Securing Smart Airports

DECEMBER 2016

www.enisa.europa.eu

European Union Agency For Network And Information Security

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its Member States (MS), the private sector and Europe’s citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU MS in implementing relevant EU legislation and works to improve the resilience of Europe’s critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU MS by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Acknowledgements

Over the course of this study, we have received valuable input and feedback from:
Jean-Jacques Woeldgen, European Commission
Vicente De-Frutos-Cristobal, European Commission
Jean-Paul Moreaux, European Aviation Safety Agency
Zarko Sivcev, EUROCONTROL
Charles de Couëssin, ID Partners
Khan Ferdous Wahid, Airbus
Fillippos Komninos, Athens International Airport
David Trembaczowski-Ryder, ACI Europe
Francesco Di Maio, ENAV
Theodoros Kiritsis, IFATSEA
Costas Christoforou, IFATSEA
Alcus Erasmus, Manchester Airport
Alexander Doehne, Fraport AG Frankfurt Airport
Iakovos Ouranos, Heraklion Airport
Charles Badjaksezian, Geneva Airport
Chris Johnson, Glasgow University
Tim Steeds, British Airways
Morten Fruensgaard, AVINOR
Matt Shreeve, Helios
Ruben Flohr, SESAR Joint Undertaking
Giuliano D'Auria, Leonardo-Finmeccanica
Philippe-Emmanuel Maulion, SITA
ADP Group
Amadeus
Zurich Airport

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

ISBN 978-92-9204-185-4 , doi: 10.2824/865081

Table of Contents

Executive Summary 7

1. Introduction 9

1.1 Objectives and scope of the study 9

1.2 Target audience 10

1.3 Why cyber security is important for airports 10

1.4 Methodology 11

1.5 Outline of the report 12

2. Key aspects in Smart airport cyber security 13

2.1 Key stakeholders in Smart airports 14

2.2 EU cyber security policy in civil aviation 16

2.3 Airport IT architecture and stakeholder interactions 18

2.4 User experience in Smart airports: the end-to-end passenger journey 19

2.5 Safety, security and cyber security in airports 21

2.6 Cyber security in Smart airports 21

3. Key asset groups and assets 22

3.1 Smart airport assets 23

4. Threat and risk analysis 25

4.1 Emerging challenges in smart airports 25

4.2 Threat analysis 25

4.2.1 Threat taxonomy 26

4.2.2 Threat modeling 28

4.2.3 Sample cyber security attacks 30

5. Attack scenarios 33

5.1 Tampering with airport self-serving e-ticketing systems 33

5.2 Network attack to the baggage handling 35

5.3 Drone intercept as mobile vehicle for jamming and spoofing aircraft-airport and traffic control-airline communications 37

5.4 Attacks tools and techniques available 39

6. Security good practices 42

6.1 Technical/tool-based good practices 43

6.2 Policies and standards 43

6.3 Organisational, people and processes 45

7. Gap analysis and identification of areas of improvement 47

Gap 1: Disparity of cyber security practices in airports 47

Gap 2: Lack of a common approach and multi-stakeholders model on cyber security of airports 47

Gap 3: Guidelines on network architecture, ownership, and remote management 48

Gap 4: Evidence-based vulnerability analysis metrics and priorities 48

Gap 5: Threat modelling and architecture analysis 48

Gap 6: Information sharing 49

Gap 7: Multi-stakeholder trust framework and trust-enable security technologies 49

Gap 8: Lack of awareness and skills 49

8. Recommendations 50

8.1 Prioritise cyber security for safety 50

8.2 Establish a clear airport cyber security posture and allocate adequate roles and resources 50

8.3 Revise cyber security policies and practices based on good practices monitoring 50

8.4 Implement network-based, holistic risk and threat management policy and processes for cyber security 51

8.5 Promote and facilitate the development of common guidelines, standards, awareness and knowledge exchange on cyber security for smart airports 51

8.6 Facilitate the development of accreditation and third party auditing for cyber security in Smart airport 51

8.7 Collaborate with key stakeholders in the development of specific standards for cyber security products and solutions 52

8.8 Work with airport operators to develop products and/or solutions that are aligned to their cyber security requirements 52

9. Annexes 53

9.1 Example of information security incidents impacting airports operations 53

9.2 Key EU Legislation and relevant legislation affecting Smart airports 57

9.3 Detailed Third Level Threat Taxonomy 62

9.4 Main Threats to Smart Airport and related affected assets 63

9.5 Detailed security good practices 70

9.5.1 Technical/Tool-based 70

9.5.2 Policies and Standards 74

9.5.3 Organisational, People and Processes 77

9.6 Glossary 82

Executive Summary

Smart airports are those airports making use of networked, data driven response capabilities that, on the one hand, provide travellers with a better and seamless travel experience and, on the other hand, aim to guarantee higher levels of security for the safety of the passengers and operators. These airports are implementing new smart components to offer travellers a portfolio of services that spans from self or automatic check-in, baggage & document check, flight booking management and way finding services to automated border control and security checks.

Smart components can be defined as any networked ICT system that has a data processing capability ranging from aggregating simple data to extracting insights to support human decisions and/or triggering an automated response. These components while enhancing the user experience, they also pave the way for new attack vectors and expose airport assets to a larger attack surface. Therefore, airport decision makers need to acknowledge the threats emerging from smart components, increase their awareness of security implications and improve the security of their infrastructure in order to enhance safety for passengers and all airport stakeholders.

In response to these new emerging threats faced by smart airports, this report provides a guide for airport decision makers (CISOs, CIOs, IT Directors and Head of Operations) and airport information security professionals, but also relevant national authorities and agencies that are in charge of cyber-security for airports. Based on an in depth examination of existing knowledge as well as validation interviews with subject matter experts, this report highlights the key assets of smart airports. Built on this, a detailed analysis and threats mapping was conducted with a particular focus on the vulnerabilities of smart components. With the feedback from airport subject matter experts, a series of attack scenarios was developed to underline the increased attack surface and challenges when smart components are integrated in the traditional IT airport systems.

On the basis of this analysis, a number of good practices for securing smart airports is identified in order to support Information security professionals and airport decision makers in their security efforts and risk management activities. The goal of this study is to provide airport operators with a start-up kit to enhance cybersecurity in smart airports. The study additionally identifies gaps on different areas, including: operational practices and the need to develop clear airport cyber security postures.

As the result of this work a total of eight recommendations for enhancing the security and resilience of Smart airports in Europe are presented, tailored specifically towards decision makers, airport operators and industry.

Recommendations for airport decision makers (CISOs, CIOs, IT Directors and Head of Operations) and airport information security professionals:

- **Prioritise cyber security for safety**
- **Establish a clear airport cyber security posture and allocate adequate roles and resources**
- **Revise cyber security policies and practices based on good practices monitoring**
- **Implement network-based, holistic risk and threat management policy and processes for cyber security**

Recommendations for policy-makers

- **Promote and facilitate the development of common guidelines, standards, metrics, awareness and knowledge exchange on cyber security for smart airports**
- **Facilitate the development of accreditation and third party auditing for cyber security in Smart airport**

Recommendations for industry representatives

- **Collaborate with key stakeholders in the development of specific standards for cyber security products and solutions**
- **Work with airport operators to develop products and/or solutions that are aligned to their cyber security requirements.**

1. Introduction

1.1 Objectives and scope of the study

The objective of this study is to improve the security and resilience of smart airports, including air traffic management for what is relevant to the functioning of smart airports. This is in order to prevent disruptions to smart components that could have an impact on the service and safety being delivered to passengers, while also promoting cost benefits and protecting the environment. The aim is to provide guidance to airports to help them ensure a seamless, safe and secure passenger experience.[1] This is in the context of ENISA's role specified in EC Communication "Internet of Things – An Action Plan for Europe" and its support for the implementation of the Network Information Security Directive. [2]

Smart airports introduce new components and functionalities to facilitate the infrastructure-to-passenger interaction and vice-versa.[3] This improvement paves the way for new attack vectors or pathways and exposes airport assets to a larger attack surface. Therefore, airport decision makers (CISOs, CIOs, IT Directors and Head of Operations) and airport information security professionals need to identify new threats applicable to smart components, increase their awareness of security issues and improve the security of their infrastructure in order to enhance safety through the most relevant good practices.

In this study smart airports are defined as those airports implementing smart components, which are value-added services built on the top of traditional legacy infrastructures. Such components and services aim to produce a more seamless, secure and safe passenger experience via digital assistance and automation.[4]

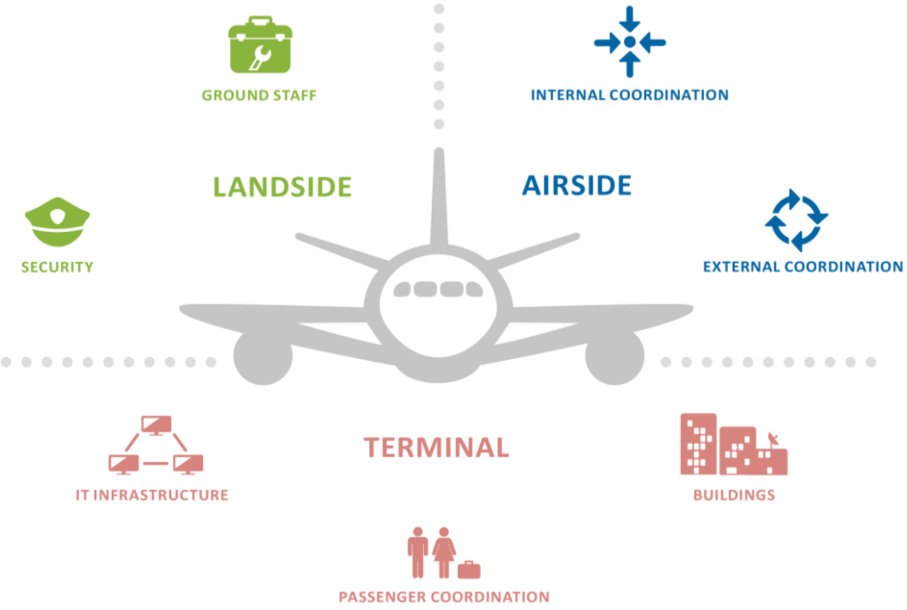


Figure 1: Airport High Level Representation

[1] Please note that privacy is not in scope for this report.
[2] See: European Commission, Communication from the commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Internet of Things — An action plan for Europe, COM(2009) 278, Brussels, 18.6.2009; and ENISA, "ENISA' s Position on the NIS Directive", January 2016.
[3] Boutin Nicolas, Achim Fechtel, Hean Ho Loh, and Michael Tan, "The Connected Airport: The Time Is Now", bcg.perspectives, January , 2016.
[4] IATA (2015). Annual Review 2015. Retrieved on 08/04/2016 from: https://www.iata.org/about/Documents/iata-annual-review-2015.pdf

1.2 Target audience

The target audience of this study are Chief Information Security Officers (CISOs), Chief Information Officers (CIOs), IT Directors, Head of Operations in charge of information security and airport information security professionals in airports. The study is also relevant for all organisations that need to ensure the security of their 'smart' integrated solutions and services they offer to airports. In addition, due to the supply chain characterising smart airports and the dependencies among airport operators, this report can also be of benefit to companies involved in the airport supply chain, including Air Navigation Service Providers (ANSP) and Air Traffic Management (ATM) operators, as well as relevant national authorities and agencies that are in charge of cyber security for airports.

1.3 Why cyber security is important for airports

Smart airports were included under the umbrella of smart infrastructures in the ENISA Work Programme 2016.[5] The aim was to identify major airports that developed and operated smart services and to take stock of the security challenges arising from usage of these services. Indeed, there has been an increase in information security incidents, including both cyber-attacks and ICT dependencies disruptions, experienced by the aviation sector worldwide, which has been widely reported in the press in recent years. Table 1 provides a timeline of the 2016 information security related incidents in airports, which illustrates their potential prevalence and impact, and the relevance of this work. A more detailed list is available in the annex. In this study, ENISA aims to provide good practices and recommendations, for airports as well as relevant public authorities, which address these challenges.

Table 1: Example of 2016 information security incidents impacting airports operations

DATE	COUNTRY	DESCRIPTION
August 2016	US	Thousands of air passengers around the world were left stranded after a power cut forced the US airline Delta to suspend flights.[6] The overnight power failure took place in Atlanta, near Delta's headquarters, causing computer systems to crash. Airport check-in systems, passenger advisory screens, the airline's website and smartphone apps were all affected by the system failure.
July 2016	Vietnam	Attackers successfully attacked Vietnam's two largest airports and the nation's flag carrier, Vietnam Airlines[7]. The attackers briefly hijacked flight information screens and sound systems inside the two airports. Instead of departure and arrival details, the airports' flight screens and speakers broadcasted what local media described as anti-Vietnamese and Philippines slogans, in turn prompting authorities to shut down both systems. Vietnam Airlines' website, meanwhile, was also seized and transferred to a malicious website abroad, while passenger data pertaining to an undisclosed number of its frequent flyers was published online as well. As a result of this attack Vietnamese authorities will carry out a comprehensive check on Chinese devices and technology to ensure information security at the Vietnamese

[5] ENISA Work Programme, https://www.enisa.europa.eu/publications/corporate/enisa-work-programme-2016.
[6] Delta: Power cut strands thousands of passengers, http://www.bbc.co.uk/news/world-us-canada-37007908.
[7] Cyberattack claims multiple airports in Vietnam, http://www.washingtontimes.com/news/2016/jul/29/cyberattack-claims-multiple-airports-vietnam-airli/.

		airports since it is feared that the Chinese hacker group 1937cn might be responsible for the attacks.[8]
July 2016	IT	A third party failure at Rome's Fiumicino airport caused the shutdown of the automated passenger check-in system, which in turn caused two hours' delays for the passenger checking operation.[9] The failure was related to the Internet provider that the automated passenger check–in at the airport uses for accessing and processing passenger data.
April 2016	UK	After landing, the pilot of a British Airways flight from Geneva reported a collision with a drone while approaching the London Heathrow airport on the 17th April.[10] The incident highlighted the issues faced with regard to drones. While the threat of bird strikes has been well researched, there is still little data about how much damage a drone could cause to an airplane.[11]
April 2016	Worldwide	The civil aircraft manufacturer Airbus Group is hit by up to 12 cyber-attacks per year, mostly in the form of ransomware and hostile actions carried out by state-sponsored attackers.[12] Airbus' chief information security officer cited an instance of ransomware compromising a computer, used by an employee offsite, which then (after the computer was connected to the company's intranet) spread over Airbus' corporate network, encrypting the contents stored on the hard drives of several machines.

1.4 Methodology

This report was developed using a combination of desktop research as well as information from interviews with key stakeholders. The goal is to define and cover the entire IT perimeter of smart airports, drawing on the approach outlined above[13] that incorporates assets inside airports, connected assets outside the airport and dependencies on the airway. The approach taken follows the ENISA methodology developed over the last three years based on the ENISA threat landscape approach, and involved:

- Mapping assets and developing a threat taxonomy that covers possible attacks via desktop research, and validating and/or identifying further gaps through interviews with security experts working in the field of airport information security.
- Enumerating possible attacks that target or affect smart components in airports.
- Developing good practices and three attack scenarios with mitigation actions to provide information on practical examples of implementation, and validating these with security experts working in the field of airport information security.
- Performing a gap analysis based on desktop research and interviews.

[8] Vietnam to inspect use of Chinese technology following cyberattacks on airports , http://tuoitrenews.vn/society/36329/vietnam-to-inspect-use-of-chinese-technology-following-cyberattacks-on-airports.

[9] Aeroporto di Fiumicino, ore di stop e code al check in per un guasto alla connessione, http://roma.repubblica.it/cronaca/2016/07/18/news/fiumicino_problema_tecnico_al_t3_code_per_i_controlli_arrivano_in_strada-144357812/?ref=HREC1-6.

[10] 'Drone' hits British Airways plane approaching Heathrow, with no damage caused, http://www.airportwatch.org.uk/2016/04/drone-hits-british-airways-plane-approaching-heathrow-with-no-damage-caused/.

[11] 'Drone' hits British Airways plane approaching Heathrow Airport , http://www.bbc.co.uk/news/uk-36067591.

[12] How Airbus defends against 12 big cyber attacks each year, http://www.itnews.com.au/news/how-airbus-defends-against-12-big-cyber-attacks-each-year-418131.

[13] Please see Section 1.1. on the objectives and scope of the study.

- Proposing recommendations for future steps in cyber security for airports in Europe.

Initial results from the desktop research were further consolidated with information acquired during the interview process, specifically in relation to the development of assets, threats, cyber-attack scenarios, good practices and recommendations. A comparative approach was employed in relation to the threats and assets in order to identify asset exposure to cyber threats. This was further validated via interviews with asset owners (i.e. individual airport operators) and a mapping approach was then employed to establish links or connections between assets, threats, good practices, and gaps with the focus on enhancing cyber security within the Smart airport perimeter. Finally, the draft report was circulated among circa 20 organisations across eight countries for additional feedbacks with more than 200 comments integrated into the final version.

1.5 Outline of the report

This document is structured as follows:

- **Section 1 – Introduction:** Introduces the topic and provides an outline of this document, the target audiences and the methodologies employed.
- **Section 2 – Key aspects in Smart airport cyber security -** Provides the contextual environment for smart airports, including definitions, the key legislative environment, the identification of the Smart airport perimeter and its smart key assets.
- **Section 3 – Key asset groups and assets -** In this chapter is provided an overview of the key asset groups and assets to be protected in smart airports.
- **Section 4 – Threat and risk analysis:** Identifies and organises the key cyber threats affecting the key assets within smart airports. The emerging cyber threat vulnerabilities inherent to Smart airport are also discussed, and examples of attacks are presented.
- **Section 5 – Security good practices:** Presents good practices for enhancing cyber security within airports together with three detailed attack scenarios, as identified through both desktop research and the expert interviews.
- **Section 6 – Gap analysis and identification of areas of improvement**: The identification and analysis of existing gaps in cyber security within the airport identified via a comparative analysis of previous findings.
- **Section 7 – Recommendations**: Key recommendations for enhancing the security and resilience of Smart airports.

