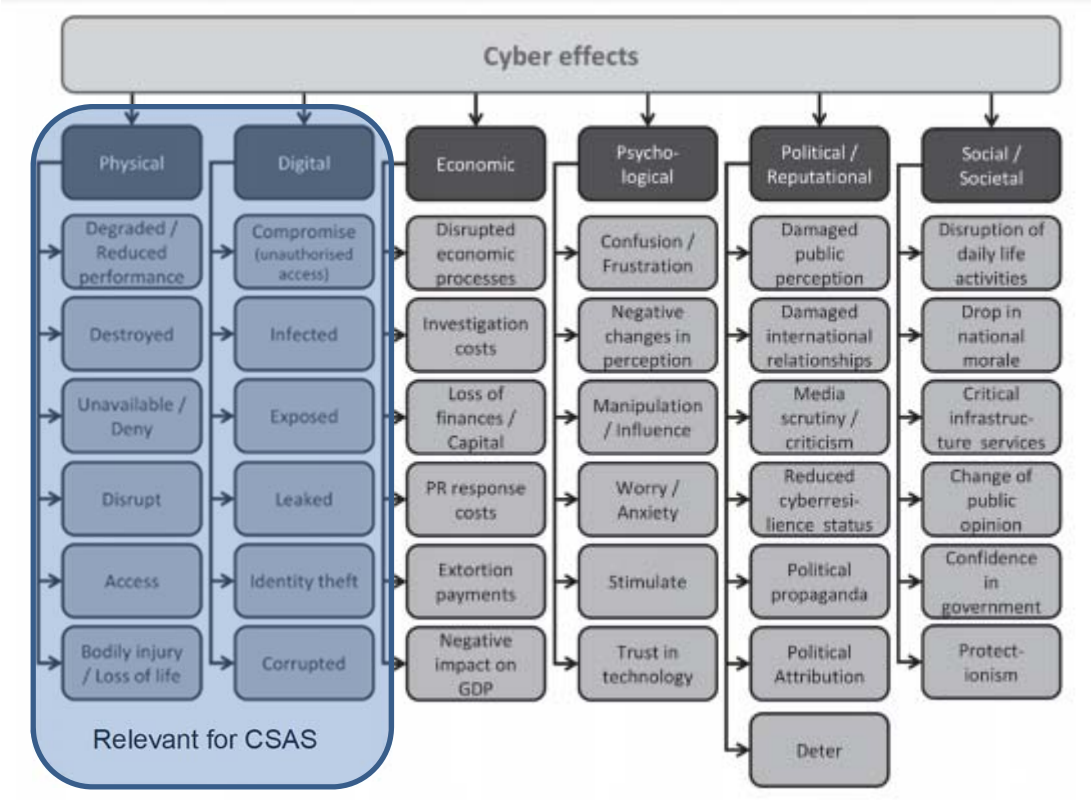

Figure 19: Cyber effects of Cyber Operations in the military world

S3.2. The Holistic Approach

A holistic approach for a Mission based Cybersecurity Risk Assessment is reported in Figure 20 as described in the US DoD Cyber T&E Guidebook.

This holistic Cyber Test & Evaluation approach may be considered as reference for Mission assurance approach. In the following paragraphs, the principles of a process that may be followed are provided.

