European Strategic Coordination Platform

Strategy for Cybersecurity in Aviation

First Issue – September 10th, 2019

Note

The European Strategic Coordination Platform (ESCP) is mindful of the ongoing global efforts in cybersecurity including the recent development of an ICAO Global Cybersecurity Strategy and a proposal for an amended ICAO Assembly Resolution A39-19 “Addressing Cybersecurity in Civil Aviation”.

This Strategy document has been adopted by the ESCP shortly before the 40th Session of the ICAO General Assembly. The ESCP recognizes the importance to review the ESCP Strategy Document with the outcomes of the Assembly and ensure consistency and update to language pertaining to the ICAO Assembly Resolution on Cybersecurity.

Executive Summary

The aviation system and its valuable assets are not immune to cyber threats.

According to observations, cybersecurity incidents are increasing in frequency, magnitude and complexity, and have no borders. Technological advances and behavioural changes in people are major drivers of this trend. Aviation is not immune to this danger; on the contrary, the multiplication of network connections, the entry into service of e-enabled aircraft, as well as new generation of CNS/ATM systems and drones are going to increase the attack's surface.

Aviation stakeholders understand that a common strategy is necessary to take control of the future evolutions.

European Aviation stakeholders agree that a cyber-incident may have a significant economic impact and a reduction of the safety margins, with harmful effects on the population. Moreover, the stakeholders acknowledge that a common strategy, constituted by actions, activities and an intergovernmental approach, is necessary to reduce and mitigate the cybersecurity risk in aviation.

In fact, a collective effort is required to change the "As-Is" Situation into a desired "To-Be" Situation, by facing the key challenges and difficulties with a concrete plan.

The desired Aviation System

This Strategy envisages a future aviation system characterised by two main improvements.

The **future aviation system** is:

- **a trustworthy and dependable environment**, so that aviation stakeholders will be able to rely on services and information provided by others for the accomplishment of their operational objectives;
- **a system-of-systems capable to adapt and therefore, to withstand new threats without significant disruptions**, developed through **a systemic approach to cybersecurity in aviation** of current and legacy systems.

The Direction

To achieve the desired improvements, aviation stakeholders agree that the common effort shall focus in two directions.

As a **guiding policy**, the collective effort is focused on:

- **Making Aviation an evolutionary cyber-resilient system,** which, under attack, can maintain its essential functionalities.
- **Making Aviation self-strengthening by adopting a "built-in security" approach,** which consider, since systems' conception, security objectives that need to be achieved along with traditional operational and safety objectives.

The Objectives

The analysis lead to the formulation of four measurable objectives to improve cyber resiliency, and…

Operations continuity assurance is enabled with protections measures distributed along functional chains, which are appropriate to the level of risk.	**Operational Systems can fail gracefully by ensuring continuity of essential functionalities.**
Operational Systems adopt multi-layered protection measures that hinder the progress of an attack.	**Aviation stakeholders understand the trans-organisational nature of the Aviation system and make use of connections to collaborate.**

four measurable objectives for a self-strengthening aviation system, implementing a built-in security approach.

Systems design practices are in place to avoid unintended use of functions exposed to users.	**Systems design practices are in place to assess the risks of loss of security attributes and to implement protection measures, including adaptive solutions.**
Assurance and scrutiny processes allow for the security effectiveness of systems during the whole lifecycle.	**The level of protection against external causes is re-evaluated following a change in the original assumptions and, if necessary, restored.**

Table of Content

List of figures

List of tables

Definitions

Several terms used along this document need some clarification when their usage is not standardised. The terms and definitions used in this document refer to the general understanding in the aviation sector and are valid only in the context of this document itself.

Information Security: Preservation of confidentiality, integrity and availability of information. In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can be involved. [BS ISO/IEC 27000:2018]

Cybersecurity: The term 'Cybersecurity' is used in this document in place of 'Information Security'.

Attack: (adopting ***ISO 27000 definition***) Attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of anything that has value to the organization.

Security Incident: adopting the following definitions as ***provided in ISO 27035-1:2016***

Security investigation

Application of examinations, analysis and interpretation to aid understanding of an information security incident

Security event:

Occurrence indicating a possible breach of information security or failure of controls.

Security incident

One or multiple related and identified information security events that can harm an organization's assets or compromise its operations.

Security incident management

Exercise of a consistent and effective approach to the handling of information security incidents.

Incident handling

Actions of detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents.

Incident response

Actions taken to mitigate or resolve an information security incident including those taken to protect and restore the normal operational conditions of an information system and the information stored in it.

Information Sharing: the exchange of a variety of network and information security related information such as risks, vulnerabilities, threats and internal security issues as well as good practice.

1. Overview of the ESCP Strategy exercise

Under the ESCP initiative, representatives of European Aviation stakeholders, as well as non-European aviation organisations participating as observers, elaborated a strategy aimed at reducing and mitigating the cyber risk in aviation. This was done by analysing, from a cybersecurity perspective, the current "As-Is" situation of the aviation system, then by defining a future "To-Be" scenario capable to improve the security level and, finally, by elaborating an actionable plan that can drive such a change, following the process sketched out in the below *Figure 1*.

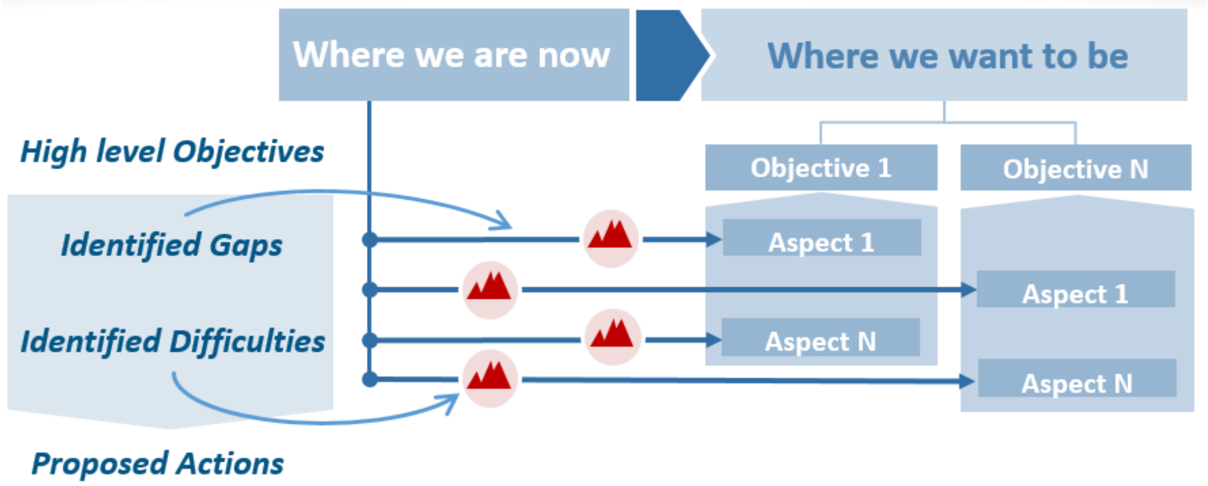

Figure 1 – process followed to elaborate the strategic objectives and actions.

1.1. Organisation of the Work

The outcome of this exercise has been divided in the following two parts:

- the strategic analysis culminating with the formulation of measurable objectives that detail the characteristics of the desired aviation system, covered in this document;
- the plan of coordinated actions aimed at reaching the above mentioned well-defined objectives, covered in the "**Implementation Plan of the Strategy for Cybersecurity in Aviation**" document.

The reason for this separation lays on the consideration that the strategic objectives described herein are stable and will remain valid over a long period (i.e. five to ten years); hence, frequent revision of the related document is unlikely. On the contrary, the implementation plan may face operational issues and unforeseen scenarios that will require reviewing and eventually adapting the proposed actions. Therefore, the ESCP members will meet on a yearly basis, if not otherwise driven by noteworthy events (e.g. significant change in the security environment), in order to assess the progress of the strategy implementation, as well as to discuss amendments when and where necessary.