2. Key aspects in Smart airport cyber security

Within the context of this study, the "Smart airport" concept has been shaped from the vision for the future of air travel that the International Air Transport Association (IATA) is promoting.[14] IATA envisages for the future "air travels [that] should be simple, smooth and hassle free".[15] Such objectives could be met by means of offering the travellers a suite of advanced solutions and services that will cover aspects such as self or automatic check-in, baggage check, document check, flight rebooking, boarding and bag recovery. At the same time, Smart airports promise to guarantee improved security. Linked to the concept of Smart airport, IATA introduced the concept of "smart security", defined as: "a risk-based system that aims to offer a fast and hassle-free passenger screening experience at airports while strengthening security and improving operational efficiency."[16] Smart security "envisions a continuous journey from curb to airside [in which] passengers will proceed through security with minimal inconvenience, with security resources allocated based on risk, and with airport facilities optimised."[17]

The definition of Smart airport that will be used throughout this document refers to **airports making use of networked, data driven response capabilities that, on the one hand, provide travellers with a better and seamless travel experience and, on the other hand, aim to guarantee higher levels of security for the safety of the passengers, operators and general public**. These networked data driven response capabilities tend to be referred to as smart components. In the context of this report these **smart components are defined as any integrated Internet of Things (IoT) components to bring added-value services that has a data processing capability ranging from aggregating simple data to extracting insights to support human decisions and/or triggering an automated response.** The foreseen increasing reliance on network technologies (including the Internet) raises, nonetheless, obvious security concerns.[18] Devising strategies for securing smart airports in face of cyber-attacks and ICT dependencies disruptions is one of the objectives of this study.

Smart components that lie internally and externally to the physical location of the airport are also included in the scope of this research. Any single device that is connected to a network of such systems, even those with minimum or no data processing capabilities, is contained in the airport perimeter overview. As a result, key functions underpinning network communication systems between aircraft, airports, air traffic control and other forms of communication are also in scope of the study. This also encompasses providers of common services and network infrastructures, including passenger and baggage processing technology.

Figure 2 shows which criteria are applied to define the scope of the airport perimeter in the context of this study, bringing together the physical location of assets and functions related to airport operations, the ownership structure and assets or functions defined as 'smart'. This study has endorsed a more encompassing view of what constitutes the Smart airport perimeter. This view recognises the importance of dependencies and interactions among assets and functions related to the overall operation of a Smart airport rather than the location of ownership of such functions and/or assets. As a result, functions and/or assets that might not be owned and/or located within the airport but they are important for the overall

[14] IATA website, http://www.iata.org
[15] IATA (2015). Annual Review 2015. Retrieved on 08/04/2016 from: https://www.iata.org/about/Documents/iata-annual-review-2015.pdf
[16] Ibid.
[17] Ibid.
[18] IATA defines cyber security as: "The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment as well as organizations' and users' assets. It encompasses the protection of electronic systems from malicious attacks and the means by which the consequences of such attacks should be handled." IATA (2015). Fact Sheet Cyber Security. Retrieved on 08/04/2016 from: https://www.iata.org/pressroom/facts_figures/fact_sheets/Documents/fact-sheet-cyber-security.pdf.

operation of a Smart airport are considered. For instance, this in the case for Air Traffic Management (ATM), which the majority of airports do not own any more.

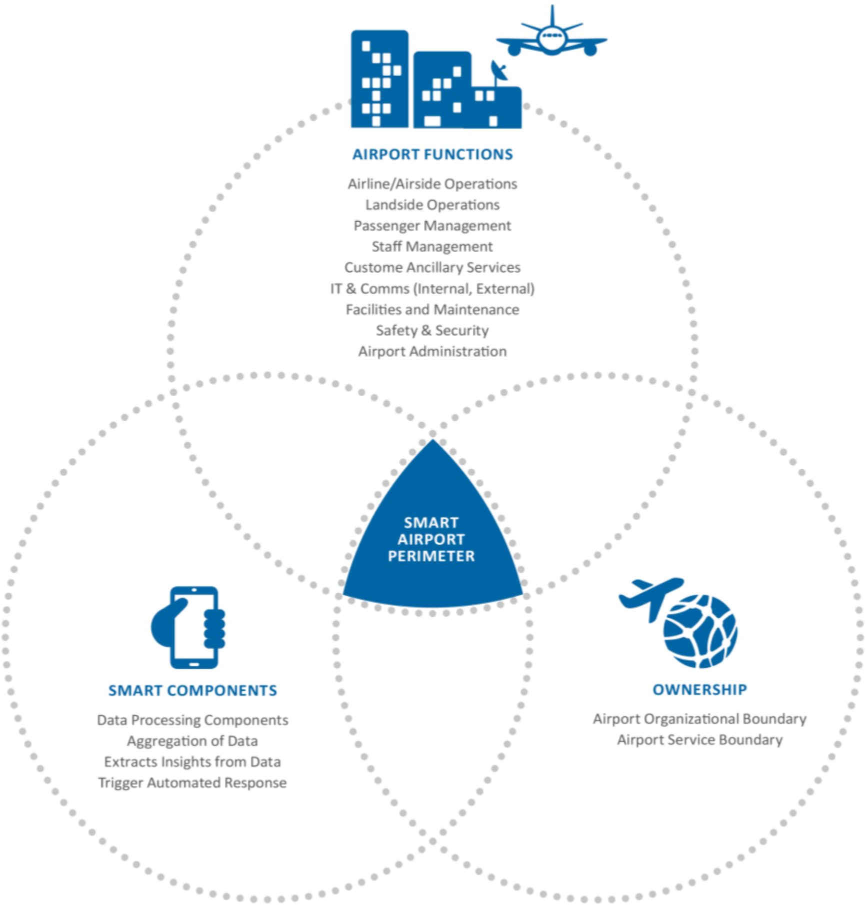

AIRPORT FUNCTIONS
Airline/Airside Operations
Landside Operations
Passenger Management
Staff Management
Custome Ancillary Services
IT & Comms (Internal, External)
Facilities and Maintenance
Safety & Security
Airport Administration
SMART AIRPORT PERIMETER
SMART COMPONENTS
Data Processing Components
Aggregation of Data
Extracts Insights from Data
Trigger Automated Response
OWNERSHIP
Airport Organizational Boundary
Airport Service Boundary

Figure 2: Scope of the Smart Airport Perimeter - Criteria

2.1 Key stakeholders in Smart airports

The Centre for Air Transportation Systems Research[19] in their analysis of airport stakeholders identified two conceptual stakeholder boundaries with regard to the functions and operations of airports. In most cases, regional airport authorities operate airports as "public utilities providing infrastructure to service providers and their supply chain under revenue neutral financial regulate".[20] These public entities work to balance the interests of all of their stakeholders to build the airport infrastructure, lease space to service providers and ensure that service providers meet the needs of seamless, safe and secure air travel services to the passenger. In so doing, two distinct boundaries are generated in the analysis of airport stakeholders:

- **Airport Organisational Boundary**, which depicts the limits of what is controlled or owned by the airport authority or management. This relates to the design and configuration of airport infrastructure (including IT infrastructure) and the operational processes and procedures that underpin the efficiency of its own organisation.

[19] Scharr, D., Sherry, L. (2011) *Analysis of Airport Stakeholders*, Centre for Air Transportation Systems Research, The Volgenau School of Information Technology and Engineering, http://catsr.ite.gmu.edu/pubs/ICNS_Schaar_AirportStakeholders.pdf

[20] Ibid.

- **Airport Service Boundary**, which incorporates the airport supply chain and support services that lie outside direct management control of the airport authority. This includes many IT and support services that are important to the functioning of the airport, but are mainly operated and maintained by third party suppliers.

Figure 3 maps the key stakeholders that contribute to the functioning and operation of the Smart airport, making a distinction between those stakeholders that lie outside the direct boundaries and/or management of the airport and those that lie within the airport organisational boundary. Based on existing related literature[19], Figure 3 provides the high level grouping of the airport key stakeholders[21] , while Table 2 describes each identified stakeholder group and provides additional sub-groups within the main grouping.

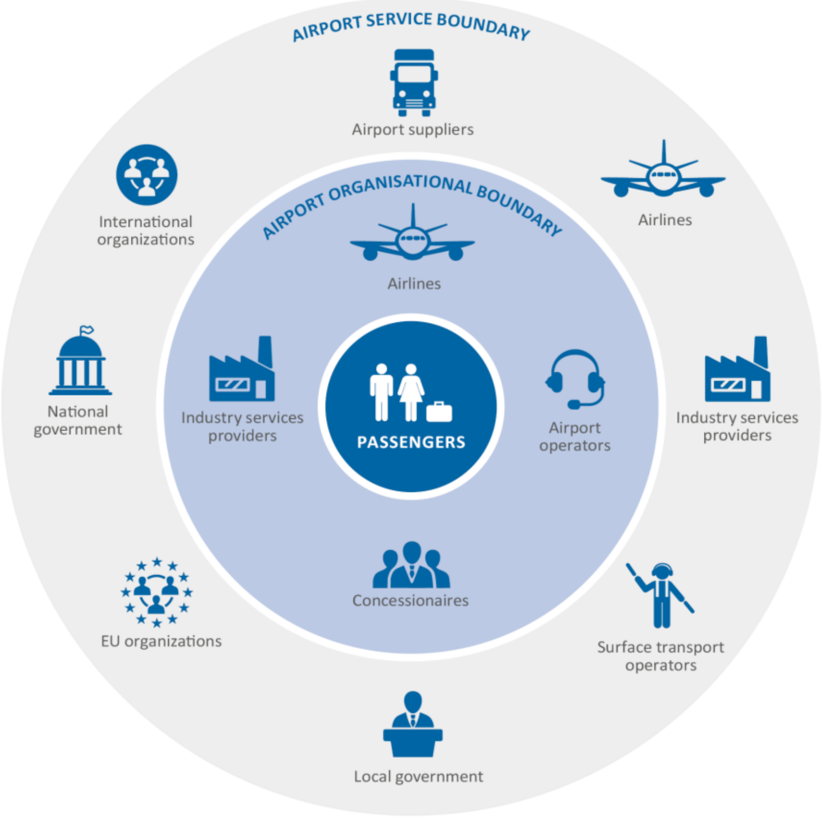


Figure 3 Smart Airports: Key Stakeholders

[21] For the sake of clarity, figure 3 shows a simplified representation of key stakeholders which emphasises the main interactive actors within a Smart airport. Above all for the service boundary reality is somehow more complex and porous since several information and data providers might involve, for instance in the case of Google Maps with information overlaid/integrated from multiple industry and non-industry sources, providing services directly to the Passenger.

Table 2: Definition of Airport Stakeholder Groups:

STAKEHOLDER	DEFINITION/EXPLANATION
Passengers	Customers of the airport, who travel between the ground and air transportation modes or wait for a connection between two flights.
International/EU Organizations	International and EU organisations participate in the airport system by providing international best practices, regulatory standards for the operation of the airport and the management of international air-space. With regard to Air Traffic Management (ATM), organisations such as EUROCONTROL collect and distribute flight information and/or plans among national air traffic controls to optimise Air Traffic Flow and Capacity Management (ATFCM) operations across Europe via the Central Flow Management Unit (CFMU).
National Government	National Government participates in the airport system in two different ways: a) as an operator, focusing on air traffic control services, transportation systems, security (e.g. baggage handling and screening, and customs and immigration); b) as a regulator with regulations applying to airport infrastructure and service providers within airport systems.
Local Government	Local Government is usually responsible for the strategic direction of the airport (in terms of planning decisions) and for appointing airport management, depending on the ownership structure. It also represents the views of local communities and contributes to capital investment projects.
Industry/Third-Party Service Providers	Service providers are private operators that offer services to air carriers and general aviation users. Services provided might include: 1) Air traffic management (i.e., Air Navigation Service Provider, ANSP), 2) fuel management; 3) baggage handling and screening; 4) cargo processing services; 5) kiosk devices (e.g. e-Ticketing); 6) Way-finding services; 7) transport systems; 8) IT and Comms services; 9) security services; etc.
Surface Transport Operators	Surface Transport Operators provide surface access to the airport and include rail services, taxicabs, buses, private rental cars and the subway/underground, while parking services may be provided both on and off the airport by the airports organization or private enterprises.
Airport Operators	The airport organisational structure varies and can be comprised of an individual airport or a group of airports managed by the same organisation e.g. MAG in the UK is a single organisation that operates Manchester, Stansted, Bournemouth and East Midlands airports.
Airlines	An airline is a company that provides air transport services for traveling passengers and freight. Airlines utilise aircraft to supply these services and may form partnerships or alliances with other airlines for codeshare agreements. Generally, airline companies are recognised via an air operating certificate or license issued by a governmental aviation body.
Airport Suppliers	Airport suppliers have the airport itself as the end-customer and includes various contractor, consulting and equipment suppliers.
Concessionaires	Airport Concessionaires operate passenger services in terminal buildings and may include food and beverage services, retail and accommodation.

2.2 EU cyber security policy in civil aviation

At the international level the most important legal instrument on civil aviation security is given by Annex 17 to the Chicago Convention , “Security – Safeguarding International Civil Aviation against Acts of Unlawful Interference” approved by the International Civil Aviation Organisation (ICAO) Council.[22] The primary objective of such instrument is safeguarding passengers, ground personnel, crew as well as the general

[22] Annex 17- Security: Safeguarding International Civil Aviation against Acts of Unlawful Interference, http://www.icao.int/secretariat/PostalHistory/annex_17_security_safeguarding_international_civil_aviation_against_acts_of_unlawful_interference.htm.

public against any acts of unlawful interference. At the European level, EU policy activities in commercial aviation are undertaken by the European Commission (EC) and the European Aviation Safety Agency (EASA) that was established by EC regulation no 216/2008.[23] EU-Lisa, an EU agency responsible for managing and promoting information and communication technology (ICT) in the area of justice, security and freedom, has also supported EU cyber security policy related to aviation above all in relation to border security[24]. Similarly, Single European Sky ATM Research (SESAR) has also provided support with studies and technological developments. [25] The majority of policies at EU level tend to focus on civil aviation in general with some of them also dealing with cyber security for safety within aviation. The ones dealing with cyber security also include concrete actions and outcomes through the use of action plans and/or the setting of specific objectives. Examples of these plans are:

- The European Aviation Safety Plan 2016 – 2020 by EASA[26] published in 2015. [27] The plan outlines key safety actions to address emerging cyber security threats and vulnerabilities in civil aviation. This has arisen, in part, due to the need for new generation aircraft to have their systems connected to the ground in real time with new Air Traffic Management (ATM) technologies requiring internet and wireless connections between the various ground centres and the aircraft. The use and multiplication of network connections serves to increase the vulnerability of the system as a whole.
- The Air Traffic Management Master Plan by SESAR (2015)[28] together with a set of solutions tested in real-life operational conditions with airlines, airports, air navigation service providers and manufacturers. The plan includes the development of an EU framework for cyber security that encompasses regulatory, policy and operational functions across multiple stakeholders including the EU, national and local service providers.

At the EU regulatory level, existing EU Directives and Regulations are categorised as follows, with individual analysis and refences for these Directives and Regulations provided in Annex 2:

- Harmonising rules across the European Community governing the protection of European citizens in the context of civil aviation, including the **protection and processing of passenger data.**
- **Ensuring ATM security and safety** in regards to air space security, personal security, computer network system security and cyber security (e.g. Commission Implementing Regulation, EU No 1035/2011).
- Creating **interoperability of Air Traffic Management (ATM)** across European Community defined airspace. In regard to ATM, EU regulators commonly formulate European Airspace Policy, establish a legal framework for Member States and ensure that legislation is implemented correctly through regular inspections and oversight.

[23] Their role is to draft implementing rules in all fields pertinent to the level of protection for EU citizens in aviation, to certify and approve products where EASA has exclusive competence (e.g. airworthiness), to provide support to Member States in the field of air operations and air traffic management and to promote the use of European and worldwide standards.

[24] Smart Borders and eu-LISA, http://www.eulisa.europa.eu/AboutUs/SmartBorders/Pages/default.aspx.

[25] SESAR 's study on cyber security in ATM, http://www.sesarju.eu/newsroom/all-news/study-details-rd-roadmap-atm-cyber-security.

[26] In a communication from the European Commission in 2015 to the European Parliament, EASA was asked to address cyber-risks in civil aviation in order to '*foster security by design and to establish the necessary emergency response capability.* As part of its role, EASA will offer support to European aviation security stakeholders on the prevention and response to information related security incidents by raising cyber security awareness (cyber security promotion initiatives); advising the EC on aviation cyber security policy/regulatory matters; and—advising the EC, MS or the European Aviation Crisis Coordination Cell (EACCC) in case of an aviation cyber security crisis. See: Communication from the Commission to the European Parliament, the European Council, the European Economic and Social Committee on an Aviation Strategy for Europe, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2015:598:FIN.

[27] EASA (2015) The European Aviation Safety Plan 2016 – 2020, http://www.easa.europa.eu/system/files/dfu/EPAS 2016-2020 FINAL.PDF.

[28] SESAR Strategy and Management Framework Study for Information Cyber-security, http://www.sesarju.eu/sites/default/files/documents/news/SESAR_Strategy_and_Management_Framework_Study_for_Information_cybesecurity_FINAL.pdf

- Rules governing **technical standards and their uniform application in the manufacture of aircraft.** It is not unusual that a producer has to produce different versions of the same type of aircraft and/or equipment depending on the country where it is used. Other regulations lay down procedures for conducting Commission inspections in the field of air safety standards.
- Detailed measures for the implementation of **common basic standards on aviation security**, in particular airport security, airport planning requirements, access control and so on.
- Rules governing **network information security** for critical infrastructures (e.g., Network Information Security Directive see Annex).

