Summary

LES DOSSIERS

CYBERMENACES
visant le transport aérien

CYBERTHREATS
targeting air transport

AAE Dossier #45 2019

Summary

CYBERMENACES
visant le transport aérien

CYBERTHREATS
targeting air transport

AAE Dossier #45 **2019**

Summary

Crédits photo couverture / *Cover credits:*
© matejmo, iStockphoto, 2015 / scyther5, iStockphoto, 2016

AAE
Ancien Observatoire de Jolimont
1 avenue Camille Flammarion
31500 Toulouse - France
Tel : +33 (0)5 34 25 03 80 - Fax : +33 (0)5 61 26 37 56
contact@academie-air-espace.com
www.academie-air-espace.com

ISBN 978-2-913331-78-5
ISSN 1147-3657
Dépôt légal : janvier 2019

Dossiers récents / *Recent Dossiers*

n°44 Le transport de passagers par appareils à voilure tournante à l'horizon 2050, 2018
Rotary wing aircraft for passenger transport by 2050, 2018

n°43 L'Espace au service de la sécurité et de la défense ;
pour une nouvelle approche européenne, 2018
Space systems supporting security and defence ; a new European approach, 2018

n°42 Aviation plus automatique, interconnectée, à l'horizon 2050, 2018
More automated, connected aviation by 2050, 2018

n°41 Les disparitions d'avions : une question pour les transports aériens, 2017
Missing aircraft: an issue facing air transport, 2017

n°40 Présent et futur des drones civils, 2015
Present and future of civilian drones, 2015

n°39 Matériaux aéronautiques d'aujourd'hui et de demain, 2014
Aeronautical materials for today and tomorrow, 2014

n°38 Comment volerons-nous en 2050 ?, 2013
Flying in 2050, 2013

n°37 Le Traitement des situations imprévues en vol, 2013
Dealing with unforeseen situations in flight; 2013

n°36 Quel avenir pour l'industrie aéronautique et spatiale européenne ?, 2013
What future for European aeronautics and space industries?, 2013

n°35 Trafic aérien et météorologie, 2011
Air traffic and meteorology, 2011

n°34 Une stratégie à long terme pour les lanceurs spatiaux européens, 2010
Long-term strategy for European launchers, 2010

n°33 Les Aéroports face à leurs défis, 2010
Airports and their challenges, 2010

n°32 Prise de risque : conclusions et recommandations, 2009
Risktaking: conclusions and recommendations, 2009

n°31 Pour une approche européenne à la sécurité dans l'espace, 2008
For a European approach to security in space, 2008

n°30 Le Rôle de l'Europe dans l'exploration spatiale, 2008
The role of Europe in space exploration, 2008

n°29 Le Transport aérien face au défi énergétique, 2007
Air transport and the energy challenge, 2007

n°28 La Sécurité des compagnies aériennes, 2007
Airline safety, 2007

n°27 L'Europe de l'Espace ; enjeux et perspectives, 2006
Space; a European vision, 2006

TABLE OF CONTENTS

Table of figures

1 FOREWORD

The number of people flying each year never ceases to increase, and yet the number of accidents continues to fall.

At the same time, it has been possible to meet the needs of greater efficiency in air transport and passenger demand for new services by means of broader connectivity delivered through greater digitalisation in the aviation world.

This increased connectivity, however, is in danger of impacting aircraft safety, with the risk of cyberattacks growing considerably in recent years. The aviation community has mobilised to deal with the threat of global attacks that are becoming increasingly sophisticated – whether motivated by terrorism, money or "hacktivism".

Patrick Ky, director of the European Aviation Safety Agency (EASA), said in October 2015 that the hacking of an aircraft in flight poses a real threat to air transport safety[1]*: "*To believe that air transport is safe from this kind of threat is to bury our heads in the sand. This is a serious subject that must be tackled.*"*

In November 2017, the Krakow High Level Conference on Cybersecurity in Civil Aviation[2] *advocated that safety and security*[3] *should be treated in a coordinated way, since security measures have the potential to reduce safety and vice versa.*

In April 2018, Guillaume Poupard, general director of ANSSI, told participants at a conference that air transport was among the most vulnerable sectors[4] *and raised the following question : "*If one day a cyberattack is shown to have caused the loss

---

1 *www.lesechos.fr/08/10/2015/lesechos.fr/021388802225_l-agence-europeenne-de-securite-aerienne-alerte-contre-le-risque-de-cyber-attaque.htm#u7YvvBmQIsm9XOLD.99*

2 *C.f. Appendix 4, p.128.*

3 *Security consists of averting intentional, malicious acts whilst safety involves the prevention of all aspects linked to accidents, by definition involuntary.*

4 *www.ihedn.fr/video/souverainete-numerique-et-cybersecurite*

of an aircraft in flight, who, in the following days, will take the decision to allow flights to resume?"

The tragedy of September 11, 2001 led the air transport community to look into how to protect itself against simultaneous cyberattacks targeting several planes. It is important to note, however, that since that date no other tragic events such as this one have occurred.

The Air and Space Academy focused on this topical issue in order to assess the operational risks incurred by air transport from cyberattacks. It aimed to raise awareness as to potential loopholes and set forth recommendations for the various stakeholders, insisting on the urgency to act.

Anne-Marie Mainguy

President of the Air and Space Academy (AAE)

2 EXECUTIVE SUMMARY AND RECOMMENDATIONS

The Working Group of the Air and Space Academy focused its thinking on the following theme:

> ***Cyberattacks may cause accidents or create serious incidents that endanger passengers and crews.***
>
> ***How to reduce the risks of occurrence and avert their consequences?***

In order to understand the subject as a whole, it should be noted that the world of commercial air transport forms an ecosystem or system of systems (SoS) composed of the following elements:

- *airliners;*
- *airlines;*
- *manufacturers, suppliers and subcontractors;*
- *air traffic management (ATM);*
- *airports;*
- *access and service providers[5];*
- *maintenance companies;*
- *and all associated personnel.*

*Civil aviation is increasingly **connected** thanks to modern communications means (internet, etc.) that allow high flow rates for passengers and crews. Ground systems*

5 *Among other aspects, service providers manage ground-to-air links and make data available.*

connectivity is also improving with the development of new air traffic management systems (notably SESAR[6] in Europe and NextGen[7] in the USA).

The openness of the systems in question significantly increases the attack surfaces of air transport. Consequently, in this digital transformation, ***safety and security models*** *must rapidly evolve to demonstrate that* ***cybersecurity***[8] *has been taken into consideration. The plane and its crew can no longer be "isolated" during the flight but must be capable of being autonomous, while being both connected and cyber-resilient.*

2.1 Risks

Attacks against air transport can take the form of "denial-of-service" or ***jamming*** *to block the incoming communication signals. Other possible attacks on communication links include* ***spoofing*** *(i.e. the transmission of* ***false data****), on the ground or on board aircraft. Depending on the corruption of such data, the consequences can be serious if there is no means of verifying the* ***availability****,* ***authenticity****,* ***integrity****,* ***confidentiality*** *and* ***traceability*** *of the information provided. Attacks may also target* ***operational software****, on board or on the ground. The presence of* ***malicious codes*** *(malware), programmed to trigger harmful actions at a specific time, is obviously a significant threat. Such malware may have been integrated at manufacturing stage of the aircraft by an agent of the manufacturer, an equipment manufacturer or a subcontractor, or may also have been inserted during maintenance operations or regular data updates.*

2.2 Risk management

As with risks involving hostile humans, it is necessary not only to provide fixed or adaptable protections, but also to set up organisational and human processes to fight against the attack with tools suited to the threat.

Cyberattackers are able to find flaws in practically all fixed defences of systems, including firewalls and other protections. The only real protection would be physical, with no wired or wireless communication and no possibility to transmit data by USB stick or other, but this type of protection is no longer practicable in a digitised, connected world. However, some relatively simple measures can slow down most attackers.

---

6 *The SESAR (Single European Sky Air Traffic Management Research) programme is designed to update current systems to provide Europe with efficient air traffic management systems.*

7 *Next Generation Air Transportation System is the new US ATM system currently under development. Designed to replace the National Airspace System, it is due to be deployed in the country between 2012 and 2025.*

8 *The term "cybersecurity" includes the notions both of security against cyberattacks and their impact on the safety of people and goods.*

*The high level coordination entity must ensure that all players comply with a predefined **security policy** (as recommended in ISO 270001 Standard[9]). When effective defence procedures are used, the different players' responsibilities must be clear at all times. In particular, in the case of defence actions, it is important to distinguish:*

*• improving **knowledge** of attack entry paths, by mapping and characterising these attacks via their signatures;*

*• **surveillance**, in order to rapidly detect and identify attackers and attacks, as well as their consequences, and thus guide actions;*

*• the **updating** of systems which have been attacked by means of software patches, in order to increase their resilience;*

*• the **defensive actions** themselves, including eradication of the attacks and their consequences, the possibility of tricking the attacker to orient them towards less dangerous actions and even, in some cases, return attacks.*

These defensive actions have repercussions on systems organisation and management and require the engagement of reliable human resources, competent in the latest technologies, including inventive professional hackers, who can work optimally with their cyberally colleagues from other organisations.

2.3 Recommendations

Vis-à-vis the industrialists

***Engineering**, **production**, **operations** and **maintenance** activities must be screened to identify, address and prevent potential vulnerabilities.*

> **► Recommendation R1**
>
> *Processes and techniques to protect manufacturers', suppliers' and subcontractors' **industrial resources** against cyberattacks shall be set up and monitored in order to achieve the same level of security as the Information System of the prime contractor.*
>
> ***Action: Manufacturers, equipment suppliers and subcontractors.***

> **► Recommendation R2**
>
> *All operators (including their freight forwarders) involved in the maintenance of onboard and ground equipment shall be certified, trained in cybersecurity procedures and regularly audited[10].*
>
> ***Action: Manufacturers, equipment suppliers and subcontractors.***

9 www.iso.org/isoiec-27001-information-security.html

10 At least as often as stipulated in the ISO 9001 and 27001 standards.

► ***Recommendation R3***

A policy for updating operational software and data shall be defined and implemented by all actors, with ***authorised personnel, dedicated and safe means*** *and* ***secure procedures****. In particular, this includes regular implementation of software protection patches.*

Action: Airlines, manufacturers, equipment manufacturers, maintenance companies and service providers.

At design stage

Although cabins are still vulnerable to possible breaches of security, aircraft ***cockpits*** *are well protected, especially on most recent aircraft, thanks to successive barriers and anti-intrusion filters.* ***Multimedia entertainment systems****, though, are much more open to cyberattacks.*

► ***Recommendation R4***

Onboard ***multimedia entertainment systems*** *for passengers shall comply with cybersecurity rules to protect system operation and passengers' data; it must be possible to* ***shut them down quickly****. Because of their rate of evolution, their* ***security condition readiness*** *shall be regularly controlled.*

Action: Airlines, IFE[11] suppliers and maintenance companies.

Tablets and Electronic Flight Bags

► ***Recommendation R5***

Software, data and internet connection of ***Electronic Flight Bags (EFB)*** *and other electronic cockpit tablets shall* ***imperatively be secured****. Safety demonstrations – including technical checks by specialised cybersecurity empowered personnel –* ***are mandatory****.*

Action: FAA, EASA and national authorities.

Communications

Digital technology is everywhere: in voice and datalink communications, in navigation, surveillance and anti-collision systems.

11 *IFE: In-Flight Entertainment.*

► ***Recommendation R6***

Ground communications between air and ground shall be ***segregated between different users (pilots, cabin crew and passengers)****. A risk reduction analysis based on the technical impacts and costs of the various solutions[12] is to be carried out.*

Action: Manufacturers and airlines.

Radionavigation and positioning data

► ***Recommendation R7***

To counter the non-availability or non-integrity of GNSS[13] satellite location information due to cyber-related events, ***SBAS*** *and* ***GBAS***[14] *systems shall evolve and* ***redundancy of ground-based radio-navigation means shall be maintained*** *in order to keep degraded mode air traffic flowing.*

Action: EASA[15], national authorities and air navigation services.

Surveillance: ADS/B

An important potential vulnerability concerns ***ADS/B***[16]*, a means of* ***surveillance*** *to identify and locate aircraft. Currently under deployment in the United States and Europe, ADS/B is a pillar of the air traffic management system renovation programmes SESAR and NextGen. ADS/B data is continuously transmitted by the transponder of the aircraft without the latter needing to be interrogated by the secondary radars on the ground.*

ADS/B allows anyone to constantly monitor planes trajectories. Attackers using ADS/B protocol are potentially capable of generating information on "false aircraft" or transmitting false locations to the ground. Ground controllers and the crew then have to manage these false aircraft and remove doubts, which can lead to a degraded safety level. ICAO[17] (in a June 2017 document), and the US GAO[18] alert

12 *This separation can be achieved either by using distinct communication terminals, or a single terminal, separating links by frequency, or again by multiplexing links on the same frequency but separating them logically (use of a virtual private network , VPN, for critical links).*

13 *GNSS: Global Navigation Satellite System, which includes the satellite constellations GPS, Galileo, GLONASS, BeiDou.*

14 *SBAS: Satellite Based Augmentation System. GBAS: Ground Based Augmentation System.*

15 *EASA: European Aviation Safety Agency – www.easa.europa.eu*

16 *ADS/B: Automatic Dependant Surveillance – Broadcast. The aircraft periodically sends its position and other information to ground stations and other aircraft in the zone equipped with ADS-B. It emits on the 1090 MHz frequency.*

17 *ICAO, International Civil Aviation Organization: www.icao.int*

18 Government Accountability Office report*, January 2018: www.gao.gov/assets/690/689478.pdf*

as to the vulnerabilities of ADS/B and recommend that States take risk reduction measures.

With ADS/B data issued by aircraft, mainstream sites (such as Flight Radar 24 and others) broadcast real-time information on the tracking of commercial flights.

> ► ***Recommendation R8***
>
> *Before switching to the use of ADS/B as the primary means of surveillance, a **risk analysis** shall be carried out, which may lead to the setting up of additional monitoring means. The ADS/B standard should evolve to improve its level of cyber-security protection (i.e. with data authentication and/or encryption[19]).*
>
> ***Action: ICAO, FAA[20] and EASA.***

Protections, human factors, supervision and control

*There can be no total protection; there will always be flaws in connected aeronautical infrastructures: the question is not whether there will be attacks, but rather when they will be. Air transport must therefore be more **cyber-resilient**, to ensure that aircraft remain safe and reliable, regardless of the type of attack. To this end, it is essential that **systems** and **personnel** develop **control** capabilities, recognise precisely what to do when an incident occurs, and of course, react immediately. It is also vital to detect "weak signals" that may precede cyber-incidents, denial-of-service or other attacks.*

> ► ***Recommendation R9***
>
> *Personnel at risk of **cyberattacks** on air transport shall be **trained** in the methods and practices for detecting, countering or limiting a possible cyberattack.*
>
> ***Action: All actors.***

*Feared events are not necessarily plane crashes, but potential disorganisation or panic, whether on board, in control centres or in terminals. These events can have significant media, economic and social repercussions, leading to loss of confidence in air transport. There can also be theft of commercial information, data or files, or disorganisation of the "Supply Chain" with manufacturing blockages at subcontractor level. All these **feared events** shall be **analysed** in order to assess on the one hand the probabilities of occurrence, depending on the criteria of **ease**, **attractiveness and impunity**, and on the other hand the potential gravity of the consequences.*

*With regard to **flight safety**, the basic principle is that the crew shall ensure data consistency relating to the trajectory and energy status of the aircraft in the short*

---

19 *Authentication and encryption means are widely used, for instance in banking and the judiciary system.*

20 *FAA, Federal Aviation Administration: www.faa.gov*

term (heading, vertical and horizontal speeds, altitude, thrust) and medium term (programmed waypoints, altitude constraints, approach and programmed track, etc.).

The aircraft must also be "transparent" and the crew should on the one hand have easy access to all information in autopilot mode and, on the other, have at their disposal tools and procedures to rapidly validate this data before its activation: one must not believe any uploaded data to be true without verifying it.

In case of doubt, the proposed data must be refused and other modes used as needed[21].

What solutions?

*Technical solutions exist, but **failings** are also often of **human** origin. It is therefore important to create devices with improved resistance to unsafe human intervention, with "deep defences" or successive barriers to be crossed before reaching the data. In addition, long-term actions should be carried out to raise the **awareness** of the personnel, not limited to crisis periods, and not overlooking aspects such as **organisation, empowerment and training** of personnel.*

Each actor in the air transport industry (large airline or small service provider) shall exercise monitoring, supervision and control through regular audits. In particular, the online and offline update and maintenance operations of the aircraft are to be monitored very closely, as they are an easy gateway to human interventions that can corrupt both the hardware and the data, and introduce malware.

Crisis management

When a cyberattack is declared during operation, despite implementation and monitoring of the previous preventive measures, then action must be taken by the concerned entities, on ground and on board, in a coherent manner at national, European, or even worldwide level when necessary.

The procedures and rules to be used by crews to thwart threats will only be effective if the time required to implement them is compatible with the time available to correct the corrupt situation. However, these can be complex, risky unexpected situations, during take-off or landing phases for instance. This available time parameter shall be taken into account in the definition of corrective actions.

*Similarly to organisation of the civil or defence security forces of each country, each actor involved in air transport must comply with a **safety policy** precisely defining the operating modes to be used when faced with the different types of attack, whether observed or anticipated.*

---

21 "Selected" or" manual" mode according to Airbus terminology, the other manufacturers provide equivalent modes with slightly different terminology.

