HAROKOPIO UNIVERSITY

SCHOOL of Digital Technology
DEPARTMENT of Informatics and Telematics
POSTGRADUATE PROGRAMME Informatics and Telematics
COURSE Information Systems in Business Administration

Main Title :
IoT in Aviation, benefits, threats and risks
Master Thesis

Efstratios Kalantzis

Athens, 2022

ΧΑΡΟΚΟΠΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΣΧΟΛΗ Ψηφιακής Τεχνολογίας
ΤΜΗΜΑ Πληροφορικής και Τηλεματικής
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ Πληροφορική και Τηλεματική
ΚΑΤΕΥΘΥΝΣΗ Πληροφοριακά Συστήματα στη Διοίκηση Επιχειρήσεων

Διαδίκτυο των πραγμάτων στην αεροπορία, οφέλη, απειλές και κίνδυνοι
Μεταπτυχιακή εργασία

Καλαντζής Ευστράτιος

Α. Μ. 15603

Αθήνα, 2022

HAROKOPIO UNIVERSITY

SCHOOL of Digital Technology
DEPARTMENT of Informatics and Telematics
POSTGRADUATE PROGRAMME Informatics and Telematics
COURSE Information Systems in Business Administration

Examining Committee

Dede, Georgia Dr. (Supervisor)
Research Associate &n Adjunct Lecturer, Department of Informatics and Telematics, Harokopio University of Athens

Michalakelis, Christos PhD (Examiner)
Assistant Professor, Department of Informatics and Telematics, Harokopio University of Athens
Kamalakis, Thomas (Examiner)
Assistant Professor, Department of Informatics and Telematics, Harokopio University of Athens

Ethics and Copywrite Statement

I, Stratos Kalantzis, hereby declare that:

1) I am the owner of the intellectual rights of this original work and to the best of my knowledge, my work does not insult persons, nor does it offend the intellectual rights of third parties.

2) I accept that Library and Information Centre of Harokopio University may, without changing the content of my work, make it available in electronic form through its Digital Library, copy it in any medium and / or any format and hold more than one copy for maintenance and safety purposes.

3) I have obtained, where necessary, permission from the copyright owners to use any third-party copyright material reproduced in the master thesis while the corresponding material is visible in the submitted work.

To my family that endures and supports me.

Acknowledgement

To the ones that planted the aviation seed many years back. It keeps growing becoming a big part of my life, in so many ways.

Cudos K. Kavathas

Keep flying high.

Safe landings.

Abstract

The aviation industry has recently begun to adopt and apply modern technologies, such as Internet of Things, in one demanding and hostile environment such as the assembly and maintenance or supply chain of aviation. However, in recent years the number of aviation sites which are based on automation is growing rapidly, and aviation companies are investing in remote controls systems that allow communication anywhere and anytime. It is generally accepted that internet connected aviation sites will be extremely vulnerable to cyber-attacks, as its operation will be highly dependent on ICT and IoT technologies, high systems integration and increased connectivity to backend systems and the Internet.

Despite the widespread acceptance that the risks stem from a desire for autonomy, the literature is still relatively poor. To address the impending threats and to discuss the issue in detail, there should be a specific risk assessment framework based on which any formulated smart aviation site will be evaluated. To this purpose we apply the Analytical Hierarchy Process (AHP) to have a holistic approach to the issue. It is very important for the industry to be able to address cyber security threats to be resilient to them. For this reason, it would be useful to study and evaluate the cybersecurity status of different aviation sites. Any lessons learnt as outcome of the AHP methodology guides the introduction of solutions based on which aviation systems can be resilient against cyber-threats.

CONTENTS

Introduction

Aviation is critical to the global economy. In a competitive environment, the industry is constantly looking for economies of scale and efficiency. That led in the introduction of Internet of Things technologies in the aviation field and the increasing use of this technology information to achieve greater automation in the supply chain, and the assembly lines. Increased digitization may prove to be beneficial for the industry in terms of productivity, efficiency, and performance optimization, but also create serious threats by connecting an assembly line or even an airplane to cyberspace. In one more and more connected and technologically dependent world, new vulnerabilities are emerging. This is due to an ever-increasing number of third parties using stolen data from various systems of aviation organizations. The technologies used are vulnerable to the same threats affecting the commercial, productive, and governmental systems.

The digital transformation has transformed the aviation industry. The decision-making process carried out to a great extent through digital information collected during a flight and transmitted to the headquarters of the organizations. However, this emerging opportunity for aviation poses serious risks. The increased interoperability creates new challenges in the aviation world, such as cyber-war, which consists of a high level of uncertainty and a lack of understanding of the risks.

The increasing complexity, digital transformation, integration, and automation of systems on which the aviation industry is based requires holistic management of the issue. More often, different systems are connected not only to the assembly's or airplane's local network but also to the Internet, which increases the risk. The security of digital systems is now mandatory not only for data protection but also to ensure secure and reliable work. In the worst case, a security incident in cyber can lead to committing criminal acts - such as intrusion to a host of the assembly line, or data theft, loss of control of the repair or assembly process or loss of data or even loss human life.

The use of new technologies such as Internet of Things can contribute to its effectiveness and safety, however, increases the likelihood of a cyber-security incident. To fully achieve the benefits, information security must be considered at all levels of an Aviation Organization. Such organizations need to establish and follow a consistent strategy in cyberspace. A large part of system security breaches is due to people and the incomplete procedures implemented by the organizations. Therefore, both its staff must be considered in the risk assessment process as well as the functions performed by the systems. Applying the best cybersecurity practices, the organization can enhance security and use as a competitive advantage by increasing its market share.

In this dissertation work, we examine the threats to the aviation industry and explores the possible attacks on systems related to physical disasters, supply chain attacks, malware attacks, human or system errors. The main objectives of the work are:

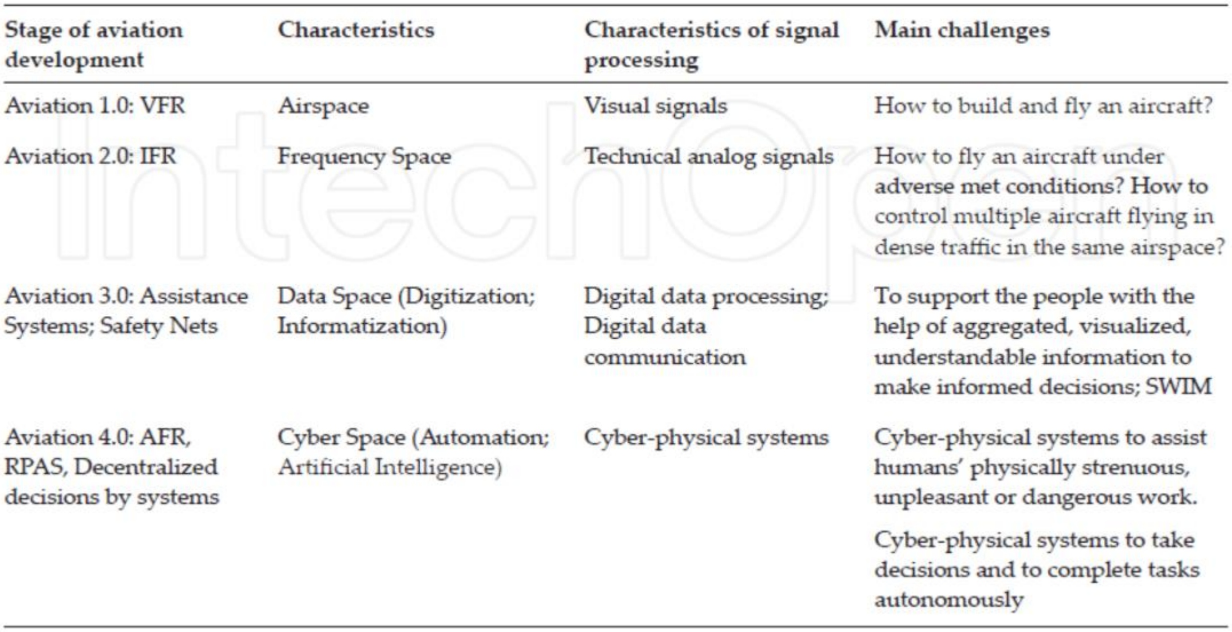
- Investigate the importance of information security throughout aviation's life cycle
- Examine an assembly or repair line's systems and the potential impact of cyber-attacks on these systems
- Investigate the various threat factors, identify the motivations, and identify the origin of the attacks
- To map the possible ways of attack and to identify the systems that create vulnerabilities in aviation security
- Identify the main aspects that contribute to risk mitigation and propose a framework for dealing with them

To fulfill the above objectives, we propose a theoretical and practical approach to the issue. Chapter two goes through a literature review of the Internet of Things and Smart Aviation technology. Also, it elaborates the main vulnerabilities and attacks. Chapter three presents a practical framework of measuring and validating the cybersecurity risks and threats in Smart Aviation utilizing the Analytical Hierarchy Process (AHP). Chapter four presents a case study of applying the AHP method and Chapter five concludes the dissertation work.

IoT and Aviation

Aviation

Just as we can establish four stages in the industrial revolution, we can establish four stages in the evolution of commercial aviation (Valdes et al, 2018). These four stages are closely related to the adoption of higher levels of automation on board aircraft; and controversially, they do not correspond to a deliberate attempt of improving aviation safety in a steady way, but rather to a continuous adaptation to the challenges imposed by its environment following a trial-and-response approach. The four stages in commercial aviation revolution, from Aviation 1.0 to Aviation 4.0 are summarized in the table below.



Stage of aviation development	Characteristics	Characteristics of signal processing	Main challenges
Aviation 1.0: VFR	Airspace	Visual signals	How to build and fly an aircraft?
Aviation 2.0: IFR	Frequency Space	Technical analog signals	How to fly an aircraft under adverse met conditions? How to control multiple aircraft flying in dense traffic in the same airspace?
Aviation 3.0: Assistance Systems; Safety Nets	Data Space (Digitization; Informatization)	Digital data processing; Digital data communication	To support the people with the help of aggregated, visualized, understandable information to make informed decisions; SWIM
Aviation 4.0: AFR, RPAS, Decentralized decisions by systems	Cyber Space (Automation; Artificial Intelligence)	Cyber-physical systems	Cyber-physical systems to assist humans' physically strenuous, unpleasant or dangerous work. Cyber-physical systems to take decisions and to complete tasks autonomously

The four stages in commercial aviation revolution: From aviation 1.0 to aviation 4.0 (Valdes et al, 2018).

Aviation 1.0, the first evolutionary stage, corresponded to the beginning of the commercial aviation were flight evolved under visual flight rules, following visuals clues and signals and there was hardly any instrumental aid to help pilots to fly. This era was dominated by the technological challenges posed by how to build and fly an aircraft. Very simple instruments constituted the so-called first steps toward "*virtualization of the environment*"; and provided basic indications required for the flight: first, anemometers and altimeters to indicate airspeed and altitude; pneumatic and electric gyroscopes to measure attitude and stabilize an artificial horizon; basic mechanical autopilots to keep a straight flight; servos and devices to perceive forces on aerodynamic surfaces (artificial feel load, Mach trim compensator), and soon. Mechanic inventions were progressively incorporated to flight controls in parallel with electric basic instruments to help pilots.

Aviation 2.0, the second stage, was dominated by the replacement of old mechanics by electric devices. Technological advances were driven by two important challenges imposed by the continuous and steady growth of aviation, with a higher number of aircraft operating in the same environment, under all weather conditions:

(i) how to fly an aircraft under adverse meteorological conditions?

(ii) how to control multiple aircraft flying in dense traffic in the same airspace? New instruments such as the VOR (Very high-frequency Omnidirectional Range) and ILS (Instrument Landing System) allowed the pilots to follow safely tracks and approach paths. On board innovations, such as electric autopilots, auto-throttle, flight directors, airborne weather radars, navigation instruments, inertial platforms, and so on, resulted in high safety enhancements.

This evolution came with a rise of information to be managed by the pilot, who could be confronted with a big number of devices and indicators to be monitored and controlled. Aviation 3.0, the third stage in the revolution of commercial aviation involved the massive incorporation of electronics in the cockpit, driven by the availability of reliable and usable digital data processing and data communication technology. At the beginning of this revolution, electronics significantly helped to diminish the clutter of analog instruments and replace the old indicators with integrated colored displays, Cathodic Ray Tube (CRT) and Liquid Crystal Display (LCD), capable of providing a synthetic and/or analytic view of multiple parameters in a limited area of the cockpit.

Technological solutions were progressively designed to support the operators (pilots and controllers) to make informed decisions, with the help of aggregated, visualized, understandable information. Operations onboard and outside of the aircraft shifted from tactical to strategic, and assistance systems and safety nets became crucial elements to increase the level of safety in aviation. The amount of information available in the system raised exponentially while becoming no longer immediately accessible and visible to the operator, who was forced to evolve his/her role from active (flying or controlling tasks) towards a monitoring one. This third revolution in aviation brings the emergence of the notion of the "electronic echo-systems."

As an example, an A-320 incorporates around 190 computers, placed all through the fuselage, which interact between them, sometimes without the pilot being aware. The complexity of the "electronic echo-systems" can be an obstacle for pilots and controllers, as they become sometimes "out of the loop."

Aviation 4.0 is concerned with the design of Cyber-Physical Systems (CPS) that are able to assist humans' demanding work by helping them to take decisions and to complete tasks autonomously, and with its integration of cyber-physical components in future aviation information systems [1]. Cyber-physical systems will make the Aviation 4.0 airframe a digital and smart airplane. The amount and diversity of operational data that can be collected onboard of the aircraft and by ground operations will raise exponentially. In Aviation 4.0, supervisory control in the manufacturing processes and big data acquisition and processing networks make possible automation and integration with IT systems. Airplane operations relay on a grand scale on the employment of CPS.

Future Air Traffic Management (ATM) systems are conceived as a cyber physical system-of-systems (CPSS) that demand tight amalgamation to provide the required capacity, efficiency, safety, and security system performance (Sampigethaya and Poovendran, 2013). In this scheme, examples of cyber components are aircraft digital communications, weather/traffic forecast, flight planning/optimization algorithms, situation awareness and decision support software, and so on, while examples of physical components are mobile aircraft, dynamic airspace traffic, weather, pollution, noise, pilots, air traffic controllers, airlines crew, and so on.

Even today, with only a limited deployment of airborne cyber-physical systems, the available information is immense: maintenance messages/fault codes, Quick Access Recorder (QAR) off light and system parameters; maintenance action logs/test results; real-time data and real-time information management for decision-making, and so on. The great technological parallel developments in data analytics will support active reaction to these enhanced aircraft operations. To illustrate the diversity and the volume of data that the total deployment of aviation 4.0 will imply, let us consider that modern engines (such as the Pratt & Whitney's Geared Turbo Fan GTF engine) can have up to 5000 sensors generating up to 10 GB of data per second. A single twin-engine aircraft with an average 12-h flight time can produce ~800TBof data. While an Airbus A320 transmits about 15,000 parameters per flight, the figure is 250,000 for the A380 and 400,000 for the A350. However, this data is "useless" without targeted analysis.

Challenges related to information assurance and cyber security include the certification of cyber security requirements for e-Enabled airplanes; the development of anti-tamper avionics hardware and software and the collaboration of industry and governments to address the cyber threat to aviation (Sampigethaya, Poovendran and Bushnell, 2008). There are also very important technological challenges for airplane operations, which are as follows:

- worldwide aeronautical networks interoperability, including signal processing and wireless performance as well as the aircraft interfaces to the Internet.
- verification and validation of the onboard software, how to secure end-to-end entire SW supply processes, the understanding of cyber-physical life cycle scale.
- improvement of airplane health, control and prognostics by exploiting sensor networks and data fusion, information management and data analytics and critical real-time data sharing, appropriate end-to-end information exchange, distributed decision-making.
- human-automation interface issues such as visualization, keeping human-in-the-loop and connection between aircraft controls and air traffic systems Industry 4.0 technologies (automation, IOT, artificial intelligence, cognitive computing, bigdata analytics, digitization, data fusion, etc.) have the potential to generate a paradigm shift in the aviation industry, generating new mechanisms to make it not only more efficient but also safer. Unexplored concepts and approaches to safety start being discovered by

companies and researchers trying to approach safety from different perspectives with the new tools that Aviation 4.0 makes available.