2.3 Airport IT architecture and stakeholder interactions

The Airport Cooperative Research Program (ACRP)[29] depicts IT system architectures in airports by organising four conceptual categories in a layered fashion. All IT systems can be categorised into one of the four layers:

- **Physical Layer.** The cabling and fibre infrastructure that provides the foundation for all IT systems in use at the airport and is made up of the non-electronic physical components, including copper cabling, fibre optic, or other components that provide for cross-connection structures.
- **Networking Layer.** Communication systems incorporate the electronic components that send cable or wireless signals. These systems underpinning the network layer communicate data and information using the wired physical layer and/or wireless infrastructure. The physical components include routers, switches, gateways and wireless access points. These IT and Comms systems can be broadly categorised as Local Area Network (LAN) (wired and wireless), Wide Area Network (WAN) (wired and wireless), and Virtual Private Networks (VPN).
- **Service Application Layer.** The application layer contains all the systems that support the operations of the airport. There are numerous smart application systems that have been identified as part of the Assets MINDMAP[30].
- **Integration Layer.** The integration layer allows all applications that are crucial to the operations of the airport to co-ordinate and share information amongst themselves. It allows systems to be directly linked together or share a common data or information pool in order to make better informed decisions. Systems integration is also a key pillar of the Smart airport.

Complex technical infrastructures, such System Wide Information Management (SWIM) and Airport Operations Plan (AOP), developed by SESAR, would combine several layers in their architecture.[31]

Figure 4 shows some of the interactions across the different IT layers, key stakeholders and key airport activities. This indicates that there are several dependencies and collaborations occurring within the airport.

[29] ACRP (2012) Information Technology Systems at Airports: A Primer, http://onlinepubs.trb.org/onlinepubs/acrp/acrp_rpt_059.pdf.
[30] Please see Figure 6.
[31] SESAR Factsheet - Airport Operations Management, http://www.eurocontrol.int/publications/sesar-factsheet-airport-operations-management; and http://www.sesarju.eu/sesar-solutions/swim.

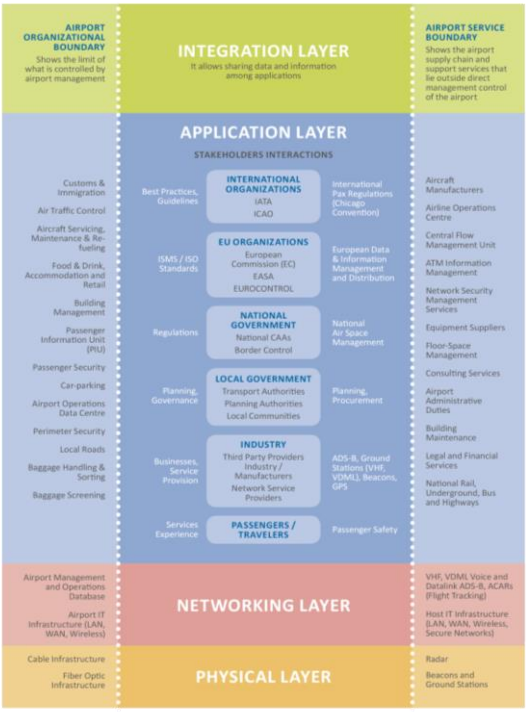

AIRPORT ORGANIZATIONAL BOUNDARY
Shows the limit of what is controlled by airport management
INTEGRATION LAYER
It allows sharing data and information among applications
AIRPORT SERVICE BOUNDARY
Shows the airport supply chain and support services that lie outside direct management control of the airport
APPLICATION LAYER
STAKEHOLDERS INTERACTIONS
Customs & Immigration
Air Traffic Control
Aircraft Servicing, Maintenance & Re-fueling
Food & Drink, Accommodation and Retail
Building Management
Passenger Information Unit (PIU)
Passenger Security
Car-parking
Airport Operations Data Centre
Perimeter Security
Local Roads
Baggage Handling & Sorting
Baggage Screening
Best Practices, Guidelines
INTERNATIONAL ORGANIZATIONS
IATA
ICAO
International Pax Regulations (Chicago Convention)
ISMS / ISO Standards
EU ORGANIZATIONS
European Commission (EC)
EASA
EUROCONTROL
European Data & Information Management and Distribution
Regulations
NATIONAL GOVERNMENT
National CAAs
Border Control
National Air Space Management
Planning, Governance
LOCAL GOVERNMENT
Transport Authorities
Planning Authorities
Local Communities
Planning, Procurement
Businesses, Service Provision
INDUSTRY
Third Party Providers
Industry / Manufacturers
Network Service Providers
ADS-B, Ground Stations (VHF, VDML), Beacons, GPS
Services Experience
PASSENGERS / TRAVELERS
Passenger Safety
Aircraft Manufacturers
Airline Operations Centre
Central Flow Management Unit
ATM Information Management
Network Security Management Services
Equipment Suppliers
Floor-Space Management
Consulting Services
Airport Administrative Duties
Building Maintenance
Legal and Financial Services
National Rail, Underground, Bus and Highways
Airport Management and Operations Database
Airport IT Infrastructure (LAN, WAN, Wireless)
NETWORKING LAYER
VHF, VDML Voice and Datalink ADS-B, ACARs (Flight Tracking)
Host IT Infrastructure (LAN, WAN, Wireless, Secure Networks)
Cable Infrastructure
Fiber Optic Infrastructure
PHYSICAL LAYER
Radar
Beacons and Ground Stations

Figure 4: Airport Stakeholders and Interactions

2.4 User experience in Smart airports: the end-to-end passenger journey

Smart airport is seen principally as technology or IT systems that connect the airport and the passenger. This covers a number of different smart systems that support the end-to-end passenger journey. Cisco (2009)[32] provides a detailed map of the end-to-end passenger journey that starts from the home and finishes with the arrival at the destination: as illustrated in Figure 5, *End-To-End Passenger Journey*. Their report suggests that airports, airlines and other stakeholders "can provide a superior passenger experience by taking an integrated approach to every touchpoint along the passenger journey".[33]

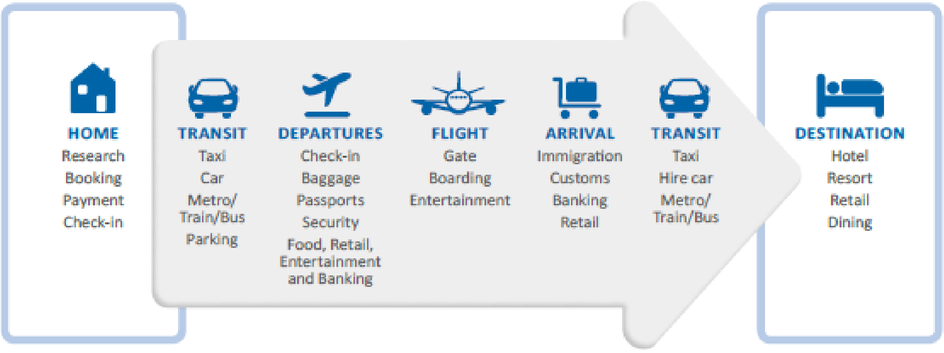


Figure 5: End-to-End Passenger Journey (source: CISCO 2009)

[32] CISCO, "Smart Airports: Transforming Passenger Experience to Thrive in the New Economy", http://www.cisco.com/c/dam/en_us/about/ac79/docs/pov/Passenger_Exp_POV_0720aFINAL.pdf.
[33] Ibid.

Indeed, smart technology is perceived as the means towards innovation and the improvement of customer experience, personalisation of services, targeted information flow (to the right people at the right time) and interactive services through the use of physical IT infrastructures, such as beacons, sensors, wireless infrastructure and mobile applications. At a technology level, this could mean automated passenger announcements or updates linked to data within the Flight Information Display System(FIDS) or the use of Near Field Communication (NFC) to allow passengers to interact with their choice of travel providers at every stage of their journey. At a higher level, this indicates a full focus on the end-to-end passenger journey, involving many interacting services.[34] Any activity that automates management of airport business in relation to the processing of passengers can be defined as a characteristic of the Smart airport, that either supports the decision-making process through the provision and acquisition of up-to-date data or facilitates automated processes that reduce manual actions and prevent human error.[35]

In order to support an end-to-end passenger journey experience, system integration is paramount. This allows all applications that are crucial to the operations of the airport to co-ordinate and share information amongst themselves. The concept of SWIM (System-Wide Information Management)[36] and Airport Collaborative Decision Making (CDM)[37] cover a complete change in paradigm for how information is managed and shared across the whole European ATM system.[38] This is underpinned by the circularity of information or data exchange among key stakeholders involved in air traffic navigation, including EU organisations (i.e., EUROCONTROL Network Manager)[39], airport operators (i.e., Airport Operation Centre and Air Traffic Control), airlines (i.e., Airline Operation Centre and aircraft) and airport providers (i.e., air navigation service providers, ANSPs). This shows the interdependencies between systems and sub-systems, which are crucial to managing airspace (reflected by the Single European Sky, SES) and the control and management of airport operations. This type of systems integration is facilitated by directly linking digital systems or infrastructure together (through shared services) or by forming a common data or information pool that is accessible and updated regularly in real-time. The results are common infrastructures that facilitate collaborative decision-making between a disparate federation of critical infrastructure owners and operators to ensure the continuity of service at airports, and efficiency in the management of airspace that extends to service providers beyond the airport.[40] Aeronautical Radio Incorporated (ARINC, 2015)[41] also discusses system integration among key stakeholders as an important feature of the Smart airport with collaboration enabled technology implemented across business units and functional silos through the utilisation of centralised and shared service strategies. The result is a set of information and data systems that are accessible to key stakeholders within the airport but also outside service operators and in some cases, passengers.

[34] CISCO has identified several smart service' categories, focused on the passenger journey, such as transport and parking, the processing of passengers through the airport and bespoke business to business services. See: CISCO, "Smart Airports: Transforming Passenger Experience to Thrive in the New Economy", http://www.cisco.com/c/dam/en_us/about/ac79/docs/pov/Passenger_Exp_POV_0720aFINAL.pdf.

[35] Ibid.

[36] SWIM, http://www.sesarju.eu/sesar-solutions/swim and http://www.eurocontrol.int/swim.

[37] Airport operations plan (AOP) and its seamless integration with the network operations plan (NOP), http://www.sesarju.eu/sesar-solutions/high-performing-airport-operations/airport-operations-plan-aop-and-its-seamless

[38] Further development in remote towers and their implementation will further strengthen this trend. See: http://www.sesarju.eu/programme/highlights/releasing-remote-towers

[39] The second regulatory package on the European Commission's Single European Sky (SES II) presented the creation of a Network Manager as a centralised function for the European Union. The Network Manager would manage air traffic management network functions (airspace design, flow management) as well as scarce resources (transponder code allocations, radio frequencies), as defined in Commission Regulation (EU) N° 677/2011.

[40] Ibid.

[41] ARINC (2015) *SMART Airports: Connecting airport, airline and aircraft.*

2.5 Safety, security and cyber security in airports

Over the past 15 years, airport safety and security have undergone significant change. Physical security controls and passenger screening have experienced substantial reform and cyber security has become an increasingly important aspect, as illustrated in Table 1 with the list of recent cyber security related incidents involving airports. These changes have simultaneously opened up opportunities for improving cyber security and safety (i.e. proper network integration can improve cyber security, while CDM can also enhance cyber situation awareness and safety) while increasing security and safety risks. The UK's Centre for the Protection of National Infrastructure (CPNI) produced a report in 2012 on cyber security in civil aviation[42]. The report noted that cyber security is an increasingly important issue. Reasons cited for this increased risk were:

- Security is not currently covered by safety management
- Aviation is increasingly making use of new and unfamiliar technologies
- IT systems are becoming increasingly interconnected; this exposes operators to risks in other people's systems.

CPNI provides also a concise summary of the cyber security issue in aviation, directly linking cyber security to safety:

"Cyber security is an issue because many civil aviation organisations rely on electronic systems for critical parts of their operations, and for many organisations their electronic systems have safety-critical functions."[43]

Particular to cyber security, risks constantly change as new threats and vulnerabilities surface along with ever-changing technology implementations. It is no longer possible to be truly safe without also being secure. This means that cyber security has a major stake in providing safety. The challenge is to address security issues not only to enhance security but also to ensure safety. ENISA works to develop cyber security for safety. Safety does not integrate security, and especially cyber security is not well integrated in organisations. For this reason, ENISA has decided to perform this study with the aim of helping asset owners and all stakeholders involved to enhance cyber security for the safety of European passengers.

2.6 Cyber security in Smart airports

Smart airports have the potential to deliver important improvements in overall security effectiveness, operational efficiency and passenger experience and safety. When electronic devices are used, for example to collect and monitor data relating to landside, terminal and airside activities at the airport, and these systems become connected following a Total Airport Management (TAM) concept[44], the airport can benefit not only from increased passenger safety and greater operational efficiency but also from an embed system of truly Collaborative Decision-Making (CDM)[45], based around real-time information that is shared across different actors. However, the increased flow of information, data processing and connections among devices and systems also bring risks that airport operators, policy makers, vendors, airlines and third party entities engaged in the provision of airport services need to address. These risks include vulnerabilities in ICT and electronic systems as well as the information and data held and processed by such systems. Vulnerabilities can be exploited by malicious actions, but also human errors, system or third party failures and natural phenomena. The cyber security threats to Smart airports are detailed in the following chapter.

[42] CPNI (2012) Cyber-security in Civil Aviation, http://www.cpni.gov.uk/documents/publications/2012/2012020-cyber_security_in_civil_aviation.pdf.
[43] Ibid.
[44] Total Airport Management: a Step Beyond Airport Collaborative Decision Making, https://www.eurocontrol.int/eec/public/standard_page/EEC_News_2006_3_TAM.html.
[45] Airport Collaborative Decision Making, http://www.eurocontrol.int/articles/airport-collaborative-decision-making-cdm.

3. Key asset groups and assets

Tackling cyber security starts from asset identification and decomposition[46]. In this chapter is provided an overview of the key asset groups and assets to be protected in Smart airports. In the ACRP Guidebook on Best Practices for Airport Cyber security - Appendix B[47], cyber security-relevant airport assets and systems are listed. Based on ACRP's work and insights from experts, we have identified the following as the key asset groups in Smart airports: *Landside Operations, Airport Administration, Staff Management, Customer Ancillary Services, Facilities and Maintenance, Passenger Management, Airline/Airside Operations, Safety and Security,* and *IT and Comms Systems.* Table 3 shows these key asset groups together with their locations within the airport. It is worth noting that there are some systems that are located across several locations and also outside the physical perimeter of the airport.[48] Specifically, Safety and Security spans multiple locations within the airport and is identified here as a cross-location asset group. IT & Communication Systems is also a cross-location asset group, while it also located inside and outside the physical perimeter of the airport. These are reflected by *External IT and Comms*, whose ownership and control is exercised by entities other than the airport authority or operator, and Internal IT and Comms, which are owned and operated by the airport authority, operator, or by airlines and other third parties within the physical airport perimeter.

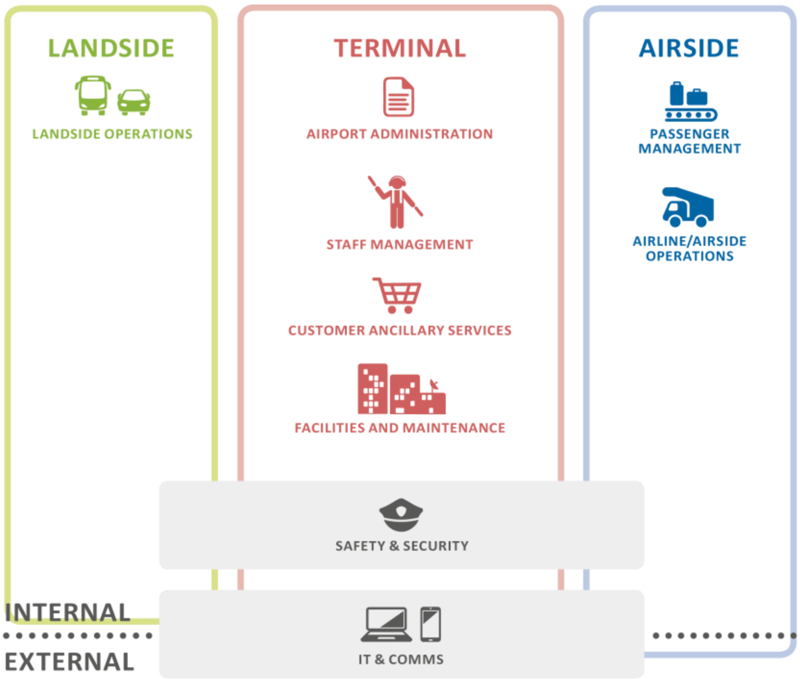


Table 3: Airport Core Asset Groups

[46] Many assets could be further decomposed into components and sub-processes, and the categorisation here attempts to strike a balance between covering key significant categories and relevant detail.
[47] Guidebook on Best Practices for Airport Cyber security (ACRP 140, 2015), Appendix B.
[48] The scope of the Smart airport perimeter, in the context of cyber security, includes internal assets that are controlled and operated by entities within the airport and located within the perimeter of the airport, and also external assets that are to a large extent controlled and operated by an entity other than the airport operator or authority. Most of these external assets reflect the navigation and communication between the aircraft and the airport itself, through intermediaries that collect and distribute the information to interested parties affected by the flight path and trajectory of the aircraft.

3.1 Smart airport assets

Based on the asset groups identified in Table 3, key smart assets for each of the groups were identified and validated with experts. Smart assets include both primary and secondary assets as categorised by ISO 27005[49]. These assets are either owned and operated by the airport authority or outside service providers. Primary assets are usually the core processes and information that underpin key airport activities. Normally primary assets include business processes and activities, and information. Accordingly, secondary assets are defined as those assets upon which the primary elements rely. These assets have vulnerabilities that are exploitable by cyber security threats aiming to impair the primary assets – processes and information. They include all types of deployable systems that allow an airport to carry out its primary functions such as hardware, software, network, personnel, and site.

Figure 6 presents the full MINDMAP of the key asset groups and assets of the 'Smart' airport as identified through the expert interviews and desktop research. All assets in the figure are 'smart' components and are important to the functioning of the Smart airport. To further validate the criticality of the assets we present in Figure 7 their prioritization according to the experts. We have collected their views on the top five most critical assets, in the sense that they deem them particularly important and representing the top priorities for cyber security.