1.2. Target Audience

This document is primarily targeted at the constituency of the ESCP, which are aviation stakeholders and their professionals at management and technical level, who want to mitigate the cyber security risk in aviation, through a coordinated sectorial approach. In light of this, the strategy will only be effective if these stakeholders buy-in to it and if the ESCP, through its members, support the dissemination and the implementation of the plan in the coming years.

2. Description of the Challenge

2.1. Introduction

According to observations, cybersecurity incidents are increasing in frequency, magnitude and complexity, and have no borders. Technological advances and behavioural changes in people are major drivers of this trend and both are modifying the risk landscape of many sectors, including air transport/aviation.

The aviation system, in its broadest sense of technologies, processes and people, is not immune to this danger, since aviation depends on Information and Communication Technology (ICT) systems and some Operators of Essential Services (OES)[1]. These dependencies range from general-purpose commercial ICT products and services, possibly adapted to aviation needs, to products and services specifically developed to serve the aviation sector.

Moreover, the rationalisation, consolidation and centralisation of the aviation IT infrastructure and the multiplication of network connections, as well as the entry into service of e-enabled aircraft, new generation CNS/ATM systems and drones will continuously transform the cyberspace, introducing also new vulnerabilities that may cause new risks.

In this scenario, there is also the need to consider the existing international legal framework for civil aviation from the perspective of cybersecurity and determine whether further elements are required, or if it is sufficient as it is.

Some general principles are already enshrined in the Chicago Convention and its technical Annexes, e.g. the existing Article 3 *bis* in the Chicago Convention requiring that "every State must refrain from resorting to the use of weapons against civil aircraft in flight", or the newly applicable Standard and corresponding Recommended Practice in ICAO Annex 17.

More recently, the Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation (Beijing Convention) and the Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft (Beijing Protocol) has enhanced the global legal framework for dealing with cyberattacks on international civil aviation as crimes. Therefore, a wide ratification by States of those instruments is desirable, as it would ensure that such attacks would be deterred and punished wherever in the world they occur.

2.2. Where we are standing – The As-Is Situation

There is a concern that many stakeholders of the aviation system are currently dealing with cybersecurity issues as if they were deterministic problems, which can be solved at source by applying technical IT solutions, such as adopting specific security products to protect their systems and keep the adversaries out. However, given the sophistication, adaptiveness, and persistence of cyber threats, which make the problems far from being deterministic, this risk-mitigation approach focussing on protection "at all costs" is not sustainable.

[1] As per definition of the Directive (EU) 2016/1148, a.k.a. "NIS Directive"

Moreover, due to increasing number of interconnections between multiple systems across a number of different stakeholders, it is extremely improbable that an organisation has full oversight of potential weaknesses, i.e. vulnerabilities of the whole system architecture underpinning its operations. In fact, the lack of means or processes to exchange cyber-risk related information between stakeholders of interconnected systems creates boundaries for and limits the effectiveness of cyber-risks assessment and management. Not appropriately considering interconnecting interfaces of the aviation system between aviation stakeholders can easily cause a vulnerability, emerging in one system or element of a system at one actor, which does not pose a big risk for the system itself, to escalate to a threat, resulting in a risk to someone else's system with negative consequences.

Another element of concern is that design, production and operational activities of aviation systems are still based, in many areas, on the assumption of a fully "cooperative" environment for what concerns the users' interaction, or the interfaces with third parties in a process chain. In other terms, from the design of an aeronautical system throughout its entire lifecycle, intentional malicious behaviours aimed at, e.g. tampering with the system may not always be systematically taken into account to the extent required. On the contrary, it is more common that possible illegitimate interactions are considered in a second step, so that cybersecurity is enforced "after-market", with solutions that are bolted-on the original product or service.

In general, aviation and aviation related stakeholders might have developed a false assumption that attackers will always be detected, vulnerabilities are under appropriate control and core systems will not fail. Consequently, some organisations may not have realised that they have in place inadequate security measures, which make them the weak link in an aviation's system-of-systems operational chain, thus increasing the overall risk for any other stakeholder.

2.3. Our destination - The To-Be Situation

Considering that aviation, as every other interconnected system-of-systems, will remain vulnerable to cyber-attacks, there is a need to define our strategy and focus our efforts on the development of a system with a minimum of residual risks and inherent fragilities.

To this extent, aviation and aviation related stakeholders need to develop the ability to identify, prevent, detect, and respond to cyber-attacks. This includes the assessment of potential impacts, the monitoring of systems under consideration, the assurance of operational continuity, even in a degraded or contested environment with appropriate mitigations and the availability of appropriate response measures to ensure normal operations are restored in a timely manner. This ability goes under the definition of cyber resilience, which also brings in the needs to identify the elements that are critical for the operational continuity, thus involving the organization's management level in the cybersecurity considerations, along with the operations.

Moreover, the aviation community needs to recognise the limit of a bolted-on security approach, which lacks a full systemic view and tends to implement security features that are effective for a limited time and scope. These features in fact are consequential to an identified problem and not a broader design goal. The aviation sector, whose products, services and processes have an operative life of decades, should lay its future development on stable foundations by making security considerations a significant and mandatory part of the design process and of the end-to-end systems architecture. With this approach, security is built-in, from the hardware components to the end user interface software, which will maintain and enhance trust amongst the aviation stakeholders.

2.4. Guiding Policy and Strategy Directions

In summary, **this strategy aims to make sure the future aviation system is a trustworthy and a dependable environment**, so that aviation stakeholders will be able to rely on services and information provided by others for the accomplishment of their operational objectives.

It will focus resources and actions to **introduce a systemic approach to cybersecurity in aviation** of current and legacy systems with the objective to **develop a system-of-systems [2]capable to adapt, and therefore, to withstand new threats without significant disruptions**.

Therefore, the **guiding policy** is to channel actions in **two directions** in particular:

Making Aviation an evolutionary cyber-resilient system

A cyber-resilient aviation system is a system, which, under attack, can maintain essential functionalities, i.e. continues to work and fulfils its operation-critical objectives. It mitigates the adverse effects of cyber-attacks as fast as possible and to the maximum extent, through an holistic multi-layered protection approach, so that a successful attack on one layer, e.g. an authentication breach that allows intrusion, does not provide sufficient authority to compromise system-critical services.

Furthermore, it follows an evolutionary process to ensure continuous improvement, i.e. learning from attacks and addresses the required organisational changes to support cooperation and information sharing between aviation and aviation related organisations, including civil and military, where appropriate.

Making Aviation self-strengthening by adopting a "built-in security" approach

Adopting a built-in security approach in aviation means that consideration should be given from systems' conception to security objectives that need to be achieved along with traditional operational and safety objectives. Ensuring security of critical service elements and processes "by design", switches the security paradigm from reactive (bolted-on) to proactive measures and fosters the development of a self-strengthening aviation system, therefore enabling it to evolve and improve its resilience in a more automated manner, where proven effective.

[2] See also: "System-of-systems notion of cybersecurity in aviation", AN-Conf/13-WP/270, 13th Air Navigation Conference, Montréal, Canada, 9 to 19 October 2018.

3. Strategic Analysis - Gaps and Difficulties

Having compared the current status and the desired target state allows the analysis of the gaps that need to be filled to implement a change, as well as the difficulties that may be encountered in doing so.

The below analysis is conducted in two steps: an initial outlook aimed at identifying potential overarching, or systemic gaps and difficulties; followed by a detailed examination of the desired, high-level properties of the future aviation system, set out in the guiding policy. For this second step, these properties will be broken down into sub elements, for which the change effort can be evaluated more easily.

The outcomes of this analysis are rational considerations that will enable the formulation of more precise and measurable strategic objectives. Also, these considerations will be guiding the definition of the actions plan for the implementation of the strategy.