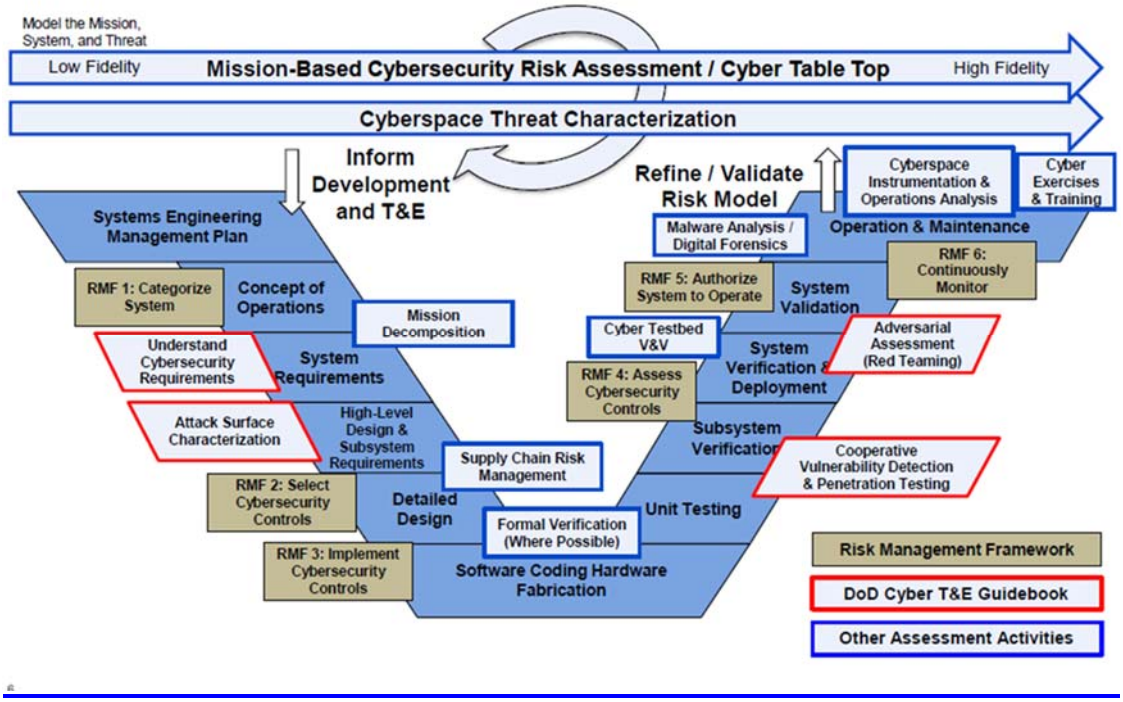

Figure 20: Mission-based Cybersecurity Risk Assessment

S3.3. Mission Assurance and Classified Information

In Section 1, the difference in the approach between the INFOSEC and CSAS has been established. Besides the attributes traditionally evaluated (Availability, Confidentiality, Integrity), the mission impact of a successful attack shall be considered.

Hence, for a military platform the ability of assuring the mission is the reference for the proposed process. Furthermore, the assurance of Information Security is not a responsibility of DAAA in accordance with the Italian Law.

The steps needed to perform a Mission Assurance Process (MAP) are:

- Establish Mission Needs;
- Identify Mission Critical Capabilities;
- Assess Cyber Mission Impacts;
- Perform Cyber Mission Risk Remediation Analysis.

In performing the aforementioned steps, a general security guideline for the deliverables/topics in the process could be considered as follow:

- UNCLASSIFIED level
  - The need for cyber resilient products and services;
  - Generic cyber security / resilience topics and questions already in the public domain (incl. Common Vulnerabilities and Exposure - CVE register);
- RESTRICTED level (would be detrimental)
  - General cyber-attack motives;
  - Processes, approaches and methods used to assess cyber vulnerabilities;

- Specific cyber problem space boundary / context diagrams (no priorities)/ Security Scope;
- Cyber security/resilience strategies, general requirements and applying cyber ”best practice”;

- CONFIDENTIAL level (would lead to damage)
  - Assessment of specific threat information;
  - Selected scope / priorities on which to focus as primary cyber concern
  - Specific cyber security / resilience technical requirements and their performance;
  - Effectiveness of the existing security measures;
- SECRET level (would lead to severe damage)
  - Specific cyber vulnerabilities, their attack vectors and their potential effect.

This guideline is for reference only and shall be amended as necessary in the Project Security Instruction (PSI) relevant to the specific platform.

S3.4. Air Systems Cyber Mission Assurance Process

The Mission Assurance Process for Air Systems is derived from the MITRE’s cyber Mission Assurance Engineering (MAE); it has been customized to include the peculiarities of avionic systems.