► ***Recommendation R10***

Crisis management procedures shall be elaborated to deal with cyberincidents and shared with all actors.

Action: All air transport stakeholders.

Management of cybersecurity and lessons learned

A cybersecurity management system should exist for all air transport stakeholders, and should include a verification that the rules of IT health are properly applied and are accompanied by measures for the prevention and treatment of incidents.

Incidents will occur. Unfortunately, the player on the receiving end of the attack tends not to divulge the information – and it is difficult, even after much digging, to find the real causes of incidents and to distinguish between failures, bugs, false manipulations or real acts of malicious intent.

As with the analyses conducted into air incidents and accidents, the human factors that cause cyberincidents should be systematically examined and exploited. These include not only the decisions and actions that have been used to detect and counter a threat in due time, but also those that have resulted in a "successful" attack.

► ***Key Recommendation R11***

All certified air transport actors shall ***mandatorily report, share and then systematically process cyber-incidents*** *in the same way as air accidents and incidents are reported, shared and analysed in a process that has led to a significant increase in air transport safety.*

Action: ICAO, FAA, EASA and national authorities.

Public actors have assumed their responsibilities. The US Department of Homeland Security holds briefings for cybersecurity professionals to share information about potential threats, new tools used by perpetrators and how they work.

The French Agency for Security Information Systems (ANSSI) and the European Centre for Cybersecurity in Aviation (ECCSA, created in 2017 under an EASA initiative) are aware of the threats related to air transport and analyse, characterise and share them (in a secure way) with the concerned actors. These agencies have yet to reach full capacity.

Industrialists in the United States have set up Information Sharing and Analysis Centers (ISACs). The same kind of centres are in the process of being created in Europe.

Standards, certification and regulatory aspects

*With regard to **regulation and certification**, some standards exist but remain to be applied, and their implementation must then be regularly monitored by audits conducted by certified authorities or laboratories. There is, however, no coordination and harmonisation of regulations at worldwide level.*

> ► ***Key Recommendation R12***
>
> *There is an **urgent** need to develop a **harmonised worldwide regulatory framework** for cybersecurity in civil aviation, within a global management system (integrating security and safety) and to ensure its implementation and compliance **through qualified cybersecurity entities**.*
>
> ***Action: ICAO Member States and regulatory bodies.***

The example of the security standards of the payment card industry is an interesting one. Set up in the 2000s, a standard was created to increase control over cardholder information in order to reduce the fraudulent use of various payment instruments. Banking authorities – while retaining their role of certification – delegated responsibility for the technical evaluation to qualified trusted third parties to enable an efficient industrial response internationally.

*The certification of interbank exchanges for credit cards, as well as procedures for updating internet "boxes", should serve as examples in order to develop a system of **cybercertification** in the area of air transport and to ensure the security condition readiness.*

> ► ***Recommendation R13***
>
> *Certification and authentication processes for sensitive data exchanges based on industry standards shall be developed or adapted and implemented.*
>
> ***Action: Industry.***

Governance

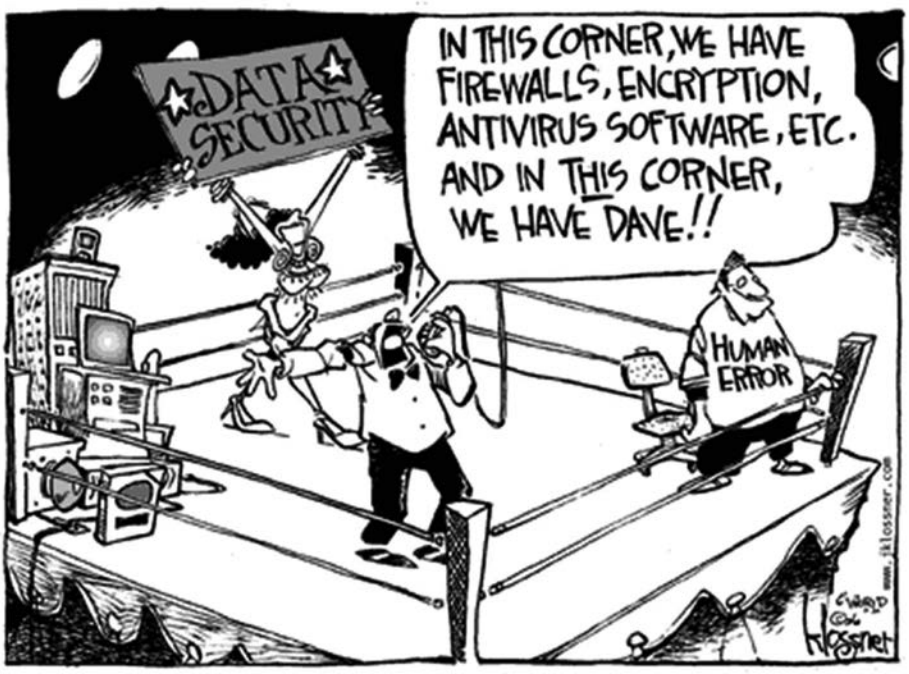
*The real difficulties concern **governance and responsibility**, complex problems linked to different legal regimes, to public and private actors and to different links in the supply chain. The chain of **cybertrust** in civil aviation needs to be strengthened.*

***International organisations** such as ICAO, IATA, CANSO, EASA, etc. are aware of cyber threats and risks to air transport. As emanations of States and of the involved actors, instead of limiting themselves to understanding, acknowledging, recognising, encouraging, promoting, supporting, welcoming... they should obtain **mandates from them to act quickly**.*

► ***Key Recommendation R14***

ICAO shall lead and coordinate at worldwide level all activities contributing to enhancing cybersecurity in civil aviation. EASA and national authorities shall be ***given a mandate*** *to* ***define and decide on cyber action plans*** *and quickly put in place* ***roadmaps*** *with associated* ***resources and timelines*** *together with minimum short term measures.*

Of course, the above recommendations can only be adopted and implemented by means of close coordination, harmonisation and collaboration between all air transport stakeholders.



3 INTRODUCTION

We hear more and more about cybersecurity, cyberspace, cyberattacks and cybercriminals. Faced with these new threats, air transport risks becoming less safe.

Hackers are able to break into computers, websites, networks – even the most highly protected – and cause considerable damage, including disruptions to service, blockages and even paralysis of up to several days. These attacks can also result in data or monetary theft but also, more insidiously, the insertion of a "Trojan horse" programme designed to activate on a given date or in a given context and corrupt onboard equipment software.

The air transport world forms an ecosystem or System of Systems (SoS) composed of the following elements (see Figure 1, p. 36):

- *commercial aircraft;*
- *airlines;*
- *manufacturers and their equipment suppliers;*
- *air traffic management (ATM);*
- *airports;*
- *access and service providers[22];*
- *authorised maintenance organisations (MROs).*

These players are more and more highly "connected", exchanging essentially digital data. They are also connected to the internet and to different types of "Clouds", potentially introducing loopholes for use by cyberattackers.

These exchanges rely on the input of many different people: crews, air traffic controllers, airline OCC staff and airport personnel, datalink suppliers, MRO services...

22 *Among other services, service providers manage air-ground links and make data available.*

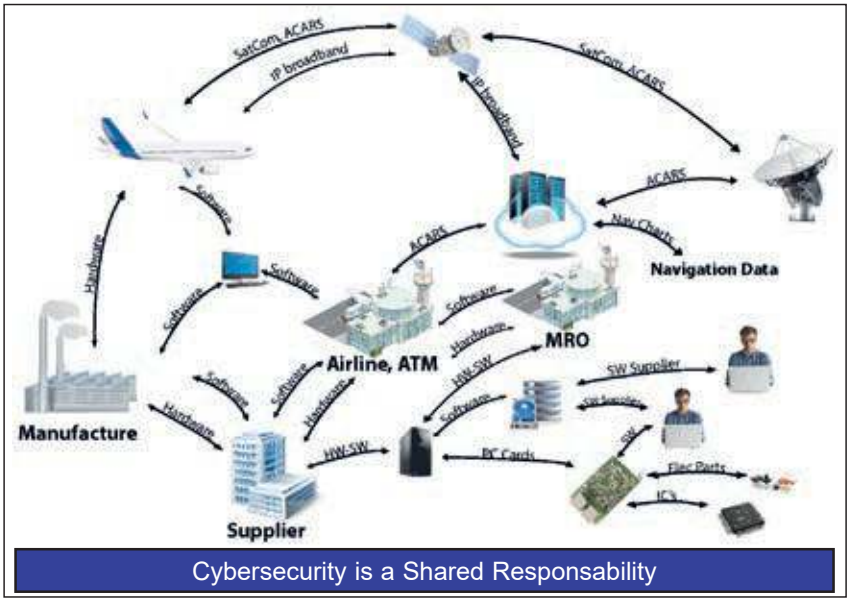


Figure 1: The air transport environment.

In its latest annual safety report[23], the International Air Transport Association (IATA) proposes to clarify concepts of cybersecurity for civil aviation by distinguishing:

- *"Aviation Cyber", which concentrates on potential damage to the aircraft when **on the ground**, before or after the flight, or during a maintenance phase;*
- *"Cyber Threat and Risk", which is focused on **Safety of Flight**[24] aspects during flight phases, from take-off to landing (in fact from engine start-up to stop).*

This dossier focuses on the above cyber threats and risks to the aircraft themselves, excluding potential cyberattacks on:

- *passengers (data theft);*
- *airlines (disruption of online ticketing, delays, data theft...);*
- *airports (delays, disruption of controls and displays, etc.);*
- *the industrial activities of manufacturers and equipment suppliers (delays in deliveries, data theft, etc.).*

The Working Group of the Air and Space Academy focused its reflections on the following subject:

Cyberattacks can cause accidents or create serious incidents that will endanger passengers and crews. How to reduce the risks of occurrence and avert their consequences?

23 *IATA Safety Report 2016.*

24 *Security deals with malicious acts whereas safety deals with accidental events.*

Cybersecurity in commercial civil aviation needs to be addressed with a Systems of Systems approach by mapping end-to-end data flows. The analysis shows that there may be loopholes in the air transport ecosystem. Vigilance should be exerted as regards the following aspects:

- ***voice communications and data links** between air and ground (uplinks and downlinks);*
- *any cabin equipment (seat, screen, etc.) involved **in In-Flight Entertainment** (IFE) for passengers, either by direct interface or by wireless link;*
- *all **individual equipment** (smartphones, tablets, PCs) belonging to passengers or to flight and cabin crews;*
- ***data links on the ground**, when taxiing or docked at gateway, by GSM, WiFi, Wimax;*
- *the **maintenance chain**, since some equipment is periodically updated by download or by direct human intervention on the equipment.*

The recommendations of this dossier highlight the need to define and apply norms and standards worldwide to protect onboard and ground systems – starting with the most critical ones – to exchange information on incidents and to raise awareness and promote good practices in the relevant players through training exercises.

4 TOWARDS EVEN MORE HIGHLY CONNECTED AVIATION

Air transport has always been a target for terrorists. Today the arrival of digital services for users (passenger WiFi and mobile applications of airlines) and crews (EFB[25] for pilots, tablets for cabin crew), together with the new networks and computer systems needed to support the growth of global air traffic, have resulted in an increase in possible ways of attacking air transport – and specifically aircraft – and in the associated risks. Means of remote interaction with this larger and more complex system of systems are more numerous and offer new exploitable vulnerabilities. Many scenarios are possible, from the interruption of airport display services to attacks on aircraft equipment software and data and even the wholescale paralysis of air traffic.

In this digital transformation, the engineering, production and operations of an aircraft fleet, as well as its security and safety models, must rapidly evolve to demonstrate their cybersecurity credentials. The plane can no longer be "isolated" during flight; it must be capable of being at once autonomous, cyber-resilient and connected.

This greater connectivity in aviation makes it possible to benefit from practically the same data and services in the air as on the ground, the challenge being to demonstrate safe, secure flights to passengers and airlines. All software is vulnerable, though, and connectivity increases risks. In addition, this growing need for connectivity is coupled with the need for frequent updates (every 28 days for AIRAC cycles[26], for example; before the flight or in real time for NOTAMs, ATIS, weather reports), thereby increasing the risk of data corruption.

---

25 EFB: Electronic Flight Bag, which replaces voluminous, cumbersome pilot cases.

26 AIRAC: Aeronautical Information Regulation And Control.

With regard to in-flight safety, the basic principle is that the crew is responsible for ensuring the consistency of data relating to the aircraft flight path and energy state, both in the short term (heading, vertical and horizontal airspeed, altitude, thrust) and the medium term (programmed waypoints, altitude constraints, programmed approach and runway, etc.).

However, this depends on the aircraft being "transparent", with the crew having easy access to this information in autopilot mode as well as possessing the tools and procedures capable of rapidly validating this data before its activation: it is important not to accept uploaded data on face value, without verifying it. In the event of doubt, the proposed data must be rejected and other modes used as needed ("selected" or "manual" according to the Airbus jargon; other manufacturers offer equivalent modes with sometimes different terminology).

How does this digital transformation impact the different aviation systems?

4.1 Engineering

Our skies contain very few connected aircraft for the moment, but this will change as certain planes benefit from STC[27] enhancements to passenger or cockpit connectivity to meet the demands of airlines; latest generation aircraft are anyway connected by design (A350, Dreamliner B787).

According to Thales[28], these improvements involve the writing, checking and securing of millions of lines of code, not only during the design stage but also in the production and maintenance phases and throughout the life of the aircraft, with software updates needed to protect it sufficiently against perceived changes in attacks. The current trend, to reduce software development costs, is to use commercial software packages and to carry out developments at low levels (DAL-D or -E). But a lack of software robustness may provide the opportunity for cyberattackers to insert corrupted files. Measures must therefore be taken to protect the software, not only at the design stage, but also during its manufacture and maintenance phases, even if this generates additional costs. One revolution in aviation will consist of managing security patches to be deployed regularly in a preventive way, whilst preserving airworthiness credits obtained by the aircraft at entry into service. This is the condition for cyber-resilience in aviation. The requirement of cyber-resilience therefore induces changes in the engineering process, but its utilisation may also require changes to aircraft architectures to reinforce the aircraft's primary points of interconnection (software or data uploading and downloading processes, data communication means, primary aids to navigation).

For example, the A380 design called for special engineering measures by which Airbus was able to define its own standards and test the aircraft with penetration

27 *STC: Supplemental Type Certificates.*

28 *www.atlanticcouncil.org/publications/reports/aviation-cybersecurity-finding-lift-minimizing-drag*

tests designed and carried out by an internal team of hackers. For even more connected, new generation aircraft (A350 and Neo versions), this method has become widespread with technical audits (penetration tests) carried out by different teams, according to a well-established protocol. In the same way, some engine manufacturers have defined and applied their own standards, because there are no security regulations as yet.

4.2 Production

It is not enough to protect only the target, i.e. the aircraft. Factories, too, are connected through their information systems and PLCs – Programmable Logic Controllers (as witness the impact of the Wannacry attack on Renault factories): they are notably equipped with remote access for real-time maintenance. What would have the worst impact: stopping production, or leaving undetected a modification to a manufacturing process that would lead to a major defect in an entire production cycle?

Here too, the digital factory will only come about if full protection is provided for its critical machines and any potential opening to public networks is managed intelligently.

Thus, in order to secure its company and its products, Airbus has launched a major cyber-protection campaign with both internal and subcontractor audits (an investment of 300 M). And in terms of its supply chain[29], Airbus has defined and imposed cybersecurity clauses on its Tier 1 subcontractors. It is not yet known as to whether the latter they have taken them into account and passed them on to their own subcontractors.

> ► ***Recommendation R1***
>
> *Processes and techniques to protect manufacturers', suppliers' and subcontractors' industrial resources against cyberattacks shall be set up and monitored in order to achieve the same level of security as the Information System of the prime contractor.*
>
> ***Action: Manufacturers, equipment suppliers and subcontractors.***

The digital transformation of companies known as the "Smart Factory – Industry 4.0" is a related subject concerning mainly aircraft and equipment manufacturers. Faith in digital equipment and tools requires a very high level of cybersecurity. This theme has been studied within the Académie des technologies*, which has highlighted the fact that cybersecurity solutions are generally prohibitively expensive for SMEs.*

29 *www.forbes.com/sites/oliverwyman/2018/04/11/how-aviations-global-supply-chain-may-open-up-the-industry-to-cyberattack/#ec47d1d31806*

4.3 Operations and maintenance

Cutting aircraft operating costs is key to improving airline profitability, so digitalisation and cost optimisation activities are both on the rise. Managing this ecosystem, which dematerialises processes and maintenance data between the aircraft and the ground, is a challenge in terms of safety and security.

On certain aircraft, technical monitoring data is transmitted by ACARS when in flight, or via a ground link after landing, when the aircraft is taxiing to the terminal gate.

Specific line maintenance equipment has been replaced by laptops with USB drives, or even by e-maintenance, authorised on the gateway, as long as the maintenance equipment itself possesses a means of communication with the maintenance centre, or even with the relevant avionics unit. The maintenance manual becomes an e-log book shared between the pilot and the maintenance operator.

If one takes the example of software reloading or database uploading, these data carriers can potentially be infected with malware if maintenance operators lack adequate training in and procedures for proper cybersecurity practices, and if these sets of equipment are not protected in the same way as the overall information system of the company. The maintenance operator must be considered trustworthy (see § 7.3: human factors).