3.1. High level Considerations

3.1.1. Facing an Evolving Threat Landscape

An aspect that should be considered in framing this strategy is the cyber-threats dimension. In particular, it is worth recognising that there are several profiles of attackers, or threat agents, which are motivated for different reasons and have access to different resources. A non-exhaustive list of the threat agents is the following:

- ***Nation States:*** this category of hacker is directly employed by an arm of a national government and they are typically very well-funded compared to small activist groups and individual cyber criminals. These entities are motivated by economic, political and military advantages.
- ***Cyber-Criminals:*** these are considered the most common adversary when discussing data theft and service disruption; cyber-criminals seek immediate financial satisfaction.
- ***Hacktivists:*** hacktivists are activist-hackers who are looking to influence political or social groups by pressuring businesses, governments and other entities to change their practices. Hacktivists may want to disrupt normal business activities in order to put the focus and media attention on their own agenda.
- ***Terrorists:*** these attackers are criminals who have ideological or political reasons for wanting to cause fear and disruption.
- ***Malicious Insiders:*** insiders are arguably the most dangerous source of attacks as they represent trusted employees and partners. Motivated by personal gain, professional revenge, or monetary reward, malicious insiders usually have easy access to the assets they are looking to expose or monetise. In some cases, they may be collaborating with other attackers such as Cyber-Criminals for personal financial gain as well as Hacktivist or Terrorist for ideological reasons.

Developing this strategy, it is necessary to consider that the threat landscape is constantly changing in relation to shifting of the global political picture, of groups or people’s motivations and with the availability of tools or other technical measures. Moreover, it should recognise that most of these dynamics are beyond the influence of aviation stakeholders’; these rest at the diplomatic and political level.

Identified Difficulties

In summary, for the development of this strategy and the implementation plan, the following difficulties should be taken into account:

- any assumptions made on the cyber-threat landscape to evaluate a cybersecurity risk needs to be re-evaluated as soon as the scenario evolves;
- some threat agents pose challenges that can only be influenced at a global political and/or diplomatic level.

3.1.2. Differences between Security and Safety Communities

Another general challenge that needs to be considered is the coexistence in aviation of two main communities, the security and the safety domains, having different objectives and perspectives.

On these differences, ECAC in the recently published Guidance Material on Cybersecurity in Aviation, argues: *"while aviation security experts often hold coordination links to threat information **sources** and are used to dealing with intentional threats and the respective methodologies, aviation safety experts have extensive know-how of the **consequences** on the safety of flight in case of system failure and know the design and set-up of systems and existing mitigation measures such as redundancies."*

In other words, from the security perspective, the cyber-threat is another potential agent of unlawful interference against which civil aviation needs to be safeguarded. From the safety perspective, an unauthorised electronic interaction of a threat agent is a potential cause of errors and malfunctions that can compromise the airworthiness and reduce the safety margins of an aviation system.

Sometimes these perspectives are complementary however, in some cases, are antagonistic and may lead to competing interests. Taking as an example a fire door to a secure area, safety requires the door to open/unlock in the event of a fire alarm or power cut, whereas security requires the opposite, as an attacker/intruder could initiate a fire alarm or remove power to access the area. A systemic approach to cybersecurity requires a wide engagement of the aviation community, a mutual understanding of different perspectives on the issue and finally an integrated approach, which aims at ensuring adequate safety margins.

Identified Gaps

In summary, as a prerequisite for a successful strategy and its implementation, aviation stakeholders need to ensure the following:

- that technical knowledge of the safety community is considered in the decision making of the security community to make security decisions more effective;
- that cyber threats knowledge of the security community is considered in the decision making of the safety community, for them to take more informed decisions, when addressing the response to cyber-related intentional acts;

- that there is a mutual understanding of the security and safety communities of the risk landscape, as well as a mutual confidence in the countermeasures being put in place.

Identified Difficulties

The aviation community should also be aware of the following difficulty that needs to be faced:

- the different perspectives of safety and security experts may lead to competing interests and clashing requirements.

3.1.3. Current Legal Requirements, Policies and Guidance

Legal requirements, policies and guidance are key elements of the aviation system and represent the playing field for this strategy and its implementation. In particular, legal requirements may require the implementation of measures that have to be taken into account in the action plan. Whereas policies and guidance may indicate a general trend that could be worth considering to facilitate the enforcement of the proposed strategic actions.

The figure below provides a schematic representation of the scope in Europe, hierarchy and potential overlaps of the current and planned **main** regulations on cybersecurity. The figure also shows, outlined in red, the legal requirements and the regulations that, at the time of writing, are expected to be published, or amended in the coming years.

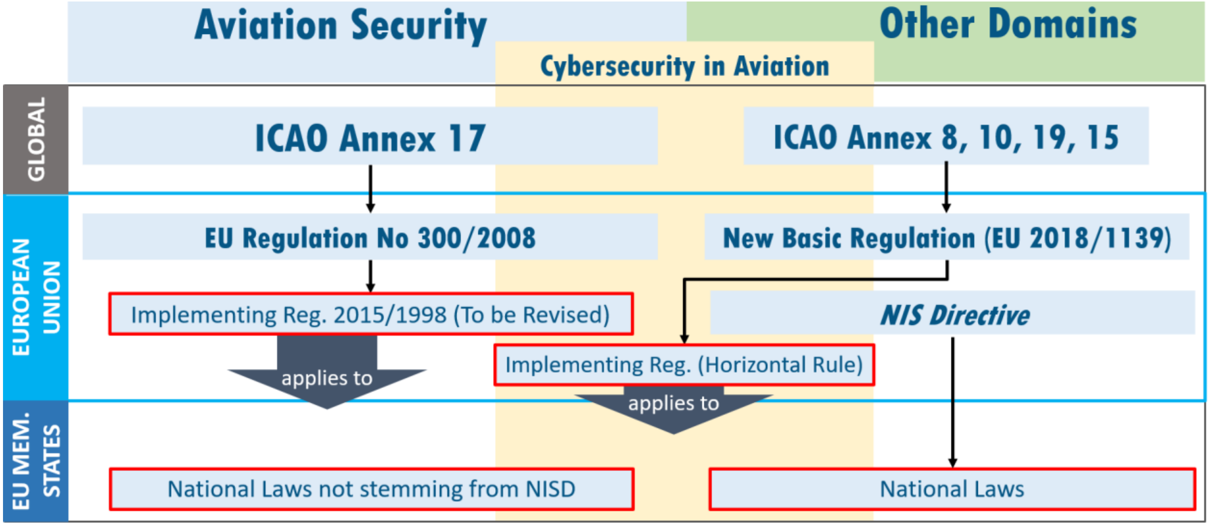
Aviation Security
Other Domains
Cybersecurity in Aviation
GLOBAL
EUROPEAN UNION
EU MEM. STATES
ICAO Annex 17
ICAO Annex 8, 10, 19, 15
EU Regulation No 300/2008
New Basic Regulation (EU 2018/1139)
Implementing Reg. 2015/1998 (To be Revised)
NIS Directive
Implementing Reg. (Horizontal Rule)
applies to
applies to
National Laws not stemming from NISD
National Laws

Figure 2 – cybersecurity in aviation high-level legal framework

Further details about the current regulations that lay down requirements about cybersecurity in the aviation domain, as well as policies and guidance, can be found in the Annex I of the document.

It appears quite clear from the above overview, that there is a stratification of legal requirements, stemming from the Aviation Security domain and other non-aviation domains, aiming at regulating aspects of cybersecurity in aviation, in some cases with overlaps.

ICAO, for the specific field of aviation, and the EU Commission for the transport sector in general, are requiring states to ensure that **appropriate measures** are implemented to protect the security attributes of **critical systems** and data, by means of national laws and regulations.