Figure 21: Air Systems Cyber Mission Assurance Process

As depicted in Figure 21, the phases of the Air Systems Cyber Mission Assurance Process are:

- Establish Mission Needs: to define what has to be done for the success of the mission and what is needed for each phase of the mission, identified as mission contributor;

- Identify Mission Critical Capabilities: to understand which are the systems that are really needed for the success of the mission;
- Analyze Cyber Threat Mission Impact: to understand how Cyber Threats could affect the mission through the analysis on how the cyber threat could cause a malfunction in the critical systems identified before. It requires the threat scenario and the level of threat understanding together with a cyber operational assessment on these capabilities.
- Cyber Mission Risk Remediation Analysis: to understand the risks on the mission, and to define acceptance criteria and mitigation actions to be within the acceptable criteria.

The first two phases have as output the identification of the critical systems or functions, depending on the granularity of the analysis, and of systems functions for each Mission Need, as identified in Table 6. In the following examples critical system are considered, but similarly to the distinction between Item DAL and Functional DAL as in ARP4754, the same approach could be applied at functional level.

Mission contributor	**Mission Needs**								
	Capability 1			**…**			**Capability N**		
	System 1	System 2	System 3	…	…	…	System 1	System 2	System 3
A	A1.1								
B								B.N.2	
C			C1.3						
…									

Mission Critical Capabilities

Table 6: Critical systems for each Mission Type

Regarding the third step, in order to analyze the impact of the Cyber Threat on the mission, the following aspects should be taken into account:

- Threat Scenario with associated threat level;
- Existing vulnerabilities of the critical systems;
- Design characteristics of the critical systems (i.e. assurance level or contribution to the Cyber Index of the systems, security measures).

In order to analyze the impact on the mission, the first step is to define the possible impact on the mission. In this document, the definitions reported in Table 7 applies.

IMPACT ON THE MISSION	DESCRIPTION
MISSION ABORT	The Air Platform is impacted in such a way that the capability needed to conduct the mission are not anymore available so the objective of the mission is impossible to achieve
MISSION HIGHLY DEGRADED	The Air Platform is impacted in such a way that the capabilities needed to conduct the mission are seriously affected so the objective of the mission can be achieve not at 100% with high risk and high compensation
DEGRADED	The Air Platform is impacted in such a way that the capabilities needed to conduct the mission are seriously affected so the objective of the mission can be not at 100% achieve with serious risk and significant compensation
MINOR	The Air Platform is impacted in such a way that the capabilities needed to conduct the mission are partially affected so the objective of the mission can still be achieved with acceptable risk and possible compensation
NO IMPACTS	The Air Platform is not impacted by the Cyber Threat

Table 7: Mission Impact Level

Once the critical systems are identified, for each threat of the threat scenario, it should be assessed the Level of Impact on the mission of each critical system previously identified. Table 8 provides an example.

CRITICAL SYSTEMS	Impact of THREAT_NAME			
	MISSION IMPACTS			
	ABORTED	HIGLHY DEGRATED	DEGRADATED	MINOR
A.1.1	X			
C1.3		X		
B.N.2			X	
…	…	…	…	…
X.Y.Z				X

Table 8: Impact Matrix Critical System vs Cyber Threat

To simplify the approach and to base the assessment against the Threat Level instead of each single cyber threat, the different Cyber Threats could be grouped. Table 9 provides an example of four levels grouping.
To indicate the level of susceptibility of a given system to a cumulative type of threats identified by a threat level, the number of threats belonging to a certain level can be summed up.
The histogram in Figure 22 provides a clear picture of the susceptibility of each critical system with respect to the threat level.

The Cumulative Cyber Threat Capabilities Impact Assessment (Figure 22) provides an overall view of the number of threats of a given level that have an impacts on the critical systems identified.

THREAT LEVEL	Possible PARAMETERS*			
	Know-How Attacker	**Know-How Of The Air Systems**	**Connection To Supply Chain**	**Level of access to system information**
A	persistent, stealthy, and sophisticated attack by advanced threat actors, also known as advanced persistent threat (APT)	Experience with the System Under Test (e.g. access to former employees)	High	Up to secret
B	Autonomous groups with high skill to use 0-day and develop dedicated attacks	Experience with avionic systems or information from insiders	Medium to High	Up to Restricted
C	Reverse engineering, exploitation and hostile code development	Low	Medium to Low	Up to For Official Use Only
D	Use only of info of public domain (*tools and exploit)*	Very Low	Low	Unclassified