Remote attacks on the airport network are also possible with all kinds of impacts: sabotage, theft of data or simply paralysis of maintenance operations.

> ► ***Recommendation R2***
>
> *All operators (including their freight forwarders) involved in the maintenance of onboard and ground equipment shall be certified, trained in cybersecurity procedures and regularly audited[30].*
>
> ***Action: Manufacturers, equipment suppliers and subcontractors.***

4.4 Connected aircraft

Aircraft systems architecture was standardised well before the demands of connectivity. The main thrust of this process was to secure operational functioning and separate areas of different criticalities. In Figure 2, four such areas are identified:

- ***pilot/cockpit**: associated with control of the aircraft, this area contains the most critical functions[31];*

30 *At least as often as stipulated in the ISO 9001 et 27001 standards.*

31 *i.e. subject to catastrophic breakdowns.*

- ***links with the airline****: information here is transmitted by means of equipment such as EFB[32] (Electronic Flight Bag), through pilot or cabin crew tablets, or directly via communications with the Operations Control Centre (OCC);*
- ***passenger cabin entertainment****: this area includes all equipment offering an interface with passengers, particularly IFE (In-Flight Entertainment) multimedia systems, whether or not connected (by LOS – Line of Sight – or via satellite);*
- ***passenger specific****: this comprises passenger equipment (PCs, tables, smartphones) that can connect to the passenger cabin Wifi with or without SATCOM connectivity service.*

Thanks to this separation of domains, data flows can be controlled at interconnections through successive firewalls and secure data exchange gateways. The basic principle is to enable unrestricted transmission of information from the most critical to the least critical area, but to prohibit or limit transfers in the other direction: a kind of "diode" (anti-return filter).

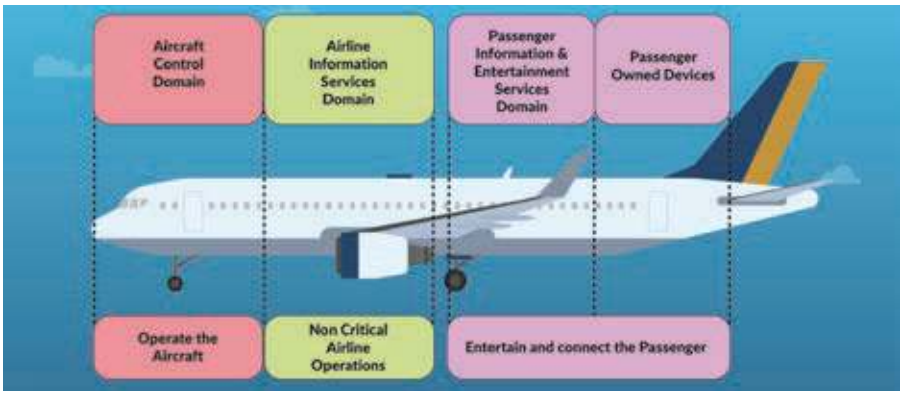


Figure 2: The different areas of the connected aircraft[33].

What does the connected plane bring to this situation?

Essentially new in-flight means of communication are provided by data link, whether LOS or satellite (Iridium, Inmarsat, Global Express).

New, more connected aircraft programmes are currently being secured, but there are of course large fleets of aircraft already in service. These older design planes can also be targets although, being less connected and less "digital", they are perhaps less vulnerable.

---

32 *There are two types of EFB: either installed in the cockpit, or mobile (tablets). The applications that are authorised in these two types of EFB are slightly different in terms of criticality. Pilots' tablets are mobile EFBs.*

33 Atlantic Council (2017): Aviation Cybersecurity – Finding Lift, Minimizing Drag*: www.atlanticcouncil.org/publications/reports/aviation-cybersecurity-finding-lift-minimizing-drag*

4.5 The connected cabin

*In the **cabin**, connectivity for passengers can be offered locally with stand-alone, real-time ("at home in the air") wifi solutions.*

***Passenger In-Flight Entertainment (IFE)** is the part of the aircraft most open to the outside world. Although not yet standardised, IFE connected multimedia solutions therefore include a host of security measures to control these flows, using successive, robust barriers to prevent penetration into critical aircraft systems (sometimes going as far as to isolate certain of them). These solutions range from simple best practices to firewalls and intrusion detectors. They have matured over time and the newest are the most up-to-date.*

> ► ***Recommendation R4***
>
> *Onboard **multimedia entertainment systems** for passengers shall comply with cybersecurity rules to protect system operation and passengers' data; it must be possible to **shut them down quickly**. Because of their rate of evolution, their security condition readiness shall be regularly controlled.*
>
> ***Action: Airlines, IFE[34] suppliers and maintenance companies.***

*In terms of **connections with the airline**, complementary connectivity for approach must be taken into account, as well as dedicated means of communication in airports (Wifi / WiMax, or 3G / 4G / 5G telecommunications).*

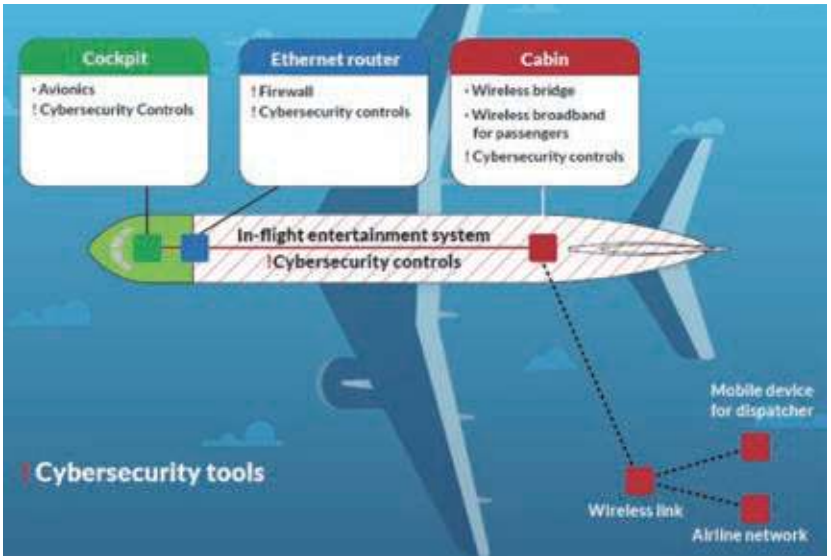


Figure 3: Permeability between cockpit, communications router and cabin[35].

34 *IFE: In-Flight Entertainment.*

35 *According to the document:* Atlantic Council (2017), Aviation Cybersecurity – Finding Lift, Minimizing Drag.

The figure 3 shows the recommended level of permeability between the three worlds: cockpit, airline information with no direct influence on the flight, and cabin.

4.6 The connected cockpit

Electronic Flight Bags (EFB)

EFBs in the cockpit may have vulnerabilities. Some EFBs are installed on aircraft, but others are portable and can be connected to the internet.

> ► ***Recommendation R5***
>
> *Software, data and internet connection of **Electronic Flight Bags (EFB)** and other electronic cockpit tablets shall **imperatively be secured**. Safety demonstrations – including technical checks by specialised cybersecurity empowered personnel – **are mandatory**.*
>
> ***Action: FAA, EASA and national authorities.***

Pilot-Air traffic controller voice communications in VHF

Controllers → Ground transmitters → Aircraft: Ground communication links between air traffic controllers and VHF transmitters are increasingly digital. The voice is digitised on the ground using the so-called Voice over internet Protocol (VoIP). In the transmitting ground station, the digital voice is then decoded and transformed into an analogue voice, modulated in amplitude and transmitted to the aircraft unencoded. There is no authentication of speakers (aircraft or controller) however and it is possible for frequencies to be scrambled or for outsiders to intrude into these links.

Aircraft → Onboard transmitters → Controllers: Conversely, the analogue voice of the pilot is modulated and transmitted by the aircraft. In the receiving station on the ground, the voice is demodulated, then digitised, encoded and transmitted using ground networks and VoIP. In the ATM structure, the voice is decoded and transmitted to the controller in analogue form.

*Ground and air networks: Ground communication terminal systems are based on software, with VHF transceivers on aircraft and on the ground increasingly using **Software Defined Radios**[36].*

***Voice communications** between pilots and controllers, which used to be analogue in clear VHF, are thus now **partially digital, processed by software**, although on dedicated networks. These digital communications remain vulnerable, easy to scramble and spoof, and by no means confidential (which is not the case in military aviation). The use of ATM-specific voice messages between pilots and air traffic controllers can mitigate this risk.*

36 *Radiocommunication system configurable using digital signal processing techniques on programmable digital circuits.*

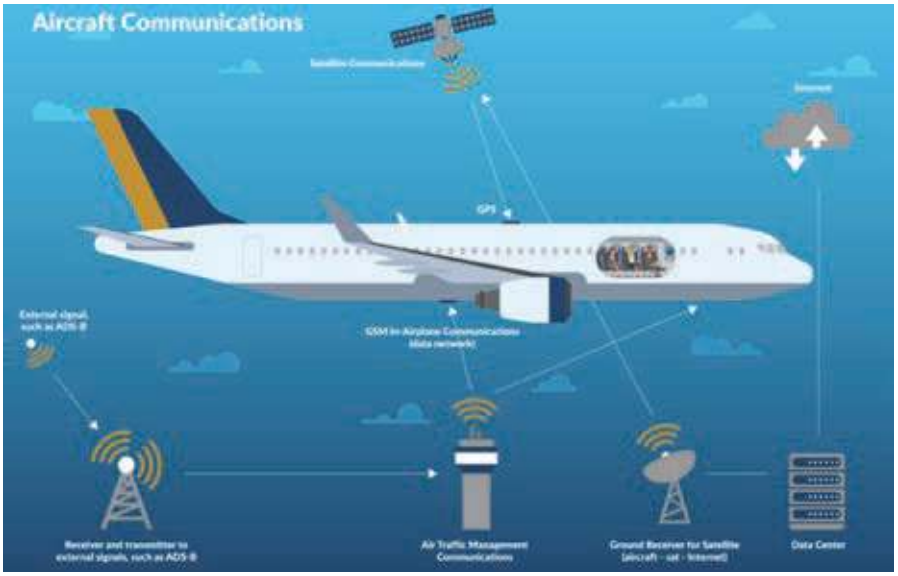


Figure 4: Communications between air and ground[37].

Voice communications between ATM bodies

These communications are also increasingly transmitted in digital form, via ground networks, using VoIP. They too are potentially open to cyberattack.

VHF datalink[38] known as VDL-Mode 2 (or VDLM2)

Communications take place in the VHF band according to an ICAO-standardised protocol[39]. A few different services are available[40]. French navigation directorate DSNA has started to implement VDLM2 data links through service contracts with SITA and ARINC and has updated its information system to allow this air-ground data link to be used as a means of air traffic control.

ACARS messaging on VHF

The ACARS communication protocol uses VHF messaging to transmit flight data that can be used for aircraft maintenance.

37 *From the document:* Atlantic Council (2017), Aviation Cybersecurity – Finding Lift, Minimizing Drag.

38 *Data link between aircraft in flight and ATM.*

39 *ATN (Aeronautical Telecommunication Network) protocol using IPS standard.*

40 *Baseline 1 (B1) defined by SESAR JU, consisting of login, change of frequency and check microphone request message.*

Satellite digital links between aircraft and ATM

Automatic position reports (ADS/C[41]) are transmitted either by SATCOM[42] or VHF. These satellite links are also used for the transmission of ACARS messages between aircraft and airline OCCs. These communications are open to cyberattack.

These new facilities open up new opportunities for data exchange, with communication channels being grouped together to reduce the amount of equipment on the plane. For example, an airline that has no means of connectivity may decide to use cockpit data link in descent or climb in order to communicate with its cabin crew in flight; or an aircraft manufacturer may wish to cut back on equipment by using the Satcom for both cockpit and cabin connections; or again an airline may wish to use a passenger Wi-Fi hotspot for exchanges with the ground.

Some airlines such as Air France/KLM use private links (and not direct internet connections) for data and software updates. This reduces the attack surface.

> ► ***Recommendation R6***
>
> *Ground communications between air and ground shall be **segregated between different users (pilots, cabin crew and passengers)**. A risk reduction analysis based on the technical impacts and costs of the various solutions[43] is to be carried out.*
>
> ***Action: Manufacturers and airlines.***

4.7 The evolution of Air Traffic Management

As air transport increases, traffic is becoming denser. The system must therefore be modernised to increase operational capacity while keeping down operating costs and maintaining a high safety level security.

*These changes require a revolution in ATM technologies, architectures and operating modes. Exchanges between ground and air are evolving towards data communications that enable automatic sharing of trajectories by the two systems. In this way, analogue voice communications are gradually being replaced by digital exchanges between computers (see § 4.5). Isolated control centres are thus transformed into **network nodes** connected to an aviation "intranet" that comprises both fixed elements – such as other control centres or radio-ground stations – and mobile elements (see Figure 5, next page). Two key trends stand out:*

---

41 *ADS, Automatic dependent surveillance - contract: the aircraft uses its satellite or inertial navigation systems to automatically determine and transmit to the centre in charge its position and other information.*

42 *Satcom: telecommunications via satellite.*

43 *This separation can be achieved either by using distinct communication terminals, or a single terminal, separating links by frequency, or again by multiplexing links on the same frequency but separating them logically (use of a virtual private network , VPN, for critical links).*

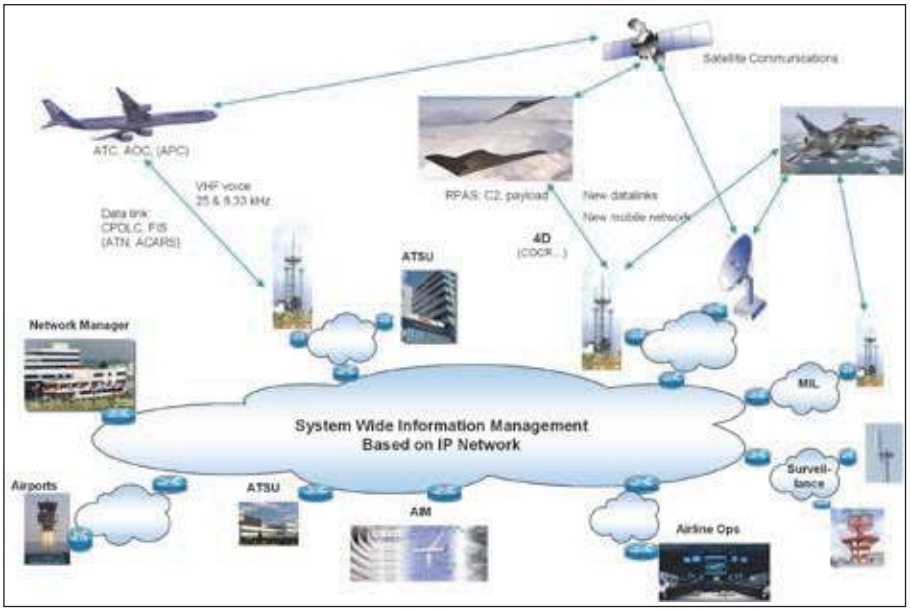


Figure 5: Links between the different components of the SWIM network.

- *greater connectivity between actors (air navigation service providers[44], airlines, airports, etc.) to increase their interaction capacity and efficiency;*
- *the use of standard business components (such as servers, workstations, routers, etc.) and standard protocols (such as TCP/IP, HTTP, SSL, etc.) to optimise development and maintenance costs and interoperability and also to increase the reactivity and speed at which new ideas can be developed.*

*The ATM system is therefore evolving towards a **SWIM (System Wide Information Management)** architecture by which each actor is a network node, exchanging data with a large number of other partners. SWIM is a dedicated set of services, connected to the "outside world" by standard internet protocols, which facilitate air traffic management: these interfaces must therefore also be secured.*

Implementation of the SWIM concept will bring additional services and efficiency. It will enable all aviation stakeholders to access the data they need to perform their tasks and enable collaborative decisions supported by an optimised use of all resources. The interoperability achieved will enable information management by means of shared Aeronautical Information Reference Models (AIRM) with exchanges facilitated by connection to service portals rather than dedicated point-to-point interfaces. SWIM will however coexist in the early years with existing data exchange systems, means and protocols (c.f. Figure 6, next page).

44 *ANSPs : Air Navigation Service Providers.*

Figure 6: Evolution of Air Traffic Management towards a SWIM network.

The interconnection of the different systems improves service but at the same time increases vulnerability to malice, intrusion or attack. To meet the safety level required of air traffic control, it is therefore necessary to ensure the cybersecurity of this set of services and to specify requirements in terms of availability, authenticity, integrity and confidentiality, as well as traceability. The flip side of this evolution is the broadening of the attack surface, through greater connectivity and the use of standard components and protocols. The resulting vulnerability is widely known to attackers, whose various exploits are available on the internet, and leads to an increased likelihood of cyberattacks on ATM networks.

4.8 Navigation systems

GNSS satellite systems[45]

Several satellite navigation systems exist. Although the American GPS is the one most used currently on board aircraft, the Russian GLONASS has also received ICAO standardisation. The European Galileo system is being rolled out, as is the Chinese BeiDou system (a regional component of which is already operational). As a result, by 2025-2030, close to 120 satellites should be in orbit for use by civil aircraft. These systems – designed to operate in a military environment (except for Galileo) – are already equipped with protections seen to be sufficiently robust (best possible state of the art) against intrusion or hijacking threats. They position the aircraft with sufficient accuracy, integrity, availability and continuity, taking into account a set of known, characterised failure modes.