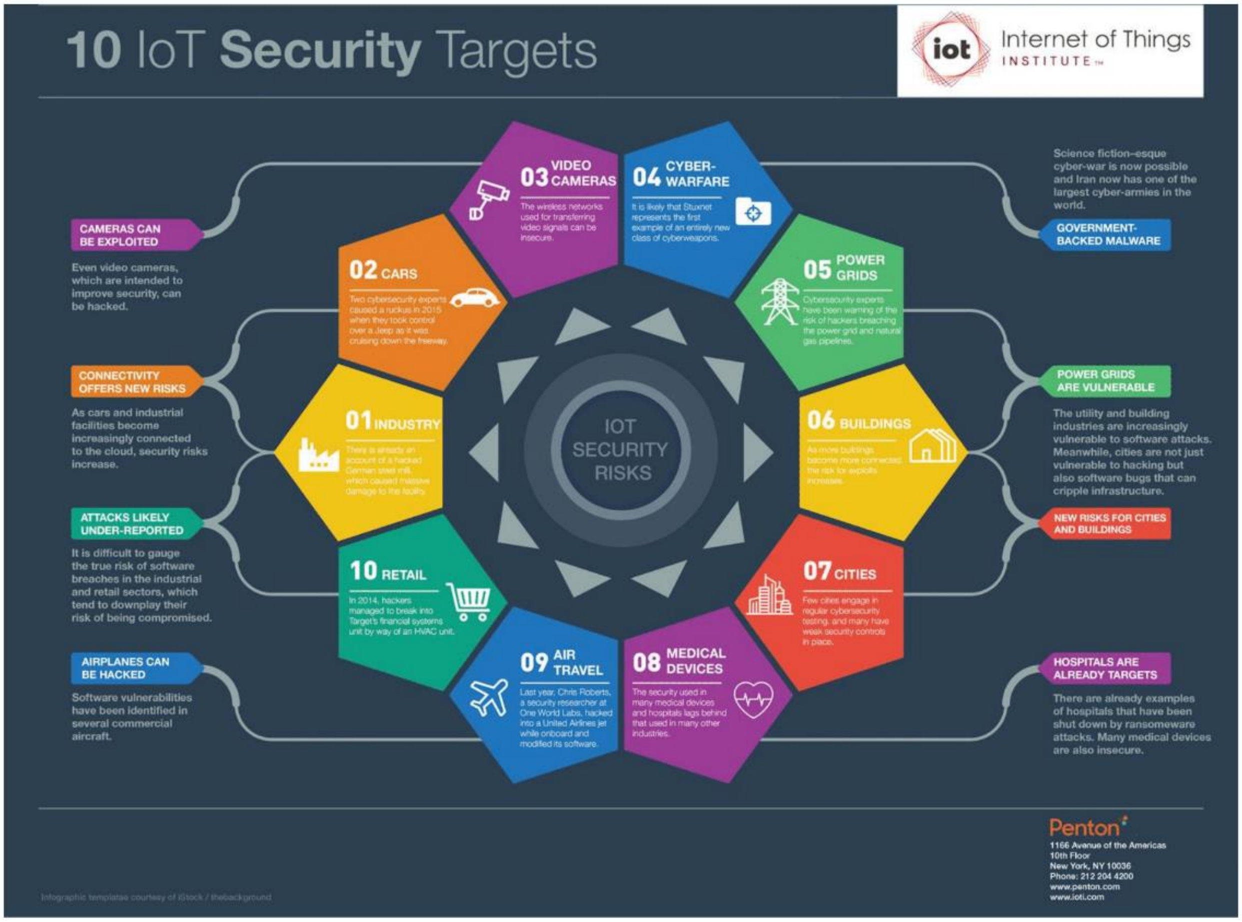
IOT

IoT is principally about attaching varying amounts of identity, interaction and inference to objects (Mukherjee, 2015). Identity can be e.g., tags, shapes and forms or IP addresses. Interaction includes acting, sensing and physical connectivity. The connectivity is not just between devices, but also between materials, spaces, phenomena, human actions, concepts, processes, data repositories etc. Embedded systems play a major role in facilitating those interactions. Varying amount of inference is used to refine the data into information. That can be turned into new applications and services via cloud computing and big data analytics and other digital means. The rapid growth of IoT technology is driven by four key developments.

First, sensors, controllers and transmitters are becoming more powerful, cheaper and smaller. Second, internet penetration, bandwidth and the availability of wireless connectivity is increasing rapidly. Third, data storage and processing capacity are becoming bigger and better, making it easier and more affordable to store and organize data. Finally, innovation in the fields of software applications and analytics, including advancements in machine-learning techniques and algorithms, has allowed people and businesses to leverage the so-called Big Data.

Applications of IoT

The Internet of Things is envisaged to bring many benefits, but it also poses many new challenges and risks (Buntz, 2016). From autos to video cameras, the Internet of Things is exponentially increasing the number of potential targets for cyber-criminals. Hackers could cause havoc in a nation by systematically targeting its power grid. Or the implications of criminals taking control over a city's network of video cameras. Or of a hacker taking control over a commercial airplane en route. In this section we will briefly describe some the most targeted IoT systems with our focus on Airplane security.



10 IoT Security Targets

Internet of Things INSTITUTE™

03 VIDEO CAMERAS
The wireless networks used for transferring video signals can be insecure.

04 CYBER-WARFARE
It is likely that Stuxnet represents the first example of an entirely new class of cyberweapons.

02 CARS
Two cybersecurity experts caused a ruckus in 2015 when they took control over a Jeep as it was cruising down the freeway.

05 POWER GRIDS
Cybersecurity experts have been warning of the risk of hackers breaching the power grid and natural gas pipelines.

01 INDUSTRY
There is already an account of a hacked German steel mill, which caused massive damage to the facility.

IOT SECURITY RISKS

06 BUILDINGS
As more buildings become more connected, the risk for exploits increases.

10 RETAIL
In 2014, hackers managed to break into Target's financial systems unit by way of an HVAC unit.

07 CITIES
Few cities engage in regular cybersecurity testing, and many have weak security controls in place.

09 AIR TRAVEL
Last year, Chris Roberts, a security researcher at One World Labs, hacked into a United Airlines jet while onboard and modified its software.

08 MEDICAL DEVICES
The security used in many medical devices and hospitals lags behind that used in many other industries.

CAMERAS CAN BE EXPLOITED
Even video cameras, which are intended to improve security, can be hacked.

CONNECTIVITY OFFERS NEW RISKS
As cars and industrial facilities become increasingly connected to the cloud, security risks increase.

ATTACKS LIKELY UNDER-REPORTED
It is difficult to gauge the true risk of software breaches in the industrial and retail sectors, which tend to downplay their risk of being compromised.

AIRPLANES CAN BE HACKED
Software vulnerabilities have been identified in several commercial aircraft.

Science fiction–esque cyber-war is now possible and Iran now has one of the largest cyber-armies in the world.
GOVERNMENT-BACKED MALWARE

POWER GRIDS ARE VULNERABLE
The utility and building industries are increasingly vulnerable to software attacks. Meanwhile, cities are not just vulnerable to hacking but also software bugs that can cripple infrastructure.
NEW RISKS FOR CITIES AND BUILDINGS

HOSPITALS ARE ALREADY TARGETS
There are already examples of hospitals that have been shut down by ransomeware attacks. Many medical devices are also insecure.

Infographic templates courtesy of iStock / thebackground

Penton
1166 Avenue of the Americas
10th Floor
New York, NY 10036
Phone: 212 204 4200
www.penton.com
www.ioti.com

10 IoT Security Targets (Buntz, 2016)

1. Industrial Facilities IIoT. It is difficult to know how off industrial plants are hacked for extortion because such breaches are rarely reported, according to Marina Krotofil of the Hamburg University of Technology. At this stage in the game, we need to operate our networks as though a breach will occur (Lee and Kyoochun Lee, 2015).

2. Cars. The most dangerous part of the connected car is the 'connected' part. The threats become much greater as cars become ever-more connected, not to mention semi-and fully autonomous. Electric cars have been drained of battery life using the vehicle

identification number (VIN) and accessing the car’s climate control system. While this, strictly speaking, isn’t life threatening, it’s a good example of how one part of the car’s anatomy can be used to get to another. This could have dangerous consequences if hackers find their way into more critical functions, such as the steering and brakes.

3. Video Cameras. Surveillance cameras are intended to make us more secure, however the wireless networks used for transferring video signals can be insecure. A risk with video cameras—and other IoT devices—is the ability for them to be used to create botnets to send spam and ransomware, launch DDoS attacks, and commit other mischief.

4. IoT-Enabled Spying and Potential for Cyber warfare.

5. Power Grids and Utilities. Targeted attacks are carefully articulated to gain entry into secure facilities like networks of power grids and utilities which are classified as critical sectors. The world of IoT creates significantly more opportunities to breach networks like the power grid and natural gas pipelines.

6. Buildings. The building industry has been slower than many to embrace digital technology. But that is beginning to change quickly as building automation technology rapidly gains in popularity. As more buildings become connected, the risk for exploits increases. When it comes to IoT in the home, people must realize that security of these devices just doesn’t exist yet.

7. City Infrastructure and Transportation Networks. Last year, Cesar Cerrudo, CTO of IO Active Labs proclaimed that many cities risk cyberattacks—even those who don't consider themselves to be so-called "smart cities." The majority of cities around the world use at least some form of connected technology to manage everything from traffic to lighting to public transit. Still, few cities engage in regular cybersecurity testing, and many have weak security controls in place. But it doesn't take a full-fledged cyberattack to cause problems. Even software bugs can cause significant glitches. "We've also seen that Transport for London is looking to IoT sensors and the data they provide to help improve congestion for commuters, but they must not overlook wider security and privacy implications this will have on the City of London," Garlati explains. "IoT, although growing at an enormous pace, is still very much in its infancy –with people eager to get their hands on the latest and greatest connected devices and manufacturers rushing to get them to market –security is often an afterthought."

At worst, poor security controls will mean terrorists will have access to a whole host of information they can use for surveillance or other nefarious purposes If IoT developers don't take steps now to improve security within devices at the development level, the results could be catastrophic, especially when used to capture data on passengers and whole cities as suggested by TfL's CIO, Steve Townsend. "At best, people's privacy and civil liberties are affected. At worst, poor security controls will mean terrorists will have access to a whole host of information they can use for surveillance or other nefarious purposes when security controls aren't properly addressed," Garlati says.

8. Medical Devices and Hospitals. Healthcare is an industry that relies on connected devices and smart sensors to help medical professionals provide more effective patient care. Medical Personally identifiable (MII)information is worth considerably more than other types of PII. The risk around compromising medical devices within hospitals, is geared around the real-time assistance the hospital provides. The risk of physical harm around compromising medical records lays in the concept of mixed medical records.

9. Aviation. Last year, Chris Roberts, a security researcher at One World Labs, made headlines after boasting that he hacked into a United Airlines jet and modified code on the craft's thrust management computer while onboard. An FBI search warrant states that he succeeded in commanding the plane to climb, altering the plane's course. Roberts told the FBI that he had identified vulnerabilities in several commercial aircraft, including the Boeing 737-800, 737-900, 757-200, and the Airbus A-320. Roberts boasted that, in 2012, he had hacked into the International Space Station. Chris Roberts was apparently able to overwrite code on the airplane's Thrust Management Computer while aboard a flight, causing a plane to move laterally in the air.

Airplanes today are controlled by complex connected computer systems. "Sensors all over the aircraft monitor key performance parameters for maintenance and flight safety," Garlati explains. "On-board computers control everything from navigation to in-cabin temperature and entertainment systems. Chris Roberts was apparently able to overwrite code on the airplane's Thrust Management Computer while aboard a flight, causing a plane to move laterally in the air."

Roberts denies having done this during a real flight and Boeing has claimed in-flight entertainment systems are isolated from flight and navigation systems. However, when it comes to the aviation industry the stakes are even higher with regards to potential flaws in IoT systems. "As airlines transition to even more advanced systems leveraging these technologies more attention needs to be focused on underlying system weaknesses that could represent a security and safety risk," Garlati explains. He asks:

- What are airports doing well on this front and what's still missing?
- What is the one major step all airports should take to avert an attack (perhaps hiring a cyber expert? employ a crisis management system?)
- "Airport managers must understand that security is likely to fail if it's not built in by design," Garlati says. "In fact, I would go so far as to say that if it's not secure, it doesn't work. So, the mindset of pen testing and bringing on cyber security experts at a later date to 'fix holes' is a false economy-having said that, it is obviously better than

nothing," he adds. "But industry as a whole, needs to change this mindset and work towards building and developing systems and devices with security at the core. The march of silicon means that it is becoming more powerful and so it is possible to add traditional security layers embedded at the hardware level, making it resilient to attack." Hackers with physical access will be able to accomplish significantly more damage, and traditionally access is the difficult part. "In the case of Chris Roberts hacking an aircraft physical access was the easy part, using the seat electronic box (SEB) which was present for the inflight entertainment system," Pore says. "Network segmentation would definitely have slowed down the attack and perhaps prevented Roberts from accessing critical aircraft management systems. It was noted in the FBI interview that Roberts used default credentials to gain access. There is always significant risk involved with leaving physical access available and not changing default credential sets."

10. Retail Stores and Consumer's Databases. While the cybersecurity risks facing retailers aren't strictly IoT related, a growing number of them are. Retail companies remain one of the most attractive targets for hackers because they store vast amounts of financial and consumer's data. Retail-related IoT devices will only add to that volume.

IoT Architecture

The key entities included in a typical IoT architecture are:

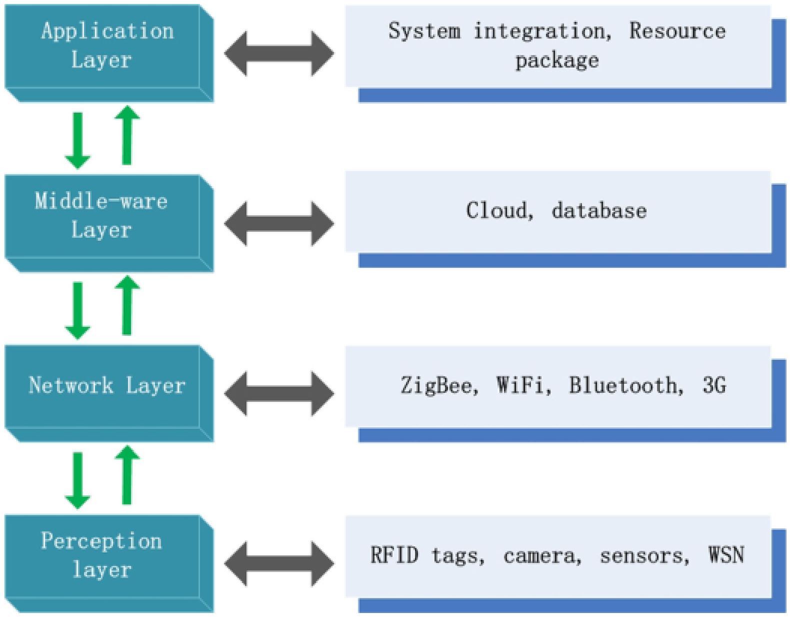
a. application areas
b. detection devices
c. Readers
d. Gateway / middleware
e. internet communication suite
f. web servers
g. cloud platforms
h. end user

An example flow is the following:

1. The point of interest, an object, can be detected. Data can be transferred using RFID or Wifi technology. For example, if the interaction with the objects is based on radio frequency identification, the objects are equipped with an appropriate label using wireless interactions (RFID, ZigBeeq.a.) (Suo et al, 2012).
2. The next level includes the detection devices. For example, in the case of RFID protocol technology, the reader reads the Electronic Product Code (EPC) from a short distance from the device. The RFID reader acts as a web portal. Similarly, in other protocol cases, the zigbee sensor gateway and the wifi router intermediate gateway serve as the gateway to the internet. The gateway can receive the data and take it to the next level.
3. Then there is an interaction of the user's device with an available network (WiFi, 3G / GPRS etc.). And in this way the device connects to the World Wide Web, to send all the traceable data to cloud software platforms (e.g. Azure, AWS, Google) or to end users (laptops, tablets, smartphones, PCs) (Perera et al, 2014), (Singh, Tripathi and Jara, 2014).

The IoT architecture is spread over at least three levels. The first three include the application level, the network level, and the perception layer. At each level different technologies can be used both in terms of the nature of their construction and operation, as well as in terms of dependence on different telecommunications, electrical and other constraints. This makes managing them a difficult and complex process.

To meet this challenge, a middleware level has recently been introduced or, as we will see in the next chapter, gateways are added as proxies to provide different services but protect internal technologies. The intermediate level (server or software) collects information from the lower levels and stores it on a permanent medium (e.g. database) either on the local network or in the cloud. It can also process or analyze data for third party purposes. The following image describes such an architecture with the corresponding technologies at each level.