On the one hand, these notable initiatives may pave the way for the implementation of this strategy, but on the other hand, without proper coordination, there is the risk that "critical systems" and "appropriate measures" will have diverse interpretations in the different laws and implementing regulations. This may then result in dissimilar risk assessments at the national level, as well as in the implementation of protection measures at varying levels of quality and effectiveness, which may finally undermine a trans-national cooperation and the implementation of a European strategy.

This strategy should identify objectives and suggest actions that minimise the difference between regulations, making sure that the cybersecurity risk is addressed in similar way. It is equally important to achieve harmonised regulatory requirements for compliance, demonstrations and oversight in order to avoid unnecessary burdens for aviation stakeholders.

Identified Gaps

In light of the above considerations, the aviation community should consider:

- agreeing upon above common definitions for "critical systems" and "appropriate measures" as well as for the their evaluation and classification criteria;
- identifying the best possible implementation, articulation and means of compliance for all the legal requirements for cybersecurity in aviation that are to be published or amended;
- influencing the enforcement of a coordinated European regulatory framework for cyber security in aviation that will support the implementation of the action plan for the achievement of this strategy.

Identified Difficulties

The aviation community should also be aware of the following difficulty that needs to be faced:

Uncoordinated developments of aviation regulations and associated compliance requirements will address cybersecurity risks in a dissimilar way, resulting in competing and potentially conflicting requirements and unnecessary burdens for aviation stakeholders and competent authorities.

3.2. Detailed Considerations

3.2.1. Obstacles towards an Aviation cyber–resilient and evolutionary system

To break down the first high-level property of the desired aviation system, it is necessary to identify the fundamental elements of a cyber resiliency from an organizational perspective. Amongst different academic publications the short paper "Cyber resilience – fundamentals for a definition"[3] provides practical elements, such as a list of characteristics of cyber resiliency, which will allow gap analyses to be performed more effectively.

The below Table 1 summarises, in accordance with the above academic publication, the main characteristics of cyber resiliency in comparison to a traditional IT security approach.

Table 1 – Aspects of IT Security vs Cyber Resiliency

Aspect	IT Security	Cyber Resiliency
Objective	Protect the systems	Ensure Operations continuity
Design Goal	No failure	Safe-to-fail
Architecture	Single Layer[4]/Perimeter protection	Multi-layered protection
Scope	Atomistic, one organisation	Holistic, trans-organisational

Challenges related to the "Objective" aspect

Concerning the Objective, cyber resiliency places a higher priority on IT operations continuity assurance rather than solely on network IT protection. First and foremost, it is necessary to clearly define which objectives are critical for the operations (e.g. safety of flight, service continuity), to then understand how to direct the efforts for their protection. Operational objectives of aviation and aviation related organisations span across trans-organisational functional chains. A cyber resilient approach should ensure that the protection effort is adequately distributed along these functional chains to ensure the operational objectives of critical systems (in the wider meaning of technology, people and processes).

A transition from a traditional IT security approach to one that emphasizes assurance and continuity of operations, requires involvement of management at the decision making level, which is essential to change an organisation's attitude. However, to enable managers to take informed, risk aware decisions, they must be supported by information that is backed with tangible elements, such as a map of the functional chains, the related critical systems, the required level of protection and potential consequences if risk mitigations fail. Management will then have to exercise due diligence to ensure the protection of these systems is fully enforced to also ensure regulatory compliance.

[3] Björck F., Henkel M., Stirna J., Zdravkovic J. (2015) Cyber Resilience – Fundamentals for a Definition. In: Rocha A., Correia A., Costanzo S., Reis L. (eds) New Contributions in Information Systems and Technologies. Advances in Intelligent Systems and Computing, vol 353. Springer, Cham

[4] As clarified in the publication "While the use of several layers of protection is commonly advocated when designing secure systems the difference here is that the architecture should be especially suited for the recovery of each layer."

Identified Gaps

In summary, the following elements need to be addressed for the achievement of cyber resiliency at the systemic level:

- identify the aviation functional chains and become aware of the critical systems along them, which ensure the safety of flight and the service continuity;
- understand the level of protection required by the security attributes (confidentiality, availability and integrity) of these systems;
- achieve the full buy-in and commitment by the management in aviation organisations for decisions concerning cyber risk management, in order to prioritise the protection of the identified critical systems.

Identified Difficulties

It is expected that the following difficulties may be identified:

- the lack of harmonised methodological principles and models, as well as different vocabulary amongst aviation stakeholders, which may jeopardise the development of a common map;
- the existence of different "risk-appetites" amongst the aviation stakeholders.

Challenges related to the "Design Goal" and the "Architecture" aspects

A desired property of a cyber-resilient system is to be ”safe-to-fail", which means that such a system has the ability to fail (gracefully), withstand, detect, recover a cyber-attack and possibly evolve. This goes hand-in-hand with an architecture designed to allow partial failure, consisting of several protection layers capable of recovering from failure.

In the aviation sector the acceptance of component failure under certain conditions, in particular for aircraft design, is not a new notion. However, in other areas of aviation, closer to traditional information technology, where there is a "no failure" approach, the paradigm shift to a safe-to-fail one is going to be a major change.

To this extent, some gaps between the two perspectives of the design goals should be further explored to allow an impact evaluation and, at least, a qualitative estimation of the financial and organisational effort required. In particular, it would be helpful to achieve an understanding of what can be defined as an acceptable degradation threshold and restoration level for a function, possibly in terms of all three security properties (availability, integrity and confidentiality).

Identified Gaps

In light of these considerations, the achievement of cyber resiliency at the systemic level requires that aviation stakeholders:

- agree upon acceptable minimum levels of service of the key functions, underpinning the mapped critical systems along the functional chains.
- develop, for the short term, contingency plans and recovery processes to be able to minimise the adverse effects of a successful attack to a critical system and avoiding cascading effects;

- identify, for the long term, viable solutions to withstand attacks, detect incidents, recover and evolve.

Identified Difficulties

- It is expected that achieving a common position amongst stakeholders concerning the acceptable minimum levels of service might be challenging, due to the different "risk-appetite" of stakeholders and operational circumstances.
- The need for the investigation of cyber-attacks, which may require letting the scenario to evolve, needs also to be taken into account.

Challenges related to the "Scope" aspect

Finally, the boundaries of a cyber resilient system are trans-organisational. It shall encompass not only the organisation and its close environment, but also the multitude of interconnections with other systems. It has been already mentioned that the current widely interconnected system-of-systems used in aviation exposes stakeholders to the vulnerabilities of others. However, as stated by Joseph[5]: "If networks expose us to vulnerabilities, they also form the basis of our resilience". Thus, a cyber-resiliency approach should make use of the connections to foster collaboration amongst stakeholders and, in turn, increase the overall level of protection.

Identified Gaps

To develop such a connection, aviation stakeholders need to work on the following:

- identify possible forms of collaboration in relation to stakeholder needs, such as good practices, information on new threats and vulnerabilities and, finally, the need for mutual support for threat analysis, incident response and management;
- agree upon the value of undertaking such collaboration for organisations and the effort required to build up and mobilise a strong community of cybersecurity professionals in aviation;
- provide support for the practical implementation of collaborative initiatives in which all the stakeholders relevant for the cybersecurity of the aviation system can participate.

Identified Difficulties

The willingness of, and the legal basis for, affected organisations to disseminate information concerning cyber incidents is often very limited, which in turns reduces the base of available and relevant information to improve resiliency. To this extent, the challenge for aviation organisations is to enable the sharing of information, by taking into account the security objectives and the policies of the European states and respecting the individual requirements for information control and confidentiality.

Moreover, any collaborative initiative will only occur if there is existing trust amongst aviation stakeholders, something that is already available in safety and aviation security cooperation, can be extended to cover sharing of information regarding cyber incidents.

[5] Joseph, J.: Resilience in UK and French Security Strategy: An Anglo Saxon Bias? Politics, 33(4), pp253-264, (2013).