The risks of signals from satellite navigation systems being spoofed are currently under assessment, together with mechanisms for mitigating the impact. It has been shown to be possible to spoof GNSS receivers into believing they are at a different location to their actual position. Any attempt to remotely ***spoof*** *satellite navigation simultaneously on several aircraft over an extended area is however difficult. Spoofing can also be carried out by a hacker in the cabin.*

In addition to spoofing satellite navigation signals, we must also consider the ***spoofing of data*** *from the SBAS and GBAS augmentation systems.*

45 *GNSS, Global Navigation Satellite System: set of satellite constellations (GPS, GLONASS, Galileo, BeiDou) used as positioning references.*

SBAS systems[46] *enable equipped aircraft to carry out* ***precision approaches*** *up to a decision height of 200 feet, similar to that of ILS*[47] *Category I, whose systems are being replaced in many aerodromes, particularly in France. The signals transmitted by the geostationary satellites of the SBAS systems use the same frequency (L1) and modulations as the navigation satellite signals. SBAS systems deploy a large number of stations to monitor signals from satellite navigation systems in and around the covered area. Ground links between these stations are vulnerable to jamming by hackers capable of* ***replacing*** *data by false information, and ground stations could also be susceptible to attempts to insert corrupted data into the system. In Europe, the next version of the regional SBAS system (EGNOS version 3), scheduled to be implemented by 2024, needs to be considerably reinforced against cyberattack. In addition to the cybersecurity of the inter-station network and individual stations, work is also underway within the ICAO Navigation Systems Panel, under the impetus of the EC, to come up with a process for authenticating messages transmitted via geostationary datalink to the aircraft.*

GBAS systems are based on monitoring stations located at the airport and have a range limited to the vicinity of equipped aerodromes. There are few GBAS systems in use in the world today. They enable Category I precision approaches. Future GBAS systems being tested should enable Category III precision approaches. A potentially weak point of these systems is the use of a VHF data link between the GBAS station and the aircraft; however this link is now equipped with a data authentication protocol, compliant with ICAO standards. The question must also be addressed of how to protect the station against an attempt to insert false GNSS signals.

Finally, it is also important to take into account operational elements that naturally reduce risks of spoofing:

- *onboard receivers make a very large number of checks before using GNSS signals and providing a position;*
- *it seems unlikely that the spoof could bypass the crew's continuous trajectory control;*
- *most airliners are equipped with* ***inertial control units*** *whose positioning is merged with that of data from the GNSS sensor, enabling them to detect abnormal drift affecting GPS signals (since inertia is not affected) and to continue navigation without GPS for a certain time. However, positioning accuracy can be insufficient at end of flight to follow certain trajectories, in particular for final approach and landing phases;*
- ***ground-based radionavigation means*** *such as NDBs, VORs and DMEs enable navigation in the event of disruption to satellite navigation signals. ILS allows*

46 *Satellite Based Augmentation System : EGNOS in Europe, WAAS in North America.*

47 *ILS, Instrument Landing System: systems provide a guidance beam for the final approach course. Slant and lateral ILS guidance information is displayed on the cockpit displays.*

landing in such disturbed conditions of disturbance, on certain terrains. This is also the case of VOR and NDB.

If a deliberate attempt at spoofing or jamming occurs, though, any significant drift or loss of GNSS will be announced by the crew to ATC who, as soon as more than two aircraft under satellite navigation have announced disrupted navigation, will suspect interference in the area.

Other aircraft in the same sector will be systematically informed and, following instructions from ATC, will then potentially have to navigate without the use of satellite navigation, either by means of radionavigation on the ground or by following radar headings provided by ATC via secondary ground radar. The presence of an area in which GPS signals are spoofed or heavily scrambled will thus be handled by ATC according to a procedure similar to that used in the case of jamming of GPS signals. It is therefore conceivable that no additional actions will be needed to cope with a spoofing crisis management, as compared to simple scrambling, when this procedure is properly in place.

ANSPs are currently in the process of streamlining ground-based radionavigation to reduce their infrastructure costs, as part of a comprehensive SESAR drive for rationalisation. Today this rationalisation works on the basis of minimum networks capable of providing an alternative service in the event of a disrupted or unusable GNSS situation. ANSPs are not required to set up these alternative navigation networks with the same level of traffic flow as nominal conditions and it is generally agreed that in densely populated areas, making extensive use of satellite navigation, economic penalties will result from this situation of reduced capacity.

In conclusion, it is important to mention that civil aviation GNSS receivers need to evolve over the next decade to embrace the use of ***DFMC***[48] *signals. The multiple redundancy of navigation signals and additional robustness of these receivers will help in further minimising the risk of external control of satellite navigation signals.*

> ► ***Recommendation R7***
>
> *To counter the non-availability or non-integrity of GNSS*[49] *satellite location information,* ***SBAS*** *and* ***GBAS***[50] *systems shall evolve and* ***redundancy of ground-based radio-navigation means shall be maintained*** *in order to keep degraded mode air traffic flowing.*
>
> ***Action: EASA***[51]***, national authorities and air navigation services.***

48 *Dual Frequency Multi Constellation services.*

49 *GNSS, Global Navigation Satellite System, which includes the satellite constellations GPS, Galileo, GLONASS, BeiDou.*

50 *SBAS: Satellite Based Augmentation System. GBAS: Ground Based Augmentation System.*

51 *EASA, European Aviation Safety Agency: www.easa.europa.eu.*

4.9 Surveillance and anti-collision systems

Transponder

*The surveillance of civil air traffic relies on the use of a **secondary radar** on the ground and at least **one mandatory transponder** on board each aircraft. The position of the aircraft is determined on the ground from the measurement of the round trip time, and the measurement of the azimuth of the aircraft by the rotating antenna of the radar. The identity and altitude of the aircraft are transmitted in coded form by the transponder. Corruptions in transponder software may allow the transmission of a false identity or an incorrect altitude. False identity will not be correlated with aircraft flight plans and may be rejected. Incorrect altitude will be harder to detect.*

Anti-collision and ACAS

*Secondary radar is also at the heart of the **ACAS collision avoidance system**. On board commercial aircraft is a **radar interrogator** that issues short-range interrogations in all directions. A directional receiving antenna is used to roughly measure the azimuth of all aircraft that have responded to the interrogations. The distance is estimated from the measurement of the response time. The estimated altitude is that transmitted by the transponder of the aircraft interrogated. There again, in the event of false altitude, this can result either in a lack of detection of the risk of collision or, on the contrary, a false alarm and a manoeuvre causing a risk of collision. The transponder transmits information that has been issued by the flight management computer. During maintenance and update operations, the software for generating the parameters to be transmitted may be intentionally modified and produce false information.*

ADS/B

*Secondary radars should gradually disappear and be replaced by the **ADS/B system**[52]. At regular intervals, approximately every second, the aircraft transponder gives off the position and speed of the aircraft as determined by an onboard GNSS receiver or by the flight management computer by merging several data sources. ADS/B broadcasts are received on the ground by means of simple receiving antennas connected to traffic control centres. They are also received directly on board other aircraft in the area, thus informing pilots as to the local air traffic situation, and by low orbiting satellites, which decode the received signals and transmit the information to a mission centre. This information is usable by airlines for global aircraft monitoring and by navigation service providers when the area*

52 *ADS/B: Automatic Dependant Surveillance / Broadcast. The aircraft sends its position and other information periodically to ground stations and other aircraft in the zone equipped with ADS-B.*

around the aircraft is not covered by a radar or a ground receiving station (in the case of oceanic regions).

***Future ATM systems** on the drawing board in Europe (**SESAR**) and the United States (**NextGen**) are planning to implement new ATM procedures based on information provided by **ADS/B**.*

Not only do onboard ADS/B devices often have WiFi and Bluetooth ports that make them vulnerable[53], but several studies have highlighted the weaknesses of ADS/B. It is possible for a hacker to create fake aircraft and also false collision risks. It is also possible to saturate controllers' and pilots' screens with false aircraft.

One way to protect against false aircraft is the use of ground, primary or secondary radars, or also by multilateration (MLAT) by which the same positioning message transmitted by an airplane is received at different times by several receiving antennas; it is then possible to calculate the position of the aircraft by triangulation and to compare it to that transmitted.

If false positions are emitted from the ground, primary or secondary radars or multilateration can detect the attack and try to locate it. However, this solution requires more complex equipment, and will probably not be deployed everywhere.

If false positions are emitted by another aircraft, pilots may not detect them, and ACAS would only prevent a collision if the altitude was correct.

*The ADS/B system makes it possible to track aircraft in flight on certain internet sites (*Flight Radar 24 *for example). Terrorists can thus know where planes are and be in a position to attack them in low-level flight, for example using portable missiles. This tracking of aircraft in flight is a breach of confidentiality, if the positioning information is disseminated in real time.*

> ► ***Recommendation R8***
>
> *Before switching to the use of ADS/B as the primary means of surveillance, a **risk analysis** shall be carried out, which may lead to the setting up of additional monitoring means. The ADS/B standard should evolve to improve its level of cybersecurity protection (i.e. with data authentication and/or encryption[54]).*
>
> ***Action: ICAO, FAA[55] and EASA.***

53 Atlantic Council Aviation report.

54 *Authentication and encryption means are widely used, for instance in banking and the judiciary system.*

55 *FAA, Federal Aviation Administration: www.faa.gov*

5 RISK OF CYBERATTACKS

Cyberattacks against operational civil aviation information and communication systems can take many forms, depending on the techniques used, the systems targeted and the perpetrators.

5.1 Main possible modes of attack

This dossier chooses to deal only with those attacks aimed to cause aircraft accidents or serious incidents. One possible type of attack is denial of service (DoS), or jamming, which consists of ***blocking incoming signals****, on board or on the ground; DoS can target communication signals, especially those carrying digital data, radio-navigation signals, particularly from GNSS satellites, and surveillance signals such as aircraft ADS-B emissions.*

Communication links are also open to a second type of attack which involves transmitting ***false data*** *to ground or onboard receivers. Depending on the nature of this data, the consequences can be serious if there is no way of verifying the authenticity, integrity and traceability of the information.*

One modus operandi consists of corrupting ***operational software****, onboard or on the ground. The presence of computer viruses programmed to trigger harmful actions at a specific time or in reaction to an event is obviously a significant threat. These viruses may have been integrated into the aircraft from manufacture by an agent or subcontractor of the manufacturer, or inserted during regular maintenance work or data updates. The weakest links here are USB drives and attachments to messages of unknown or falsified origin, which are the main sources of viral infection and the introduction of "Trojan horses".*

5.2 Potential targets

*Potential targets are very varied, due to the great complexity of the overall ecosystem. They mainly include **radio links between air and ground**, possibly via space if satellites are involved.*

- *These links are primarily dedicated to **air traffic management**, being used for communication (exchanges between pilots and controllers), navigation (in particular signals from navigation satellite such as GPS or Galileo) and surveillance (either from secondary radar, or from positions issued by aircraft). The jamming of GNSS signals is a denial of service attack because the navigation service is no longer available. This vulnerability to jamming was revealed in 2001 with the publication of the Volpe Center[56] report in the United States. The free marketing of jamming equipment via the internet poses a serious problem for the use of satellite navigation in civil aviation.*

  *Another means of attacking satellite navigation signals is spoofing. This type of attack is within the reach of hackers. A signal simulator can be used to trick a nearby receiver into calculating a false position. The solution to this type of attack involves signal **authentication**, which will be available with Galileo on open signals, or the kind of **encryption** today reserved for the military on GPS, GLONASS and BeiDou, and for governmental users on Galileo.*
- *Aircraft communications equipment provides **voice communication** (VHF and HF) and data link (VHF, HF and L and C band) as part of a chain for which **availability, authenticity, integrity, confidentiality and end-to-end traceability** must be ensured. Comprehensive risk analysis must be carried out over this entire chain by carefully studying reconfigurations in degraded mode.*
- ***Data links** are also allocated to **passengers**, particularly on long-haul flights, enabling them to connect to a Wi-Fi cabin network[57] in order to watch videos or surf the internet from their seats, by means of a PC or tablet or a smartphone; these links are in theory kept completely separate from operational links, a separation that is increasingly compromised by airlines taking advantage of the high bandwidth to transmit operating data from the aircraft systems.*

***In-flight passenger entertainment (IFE)** can also be attacked, although successive, robust barriers prevent the penetration of critical aircraft systems. Attacks on the cabin are mainly aimed at hacking videos, creating fake Wifi access points to retrieve personal information (passwords, bank codes...) or interfering with a passenger's environment (e.g. lighting). Attacks could create a wave of panic in the cabin by relaying false information on the screens. These attacks would create the buzz and could damage the reputation of aircraft manufacturers and carriers.*

*Information **processing systems and equipment** may also be targeted, either on board or on the ground, in ATM centres or airline OCCs. These numerous systems tend to have complex architectures, with often very large memories in which to store*

56 www.navcen.uscg.gov/pdf/vulnerability_assess_2001.pdf

57 IFEC: In-Flight Entertainment and WiFi Connectivity Systems.

software and data, and data exchange buses between the processors. This software and data are targets for attacks. The most exposed software is that controlling the functioning of the processors, i.e. the operating systems. In many cases, these software products are purchased off-the-shelf and are not subject to the same tests as dedicated software[58]. Some software is updated regularly, especially for ground systems, and these updates can provide the opportunity to insert a hidden computer virus in the code (Trojan horse). Software and data processing equipment can also be attacked, with the creation of backdoors, for instance, that allow attackers direct access. There are actually two types of backdoors: those inserted into the software, especially the operating systems, and those inserted into the hardware, much more difficult both to insert and to detect. FPGAs (Field-Programmable Gate Arrays) are programmable integrated circuits used to perform many functions – router, encryption, etc. Suited specifically to the functions for which they are designed, it is possible to include backdoors during the design stage, at the foundry. Real cases of the existence of such backdoors and information leaks in the processors have come to light[59], but the real question is how to detect if there are others.

The introduction of electronic tablets with on-board documentation[60] is also a potential weak spot, depending on whether or not they are connected to the internet or to critical cockpit systems and whether they are movable.

*The **data** required by these processing systems can also be targeted for attack; there are two types of sensitive data: **static data**, periodically updated, such as aeronautical navigation information (routes, tags, waypoints, frequencies, arrival and departure procedures) updated every 28 days, and **dynamic data**, which can change in real time, such as the position of the aircraft and other aircraft. Attacks can target both types of data.*

5.3 Profile and motivation of potential attackers

*Potential attackers can be classified according to several criteria. The first criterion concerns the location of the attacker: usually we consider two types of attackers, "**insiders**", who are employees of companies producing the operational software or ensuring its maintenance, and "**outsiders**" who are not employees of the companies concerned. A specific category is that of attacks coming from passengers on board aircraft. The category of insiders is also dangerous: it can include employees wishing to take revenge on their employer for having refused them a promotion, for example.*

58 *COTS : Commercial Off-The-Shelf.*

59 *www.cert.ssi.gouv.fr/alerte/CERTFR-2018-ALE-001*

60 *EFB : Electronic Flight Bag.*

Outsiders can be divided into different categories, depending on their motivations:

- *The first category includes the hackers; this category can be further subdivided into two groups: the "**white hats**" who seek to penetrate specific operational systems and discover loopholes in order to be paid by the companies producing the systems for their "exploit" in finding these weaknesses; then there are the "**black hats**" who exploit whatever loopholes they have found or retrieved from the internet in general for money. Black hats tend to be motivated by financial gain, but they can threaten airlines with accidents or serious incidents if they are not paid a ransom.*
- *The second category consists of cyberc**riminals**, who are often organised into real gangs, with a distribution of tasks between the different members. These gangs, which are to be found in a number of countries with looser regulations than France, are motivated by financial gain. Occasionally they work as contracted mercenaries for companies seeking to undermine and discredit the competition, or can even be under contract to certain states unwilling to be identified as the source of attacks. Another category of organised cyberattackers may trigger coordinated attacks on targets to express their opposition to certain projects or companies, for reasons as diverse as environmental protection (for example against the construction of a new airport) or the defence of certain political causes. Known as "**hacktivists**", they are not motivated by financial gain but by the disruption they cause.*
- *The third category is the most dangerous: **cyberwarriors**, who exist in certain countries, usually with a military status, and are preparing for a future cyber war. They enjoy significant financial backing and are organised into real multidisciplinary teams specialised in certain fields. These personnel are specially trained for the tasks they are to perform, particularly that of causing destruction.*
- *A fourth category, in some ways resembling the cyberwarriors, consists of **cyberterrorists** who generally act in a coordinated manner and seek to **cause accidents or serious incidents**. With **terrorists** finding it increasingly difficult to board planes armed with weapons and explosives, they are now in danger of refocusing their criminal actions on **cyberterrorism**. These terrorists possess significant financial means, whether obtained legally or illegally. This last category of cyberterrorists has not yet caused an aviation accident, but the high emotions generated by such accidents in the general public and the intense media coverage they provoke could be sufficient motivation to goad them into action.*

5.4 Examples of cyberattack scenarios

The most likely cyberscenarios are those that offer their perpetrators:

- *the greatest chance of impunity;*
- *the best "return on investment";*
- *the easiest means of accomplishment.*

It is very difficult to draw up an exhaustive list of cyberattacks potentially threatening civil aviation. Only a few examples of scenarios are presented to make this chapter more concrete. These scenarios are not based on real attacks that have actually occurred; they have been imagined by the writers of the dossier.