Application Layer
System integration, Resource package
Middle-ware Layer
Cloud, database
Network Layer
ZigBee, WiFi, Bluetooth, 3G
Perception layer
RFID tags, camera, sensors, WSN

IoT Architecture (Iqbal et al, 2017)

Security of storage through or secure communication with the infrastructure in the cloud computing are the key issues at the level of the middle software in terms of security. The application level implements different applications for different scenarios. Utilizes the results of the analysis or processing of the intermediate level by providing additional information to the end user. At this level, too, security vulnerabilities have been recorded resulting in malicious access to data, or data corruption (Chrysostomou and Hadjichristofi, 2015).

The middleware layer manages the interoperability of the IoT infrastructure. It receives streams of data from the perception and network layer to parse, process, and transfer to the application layer. Depending on the domain of application and the restrictions of the physical environment, the communication medium may vary, while the wireless technologies are dominating the field taking into account their flexibility (e.g. WiFi/WiMax, Zigbee/Bluetooth, 4G / 5G, etc.). Most common attacks to the network layer include man-in-the-middle, and DDoS (Distributed Denial of Service) (Bhushan et al, 2017).

Also, the data collection layer can collect data through sensor systems or protocols. For example, data available from RFID tags (updated by the respective scanners), images / motion data from, environment data from the sensors, are some examples. Technologies at this level are exposed to a variety of risks in addition to cyber-attacks (e.g. natural disasters, malicious actions). This can affect the operation of the whole architecture if there is a significant dependence on data collection (Bhushan et al, 2017).

Security requirements

IoT security is being tackled through the modern challenges facing hundreds of manufacturers of such technologies:

- restrictions on communication
- restrictions on the natural environment
- inadequate protection of data and information.

In the first case, IoT applications become vulnerable to a number of security vulnerabilities due to the different communication protocols used to transmit important data. Depending on the means of communication, the version of the vulnerability becomes unique. Wireless communication protocols in particular are more vulnerable to attacks (e.g. undetected encrypted data packets, signal alteration, denial of service, transmission delay, code implantation in the wireless routing node). In large-scale wireless sensor networks that may involve low-, medium-, and high-bandwidth wireless technologies or transmission range, attacking a single node can affect the operation of the entire system (Bhushan et al, 2017).

In the latter case, the natural environment sets its own constraints and requirements regarding the physical safety of the equipment. If intruders have physical access, then they can obtain information directly from the devices or clone them to spy on the data or even destroy the devices. Also, their designers must consider the requirements in energy consumption or power. Intruders can take advantage of these restrictions and carry out attacks such as Denial of Service. It also appears that due to the above limitations, manufacturers cannot develop more effective security mechanisms on these devices (Seul-Ki et al, 2018).

In the third case, intruders often exploit the lack of mechanisms for identifying and controlling access rights to individual technologies. This way an intruder can access and remotely modify any data moving through the device. This is done in conjunction with the lack of vigilance and information of the end users who may receive a malicious message in their mail that allows the attacker to implant a control program of the device and therefore any IoT device in the network. Thus, the privacy of users' data is violated due to the lack of authentication mechanisms at the entrance of users. Vulnerabilities in the code of application software in th e program may allow malicious users to ingest backdoor code into the system and perform command and control remotely (Belguith et al, 2020).

Additional requirements are presented in the table below.

Security attribute	**Description**
Data integrity	Ensures non-modification of data by unauthorized users
Data confidentiality	Guarantees that the data is not disclosed to non-authorized entities
Data availability	Ensures the non-interruption of access to data and services.
Identification	It aims to prove the identity of an entity and ensure the authenticity of any messages exchanged with other entities. We distinguish in: Peer Entity Authentication and Data Source Authentication.

Authorization	Provides protection of system resource usage, by unauthorized entities.

IoT Security Attributes (Belguith et al, 2020)

Data integrity

Transmitting data in the form of messages on the Internet requires mechanisms in place to confirm the authenticity of the sender and the integrity of the message at the point of receipt. Message digests is one of the key mechanisms for validating data integrity. At the time, a message is received, the mechanism must ensure that the message has not been modified (integrity check), but also that it comes from the sender who claims to have sent it (authentication check).

Furthermore, integrity can be achieved by using the Message Integrity Code (MIC) or the checksum, which is essentially a stream of bits used to verify the integrity of the binary packets. The message integrity code can detect modifications to messages due to misconfigurations or malicious actors. The checksum on the other hand can only detect transmission errors. Examples of attacks on integrity are tampering and spoofing. Typical cryptographic techniques consume large amounts of resources in terms of energy and bandwidth to both the source and the destination.

Data confidentiality

Confidentiality ensures that only authorized IoT nodes can access and control the sensors data. Also, it validates that the data transmitted from one node to another has not been made accessible and interpreted by another node in the middle or third party. This is usually accomplished using an encryption mechanism (e.g. symmetric key), so both the sender and receiver use a common secret key for both encrypting and decrypting the data.

Data availability

Authorized users have uninterrupted access to system information. The system must be functionally available and able to provide its services whenever required. This includes the properties of scalability and the ability to function. Availability attacks include denial of service

(DoS), jamming, and malware. An attack on availability of IoT nodes is usually referring to DoS attacks which may damage nodes at a physical level, mainly through the exhaustion of energy resources. Continuous questions from an attacker to an IoT device that will force it to answer can result in the inefficient operation of a device and the exhaustion of its battery resources in a very short time.

Privacy

Privacy rules determine how independent users can access data. Different IoT systems and devices have different privacy requirements. Hence, privacy policies should complement the identification models and give to the users some specific control, if not all of it. In IoT systems, applications can be included in the standalone system for greater compatibility offering the following capabilities:

- Non-linkability: partitioning personal data for the same user so that no one can create a profile based on that data. For an individual user who owns a multitude of devices, the standalone system should be able to dynamically add noise to the data and then filter it. This will prevent extraction of pattern snippets and reverse reproduced by an attacker. However, the disadvantage of such a method is the increase in the range of data required. Another important task for an IoT system is to determine the optimal amount of added noise and the selected frequency.
- Location privacy: guarantees that the current and past location of a device will not be revealed.
- Context privacy: In context privacy, access information must be kept confidential. The self-protection of personal information as well as the type of data that can be generated and processed by the device must be guaranteed.
- Anonymity: The identity of an IoT node remains hidden, which also helps to ensure the privacy of the infrastructure. A purely anonymous communication is necessary due to possible deficiencies in the existing communication protocols.

Authentication and authorization

It concerns the legitimacy of the parties to be considered to ensure that the communication data must come from an authorized entity. Similarly, for IoT, it is also important to legitimize the parties involved in IoT communications, while respecting restrictions. Authentication requirements include:

Many attacks target authentication to gain access to data. These include eavesdropping, traffic analysis, cloning, replay, spoofing, and man in the middle (MITM) attacks. MITM is a form of active interception where the attacker acts as a router and makes independent connections to the targets and then transmits messages between them. Such an attack can only be successful when the attacker can impersonate each end point to the satisfaction of another.

Self-protection for an IoT system would in this case refer to methods of preventing this process. For this reason, the system should be able to dynamically modify the basic information for a given device, as static information is easier to imitate, so that nodes believe they are communicating with each other through a private connection but in fact the collaboration session is completely controlled by the intruder. Various defense mechanisms against MITM attacks use authenticity techniques based on public key infrastructure, secret keys, mutually trusted certification authorities, delays, and channel confirmation focusing to solving the problem of trust management.

IoT in Aviation

In the previous sections it was made apparent that the IoT can find rich ground in both consumer and industrial applications. Retaining the focus on Industrial IoT and automation applications we consider that the IoT can provide solutions for more effective control and monitoring of processes running in the aviation field. Various protocols can be used to define ways to communication between operation, maintenance, diagnosis or even flight control machines.

At the same time, the technologies used in sensors are appearing improved, thus reducing their size and cost while enable the development of a range of practical applications in the field.

Additionally, the sensors can provide data in addition to the measurements, such as condition in which they are located, which allows the settings to be adjusted or to diagnose possible problems. At the same time, the existence of an internet connection enables the creation of data streams, which can be stored and processed in the backend computing infrastructure.

Under this regime, an aviation company now has at its disposal a large volume of new data types for analysis and optimization of the procedures it implements. Finally, IoT requires the existence of modern safeguards to prevent unwanted access to data and devices from attacking users. Also, from the point of view chosen by adoption of the IoT is vital, as it allows the saving significant financial resources from further automation and the acceleration of production, while at the same time significantly reducing the potential problems.

'Smart Aviation' is a new paradigm which combines the state-of-the-art technologies of Internet of Things, Machine Learning/Artificial Intelligence, and Big Data. This new paradigm focuses to the adoption of the technologies to the manufacturing, maintenance, and diagnosis operations in the aviation field. Additionally, robotics bring automation, precision and flexibility to using new tools such as 3D printing, and augmented reality in respect to safety regulations (Raju et al, 2019). Furthermore, "Smart Aviation" seeks to achieve unification of the ICT and IoT components in a common information system. The merit of a unified system is real-time analysis of data, reactive and proactive controls to production, maintenance, and supply chain-related plans.

In the case of the aviation supply chain, the aircrafts are treated as cyber physical systems whose components, engines, cabins, and others are fitted with IoT capabilities (i.e., sensing, transmitting and sometimes self-healing functions) which monitor in real time the status of the aircraft and alert for repair issues and maintenance needs (Zhang 2014).The sensor data provide useful information to technical teams regarding assembling or repairing steps that the technicians need to plan ahead or follow urgently. Due to the complexity of these processes, it may not be feasible to increase the automation or robotics utilization, hence they may need to be done manually. Therefore "Smart Aviation" focuses in supporting technical teams with providing them the right information and the right tools at the right time. The technical teams and tools are interconnected with the IoT components to streamline assembly and maintenance processes efficiently and precisely.

For example, an assembly task requires a stock of more than 300,000 bolts and screws, using more than 1000 tools (Karakuş et al, 2019). The IoT components guide the assembly process throughout the field identifying, for instance, the size of a bolt needed in a particular hole to a specific part of the plane. This information is communicated to a tool (automated or semi-automated) to apply the required rotation force.

The IoT network maintains an inventory of the available equipment which is updated in real time regarding its allocation and actual location on the floor. The task data are communicated to the backend ERP system having a global view of the tool, technical teams' allocation in a safety and security context. Frequently re-occurring audits and quality checks emphasize to the following policy statements:

- Only trained and authorized technicians are allowed to perform a step X at floor area Y.
- Aircraft X must be on floor X at date time Y for a duration Z to perform preventive maintenance plan P.
- Key performance indexes of the aircraft which are monitored in real time must be communicated to authorized operators.

In this way, the maintenance procedures seek to optimize the aircraft on ground (AOG) time and other related cost factors without degrading the quality of maintenance and keeping the airline's reputation to high standards (Wang et al, 2013).

Increased fuel efficiency

Monitoring data regarding the engine performance, predictive maintenance guided by IoT can result in fuel efficiency. An engine equipped with sensors that monitor performance metrics facilitate a precise monitoring of the engine performance. Then big data analytics predict and adjust the levels of fuel consumption to achieve further tuning (Chung et al 2020).

Evolution of the value chain

For the aviation industry the flexibility and efficiency which can be achieved due to higher adoption of the IoT technologies lead to further evolution of the value chain, with new innovations and value-added services. The interconnected ICT and IoT components is one of these innovations in the value chain of smart aviation with emphasis to cost reduction, precise manufacturing and maintenance plans, less labor intensive tasks under the umbrella of safety regulations and security defense.

Smart Aviation

Aviation organizations which are responsible for the maintenance, operations, manufacturing, and other aviation-related application domains offer relevant systems and devices necessary for their daily use and therefore must be protected. Smart aviation systems are interconnecting traditional aviation operations and digital services offering smart connection and autonomous decision-making features. These systems and devices include, for example, authentication and identification services, portals for mobile users and operators, and interconnected aviation information systems. The specific assets of smart aviation are presented in more detail in this section.

The elements of a remote diagnosis and maintenance system define a range of Information and Communication Technologies (ICT) technologies that allow the smart aviation to expand its boundaries and provide diagnosis and maintenance services to aircrafts in remote locations:

- IoT equipment for tele-monitoring and tele-diagnosis which send alerts if the values exceed certain control limits.
- IoT equipment for automatically fixing a fault or configuring an aircraft part
- Remote diagnosis equipment, such as cameras, sensors with internet connectivity, electronic system for technicians on the maintenance field to enter their measurements themselves

Identification systems

They aim to tracking and verifying the identity of aircrafts, parts, maintenance equipment and personnel. Identification can be established with smart systems such as biometric scanners, smart IP cameras or voice control authenticating personnel before entering specific floor areas (Liu et al, 2021). Other examples include:

- RFID labels, bracelets, tags and badges
- RFID-based positioning components for tracking the movement of tools, parts, personnel in the floor area.
- IPTV devices with motion detection, face, and object recognition capabilities

The unified ICT-IoT network plays significant role to implementing the digital universe of the smart aviation paradigm (Budakoti et al, 2018), e.g.

- Physical communication protocols (e.g. wifi, ethernet, ZigBee/Bluetooth, RFID, etc.)
- Network transmission components (e.g. network interface cards, wireless shields)
- edge network devices (e.g. IoT edge nodes, network switches, etc.)

End-user mobile devices (e.g. maintenance equipment, laptops, tablets, smartphones) are integrated into the smart aviation ecosystem for a range of applications which have to be done by mobile operators. Also, diagnosis and maintenance devices are also integrated to provide diagnosis, preventive maintenance and repair procedures. To this end, the accumulated data by all processes is a valuable input not only for decision making but also for the security defense. Examples include (Edward et al, 2017):

- Diagnosis and administrative aviation data (e.g. repair history)
- Financial, and organizational data
- Maintenance data (e.g. stress test reports)
- Staff allocation data
- Monitoring of recordings
- Supply chain data (e.g. which parts were used by which supplier).

Facility management systems equipped with intelligent processes are critical to the operation of the aviation operations. Some critical aviation safety related controls and their functions include (Wang et al, 2013):

- Control systems, including intelligent power, air conditioning, ventilation, supply chain systems
- Replacement or maintenance sensors
- Smart features and maintenance management systems, including smart signs, monitoring displays
- Automated door locking systems and applications.

Smart Aviation Vulnerabilities

In this section we describe in detail the most common vulnerabilities to be considered by smart aviation systems. The list consists of vulnerabilities related to technical, organizational, and social aspects. Attackers will seek to exploit these vulnerabilities associated with systemic data and people in the ICT sector, especially vulnerable groups (e.g. secretarial staff and senior management) who procure, manage and operate ICT systems and devices (Fiaidhi and Mohammed, 2019).

A major challenge in smart aviation is that the aircraft's data are considered even more valuable information to intruders than even financial data. Hence, the security defense must minimize the existence of vulnerability areas especially in connection to IoT. Despite the low cost and special capabilities of IoT components their selection must consider that they will not put at risk human life. The price of protecting the maintenance staff's lives is inferior to the cost of system components. On the other hand, significant vulnerabilities or attacks (e.g. ransomware) may trigger malicious actions whose impact to human lives or system operations may be disastrous.

In many cases, IoT or other aviation devices were designed without an interconnection orientation. Communication gaps between IoT and core aviation devices can provide the attack surface that malicious attackers need to obtain access to systems and perform lateral movements for further data breaches (Malik and Singh, 2019). IoT devices are scattered throughout the aviation (sensors, biometric scanners, IP cameras and RFID readers) and their physical defense across the field is not feasible. Perimeter controls minimize the risks but following a defense-in-depth principle more security controls are required.

The design of diagnosis and repair devices does not include the description of threats. The devices are made according to the specifications for their "intended use". Third party breach and other network-related accidents are "unintentional" cases of systemic vulnerabilities and risks throughout the aviation environment. It is not possible to mitigate all the vulnerabilities for all the devices due to their massive development. Attackers are exploring new attack paths as the IoT protocols and technologies proliferate. Especially for diagnosis and repair devices, their shelf life is a very important disadvantage that must be considered. Aviation organizations may not change equipment every X number of years and their technologies may soon or later be outdated. Similarly, the replacement lifecycle of IoT devices is short.

Especially the operating systems and applications of IoT systems do not embed strong threat detection and prevention capabilities. This is due to their limited processing units which allows them to perform sensing and transmission of data without any further security control (e.g. authentication or encryption). The IoT manufacturers may not always cope with latest vulnerabilities and time to market may enforce them not to consider further protection measures for human life. Furthermore, their initial design may not consider further parameters to the domain of their use, e.g. how they contribute to the security or the well-functioning of aircrafts.