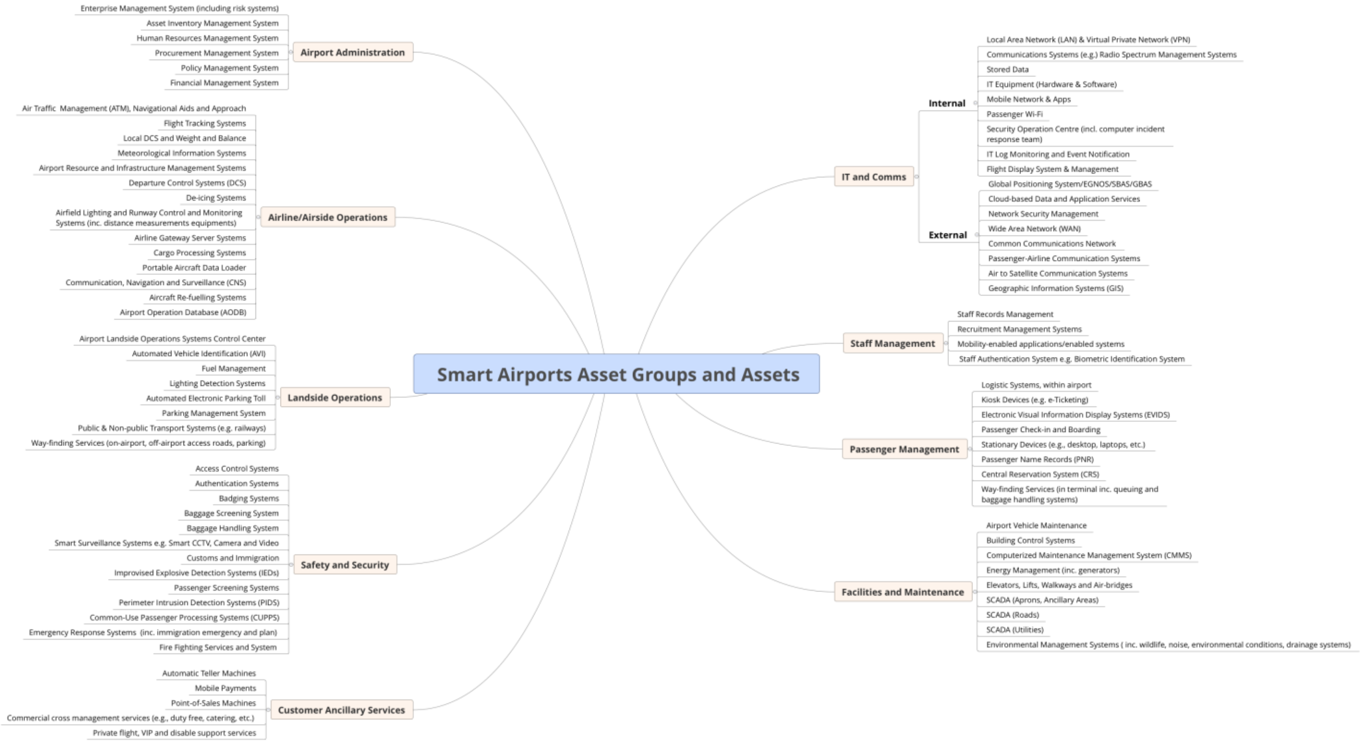

Smart Airports Asset Groups and Assets
Airport Administration
Enterprise Management System (including risk systems)
Asset Inventory Management System
Human Resources Management System
Procurement Management System
Policy Management System
Financial Management System
Airline/Airside Operations
Air Traffic Management (ATM), Navigational Aids and Approach
Flight Tracking Systems
Local DCS and Weight and Balance
Meteorological Information Systems
Airport Resource and Infrastructure Management Systems
Departure Control Systems (DCS)
De-icing Systems
Airfield Lighting and Runway Control and Monitoring Systems (inc. distance measurements equipments)
Airline Gateway Server Systems
Cargo Processing Systems
Portable Aircraft Data Loader
Communication, Navigation and Surveillance (CNS)
Aircraft Re-fuelling Systems
Airport Operation Database (AODB)
Landside Operations
Airport Landside Operations Systems Control Center
Automated Vehicle Identification (AVI)
Fuel Management
Lighting Detection Systems
Automated Electronic Parking Toll
Parking Management System
Public & Non-public Transport Systems (e.g. railways)
Way-finding Services (on-airport, off-airport access roads, parking)
Safety and Security
Access Control Systems
Authentication Systems
Badging Systems
Baggage Screening System
Baggage Handling System
Smart Surveillance Systems e.g. Smart CCTV, Camera and Video
Customs and Immigration
Improvised Explosive Detection Systems (IEDs)
Passenger Screening Systems
Perimeter Intrusion Detection Systems (PIDS)
Common-Use Passenger Processing Systems (CUPPS)
Emergency Response Systems (inc. immigration emergency and plan)
Fire Fighting Services and System
Customer Ancillary Services
Automatic Teller Machines
Mobile Payments
Point-of-Sales Machines
Commercial cross management services (e.g., duty free, catering, etc.)
Private flight, VIP and disable support services
IT and Comms
Internal
Local Area Network (LAN) & Virtual Private Network (VPN)
Communications Systems (e.g.) Radio Spectrum Management Systems
Stored Data
IT Equipment (Hardware & Software)
Mobile Network & Apps
Passenger Wi-Fi
Security Operation Centre (incl. computer incident response team)
IT Log Monitoring and Event Notification
Flight Display System & Management
External
Global Positioning System/EGNOS/SBAS/GBAS
Cloud-based Data and Application Services
Network Security Management
Wide Area Network (WAN)
Common Communications Network
Passenger-Airline Communication Systems
Air to Satellite Communication Systems
Geographic Information Systems (GIS)
Staff Management
Staff Records Management
Recruitment Management Systems
Mobility-enabled applications/enabled systems
Staff Authentication System e.g. Biometric Identification System
Passenger Management
Logistic Systems, within airport
Kiosk Devices (e.g. e-Ticketing)
Electronic Visual Information Display Systems (EVIDS)
Passenger Check-in and Boarding
Stationary Devices (e.g., desktop, laptops, etc.)
Passenger Name Records (PNR)
Central Reservation System (CRS)
Way-finding Services (in terminal inc. queuing and baggage handling systems)
Facilities and Maintenance
Airport Vehicle Maintenance
Building Control Systems
Computerized Maintenance Management System (CMMS)
Energy Management (inc. generators)
Elevators, Lifts, Walkways and Air-bridges
SCADA (Aprons, Ancillary Areas)
SCADA (Roads)
SCADA (Utilities)
Environmental Management Systems (inc. wildlife, noise, environmental conditions, drainage systems)

Figure 6: Mapping Smart Assets and Asset Groups of the Airport

To facilitate information security professionals in their risk assessment, the complete list of assets is available as an annex of the present document. The goal is to give the interested parties an input regarding the

[49] It outlines the international standard for managing information security risk that provides a framework for the identification of smart assets (based on the criteria above) for the Smart airport. See: ISO/IEC (2011) ISO 27005 Information technology – Security Techniques – Information Security Management.

possible assets to envision that they can they later tailor based on the size and characteristics of their airport infrastructure.

In the following table it is proposed a view of the assets based on the priorities defined by the subject matter experts during the interview. This table can give an overview of the most critical assets for the 20 organisations across eight countries that provided feedback for the present report.

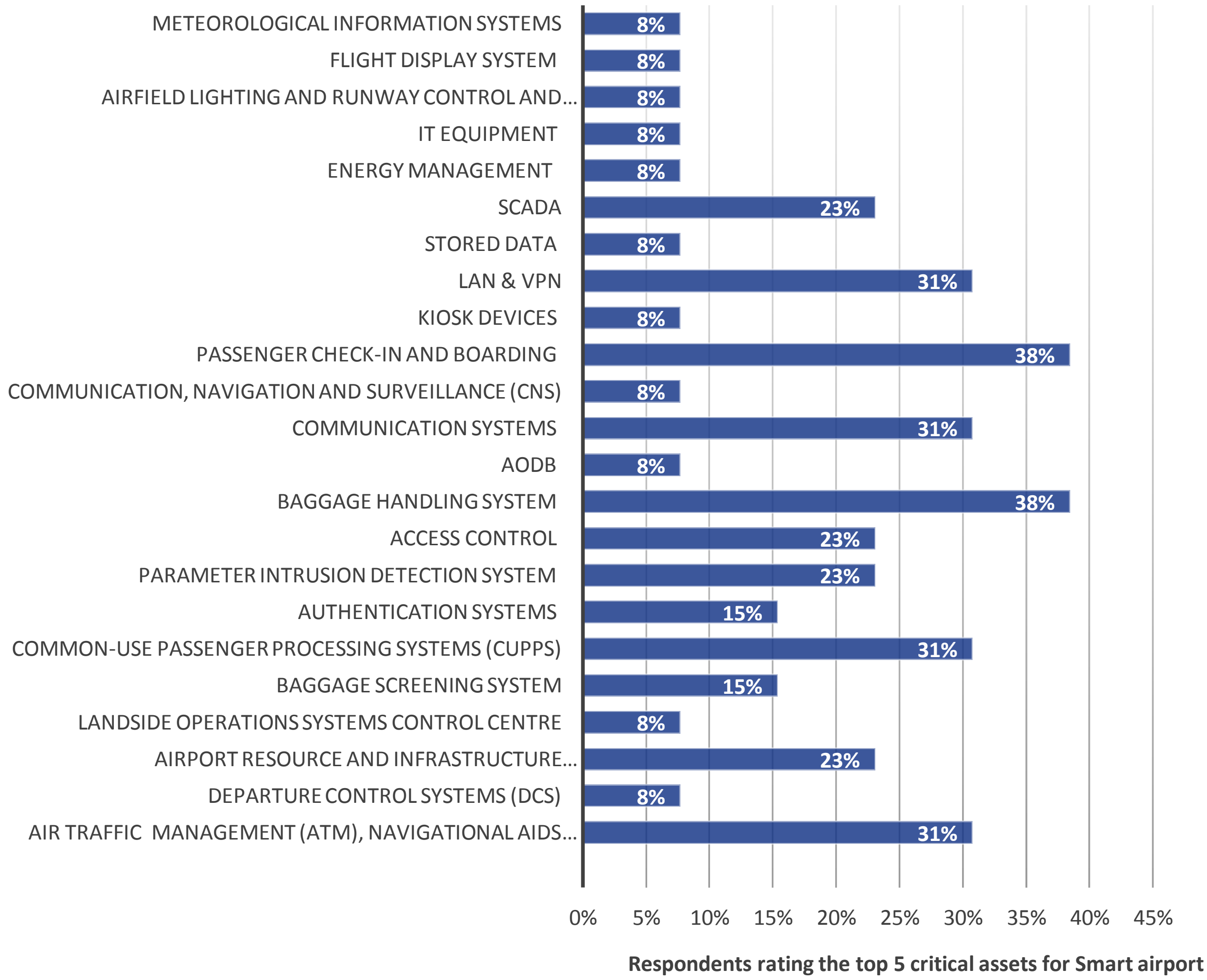


Figure 7: Prioritised Assets

4. Threat and risk analysis

4.1 Emerging challenges in smart airports

The Airport Cooperative Research Program (ACRP, 2015)[50] has identified a trend toward greater interconnectivity as airports and their stakeholders leverage digital technology to optimise resources and work together more efficiently. Airports are also becoming increasingly reliant on computer services delivered via Internet, with some airports allowing passengers and staff to use their own hardware (smart phones, tablets and computers/laptops) to access airport data, systems and network resources.

A report by the UK Centre for Protection of National Infrastructures (CPNI) identifies the consolidation of IT systems and Internet-based solutions in civil aviation management and operation as a major reason for increased vulnerability to malicious cyber security attacks. The report suggests that "Interconnected and interdependent systems are becoming more prevalent in commercial aviation, increasing the possibility that different operators inside and outside the airport become exposed to risks caused by security weaknesses in other people's systems".[51] Indicatively, SESAR system-wide information management (SWIM)[52], once deployed, will allow all aviation sectors to access the data they require to undertake their role, clear in the knowledge that it is consistent with the data being used by different actors. However, SWIM was not designed with mechanisms that integrate cyber security requirements.[53]

An additional challenge arises from the use of open and unencrypted communication capabilities, such as communication of routine air traffic commands between air traffic control and the aircraft. This introduces further vulnerabilities that can cause rise to cyber attacks and subsequently can risk the safety and performance of civil aviation.

4.2 Threat analysis

This Section presents a taxonomy of threats to the cyber security of Smart airports, including mapping to Smart airport assets. The threat taxonomy focuses on cyber security aspects with relevance to Smart airports, many of which also generalise to any IT systems. The taxonomy was developed drawing on findings from the interviews and desktop research. Previous ENISA reports have also been employed as a basis for the taxonomy (including ENISA *Threat Landscape and Good Practice Guide for Internet Infrastructure 2015*[54], and ENISA *Study of IPT and smart grids in 2016*[55]).

A taxonomy of cyber security threats to smart components within the airport perimeter is presented, followed by the attack vectors and actors involved. The threats are mapped to categories of assets they

[50] Airport Co-operative Research Program (2015)

[51] CPNI (2012) Cyber-security in Civil Aviation, http://www.cpni.gov.uk/documents/publications/2012/2012020-cyber_security_in_civil_aviation.pdf?epslanguage=en-gb.

[52] "The 2016 SESAR SWIM Global Demo shows that system-wide information management (SWIM) is no longer a concept on paper, but is progressively becoming a reality that will propel aviation into a new era of global connectivity", http://www.sesarju.eu/newsroom/all-news/global-partners-deliver-digitised-and-connected-aviation.

[53] To cope with these emerging vulnerabilities enhanced System Monitoring and Control (SMC) and technical supervision become paramount together with health status checks, predictive capabilities, machine learning and pattern recognition based on operational baselines. See: http://www.gamma-project.eu.

[54] ENISA, ENISA *Threat Landscape and Good Practice Guide for Internet Infrastructure*, European Network and Information Security Agency, Heraklion, January 2015, https://www.enisa.europa.eu/publications/iitl.

[55] ENISA, *ENISA Threat Landscape 2013: Overview of current and emerging cyber threats*, European Network and Information Security Agency, Heraklion, 11 December 2013. http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats.

relate to. Finally, specific attacks are highlighted against target elements, illustrating the threats to Smart airport assets.

4.2.1 Threat taxonomy

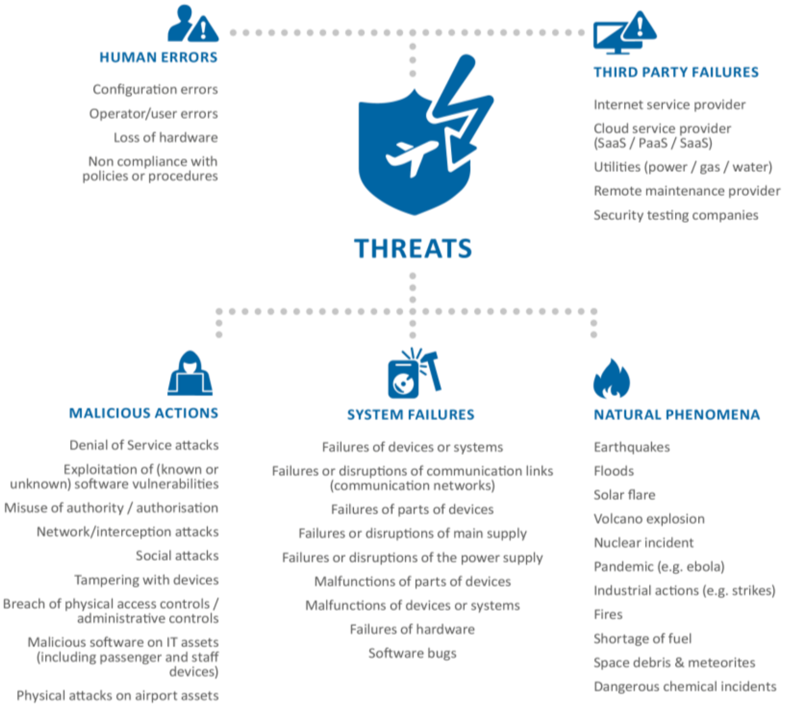

HUMAN ERRORS
Configuration errors
Operator/user errors
Loss of hardware
Non compliance with policies or procedures
THIRD PARTY FAILURES
Internet service provider
Cloud service provider (SaaS / PaaS / SaaS)
Utilities (power / gas / water)
Remote maintenance provider
Security testing companies
THREATS
MALICIOUS ACTIONS
Denial of Service attacks
Exploitation of (known or unknown) software vulnerabilities
Misuse of authority / authorisation
Network/interception attacks
Social attacks
Tampering with devices
Breach of physical access controls / administrative controls
Malicious software on IT assets (including passenger and staff devices)
Physical attacks on airport assets
SYSTEM FAILURES
Failures of devices or systems
Failures or disruptions of communication links (communication networks)
Failures of parts of devices
Failures or disruptions of main supply
Failures or disruptions of the power supply
Malfunctions of parts of devices
Malfunctions of devices or systems
Failures of hardware
Software bugs
NATURAL PHENOMENA
Earthquakes
Floods
Solar flare
Volcano explosion
Nuclear incident
Pandemic (e.g. ebola)
Industrial actions (e.g. strikes)
Fires
Shortage of fuel
Space debris & meteorites
Dangerous chemical incidents

Figure 8: Threat Taxonomy

Figure 8 illustrates a two-level threat taxonomy, based on root causes, including human errors, system failures, natural phenomena, third party failures, and malicious actions. Annex 3 includes an expanded diagram of the taxonomy, which provides a three-level categorisation of malicious attacks.