***The first scenario** hinges on radio links: an attack targeting the ADS-B automatic aircraft position reporting system.*

***The second scenario** concerns navigation data updated every 28 days in aircraft flight management computers.*

***The third scenario** relates to line maintenance of onboard equipment[61].*

Below are the five most serious (i.e. "catastrophic") types of feared events taken from the taxonomy known as CAST/ICAO[62]:

- *Controlled Flight Into Terrain;*
- *Loss of Control In Flight;*
- *Mid-Air Collision;*
- *Runway Collision;*
- *Runway Excursion.*

For each of these feared events, a number of "barriers" have been put in place upstream to make such accidents very unlikely. Manufacturers should examine these barriers for vulnerability to cyberscenarios.

61 *LRU : Line Replaceable Unit.*

62 *Ref*. Common Taxonomy Team (CICTT) Aviation Occurrence Categories: *www.intlaviationstandards.org*

6 HOW TO MANAGE RISKS

Risk management is known and applied by large, ISO-certified (9001, 14001, 27001) organisations, but this is not necessarily the case for many other actors involved in air transport such as airport operators, maintenance companies, service providers, small airlines, etc.
The general goal is based on the so-called "ALARP" principle, i.e. to maintain the risk "As Low As Reasonably Practicable".

6.1 Analysing and quantifying risks

The risk analysis process must follow the following steps:

- *Establishment of framework;*
- *Assessment of risk:*
  - *valuation of assets according to criteria set out in the framework with regard to authenticity, availability, integrity, confidentiality and traceability;*
  - *identification of threats and vulnerabilities (including their likelihood and a quantification of their occurrence);*
  - *identification of existing security measures and their effects on identified risk;*
  - *quantification of possible consequences (impacts);*
  - *prioritisation and sequencing of risk processing.*

A threat targets an asset. It searches for vulnerabilities to be exploited according to a set scenario. The impact is the result of the accomplishment of the scenario.

The risk analysis process[63] *must enable a definition of actions and means aimed at reducing risks and therefore impact. Risk quantification is expressed by the formula:*

63 *C.f. the* Eurocae Standard 202 – Airworthiness Security Process Specification*: https://standards.globalspec.com/std/9862360/eurocae-ed-202*

Risks = probability of occurrence x severity of consequences

Feared events must be analysed. What information or assets will attract an attacker and what type of attacker? It is not a question of building up protections without knowing who we are facing, but rather of focusing on detection in order to be in a position to react.

Feared events are not necessarily plane crashes, but rather the potential for disorganisation or panic on board, in control centres or airports. Such events can have significant media, economic and social repercussions leading to loss of confidence in air transport. They can also involve theft of commercial information, data or files, or disruption to the supply chain with manufacturing blockages at subcontractors.

For example, Airbus performs a systematic risk analysis on the basis of a list of potential cyberattacks. The probability of these attacks is weighted according to three criteria: ease, attractiveness and impunity (see beginning of §6.4).

The priority for Air France and KLM (which share a Cybersecurity solutions & IT compliancy directorate) is to maintain resilience to attack throughout the operational life of the fleets, forestalling anything that could generate delays and especially undermine the brand image. All branches – air operations, engineering, maintenance, cargo and marketing – are involved in security aspects. Risk analysis aims to map and target those risks that are most feared in order to best reduce their occurrence probability and impact.

6.2 Technical solutions

Data exchange

Secure exchanges between the cockpit and the ground rely on the presence of firewalls, encryption, dedicated links, etc. Between the cabin and the cockpit, exchanges must go only one way – in the cockpit to cabin direction – in order to prevent critical data from being accessible from the cabin.

Software security

Software programmes must benefit from protection measures from design stage and during their production and maintenance, even if this generates additional costs. One means of protection is the use of encryption keys (some of which can remain secure for several years).

In-flight entertainment

One possibility for updating IFE software would be to use two-way procedures that require a second password for the software to be reloaded (such a system is used

to secure bank payments on the internet). This solution, more flexible than PKI systems[64], would be more acceptable to airlines.

> ► ***Recommendation R3***
>
> *A policy for updating operational software and data shall be defined and implemented by all actors, with* ***authorised personnel, dedicated and safe means*** *and* ***secure procedures****. In particular, this includes regular implementation of software protection patches.*
>
> ***Action: Airlines, manufacturers, equipment manufacturers, maintenance companies and service providers.***

Workstations

Although air traffic controllers' workstations will never be 100% secure, surveillance must be set up in the form of incident detection systems.

Ground radars

With regard to ATM radars, it must be possible to detect in real time whether a system's operation is normal or abnormal and to report any incoherent information to operators.

Ground antennas

Access to ground antennas is physically protected and potential intrusions are detectable by supervision (detection of outages); in this case, the failed system is invalidated.

Probes in the IS

Detection can be carried out by means of probes placed in different areas of the systems in order to:

- *find the relevant information, which can be weak signals in a forest of information;*
- *determine if there is an ongoing attack or if it is a dormant threat;*
- *specify the attack scenario, the attack method and the attacker's signature.*

6.3 Human factors

The vast majority of aircraft accidents result from the combination of one or more latent failures (systemic factors) with one or more active failures (linked to individuals). How individuals act – their attitudes, decisions and actions – is closely related to the characteristics of the organisations in which they work. Risks linked to

64 *PKI : Public Key Infrastructure.*

human activities, whether in terms of safety or cybersecurity, must therefore be examined at both these levels.

The "human factor" is often seen as synonymous with "risk factor". This restrictive vision tends to obscure the ability of operators to detect and recover from unforeseen situations, an idea that must equally inform studies into cybersecurity.

Much of the progress made in safety is due to the development of overall attitudes, behaviours and practices, which go to make up a company's safety culture. This culture, when it is mature and assimilated at the highest level, leads to a great coherence between an organisation's general philosophy – its policy and procedures – and the hands-on practices observed in situ. If the overall goals set by a company are in contradiction with certain safety procedures, employees will clearly conclude that these safety aspects are a secondary issue. Managers will often be the first to play down the importance of procedures which stand in the way of them reaching their goals. The same difficulties are faced when implementing cybersecurity measures.

Finally, any possible interaction between envisaged cybersecurity measures and existing security measures should be examined with the utmost objectivity to avoid compromising the very high safety level of air transport achieved today. The installation of armoured doors to the cockpit paved the way to the Germanwings crash over the Alps. This example shows that it is essential for cybersecurity and safety policymakers to work together.

Why do attacks so often succeed in penetrating information systems?

Apart from quasi-autonomous and integrated technical systems, which intruders will hack into at a distance in the cybersphere, interfaces designed for humans also carry potential faults, not only technical but, very often, ***human****.*

Individuals can act against their employer because of lack of motivation, in reaction to disrespect on the part of a supervisor or colleague, due to a bad climate or a deleterious working environment. Promoting a sense of belonging and ownership in employees would seem to be a good way of building up trust.

It is therefore vital to create systems that are more resistant to unsafe human intervention, by working on workstation ergonomics and setting up "deep defences", successive barriers to be crossed before reaching data. In addition, action into raising staff awareness must be carried out on a ***long-term basis****, not limited to periods of crisis, and should include aspects such as organisation, certification and staff training.*

Measures of this type will be all the more relevant and effective if they are based on a proper knowledge of human behaviour as revealed in cyberscenarios. The human factors that have led to cyberincidents will need to be systematically examined and processed in a manner akin to air incidents and accidents analyses. This process must include decisions and actions that have been successful in detecting and

countering a threat in time, as well as those that have enabled a threat to "succeed". Nevertheless, the implementation of safety systems should not curb activity.

Raising awareness

The idea that "overprotective" technology – which can be extremely expensive – ensures better safety and security must be counterbalanced by efforts to increase staff awareness and set up appropriate organisational structures to enable monitoring and supervision.

The ISSM (Information Systems Security Manager) must have access to the highest level of the entity in question in order to inform their management of any risks and incite them to take the necessary preventive actions.

ISS[65] incidents - whether malicious or purely technical - highlight the importance of appropriate communication and proper crisis management procedures.

Enhanced awareness reinforces human intuition in detecting weak signals that may be precursors to an intrusion or cyberattack.

Security clearance

A rigorous selection process must go into the security clearance of personnel and its monitoring, even for subcontractors and suppliers. The supply chain and maintenance circuits remain sensitive areas in which staff clearances must be mandatory, with regular monitoring and supervision.

Training

Staff in air transport organisations or companies must be trained in methods and practices for detecting, countering or mitigating a possible cyberattack. Procedures for analysing, anticipating and preventing such attacks must be established within a suitable framework without reducing confidence, hampering exchanges or inhibiting innovation. It is a case of "educating to protect".

Documents should be drawn up containing response procedures for cyberattacks. They must be consistent for all players and define their respective responsibilities and mode of cooperation as closely as possible. Staff training in the application of these procedures must then be properly ensured, for example through regular drills and audits.

Developers and users need to be trained in good practices. The following are examples of good development practices:

- *ISS code audits;*
- *attack-defence role-playing with real hackers as attackers.*

---

65 ISS: Information Systems Security.

In France, at the directorate for air navigation safety (DSNA), a three-level training plan has been set up for all staff (ISS passport, ISS enhanced training, ISS expert training for around 20% of electronic engineers).

> ► ***Recommendation R9***
>
> *Personnel at risk of **cyberattacks** on air transport shall be **trained** in the methods and practices for detecting, countering or limiting a possible cyberattack.*
>
> ***Action: All actors.***

IS monitoring, supervision and management

All air transport players must have an Information System Security Manager (ISSM) whose mission is to monitor and supervise the information system, applying the loop Anticipate → Protect → Detect → React.

Equally important are the IS security audits that should be conducted regularly, covering technical as well as human and organisational aspects. For example, care must be taken to ensure that no verification level is missing (check that all USB keys have gone through a cleaning station), or that access to workstations is controlled (by means of individual codes and locking when absent).

Above all, incidents occurring in different companies must be pooled in order to better anticipate potential future threats. See § 7.6.

Supervision and control by operational staff

Voice and data links must be checked for authenticity, availability and integrity along the entire chain: the communication equipment of the aircraft forms one link in this chain and it is vital to understand how pilots assess the coherence of the information transmitted and identify dubious or degraded data. What is true for aircraft is also true for air traffic controllers on the ground. Corruption of flight plans is a potential risk, although the crew has responsibility for checking them before their implementation, which limits this risk.

*In the end it is the **crew** who must verify data consistency, hence the need for appropriate procedures: it is vital not to accept uploaded data on face value without carrying out checks. In the event of any doubt, the proposed data must be rejected and other modes used if necessary.*

AAE Dossier 42[66] *covers the case of Single Pilot Operations, with the need for excellent data transmission between the aircraft and the ground. It makes mention of cybersecurity and highlights its importance in the case of dynamic, high-risk situations. The Dossier's initial analysis on cyberattack prevention would argue in favour of maintaining a crew of two pilots, at least for a while.*

66 *AAE – Dossier 42:* More automated, connected aviation by 2050.

Supervision and control by industrialists

MRO providers, often small subcontractors, seek to reduce costs and facilitate the work of their operators. Some for instance have scanned data and design schemas and put them on the internet.

Equipment manufacturers must also be vigilant, because they will be the first in the hot seat in the event of any security breach. These equipment manufacturers must impose stricter data protection rules as well as procedures for updating software or even, for more critical equipment, take charge of their own reloading.

MRO organisations and/or STC managers must be shown to apply the same level of safety requirements as aircraft manufacturers. This tends to be one of the weak links in the chain.

Intervention by subcontractors during stopover or maintenance may create vulnerabilities. A large airline like Air France/KLM maintains control over these players by means of security clearances for personnel and by certifying the organisations concerned. The danger still remains, though, in the case of airlines which do not have the same level of security requirements.

6.4 Cybersecurity management

*Cybersecurity management should be detailed at the highest level of the entities concerned in a document displaying the **information systems security policy** to be implemented. This should include the main cybersecurity principles as well as more detailed guidelines.*

High-level ISS requirements must then be defined based on three criteria: confidentiality, integrity and availability.

It is important to ensure the pertinence of such requirements so as to prevent operators (who are human) from circumventing them or even ignoring them entirely.

Agencies and state organisations

ANSSI (French cybersecurity agency, see Appendix 1) has published an IT system hygiene guide[67] which lays out 42 rules as well as a set of guidelines[68] for best practices. If the measures described in these guidelines were properly applied, they would avert 80 % of attacks.

Emphasis should be placed on the following common sense solutions described in this guide:

- *password management policy;*
- *regular systems updates;*
- *user/administrator separation;*

67 www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf

68 www.ssi.gouv.fr/administration/bonnes-pratiques

- *separation of networks;*
- *systems partitioning.*

Industrialists

Service providers must be verified, whether this concerns the DSNA network (SFR or Orange) or satellite networks (with suppliers such as SITA or integrators like ENGIE).

Security control equipment at airports is certified by French civil aviation agency DGAC, but checks must still be performed to prevent security failures during their use.

Incident prevention

One of the best ways of checking the safety of different systems is to invite professional hackers to perform a vulnerability analysis. This practice has been implemented by aircraft manufacturers for their newest programmes.

Regarding security requirements, Airbus has defined Security Assurance Levels (SALs) for future compliance with the Do-356/ED 203a, equivalent to the Do-178 Development Assurance Levels (DAL) for onboard equipment software.

To enable operators to maintain the maximum safety level, Airbus provides each customer airline with a Security Handbook, a collection of regularly updated recommendations that must be applied throughout the operational life of the aircraft. This document also serves as a guide for regular security audits.

The role of the crew in neutralising threats (the procedures and rules to be applied) can only be effective if the time required to correct the corrupt situation is compatible with the time available. And yet these can be complex, unexpected situations in high-risk phases (take-off, landing or others). This available time parameter must be taken into account in the definition of corrective actions.

The response of crews to abnormal and unexpected behaviour on the part of automated systems was tested on a simulator at DGAC a few years ago. Pilots were exposed to programmed "bugs", which triggered trajectory anomalies but no alarm, although the parameters inserted by the pilots were correct. This kind of test works for navigation database corruption, system jamming, or abnormal behaviour of automated systems.

One avenue could be to establish an inventory of irreversible, catastrophic commands, which may not actually be very long. Systems would then be checked for vulnerability to cyberattacks capable of issuing such commands. It is possible that manufacturers and equipment manufacturers are already working on this axis.

Humans might then be seen to be effective at countering certain types of attacks.

Incident handling

When a cyberattack is triggered during operation, even if all the preventive measures mentioned previously have been put in place and monitored, real-time, coherent actions must be taken by the onboard and ground entities concerned.

Each air transport player must adopt a similar organisation to civilian or defence security forces and adhere to precise guidelines as to the operating modes to be used in the different types of attacks, whether such attacks have already been observed or merely anticipated.

> ► ***Recommendation R10***
>
> *Crisis management procedures shall be elaborated to deal with cyberincidents and shared with all actors.*
>
> ***Action: All air transport stakeholders.***

When new malware is discovered, Computer Emergency Response Teams (CERTs) alert computer security companies so that an antivirus can be developed very quickly. Thales has its own CERT with fifteen or so employees (mainly used to ensure the security of interbank exchanges). One idea might be to develop a ***CERT specialised in aeronautics****.*

Incident analysis

One of the lessons learned from examining past incidents is the need for a very different procedure to the usual immediate reaction to any glitch. In the case of cybersecurity, on the contrary, it is often best not to isolate networks from the rest of the world, but rather to monitor and supervise the situation in order to trace the source of the attack and sever all its roots, a process which can take several months. 200 to 250 days can be needed to detect and deal with new malware.

6.5 Incident reporting and exchanges between actors

Since 100% security does not exist, incidents will occur. However, there is no database to assemble these incidents because the players involved lack transparency. The player having suffered the attack tends not to disclose the information and, even digging deep, it is difficult to ascertain the real causes of incidents and distinguish between breakdowns, bugs, handling errors or truly malicious acts.

► ***Key Recommendation R11***

All certified air transport actors shall ***mandatorily report, share and then systematically process cyberincidents*** *in the same way as air accidents and incidents are reported, shared and analysed in a process that has led to a significant increase in air transport safety.*

Action: ICAO, FAA, EASA and national authorities.

ANSSI *staff are well informed; they can thus analyse incidents and begin to create feedback from experience (e.g. the attack against TV5 Monde).*

In Europe, the European Centre for Cybersecurity in Aviation (ECCSA) – created in 2017 on the initiative of EASA (European Aviation Safety Agency) – is informed of threats to air transport, analyses them, characterises them and shares them (in a secure way) with the players concerned. This centre must continue to develop before reaching its full capacity.

Aviation-ISAC *(see Appendix 2) is a good initiative that allows exchanges outside the often state-based framework of protection of secrecy.* Annual Aircraft Security User Panels *encourage the exchange of information between aircraft manufacturers and airlines. Post-flight, operational reports of attacks occurring in flight (departure from gate to arrival) could therefore be gathered within these exchange groups.*

7 REGULATION AND GOVERNANCE AT THE INTERNATIONAL LEVEL

Major organisations such as ICAO, EASA, Eurocontrol, SESAR/JU, etc. are working on cybersecurity and various working groups have been set up, but concrete steps forward are slow to be implemented. European agencies or centres such as ENISA and ECCSA have been created and have begun operating.