The aviation operator has no further insight about the device protocols and the exact data streams which are created. In the case of aviation devices, the maintenance staff, the IT staff, and the administration team have little or no idea of their characteristics. Risk management decisions that may have been made by the IoT manufacturer are not disclosed in any material way to the aviation equipment user or system designer. Hence it is difficult for the security officers to understand potential threats and therefore take timely action to address the issue.

The lack of threat detection and alerting capabilities can lead to a breach of security that remains for a long time undetected and non-mitigated. Without further network security measures, the interconnection with ICT networks or aviation devices forms a bridge for the spread of the malicious programs in aviation centers. In aviation this may lead to further risks related to aircraft safety.

Lack of access control in the aviation environment can cause unauthorized users to access a critical system through an end device. The above may relate to the authorization of staff handling controls. The lack of vigilance or security awareness processes from a cyber security perspective makes staff members to bypass security measures, policies and procedures, if they find them annoying or time consuming in the diagnosis flow. The lack of a policy on the use of personal devices in a smart aviation environment can have serious implications to cyber security. The security teams should be aware of any device used in the field and sufficient time should be allowed for the appropriate testing of any new device before it is introduced to the maintenance procedures.

Many IoT devices which are deployed in aviation field do not conform to security standards. Particularly regarding the introduction of IoT into the ICT environment of the aviation organization, the degree of penetration of new devices can often exceed the ability of the ICT security department to follow the appropriate systems / device management procedures. From an organizational point of view, user behavior is very important, which is especially important in the case of aviation. The primary goal is aircraft safety and technical staff make all the decisions needed on the spot to achieve this goal. Often this means that rough, improvised solutions can be followed. In a smart environment, where a security check is difficult to implement due to the natural dispersion of the environment, any improvised solutions that endanger the level of security should not be accepted. These solutions are often not well documented or extensively tested and are a key vulnerability.

Due to diagnosis or maintenance needs or lack of proper management procedures for any system settings, the settings of the systems or devices may not conform to industry standards. This results to setup of an infrastructure of no unified point of reference. Additionally, devices and network may be exposed to certain security vulnerabilities which will be difficult or will delay the implementation of mitigation actions if ever needed.

All the above vulnerabilities generally involve technical aspects related to Information / Communication Technologies (ICT) and devices. Clearly some of the vulnerabilities are more relevant to some systems / devices than others. For example, vulnerabilities associated with lack of proper security controls or non-compliant systems are more referring to networked aviation devices or end-users without excluding facility management systems (power, air conditioning or door locking systems) (Zhang, 2014).

Smart Aviation Vulnerabilities Taxonomy

Natural disasters	**Supply chain errors**	**Malicious actions**
• Fire • Flood • Earthquake	• Errors in cloud computing services • Errors in network services • Power outage • Error on diagnosis device	• Malware (virus, ransomware) • Invasion (in transaction, in the network, in diagnosis devices) • Social engineering (phishing, RFID device cloning) • Theft (devices, data) • Spying on data from a diagnosis device • Scan systems on the network • Denial of Service (DoS)
Human Errors	**System Errors**	
• Errors in diagnosis device settings • Loss of records	• Software bugs • Insufficient firmware • Device error (or inadequate device capabilities) • Error in parts of the network	

- Unauthorized access / lack of control procedures - Non-compliance with standards - Mistakes of technical staff	- Insufficient maintenance - Overload - Communication between IoT and non-IoT systems

Taxonomy of the threats to a Smart Aviation Center

1. Malicious actions

Malicious actions are intentional acts by an individual or an organization. Different types of malware include viruses, worms, trojans, ransomware, spyware, adware, rootkits, etc. This type of software aims to either harm the victim's system by intercepting or destroying sensitive data, by either monitoring the user's actions, or even taking control of the system. The methods by which an ICT or IoT host can be infected come in many forms, but in the end, they always require the user to take some action, such as running and installing software. This can be done by downloading an "innocent" attachment, as well as running an add-on suggested by an infected website. Regarding the different types of malware which are applicable to smart aviation, below is a brief description of its main forms.

- Virus: Software, which is hidden inside another, harmless by making copies of itself. These copies are transmitted, distributed, and embedded in other software, networked from one computer to another. The goal is the malfunction of the systems and the destruction of the data.
- Worm: It has a similar logic to the virus as it also makes copies of itself and has as its main goal to hit systems and destroy data. The difference is that they are standalone and do not require any other software. The spread is done by exploiting possible vulnerabilities of the system, so the user falls into their execution trap.

- Trojan: Its format is such that it convinces the user that it is useful for him to proceed with its installation. It does not aim to spread and infect other files, such as a virus. Its purpose is to intercept and delete files, as well as delete vulnerabilities in the systems.
- Ransomware: Software that encrypts user data, preventing access to it, and then requires a fee to decrypt and retrieve it. The way it is transmitted is either through phishing emails or through websites that contain malicious code.
- Rootkit: A software package that helps when a system is infected by malware. It can allow malware to remain undetectable in controls because it is located too close to the system kernel. Its purpose is to install the necessary tools, which will enable the malicious user to gain remote access to his victim's system in the future.
- Backdoor: It is a tactic followed in the development of software systems and allows remote access to it, by its creators, to perform troubleshooting procedures, upgrades, and controls. These access paths can be turned into vulnerabilities and target the malicious user, who can detect them using a worm or trojan. Thus, by having them, it bypasses the authentication processes of the system and has access to it.

In general, malware is a major threat to smart aviation centers, however we should discriminate malicious activity from other actions done on purpose to bypass policies and procedures but without malicious intent. A malicious actor may be a team member or an outside agent. The so-called malware has the feature that it can attack many organisms with low effort. Especially ransomware programs are considered a major threat to aviation organizations.

2. Human errors

Human errors occur during the execution of maintenance, diagnosis or repair tasks using the networked aviation equipment. This can be due to an inadvertent action, labor consuming task, lack of sufficient knowledge or training. Examples of human errors include:

- Errors setting up an aviation system that could compromise system operation or expose the system to a cyber threat.
- Absence or loss of records to allow proper control and event detection and evaluation of remedial / remedial actions
- Unauthorized access or lack of access procedures are significant risks for smart aviation fields, as they handle sensitive aircraft data and the fact that maintenance procedures involve highly specialized roles in a variety of fields.
- Non-compliance with various policies and standards. This is especially important for IoT-based smart aviation components which are deployed with no further testing.
- The potential errors of technical staff or vendors may cause threats to the safety of the aviation systems and objects (e.g. aircrafts or parts) where there is a high reliance on IT technology. For example, such errors may be due to fatigue and poor concentration due to workload or the implementation of rough, improvised solutions due to other policies and procedures that are considered too painful or time consuming (and therefore hinder the aircraft maintenance process).

Also phishing attacks is a tactic used by emails, according to which the message contains the details of a sender that the user would trust, such as a business associate. The message is in the form of a legitimate email and includes an attachment or link. This achieves the installation of the malware when the user opens the file, or in the other case, the link leads to a fake website (same in appearance of that business associate) where the goal is to intercept the user's credentials or other information.

A basic category of Phishing is Deceptive Phishing which uses emails, has a general character and invites its victim to confirm his credentials, following a link contained in the message. Spear Phishing is a targeted implementation, which targets specific people in a company, using the name, location, contact information and any other information will convince the victim of the authenticity of the message. It is often the first step in the process of bypassing the defense of a corporate target.

3. System level errors

System-level errors are extremely important in aviation and are associated to the complexity of some of the processes. Examples of this include:

- Software weaknesses affecting or interrupting a maintenance or administrative process
- Insufficient hardware and software that can be especially important for the number of connected aviation devices in a smart aviation field
- The failure of the device or simply its limited / reduced capacity can seriously affect the procedures based, e.g. in real-time aircraft data collection.
- A network-level error can have a major impact on the operation of a network of IoT devices.
- Inadequate maintenance can cause incalculable and unresolved operational problems, both in terms of cybersecurity and aircraft maintenance functions.
- Overload can cause resource exhaustion.
- Network communication errors.

4. Errors of third parties

As smart aviation fields become highly dependent on third parties, their failures may have impact to the supply chain of the aviation procedures. Examples of third parties whose failures that would adversely affect the operation of smart aviation systems include:

- Cloud service providers that host important data regarding aviation applications, etc.
- Manufacturers of maintenance and repair devices
- Network or internet service providers
- Energy suppliers.

5. Natural phenomena

Natural phenomena (earthquakes, floods, fires) may have catastrophic effects, especially on intelligent aviation diagnosis and repair facilities and overall infrastructure (especially if no Disaster Recovery sites are not available). They may affect the continuation of the aviation services for a long time.

Attack profile

Starting with the identity of the attackers, it is easier to understand their motives and goals. Attackers can be cybercriminals seeking profit by cheating users, hackers seeking pleasure by launching attacks on foreign computers, foreign intelligence services seeking to obtain information mainly in the military and economic sectors, companies seeking to gain a competitive advantage over their competitors and the last category of attackers are hacktivists driven mainly by political motives and ideology.

Attackers can use tools that are already available on the Internet and are simpler techniques to use and operate. These tools were originally designed to be used by security technicians and their main function is to detect vulnerabilities and vulnerabilities in systems and applications software. This is the point that attackers take advantage of using these points, but not to correct them but to enhance them and gain access to data.

The most experienced attackers use tools and techniques that are developed and used for specific purposes and for this requires specialized knowledge. The difficulty with dealing with these types of software lies in the fact that because they are created by attackers from the beginning, they are not known by antivirus software companies, making it easier for attackers to infect more and more computers with their software until they are dealt with.

The attackers mainly exploit the characteristics of cyberspace and its weaknesses. Anonymity as well as insufficient internet security are the first qualities that allow attackers to attack. Also, various errors in the design of various software allow them to take advantage of vulnerabilities that may arise from them and carry out their attacks. Unlike bugs that are unintentional functions in a system, attackers can also take advantage of software features that were originally created by the developers to improve the user experience and troubleshoot issues that may arise. However, even if a system does not have any of the above that can be helpful tools for the attacker, there is a case of error to which the user will fall. A well-designed and carefully implemented system can minimize the vulnerabilities arising from its exposure to the Internet. However, an inexperienced user who does not manage the software properly can cause vulnerabilities. In general, user behavior plays a major role, as they can be a source of vulnerabilities. Even experienced users can fall into well-established traps by giving personal data or passwords to hackers who will use them for fraud.

The intentions of the attackers are inextricably linked to their identity and purpose. Espionage is a key target of attacking individuals or states. Every day, huge amounts of data are stolen from various networks. Espionage is one of the main targets of attackers, especially the State Intelligence Service, as it can provide the state with useful information for other states both strategically and economically. Espionage is also used to monitor other countries' armies and how they operate and organize. Another use for espionage can be found in technology. In today's era, which is characterized as the age of technology, it is logical that technological superiority brings multiple benefits to companies and states. Whenever the theft of technological advances and their patents or drafts is a common practice applied by governments and companies.

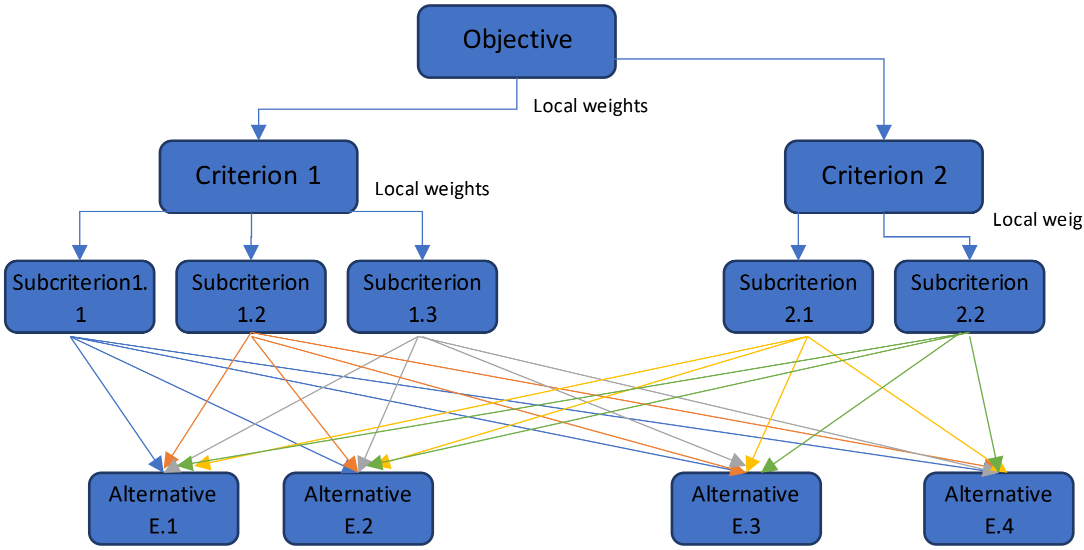
Stealing and copying them can bring new dynamics to the operation and organization of a state, as well as military superiority over states, while in a business it can bring a competitive advantage over its competitors, resulting in its profit and survival of a business in the market. Propaganda is another purpose of cyber-attacks. Usually coming from other countries or from internal opponents of the government, it aims to spread false or untrue information to manipulate the public. In addition, attackers often modify the data of their targets to deceive them. This practice can result in either propaganda or the malfunctioning of the systems on which the services of a state or a company are based. In its most extreme form this method can be used to distort the data into sophisticated weapons.

Finally, many attackers aim to gain control of the infrastructure. Power outages or other similar infrastructure interruptions or distortions can cause major damage to both equipment and software.

AHP Methodology

Decisions that require support methods are difficult and therefore require complex models to solve them (Ishizaka & Labib, 2009). Therefore, it is necessary to compensate between the perfect modeling and the usability of the model. The Analytical Hierarchy Methodology (AHP) is one method that covers these assumptions (Ishizaka & Labib, 2011).

The AHP methodology was first introduced by Thomas Saaty (1977) as an effective tool for complex decision making. The process begins by describing the problem in a hierarchical structure that includes at the highest level an overall (quantifiable) goal, which is further decomposed into criteria and subcriteria, while at the lower level of the hierarchy alternatives are set to achieve the goal. This approach is applied in cases where decision-makers and experts are available. Therefore, decision makers are the ones who set the goal and distinguish the alternatives for achieving it, while the experts are called to evaluate the alternatives based on specific criteria (Rezaei & Ortt, 2013). The structure of a typical problem during the application of the AHP method is shown below.



Analytical Hierarchy Methodology

The structure of the method starts by breaking the problem into smaller pieces and then uses binary comparisons to determine the priorities in each hierarchy. AHP is essentially based on three principles: decomposition, relative comparisons, and prioritization (Saaty, 1986). These three principles must first be fully understood:

- Decomposition: According to the principle of decomposition, to construct a hierarchy, which is a key component of the method, the basic elements of the problem must be identified. To locate these elements, it is necessary to decompose the problem into levels in the form of a tree. At the first level of the tree is the final goal - decision. It is followed by the basic criteria that influence the decision at the second level, their sub-criteria at the third and continues in a similar way. Each level, then, is the decomposition of exactly the previous one. In this way, the problem is broken down into individual parts: general concepts, which are uncertain, become more specific and clearer. At the last level of the tree are listed the alternative decisions.
- Relevant comparisons: The pairwise comparisons that follow the decomposition of the problem, quantify the importance of each criterion (or sub-criterion) at the respective level in relation to each element that is connected to the exact higher level. These comparisons give rise to preference tables, which then provide an estimate of the relative weights for each criterion (or subcriteria) and for each alternative.
- Priority synthesis: The relative weights calculated through the preference tables indicate the synthesis of the priorities, which then leads to the construction of the hierarchy.

The solution of decision-making problems in recent decades is now addressed through the systems approach, mainly for problems related to the social sciences. Essentially, a system is designed to solve each problem, which reflects a microcosm. Through the system that is designed, the impact of the various components of the system for the whole system is evaluated and their priorities are identified.

Hierarchy is a special type of system, which assumes that the identified entities can be grouped into discontinuous sets, with the entities of one group affecting only one other group and being influenced by only one other group, respectively. The elements in each group - level of the hierarchy are assumed to be independent (In cases where there is a dependence between the levels of the hierarchy, those in which there is a dependency are examined separately and the independent ones. Then they are combined.