Table 9: Threat Levels

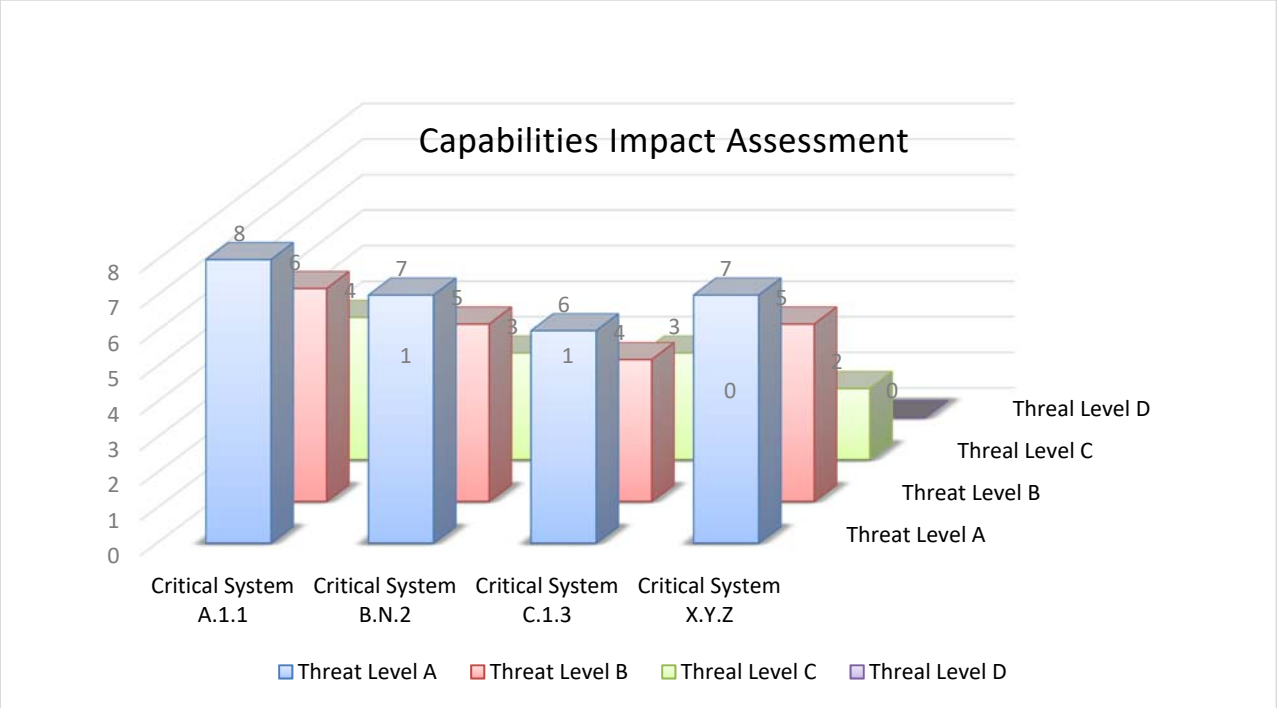

Figure 22: Cumulative Cyber Threat Capabilities Impact Assessment

Once it is clear the cumulative impact on a given system due to threats of a given level, a Mission Cyber Risk Index could be defined (Figure 23). This index identifies the risk level of a mission in the given Cyber Contested Environment due to the vulnerability of the critical system under evaluation.
The spider diagram in Figure 24 reports the number of risks (from 1A to 4D) for each critical system. To each risk level (1A to 4 D) a different subjective weight could be assigned (depending on the assessor) to define a different scale in each line of the spider diagram.
The area of the spider diagram provides the overall mission risk for each critical system. Remediation activities could reduce the mission risk.
Summing up the areas of the spider diagrams for each critical system, the overall Mission Risk for the Air System could be computed.
Weights and numbers could be established by the assessor depending on its operative experience and system knowledge.