- **Malicious actions:** Many cyber security threats are the result of malicious actions. Various methods can be used by those with malicious intent to compromise IT assets or to perform elevation of privilege attacks (where the attacker ends up with a different level of access). Each of these attacks often leads to risk of breach of confidentiality, integrity, availability and should be considered in terms of the available attack vectors for each asset in order to protect the safety and capacity of an airport (discussed in Section 3.2.2). For the purposes of this report, major technical threats against Smart airports have been summarised into nine categories:
    - **Denial of Service**: Denial of service (DoS) attacks impact on system availability and can enable well equipped attackers to disrupt all but the most resilient of systems and networks. Jamming devices can overshadow various kinds of wireless communications, such as Wi-Fi, and mobile telephony, and ATM signals. Denial of service poses something of a challenge for network architecture, including Smart airports where protection against mass DDoS may not be in place. Consequences can include network outage, security check slow down, passenger delays, cancelled flights, loss of confidence, damages to reputation, and/or financial damage.
    - **Exploitation of software vulnerabilities**: Vulnerabilities may exist in Smart airport systems, including security issues that the vendors of the IT/smart assets are unaware of, or issues for which a fix has been

created but not applied to the airport's systems. Any Smart airport systems with an available attack surface that are not running with all the latest security patches are likely targets, and even systems for which no security issues are known may be the target of sophisticated attacks7.

- **Misuse of authority / authorisation**: Attackers may be in possession of credentials and/or authorisation, and may misuse their privilege. Examples of attacks to gain this level of access include credential theft via social engineering, such as spear phishing against airport personnel, or simply insider threats. Once an attacker has gained a privileged level of access and/or holds a legitimate user's credentials (which can also be the result of software exploitation, network interception attacks, or malware), the attacker will be in a position to misuse the privileges, and the damage potential on the Smart airport depends on the level of privilege obtained.

- **Network/interception attacks**: Attacks can be network-based or focused on interception (including physical tampering). This includes wiretaps, and physical tampering (including keyloggers, or internal modification of assets). Depending on the attack surface and controls in place, networks or physical devices in Smart airports may be the target of tampering or network attacks which could enable attackers to compromise systems or communications.

- **Social attacks:** Social engineering attacks manipulate people into divulging information or performing actions on behalf of the attacker**Error! Bookmark not defined.**. Social attacks are effective as they ircumvent technical and physical controls. Airport employees who are not adequately security aware and trained on these issues, or who do not follow procedures can pose a significant risk to airport cyber security; as the attackers may gain full access to the victims' accounts, identity, and authorisation[12].

- **Tampering with airport devices:** This threat is that systems are tampered with in unauthorised ways. Unauthorised modification includes data at rest, such as writing to central reservation systems (CRS), passenger name records (PNR), airport administration IT solutions (including enterprise and human resources management systems), or stored sensor data. The threat of tampering also includes unauthorised modification of hardware or software, including modification of the behaviour of kiosk devices (such as insertion of keyloggers or modification of firmware), or any IT and communications systems. Data deletion or corruption is also another related threat. Tampering can have severe consequences, as attackers can potentially gain complete control over systems, and can result in malicious behaviour which can directly lead to breaches in physical safety and have an impact on accountability and authentication.

- **Breach of physical access controls / administrative controls:** This threat refers to a failure in the verification of identity or authorisation. Breaches in authentication includes identity fraud, such as impersonating a legitimate airport staff member, and breaches of physical access controls or administrative controls, such as an attacker bypassing an authentication check, thereby gaining access to a new attack surface (different systems they can interact with).

- **Malicious software on IT assets**: Malware may become present on end user devices, including passenger and staff devices, servers, or other smart components, such as sensor nodes or Supervisory Control and Data Acquisition (SCADA) systems. Malware can cause severe impact on infrastructure, and business as the software acts maliciously, misusing its ambient authority on the computer it runs on. Malware often propagates to systems via social engineering (tricking the user to action): for example, by sending phishing emails to victims (spear phishing is where the attack is targeted). Malware can also spread via direct exploitation of software vulnerabilities (not requiring user interaction), or through the tampering of devices. [56]The degree of harm malware is likely to cause to Smart airports is dependent on whether the malware is targeted and launched by an advanced attacker, or simply has opportunistically or automatically infected airport systems, and the motivation of the attacker.

  - **Physical attacks on airport assets:** This threat is that an incident can result in physical damage to assets or other stakeholders, including passengers or bystanders. This includes explosives, sabotage, and vandalism. Much of traditional airport security is focussed on physical safety; however, in terms of cyber security, this also includes physical attacks on airport smart assets (such as theft of damage of airport IT infrastructure) or control of assets resulting in damage.

- **Human errors:** Another major category of threats are those caused by human error. Administrative IT personnel or network administrators may make configuration errors that negatively impact operations or security. For example, configuration errors can lead to administrator defined secure passwords not being set on devices before they are deployed. The impact of which can include system downtime, cancelled flights, or introducing major security weaknesses. Similarly, end users, such as airport personnel, can inadvertently introduce errors into systems, by entering incorrect information or data. Lost hardware, such as laptops containing sensitive data or authentication details (passwords, or VPN certificates) can introduce vulnerability and lead to subsequent attacks. Policies and procedures should be designed to avoid inappropriate actions that increase risk; however, personnel may inadvertently not correctly follow these due to insufficient awareness, negligence, or when falling victim to previously mentioned social engineering attacks.

- **System failures**: Failures and malfunctions also have a cyber security element, as they can impact on the security posture and operational capacity of the airport. Failures include parts of devices, devices or systems, disruptions of communication links, disruptions of main supply, disruptions of service providers, disruptions of the power supply[6], failures of hardware, and software bugs.

- **Natural and social phenomena:** Natural and social phenomena, such as earthquakes, extreme weather (e.g. flood, heavy snow, blizzard, high temperatures, fog, sandstorm), solar flare, volcano explosion, nuclear incidents, dangerous chemical incidents, pandemics, social disruptions (e.g. civil unrest, strikes, military actions, terrorist attacks, political instability) impacting airport operations, shortage of fuel, and space debris and meteorites can impact the systems supporting critical business functions, and therefore pose a threat to cyber security to Smart airports.

- **Third party failures:** Third party service providers play a critical role in Smart airport operations. For example, Internet-based smart technologies can rely on cloud service providers, Internet service providers, and utilities (including power). Also, management or maintenance of IT systems may be outsourced to third-party remote maintenance providers. Any service interruptions by external third-party providers impact on those business functions, e.g. recent incident at the airport of Rome[9].

4.2.2 Threat modelling

In order to reason about security, it is helpful to clearly define the threat actors (who the potential attackers are) and potential attack surfaces (how they can interact). Each of these threat actors have different attack surfaces available within Smart airports. Threat actors in airports include:[57]

- **Insider threats**: These are airport staff (any role) with malicious intent. Many staff members have access to otherwise restricted areas, access to restricted IT systems, direct access to interconnected devices and

[56] Blended attacks that use a mix of techniques such as firmware modification, VOIP DoS, HMI attacks ,etc. could be also Included in this groups.

[57]ACRP, Guide Book on Best Practices for Airport Cyber Security, 2015.

networks, and may be subject to lower levels of scrutiny. These actors require authorisation to carry out their duties, yet may misuse their authority and may have more authority than they require. As a consequence, the attack surface is the largest for these attackers.

- **Malicious airport passengers and guests**: These attackers are physically present within the Smart airport. They have restricted access to physical areas (unless controls are circumvented).
- **Remote attackers**: These attackers are not physically present within the Smart airport, and include automated attacks, such as malware, and targeted attacks such as advanced persistent threats (APT). This limits these actors to remotely available attack vectors (but could also include remotely compromising legitimate staff or passengers' devices).
- **Other causes**: Environmental or accidental equipment/software failure can cause security incidents, yet have no active attacker.

Potential attack surfaces in airports include:

- **Physical interaction with IT assets**: Physically present attackers (insiders or passengers/guests) can directly interact with devices that they have access to. For example, an attacker can type into Common Use Passengers Processing System (CUPPS) ticketing kiosks using the provided interface (potentially exploiting vulnerabilities in the software), or may attempt to insert USB devices, if a port is available, or may physically tamper with a ticket machine to capture or modify input, or to compromise the underlying computer. Likewise, a physically present attacker may install a keylogger on a staff PC to capture passwords and other inputs, or may simply approach a staff PC and begin interacting with it, potentially misusing the authority of a staff member. This applies to any smart assets the attacker can directly access.
- **Wireless communication with IT assets**: Attackers within range of the wireless technologies (potentially including remote attackers, depending on the technology), can interact with or receive wireless communications, including: Automated Vehicle Identification (AVI) and other Radio-Frequency Identification (RFID) based asset tracking systems, Wi-Fi, ground-based line of sight data-links, and Air Traffic Management (ATM) signals, such as ADS-B.
- **Wired communication with IT assets**: Attackers with wired network communications (including access to the Internet) can interact with related IT assets including cloud services, and online reservation systems. Attackers with physical presence may have direct access to network infrastructure (such as routers and switches, or CAT5 cables that can be tapped), which they can connect to in order to communicate with other connected smart devices.
- **Interaction with other staff or passengers**: Rather than directly target airport assets, attacks may be targeted at (or via) other staff or passengers. Reflected attacks (such as CSRF or reflected XSS) and social engineering attacks can involve fooling or convincing a person to send commands or carry out tasks on their behalf. Tampering with the environment, by inserting themselves into a position where they can intercept and modify communications is a typical attack vector: for example, man in the middle, man in the phone, or man in the browser, or by introducing rogue Wi-Fi access points.
- **Pivoting attacks between assets**: As an attacker compromises a system a new attack surface becomes available to them. For example, after compromising a publicly facing web server, the attacker may gain access to an internal network segment and may use the web server to attack the airport intranet local area network systems and/or disrupt the supply chain. Any smart asset that has the potential to be compromised is a potential attack vector for any other connected systems. Therefore, compromised systems can have cascading effects on overall airport cyber security

In the annex 4 “Asset exposure to cyber threats” the threat exposure of assets is presented. The threats to airport cyber security apply to broad categories of assets, such as communication networks, servers and control systems, internal/sensitive information, authentication and access control systems, and end-point systems (which include PCs, laptops, tablets, smartphones and other external installations, such as e-ticketing devices). The next Section gives more detailed examples of specific Smart airport infrastructure assets that can be targeted by specific attacks.

4.2.3 Sample cyber security attacks

Table 4 illustrates a few samples of threats (previously described Section 4) and how they relate to airport assets (described in Section 2), in terms of specific target elements and attacks. This list of examples highlights likely attacks and is based on desktop research and expert interviews. The good practices section list the relevant good practices collected in chapter 5 “security good practices”.

Table 4: Sample Cyber security Attacks

ASSET: TARGET ELEMENT	*THREAT:* ATTACKS	GOOD PRACTICES
Airport Administration: Enterprise Management System	*Social attacks:* Personnel with access to highly sensitive data, such as administrator authority to the enterprise management system, e.g. enterprise resource planning (ERP) software, are at heightened risk of social engineering spear phishing attacks. Attackers create realistic and incentivised scenarios, targeted to employees (such as by impersonating co-workers). For example, sending a link to a convincing fake website requesting existing credentials; the attacker can then leverage those credentials to gain control of enterprise management systems.	GP01, GP11, GP13, GP14, GP33,GP34
Airline/Airside Operations: ATM navigation communications	*Network / interception attacks:* ADS-B ATM and older radio ATM technologies are typically unauthenticated, meaning that a well-equipped attacker can broadcast messages or overshadow existing signals. Similarly, GPS, which aids navigation and positioning, is vulnerable to untruthful signals, which can maliciously alter positioning.	GP3, GP10, GP11, GP12, GP26, GP27, GP28, GP33, GP34, GP41, GP42, GP43, GP44
Landside Operations: Airport Landside Operations Systems Control Centre	*Misuse of authority / authorisation:* Personnel with high levels of access are also high risk insider threats. For example, personnel misusing their authority in the landside operations systems control centre could misuse their authority to send malicious commands to SCADA systems.	GP05, GP09, GP16, GP24, GP29, GP30, GP31, GP32
Safety and Security / Passenger Management: Common Use Passengers Processing System (CUPPS) central reservation system (CRS) and ticketing kiosks	*Tampering with airport devices:* Common Use Passengers Processing System (CUPPS) self-service ticketing kiosks are located in public spaces, are operated by various airlines, and are subject to tampering attacks, and software or authentication errors that can result in boarding passes incorrectly produced or provided to the incorrect person. If CUPPS is compromised, central reservation system (CRS) and passenger name records (PNR) could potentially be affected, which can cause data leakage or service outage. A compromised system such as this also grants the attacker	GP02, GP05, GP07, GP08, GP09, GP10, GP11, GP12, GP13, GP15

	with access to internal networks for further penetration attacks.	
Safety and Security: Baggage Screening Systems	*Network / interception attacks:* Wi-Fi is used extensively in many airports, from passenger Internet access, to various business functions. Insecure Wi-Fi networks have been demonstrated to exist in airports, including insecure networks for operations such as baggage scanning systems.[58] Attackers can gain access to insecure Wi-Fi networks (for example, cracking WEP) and begin to interact with systems on the network, such as launching further attacks on baggage tracking systems.	GP02, GP04, GP05, GP08, GP10-GP13, GP16-GP25, GP27, GP28, GP33-GP44
Customer Ancillary Services: Point-of-Sales Machines	*Malicious software on IT assets:* Malware can potentially infect any device, though malware is often found on end-point systems. Point-of-Sales (POS) systems are often the target of malware attack, and malware exists that targets these systems, often resulting in fraudulent transactions.[59] When any devices are infected by malware (such as POS in smart airports) any shared network infrastructure can enable infected systems to attack and compromise connected systems, resulting in remote command and control over critical infrastructure.	GP01-GP06, GP11-GP25, GP27, GP28, GP33-GP44
IT and Comms: Passenger Wi-Fi	*Network / interception attacks:* Attackers can intercept, modify and replay passenger Wi-Fi signals. Attackers can create rogue access points, by posing as a legitimate Wi-Fi networks. On insecure Wi-Fi networks attackers can use session hijacking attacks to take control of passengers' online identities or alter booking requests.	GP02, GP04, GP05, GP08, GP10-GP13, GP16-GP25, GP27, GP28, GP33-GP44
IT and Comms: Cloud-based data and application services	*Denial of Service:* Airports are increasingly dependent on third party cloud-based IT services, such as office software, email, and data processing services.[60] Online services can be impacted by distributed denial of service (DDoS) attacks, which overwhelm servers with requests resulting in outage of service. DDoS may cause outage of staff systems, online reservation systems and other cloud-based services (such as SaaS, PaaS, or IaaS).	GP01, GP05, GP07, GP08, GP11, GP13, GP15-GP28, GP32-GP44
Facilities and Maintenance: SCADA (Apron)	*Exploitation of software vulnerabilities:* In recent years many security vulnerabilities (and attacks) have been discovered in industrial control systems (ICS) such as Supervisory Control and Data Acquisition (SCADA) and Programmable logic controller (PLC). Airports make extensive use of ICS systems for controlling baggage handling, airfield lighting control systems, HVAC, and Apron services.[61] ICS is sometimes	GP01, GP05-GP08, GP11, GP14, GP16-GP25, GP27, GP28, GP33-GP44

[58] Wireless vulnerability assessment – airport scanning report part II, http://www.mojonetworks.com/fileadmin/pdf/AirTight-Airport-Scan-Results-Part2.pdf.

[59] Attacks on point-of-sales systems, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/attacks_on_point_of_sale_systems.pdf.

[60] Guidebook on Best Practices for Airport Cybersecurity, http://onlinepubs.trb.org/onlinepubs/acrp/acrp_rpt_140.pdf.

[61] Cyber security for airports, http://www.ijtte.com/uploads/2013-12-30/5ebd908d-7f47-e96dIJTTE_Vol%203%284%29_2.pdf.

	connected directly to the Internet; however, vulnerable ICS may be attacked even when not connected to the Internet: via USB, infrared, or connected wired or wireless networks.[60] A successful attack typically results in the attacker gaining full control over the ICS device, and the ability to send malicious control commands.	

5. Attack scenarios

This study has identified three attack scenarios relevant to Smart airports based on current trends emerging from the desktop research and experts' insights. Indeed, the final three scenarios were selected based on the experts' recommendations taking into account which scenarios were identified by the majority of experts as the most relevant. These three attack scenarios have been identified by the interviewed experts as the most important in regards to security and resilience in Smart airports. The attack scenarios are presented in the following tables. For each of them, the table indicates: the type of attack; a more detailed description of the scenario; the domains where those scenarios have been or could be potentially applied; their likelihood; and the key users and stakeholders that actively take part in each scenario. Additionally, security parameters are mentioned such as cascading effects, recovery time and efforts, assets involved, and criticality. Finally, the table proposes which existing good practices could be deployed in each scenario in order to enhance security and resilience. The most specific and relevant good practices for the scenario are listed at the beginning followed by more generic good practices. The top five most relevant good practices for the scenario are presented in bold.

5.1 Tampering with airport self-serving e-ticketing systems

Self-service check-in systems are operated and shared by various airlines and located in public spaces. Where such kind of devices are unattended, physical access to these machines from a malicious user and/or attacker can be an easy task. Self-serving e-ticketing infrastructures are becoming more and more used and shared by multiple airlines, with third parties also starting to operate the service. This increases the complexity and connections of the self-serving check-in infrastructure. The majority of these devices run commonly used operating systems, such as (often obsolete versions of) Windows or Linux and kiosk ticketing software, which are installed in a custom hard-shell case. These devices usually leverage intranet connectivity in order to access content on company servers, and provide remote management functionalities. These devices may be subject to tampering attacks as they are in public spaces. Furthermore, the tempering attacks can be assisted or conducted by an insider, for instance an employee of the third- party provider in charge of operating the service. There are some tactics that insiders are likely to use in the course of preparing or conducting their attacks; this includes manipulation (access gained by manipulating external staff). Tampering may involve physically altering the hardware, such as gaining access to the contained PC via picking a lock on the side of the device or drilling/punching a small hole through the side of the device; or tampering with the interface between the passenger and the device by installing inconspicuous keyboard, reader, or screen overlays; or exploiting a software vulnerability. Successful tampering can then result in the attacker having unauthorised access to the machine and potentially lead to privilege escalation to super user root/administrator access of this machine. This enables the attacker to change the behaviour of the machine both in terms of the customer facing actions and the interactions with other connected systems. This can potentially allow the attacker to: access passenger boarding passes, print arbitrary boarding passes, invalidate and/or modify existing passenger passes (i.e. via record tampering) and steal sensitive passenger's data (i.e., passport or credit card details when these are used to initiate the check-in operation at the kiosk).