After structuring the problem, the next step in the AHP process is to calculate the weights for the various proposed criteria. This process is performed through pairwise comparison tables, which are constructed to assess how the proposed criteria contribute to the overall goal, starting from the first level of criteria and continuing to the lower levels, comparing criteria of the same level. Each table A is a real table n x n where n is the number of evaluation criteria taken into account. The data in table (aij) represent the importance of criterion i in relation to criterion j, while meeting the following limitations:

$$a_{ij} = \frac{1}{a_{ji}}\ where\ i \neq j \neq 0\ and\ a_{ii} = 1$$

Based on the above, the pairwise comparison tables are as follows:

$$A = a_{ij=}\begin{array}{cc} Criteria & \begin{array}{cccc} C_1 & C_2 & \cdots & C_n \end{array} \\ \begin{array}{c} C_1 \\ C_2 \\ \vdots \\ C_n \end{array} & \begin{pmatrix} 1 & a_{12} & \cdots & a_{1n} \\ {}^{1}/_{a_{12}} & 1 & \cdots & a_{2n} \\ \vdots & \ddots & \ddots & \vdots \\ {}^{1}/_{a_{1n}} & {}^{1}/_{a_{2n}} & \cdots & 1 \end{pmatrix} \end{array}$$

- For aij> 1, the criterion i is considered more important than criterion j
- For aij< 1, the criterion i is considered less important than criterion j
- For aij = 1, the criterion i is considered equal to criterion j

Decision makers then evaluate the criteria for their relevance. Saaty (1977) suggested the use of the numerical scale from 1 to 9 to assess the relative importance between two criteria as shown in the table below.

Intensity of Relative Significance	**Definition**	**Description**
1	Equally preferable	Two elements contribute equally to the goal
3	Slightly preferred	Experience and judgment favor one element over the other
5	Moderately preferred	Experience and judgment favor each other significantly
7	Highly preferred	One element is strongly favored, and its dominance is manifested in practice
9	Absolutely preferable	The reasons that favor one element over another are of the highest degree of confirmation
2,4,6,8	Intermediate values	When a compromise is required

Table 1. Fundamental scale of absolute numbers proposed by Thomas Saaty (1985)

After creating the pairwise comparison tables, it is possible to calculate the vector of the weight coefficient of the criteria $\widehat{w} = (w_1, w_2, w_3, \dots, w_n)^T$ by applying a mathematical procedure, such as for example the calculation of the eigenvector (Egi) of the table A (Saaty & Hu, 1998), the use of the least squares method (Chu, Kalaba, & Spingarn, 1979) or a fuzzy logic programming method (Mikhailov, 2000). The resulting vector of gravity must meet the requirement:

$$\sum_{i=1}^{n} w_i = 1$$

In the case where more than one level is involved, this method leads to the calculation of local priorities (wi). The final total priority coefficients $\widehat{w_i}$) against which the alternatives should be evaluated are taken into account at the lowest level of the individual criteria for all groups of basic criteria, multiplying successively by the local priorities. Based on the final score, i.e. the result of a weighted average, the alternatives are classified according to their ability to achieve the set goal.

Consistency

When many comparisons are made in pairs, inconsistencies may arise in the answers of the experts. AHP allows control of the consistency of paired comparisons and acts as a feedback mechanism for decision makers to reconsider and review their choices (Saaty, 1977). This integrated function of verifying the results is the main reason for differentiating this method from the others used in decision making (Govindan et al 2015). To determine the consistency of the answers, Saaty proposed the Consistency Index (CI), which is related to the method of the eigenvector applied in Table A, and is given by the relation:

$$CI = \frac{\lambda_{max} - n}{n - 1}$$

where n is the dimension of table A, and λmax the maximum eigenvalue.

If CI / RI <0.1, the pairwise comparison table is characterized by an acceptable level of coherence. RI is a random index (mean of CIs derived from 500 randomly completed tables), whose values are predetermined by Saaty (Saaty, 2001), for problems with n ≤ 10 as indicated in the following table.

n	1	2	3	4	5	6	7	8	9	10
RI	0	0	0.52	0.89	1.11	1.25	1.35	1.40	1.45	1.49

Random Index (RI) Values (Saaty, 2001)

Applications of AHP

The hierarchical process was used by IBM as part of a quality improvement strategy for the design of the AS / 400 computer and won the prestigious Malcolm Baldrige National Quality Award.

In 1986, the Institute for Strategic and Defense Studies in Pretoria, a government agency, used the AHP method to analyze instability and conflict in South Africa and propose actions to alleviate the situation. The actions proposed through the analysis ranged from the release of Nelson Mandela, the abolition of apartheid to the granting of equal rights to the colored majority.

In 1987 a company used AHP to select the type of platform it would build for oil extraction in the North Atlantic. The cost of the platform was $ 3 billion to build, but the cost of demolishing it was an even more important factor in the decision.

The method was applied in the 1995 US-China intellectual property dispute over the pirated copying and marketing of music, movies, and software. The AHP analysis, which included three hierarchies of benefits, costs, and risk, showed that it would be best for the US not to impose sanctions on China. Shortly after the study was completed, the United States named China the preferred trading country. Also, British Airways in 1998 used the method to select the entertainment system that would be provided for their entire fleet.

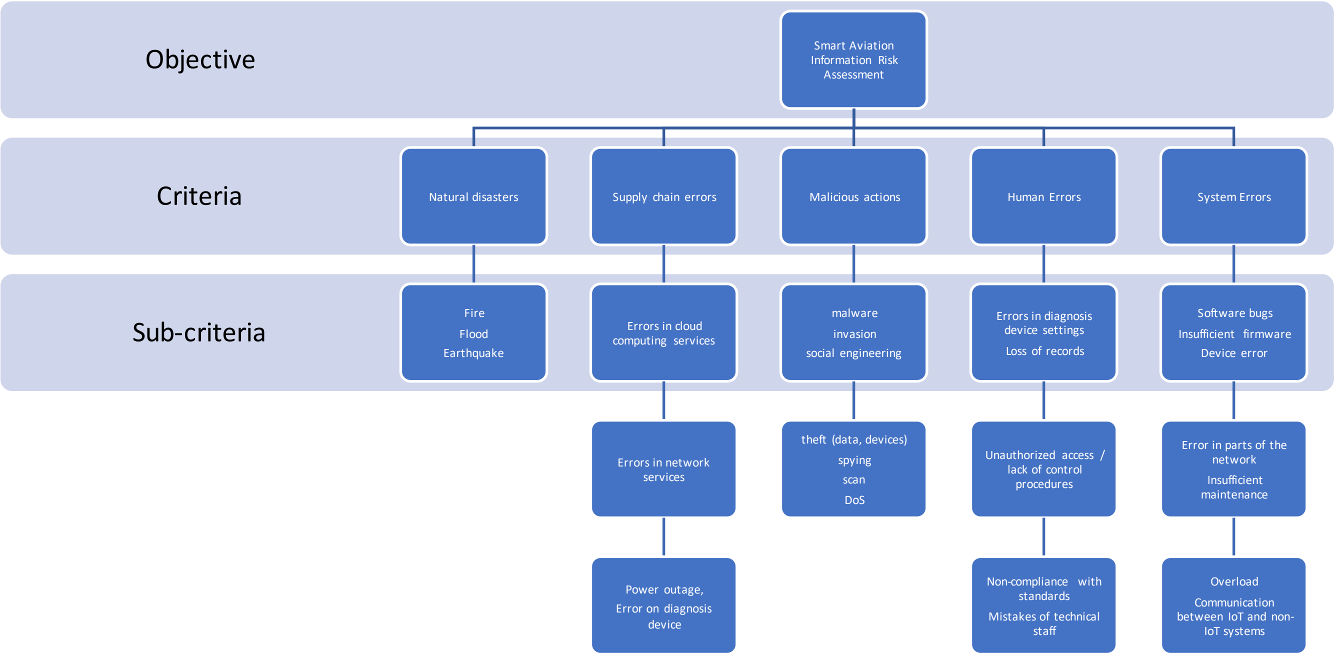
Xerox applied AHP in 1999 to a decision to award close to $ 1 billion to a research project. That same year, Ford used the method to set priorities for criteria that improve customer satisfaction. Ford then awarded Expert Choice Inc.2 for its efficiency and assistance in achieving greater customer satisfaction. In 2001 the method was used to determine the ideal location for the resettlement of the Turkish city of Adapazari, which was destroyed by a strong earthquake.

AHP has been widely used in staff selection problems, staff appraisals and the selection of those to be promoted to senior positions, as well as for the selection of students admitted to various educational institutions. In addition, it has been widely used in the field of sports, e.g. in Baseball, a sport particularly popular in the US, has been used to analyze which of a team's players should be retained for next year. The AHP has also been applied to many military issues and various government programs. Of particular interest is the widespread use of the method in China, where it is often used in the construction industry in various decisions such as determining the best orientation of a building or a bridge.

Case study: Aviation 4.0

Risk Assessment in Smart Aviation based on the AHP methodology

Following the AHP methodology we can determine the weight of various information security threats in Smart Aviation: these will be in the form of assessment criteria and sub-criteria. Using the taxonomy of vulnerabilities that established before, we define five main criteria: Natural disasters, Supply chain errors, Malicious actions, Human Errors, System Errors. The hierarchy of the associated sub-criteria is presented to the following figure:


Objective
Smart Aviation Information Risk Assessment
Criteria
Natural disasters
Supply chain errors
Malicious actions
Human Errors
System Errors
Sub-criteria
Fire
Flood
Earthquake
Errors in cloud computing services
malware
invasion
social engineering
Errors in diagnosis device settings
Loss of records
Software bugs
Insufficient firmware
Device error
Errors in network services
theft (data, devices)
spying
scan
DoS
Unauthorized access / lack of control procedures
Error in parts of the network
Insufficient maintenance
Power outage,
Error on diagnosis device
Non-compliance with standards
Mistakes of technical staff
Overload
Communication between IoT and non-IoT systems

Hierarchical model of the Information Risk Assessment problem

Step 1: collect user data to an AHP-formatted questionnaire

The first step is to fill in an Excel sheet with data from questionnaires which are collected from a set of users who participate in a survey. The data correspond to the parameters of a decision problem about the main threats in Smart aviation. We consider three (3) evaluators which we name them: A, B, C and who participate in the decision making. These are the security officers (CISO) of three alternative Smart Aviation Sites. Hence, they are fully aware of the cybersecurity status of the aviation sites respectively.

The criteria are the Natural disasters, supply chain errors, malicious actions, human errors and system errors as shown above. Each of the criteria is divided into sub-criteria. Three Smart Aviation sites are evaluated using all criteria and subcriteria. The solutions to the problem are called alternatives. The data is grouped in a table as follows:

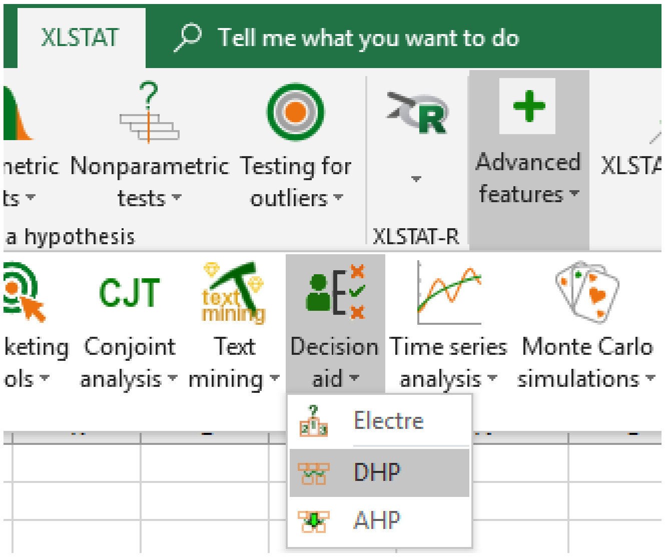
Criteria	**Natural disasters**	**Supply chain errors**	**Malicious actions**	**Human errors**	**System errors**	**Alternatives**	**Eval**
Natural disasters	Fire	Errors in Cloud Computing services	malware	Errors in diagnosis device settings	Software bugs	Site1	A
Supply chain errors	Flood	Errors in Network services	invasion	Loss of records	Insufficient firmware	Site2	B
Malicious actions	Earthquake	Power outage	social engineering	Unauthorized access	Device error	Site3	C
Human errors		Errors on diagnosis services	theft (data, services)	Lack of control procedures	Error in parts of the network		
System Errors			spying	Non-compliance with standards	Insufficient maintenance		

			scan	Mistakes of technical staff	Overload		
			DoS		Communication between IoT and non-IoT systems		

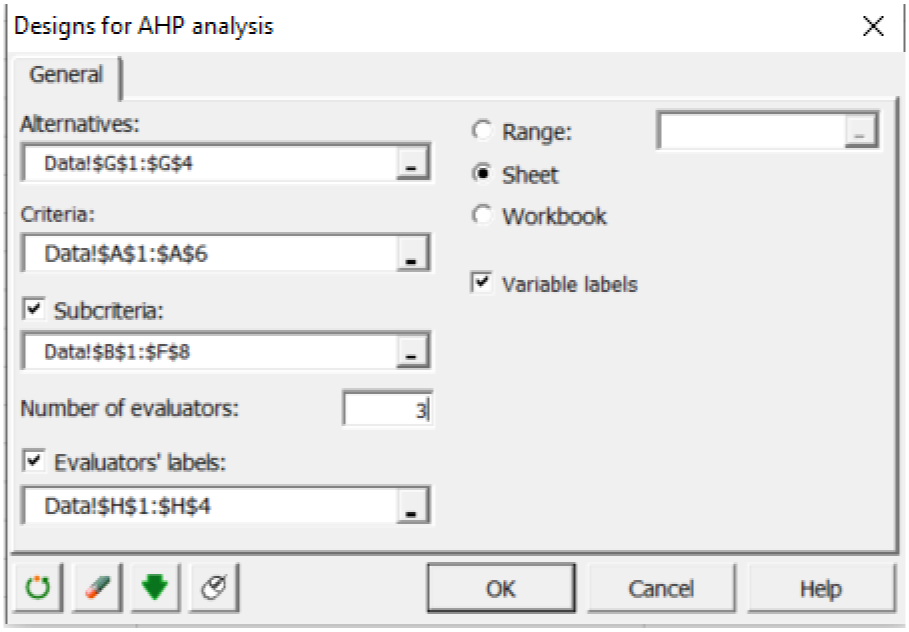
Based on the evaluators' feedback, the goal of this case study is to perform an evaluation of which Smart Aviation site has the less risks.

Step 2: Generate the AHP design

The second step is to generate a design of experiment with a Design for AHP (DHP)template. For this purpose, we use the excel plugin XLSTAT and we click on the excel menu XLSTAT / Advanced features / Decision aid / DHP:



The dialog box Designs for AHP analysis appears.



Alternatives: Data!$G$1:$G$4

Criteria: Data!$A$1:$A$6

☑ Subcriteria: Data!$B$1:$F$8

Number of evaluators: 3

☑ Evaluators' labels: Data!$H$1:$H$4

○ Range:

● Sheet

○ Workbook

☑ Variable labels

In the General tab, we select the list of the Aviation sites in the Alternatives field. Then select the column that contains the criteria in the field with the same name, the 5 subcriteria columns in the respective field and finally the column that contains in the field Evaluators labels.

After clicking the OK button, the design of the experiment is generated and displayed in a new sheet named AHP design. The data summary table, the Saaty table and the instructions for filling in the comparison tables of the design are displayed in the output sheet.

The Saaty table provides the values to be used by the 3 evaluators in order to fill in the comparison tables. Below is an example of filling in the criteria comparison table by the evaluator A.