Mission Cyber Risk Index (MCRI) *Threat Level vs Mission impact*	(1) ABORTED	(2) HIGHLY DEGRATED	(3) DEGRADATED	(4) MINOR IMPACTS	NO MISSION IMPACT
A	1A	2A	3A	4A	No MISSION Impact
B	1B	2B	3B	4B	
C	1C	2C	3C	4C	
D	1D	2D	3D	4D	
E	1E	2E	3E	4E	

Figure 23: Mission Cyber Risk Index Matrix for each Critical System

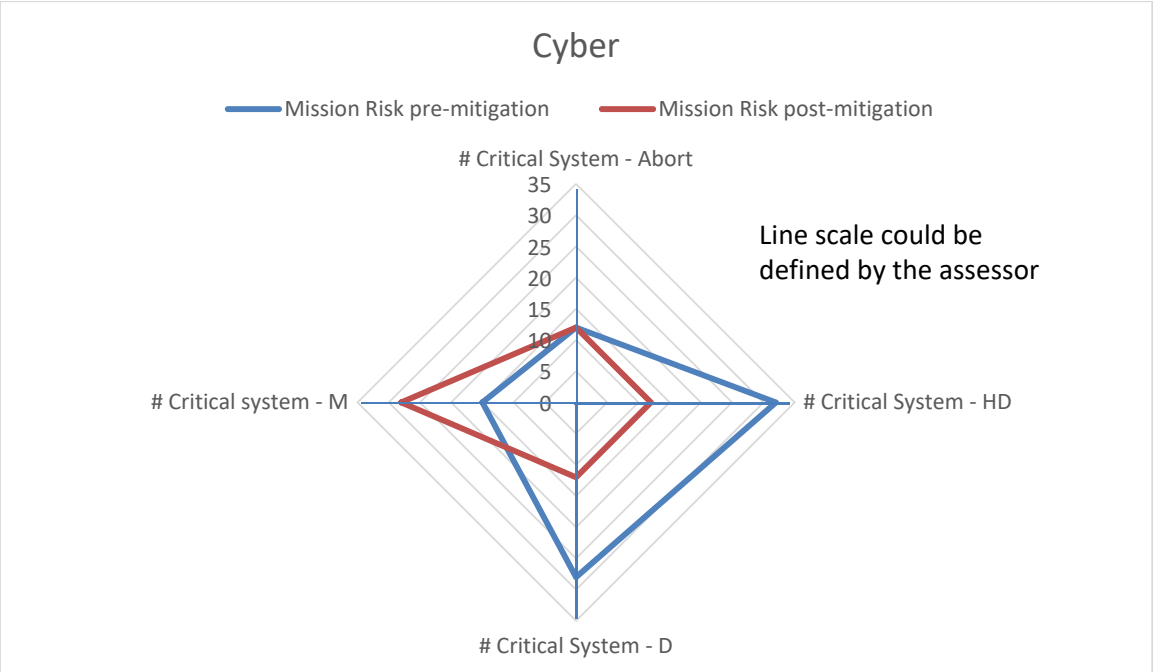

Figure 24: Mission Risk for a given Critical System - Spider Graph

S3.5. Link to Airworthiness Security Process

The Airworthiness Security Process is focused on understanding the implications of Cyber Threats on the airworthiness characteristics of an Air System. The need to ensure security implementing additional requirements is synthetized through the definition of a Cyber Risk Index, which it is fundamental to explain the need for the creating a criteria to ensure security, named Assurance Level.

The Mission Assurance Process is focused, instead, on understanding the implication of a cyber threat on the capability to conduct the assigned mission. It includes for sure the airworthiness aspects (in order to accomplish the mission an Air System should be first Fit for Flight), but embraces a capability assessment of the equipment needed to accomplish the mission. The different equipment may be categorized and in accordance with their impact on the mission and a similar Mission Cyber Risk Index could be defined. In this case, different scales of acceptability could be defined with respect to the airworthiness criteria. The two processes are deeply interlinked: once an equipment has been identified as critical for the accomplishment of the mission, it may be desired to elevate the level of assurance required to protect the equipment in a given Cyber Contested Environment. Therefore, a different Assurance Level with respect to the one defined at the end of the Airworthiness Security Process could be assigned to enhance the capability of the equipment to keep working, ensuring the achievement of the mission in case a cyber-attack is conducted. Linking these two processes may imply an increasing numbers of equipment with ah higher Assurance Level in order to ensure simultaneously both the airworthiness characteristics and the capability to successfully accomplish the mission.