3.2.2. Obstacles towards adoption of Built-In security for a self-strengthening Aviation

As mentioned in the guiding policy and strategy directions, the concept of built-in security is very much related to the approach to aviation systems design and modification during the whole lifecycle, which includes, *inter alia*, development, operations and maintenance, as well as related training activities. It should be expected that any change to the current, well consolidated, processes would be challenging. A crucial success factor, which is particularly pertinent for the adoption of built-in security in aviation, is the collaboration between security and safety.

As done for the cyber resilience property, it is worth trying to deconstruct the current "airworthiness driven" lifecycle into its main characteristics to identify gaps and to develop means for identifying the characteristics of a lifecycle, which incorporates a built-in security perspective. To cater for the specific requirements in complex aviation systems the extent to which extent the current and generic processes must be adapted should be analysed. Table 2 summarises the main aspects related to the traditional airworthiness driven lifecycle in aviation versus one characterised by a built-in security approach.

Table 2 – Airworthiness Driven vs Built-in Security approaches in lifecycle

Aspect	Airworthiness Driven	Built-in Security
Users Interaction	Cooperative Behaviour	Cooperative and Un-Cooperative Behaviours
Approach	Failure modes driven design	Threat Conditions and Failure modes driven design
Ability to autonomously Evolve	Not Applicable	Possible design objective
Assurance	Safety Development Assurance	Security and Safety Development Assurance
Configuration and Change Management	Reach a stable condition	Ensure cyber resilience is maintained

Challenges related to the "Users Interaction" aspect

The traditional, airworthiness driven, design approach in aviation assumes that users interact cooperatively with systems, thus triggering expected outcomes of the system's functions. However, unintended, non-cooperative behaviours are those that can expose a system to security risks. These behaviours can have either a malicious, or a non-malicious purpose, but be equally dangerous. For example, a function may be exercised repeatedly, maliciously and intentionally, to overload a system and make it incapable of dealing with other legitimate requests (technically a denial of service attack). As another example, a device may be compromised with a virus due to non-malicious, although intentional, improper use, causing damage to other assets of the infrastructure.

A built-in security approach needs to consider these behavioural aspects in the system lifecycle, to enable the identification of preventing mechanisms at an early stage in the design, or modification processes. In other words, this approach attempts to intervene systematically at the conceptual stage by avoiding that a security vulnerability is introduced during the system's lifecycle. This may lead to an evaluation of how legitimate functions may be utilised for unintended purposes and similarly, if a system under analysis may make available unintended functions, inadvertently.

Identified Gaps

The aviation community, to support the achievement of the built-in security strategic goal in systems lifecycle, needs to:

- modify the design analysis of critical systems to include an assessment of possible unintended, non-cooperative, and malicious behaviours, evaluating the risk of unexpected results through the misuse of intended functions in an uncontrolled and uncooperative environment;
- develop and agree upon a methodological approach, based on solid industry standards, to introduce the above risk assessment in both the ground and air domains for critical systems;
- ensure that regulations across all fields of aviation are properly adapted to enforce a built-in security approach.

Identified Difficulties

Organisations may have a different cybersecurity risk appetite thus, allocate different financial resources for risk mitigation measures. Therefore, concerns about the financial impact and reluctance for the introduction of new processes related to introduce the necessary changes are to be expected.

Moreover, the development of a methodological approach may be challenging, due to the lack of harmonisation regarding the application of industry standards amongst aviation stakeholders.

Challenges related to the "Approach" and "Ability to Evolve" aspects

The traditional, airworthiness driven, design approach focuses on the identification of hazardous situations that may arise because of a fault. Deductive methodologies such as the "failure mode and effects analysis" (FMEA) and the "Fault Tree Analysis" (FTA) have been developed to identify qualitatively and quantitatively possible failures and their effects.

As cybersecurity introduces the notion of intent, it becomes necessary to consider other scenarios, which may develop as a consequence of unauthorised interactions and may not necessarily emerge out of a system's component failure. The manipulation of an information asset, which goes undetected and provides incomplete indication, threatens the integrity security attribute, and is an example of a possible threat condition. For instance, malicious navigation or surveillance information on board an aircraft, which are taken as genuine by the crewmembers, can cause erroneous piloting actions, with significant reductions in the safety margins.

To this extent, a Built-in Security design approach must assess how security attributes of integrity, availability, or confidentiality of a system are at risk of being compromised, as well as assess the potential, resulting consequences especially on the safety of flight. In doing so, we will have to expect that some systems must be identified as "critical" in a cybersecurity perspective, even when they are not, according to a traditional hazard analysis.

A different approach should also be taken in the design of mitigations for potential threat conditions, as traditional solutions may no longer be effective. As an example, identical physical redundancy helps the safety posture, however, does not necessarily help to mitigate cybersecurity risks. In fact, if attackers can defeat a system, they can also defeat the identical redundant one, so in this specific case, functional redundancy can be an effective measure for cybersecurity, only if accompanied by systems' physical diversity/dissimilarity.

In summary, an effort to identify the appropriate means to mitigate security risks should be made, while also exploring the possibility of designing novel solutions as suggested by academic research, such as adaptive approaches. To this extent, it is envisaged that to build-in the system the capability to improve its resilience in a more automated manner through adaptive protection measures.

Identified Gaps

In summary, the following elements need to be addressed to adopt a built-in security approach in Aviation:

- reinforcing the position already expressed in the challenges related to the "User Interaction", the aviation community, needs to develop and agree upon a harmonised approach to properly assess the effect of loss of security attributes in conjunction with the traditional failure modes and effects evaluations;
- new methods to built-in fault tolerance measures against cyber-incidents should be considered and assessed for adoption in the design of aviation systems.

Identified Difficulties

Any new design approach will need to include rational means to demonstrate compliance with safety requirements, in a way that is financially and technically feasible.

Challenges related to the "Assurance" aspect

The structure of the development process in aviation is aimed at assuring that errors and possible system failures are identified and resolved before systems enter into service. In this approach, the effort is proportional to the safety risk, so higher levels of severity of impact require higher levels of scrutiny in the development process. A built-in security approach will need to implement a similar assurance process and scrutiny in order to assure that vulnerabilities (flaws that are detrimental to security properties) are captured and resolved at an early stage.

Identified Gaps

The gap between the traditional methodology and a built-in security approach in development is probably more conceptual rather than procedural. The aviation community needs to introduce good practices to assure that security measures perform as intended, are adequately effective and that the final product is free of known and unacceptable exploitable vulnerabilities, in addition to other development assurance that covers quality, reliability and safety aspects.

Identified Difficulties

Cultural difficulties may be encountered when taking into account cybersecurity in design and lifecycle assurance and its harmonisation with safety design assurance.

Challenges related to the "Configuration and Change Management" aspect

The outcome of an aviation design process, being it a product or a service, is normally kept as stable as possible along its life cycle in order to avoid that modifications introduce unwanted reductions of safety margins. When a change event occurs, it is normally driven by the requirement of adding functional improvements and it can be largely controlled. In fact, the extent of the functional changes is *a priori* known so that the change process can be optimised in terms of duration, cost and operational impact.

In the realm of cybersecurity, there is a constantly changing threat landscape that is beyond a system operator's influence. This requires the establishment of additional processes to ensure through-life cyber security that takes into consideration, as reasons for implementing a change, external causes such as new threats or the discovery of vulnerabilities, which need to be treated, with no other scope than maintain the original level of system's protection.

Identified Gaps

To cope with the identified challenge, aviation stakeholders will need to:

- develop a harmonised approach to re-evaluate the effectiveness of the security measures of the systems and the validity of the initial risk assessment. This should take into account the changes in the operating environment as well as the discovery of new vulnerabilities on the operated systems and the changes in the threat landscape;
- identify the most effective procedure to implement and deploy corrective actions to restore or maintain an acceptable level of residual risk.