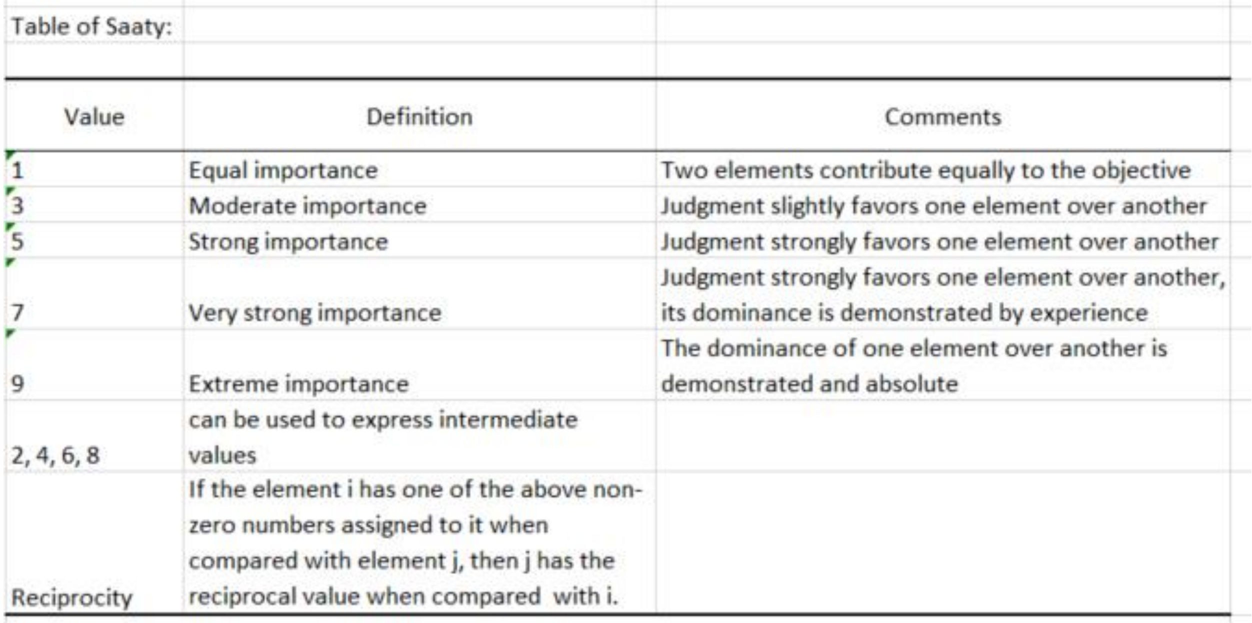


Table of Saaty:

Value	Definition	Comments
1	Equal importance	Two elements contribute equally to the objective
3	Moderate importance	Judgment slightly favors one element over another
5	Strong importance	Judgment strongly favors one element over another
7	Very strong importance	Judgment strongly favors one element over another, its dominance is demonstrated by experience
9	Extreme importance	The dominance of one element over another is demonstrated and absolute
2, 4, 6, 8	can be used to express intermediate values	
Reciprocity	If the element i has one of the above non-zero numbers assigned to it when compared with element j, then j has the reciprocal value when compared with i.	

Step 3: define the comparison matrices per evaluator

Use the Saaty table values we evaluate the set of comparison matrices per evaluator below. A value x of Saaty on the line i and the column j of a matrix means that the element i has an importance of the value x over the element j. On the contrary, the element of line j and column i has a value of 1/only cells above the diagonal must be entered.

Comparative matrices of evaluator A:

Evaluator A defines preferences of element i over element j over the criteria:

Criteria	Natural disasters	Supply chain errors	Malicious actions	Human errors	System Errors
Natural disasters	1,00	7,00	7,00	9,00	3,00
Supply chain errors	0,14	1,00	3,00	5,00	7,00
Malicious actions	0,14	0,33	1,00	7,00	7,00
Human errors	0,11	0,20	0,14	1,00	3,00
System Errors	0,33	0,14	0,14	0,33	1,00

On subcriteria of criterion Natural disasters:

Subcriteria	Fire	Flood	Earthquake
Fire	1,00	2,00	0,50
Flood	0,50	1,00	0,50
Earthquake	2,00	2,00	1,00

On subcriteria of criterion Supply chain errors:

Subcriteria	Errors in Cloud Computing services	Errors in Network services	Power outage	Errors on diagnosis services
Errors in Cloud Computing services	1,00	1,00	0,30	7,00
Errors in Network services	1,00	1,00	0,30	7,00
Power outage	3,33	3,33	1,00	9,00
Errors on diagnosis services	0,14	0,14	0,11	1,00

On subcriteria of criterion Malicious actions:

Subcriteria	malware	invasion	social engineering	theft (data, services)	spying	scan	DoS
malware	1,00	0,30	3,00	0,10	0,10	7,00	3,00

invasion	3,33	1,00	5,00	0,30	0,20	7,00	3,00
social engineering	0,33	0,20	1,00	0,10	0,10	5,00	0,20
theft (data, services)	10,00	3,33	10,00	1,00	1,00	7,00	7,00
spying	10,00	5,00	10,00	1,00	1,00	9,00	9,00
scan	0,14	0,14	0,20	0,14	0,11	1,00	0,50
DoS	0,33	0,33	5,00	0,14	0,11	2,00	1,00

On subcriteria of criterion Human errors:

Subcriteria	Errors in diagnosis device settings	Loss of records	Unathorised access	Lack of control procedures	Non-compliance with standards	Mistakes of technical staff
Errors in diagnosis device settings	1,00	0,20	0,20	0,15	0,15	0,20
Loss of records	5,00	1,00	0,13	5,00	5,00	0,30
Unathorised access	5,00	7,69	1,00	7,00	5,00	3,00
Lack of control procedures	6,67	0,20	0,14	1,00	7,00	5,00
Non-compliance with standards	6,67	0,20	0,20	0,14	1,00	0,20
Mistakes of technical staff	5,00	3,33	0,33	0,20	5,00	1,00

On subcriteria of criterion System Errors:

Subcriteria	Software bugs	insufficient firmware	Device error	Error in parts of the network	Insufficient maintenance	Overload	Communication between IoT and non-IoT systems
Software bugs	1,00	7,00	1,00	3,00	5,00	3,00	3,00
insufficient firmware	0,14	1,00	1,00	3,00	7,00	5,00	3,00
Device error	1,00	1,00	1,00	5,00	3,00	5,00	7,00
Error in parts of the network	0,33	0,33	0,20	1,00	5,00	3,00	3,00
Insufficient maintenance	0,20	0,14	0,33	0,20	1,00	5,00	3,00
Overload	0,33	0,20	0,20	0,33	0,20	1,00	7,00
Communication between IoT and non-IoT systems	0,33	0,33	0,14	0,33	0,33	0,14	1,00

The alternatives of Evaluator A are depicted in Appendix A'.

Comparative matrices of evaluator B:

Evaluator B defines preferences of element i over element j over criteria:

Criteria	Natural disasters	Supply chain errors	Malicious actions	Human errors	System Errors
Natural disasters	1,00	9,00	9,00	9,00	9,00
	0,11	1,00	5,00	7,00	7,00
Supply chain errors	0,11	0,20	1,00	7,00	7,00
Malicious actions	0,11	0,14	0,14	1,00	5,00
Human errors	0,11	0,14	0,14	0,20	1,00
System Errors	1,00	9,00	9,00	9,00	9,00

On subcriteria of criterion Natural disasters:

Subcriteria	Fire	Flood	Earthquake
Fire	1,00	1,00	1,00
Flood	1,00	1,00	3,00
Earthquake	1,00	0,33	1,00

On subcriteria of criterion Supply chain errors:

Subcriteria	Errors in Cloud Computing services	Errors in Network services	Power outage	Errors on diagnosis services
Errors in Cloud Computing services	1,00	3,00	0,30	5,00
Errors in Network services	0,33	1,00	0,20	5,00
Power outage	3,33	5,00	1,00	9,00
Errors on diagnosis services	0,20	0,20	0,11	1,00

On subcriteria of criterion Malicious actions:

Subcriteria	malware	invasion	social engineering	theft (data, services)	spying	scan	DoS
malware	1,00	0,30	5,00	0,20	0,30	9,00	5,00
invasion	3,33	1,00	7,00	0,20	0,30	5,00	7,00
social engineering	0,20	0,14	1,00	0,20	0,20	7,00	0,30
theft (data, services)	5,00	5,00	5,00	1,00	1,00	9,00	9,00
spying	3,33	3,33	5,00	1,00	1,00	7,00	7,00
scan	0,11	0,20	0,14	0,11	0,14	1,00	0,30
DoS	0,20	0,14	3,33	0,11	0,14	3,33	1,00

On subcriteria of criterion Human errors:

Subcriteria	Errors in diagnosis device settings	Loss of records	Unathorised access	Lack of control procedures	Non-compliance with standards	Mistakes of technical staff

Errors in diagnosis device settings	1,00	0,30	0,20	0,50	0,70	0,50
Loss of records	3,33	1,00	3,00	5,00	3,00	3,00
Unathorised access	5,00	0,33	1,00	5,00	3,00	7,00
Lack of control procedures	2,00	0,20	0,20	1,00	0,50	0,50
Non-compliance with standards	1,43	0,33	0,33	2,00	1,00	5,00
Mistakes of technical staff	2,00	0,33	0,14	2,00	0,20	1,00

On subcriteria of criterion System Errors:

Subcriteria	Softwar e bugs	insufficie nt firmware	Devic e error	Error in parts of the network	Insufficien t maintenan ce	Overloa d	Commu nicatio n betwee n IoT and non-IoT system s
Software bugs	1,00	0,50	0,50	0,50	3,00	0,30	3,00
insufficient firmware	2,00	1,00	0,50	0,50	5,00	5,00	5,00
Device error	2,00	2,00	1,00	3,00	3,00	3,00	3,00

Error in parts of the network	2,00	2,00	0,33	1,00	0,50	0,30	5,00
Insufficient maintenance	0,33	0,20	0,33	2,00	1,00	0,50	3,00
Overload	3,33	0,20	0,33	3,33	2,00	1,00	5,00
Communication between IoT and non-IoT systems	0,33	0,20	0,33	0,20	0,33	0,20	1,00

The alternatives of Evaluator B are depicted in Appendix A'.

<u>Comparative matrices of evaluator C:</u>

Evaluator C defines preferences of element i over element j over criteria:

Criteria	Natural disasters	Supply chain errors	Malicious actions	Human errors	System Errors
Natural disasters	1,00	9,00	9,00	9,00	9,00
	0,11	1,00	7,00	7,00	7,00
Supply chain errors	0,11	0,14	1,00	3,00	3,00
Malicious actions	0,11	0,14	0,33	1,00	0,50
Human errors	0,11	0,14	0,33	2,00	1,00
System Errors	1,00	9,00	9,00	9,00	9,00

On subcriteria of criterion Natural disasters:

Subcriteria	Fire	Flood	Earthquake
Fire	1,00	5,00	5,00
Flood	0,20	1,00	5,00

Earthquake	0,20	0,20	1,00

On subcriteria of criterion Supply chain errors:

Subcriteria	Errors in Cloud Computing services	Errors in Network services	Power outage	Errors on diagnosis services
Errors in Cloud Computing services	1,00	3,00	0,20	5,00
Errors in Network services	0,33	1,00	0,20	5,00
Power outage	5,00	5,00	1,00	9,00
Errors on diagnosis services	0,20	0,20	0,11	1,00

On subcriteria of criterion Malicious actions:

Subcriteria	malware	invasion	social engineering	theft (data, services)	spying	scan	DoS
malware	1,00	0,30	5,00	0,30	0,30	5,00	3,00
invasion	3,33	1,00	3,00	0,30	0,50	7,00	5,00
social engineering	0,20	0,33	1,00	0,30	0,20	7,00	3,00
theft (data, services)	3,33	3,33	3,33	1,00	5,00	7,00	5,00
spying	3,33	2,00	5,00	0,20	1,00	7,00	5,00
scan	0,20	0,14	0,14	0,14	0,14	1,00	0,50
DoS	0,33	0,20	0,33	0,20	0,20	2,00	1,00

On subcriteria of criterion Human errors:

Subcriteria	Errors in diagnosis device settings	Loss of records	Unathorised access	Lack of control procedures	Non-compliance with standards	Mistakes of technical staff
Errors in diagnosis device settings	1,00	0,20	0,30	0,30	0,30	0,50
Loss of records	5,00	1,00	3,00	3,00	3,00	5,00
Unathorised access	3,33	0,33	1,00	3,00	3,00	5,00
Lack of control procedures	3,33	0,33	0,33	1,00	5,00	5,00
Non-compliance with standards	3,33	0,33	0,33	0,20	1,00	7,00
Mistakes of technical staff	2,00	0,20	0,20	0,20	0,14	1,00

On subcriteria of criterion System Errors:

Subcriteria	Software bugs	insufficient firmware	Device error	Error in parts of the network	Insufficient maintenance	Overload	Communication between IoT and non-IoT

							systems
Software bugs	1,00	0,30	0,50	0,50	3,00	0,50	0,50
insufficient firmware	3,33	1,00	1,00	3,00	3,00	3,00	3,00
Device error	2,00	1,00	1,00	1,00	3,00	5,00	5,00
Error in parts of the network	2,00	0,33	1,00	1,00	3,00	5,00	5,00
Insufficient maintenance	0,33	0,33	0,33	0,33	1,00	0,50	0,50
Overload	2,00	0,33	0,20	0,20	2,00	1,00	3,00
Communication between IoT and non-IoT systems	2,00	0,33	0,20	0,20	2,00	0,33	1,00

The alternatives of Evaluator C are depicted in Appendix A'. Considering that the purpose our experiment is to validate the security status of each Aviation site and compare to each other, the evaluators set no preference between sites.

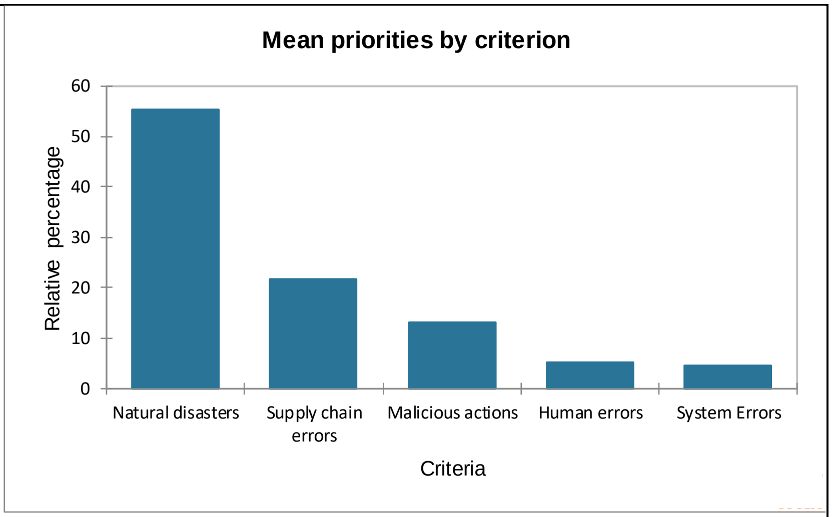
Step 4: run the AHP analysis

The excel template allows the execution of the AHP analysis based on the formulas of the methodology.

The mean priorities by criterion highlight that natural disasters, and supply chain errors are considered the most important factors of security risks on the three different sites according to the three evaluators.