Annex A: Cyber Risk Index

This annex aims to provide an example of a cybernetic risk analysis methodology applicable to different types of aircraft and to different approaches by providing a formal method for the characterization of the elements involved, with particular reference to the threat probability level. This last aspect is of particular relevance as there is no shared and universally applicable methodology in the literature. However, the formalization of a method applicable to different contexts is the indispensable prerequisite for descending considerations in the field of cyber security.

The RTCA-DO-326A, for example, proposes an approach based on the level of reliability of the population (potential attackers) and considers several factors that can contribute to determining possible metrics; it is particularly applicable to airline aircraft that provide network services and is recommended by the FAA for aircraft with more than 19 passengers, but is generally considered difficult to extend to different types of aircraft.

The analysis of cyber risk is aimed at defining the Cyber Risk Index, which is a matrix that considers the level of probability of the threat and its impact in terms of safety. Once the Cyber Risk Index has been defined, it is possible to assess the acceptability of the risks deriving from a given threat scenario and define the Assurance Level necessary for the development of the specific components involved in the threat scenario, so as to ensure the necessary guarantee in the management of the security requirements. The level of impact of a threat can be defined by categorizing the threat condition as catastrophic, critical, major, minor and of no effect. Table 10 provides a detailed description of the various categories. Probability levels, on the other hand, can be defined as:

P_E=*Unlikely;*
P_D=*Remote;*
P_c=*Occasional;*
P_B=*Likely;*
P_A=*Frequent.*

The probability level can be calculated according to innumerable approaches. Below, a formal method is proposed, available in the literature, based on 2 elements: Attacker Capability and Level of Exposure for an assessment of the probability through a two-dimensional matrix. This example can be extended to *n* elements for a characterization of the *n*-dimensional probability level. Considering the two-dimensional example, as far as the level of probability is concerned, the Attacker Capability can be defined as the set of *n* qualitative attributes:

$X=[X1,….Xn].$

CATEGORY	DEFINITION FOR AIRCRAFT WITH PILOT ON BOARD	DEFINITIONS FOR REMOTE PILOT AIRCRAFT (APR)
CATASTROPHIC (CAT. 1)	Threatening condition that could cause the loss of the aircraft or part of it or the death of one or more people. Threat condition that could lead to fatal injury due to operators' aircraft during ground operations.	Threat conditions that are expected to lead to uncontrolled flight conditions (including flight out of areas and / or planned flight profile) and / or uncontrolled crashes. Threat conditions that can result in the death of crew members or ground staff.
HAZARDOUS (CAT. 2)	Threat condition that could cause serious damage to one or more aircraft systems or serious injury or malaise of one or more people. This condition could include a large reduction in safety margins or functional capabilities. This condition could result in a state of physical discomfort and / or a high increase in workload for the crew such as to compromise the complete and accurate performance of the tasks related to the conduct of the flight.	Threat conditions that, either in themselves or combined with increased crew workload, are expected to lead to a flight termination with a controlled trajectory or forced landing that potentially leads to the loss of the APR, where it is reasonably expected to cannot cause the death of any person. Conditions of threat for which it is reasonably expected that it will not cause the death of any person of the crew or ground staff.
MAJOR (CAT. 3)	Threat condition that could cause slight damage to one or more aircraft systems or slight injury or malaise of one or more people. This condition could include a significant reduction in safety margins (e.g. detectable loss of redundancy) or functional capabilities. This condition could lead to a significant increase in the workload of the crew.	Threat conditions that, either in themselves or combined with an increased workload of the crew, are expected to lead to an emergency landing of the APR at a designated site, where it is reasonably expected that it will not cause serious injury to no one. Threat conditions that could potentially result in injuries to crew or ground staff.
MINOR (CAT. 4)	Condition of threat that does not cause significant damage to safety to any aircraft system and no injury or discomfort to people. This condition could include a slight reduction in safety margins or functional capabilities. This condition could result in a slight increase in crew workloads.	Threat conditions that do not significantly reduce the security of the APR system and imply actions on the part of the crew that easily return to their abilities. These conditions could include a slight reduction in safety margins or functional capabilities. Such conditions could result in a slight increase in crew workloads

Table 10: Impact category for Threat Condition

Some possible attributes could be:

X_1 = attacker experience,
X_2 = system know how,
X_3 = usable means, etc.