Criticality

Disruption of check-in services may create inconvenience to passengers (i.e., longer time for boarding) but it might also lead to more serious service outage and further security risks involving safety (e.g. it might assist with the boarding of unknown passengers into the plane).

Likelihood

Based on interviews' key findings, this was one of the most cited possible attack scenarios. Airline companies foster strongly the use of e-ticketing systems to speed up the check-in process via automation. This scale of popularity, combined with a low level of control of check-in devices within the airport, make them a very good/likely target for cyber-attacks. Unless these devices are equipped with the latest tamper-proof technology and/or readers that encrypt data, they are highly prone – given their public locations – to criminal tampering and are a perfect target for attackers. Exploiting software bugs as well as systems that are not often updated are seen by attackers as weak points to acquire access into check-in devices in order, for instance, to add or modify passengers' information.

Cascading effects

Once a check-in system is compromised the attacker can pivot from this device to attack connected systems and databases. Also, in addition to any interruption or black out on the whole system, a threat that arises here is the alteration of data aiming at whatever act that can compromise the safety of passengers, including potential terrorist acts. Although the majority of airports use segregated networks, depending on the effectiveness of the controls, cascading effects have the potential to impact on the entire Common Use Passenger Processing System (CUPPS).

Attack scenario

Type of Attack	Asset affected
Tampering with airport devices	• Self-service Check-in devices, and connected IT Comms • Network Security Management

CRITICALITY	LIKELIHOOD
Medium to High	Medium

CASCADING EFFECTS	STAKEHOLDERS INVOLVED
• Passenger Check-in and Boarding • Passenger Name Records (PNR) • Passenger-Airline Communications System (e.g., delays, disruption) • Local area network	• Passengers • Airline and Airport personnel • IT Support Services • Third party providers (If services managed by third party)

RECOVERY TIME AND EFFORTS	GOOD PRACTICES
Attacking check-in devices can compromise the whole chain of entities and processes involved in the e-ticketing system. Often third party providers will be involved in managing part of the service (e.g. local area network). This will require the whole chain to react to the attack by providing the effort needed to detect the flaw, and provide the solution to fix it.	• **GP 07 – Disable services, close ports, restrict usage of external devices** • **GP 10 – Data encryption** • **GP 01 – Intrusion Detection Systems (IDS)** • **GP 08 – Conduct vulnerability and penetration tests** • **GP 22 – Conduct risk assessments** • GP 06 – Operating systems updates and backups • GP 25 – Manage risk according to international standards and a methodological approach. • GP 26 – Require that providers of external information system services comply with airport information security requirements and/or be certified against relevant standards • GP 17 – Rely on an information security framework and external audits to assess maturity and demonstrate compliance • GP 23 – Create a risk registry and monitor risk effectively • GP 34 – Provide basic security awareness training to all information system users • GP 38 – Develop a contingency plan • GP 42 – Provide incident response capabilities for airports • GP 45 – Track and document information system security incidents

CHALLENGES AND GAPS

The degree of interconnection among physical devises (in our case the kiosk) and ICT systems as well as among systems is challenging since it opens up more vectors of attack for connected systems and entry gates to others (see Gap 8). Another key challenge lies in the effective and efficient monitoring of check-in devices and all their components (physical, hardware and software) due to the number of devices and spread and size of areas where they are located. In addition, as underlined in the gap section there is a gap in industry models and guidelines on airport network architecture, ownership, and remote management (see Gap 3). There are few guidelines and standards specifically addressing cyber security practices in Smart airports, in particular in relation to the security of shared infrastructures (software or hardware), which is usually the case for automated e-ticketing devices.

5.2 Network attack to the baggage handling

Airports make extensive use of ICS SCADA systems for baggage handling.[62] Most ICS advanced systems allow the centralisation of the baggage handling control and visualisation, display of the relevant data, control of the site CCTV systems giving the operators all the information required to confidently and remotely make their control decisions. SCADA are also becoming increasingly interconnected and interdependent with other airport information systems or airside systems, which may introduce additional vectors of attack. Because of this interconnectivity, ICS SCADA systems are exposed to similar vulnerabilities as computers and networked devices. Specifically, weak network security (e.g. poorly configured firewalls, interconnected peer networks, weak authentication features, etc.) often combined with SCADA running old or not updated/unpatched out-of-date software, allow attackers to open a backdoor and exploit weaknesses in these systems: for example, a software vulnerability may enable the attacker to gain super user access. Malware could be uploaded during patching (a key vulnerability) and with the collaboration of compromised employees (i.e. insider threat). A successful attack on SCADA systems would then facilitate an attack on physical airport infrastructure. The attacker may send malicious commands, such as halt baggage handling, or disrupt normal operations of baggage handling.

Criticality

Depending on the severity of the cascading affect this could lead to significant disruption in disembarking and loading procedures with a consequent serious disruption on the airside operations. Furthermore, similar to the other scenarios, a further threat and cascading effect that could rise here is related to acts that can compromise the safety of passengers, including: terrorist acts, such as the combination of a network attack with the loading of explosives into the luggage in order to attack the aircraft; or the hiding of other illegal products in the luggage (e.g. drugs).[63]

Likelihood

In recent years SCADA systems have suffered several cyber-attacks. The increasing interconnection and interdependency between SCADA systems and other airport assets, together with the lack of security countermeasures applied to them have opened up vulnerabilities that can be easily exploited.

Cascading effects

Once a malware is uploaded into an ICS SCADA this will disrupt the logic of the real time control system and its components (e.g. system sensors, reading, etc.) but also the functions of the dependent infrastructures.

[62] ICS SCADA systems are used in airport to monitor and control several physical infrastructures ranging from air-conditioning, power supply including airfield lighting to apron services ('finger' or air bridges).

[63] A similar attack has occurred at the port of Antwerp. See http://www.magals3.com/contentManagment/uploadedFiles/White_Papers/Cyber_For_ICS_Antwerp_Case_web.pdf.

Attack scenario

Type of Attack	Asset affected
Network attack	• Baggage handling • ICS SCADA • Way-finding services

CRITICALITY	LIKELIHOOD
High with emphasis on operations but it could also escalate to safety.	Medium

CASCADING EFFECTS	STAKEHOLDERS INVOLVED
• Baggage handling systems • Computerised Maintenance Management Systems (CMMS) • Energy Management	• IT support services • Passengers • Baggage handling • Building and other maintenance

RECOVERY TIME AND EFFORTS	GOOD PRACTICES
System recovery and efforts depend on the time needed to identify the security flaw as well as isolate and block the attack. Due to the interconnection among systems and possible cascading effects this could require a significant effort from several of the stakeholders involved. Recovery time could be reduced by prioritising which services should be recovered first focusing on recovering the most relevant in the first instance.	• **GP13 – Integrate shutdown procedure / remote deactivation of capabilities for assets based on assets** • **GP 11 – Firewalls, network segmentation and defence in depth** • **GP 12 – Strong user authentication** • **GP 03 – Change default administrator credentials of devices** • **GP 01 – Intrusion Detection Systems (IDS)** • GP08 – Conduct vulnerability and penetration tests • GP06 – Operating systems updates and backups • GP 16 – Set up an information security management system and implement international standards • GP 19 – Establish an inventory of the information and information systems available • GP 22 – Conduct risk assessments • GP 23 – Create a risk register and monitor risk effectively • GP 24 – Perform continuous monitoring of information security • GP 25 – Manage risk according to international standards and a methodological approach • GP 35 – Provide specialised information security training • GP 38 – Develop a contingency plan • GP 42 – Provide incident response capabilities for airports • GP 43 – Train airport personnel in their incident response roles with respect to the information system • GP 45 – Track and document information system security incidents

CHALLENGES AND GAPS
One of the key challenges in relation to SCADA is that cyber security good practices and countermeasures commonly applied to IT infrastructure have not been applied to ICS. Another challenge is related to the increasing interdependence and connection of SCADA with other airport systems. The degree of interconnections among systems increase the number of vectors attacks while opening up back doors to connected systems. This increase in complexity and functionality requires an enhanced approach to cyber security focusing on holistic assessments and planning (see Gap 8). ENISA has released several guidelines on ICS SCADA security[64].

[64] ENISA ICS SCADA, http://enisa.europa.eu/scada

5.3 Drone intercept as mobile vehicle for jamming and spoofing aircraft-airport and traffic control-airline communications

Drones, fitted with electronic devices, can be used to spoof, and jam aircraft-airport and traffic control-airline communications. Aircrafts use the Automatic Dependent Surveillance – Broadcast (ADS-B) system to transmit their positions based on on-board navigational instruments and GPS technology. ADS-B broadcasts information periodically and its signal can be received by the ground surveillance systems including air traffic control centres and Approach Control Services, and also by aircraft in the vicinity when appropriately equipped for receiving and processing this signal. ADS-B is unencrypted and unauthenticated, showing aircraft ID, altitude, latitude and longitude position, bearing and speed. ADS-B is used to support surveillance in ensuring that aircraft are safely separated. Lack of authenticity, and, to a lesser extent, lack of encryption, facilitate spoofing and/or jamming of communications, allowing a malicious person to inject false data or disable sending or receiving messages into these real ATM Surveillance communications. Indeed, an attacker may decide to spoof existing signals on the ADS-B frequencies in order to generate crafted and false ADS-B messages, containing tampered information (e.g. fake GPS positions but also other fake information contained in the ADS-B messages), which show aircrafts not existing in the air space on screens of the air traffic controllers and/or lead to conflicting data between Air Traffic Control (ATC) and cockpit displays. This may lead to different situational awareness pictures for pilots and ATC, provoke false collision warnings and thus generate safety issues, while potentially impacting the airport flight management operations.

Criticality

The presence of mitigation actions, focusing on reconciling messages using primary and secondary transmission sources (i.e. radar), means that criticality is medium. However, in the case of a successful attack the criticality should be considered high.

However, it is worth considering that the use of drones, as we see it nowadays, will develop into a possible weapon (for instance ad hoc communication networks could be used to direct flocks of drones near jet intakes or drones could be used to pass forbidden liquids or other dangerous materials and products over the controlled perimeter of the airport). In the present and immediate future, beside any interruption or disruption of airport flight management operations a threat that arises here is related to acts that can compromise the safety of passengers, including terrorist acts.

Likelihood

The lack of encryption and authentication features in the ADS-B system together with low technical difficulty required to perform the attack make the likelihood that an attack might occur high. Indeed, ADS-B equipped planes are widely used and operating right now since many airlines worldwide have already embraced the technology. In addition, ADS-B is expected to be mandatory in the United States and in Europe by 2020. This will make this type of attacks even more likely in the near future. However, due to mitigation measures in place, the likelihood that this type of attack would be successful should be considered as medium.

Cascading effects

Spoofing attacks on ATM infrastructure can affect the reliability of communications from aircraft to air traffic control/airport and vice-versa as well as aircraft-to-aircraft communications. This can impair the entire management of flight operations due to the injection of unreliable data into other information systems that make use of these flight data.

Attack scenario

Type of Attack	Asset affected
Spoofing and/or jamming attack	- Comms - Communications, Navigation and Surveillance - Global Positioning System/EGNOS/SBAS/GBAS - Geographic Information Systems (GIS)

CRITICALITY	LIKELIHOOD
Medium with focus on safety and operational aspects.	Medium.

CASCADING EFFECTS	STAKEHOLDERS INVOLVED
- Air Traffic Management Navigational Aids and Approach - Flight Tracking Systems - Flight Display System and Management - Departure Control Systems - Communication, Navigation and Surveillance Systems - System Monitoring & Control Centre (SMC) - Passenger-Airline Communication System (e.g., delays, disruption linked with the ATC flight information).	- Airlines Operation Centre (including pilots) - Air Traffic Control (ATC) - Systems Monitoring and Control (SMC) - Airport operators

RECOVERY TIME AND EFFORTS	GOOD PRACTICES
Recovery time depends on the ability of the Air Navigation Service Providers (ANSP) to identify, isolate and address the attack. The response time for the resolution of the cyber security attack will be proportional to the time taken from the ANSP to resolve the situation. Having the required technical tools to identify fake aircrafts may significantly reduce recovery time and efforts especially in case of single attacks.	- **GP 12 – Strong user authentication** - **GP 01 – Intrusion Detection Systems (IDS)**[65] - **GP 25 – Manage risk according to international standards and a methodological approach** - **GP 35 – Provide specialised information security training** - **GP 40 – Train airport personnel in their contingency and disaster recovery roles (specifically for air traffic control personnel)** - GP 38 – Develop a contingency plan - GP 39 – Develop a disaster recovery plan - GP 42 – Provide incident response capabilities for airports (including airlines) - GP 45 – Track and document information system security incidents - GP 37 – Maintain on-going contacts with security groups and associations

CHALLENGES AND GAPS
Communication systems and protocols, especially for legacy Air Navigation Systems, have not been developed with security in mind since the emphasis was to provide an open and interoperable system and protocol. Interdependence among systems and the combination of threat vectors resulting from the interdependence is a key challenge for cyber security (see Gap 8). In addition, effective legislation could control the production and operation of drones, at least for commonly used ones, but also, to a certain extent, for military usage.[66] There is also a need for more information sharing (see Gap 6) leading to quickly identifying early warning of vulnerabilities and/or occurring attacks and multi-stakeholder enable security technologies (see Gap 7) that could offer real-time authentication in a complex and interdependent multi-stakeholder environment.

[65] This should also include appropriate procedures at Air Traffic Controller level to facilitate better reaction to such threat detection.

[66] The military use of drones might represent the biggest threat in some cases.

5.4 Attacks tools and techniques available

This section provides some more detailed examples of some of the tools, techniques and procedures available to potential attackers. There are already many available hacking tools as well as general purpose technical tools that an attacker can use in order to compromise airport security both in airside, landside and terminal operations. One of these technical tools is Software Defined Radio (SDR) which is a radio communication system that consists of a computer equipped with radio receivers (i.e. antennas, dongles) and the appropriate software (i.e. SDR software). Antennas, dongles and SDR software can be easily procured and then used to spoof, intercept and decode or jam any air-to-ground or air-to-air radio frequency communications, such as ACARS, ADS-B etc. Attackers have also other means to compromise security in airports by manipulating devices inside the airport, such as barcode scanners, biometric devices, point of sales devices, self-serving check-in kiosks and SCADA systems where they apply common hacking methods and techniques.

ACARS messages are transmitted in plaintext even though their content can reveal which aircraft is flying nearby by decoding the flight number and aircraft registration details. While this information might not seem as sensitive as the airplane location position that ADS-B messages carry, nonetheless it can provide meaningful input to potential attackers[67]. To eavesdrop on ACARS messages, one needs to consider that the worldwide frequency of ACARS transmissions is at 131.550 MHz. A list of all frequencies of ACARS (primary and secondary) for Europe, US and other countries is available online[68]. An antenna (e.g. a J-Pole antenna) has to be placed within a specific range nearby an aircraft and ground stations as a radio scanner and it has to be synchronized to the frequency of ACARS in order to receive these transmissions. Subsequently and with the help of the dongle (e.g. RTL-SDR dongle) the intercepted transmissions are passed on to the ACARS decoding software[69], to decode and display the digital messages of ACARS. Moreover, online services[70] which are publicly available provide to anyone access to aggregated data from all over the world in order to either locate aircrafts in real time or access real time ACARS web servers or even search for aircrafts, airlines and flights through ACARSD search[71] without the need of knowledge or any sophisticated cyberattack method.

In the case of ADS-B the process is along the same lines as in ACARS. However, whereas the J-pole antenna could still be employed, other antennas[72] have proven to be more suitable in receiving the vertically polarized signal of ADS-B (it transmits at 1030 MHz for interrogation and 1090 MHz for replies). The Collinear Coax Antenna is considered as the most suitable[73] one for high quality reception of ADS-B signals. Subject to the signal having been intercepted, software tools[74] can decode ADS-B transmissions in a very effective manner providing among other information the geolocation of all aircrafts in the range. A recent proof of concept[75] shows how easy it is to develop a homemade aircraft radar to collect the geolocation coming from the ADS-B messages of nearby aircrafts. Another proof of concept[76], has demonstrated the possibility to mount replay attacks and to inject false data into an aircraft's real ADS-B air-to-air communications rather than simply intercepting these messages. ADS-B messages are both unencrypted and unauthenticated and therefore an attacker can transmit falsified messages of this type thus succeeding in mounting an

[67] European Aviation Safety Agency European Aviation confirmed the concerns about the Airplane hacking. Hackers could easily infiltrate critical systems, http://securityaffairs.co/wordpress/40975/hacking/easa-airplane-hacking.html.
[68] ACARS frequencies, http://www.acarsd.org/ACARS_frequencies.html.
[69] SDR#, Planeplotter, AirNav ACARS , rtl_acars, acarsed or acarsd.
[70] For example: https://bluehorizon.network/map/, https://adsbexchange.com, http://sdrsharp.com:8080/virtualradar/desktop.html.
[71] http://www.acarsd.org/acars_search.html.
[72] PCB antenna, Quarter Wave Ground Plane antenna, Wine Cork Dipole Antenna, Collinear Wire Antenna, Collinear Coax Antenna.
[73] Review: FlightAware 1090 MHz ADS-B Antenna and Filter , http://www.rtl-sdr.com/review-flightaware-ads-b-antenna-and-filter/ .
[74] Airspy, HackRF, SDRplay, etc.
[75] Building the Internet of Wrongs, https://www.rawhex.com/2016/06/building-internet-wrongs/ .
[76] Ghost in the Air(Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices, https://media.blackhat.com/bh-us-12/Briefings/Costin/BH_US_12_Costin_Ghosts_In_Air_WP.pdf.

impersonation attack utilising an ADS-B transceiver[77] and appropriate software[78] to encode high-level ADS-B messages.