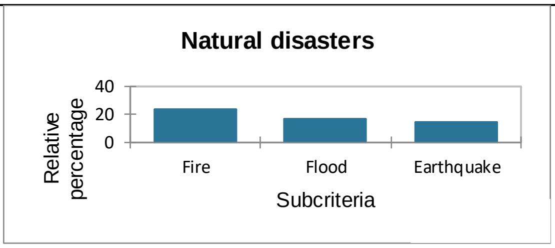
Mean priorities by criterion:

Criteria	%
Natural disasters	55,24
Supply chain errors	21,86
Malicious actions	13,19
Human errors	5,20
System Errors	4,51

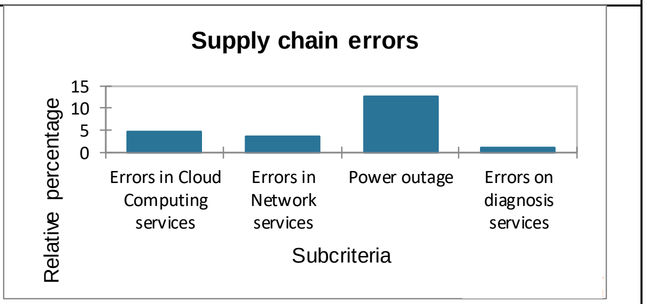


Mean priorities by subcriterion of criterion:

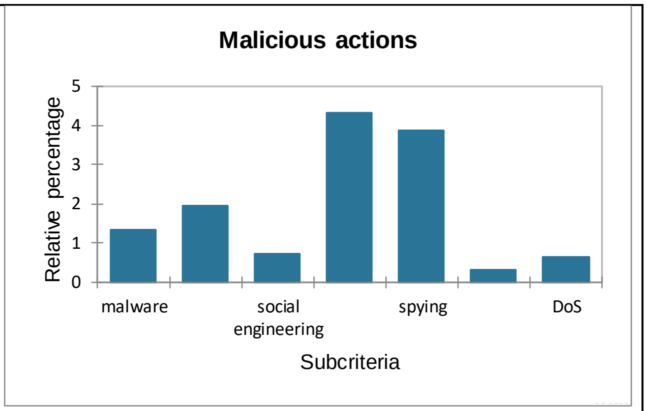
Natural disasters	%
Fire	24,12
Flood	16,81
Earthquake	14,30



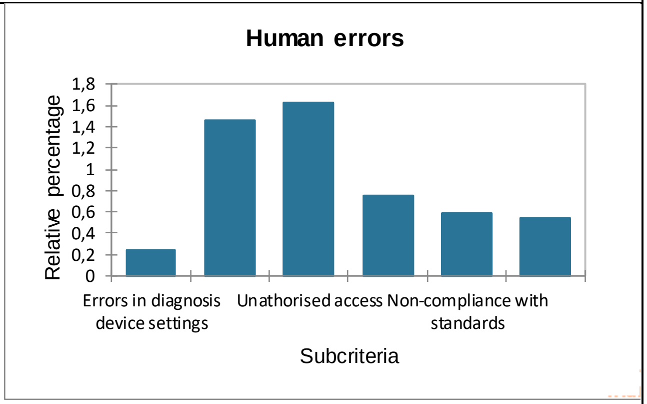
Supply chain errors	%
Errors in Cloud Computing services	4,84
Errors in Network services	3,47
Power outage	12,61
Errors on diagnosis services	0,94



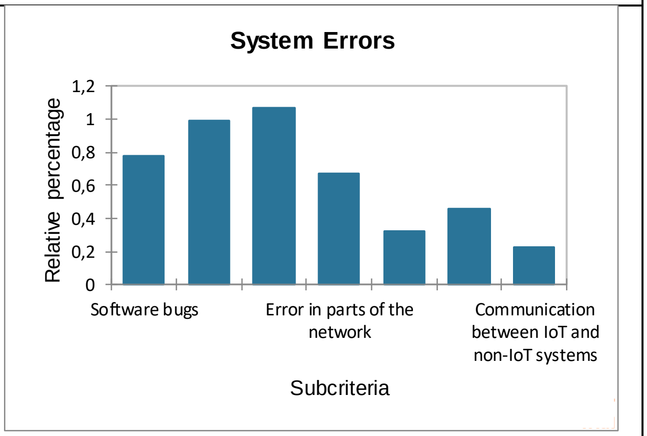
Malicious actions	%
malware	1,35
invasion	1,95
social engineering	0,72
theft (data, services)	4,31
spying	3,89
scan	0,31
DoS	0,66



Human errors	%
Errors in diagnosis device settings	0,25
Loss of records	1,45
Unathorised access	1,63
Lack of control procedures	0,75
Non-compliance with standards	0,58
Mistakes of technical staff	0,54



System Errors	%
Software bugs	0,77
insufficient firmware	0,99
Device error	1,07
Error in parts of the network	0,67
Insufficient maintenance	0,32
Overload	0,46

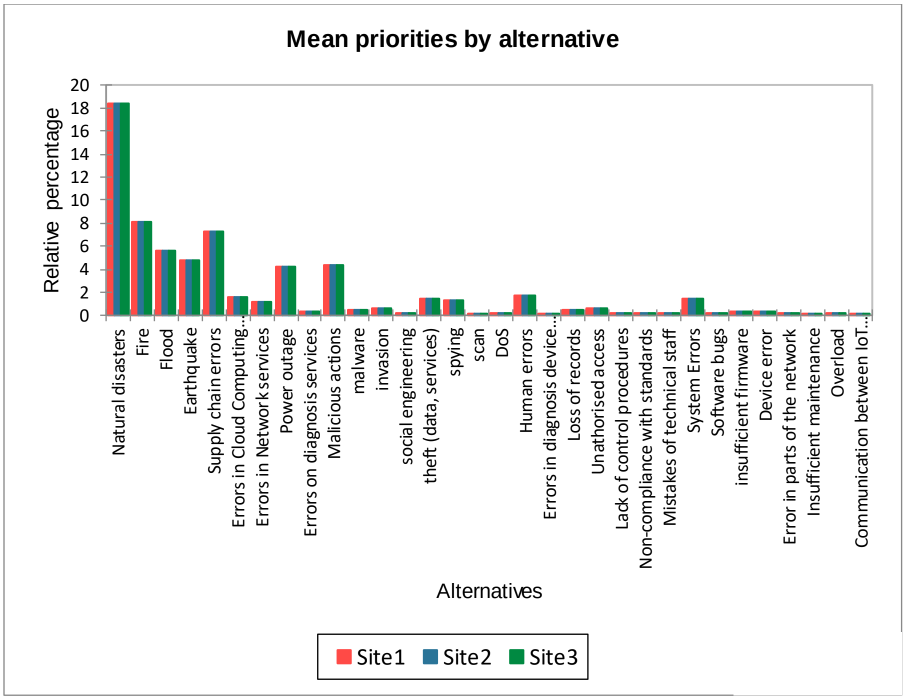


Communication between IoT and non-IoT systems	0,23	

Mean priorities by alternative:

Crit./Alt.	Site1	Site2	Site3
Natural disasters	18,41	18,41	18,41
Fire	8,04	8,04	8,04
Flood	5,60	5,60	5,60
Earthquake	4,77	4,77	4,77
Supply chain errors	7,29	7,29	7,29
Errors in Cloud Computing services	1,61	1,61	1,61
Errors in Network services	1,16	1,16	1,16
Power outage	4,20	4,20	4,20
Errors on diagnosis services	0,31	0,31	0,31
Malicious actions	4,40	4,40	4,40
malware	0,45	0,45	0,45
invasion	0,65	0,65	0,65
social engineering	0,24	0,24	0,24
theft (data, services)	1,44	1,44	1,44
spying	1,30	1,30	1,30
scan	0,10	0,10	0,10
DoS	0,22	0,22	0,22
Human errors	1,73	1,73	1,73
Errors in diagnosis device settings	0,08	0,08	0,08
Loss of records	0,48	0,48	0,48
Unathorised access	0,54	0,54	0,54
Lack of control procedures	0,25	0,25	0,25
Non-compliance with standards	0,19	0,19	0,19

Mistakes of technical staff	0,18	0,18	0,18
System Errors	1,50	1,50	1,50
Software bugs	0,26	0,26	0,26
insufficient firmware	0,33	0,33	0,33
Device error	0,36	0,36	0,36
Error in parts of the network	0,22	0,22	0,22
Insufficient maintenance	0,11	0,11	0,11
Overload	0,15	0,15	0,15
Communication between IoT and non-IoT systems	0,08	0,08	0,08

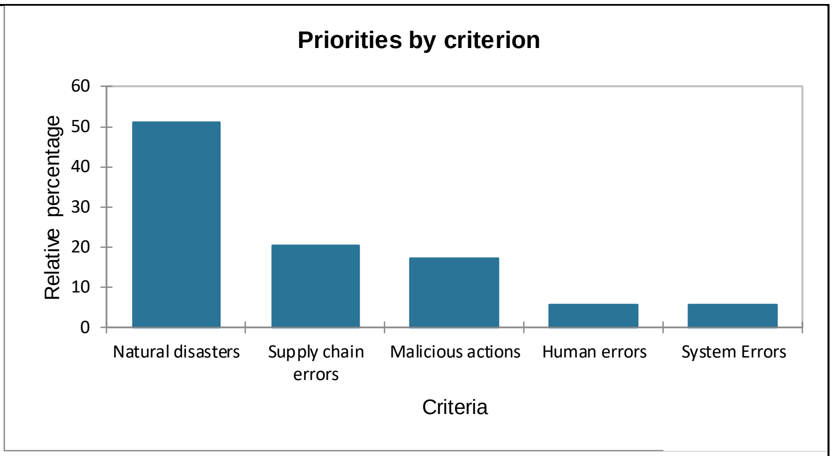


Results obtained from the ratings of evaluator A:

Priorities by criterion:

Criteria	%
Natural disasters	51,02
Supply chain errors	20,42
Malicious actions	17,13
Human errors	5,75
System Errors	5,69

IC = 0,379 ; RC = 33,87%

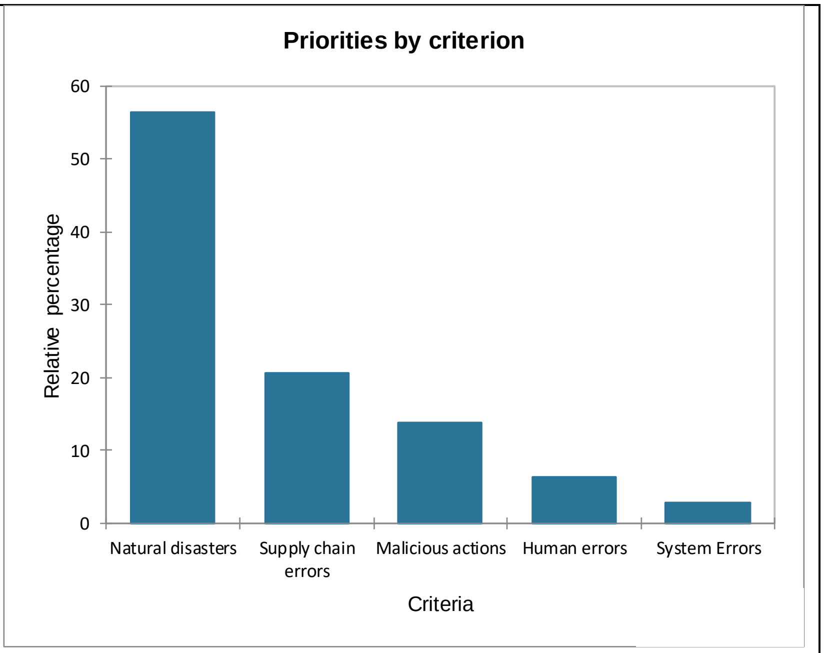


Results obtained from the ratings of evaluator B:

Priorities by criterion:

Criteria	%
Natural disasters	56,43
Supply chain errors	20,60
Malicious actions	13,84
Human errors	6,27
System Errors	2,85

IC = 0,375 ; RC = 33,48%

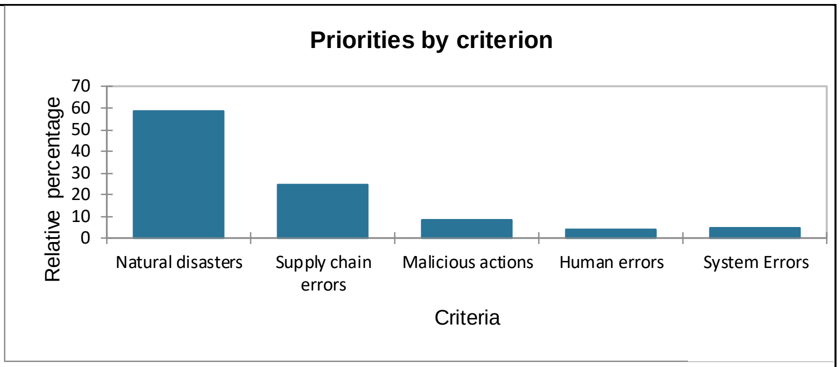


Results obtained from the ratings of evaluator C:

Priorities by criterion:

Criteria	%
Natural disasters	58,26
Supply chain errors	24,57
Malicious actions	8,60
Human errors	3,59
System Errors	4,98

IC = 0,202 ; RC = 18,08%



Conclusions

In the previous chapters we analyzed the different factors that affect cyber security in smart aviation. An attempt was made to create a holistic approach to cyber security in the aviation industry. To ensure the success of this approach we applied an Analytical Hierarchy Process (AHP) to identify those systems /parts of the systems which are identified as more vulnerable. Also, the methodology helps us to gather information on potential risks and vulnerabilities to these systems and to identify potential factors that threaten smart aviation.

The application of the AHP methodology correlates the results of our analysis to three different aviation sites. The analysis results highlight three dominating factors which should drive any decisions regarding the cyber security framework on each site: natural disasters, supply chain errors, and malware. The case study verified the need of integrating an IoT-based monitoring on the production lines of the aviation industry. The process should be based on IoT and notify of any errors and complications in the process or receive data from third systems which predict for any physical disasters. The data can be sent to the cloud to avoid any impact in case of a physical disaster as well as support real time detection and classification using specialized tools.

To reduce the risk of a cyber - attack it is essential that aviation companies reorganize the network topology on IoT and IT components and information systems. Some procedures to address the vulnerabilities and consequences of a cyber-attack are grouped into three categories:

a. The Anthropocentric approach: the not educated or threat-aware staff is one of the main reasons for the increase in cyber-attacks.

Therefore, to properly deal with these attacks on aviation, it is necessary to adopt a human-centered approach, considering human interaction with systems. The International Organization for Standardization - ISO) has developed standards for enhancing human contribution throughout the life cycle of systems. The ISO 9241-210: 2010 standard provides the requirements that will be implemented by the companies that design and develop the hardware and software used in industry so that the final system works in harmony with the final one user.

b. Data and Systems: The goal of networks and communication systems is to ensure that the provisioned IoT-based service systems meet security and interoperability requirements for the operation of the aviation lines.

The purpose of these requirements is to make them integral part of the system processes ensuring that the needs of all are considered users. These communication requirements should be provided by a sophisticated infrastructure network capable of:

- Provide the ability to handle the required load plus a margin for expansion and overload
- Be resistant to damage to the extent necessary for their criticality information it carries
- Be resistant to unauthorized and unintentional use
- Be able to provide system performance information and supports data continuity requirements
- The management of an appropriate network system that defines their processes rules and strategies for monitoring, controlling, and managing the network data communications

In addition, locating an event is important to prevent it from spreading or even to prevent it as soon as it is detected. Watching and detecting possible incidents in the systems, the body can activate the mechanisms deal with the attack and respond appropriately. Information should be provided for the operation of sensors and systems, including components for verification and validation of systems performance. The process of identifying unusual activities should include:

- Use analysis procedures that can detect abnormalities behaviors
- The definition of an individual or a group to undertake all aspects related to it in the field of cyber security, on behalf of the company

- Complete history of incidents

Risk assessment should be organized in relation to its systems and functions of the Smart Aviation domain. The consequences of system failures at all levels should be analyzed to determine the impact on the system as a whole. The risk assessment body should also identify possible risk mitigation measures and determines the necessary actions to be followed. In the risk assessment the following actions should be done:

- Study of the organization's systems
- Identification of possible faults and their causes
- Evaluation of the effects of the non-availability of the systems in its operation organization
- Identification of possible measures to reduce the risk
- Identification of control methods to produce conclusions

c. The architecture of the Network

An intermediate concern when designing a network should be the interconnections between the various IoT components and backend IT systems. The basic idea of creating an optimized network topology is the application of the concept of "Defense-in-depth" that increases the resilience of the network by partitioning its components. Deep defense is one safeguard policy intended to provide a surplus in the event of a failed audit security or exploitation of a vulnerability.

Traditionally, networks on aviation lines are designed in one level. One-tier networks are an approach that aims to reduce costs maintenance and management. Flat networks reduce the number of routers in a network connecting the device to one rather than multiple switches. However, its networks of the press face significant security problems. They have no intermediate boundaries which are used to separate network traffic and meet its requirements regarding deep defense. By implementing a network separation model, the designer has the option to secure each zone individually with firewalls and access control lists (ACLs), which control the network.

In the future, real-time monitoring systems should help the aviation managers to monitor the processes in the aviation industry as well as provide early warning when an error is detected in the supply chain or due to a malware or human/system error. The IoT-based sensors should support large data processing and forecasting models so that the detection of any security threat triggers the execution of automated incident response plans. For example, IoT-based sensors attached to aviation assembly tools transmit data wirelessly to a cloud server where the large data processing system is installed. The system allows large amounts of sensor data to be processed quickly. A corresponding detection method should identify and filter impaired data and correlate them with other security events or alerts to automatically isolate a workstation, or part of the network, suspend part of the production line, block an assembly tool.

The IoT solution should be integrated to a SIEM solution for real time event and log management. The security, integrity, and accountability of the IoT devices and data will be monitored in real time for detecting anomalies to the network, the data processing, suspicious user behavior or malware. The SIEM aggregates data from multiple sources in relation to the security issues, normalizes them and processes them through a policy engine based on rules to alert for any policy violations.

References

Y. Liu et al. (2021), "Zero-Bias Deep Learning for Accurate Identification of Internet-of-Things (IoT) Devices," in IEEE Internet of Things Journal, vol. 8, no. 4, pp. 2627-2634, 15 Feb.15, 2021, doi: 10.1109/JIOT.2020.3018677.

Govindan, K., Rajendran, S., Sarkis, J., & Murugesan, P. (2015). Multi criteria decision making approaches for green supplier evaluation and selection: a literature review. *Journal of Cleaner Production, 98*, 66-83.