Each attribute of qualitative type X_i can assume m values $[X_i^1 \ldots . X_i^m]$ with X_i^j more critical than X_i^{j-1}.
To define a metric, each qualitative type characteristic can be associated with a quantitative characteristic $x_i^j > x_i^{J-1}$.
Depending on the type of cyber scenario, security analysts can define an evaluation function f_A to assign a specific value a_i to each qualitative attribute X_i, ie:

$$a_i = f_{Aj=1}^{m}(x_i^j)$$

The Attacker Capability can be expressed as the normalized sum of the assigned values all the attributes.

$$A = \sum_{i=1}^{n} \left(\frac{a_i}{x_i^m} \right), x_i^m \geq x_i^j, \forall i = 1 \ldots n, \forall j = 1 \ldots m$$

Similarly, the System Exposure Level can be defined as the set of n qualitative attributes that characterize it

$Y=[Y_1, \ldots . Y^n]$.

Some possible attributes could be:

Y_1 = type of architecture,
Y^2 = presence of vulnerability,
Y^3 = presence of safety mechanisms, etc.

As in the previous example, each qualitative attribute Y_i can take m values $[Y_i^1 \ldots . Y_i^m]$ with Y_i^j more critical than Y_i^{j-1} and for each qualitative type characteristic, a quantitative characteristic $y_i^j > y_i^{J-1}$ can be associated 1.
Depending on the type of cyber scenario, security analysts can define an evaluation function f_E to assign a specific value e_i to each qualitative attribute Y_i, ie:

$$e_i = f_{Ej=1}^{m}(y_i^j)$$

The *Exposure Level* can therefore be expressed as the normalized sum of the assigned values, all the attributes.

$$E = \sum_{i=1}^{n} \left(\frac{e_i}{y_i^m} \right), y_i^m \geq y_i^j, \forall i = 1 \ldots n, \forall j = 1 \ldots m$$

The level of probability can be obtained by combining the occurrences of the Level of Exposure and Capability of an Attacker according to the following table:

		ATTACKER CAPABILITY				
	VALUES	VERY LOW	LOW	MEDIUM	HIGH	VERY HIGH
EXPOSURE LEVEL	VERY LOW	P_E	P_E	P_D	P_C	P_B
	LOW	P_E	P_E	P_D	P_C	P_B
	MEDIUM	P_D	P_D	P_C	P_B	P_A
	HIGH	P_C	P_C	P_B	P_A	P_A
	VERY HIGH	P_B	P_B	P_A	P_A	P_A

Table 11: Threat Condition probability level

Once the probability level has been defined as well as the impact on safety, similarly to the failure conditions, the cyber risk matrix (Cyber Risk Index) can be determined as follows, always taking into account that individual vulnerability points are not allowed:

Cyber Risk Index (CRI)	(1) CATASTROPHIC	(2) HAZARDOUS	(3) MAJAOR	(4) MINOR	No effect on safety
(A) FREQUENT	1A	2A	3A	4A	No effect on safety
(B) MOST LIKELY (PROBABILE)	1B	2B	3B	4B	
(C) OCCASIONAL	1C	2C	3C	4C	
(D) REMOTE	1D	2D	3D	4D	
(E) IMPROBABLE	1E	2E	3E	4E	

Table 12: Cyber Risk Index

For each Threat Scenario (TS), based on the methodology described, it is possible to define the risk acceptability level and the required Assurance Level (AL), using the following table:

TS	*Attacker Capability*						*Level of Exposition*						*Likelihood*	*Impact*	*Acceptable*	*AL*
	a_1	a_2	a_3	a_4	a_5	*A*	e_1	e_2	e_3	e_4	e_5	*E*				
1																
2																
3																
…																
n																

Table 13: Risk acceptability matrix for each threat scenario

Assurance Levels are defined as follows:

ASSURANCE LEVEL	CLASSIFICATION
E	No effects
D	Sufficient protection against Minor Safety Effect due to IE
C	Sufficient protection against Major Safety Effect due to IE
B	Sufficient protection against Hazardous Safety Effect due to IE
A	Sufficient protection against Catastrophic Safety Effect due to IE

Table 14: Assurance Level Classification

The term "sufficient protection" refers to the result of the Risk Assessment and requires that there are no single vulnerabilities that can compromise all countermeasures and cause a significant safety event.