► ***Key Recommendation R12***

*There is an **urgent** need to develop **a harmonised worldwide regulatory framework** for cybersecurity in civil aviation, within a global management system (integrating security and safety) and to ensure its implementation and compliance **through qualified cybersecurity entities**.*

Action: ICAO Member States and regulatory bodies.

Regulation and certification can provide some risk prevention. Norms and standards exist (see Appendix 5) but need to be applied, and their implementation must then be regularly monitored by audits conducted by certified authorities or laboratories.

► ***Recommendation R13***

Certification and authentication processes for sensitive data exchanges based on industry standards shall be developed or adapted and implemented.

Action: Industry.

World aviation authorities (FAA – EASA – civil aviation authorities...) have not yet harmonised these cybersecurity standards and regulations and this will take time! IATA has proposed a kit, but it is considered insufficient.

Whilst all these international bodies and authorities are aware of the importance of the threats and risks involved, as well as the ***urgency*** *of making progress towards European and global harmonisation, there is a clear* ***lack of directivity in the recommendations and a tardiness in defining action plans, roadmaps and a calendar****.*

For example, Appendix 3 of this dossier presents the resolutions of the General Assembly of ***ICAO*** *(39th session of October 2016) on cybersecurity: after recognising, considering, reaffirming and recalling a number of facts, ICAO confines itself to* ***inviting*** *states and industry to take action! Those who drafted these ICAO resolutions did their job well, and the 11 points "of invitation" that are highlighted are totally relevant. But how many more years will be needed to move from an invitation to an action plan + roadmap with associated calendar?*

Second example: Appendix 4 comprises the EASA statement following the High Level Conference on Cybersecurity in Civil Aviation in Krakow of 8 and 9 November 2017. Here again, of the 22 points of this declaration, more than half (12) are ***non-directive*** *and restricted to recognising needs and accepting roles, and also to supporting, encouraging, welcoming and suggesting initiatives and actions. Nevertheless, some* ***positive points*** *should be highlighted:*

- *Once it has received its mandate from the Council and the European Parliament, EASA will be called on to develop and push through a* ***harmonised European set of regulations*** *on cybersecurity in civil aviation (in particular on methods for analysing cyberrisk), in accordance with the European NIS directive.*
- *A* ***European Strategic Coordination Platform***[69] *set up at the end of 2017 is tasked with coordinating with EASA in order to adopt an* Aviation[70] Cybersecurity Strategy and associated roadmap*, in late 2018.*
- ***Ground systems*** *are a priority in ensuring a safe cyberspace environment.*
- *Airports, ground operators, maintenance organisations and service providers are specifically invited to set up a* ***cybersecurity management system*** *with specific procedures and appropriate standards.*
- *Aviation cybersecurity research (R&D) activities should be continued and expanded to other transportation sectors (road, rail and marine).*

69 *ESCP: European Strategic Coordination Platform. It brings together about thirty actors as varied as agencies, EU States, DGs of the European Commission, EASA, Eurocontrol, SESAR JU, ENISA, CERT-EU, as well as company, airline and airport groups and associations…*

70 *Aviation Cybersecurity Strategy.*

► ***Key Recommendation R14***

*ICAO shall lead and coordinate at worldwide level all activities contributing to enhancing cybersecurity in civil aviation. EASA and national authorities shall be **given a mandate** to **define and decide on cyber action plans** and quickly put in place **roadmaps** with associated **resources and timelines** together with minimum short term measures.*

*In France, the creation on 12 April 2018 of the **Council for Air Transport Cybersecurity**[71] **(CCTA)**, under the aegis of the DGAC, is a welcome initiative (see Appendix 1). This body, which brings together all French stakeholders, could progress rapidly by taking into account the recommendations made in this Dossier. France could thus play a leading role by promoting the CCTA' proposals to other European players.*

Moreover, the need for civil aviation and military aviation to work together is also highlighted, not only for the purpose of harmonisation, but also to take advantage of the protective measures implemented in military systems. Work remains to be done to identify recommendations applicable to civil aviation.

71 *www.assisesdutransportaerien.gouv.fr/comprendre/les-actualites/elisabeth-borne-installe-le-conseil-pour-la-cyber-securite-du-transport*

8 CONCLUSIONS

Air transport is often a chosen target of terrorists but, since the attacks of 11 September 2001, very strict measures adopted internationally and implemented in all commercial aircraft and airports have made attacks much more difficult. It is highly likely therefore that terrorists will seek other non-physical attacks, based on as yet unsecured vulnerabilities.

*The **digitalisation** of the air transport sector, particularly airliners, and the development of radio links between aircraft and ground-based services (for the purposes of air traffic management, airline operations control, monitoring the functioning of onboard equipment and passenger access to the internet) were implemented **without security regulations against cyberattacks**. This has resulted in a large number of **potential vulnerabilities** that must be secured without delay. A security effort, as significant as that implemented in 2001, must urgently be agreed on at the international level and rapidly implemented on board aircraft and on the ground. It will be able to draw on all the recommendations of this Dossier.*

*Civil aviation takes place by nature within an international framework. Its technical organisation must necessarily obey globally harmonised rules, under the aegis of **ICAO** in particular, without which it will not be in a position to guarantee the safety and services it owes its customers.*

This is why cybersecurity in aviation cannot have borders and national policies need to be, if not harmonised, at least coherent and coordinated, to eliminate any weak links that cancel out the efforts of others.

Of course, the major powers such as the United States, Europe, China or Russia will always have their own policies on the general issue of cybersecurity. But the common core of rules to be implemented for aviation can only be situated in ICAO, with the effective contribution of its Member States (see Appendix 3).

It is important to determine what is useful to regulate and what is not. Given the permanently evolving nature of the threat, there can be no question of imposing software or computer tools to neutralise it. Protections must be conceived at the ***design*** *stage, with* ***those parts that are vital for safety being completely hermetic*** *as compared to other elements more open to external intrusion.*

On the other hand, the most significant risks emerge in the ***subsequent life of the systems****, on board aircraft or on the ground, during maintenance operations or modifications carried out by the operators or under their responsibility. Industrial processes within subcontracting chains as well as updates and maintenance of software and data should be subject to strict regulations, which would make certain interventions conditional on coordination between actors.*

It is important to emphasise the importance of ***human factors*** *in the possible execution of cyberattacks, as well as their detection and management. The main operational actors – pilots and particularly controllers – must be prepared for these events, which could implicate several aircraft or several ground or satellite means simultaneously. Simulated attacks should be performed regularly to train the operational actors. Operational procedures should include predictive management of cyberattacks.*

With regard to ***sharing information*** *on the evolution of the threat, an initiative has already been taken in the United States with the creation of an Aviation-ISAC group bringing together manufacturers, airlines and public agencies (FAA, FBI, NSA, see Appendix 2). A similar initiative is being set up in Europe. This form of coordination, which is essential, should be extended and structured within a framework defined not simply at a European level, but at a* ***global****, ICAO level.*

GLOSSARY

AAE	Académie de l'air et de l'espace / Air and Space Academy
ACARS	Aircraft Communication Addressing and Reporting System
ACAS	Airborne Collision Avoidance System
ADS/B	Automatic Dependent Surveillance – Broadcast
ADS/C	Automatic Dependent Surveillance – Contract
AESA	Agence européenne de la sécurité aérienne
AIRAC	Aeronautical Information Regulation And Control
AIRM	ATM Information Reference Model
ANSP	Air Navigation Service Provider / Fournisseur de services de navigation aérienne
ANSSI	Agence nationale de la sécurité des systèmes d'information
AOC	Airline Operation Centre / Centre d'opérations aériennes
APT	Advanced Persistent Threat
ATC	Air Traffic Control / Contrôle de la circulation aérienne
ATIS	Automatic Terminal Information Service
ATM	Air Traffic Management / Gestion de la circulation aérienne
BEA	Bureau d'enquêtes et d'analyses
CANSO	Civil Air Navigation Services Organisation
CCTA	Conseil pour la cybersécurité du transport aérien
CERT	Computer Emergency Response Team
CoTS	Commercial Off-the-shelf (produit sur étagère)
CPDLC	Controller – Pilot Data Link Communication
CSIRT	Computer Security Incident Response Team
DAL	Development Assurance Level / Niveau de développement logiciel
DataLink	Liaisons de données
DFMC	Dual-Frequency Multi-Constellation
DGAC/DSNA	Direction générale de l'aviation civile / Direction des services de la navigation aérienne
DoS/DDoS	Denial of Service / Distributed Denial of Service (Déni de service)
DME	Distance Measuring Equipment
EASA	European Aviation Safety Agency
ECAC	European Civil Aviation Conference

ECCSA	European Centre for CyberSecurity in Aviation
EFB	Electronic Flight Bag (Tablettes électroniques d'équipage)
EGNOS	European Geostationary Navigation Overlay Service
ENISA	European Union Agency for Network and Information Security
EPAS	European Plan for Aviation Safety
EU	European Union
EUROCAE	European Organisation for Civil Aviation Equipment
FAA	Federal Aviation Administration
FPGA	Field-Programmable Gate Array
FMS	Flight Management System
GAO	Government Accountability Office (USA)
GBAS	Ground-Based Augmentation System
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GSM	Global System for Mobile Communications
IATA	International Air Transport Association / Association internationale des transporteurs aériens
ICT	Information and Communication Technologies
IFE	In-Flight Entertainment
IS	Information System
HF	High Frequency (bande de fréquence de 3 à 30 MHz)
ICAO	International Civil Aviation Organisation
ILS	Instrument Landing System
IP	Internet Protocol
ISO	International Organisation for Standardisation / Organisation internationale de normalisation
ISS	Information Systems Security
ISAC	Information Sharing and Analysis Centre
LPM	Loi de programmation militaire
LRU / URL	Line Replaceable Unit / Unité (équipement) remplaçable en ligne (piste)
LTE	Long Term Evolution: évolution des normes de téléphonie mobile

MRO	Maintenance, Repair and Overhaul
NDB	Non Directional Beacon
NextGen	Next Generation Air Transportation System / Système de transport aérien de nouvelle génération (USA)
NIS	Network and Information Security
NOTAM	Notice to Airmen - Message aux navigants aériens
OACI	Organisation de l'aviation civile internationale
OIV	Opérateur d'importance vitale
PKI	Public Key Infrastructure
RSSI	Responsable de la sécurité des systèmes d'information
SAL	Security Assurance Level / Niveau d'assurance de sûreté
SatCom	Communications par satellite
SBAS	Satellite-Based Augmentation System
SESAR	Single European Sky Air Traffic Management Research
SGDSN	Secrétariat général de la défense et de la sécurité nationale
SI	Système d'information
SMS	Safety Management System / Système de gestion de la sécurité
SOC	Security Operations Center / Centre d'opérations de sécurité
SSI	Sécurité des systèmes d'information
STC	Supplemental Type Certificate
SWIM	System Wide Information Management
TC	Type Certificate / Certificat de Type
TIC	Technologies de l'information et de la communication
UE	Union européenne
UIT	Union internationale des télécommunications
VDL / VDLM2	VHF DataLink / VHF DataLink Mode 2
VHF	Very High Frequency (bande de fréquence de 30 à 300 MHz)
VoIP	Voice on Internet Protocol
VOR	VHF Omnidirectional Range
WiFi	Réseau local hertzien sans fil / Wireless radio technology
WiMax	Worldwide Interoperability for Microwave Access (Wireless communication standard used as a transmission and high-speed Internet access system over a wide geographical area).

APPENDIX 1: AGENCIES AND ORGANISATIONS IN CHARGE OF CYBERSECURITY

National Agency for Information Systems Security – ANSSI

ANSSI, in France, is attached to the General Secretariat of Defence and National Security (SGDSN), which reports directly to the Prime Minister. ANSSI had a staff of 550 in 2017, as compared to 120 in 2009.

ANSSI has two main missions:

- *a preventive mission (regulations – assistance and advice to state IS operators and OIVs and inspection of these systems – qualification and certification - international negotiations – training – creation and exploitation of secure means of communication).*
- *A 24/7 IS defence mission (detection/intervention/response in the event of major attacks against critical information systems: ANSSI has delegation from the Prime Minister to decide on protective measures and implement the crisis response.*

The 2014-2019 Military Programme Law (LPM) imposes a reinforcement of the safety of the Organisations of Vital Importance (OIVs) and introduces the concept of Information Systems of Vital Importance (SIIV) which ensure a vital mission in the form of National Security Directives (DNS).

The provisions of Article 22 of the Military Law provide for: Mapping and risk analysis – Incident reporting – Security checks – Crisis responses.

*For **air transport**, the decree of 11 August 2016 fleshes out this framework and sets rules in its Appendix I. IS Security policy – Homologation – Cartography – Maintenance in safety conditions – Logging – Correlation and analysis of logs – Detection – Incident and Alert Processing – Crisis Management - Identification – Authentication – Access Rights – Administrative Accounts – Administrative information systems – Partitioning – Filtering – Remote Access – Service and Equipment Installation – Indicators.*

DGAC/DSNA

In France, the DSNA is a certified operator within the context of the "Single Sky" European texts, which have obligations in terms of ISS. Since the mid-2000s it has been subject within this framework to controls by the supervisory authority (DSAC) through audits.

The modernisation of all ground networks with numerous interconnections (VOIP, SESAR, etc.) has been accompanied by a strengthening of the protection modes including physical redundancies with associated reconfiguration modes, enabling, among other things, the risk of ATM black screens to be covered for several minutes.

The DGAC/DSNA has decided to set up a new security and protection system akin to a SOC[1] in order to obtain integrated ISS, including both operations and administration. This organisation complements a robust, proven core by adding a layer of supervision and control.

Council for Air Transport Cybersecurity

On 12 April 2018, Elisabeth Borne, French Minister for Transport, set up the Council for Air Transport Cybersecurity (CCTA) to assess the overall French cyber-risk with essential coordination between professionals: state services, aircraft and equipment manufacturers, operators and professional federations. This body is a place of reference for civil aviation stakeholders to frame, structure and coordinate cybersecurity initiatives in the French air sector. This council will be France's voice in the European and international technical working groups.

The presidency of the Council for Air Transport Cybersecurity is entrusted to the Director General of Civil Aviation. Three vice-presidents are also appointed: the Director General of the National Agency for Information Systems Security (ANSSI), for the state sector, and the management of Airbus and ADP groups for the Industry and Operators sectors respectively.

The Council is composed of three technical committees:

- *CT1: "cyber risks", responsible for updating a hierarchy of risks possibly affect the air transport sector;*
- *CT2: "impact", responsible for proposing measures to mitigate these risks, taking into account the impact of these measures (security, economy, etc.);*
- *CT3: "regulation", responsible for formulating national draft texts and deploying a strategy to influence international bodies.*

The Council will have the mission of piloting the cyber resilience of air transport according to three major axes:

- *establish and update a hierarchical threat map;*
- *assess the adequacy of mitigation measures;*
- *initiate good practices, standards or rules, with the aim of promoting them in the international debate.*

1 SOC : Security Operations Center.

European Network and Information Security Agency (ENISA)

ENISA is a European agency responsible for ensuring the security of the information society in Europe. It is located in Heraklion in Crete (Greece).

ENISA's mission is to ensure a high level of network and information security. It acts in different ways:

- *by providing expert advice on network and information security to national authorities and European institutions;*
- *by promoting the exchange of best practices;*
- *by facilitating contacts between institutions (national and European) and businesses.*

ENISA, in collaboration with the national authorities and the European institutions, is working to develop a culture of information network security throughout the European Union.

In June 2018, ENISA organised a cyber-exercise with all air transport stakeholders, using different attack scenarios that were as realistic as possible.

European Centre for Cybersecurity in Aviation (ECCSA)

ECCSA is primarily an information centre for cybersecurity in aviation providing, amongst other services, stakeholders networking and information sharing, which are key enablers to enforce a resilient aviation cyberspace.

ECCSA makes available to its members secure means to exchange domain relevant cybersecurity information, such as vulnerabilities, i.e. weakness that can be used for malicious purposes, as well as events and incidents that might be worth sharing with the aviation community.

The ECCSA's operational team of analysts provides additional inputs as well as context to the information shared by the participants, with the aim to facilitate the creation and the management of an aviation cybersecurity threats knowledge and risk picture.

The participation to ECCSA is voluntary as well as the information sharing. Organisations relevant for the safety and security of European Civil Aviation may apply for ECCSA membership, assured to meet applicable security selection criteria.

APPENDIX 2: INFORMATION SHARING AND ANALYSIS ORGANISATIONS (ISAOs)

European Aviation ISAC (EA-ISAC)

The purpose of the EA-ISAC preparation group, an industry initiative, is to define the rules governing the exchange and protection of Confidential Information such as threats, incidents, vulnerabilities between the Members related to the formation of the EA-ISAC, an initiative with other European aviation sector stakeholders with the intent to establish an European Aviation Information Sharing and Analysis Center (EA-ISAC).

The primary objectives of the EA-ISAC are the following:

- *sharing of information and analysis*
- *coordinated responses to threats*
- *raising outside awareness*
- *promotion of EA-ISAC work*

The EA-ISAC distinguish between two Membership Categories:

- *the Principal Members – which are from the civil aviation industry: e.g. operators (airlines, airports), manufacturers (aircraft, aircraft & ground systems), air navigation service providers, MRO's,*
- *and Associated Members – (Administration, Industry Partners, other relevant organizations; e.g. EASA, ENISA, CERT-EU)*

Providing a common governance structure considering and anticipating the different stakeholder groups, member profiles their advantages and constraints supporting timely, securely Sharing of Information and analysis using a formal protocol – TLP (Traffic Light Protocol) is challenging.