Identified Difficulties

- There might be a clash between the process agility, required by cybersecurity change management and the safety perspective, which needs stability and a highly scrutinised change process, with a dynamic that is much longer than threat scenarios evolutions.
- Proactive implementation of cybersecurity changes requires resources and effort that may not be available, because it is hard to justify the effort with "return of investment" considerations (when a system is secure, no one notices, the value is recognised only in case of a security breach).

4. Strategic Objectives

In this document, the aspects of a resilient and intrinsically secure aviation system have been identified through an analytical deconstruction process. Each aspect represents a characteristic of the future aviation system, i.e. the “to-be” situation that we want to achieve.

Therefore, eight strategic objectives have been derived by formulating the characteristic of the future aviation system a declarative format, as summarised in the below diagrams at Figure 3.

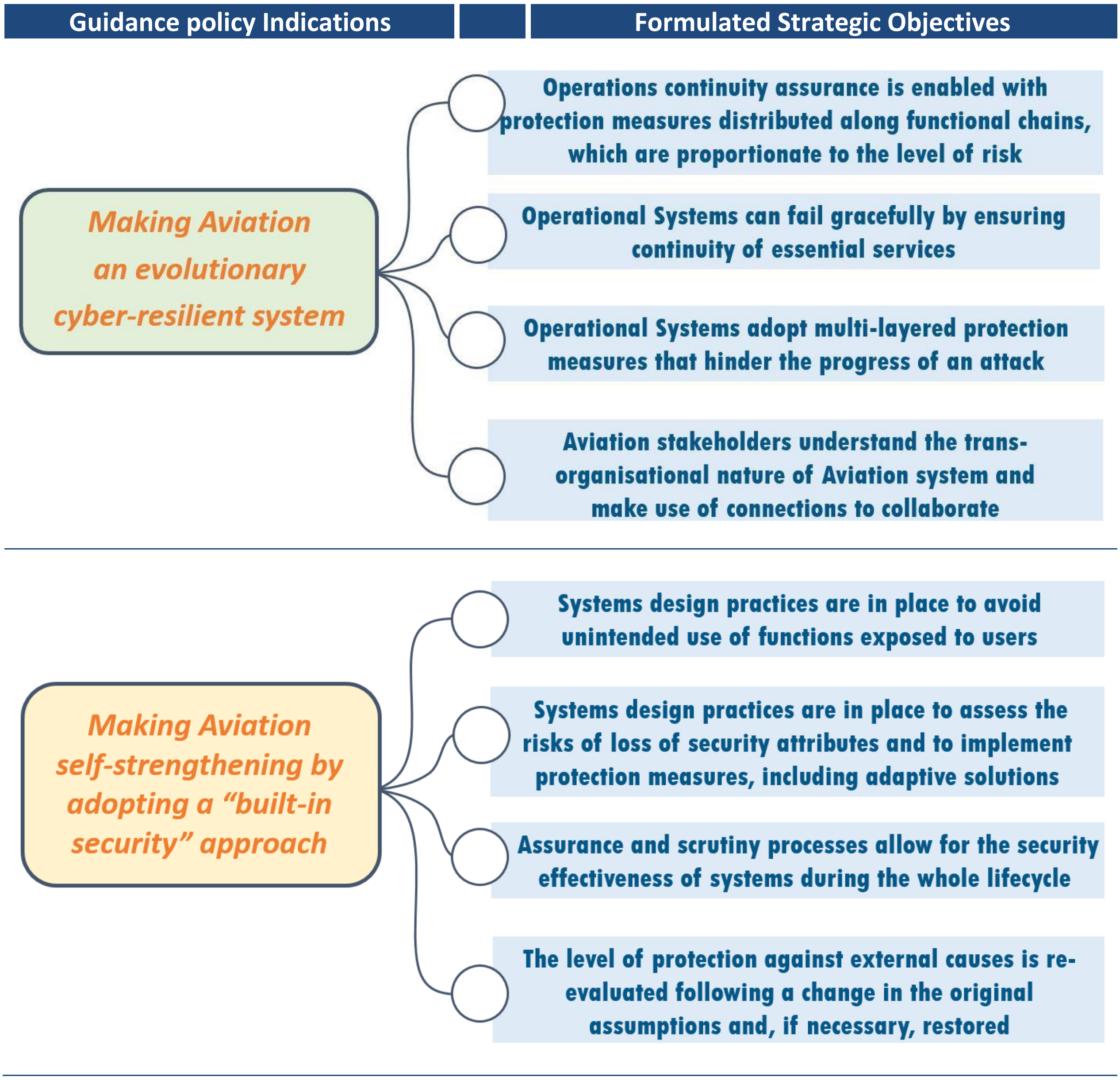
Guidance policy Indications
Formulated Strategic Objectives
Making Aviation an evolutionary cyber-resilient system
Operations continuity assurance is enabled with protection measures distributed along functional chains, which are proportionate to the level of risk
Operational Systems can fail gracefully by ensuring continuity of essential services
Operational Systems adopt multi-layered protection measures that hinder the progress of an attack
Aviation stakeholders understand the trans-organisational nature of Aviation system and make use of connections to collaborate
Making Aviation self-strengthening by adopting a “built-in security” approach
Systems design practices are in place to avoid unintended use of functions exposed to users
Systems design practices are in place to assess the risks of loss of security attributes and to implement protection measures, including adaptive solutions
Assurance and scrutiny processes allow for the security effectiveness of systems during the whole lifecycle
The level of protection against external causes is re-evaluated following a change in the original assumptions and, if necessary, restored

Figure 3 – formulated strategic objectives.

The analysis also pointed out a number of gaps and difficulties that need to be considered towards the achievement of the strategic objectives. The mapped gaps and difficulties provide initial indications, but need to be further elaborated to define an implementation plan. This activity constitutes the second part of the ESCP strategic exercise, which has been documented in the “Implementation Plan of the Strategy for Cybersecurity in Aviation”.

Annex I

EU Strategies & Policies, Regulations and Guidance relevant for Cybersecurity in Aviation

1. EU Strategies and Policies

Cyber security is a priority within the Global Strategy on the EU Foreign and Security Policy. Indeed, the EU Global Strategy in the chapter related to cyber security is referred to the EU's will to increase its focus on cyber security, equipping the EU and assisting Member States in protecting themselves against cyber threats while maintaining an open, free and safe cyberspace.

In 2013, the Council welcomed Cybersecurity Strategy of the European Union and highlighted that it is essential and urgent to develop further and implement a comprehensive approach for EU cyberspace policy.

In 2014, the Council adopted the Cyber Defence policy Framework (CDPF) identifying priority areas to promote civil-military cooperation and synergies with wider EU cyber policies, relevant EU institutions and agencies, as well as with the private sector. These areas have been recently revised to adapt to the changing environment of the cyber domain, as well as EU's initiatives on security and defence on the implementation of the EU Global Strategy.

In September 2017, the Commission launched an updated package of initiatives on cybersecurity via the Joint Communication "*Resilience, Deterrence and Defence: Building strong cybersecurity for the EU* "presented by the Commission and the HR/VP. This recognised that in tandem with growing digitalisation and the associated benefits of a connected economy and society with connected objects through the Internet of Things, the threat landscape has increased significantly.

Furthermore, cyber is now perceived by State and State-affiliated groups as a strategic weapon with destruction of infrastructure and data caused by targeted cyber-attacks. Such attacks have now the depressing capability to lead to loss of life as safety critical systems, including transport means, are becoming reliant on digital. The level of complexity and scale such attacks continue to increase. Hybrid threats involving cyber-attacks blended with online disinformation have been used to interfere with decision making in our liberal democracies. In addition, it is predicted that cybercrime will continue rising and cost businesses globally more than 5 trillion EUR annually by 2021.