The level of impact in general is not changed, since it is proper to the threat condition. In the proposed simplification model, to mitigate the risk, it is possible to act on the level of probability, especially relative to the level of exposure (additional security measures), considering that the capabilities of the attacker can be considered stable.

Therefore, if the probability level calculated with the previous method is such that one is in the red zone of the Cyber Risk Index matrix, the required Assurance Level is relative to the level of protection that must be guaranteed based on the possible impact as reported in table 3

If, on the other hand, you are in the green zone, the required assurance level is the one related to no effect, or E.

The methodology is applicable both whether the risk assessment parameters are available from the intelligence or in the case of estimates based on analytical assessments.

A possible reference for assessing levels of exposure and vulnerability is available at: http://cwe.mitre.org/data/index.html, where the main Common Vulnerability and Exposure are published.

Using the Cyber Risk Index it is possible to define, as for the software, an Assurance Level that must be guaranteed in the development and implementation of the

requirements, especially for the safety requirements. This approach can be considered sufficient to consider the impacts of IEs on safety aspects.
By defining appropriate metrics, at each risk it would also be possible to define a Priority Risk Number (PRN) to identify the priority in defining any countermeasures.
A possible further approach, to be expanded for the different types of aircraft, can lead to the extension of the Guidelines to Define the Quantitative Requirements reported in AER(EP).P-6 in order to take into account the impact of IEs on safety aspects.
The Cyber Risk Index matrix is similar to the Hazard Risk Index matrix, in fact the definition of the impact categories changes because the threat conditions are considered instead of the failure conditions.
To take account of threat conditions in the cumulative probability of catastrophic event per flight hour, a possible approach is to consider that IEs can contribute to increasing the NEC, defined as the expected number of catastrophic events for the type of aircraft.
Catastrophic events can therefore be determined not only by failure condition but also by threat condition.
The types of analysis illustrated above should allow determining the number of catastrophic threat conditions downstream of the analysis, but a reference or technical rationale is not currently available that will allow the preliminary determination of the Number of Catastrophic Event (NEC). In this case, an engineering judgment can be carried out based on the number of critical software / firmware components, type of connections, operating environment of more or less dense use of cyber threats, threat level, capacity needed to perform certain types of attacks, historical series of attacks on certain types of aircraft, etc.
NEC values by type of aircraft that can be used in the absence of statistical data depending on the type of aircraft and operating environment are shown in Table 15.

Likelihood Levels	**Assumed N_{EC}**	**Additional N_{EC} value for IE**
(S1) Airplanes in the "Normal", "Utility" and "Acrobatic" categories with single reciprocating engine and weight <6000 lb	10	+5%
(S2) Airplanes in the "Normal", "Utility" and "Acrobatic" categories with more than one alternative engine or single turbine engine and weight <6000 lb (S2) Helicopters with a weight ≤20000 lb and a number of passengers <10	10	+5%
(S3) Airplanes in the "Normal", "Utility" and "Acrobatic" categories with weight ≥6000 lb	50	+5%
(S4) Airplanes in the "Commuter" category (S4) Airplanes of the “Large Aircraft” category (S4) Helicopters of the “Large Rotorcraft” Category with weight> 20000 lb and any number of passengers or ≤20000 lb and a number of passengers ≥10	100	+10%
(S5) Aircraft of the troop transport and rescue category, reconnaissance aircraft, maritime patrol vessels, for in-flight refueling, for Electronic Warfare missions, etc.	100	+15%
(S6) Combat aircraft, training aircraft, etc.	100	+15%
(S7) APR MTOW< 15 kg	10	+5%
(S8) APR 15kg ≤ MTOW <150 kg	10	+5%
(S9) APR 150 kg ≤MTOW<750 kg	10	+5%
(S10) APR 750 kg ≤MTOW<4000kg	50	+5%
(S11) MTOW ≥ 4000 kg	100	+5%

Table 15: Additional N_{EC} value for IE