ADS-B is also susceptible to jamming attacks that can be performed by using only a ground-based radio-frequency source radiating within a specific range. Jamming, which implies disrupting the ADS-B frequencies, is also an attack with high impact as it is capable to result in outage of the GPS service over an entire airport. Drones and UAVs in general, that can be easily equipped with advanced computing and communication capabilities are an additional means to perform spoofing, replay or jamming attacks in these days[79].

Furthermore, attacks are not limited only to interception of air traffic messages and radio signals. Another attack surface involves security compromises and manipulation of assets inside the airport. Such attacks may affect both customer services and passenger management; for example, self-serving check-in kiosks can be exploited via their input communication channels. Input channels that allow input from external users to a device include USB, parallel, serial or Ethernet ports or even wireless connections, such as Bluetooth or Wi-Fi. Usually, ports such as USB are installed to support hardware or software update using peripheral devices. However, there exists a wide variety of USB dongles[80] and corresponding software[81] that generate payload which will force a device to execute commands and therefore exploits resulting in unauthorised modification of hardware or software (e.g. installation of malware, key loggers). In case the compromised device is also Internet connected, an attacker could be also able to execute remotely arbitrary code.

In another interesting recent proof of concept[82], the manipulation of the flight ticket barcode scanner was illustrated. While this is one of the many ways to manipulate barcodes[83], in this case, the manipulated input was the flight ticket barcode itself. Many tools[84] offer the ability to convert a barcode to plaintext and then modify the corresponding text. The simpler the logic of the coded plaintext is, the easier it can be manipulated. This text can be modified through a notepad and then a new barcode can be generated using specialized tools or online services[85].

Additionally, ICS SCADA systems that reside on and support airport infrastructures[86], e.g. utilised for many functions such as baggage handling[87], are equally exposed to vulnerabilities as computers and network devices. In case these systems are connected to the Internet, the probability of being discovered through SCADA specific online scanning tools[88] is increased. Moreover, numerous metasploit modules[89] and tools[90] for fuzzing and vulnerability discovery facilitate network attacks since the discovery of vulnerabilities and

[77] KGX 150/130 or PING-2020
[78] GNURadio and Matlab
[79] http://theconversation.com/are-drones-really-dangerous-to-airplanes-56770
[80] Rubber ducky, usb armory, etc.
[81] https://ducktoolkit.com/
[82] http://www.slideshare.net/PrzemekJaroszewski/how-to-get-good-seats-in-the-security-theater
[83] http://hackaday.com/2016/02/17/barcodes-that-hack-devices/
[84] http://www.onlinebarcodereader.com/
[85] http://www.barcode-generator.org/
[86] http://www.schad-automation.com/en/industries/airport-scada
[87] http://www.ats-global.com/baggage-handling_351_gben
[88] https://shodan.io , https://www.censys.io/
[89] https://scadahacker.com/resources/msf-scada.html
[90] https://nmap.org/nsedoc/scripts/bacnet-info.html
https://github.com/digitalbond/Redpoint
https://github.com/scadastrangelove/SCADAPASS
https://www.automatak.com/aegis/
http://gleg.net/agora_scada_upd.shtml
https://www.wurldtech.com/products/achilles
http://immunityinc.com/products/canvas/
http://www.tenable.com/products/nessus-vulnerability-scanner

exploitations can lead to possible attacks at a second hop, namely the airport IT & Comms. A recent research[91] reveals that a piece of malware targeting SCADA systems was discovered and most likely posed a proof of concept of ICS attack techniques. A malware, named IRONGATE, was first placed to this system by a dropper which installed the payload under certain conditions[92]. This malware unravelled a man-in-the-middle attack and could potentially cause unauthorised modification of hardware, software or data. This particular case happening in a SCADA responsible baggage handling processes would greatly impact the passenger management function of an airport.

[91] http://www.securityweek.com/mysterious-ics-malware-targets-scada-systems

[92] ibid.

6. Security good practices

Securing Smart airports and staying ahead of evolving cyber threats is a shared responsibility, involving governments, airlines, airports, vendors and regulators. Therefore, it is imperative to put in place a collaborative model to set goals and define an appropriate cyber security approach to strengthen the aviation system's resilience against attacks. To this aim, significant effort is being invested across the aviation community at different levels, including standardisation, security working groups, research and education. Identification of challenges posed by cyber threats, risk assessment approaches and guidelines to enhance cyber security, either in terms of high level governance strategies[93,94] or in terms of specific technological supports[95], are priorities currently tackled.

In order to help both asset owners and all the actors involved in securing Smart airports, ENISA has taken stock of the current good practices. These practices represent what exists at the moment and have been consulted in order to form the groups of good practices and the categories for each one of them. As a result, some of them are general and not airport specific practices. As noticed in the Gap Analysis Section (see Gap 1), existing good practices tend to be general with few specifically addressing cyber security practices in Smart airports. The identified good practices for Smart airports are presented here and arranged according to three main groups: *Technical/tool-based*; *Policies and standards*; and *Organisational, people and processes*. Figure 9 presents the full mind map of the identified good practices. Each main group is then discussed in details in the following sub-sections.

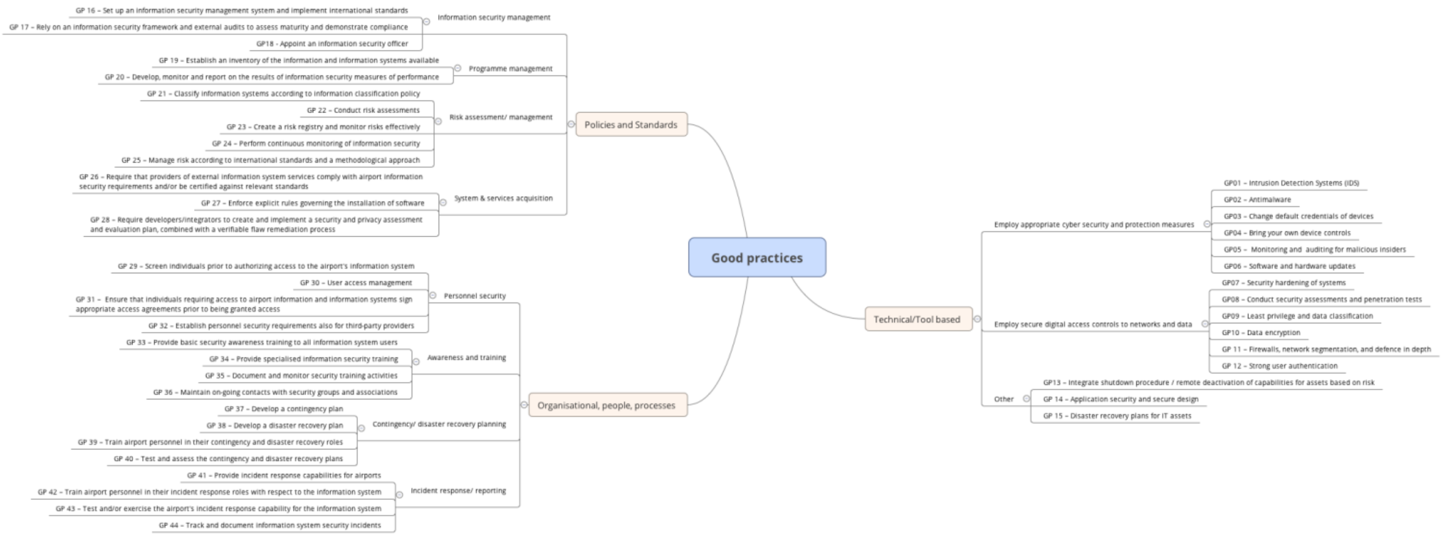

GP 16 – Set up an information security management system and implement international standards
GP 17 – Rely on an information security framework and external audits to assess maturity and demonstrate compliance
GP18 - Appoint an information security officer
Information security management
GP 19 – Establish an inventory of the information and information systems available
GP 20 – Develop, monitor and report on the results of information security measures of performance
Programme management
GP 21 – Classify information systems according to information classification policy
GP 22 – Conduct risk assessments
GP 23 – Create a risk registry and monitor risks effectively
GP 24 – Perform continuous monitoring of information security
GP 25 – Manage risk according to international standards and a methodological approach
Risk assessment/ management
GP 26 – Require that providers of external information system services comply with airport information security requirements and/or be certified against relevant standards
GP 27 – Enforce explicit rules governing the installation of software
GP 28 – Require developers/integrators to create and implement a security and privacy assessment and evaluation plan, combined with a verifiable flaw remediation process
System & services acquisition
Policies and Standards
Good practices
GP 29 – Screen individuals prior to authorizing access to the airport's information system
GP 30 – User access management
GP 31 – Ensure that individuals requiring access to airport information and information systems sign appropriate access agreements prior to being granted access
GP 32 – Establish personnel security requirements also for third-party providers
Personnel security
GP 33 – Provide basic security awareness training to all information system users
GP 34 – Provide specialised information security training
GP 35 – Document and monitor security training activities
GP 36 – Maintain on-going contacts with security groups and associations
Awareness and training
GP 37 – Develop a contingency plan
GP 38 – Develop a disaster recovery plan
GP 39 – Train airport personnel in their contingency and disaster recovery roles
GP 40 – Test and assess the contingency and disaster recovery plans
Contingency/ disaster recovery planning
GP 41 – Provide incident response capabilities for airports
GP 42 – Train airport personnel in their incident response roles with respect to the information system
GP 43 – Test and/or exercise the airport's incident response capability for the information system
GP 44 – Track and document information system security incidents
Incident response/ reporting
Organisational, people, processes
Technical/Tool based
Employ appropriate cyber security and protection measures
GP01 – Intrusion Detection Systems (IDS)
GP02 – Antimalware
GP03 – Change default credentials of devices
GP04 – Bring your own device controls
GP05 – Monitoring and auditing for malicious insiders
GP06 – Software and hardware updates
Employ secure digital access controls to networks and data
GP07 – Security hardening of systems
GP08 – Conduct security assessments and penetration tests
GP09 – Least privilege and data classification
GP10 – Data encryption
GP 11 – Firewalls, network segmentation, and defence in depth
GP 12 – Strong user authentication
Other
GP13 – Integrate shutdown procedure / remote deactivation of capabilities for assets based on risk
GP 14 – Application security and secure design
GP 15 – Disaster recovery plans for IT assets

Figure 9: Good Practices

[93] AIAA (2013) *The connectivity challenge: Protecting critical assets in a networked world – a Framework for aviation cyber security*, an AIAA Decision Paper, http://www.aiaa.org/uploadedFiles/Issues_and_Advocacy/AIAA-Cyber-Framework-Final.pdf.

[94] Di Maio, Francesco (2014) "*Centralized security governance for air navigation services: Innovative strategies to confront emerging threats against Civil Aviation*, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6986968&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber=6986968.

[95] Airport Cooperative Research Program (ACRP, 2015) Report 140: Guidebook on Best Practices for Airport Cyber security, http://onlinepubs.trb.org/onlinepubs/acrp/acrp_rpt_140.pdf.

6.1 Technical/tool-based good practices

There are various good practices published for all aspects of airport-based technical and tool-based practices. Below we provide an overview of each good practices that can be applied. Detailed description of each good practices and the detail of the threats that they address is provided in Annex 5.

Employ appropriate cyber security and protection measures

- GP01 – Intrusion Detection Systems (IDS)
- GP02 – Antimalware
- GP03 – Change default credentials of devices
- GP04 – Bring your own device (BYOD) controls
- GP05 – Monitoring and auditing for malicious insiders
- GP06 – Software and hardware updates

Employ secure digital access controls to networks and data

- GP07 – Security hardening of systems
- GP08 – Conduct security assessments and penetration tests
- GP09 – Least privilege and data classification
- GP10 – Data encryption
- GP 11 – Firewalls, network segmentation, and defence in depth
- GP 12 – Strong user authentication

Other

- GP13 – Integrate shutdown procedure / remote deactivation of capabilities for assets based on risk
- GP 14 – Application security and secure design
- GP 15 – Disaster recovery plans for IT assets

The documents that have been considered as part of this section are:

- K. Gopalakrishnan, M. Govindarasu, D. W. Jacobson, B. M. Phares (2014), *Cyber Security for Airports*[96]
- ENISA (2014) *Algorithms, key size and parameters report*[97]
- ANSSI (2014) *Mécanismes cryptographiques*[98] V2.03
- BSI (2015) *Kryptographische Verfahren: Empfehlungen und Schlussellangen*
- IBM Systems & Technology Group, *VPN Security and Implementation*[99]
- Gemalto, *Strong Authentication Implementation Guide*[100]
- PwC (2015) *Smart Borders Pilot Project, Technical Report Annexes, Volume 2*[101]
- Keenan, Thomas (Unknown) *Risks of Biometric Identifiers and How to Avoid*[102]
- Katharina Krombholz, Heidelinde Hobel, Markus Huber, Edgar Weippl (2014) *Advanced Social Engineering Attacks*[103]

6.2 Policies and standards

There are various good practices published for all aspects of airport-based policies and standards. The following overview presents a list of those good practices. Detailed description of each good practices and

[96] Cyber security for airports, http://www.ijtte.com/uploads/2013-12-30/5ebd908d-7f47-e96dIJTTE_Vol 3(4)_2.pdf.
[97] Algorithms, key size and parameters report 2014, https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014.
[98] Référentiel Général de Sécurité, https://references.modernisation.gouv.fr/sites/default/files/RGS_v-2-0_B1.pdf.
[99] VPN Security and Implementation, http://www-01.ibm.com/support/docview.wss?uid=ssg1S1002693&aid=1.
[100] Strong Authentication Implementation Guide, http://www.gemalto.com/dwnld/6953_Strong_auth_implementation_guide.pdf.
[101] Smart Borders - Technical Report, http://www.eulisa.europa.eu/Publications/Reports/Smart Borders - Technical Report.pdf.
[102] Hidden Risks of Biometric Identifiers and How to Avoid Them, http://www.blackhat.com/docs/us-15/materials/us-15-Keenan-Hidden-Risks-Of-Biometric-Identifiers-And-How-To-Avoid-Them-wp.pdf.
[103] Advanced Social Engineering Attacks , https://www.sba-research.org/wp-content/uploads/publications/jisa_revised.pdf.

the detail of the threats that they address is provided in Annex 5.

Information security management

- GP 16 – Set up an information security management system and implement international standards
- GP 17 – Rely on an information security framework and external audits to assess maturity and demonstrate compliance
- GP 18 – Appoint an information security officer

Programme management

- GP 19 – Establish an inventory of the information and information systems available
- GP 20 – Develop, monitor and report on the results of information security measures of performance Risk assessment
- GP 21 – Classify information systems according to information classification policy
- GP 22 – Conduct risk assessments
- GP 23 –Create a risk registry and monitor risks effectively
- GP 24 – Perform continuous monitoring of information security
- GP 25 – Manage risk according to international standards and a methodological approach management

System & services acquisition

- GP 26 – Require that providers of external information system services comply with airport information security requirements and/or be certified against relevant standards
- GP 27 – Enforce explicit rules governing the installation of software
- GP 28 – Require developers/integrators to create and implement a security and privacy assessment and evaluation plan, combined with a verifiable flaw remediation process

The documents that have been considered as part of this section are:

- ISO/IEC 27001 (2013) - Information security management[104]
- ISO/IEC 27002 (2013) - Information security management[105]
- ISO/IEC 27033 (20015) - IT network security standard[106]
- ISO 22301 (2012) - Societal security[107]
- CANSO (2014) *CANSO Position Paper on Cyber security*[108]
- NIST (2013) *Framework for Improving Critical Infrastructure Cyber security*[109]
- NIST (2010) *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*[110]
- NIST (2012) *Guide for Conducting Risk Assessments*[111]
- NIST (2014) *Assessing Security and Privacy Controls in Federal Information Systems and Organisations: Building Effective Assessment Plans*[112]

[104] ISO/IEC 27001 - Information security management, http://www.iso.org/iso/iso27001.
[105] ISO/IEC 27002:2013, http://www.iso.org/iso/catalogue_detail?csnumber=54533.
[106] ISO/IEC 27033-1:2009, http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=51580.
[107] ISO 22301:2012, http://www.iso.org/iso/catalogue_detail?csnumber=50038.
[108] CANSO Position Paper on Cyber Security, https://www.canso.org/sites/default/files/CANSO position paper on Cyber Security_v1 1.pdf.
[109] Cybersecurity Framework, http://www.nist.gov/cyberframework/index.cfm.
[110] Guide For Applying the Risk Management Framework to Federal Information Systems, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf.
[111] Guide for Developing Security Plans for Federal Information Systems (February 2006), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-18r1.pdf .
[112] Assessing Security and Privacy Controls in Federal Information Systems and Organizations, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf.

- NIST (2006) *Guide for Developing Security Plans for Federal Information Systems*[113]
- NIST (2008*) Performance Measurement Guide for Information Security*[114]
- NIST (2004) Standards for Security Categorization of Federal Information and Information Systems[115]
- Airport Cooperative Research Program (2015) *Report 140: Guidebook on Best Practices for Airport Cyber security*[116]
- ENISA (2010) *Risk Management Inventory Methods – EBIOS*[117]
- ENISA (2010) *Risk Management Methods - MEHARI*[118]
- CoESS, ASSA (2011) *CEN 16082: A European Standard for Aviation Security Standards*[119]

6.3 Organisational, people and processes[120]

There are various good practices published for all aspects of airport-based organisational, people and processes. Detailed description of each good practices and the detail of the threats that they address is provided in Annex 5.

Personnel security

- GP 29 – Screen individuals prior to authorising access to the airport's information system
- GP 30 – User access management
- GP 31 – Ensure that individuals requiring access to airport information and information systems sign appropriate access agreements prior to being granted access
- GP 32 – Establish personnel security requirements also for third-party providers

Awareness and training

- GP 33 – Provide basic security awareness training to all information system users
- GP 34 – Provide specialised information security training
- GP 35 – Document and monitor security training activities
- GP 36 – Maintain on-going contacts with security groups and associations

Contingency/ disaster recovery planning

- GP 37 – Develop a contingency plan
- GP 38 – Develop a disaster recovery plan
- GP 39 – Train airport personnel in their contingency and disaster recovery roles: integrity of the information system.
- GP 40 – Test and assess the contingency and disaster recovery plans

Incident response/ reporting

- GP 41 – Provide incident response capabilities for airports
- GP 42 – Train airport personnel in their incident response roles with respect to the information system
- GP 43 – Test and/or exercise the airport's incident response capability for the information system

[113] Guide for Developing Security Plans for Federal Information Systems, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-18r1.pdf.