In this context, it is essential that support be provided for the further development of cybersecurity capabilities. In order to boost investments in the EU cybersecurity market and increase resilience, in September 2018, the Commission proposed the creation of a **Network of Cybersecurity Competence Centres** and a new **European Cybersecurity Industrial, Technology and Research Competence Centre,** while ensuring complementarity and avoiding duplication within the Network of Cybersecurity Competence Centres and with other EU agencies. The Centre should, inter alia, enhance cooperation between civilian and defence technologies and applications, working closely and in full complementarity with the European Defence Agency in the area of cyber defence**.**

Moreover, the EU has recently given to ENISA, the European Union Agency for Cybersecurity, a permanent and broader mandate, with the approval and entry in to force of the EU Regulation 2019/881, which is also enabling a new EU-wide cybersecurity certification framework. The main objective of the new mandate of ENISA is to make the Agency stronger and more effective in dealing with cybersecurity issues by actively helping Member States, EU institutions, businesses and citizens.

At operational level, the Computer Emergency Response Team for the EU institutions, CERT-EU deploys specialised tools to detect and mitigate increasingly complex threats. CERT-EU also participates in a variety of cyber exercises, such as ENISA's CyberEurope, to improve situational awareness and test levels of preparedness.

In May 2018, CERT-EU ENISA, Europol's EC3 and the European Defence Agency signed a Memorandum of Understanding in order to promote swift and effective cross-sectorial cooperation.

A Technical Arrangement between the CERT-EU and the NATO Computer Incident Response Capability (NCIRC), signed in February 2016, is facilitating technical information sharing to improve cyber incident prevention, detection and response in both organisations.

2. Regulations

2.1. Global - ICAO

Changes to Annex 17 on Measures relating to cyber threats

The 2017 AVSEC Panel proposed changes to the Annex 17 that split Article 4.9. "Measures relating to cyber threats" and **upgraded 4.9.1 from recommendation to a standard as follows**:

"4.9 Measures relating to cyber threats

4.9.1 Each Contracting State shall ensure that operators or entities as defined in the national civil aviation security programme or other relevant national documentation identify their critical information and communications technology systems and data used for civil aviation purposes and, in accordance with a risk assessment, develop and implement, as appropriate, measures to protect them from unlawful interference."

And **amended the existing Recommendation as follows**:

*"4.9.2. Recommendation***.** **-** *Each Contracting State should ensure that the measures implemented protect, as appropriate, the confidentiality, integrity and availability of the identified critical systems and/or data. The measures should include, inter alia, security by design, supply chain security, network separation, and the protection and/or limitation of any remote access capabilities, as appropriate and in accordance with the risk assessment carried out by its relevant national authorities."*

ICAO States were informed by the State letter of 6 July 2017 on the proposed Amend.16 to Annex 17.

These proposed **changes were presented to the Council for adoption during its 213th Session** (26 February to 16 March 2018).

Amendment 16 to Annex 17 became effective on 16 July 2018 and will be applicable as of **16 November 2018**.

Other Relevant ICAO Annexes

Existing provisions regarding confidentiality, integrity and availability in others ICAO Annexes may also have to be considered for a comprehensive view, in particular: **Annex 8** – Airworthiness of Aircraft, **Annex 10** – Aeronautical Communications, **Annex 19** – Safety Management, **Annex 15** – Aeronautical Information Services, as well as **Annex 13** – Accident Investigation for what concerns the procedure for protection of evidence applicable to cyber data in the event of accident/incident.

A comprehensive review of the existing ICAO Annexes is currently underway in the ICAO Secretariat Study Group on Cybersecurity.

ICAO Cybersecurity Resolution A39-19

At the 39th ICAO Triennial assembly, the ICAO's Executive Committee expressed unanimous support for the Cyber security resolution presented as a joint paper by US, EU and its Member States. The Cybersecurity Resolution A39-19- has been adopted and represents a global milestone in the field of cyber in aviation.

UN Resolution 64/211, March 2010

The UN resolution 64/211 on the "Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures" affirms the right of each country to determine its own critical infrastructure. It also calls for enhanced efforts to close the digital divide, recognises national efforts should be supported by international information-sharing and collaboration, calls for public-private cooperation on information sharing and identify networks and processes of international cooperation that may enhance incident response and contingency planning.

2.2. European

Regulation (EU) No 300/2008

As one of the two main objectives of Regulation 300/2008 EU on common rules in the field of civil aviation security is to provide the basis for a common interpretation of Annex 17, **cybersecurity shall be addressed in European aviation security legislation outlining requirements how to set up these preventive security measures and have** – as broadly as possible - a common interpretation across the EU (EEA).

Commission Implementing Regulation (EU) 2015/1998

Implementing Regulation (EU) 2015/1998 of November 2015, provides for the detailed measures for the implementation of the common basic standards for safeguarding civil aviation against acts of unlawful interference that jeopardise the security of civil aviation, referred to in Article 4(1) of Regulation (EC)

No 300/2008, and the general measures supplementing those common basic standards, referred to in Article 4(2) of that Regulation, are set out in the Annex. The Implementing Regulation 2015/1998 imposes obligations on entities to e.g. ensure airport security, aircraft security, awareness/training, etc.

Cybersecurity measures – to be taken on board by virtue of Implementing Regulation 2015/1998 - are more detailed **elements adding a layer in pursuing better protection of civil aviation – in this case – against acts of unlawful interference posed by cyber threats**.

The European Commission (Directorate-General for Mobility and Transport) currently works with Member States and stakeholders on transposition of the new ICAO cybersecurity standard.

Regulation (EU) No 376/2014

The Regulation (EU) No 376/2014 on the "reporting, analysis and follow-up of occurrences in civil aviation" aims at improving aviation safety by ensuring that relevant safety information relating to civil aviation is reported, collected, stored, protected, exchanged, analysed and disseminated with follow-up at Industry, National and EU level.

The Regulation through its implementation and adoption provides the means to increase information exchange between the Member States and ensures continued availability of safety information (enhanced Just Culture).

In particular the regulation requires that:

- Member States, EASA and organisations shall establish both a mandatory and a voluntary occurrence reporting system in order to collect **any event representing a serious risk to the aircraft or its occupants**.
- The storage of occurrences is carried in a ECCAIRS/ ADREP compatible format Database in order to facilitate data exchange

Regulation (EU) 2018/1139

On 26 June 2018, the Council of the European Union adopted a new Basic Regulation on common rules in the field of civil aviation, which includes a revised mandate for EASA.

In particular Article 4 and Article 88 require the Agency to consider interdependencies between aviation safety and cybersecurity when taking measures under the regulation.

Commission Implementing Regulation (EU) 2017/373

Implementing Regulation (EU) 2017/373 lays down common requirements for providers of Air Traffic Management/Air Navigation Services and other air traffic management network functions and their oversight. Currently contains requirements for the service providers related to "security management", including:

- The need to describe the overall philosophies and principles with regard to the security of the services.

- The need to define the authority, duties and responsibilities of the management personnel responsible for security.
- The establishment of a "security management system" which, among other aspects, ensures:
  - The prevention of unlawful interference with the provision of services.
  - The security of the operational data.
  - The protection of their systems, constituents and data.
  - The protection of the network against information and cyber-security threats.

It also contains training requirements for the Air Traffic Safety Electronic Personnel related to data security and software integrity and security. Although Regulation (EU) 2017/373 has already been adopted, most of the provisions are not applicable until 2nd January 2020.

Directive 2016/1148 (NIS Directive)

In 2016, Directive 2016/1148 ("NIS Directive") concerning measures on a high common level of security of network and information systems across the Union entered into force. This established a European competence in cybersecurity to protect the digital single market.

The Directive has three main objectives:

- Improving national cybersecurity capabilities, through requiring all Member States to have a common minimum baseline set of capabilities;
- Facilitating cross-border cooperation at EU level between Member States and the Union at both strategic/policy and operational cybersecurity levels; and
- Promoting a culture of risk management and incident reporting among key economic actors, notably operators providing essential services (OES) for the maintenance of economic and societal activities and Digital Service Providers (DSPs).