J. Budakoti, A. S. Gaur and C. Lung (2018), "IoT Gateway Middleware for SDN Managed IoT," 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 2018, pp. 154-161, doi: 10.1109/Cybermatics_2018.2018.00057.

Edwards T., Bayoumi A., Lester Eisner M. (2017) Internet of Things – A Complete Solution for Aviation's Predictive Maintenance. In: Bahei-El-Din Y., Hassan M. (eds) Advanced Technologies for Sustainable Systems. Lecture Notes in Networks and Systems, vol 4. Springer, Cham.

J. Fiaidhi and S. Mohammed (2019), "Security and Vulnerability of Extreme Automation Systems: The IoMT and IoA Case Studies," in IT Professional, vol. 21, no. 4, pp. 48-55, 1 July-Aug. 2019, doi: 10.1109/MITP.2019.2906442.

Vinita Malik & Sukhdip Singh (2019) Security risk management in IoT environment, Journal of Discrete Mathematical Sciences and Cryptography, 22:4, 697-709, DOI: 10.1080/09720529.2019.1642628

Valdés, Rosa & Gomez Comendador, Victor & Sanz, Álvaro & Pérez Castán, Javier. (2018). Aviation 4.0: More Safety through Automation and Digitization. 10.5772/intechopen.73688.

K. Sampigethaya and R. Poovendran (2013). "Aviation Cyber–Physical Systems: Foundations for Future Aircraft and Air Transport," in Proceedings of the IEEE, vol. 101, no. 8, pp. 1834-1855, Aug. 2013, doi: 10.1109/JPROC.2012.2235131.

K. Sampigethaya, R. Poovendran and L. Bushnell (2008). "Secure Operation, Control, and Maintenance of Future E-Enabled Airplanes," in Proceedings of the IEEE, vol. 96, no. 12, pp. 1992-2007, Dec. 2008, doi: 10.1109/JPROC.2008.2006123.

A. Mukherjee (2015) "Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality Under Resource Constraints," in Proceedings of the IEEE, vol. 103, no. 10, pp. 1747-1761, Oct. 2015, doi: 10.1109/JPROC.2015.2466548.

B. Buntz (2016). The 10 Most Vulnerable IoT Security Targets, https://www.iotworldtoday.com/2016/07/27/10-most-vulnerable-iot-security-targets/ , accessed 24/02/2021.

In Lee, Kyoochun Lee (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises, Business Horizons, Volume 58, Issue 4, 2015, Pages 431-440.

H. Suo, J. Wan, C. Zou and J. Liu (2012), "Security in the Internet of Things: A Review," 2012 International Conference on Computer Science and Electronics Engineering, Hangzhou, China, 2012, pp. 648-651, doi: 10.1109/ICCSEE.2012.373.

C. Perera, P. P. Jayaraman, A. Zaslavsky, D. Georgakopoulos and P. Christen (2014). "Sensor discovery and configuration framework for the Internet of Things paradigm," 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, Korea (South), 2014, pp. 94-99, doi: 10.1109/WF-IoT.2014.6803127.

D. Singh, G. Tripathi and A. J. Jara (2014). "A survey of Internet-of-Things: Future vision, architecture, challenges and services," 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, Korea (South), 2014, pp. 287-292, doi: 10.1109/WF-IoT.2014.6803174.

Iqbal, M., Olaleye, O., & Bayoumi, M. A review on Internet of Things (IoT): security and privacy requirements and the solution approaches. Global Journal of Computer Science and Technology. 2017.

I. Andrea, C. Chrysostomou and G. Hadjichristofi (2015), "Internet of Things: Security vulnerabilities and challenges," 2015 IEEE Symposium on Computers and Communication (ISCC), Larnaca, Cyprus, 2015, pp. 180-187, doi: 10.1109/ISCC.2015.7405513.

B. Bhushan, G. Sahoo and A. K. Rai (2017), "Man-in-the-middle attack in wireless and computer networking — A review," 2017 3rd International Conference on Advances in Computing,Communication & Automation (ICACCA) (Fall), Dehradun, India, 2017, pp. 1-6, doi: 10.1109/ICACCAF.2017.8344724.

Choi, Seul-Ki, Yang, Chung-Huang, Kwak, Jin (2018), "System Hardening and Security Monitoring for IoT Devices to Mitigate IoT Security Vulnerabilities and Threats," KSII Transactions on Internet and Information Systems, vol. 12, no. 2, Feb. 2018.

Mrabet H, Belguith S, Alhomoud A, Jemai A (2020). A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis. *Sensors*. 2020; 20(13):3625.

Raju D., Eleswarapu L., Saiv R., Nath V. (2019) Study and Design of Smart Embedded System for Aviation System: A Review. In: Nath V., Mandal J. (eds) Nanoelectronics, Circuits and Communication Systems. Lecture Notes in Electrical Engineering, vol 511. Springer, Singapore.

L. Zhang (2014), "Convergence of physical system and cyber system modeling methods for aviation cyber physical control system," 2014 IEEE International Conference on Information and Automation (ICIA), Hailar, China, 2014, pp. 542-547, doi: 10.1109/ICInfA.2014.6932714.

Karakuş G., Karşıgil E., Polat L. (2019) The Role of IoT on Production of Services: A Research on Aviation Industry. In: Durakbasa N., Gencyilmaz M. (eds) Proceedings of the International Symposium for Production Research 2018. ISPR 2018. Springer, Cham.

Wang X., Liu Y., Li Z., Li M., Zhang S. (2013) Aviation Equipment Maintenance Safety Management Based on the Technology of IOT. In: Qi E., Shen J., Dou R. (eds) The 19th International Conference on Industrial Engineering and Engineering Management. Springer, Berlin, Heidelberg.

Sai-Ho Chung, Hoi-Lam Ma, Mark Hansen, Tsan-Ming Choi (2020), Data science and analytics in aviation, Transportation Research Part E: Logistics and Transportation Review, Volume 134, 2020, 101837, ISSN 1366-5545,

Ishizaka, A., & Labib, A. (2009). Analytic Hierarchy Process and Expert Choice: Benefits and limitations. *OR Insight, 22*(4), 201-220.

Ishizaka, A., & Labib, A. (2011). Review of the main developments in the analytic hierarchy process. *Expert Systems with Applications, 38*(11), 14336-14345.

Saaty, T. (1977). A scaling method for priorities in hierarchical structures. *Journal of Mathematical Psychology, 15*(3), 234-281.

Saaty, T. (2012). Decision making for leaders. *IEEE Transactions on Systems, Man, and Cybernetics, SMC-15*(3), 450-452.

Saaty, T., & Hu, G. (1998). Ranking by Eigenvector Versus Other Methods in the Analytic Hierarchy Process. *Applied Mathematics Letters, 11*(4), 121-125.

Saaty, T., & Kearns, K. (1985). *Analytical planning: the organization of systems.* Oxford, New York: Pergamon Press.

Rezaei, J., & Ortt, R. (2013). Multi-criteria supplier segmentation using a fuzzy preference relations based AHP. *European Journal of Operational Research, 225*(1), 75-84.

Chu, A., Kalaba, R., & Spingarn, K. (1979). A comparison of two methods for determining the weights of belonging to fuzzy sets. *Journal of Optimization Theory and Applications, 27*(4), 531-538.

Mikhailov, L. (2000). A fuzzy programming method for deriving priorities in the analytic hierarchy process. *Journal of the Operational Research Society, 51*(3), 341-349.

Appendix A’

A1. Alternatives of Evaluator A, B, and C

Alternatives for subcriterion Fire:

Alternatives	Site1	Site2	Site3
Site1	1,00	1,00	1,00
Site2	1,00	1,00	1,00
Site3	1,00	1,00	1,00

Alternatives for subcriterion Flood:

Alternatives	Site1	Site2	Site3
Site1	1,00	1,00	1,00
Site2	1,00	1,00	1,00
Site3	1,00	1,00	1,00

Alternatives for subcriterion Earthquake:

Alternatives	Site1	Site2	Site3
Site1	1,00	1,00	1,00
Site2	1,00	1,00	1,00
Site3	1,00	1,00	1,00

Alternatives for subcriterion Errors in Cloud Computing services:

Alternatives	Site1	Site2	Site3
Site1	1,00	1,00	1,00
Site2	1,00	1,00	1,00
Site3	1,00	1,00	1,00

Alternatives for subcriterion Errors in Network services:

Alternatives	Site1	Site2	Site3
Site1	1,00	1,00	1,00
Site2	1,00	1,00	1,00
Site3	1,00	1,00	1,00

Alternatives for subcriterion Power outage:

Alternatives	Site1	Site2	Site3
Site1	1,00	1,00	1,00
Site2	1,00	1,00	1,00
Site3	1,00	1,00	1,00

Alternatives for subcriterion Errors on diagnosis services:

Alternatives	Site1	Site2	Site3
Site1	1,00	1,00	1,00

Site2	1,00	1,00	1,00
Site3	1,00	1,00	1,00

Alternatives for subcriterion malware:

Alternatives	Site1	Site2	Site3
Site1	1,00	1,00	1,00
Site2	1,00	1,00	1,00
Site3	1,00	1,00	1,00

Alternatives for subcriterion invasion:

Alternatives	Site1	Site2	Site3
Site1	1,00	1,00	1,00
Site2	1,00	1,00	1,00
Site3	1,00	1,00	1,00

Alternatives for subcriterion social engineering:

Alternatives	Site1	Site2	Site3
Site1	1,00	1,00	1,00
Site2	1,00	1,00	1,00
Site3	1,00	1,00	1,00

Alternatives for subcriterion theft (data, services):

Alternatives	Site1	Site2	Site3
Site1	1,00	1,00	1,00
Site2	1,00	1,00	1,00
Site3	1,00	1,00	1,00

Alternatives for subcriterion spying:

Alternatives	Site1	Site2	Site3
Site1	1,00	1,00	1,00
Site2	1,00	1,00	1,00
Site3	1,00	1,00	1,00

Alternatives for subcriterion scan:

Alternatives	Site1	Site2	Site3
Site1	1,00	1,00	1,00
Site2	1,00	1,00	1,00
Site3	1,00	1,00	1,00

Alternatives for subcriterion DoS:

Alternatives	Site1	Site2	Site3
Site1	1,00	1,00	1,00
Site2	1,00	1,00	1,00
Site3	1,00	1,00	1,00

Alternatives for subcriterion Errors in diagnosis device settings:

Alternatives	Site1	Site2	Site3
Site1	1,00	1,00	1,00
Site2	1,00	1,00	1,00
Site3	1,00	1,00	1,00

Alternatives for subcriterion Loss of records:

Alternatives	Site1	Site2	Site3
Site1	1,00	1,00	1,00
Site2	1,00	1,00	1,00
Site3	1,00	1,00	1,00

Alternatives for subcriterion Unathorised access:

Alternatives	Site1	Site2	Site3
Site1	1,00	1,00	1,00
Site2	1,00	1,00	1,00
Site3	1,00	1,00	1,00

Alternatives for subcriterion Lack of control procedures:

Alternatives	Site1	Site2	Site3
Site1	1,00	1,00	1,00
Site2	1,00	1,00	1,00
Site3	1,00	1,00	1,00

Alternatives for subcriterion Non-compliance with standards:

Alternatives	Site1	Site2	Site3
Site1	1,00	1,00	1,00
Site2	1,00	1,00	1,00
Site3	1,00	1,00	1,00

Alternatives for subcriterion Mistakes of technical staff:

Alternatives	Site1	Site2	Site3
Site1	1,00	1,00	1,00
Site2	1,00	1,00	1,00
Site3	1,00	1,00	1,00

Alternatives for subcriterion Software bugs:

Alternatives	Site1	Site2	Site3
Site1	1,00	1,00	1,00
Site2	1,00	1,00	1,00
Site3	1,00	1,00	1,00

Alternatives for subcriterion insufficient firmware:

Alternatives	Site1	Site2	Site3
Site1	1,00	1,00	1,00
Site2	1,00	1,00	1,00
Site3	1,00	1,00	1,00

Alternatives for subcriterion Device error:

Alternatives	Site1	Site2	Site3
Site1	1,00	1,00	1,00
Site2	1,00	1,00	1,00
Site3	1,00	1,00	1,00

Alternatives for subcriterion Error in parts of the network:

Alternatives	Site1	Site2	Site3
Site1	1,00	1,00	1,00
Site2	1,00	1,00	1,00
Site3	1,00	1,00	1,00

Alternatives for subcriterion Insufficient maintenance:

Alternatives	Site1	Site2	Site3
Site1	1,00	1,00	1,00
Site2	1,00	1,00	1,00
Site3	1,00	1,00	1,00

Alternatives for subcriterion Overload:

Alternatives	Site1	Site2	Site3
Site1	1,00	1,00	1,00

Site2	1,00	1,00	1,00
Site3	1,00	1,00	1,00

Alternatives for subcriterion Communication between IoT and non-IoT systems:

Alternatives	Site1	Site2	Site3
Site1	1,00	1,00	1,00
Site2	1,00	1,00	1,00
Site3	1,00	1,00	1,00

A2. Priorities by Subcriterion

Evaluator A

Priorities by subcriterion of the criterion:

Natural disasters	%
Fire	15,91
Flood	10,08
Earthquake	25,02

IC = 0,027 ; RC = 4,63%

Supply chain errors	%
Errors in Cloud Computing services	4,25
Errors in Network services	4,25
Power outage	11,11
Errors on diagnosis services	0,81

IC = 0,039 ; RC = 4,32%

Malicious actions	%

Human errors	%

System Errors	%

malware	1,32
invasion	2,13
social engineering	0,68
theft (data, services)	5,46
spying	6,20
scan	0,41
DoS	0,93

IC = 0,198 ; RC = 14,98%

Errors in diagnosis device settings	0,18
Loss of records	0,89
Unathorised access	2,23
Lack of control procedures	1,16
Non-compliance with standards	0,40
Mistakes of technical staff	0,90

IC = 0,539 ; RC = 43,45%

Software bugs	1,60
insufficient firmware	1,05
Device error	1,36
Error in parts of the network	0,60
Insufficient maintenance	0,45
Overload	0,42
Communication between IoT and non-IoT systems	0,21

IC = 0,348 ; RC = 26,35%

Evaluator B

Priorities by subcriterion of the criterion:

Natural disasters	%
Fire	18,09
Flood	25,62

Supply chain errors	%
Errors in Cloud Computing services	4,98
Errors in Network services	2,84

Earthquake	12,72

IC = 0,068 ; RC = 11,74%

Power outage	11,84
Errors on diagnosis services	0,94

IC = 0,068 ; RC = 7,58%

Malicious actions	%
malware	1,68
invasion	2,26
social engineering	0,76
theft (data, services)	4,47
spying	3,67
scan	0,30
DoS	0,70

IC = 0,238 ; RC = 18,04%

Human errors	%
Errors in diagnosis device settings	0,39
Loss of records	2,19
Unathorised access	1,85
Lack of control procedures	0,43
Non-compliance with standards	0,88
Mistakes of technical staff	0,53

IC = 0,144 ; RC = 11,63%

System Errors	%
Software bugs	0,29
insufficient firmware	0,64
Device error	0,70
Error in parts of the network	0,39
Insufficient maintenance	0,24
Overload	0,48
Communication between IoT and non-IoT systems	0,11

IC = 0,246 ; RC = 18,66%

Evaluator C

Priorities by subcriterion of the criterion:

Natural disasters	%
Fire	38,36
Flood	14,73
Earthquake	5,17

IC = 0,154 ; RC = 26,53%

Supply chain errors	%
Errors in Cloud Computing services	5,29
Errors in Network services	3,33
Power outage	14,87
Errors on diagnosis services	1,08

IC = 0,099 ; RC = 11,06%

Malicious actions	%
malware	1,04
invasion	1,47
social engineering	0,73
theft (data, services)	2,99
spying	1,81
scan	0,21
DoS	0,35

Human errors	%
Errors in diagnosis device settings	0,17
Loss of records	1,27
Unathorised access	0,81
Lack of control procedures	0,68
Non-compliance with standards	0,47
Mistakes of technical staff	0,19

IC = 0,192 ; RC = 15,49%

System Errors	%
Software bugs	0,42
insufficient firmware	1,28
Device error	1,15
Error in parts of the network	1,02
Insufficient maintenance	0,26
Overload	0,48
Communication between IoT and non-IoT systems	0,37

IC = 0,171 ; RC = 12,96%

IC = 0,137 ; RC = 10,38%