In the aeronautic environment Cybersecurity as a "shared responsibility" requires reliable and secure channels for exchange of information. The establishment of an EA-ISAC is therefore a corner stone and major pre-requisite for Cybersecurity Management.

US Aviation ISAC (US A-ISAC)

The purpose of the US A-ISAC, an industry initiative supported by the US Government, is to provide aviation focused information sharing and analysis functions to help and protect global aviation businesses, operations and services.

The US A-ISAC is setup as a company to define and govern the rules for the exchange and protection of Confidential Information.

The primary objectives of the US A-ISAC are analysis and timely sharing, of relevant and actionable cyber security information as it pertains to vulnerabilities, incidents and threats.

The US A-ISAC membership is open to trusted private sector global aviation companies. It distinguishes between three Membership Categories – Silver, Gold and Platinum (www.a-isac.com/join).

To which Tiered status Members belong is determined by the US A-ISAC, given criteria's are established cyber security capabilities and annual revenue.

For information sharing as formal protocol – TLP (Traffic Light Protocol) is used.

APPENDIX 3: EXTRACT OF THE REPORT OF THE 39th SESSION OF ICAO (OCT. 2016)

Resolution 16/2: Addressing Cybersecurity in Civil Aviation

The Assembly,

Whereas *the global aviation system is a highly complex and integrated system that comprises information and communications technology critical for the safety and security of civil aviation operations;*

Noting *that aviation sector is increasingly reliant on the availability of information and communications technology systems, as well as on the integrity and confidentiality of data;*

Mindful *that the threat posed by cyber incidents on civil aviation is rapidly and continuously evolving, that threat actors are focused on malicious intent, disruption of business continuity and theft of information for political, financial or other motivations, and that the threat can easily evolve to affect critical civil aviation systems worldwide;*

Recognizing *that not all cybersecurity issues affecting the safety of civil aviation are unlawful and/or intentional, and should therefore be addressed through the application of safety management systems;*

Reaffirming *the importance and urgency of protecting civil aviation's critical infrastructure systems and data against cyber threats;*

Considering *the need to work collaboratively towards the development of an effective and coordinated global framework for civil aviation stakeholders to address the challenges of cybersecurity, along with short-term actions to increase the resilience of the global aviation system to cyber threats that may jeopardize the safety of civil aviation;*

Acknowledging *the value of relevant initiatives, action plans, publications and other media designed to address cybersecurity issues in a collaborative and comprehensive manner;*

Recalling *initiatives by the principals of Airports Council International (ACI), the Civil Air Navigation Services Organisation (CANSO), the International Air Transport Association (IATA) and the International Coordinating Council of Aerospace Industries Associations (ICCAIA) and ICAO that recognized the need to work together and be guided by a shared vision, strategy and roadmap to strengthen the global aviation system's protection from and resilience to cyber threats;*

Recognizing *the multi-faceted and multi-disciplinary nature of cybersecurity challenges and solutions;*

1. Calls upon *States and industry stakeholders to take the following actions to counter cyber threats to civil aviation:*
   a) *Identify the threats and risks from possible cyber incidents on civil aviation operations and critical systems, and the serious consequences that can arise from such incidents;*
   b) *Define the responsibilities of national agencies and industry stakeholders with regard to cybersecurity in civil aviation;*
   c) *Encourage the development of a common understanding among Member States of cyber threats and risks, and of common criteria to determine the criticality of the assets and systems that need to be protected;*
   d) *Encourage government/industry coordination with regard to aviation cybersecurity strategies, policies, and plans, as well as sharing of information to help identify critical vulnerabilities that need to be addressed;*
   e) *Develop and participate in government/industry partnerships and mechanisms, nationally and internationally, for the systematic sharing of information on cyber threats, incidents, trends and mitigation efforts;*
   f) *Based on a common understanding of cyber threats and risks, adopt a flexible, risk-based approach to protecting critical aviation systems through the implementation of cybersecurity management systems;*
   g) *Encourage a robust all-round cybersecurity culture within national agencies and across the aviation sector;*
   h) *Determine legal consequences for activities that compromise aviation safety by exploiting cyber vulnerabilities;*
   i) *Promote the development and implementation of international standards, strategies and best practices on the protection of critical information and communications technology systems used for civil aviation purposes from interference that may jeopardize the safety of civil aviation;*
   j) *Establish policies and allocate resources when needed to ensure that, for critical aviation systems: system architectures are secure by design; systems are resilient; methods for data transfer are secured, ensuring integrity and confidentiality of data; system monitoring, and incident detection and reporting, methods are implemented; and forensic analysis of cyber incidents is carried out; and*
   k) *Collaborate in the development of ICAO's cybersecurity framework according to a horizontal, cross-cutting and functional approach involving air navigation, communication, surveillance, aircraft operations and airworthiness and other relevant disciplines.*

2. Instructs *the Secretary General to:*

   a) Assist and facilitate States and industry in taking these actions; and

   b) Ensure that cybersecurity matters are fully considered and coordinated across all relevant disciplines within ICAO.

APPENDIX 4: HIGH LEVEL CONFERENCE CYBERSECURITY IN CIVIL AVIATION DECLARATION

8-9 November 2017, Kraków, Poland

The Krakow Conference has been built on the discussion held during ***Key Recommendation R14****: ICAO shall lead and coordinate at worldwide level all activities contributing to enhancing cybersecurity in civil aviation[2]. EASA and national authorities shall be* ***given a mandate to define and decide on cyber action plans*** *and quickly put in place* ***roadmaps*** *with associated* ***resources and timelines*** *together with minimum short term measures.*

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.

The Conference:

- *called upon the Council and the European Parliament to conclude the negotiations on the revision of Regulation 216/2008 namely to clarify the role of EASA within cybersecurity;*
- *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);*

2 *www.easa.europa.eu/newsroom-and-events/events/high-level-meeting-cybersecurity-civil-aviation*

- *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[3]) 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;*
- *encouraged the European Aviation Safety Agency (EASA) to ensure that the European Plan for Aviation Safety (EPAS) reflects all efforts required at European level;*
- *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, rule-making, 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;*
- *acknowledged the objective to secure the use of solely digital information from the origin of the Definition of Need to its fulfilment in aviation, in response to the benefits possible by the emergence of new digital technologies;*
- *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;*

---

3 *Members: ACI Europe, Aerospace Industries Association of America Inc.- AIA (Boeing), Airlines for Europe - A4E (Lufthansa), ASD, CANSO (ENAV), CERT-EU, DG CNECT, DG Move, ECA, ECAC (FOCA), ENISA, EUROCONTROL NM, European Defence Agency, European Independent Maintenance Group – EIMG, GAMA, IATA, ICAO, SESAR Deployment Manager, SESAR Joint Undertaking, Member States (Poland), Member States (UK), Member States (Finland), EASA.*

- *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;*
- *recognised that cybersecurity is an interdisciplinary problem in transport that has its challenges in aviation, but also in shipping, rail and road transport;*
- *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,*
- *welcomed the joint EASA / Computer Emergency Response Team (CERT-EU) initiative to inform on a regular basis the transport community on the cyber situation an threats.*
- *acknowledged the need to evaluate the progress made together with ESCP within 12 months.*

APPENDIX 5: INTERNATIONAL NORMS AND STANDARDS

ISO 27000 standards

The ISO standards applicable to safety are grouped together in an Integrated Management System (IMS) which includes aspects linked to safety and security (ISO 27000), quality (ISO 9000) and environment (ISO 14000).

The ISO 27001 certifying standard demonstrates that an organisation is in control of its cybersecurity. However, this standard, while an essential component, is not the only key to controlling cyber-risks. It is also necessary to add a powerful risk management process that can draw on ISO 27005 (which puts forward a methodology) as well as a set of technical skills. Safety and security aspects are difficult to dissociate, as acts of malicious intent can lead to both safety and/or security risks. IS flaws should be considered broadly as software bugs.

EU NIS Directive

The NIS directive is the first European legislation on cybersecurity. It provides legal measures designed to raise the overall level of cybersecurity in the EU.

The NIS Directive was adopted by the European Parliament on 6 July 2016 and came into force in August 2016. Member States have 21 months to transpose the Directive into their national legislation and another 6 months to identify operators of essential services. In France, it was endorsed in a law passed on February 26, 2018[4].

The NIS Directive provides for legal measures to strengthen the overall level of cybersecurity in the EU by, inter alia, ensuring:

- *that Member States are properly equipped (creation of a Computer Security Incident Response Team, or CSIRT) and put in place a competent national authority (in France the ANSSI);*
- *that collaboration between all Member States is strengthened by setting up a cooperation group to support and facilitate strategic cooperation and exchange of information between Member States. They must also establish a CSIRT network, to promote rapid, effective operational cooperation on specific cybersecurity incidents and to share information on risks.*
- *the development of an intersectoral security culture vital for the European economy, relying heavily on ICT (Information and Communication Technologies)*

4 *www.ssi.gouv.fr/actualite/adoption-du-projet-de-loi-transposant-la-directive-europeenne-nis/ www.legifrance.gouv.fr/eli/loi/2018/2/26/INTX1728622L/jo/texte*

*in sectors such as energy, **transport**, water , banking, financial market infrastructures, healthcare and digital infrastructure. Enterprises in these sectors identified by Member States as essential services operators will be called on to take appropriate security measures and report serious incidents to the competent national authority. Similarly, leading digital service providers (search engines, cloud computing services and online markets) will have to comply with the security and reporting requirements of the new directive.*

LPM

Passed in France on 18 December 2013, the Military Programming Law follows on from the guidelines set out in the 2013 White Paper on Defence and National Security.

This law, in particular Article 22, provides for measures to strengthen the cybersecurity of Operators of Vital Importance (OIV) and gives ANSSI new prerogatives: the agency, on behalf of the Prime Minister, may impose security measures on OIVs and checks of their most critical information systems. In addition, Article 22 makes it mandatory for OIVs to report any incidents noted in their information systems.

Strategic Review of Cyberdefence

This document, a veritable White Paper on Cyberdefence, is the first major strategic overview in this area. Organised into three parts, it presents a panorama of the cyberthreat, formulates proposals for improving the cyberdefence of the Nation and offers perspectives for improving the cybersecurity of French society.

The strategic review of cyberdefence, entrusted by Prime Minister Edouard Philippe to Louis Gautier, Secretary General of Defence and National Security (SGDSN), marks the beginning of a cyberdefence strategy based on reinforcing the protection of state security systems and organisations of vital importance as well enhancing digital security for citizens, institutions and all actors who participate in the economic, industrial, social and cultural dynamism of our country.

FAA - EASA - ICAO

Many international organisations are dealing with aeronautical cybersecurity, but there is still no harmonised set of regulations: the FAA is devoting significant means to the subject, EASA too, although with more limited resources. ICAO has issued incentive recommendations (see Appendix 3) but these remain to be implemented.

APPENDIX 6: PROTECTION OF INTERBANK EXCHANGES

How has the banking world organised itself in terms of security standards and associated certification? The Payment Card Industry Data Security Standard[5] (PCI DSS) was introduced in the 2000s when online payment by credit cards began to develop. This standard was created to increase controls on cardholder information so as to reduce the fraudulent use of various payment instruments. The stakes were high. It was necessary to join the forces of banks, retail outlets, card issuers and even equipment manufacturers and service providers – smart cards, payment terminals, network infrastructures – until each banking transaction was consolidated.

An international forum, the PCI Security Standards Council (PCI SSC), was set up to act as an authority for the enhancement, propagation and implementation of security standards aimed at protecting account data, under the leadership of the principal payment card groups such as Visa, MasterCard, American Express, Discover Card and JCB. Each group could still keep its specificity, however, which means that the MasterCard Security Data Protection programme and Visa's Account Information Security programme consist of contractual rules established between their networks and affiliates (credit and payment institutions) ***which define the level of conformity with the standards defined by PCI SSC****. It is not PCI SSC that applies any penalties but each network according to its rules.* ***This flexibility has led to global adoption of the PCI standard****.*

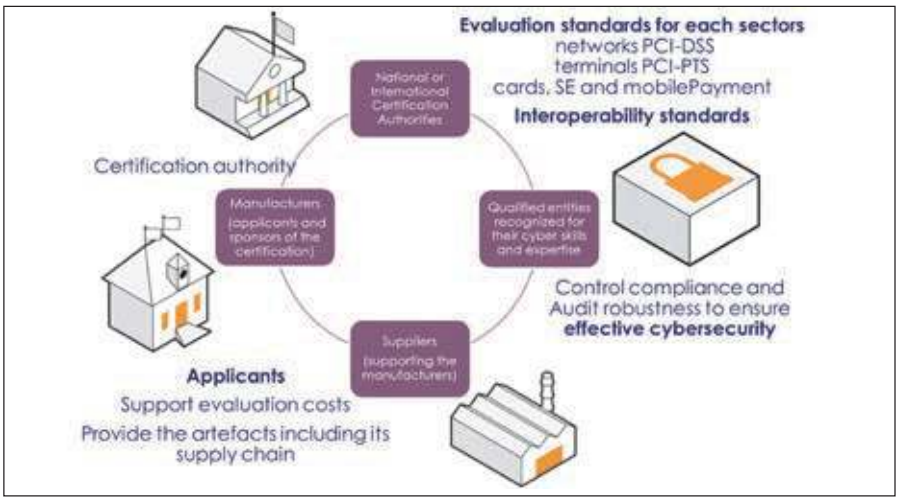


Figure 7: Certification of inter-bank exchanges.

5 *www.pcisecuritystandards.org/security_standards*

The PCI SSC therefore focused on developing a two-tier system: ***on the one hand the standard PCI DSS*** *for infrastructures and PCI PTS for terminals, with the goal of international interoperability;* ***on the other hand a certification eco-system*** *enabling checks on the conformity of all actors through certifications and entities qualified by the certification authorities, capable of carrying out technical audits performed by experts in cyber-security.*

It can thus be noted that the banking authorities – while retaining their certification role – have delegated responsibility for technical evaluation to qualified, trusted third parties in order to enable an efficient industrial, international response.

On the one hand, the PCI DSS standard lists a set of checkpoints relating to information systems that capture, transport, store and process credit card data. These checkpoints are linked to computer techniques but also to organisational procedures and verifications on these systems.

On the other hand, the PCI SSC maintains a list of approved companies to perform compliance checks and vulnerability analyses of information systems. On the basis of the PCS DSS technical standard, qualification and training criteria were established. PCI SSC thus provides training courses in assessment (ISA, Internal Security Assessor) and qualifies security auditors (QSA, Qualified Security Assessor) authorised to perform on-site audits and approve security solution providers to perform vulnerability scans (ASV, Approved Scanning Vendor). These audits are to be renewed each year.

It is interesting to note from this example that, for questions of cybersecurity, interoperability requires technical standards, and also that it is essential, to maintain robustness against ever-changing attack capabilities, not to operate in an open loop, and to ensure that technical audits are carried out by qualified cybersecurity experts.

It is this last point that constitutes a real change for our aeronautical eco-system: maintaining in a state of security.

APPENDIX 7: RETHINKING THE SAFETY OF ATM SYSTEMS[6]

Many experts are currently working on this subject and a number of proposals are currently being studied by ICAO, notably those stemming from the European SESAR research programme. While opinions still diverge, experts seem to agree on a number of principles:

- *the need for a realistic* ***security policy,*** *defining the goals, means and procedures implemented for safety and cybersecurity. This policy must among other things define degraded modes, or how to continue functioning in the event of an attack;*
- *the need for very* ***strict checks to identify players*** *authorised to connect to the network;*
- *the adoption of various levels of security to* ***restrict access to the core*** *of systems through secure interface devices;*
- *the setting up of* ***authentication*** *and, if necessary,* ***encryption*** *devices depending on the sensitivity of the data to be exchanged;*
- *the deployment of a* ***Security Operational Centre*** *(SOC) aimed at detecting and responding to potential attacks. The SOC can be supported by a Security Information and Event Management (SIEM) system capable of real-time analysis of multiple network events;*
- *the interfacing of the different SOCs with* ***Computer Emergency Response Teams*** *(CERT), responsible for concatenating events reported by SOCs at the national or international level so as to identify, anticipate and inform on the state of threat. A typical example is the CERT-EU set up at European level, compliant with the RFC 2350 standard, which works as a kind of centre centralising all threats and identifying whether an attack is localised or global.*

Among these professionals, one group of experts is looking into ways to ***secure air-ground links****. These links are particularly important especially for data link applications (instructions or clearances transmitted by means of digital data from the ground to the plane), for trajectory management exchanges between ground and onboard systems and for the remote piloting of unmanned aircraft (drones).*

The security challenges of digitalisation

The IP (Internet Protocol) standard is the reference chosen for fixed and mobile communications (ground/ground or air/ground), including voice (ground-ground

6 *Presentation by Jacky Pouzet (Eurocontrol) at the* Entretiens de Toulouse *(Toulouse Encounters) 2018.*

VoIP). The use of this widely used industrial protocol must be secured to meet the safety and security requirements inherent to air traffic control operations.

Pending a global solution from ICAO, progress is being made step by step: a first step has been taken with the implementation of a pan-European network for ground/ground communications. This network, which has been operational for ten years, is private, connecting only operational control centres.

These first experiments with opening up communications have proved conclusive in the sense that no serious attack has been recorded. Moreover, during network security tests under the SESAR programme, the effectiveness of SOCs/SIEMs has been demonstrated, ensuring rapid detection of intrusions. Aviation is therefore proceeding to open things up even more by expanding the number of users with access to aviation networks, notably via web (public) services.