Member States are required to identify both those services, which they consider critical for the functioning of their societies and economies, and also those operators of these essential services (OES). The Commission anticipates that by 9th November 2018, Member States will have completed this task with consequential arrangements in place regarding security and mandatory reporting of important incidents for relevant air carriers, airport managing bodies, airports, entities operating ancillary installations contained within airports and providers of air traffic control services.

In addition to the identification process with OES, Member States are required to ensure that national competent authorities regulate and enforce the application of security and reporting requirements on both OES and DSPs. Reporting can also be made to the CSIRTs and there are provisions for single points of contact at Member State level where multiple national competent authorities are involved.

The NIS Directive established a **Cooperation Group** consisting of **Member States**, the **EU Commission** and **ENISA** in order to support and facilitate strategic cooperation and the exchange of information so as to contribute to enhanced cybersecurity in the Union. The Cooperation Group meets at least 4 times annually. It presently has multiple work-streams developing non-binding guidance on the following topics: identification of OES, security measures for OES, incident reporting for OES, incident reporting for DSPs and cross border dependencies. The group through two additional work-streams has also finalised a compendium on cyber security with election technology and a reference taxonomy for large scale cyber incidents and crises.

3. GUIDANCE

Here below are mentioned the main Institutional guidance.

ECAC Doc 30

The ECAC Doc 30 Chapter 14 provides recommendations to cyber security governance at national level and cyber security activities at organisational level, based on risk-based approach. The recommendations, when included in national civil aviation security programmes, will need to be implemented by operators or other entities in civil aviation with critical systems. These may include service providers, air navigation service providers, airport operators, air carriers, regulated agents and other entities or authorities in the field of civil aviation. The aim is to ensure safe and secure aviation operations through the application of cyber security processes and procedures that would preserve the confidentiality, integrity and availability of the systems and data involved.

The ECAC Consolidated Guidance Material on Cyber Security in Civil Aviation, supports in more detailed level the efforts undertaken by the appropriate authority and by the relevant aviation stakeholders to best address the cyber threats to civil aviation sector. The document focuses on malicious and deliberate acts with an effect on civil aviation and emphasises the potential consequences of cyber threats on the safety and security of civil aviation, consisting at the moment of two major parts: addressing governance and coordination and risk management. The need for coordination between cyber security, aviation security and aviation safety regulatory bodies and experts is highlighted both at national and organisational levels.

ICAO - ASSEMBLY / 39TH SESSION Working Paper[6]

> *"The civil aviation system consists of a patchwork of interconnected components, systems and networks. The potential for cyber incidents that could jeopardise communications and information exchanges between various aviation stakeholders, impact safety and security and damage aviation business continuity has increased over the years. While the importance of defining an appropriate cybersecurity approach in civil aviation has been recognised by ICAO, additional efforts are still required to increase global awareness and to further develop globally coherent cyber resilience approaches for the aviation system.*
>
> *Action: The Assembly is invited to:*
>
> *a) request that ICAO address cyber resilience in civil aviation in a comprehensive manner;*
>
> *b) request that ICAO and its contracting States promote awareness on cyber threats and vulnerabilities in civil aviation notably through the inclusion of the cyber resilience dimension in relevant processes and activities such as system design, ATM procedures and safety management and aviation security;*

[6] "Cyber Resilience in Civil Aviation." ICAO, 26.07.2016, https://www.icao.int/Meetings/a39/Documents/WP/wp_099_en.pdf

c) request that ICAO facilitate, in a secure manner, information sharing between States and relevant stakeholders on cyber-threats, vulnerabilities and mitigating measures;

d) request that ICAO consider necessary steps for the development of guiding principles for managing current and future cyber-threats and vulnerabilities, from identification to mitigation taking into account relevant existing States' measures and industry standards; and

e) request that ICAO instruct existing panels and expert groups to take into account, where relevant, those guidelines, while performing their work. "

The Krakow Declaration

"The Krakow Conference has been built on the discussion held during the High Level Meeting on Cybersecurity in Civil Aviation held in Bucharest on 8-9 November 2016 and the High Level Conference on Drones held in Warsaw on 23-24 November 2016.

Subsequent to these two Conferences, the European Strategic Coordination Platform (ESCP) has been established and initiated its Engagement Phase. It is developing its Charter until end of 2017 and coordinates the work on the Cybersecurity in Aviation horizontal rule EASA is proposing to address objectives common to all aviation stakeholders. The objective is to engage all stakeholders in a fair and non-discriminatory fashion in establishing a resilient European civil aviation system, creating the largest level playing field in the world.

The Conference discussed the progress achieved for aviation ground systems so far, including institutional set-up, legislation advancement, risk assessment methodology, cybersecurity promotion, research activities, commitments and resources devoted to cybersecurity and to establish a ground for the future European strategy for Cybersecurity in Aviation and the Cybersecurity Road Map that will define the future actions that have to be undertaken at European level in order to ensure a secure environment for aviation covering the cyber-space. "

In particular the Conference:

- called upon the European Commission and the European Aviation Safety Agency to develop and adopt Implementing Regulations addressing Cybersecurity in Aviation with harmonised common objectives but tailored requirements for subjects and sub-sectors, assuring commensurate responses to risks,
- called on the Member States of the European Union to address cybersecurity nationally, in line with Directive 2016/1148 (NIS Directive),
- recognised the need that the safety critical elements of aviation flow in a consistent and coordinated way with the existing EU NIS Directive ground base,
- acknowledged the role of the European Union Agency for Network and Information Security (ENISA) in aligning the responses of cyber threats against essential services, including civil aviation, at European level,
- acknowledged the importance of the European Strategic Coordination Platform (ESCP) to coordinate the European approach to Cybersecurity in Aviation in Europe,
- called upon the European Commission, the European Aviation Safety Agency (EASA) and the National Aviation Authorities to take the next steps in their System-of-Systems approach in order to create a level playing field in Cybersecurity in Aviation among all stakeholders relevant for European aviation,

- acknowledged the role of the European Centre for Cyber Security in Aviation (ECCSA) to facilitate information sharing among aviation stakeholders including the drone industry and to coordinate the response to cyber-threats,
- supported the international commitment of EASA to support other Regional Safety Oversight Organisations (RSOOs) with its experience related to concepts, rulemaking, and training for oversight,
- called upon the continuation of the research and development activities for Cybersecurity as part of the overall Cybersecurity strategy of the European Union, e.g. to find solutions resolving the "stability/agility" dilemma,
- suggested to invite EU institutions to ensure a high level of priority of aviation-relevant subjects in the next Research Framework Programme (FP9),
- invite all relevant research actors including SESAR Joint Undertaking, Shift2Rail, national research institutions, industry, etc. to join efforts,
- recognized the valuable contribution on Cybersecurity in Aviation from the European Civil Aviation Conference (ECAC), notably the works of its Study Group on Cyber Security in Civil Aviation, including the updated ECAC Doc 30 Recommendations on cyber security and supporting Guidance Material and invite ECAC and EASA to join efforts,
- called on airports, Ground Handling Operators, maintenance organizations, air navigation service providers to develop information security management systems in accordance with specific procedures and appropriate standards,
- recommended to harmonise the security risk assessment methodologies,
- called upon a stronger partnership between regulators, operators, service providers, and manufacturing industry, in particular within the ESCP, where EASA welcomes and supports the Industry to come with standards,
- stressed the need to conclude the ESCP engagement phase before end of 2018 with:

    - the signing of the partnership Charter,
    - the adoption of the Aviation Cybersecurity Strategy, including its Roadmap,
    - and underlined the importance to start immediately afterwards the operational phase,
    - acknowledged the need to evaluate the progress made together with ESCP within 12 months.