An interesting example is migration to the Voice over IP (VoIP) standard. The transmission of the "aviation" voice by an IP standard has strong performance requirements to avoid distortion related to transmission delays; this requirement prohibits the use of conventional security "firewall" devices and therefore makes it necessary to integrate security into the communication protocol.

To do so, the new VoIP standard calls for implementation of IPv6 communications protocol to secure transmissions, mainly based on the "Secure Real-time Transport Protocol" (SRTP) and "IPSEC" protocol, ensuring security and encryption if necessary. The purpose of this security protocol is to authenticate, authorise and verify the integrity of communications while ensuring traceability.

In addition to these secure protocols, the systems architecture must benefit from physical security to protect the infrastructure against possible sabotage.

Active management of security is also recommended with the implementation, for instance, of real-time monitoring of log files made by an expert system (SIEM, as mentioned above). The architecture must also include secure areas to access the core of the system. This results in technical requirements for the operational network transporting this data and voice, in particular access control, resistance to incidents, a monitoring and supervision device and network control services enabling immediate action in the event of an intrusion (shut-down of certain branches of the network for example). The following figure, extracted from the "VoIP" standard, shows the different zones mentioned above (c. f. Figure 8, next page).

This security scheme, currently being deployed for voice links, may also be applied to mobile data links.

The security challenges of digitalisation, the case of mobile data links

The security challenge is even more complex for mobile links because physical links (radio links in this case) are accessible to all, so it is important to secure them via other devices such as frequency agility techniques, for example.

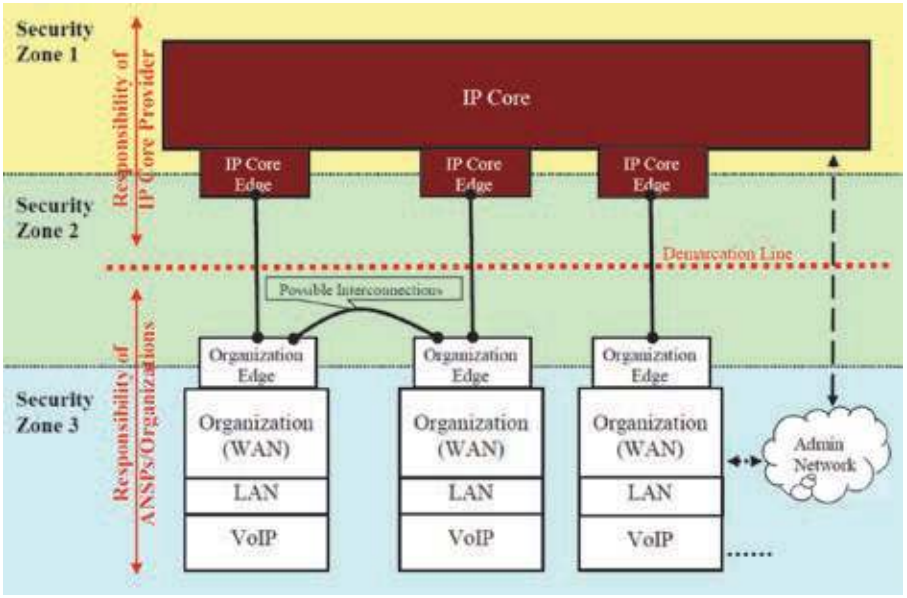


Figure 8: Architecture of a communications network with VoIP standard.

The (binary) VHF data links currently used are not secure and are therefore easily "observable"; this vulnerability is acceptable insofar as the applications transiting these links are not critical.

To support more critical applications, ICAO has recently standardised a new technology for airport communications, particularly exposed to potential cyberattacks. This technology, derived from the WIMAX industry standard, integrates from the outset safety devices such as:

- *a technology operating over a protected broad spectral band (as opposed to the narrow VHF bands) so as to benefit from the agility of random frequency, making unauthorised eavesdropping difficult;*
- *the possibility of dividing the communication channel into several independent channels, separated hermetically;*
- *a device integrated into the technology for authenticating subscriber stations using X.509-compliant certificates. It should be noted that this type of certificate is already used by the aeronautical messaging standard that has not had a failure in the last 10 years;*
- *finally, in addition to this authentication, ICAO advocates the use of IPSEC security protocol as referenced previously as for voice over IP.*

Open questions

Are security and interoperability definitively contradictory? How to put our trust in safety devices? What solutions need to be put in place to detect, identify and respond to threats? How to maintain minimal operations (degraded mode) in the event of attacks? How to isolate infected or contaminated parts without endangering the safety of the entire system. Can we proceed with standardisation (see interoperability) while ensuring a high level of safety?

APPENDIX 8: INMARSAT INTRODUCES SB-S INTO COMMERCIAL SERVICE

18-04-2018

Inmarsat has entered its next-generation satellite IP platform SwiftBroadband-Safety (SB-S) into commercial service.

SB-S is designed to meet the needs of aviation data communications in the digital age and offers airlines game-changing visibility into their airline operations. It is the first and only global, secure, broadband platform for operations and safety communications.

SB-S unlocks a world of digital intelligence for airlines, transforming the role of satcom from a safety utility to a key source of strategic value. The platform enables a range of value-added applications, allowing airlines to utilise rich, real-time data to drive decision-making, improve operational efficiency and assure the highest levels of safety in the skies.

The commercial service introduction follows a successful in-flight evaluation on Hawaiian Airlines' Boeing 767-300 aircraft and installations on the airline's entire Airbus A321neo fleet. SB-S is also in flight evaluations with United Airlines and Shenzhen Airlines, and has been selected by Airbus as a Light Cockpit Satcom (LCS) solution on its A320 and A330 families.

The platform is already attracting significant industry recognition. It has undergone successful evaluation by the US Federal Aviation Administration (FAA)'s Performance-Based Aviation Rulemaking Committee (PARC) as a platform to provide direct data link communication between pilots and air traffic control (ATC). In addition, SB-S received the prestigious 2018 Jane's ATC Award in the Technology category last month.

Captain Mary McMillan, Inmarsat Aviation Vice President of Safety and Operational Services, said: "With SB-S in commercial service, the aviation industry can now fully realise the benefits of the connected aircraft – driving greater efficiency in airline operations, while leading the way for the future of aviation safety. We are excited to see the real-world impact that SB-S will have on aviation efficiency and safety in the months and years to come".

SB-S reduces airlines' fuel costs and CO_2 emissions through enabling connected Electronic Flight Bag (EFB) applications, including real-time weather reports, optimised profile descent and trajectory-based operations. Flight tracking, real-time flight data streaming (Black Box in the Cloud) and interface with rescue coordination centres will assure safety by providing a solution to the International Civil Aviation Organization (ICAO)'s imminent new Global Aeronautical Distress & Safety System (GADSS) requirements on flight tracking and data recoverability.

With SB-S, remote, secure access to onboard data delivers aircraft health and performance information to the ground in real time, improving predictive maintenance and assisting in quick fault resolution for faster on-the-ground turnaround.

Increased periodic position reporting enables reduced separation minima, unlocking additional airspace capacity to match growing demand, while digital SatVoice capabilities relieve pressure on currently crowded VHF radio links. SB-S provides a secure communications and surveillance solution for ATC requirements, and its broadband capability is essential for air traffic management (ATM) modernisation.

SB-S also serves as the platform for Iris, a ground-breaking programme with the European Space Agency (ESA) that will enable 4D trajectory ATM which is expected over Europe by 2020.

Inmarsat is the only aviation broadband provider capable of connecting the complete aircraft from cabin to cockpit with its own network. Inmarsat's networks are designed for total data segregation between regulated safety and operational services and passenger connectivity, with a 'data fortress door' ensuring the highest level of information security.

SB-S is available through a global network of leading distribution partners including SITAONAIR, Rockwell Collins and China Transport Telecommunication Information Group Company Limited (CTTIC) / Aviation Data Communication Corporation (ADCC) in China[7]*.*

7 *www.adsadvance.co.uk/inmarsat-introduces-sb-s-into-commercial-service.html*

APPENDIX 9: PERSONS INTERVIEWED

Pascal ANDREI	Airbus Group	Director of Aircraft Security
Philippe BOISSAT	AKKA Technologies	Senior VP Aerospace & Defense
Thierry BON	Thales Raytheon	Responsable Export nouveaux produits
Éric COUDRIER	DGAC/DSNA/DTI	Head of Voice & Air-Ground Comm
Maurice GEORGES	DGAC/DSNA	Directeur DSNA
Stéphane KARDAS	ANSSI	Coordonnateur secteur transport aérien
Marc LEYMONERIE	Air France KLM Group	IT Director of Security Solutions
Éric MELCHIORI	Liebherr Aerospace	Responsable Sûreté
Bruno NOUZILLE	Thales Avionics	VP - directeur Technique
Jacky POUZET	Eurocontrol	Head of Frequency & Communication
Philippe PRIOUZEAU	Thales	Directeur Technique Commercial Avionics
Nicolas REICHERT	Airbus	Security – Vulnerability Management
Alain ROBIC	Deloitte / ex-Cassidian	Partner Enterprise Risk Services
Loïc ROBIN	DGAC/DSNA	Responsable SSI
Philippe ROQUES	CLS	Directeur général adjoint Digital et Opération
Benoît ROTURIER	DGAC/DSNA	Directeur programme Navigation par satellite
Éric VAUTIER	Aéroports de Paris	Responsable SSI

APPENDIX 10: MEMBERS OF THE WORKING GROUP

Cordula BARZANTNY	AAE
Michel BRAFMAN	AAE
Dominique COLIN de VERDIERE (relecteur/*proofreader*)	AAE
Bertrand de COURVILLE	AAE
Nathalie FEYT	Thales Avionics
Patrick GOUDOU	AAE
Philippe MORIO	DGAC/DSNA
Alain POUYAT	Académie des technologies
Thierry PRUNIER	AAE
Claude ROCHE (relecteur/*proofreader*)	AAE
Guy RUPIED	AAE
Raymond ROSSO	AAE
Michel WACHENHEIM	AAE

BIBLIOGRAPHY

AAE – Académie de l'air et de l'espace (2018) – *Dossier # 42 :* "Aviation plus automatique, interconnectée, à l'horizon 2050", Toulouse.

AIAA – American Institute of Aeronautics and Astronautics – *Decision Paper (2013)* : "A framework for aviation cybersecurity".
www.aiaa.org/AviationCybersecurity (accessed 5 Jan 2018).

Air Transport Association of America, Inc (2009) : "Air Traffic Control Modernization and NextGen: Near-Term Achievable Goals," Subcommittee on Aviation, House Committee on Transportation and Infrastructure, March 18, 2009.

Atanasov, A. & Chenane, R. (2015) : "Security vulnerabilities in next generation air transport system". Chalmers University of Technology.
http://studentarbeten.chalmers.se/publication/193792-security-vulnerabilities-in-next-generation-air-transportation-system (accessed 4 Jan 2018).

Atlantic Council (2017) : "Aviation Cybersecurity – Finding Lift, Minimizing Drag".
www.atlanticcouncil.org/images/Aviation_Cybersecurity_web_1107.pdf
(accessed 3 Jan 2018).

Boeing (2013) : "National Institute of Standards and Technology Request for Information: Developing a Framework to Improve Critical Infrastructure Cybersecurity" April 2013.
http://capinvestinnov.fr/wp-content/uploads/2016/09/SSI-Cyber-security-in-Aviation-White-paper.pdf (accessed 04 Jan 2018).

CANSO – Civil Air Navigation Services Organisation – (2014) : "Cyber Security and Risk Assessment Guide".
www.canso.org/canso-cyber-security-and-risk-assessment-guide
(accessed 4 Jan 2018).

Choi, J, J. Kaplan & Lung, (2017) : "A framework for improving cybersecurity discussions within organizations?" McKinsey Global Institute.
www.mckinsey.com/business-functions/digital-mckinsey/our-insights/a-framework-for-improving-cybersecurity-discussions-within-organizations
(accessed 5 Jan 2018)

Deloitte (2012) : "Transforming the Air Transportation System: A business case for program acceleration", Deloitte, June, 2011.

European Commission (2014) : "What is the SESAR project?", European Commission, 26 February 2014.
http://ec.europa.eu/transport/modes/air/sesar/index_en.htm (accessed 8 Jan 2018)

GAO – Government Accountability Office – (2015) : “Air Traffic Control: FAA needs a more comprehensive approach to address cybersecurity as agency transitions to Nextgen”.
www.gao.gov/products/GAO-15-370 (accessed 4 Jan 2018)

GAO – Government Accountability Office – (2018) : “Homeland Defense: Urgent need for DOD and FAA to address risks and improve planning for technology that track military aircraft”.
www.gao.gov/products/GAO-18-177 (accessed 4 Jan 2018)

ICAO – International Civil Aviation Organisation – Asia and Pacific Office (2017) : “AIGG : ADS-B Implementation and operations Guidance Document (Ed. 10.0)”.
www.icao.int/APAC/Documents/edocs/AIGD%20Edition%2010.pdf
(accessed 4 Jan 2018)

IFALPA – International Federation of Airline Pilots’ Associations – (2013) : “Cyber threats: who control our aircraft ?”.
www.ifalpa.org/store/14POS03%20-%20Cyber%20threats.pdf (accessed 04 Jan 2018)

Mac Callie, Donald (2011) : “Exploring potential ADS-B vulnerability in the FAA’s Nextgen air transport system”. Air Force Institute of Technology
www.hsdl.org/?view&did=697737 (accessed 4 Jan 2018)

NACD – National Association of Corporate Directors – USA (2017) : “Cyber-Risk Oversight. Director’s Handbook Series”.
www.nacdonline.org/files/FileDownloads/NACD%20Cyber-Risk%20Oversight%20Handbook%202017.pdf (accessed 03 Jan 2018)

PwC – PricewaterhouseCoopers – (2016) : “Aviation perspectives: Cyber security and airlines”. (4 Parts: Introduction, Prevention, Detection, Reaction).
www.pwc.com/us/en/industries/industrial-products/library/airline-industry-perspectives-cybersecurity.html (accessed 4 Jan 2018)

SESAR (2015) : “Strategy and management framework study for information cyber security – Application to SWIM research and development”.
www.sesarju.eu/newsroom/all-news/new-study-reports-cyber-security-sesar%E2%80%99s-airport-operations-centre (accessed 10 Jan 2018)

Strohmeier, M., Lender, V. & Martinovic, I. (2014) : “IEEE Communication survey and tutorials: On the security of the Automatic Dependant Surveillance Broadcast Protocol”.
https://ieeexplore.ieee.org/document/6940209 (accessed 3 Jan 2018)

Strohmeier, Martin (2016) : ’’Security in Next Generation Air Traffic Communication Networks’’. University of Oxford.
www.cs.ox.ac.uk/files/8693/Strohmeier%20-%20Security%20in%20Next%20Generation%20Air%20Traffic%20Communication%20Networks.pdf
(accessed 3 Jan 2018)

US Federal Aviation Administration – FAA a – (2013) : “What Is NextGen?,” US Federal Aviation Administration (FAA), 13 May 2013.
www.faa.gov/nextgen (accessed 3 Jan 2018)

US Federal Aviation Administration – FAA b – (2016) : “NextGen Implementation Plan”.
www.faa.gov/nextgen/media/NextGen_Implementation_Plan-2016.pdf
(accessed 3 Jan 2018)

ISAO Standards Organization – ISAO SO
www.isao.org/information-sharing-group/sector/aviation-isac

Summary

Alors que le nombre de personnes qui prennent l'avion chaque année ne cesse d'augmenter, le nombre d'accidents a continué à diminuer. En parallèle, la recherche d'une plus grande efficacité du transport aérien et la demande accrue des passagers d'accéder à de nouveaux services ont été rendues possibles par une large connectivité grâce à la digitalisation croissante du monde de l'aviation.

Mais cette connectivité accrue augmente de manière significative les surfaces d'attaques du transport aérien et risque d'affecter la sécurité des avions.

L'Académie de l'air et de l'espace s'est penchée sur ce sujet d'actualité afin de faire le point sur les risques opérationnels courus par le transport aérien face aux possibilités de cyberattaques. Elle alerte sur les failles potentielles et propose des recommandations aux différents acteurs concernés (industriels, compagnies aériennes, services de navigation aérienne, institutions et autorités publiques), en insistant sur l'urgence d'agir.

En particulier, une des recommandations insiste sur le rôle que l'OACI doit jouer pour aboutir à des règles harmonisées mondialement qui renforceront la chaîne de cyber-confiance dans l'aviation civile.

The number of people flying each year is constantly rising and yet accident rates continue to fall. At the same time, the need for greater efficiency in air transport and the demand for new services on the part of passengers have been successfully met through broader connectivity thanks to greater digitalisation in aviation.

This increased connectivity, however, significantly increases the attack surfaces of air transport and is in danger of impacting aircraft safety.

The Air and Space Academy looked into this pressing subject in order to gauge the operational risks to air transport of possible cyberattacks. This dossier warns of potential weak links and puts forwards recommendations for the various stakeholders (industry, airlines, air navigation services, institutions and public authorities), emphasising the need for urgent action.

One recommendation in particular emphasises the role ICAO must play in pushing through globally harmonised rules to strengthen the cybertrust chain in civil aviation.

www.academie-air-espace.com

ISBN 978-2-913331-78-5
ISSN 1147-3657

15€