[114] Performance Measurement Guide for Information Security, http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf.

[115] http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

[116] Guidebook on Best Practices for Airport Cybersecurity, http://onlinepubs.trb.org/onlinepubs/acrp/acrp_rpt_140.pdf.

[117]Standards for Security Categorization of Federal Information and Information Systems, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_ebios.html.

[118] ENISA Risk Management, Mehari, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_mehari.html.

[119] A European Standard for Aviation Security Services, http://www.assa-int.org/_Uploads/dbsAttachedFiles/2011-June_ASSA-I-CoESS_WhitePaper_CEN-EN-16082-FINAL.pdf.

[120] Administrative/Procedural Controls/Physical Controls are also included (ID cards, Physical Access Controls, CCTV, Fences, Doors, Locks, guards, etc.).

- GP 44 – Track and document information system security incidents

The documents that have been considered as part of this section are:

- Airport Cooperative Research Program (2015) *Report 140: Guidebook on Best Practices for Airport Cyber security*[121]
- ASAC (2015) *Final report of the Aviation Security Advisory Committee's Working Group on Airport Access Control*[122]
- NIST (2012) *Computer Security Incident Handling Guide*[123]
- NIST (2010) *Contingency Planning Guide for Federal Information Systems*[124]
- NIST (2006) *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*[125]
- NIST (2003) *Guide to Technology Information Security Services*[126]
- NIST (2003) *Building an Information Technology Security and Awareness Training Programme*[127]
- NIST (1998) *Information Security Training Requirements: A Role and Performance Based Model*[128]
- ISO 22301 (2012) *Societal security -- Business continuity management systems --- Requirements*[129]
- ACRP (2013) *Operational and Business Continuity Planning for Prolonged Airport Disruptions*[130]
- AIAA (2013) *The connectivity challenge: Protecting critical assets in a networked world – a Framework for aviation cyber security*[131]

[121] Guidebook on Best Practices for Airport Cybersecurity, http://onlinepubs.trb.org/onlinepubs/acrp/acrp_rpt_140.pdf.

[122] ASAC groups, https://www.tsa.gov/sites/default/files/asac-employee-screening-working-group-04-15.pdf.

[123] Computer Security Incident Handling Guide, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

[124] Contingency Planning Guide for Federal Information Systems, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf.

[125] Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, http://csrc.nist.gov/publications/nistpubs/800-84/SP800-84.pdf.

[126] Guide to Information Technology Security Services , http://csrc.nist.gov/publications/nistpubs/800-35/NIST-SP800-35.pdf.

[127] Building an Information Technology Security Awareness and Training Program, http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf.

[128] Information Technology Security Training Requirements: A Role-andPerformance-Based Model, http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf.

[129] ISO 22301:2012, http://www.iso.org/iso/catalogue_detail?csnumber=50038.

[130] Operational and Business Continuity Planning for Prolonged Airport Disruptions, http://onlinepubs.trb.org/onlinepubs/acrp/acrp_rpt_093.pdf.

[131] A Framework for Aviation Cybersecurity, http://www.aiaa.org/uploadedFiles/Issues_and_Advocacy/AIAA-Cyber-Framework-Final.pdf.

7. Gap analysis and identification of areas of improvement

This section provides an analysis of the main gaps in relation to cyber security in smart airports. Gaps have been identified via a comparison among the identified assets, vulnerabilities, threats and good practices. Expert interviews were used to further identify and validate the gaps. Gaps to be addressed focused on different areas, including: operational practices, policy and standardisation, and the need to develop more comprehensive and integrated tools. This section summaries seven identified key cyber security gaps in Smart airport. While they are numbered 1 to 7 below, these gaps have not been ranked according to any measure of importance.

Gap 1: Disparity of cyber security practices in airports

There is a disparity amongst airports in the methods and degree to which cyber security is addressed. While certain airports are often described as having a very mature cyber security posture[132], in the expert interviews other airports admitted to having limited capabilities or resources dedicated to cyber security. Poor practices include password reuse/sharing, a lack of a centralised centre for incident handling, and low levels of cyber security awareness and prioritisation.

Individual airports are required to develop their own posture to cyber security, typically in relation to adhering to various (mostly non-airport specific) guidelines and standards. Each airport is therefore responsible for interpreting existing guidelines and standards, and adapting these to suit the context of an airport. While many of the threats (as documented in Section 4) are common to the security of various ICT systems, there are specific risks (such as public Wi-Fi and kiosks, and infrastructures with passenger risk to life) and network design considerations that are specific to airports and critical infrastructure.

Existing security guidelines and standards (such as ISO27001[133], EN16495,[134] and EN16082[135]) serve an important role in providing assurance that a baseline level of security processes is in place. However, there is still a gap in that there are few guidelines and standards specifically addressing cyber security practices in Smart airports, and those that do exist are not consistently applied.

Gap 2: Lack of a common approach and multi-stakeholders model on cyber security of airports

There is not a common EU approach to cyber security of smart airports or a common multi-stakeholder model on cyber security. Both could facilitate harmonisation of practises and interventions in a very competitive environment, with the aim to protect public safety, regularity and efficiency of transportation by air, and rights such as life in flight and on the ground. Furthermore, the rapid advance of technology and the slower pace of the legislative processes, may lead to serious legal gaps within the future environment of smart airports. These gaps might pose some challenge to both Member States and the European Institutions to address security and safety of European citizens.[136] The NIS Directive (NISD) is expected to provide some directions and high-level consistency, especially in terms of baseline security measures and incident reporting.

[132] For example, see: ACI , “Cyber Security: Potential Impact on European Airports”, *Briefing Paper.*

[133] ISO/IEC 27001 - Information security management http://www.iso.org/iso/iso27001.

[134] BS EN 16495:2014 Air Traffic Management. Information security for organisations supporting civil aviation operations, http://shop.bsigroup.com/ProductDetail/?pid=000000000030269415.

[135] BS EN 16082:2011 Airport and aviation security services http://shop.bsigroup.com/ProductDetail/?pid=000000000030202610.

[136] ENISA, “Fly 2.0”, 2010, https://www.enisa.europa.eu/publications/flying-2.0-enabling-automated-air-travel-by-identifying-and-addressing-the-challenges-of-iot-rfid-technology.

Gap 3: Guidelines on network architecture, ownership, and remote management

There is a large variation in how airports design and implement network infrastructure, manage vendors, and design online solutions. This is complicated by the fact that each airport has many ICT networks being operated within the airport, many of which the airport does not have direct control over. Networks in airports include those supporting landside, airside and terminal operations systems; this includes (sometimes multiple) passenger Wi-Fi networks run by external vendors, mobile telecoms and devices to manage people and assign tasks, cloud-based infrastructure for the solutions to be deployed at the airport for passenger management, CUPPS (Common Use Passenger Processing Systems) solutions for border control, e-ticketing, and biometric controls. Each of these networks are often managed by, and externally connected to, various external organisations. Critical and non-critical networks should be segregated. Many networks and systems are remotely managed. The resulting airport cyber security landscape can be described as having a large and complex attack surface.

The complexity of the situation and the lack of IT architecture reference models, suggests a gap in industry models and guidelines on airport network architecture, ownership, and remote management. There is currently no reference model that focuses on the IT architecture of smart airports that can be used to inform the development of ICT and network security. Such a reference model should take account of the changing ownership structure of airports that are increasingly being turned over to private hands with more fragmentation of service providers in relation to the ICT network, clearly define the segregation of critical and non-critical networks, and provide a common basis for designing network interoperability.

Gap 4: Evidence-based vulnerability analysis metrics and priorities

Risk assessments, vulnerability assessments, and penetration tests should be carried out on a regular basis to identify potential security issues. Airports can formally define and assess risks and aim for compliance with standards, such as ISO27001 and PCI DSS.[137] Guidance on security assessments within aviation and airports exists (CANSO Cyber Security and Risk Assessment Guide)[138] as do generic and adaptable security assessment approaches.[139] However, there is little consensus on what metrics or standards should be used to measure the cyber security of smart airports. There also lacks an evidence-based understanding of the systems that are critical to the airport and incident control management: for example, what systems should be prioritised in the case of an incident to best avoid panic that could cause further disruption and security risk.

Gap 5: Threat modelling and architecture analysis

The software vendors surveyed for this research had detailed security processes in place for the development of infrastructure components for airports. In one example, Microsoft Security Development Lifecycle was used to design security into the systems that were developed. Formal threat modelling is used to model the interactions of systems to identify and analyse potential security threats. However, there is a lack of modelling of the networks *in place at airports* to analyse the interactions between systems and networks for potential security issues within this airport environment. Introducing formal threat modelling and architecture analysis to airport systems and networks may identify otherwise difficult-to-identify weaknesses, such as insufficient authentication or validation between back-end systems.

[137] Helping Airports Understand the Payment Card Industry Data Security Standard (PCI DSS)http://onlinepubs.trb.org/onlinepubs/acrp/acrp_rrd_011.pdf
[138] CANSO Cyber Security and Risk Assessment Guide https://www.canso.org/sites/default/files/CANSO%20Cyber%20Security%20and%20Risk%20Assessment%20Guide.pdf and ACI, “Cyber Security: Potential Impact on EU Airports.
[139] Open Source Security Testing Methodology Manual (OSSTMM) http://www.isecom.org/research/.

Gap 6: Information sharing

There is arguably the need for a collaborative platform for airports to share data with airport authorities and national governments. Delegates tend to convene for physical security activities, but to date there is no real network to collaborate on specific issues of cyber security, and this is reflected in the structure of the airport and the security priorities within it. A data sharing platform would enable airports to share information on new vectors of attacks, and early warning of vulnerabilities in systems to provide continuous improvements of systems. Cooperation among cyber security agencies, law enforcement, industry, and academia would further benefit information sharing.

Gap 7: Multi-stakeholder trust framework and trust-enable security technologies

Smart airports are paving the way for a change in how airports operate; moving from an uncooperative and independent approach to one that is cooperative and dependent.[140] This is due to the number of communication networked technologies and connected systems applied across the airport systems, often belonging to different operators and displaying multiple interdependence.[141] However, lack of trust among the diverse operators and providers can hinder further development within Smart airports. As a result there is a need for more advanced security IT infrastructures allowing the formation of transient trust within a highly mobile environment.[142] This could lead to further work and development combining light-weight cryptography protocols (for light duty devices usage) and regular cryptography framework (e.g. PKI - Public Key Infrastructure, for back- end infrastructures) as well as the exploration of implementation technology and testbeds (e.g. elliptic- curve cryptography mutual authentication RFID).[143] Furthermore, there is the need for the identification and development of airport specific trust framework helping operators navigate their trust relationships and dictate how the devices, sensors, readers and operators exchange data and operate together (e.g. how much a passenger's smart phone can interact with the airport concession kiosk). Within this trust framework, considerations around key management should also be addressed (i.e., identifying the actors generating the encryption keys- private/public keys, how these will be distributed and who, i.e. which agencies/companies/authorities, will eventually be given access to such keys when necessary).[144]

Gap 8: Lack of awareness and skills

This relates to the increasing move toward connected and interdependent systems and devices. Due to the fast growing interconnect nature of Smart airport, operators are struggling to achieve a full awareness of the new security landscape including the full range of cyber threats and boundaries for securing the Smart airport perimeter. Moreover, there is the need to educate a new generation of experts and train them both in safety and cyber security[145]; to increase awareness and promote education of passengers and airports' personnel on the security risks posed by new technologies and ways to be prepared; and properly train airports' personnel and passengers on the use of the new devices and technologies.

[140] Strohmeier Martin "On the Security of the Automatic Dependent Surveillance-Broadcast Protocol".

[141] Boutin Nicolas, Achim Fechtel, Hean Ho Loh, and Michael Tan, "The Connected Airport: The Time Is Now", bcg.perspectives, January 2016.

[142] Strohmeier Martin "On the Security of the Automatic Dependent Surveillance-Broadcast Protocol".

[143] ENISA, "Fly 2.0", 2010, https://www.enisa.europa.eu/publications/flying-2.0-enabling-automated-air-travel-by-identifying-and-addressing-the-challenges-of-iot-rfid-technology.

[144] Ibid.

[145] ARINC, Smart Airport: Connecting Airports, Airline and Aircraft, 2015.

8. Recommendations

This section of the report provides some key, high level recommendations on how to enhance cyber security and resilience within the Smart airport. Recommendations are mainly directed towards airport CISOs. However, some recommendations have also been developed for policy-makers, service providers and industry representatives. This is because enhancement of cyber security in Smart airports will require the integrated efforts of all the stakeholders involved. Each recommendation has been developed based on the information and analysis presented in earlier sections and insights from stakeholders. Below each recommendation are brief explanatory notes.

Recommendations for airport decision makers (CISOs, CIOs, IT Directors and Head of Operations) and airport information security professionals

8.1 Prioritise cyber security for safety

Airport operators should prioritise cyber security to untimely promote the safety of passengers, personnel and public in general. Cyber threats and risks will continue to grow driven by developments in technologies, while the relationship between safety and security will become more and more interwoven. It is no longer possible to be truly safe without also being secure. Therefore, it is responsibility of airport operators to recognise the threat and to ensure that their organisation is adequately prepared and protected in order to provide proper cyber security for safety. This is also aligned with regulatory development at the EU level (see Annex 1) stressing the relevance of cyber security as a key enabler of safety, which is becoming paramount in the aviation context. This recommendation directly addresses gap 1 and 8.

8.2 Establish a clear airport cyber security posture and allocate adequate roles and resources

Substantial changes to business-as-usual processes are required to adequately safeguard critical assets, satisfy regulatory requirements, and protect passenger security and airport business processes. In order for such changes to be accomplished, the full support and leadership of smart airport senior executives, together with a new and holistic approach to Enterprise Security Governance, is required. Responsibility for cyber security should be clearly allocated by the board of directors and adequate roles and resources should be clearly defined. Smart airports should envision the role of Chief Security Officer with senior leadership at the CEO and board level and information security teams. This clear allocation of responsibility and senior leadership will enable prioritisation of cyber security for safety within the whole organisation. Third party responsibilities and roles should also be considered. Cyber security would be then promoted by senior leadership at the CEO and board level and extend throughout the enterprise including third parties to foster a more security-aware culture. This recommendation directly addresses gap 1 and indirectly 4, 5 and 8.

8.3 Revise cyber security policies and practices based on good practices monitoring

Airport operators should consistently review cyber risk management policies and practices to ensure that they remain appropriate and effective in light of changing circumstances and risks. The establishment of regular monitoring, via checks and penetration testing, and regular assessment of airport preparedness should be linked to the revision of existing policies and practices so supporting an enterprise culture of continuous process and technology improvement. The revision of cyber security practices should be done on an enterprise-wide basis. This recommendation directly addresses gap 1 and indirectly 4, 5, 7 and 8.

8.4 Implement network-based, holistic risk and threat management policy and processes for cyber security

Airport operators should have tailored risk and threat management policy and processes in place for cyber security, which focus on network dependencies and the interactions between systems, and systems and networks for potential security issues. This also needs to take into account the changing ownership structure (i.e., third party providers and privatisation of key functions) and key operational aspects of Smart airports. The interconnection among the different systems, which can offer vectors of attack for those systems and entry gates to others, requires traditional aviation security to work hand by hand with ATM and aviation safety from the perspective of technology, operations and human factors. This will improve awareness of cascading effects and critical systems as well as support prioritisation efforts and promote consistency on how to holistically manage cyber security risks within Smart airports. The focus is to implement methodologies and processes for systemic/holistic risk assessment where threats and vulnerabilities are analysed from the whole aviation perspective and not in isolation. This recommendation directly addresses gap 1, 5 and 7, and 8.

Recommendations for policy-makers

8.5 Promote and facilitate the development of common guidelines, standards, metrics, awareness and knowledge exchange on cyber security for smart airports

Relevant EC institutions and agencies (e.g., ETSI, CEN, CENELEC, ENISA, DG MOVE, European Civil Aviation Conference, ECAC, etc.) together with international organisations (e.g., IATA and ICAO, etc.) should facilitate and promote, via open coordination initiatives, the use and development of common standards, guidelines and metrics aimed at enhancing cyber security in smart airports. These should be further supported by organisation at the national level, e.g. Civil Aviation Authorities (CAAs), providing implementation recommendations. In addition, awareness initiatives and the cross-exchange of know-how and practices among airport operators should be supported to leverage lessons learned and existing good practices. These actions would enable the identification of common standards and guidelines in areas where these are currently less effective and mature (e.g., how to design a new smart airport; how to measure the security of a smart airport and monitor threats including threat modelling and architecture analysis; networked architecture; ownership, and remote management; evidence-based vulnerability analysis metrics and priorities; data retention practices; etc.). Such guidelines and common practices could be based on the work of IATA, ICAO, ENISA, ECAC, ETSI and/or national CSIRTs. This recommendation directly addresses gap 1, 2, 3, 4, 5 6 and 8.

8.6 Facilitate the development of accreditation and third party auditing for cyber security in Smart airport

EU institutions should facilitate the development of accreditation schemes aimed at cyber security in Smart airports as well as third party auditing of Smart airports' operations related to cyber security. General objectives of such initiatives could either be to generate new certification strategies or harmonise existing ones, with the aim of ensuring that certification frameworks, targeted to Smart airport security operations, are adequate to meet existing and new EU requirements. Moreover, moving to greater mutual recognition among EU countries, increasing transparency of procedures, and improving the level and quality of interaction between approval and auditing bodies could raise the efficiency of the Smart airports in Europe and support constant improvement in EU security technology aimed at Smart airports. This recommendation directly addresses gap 1, 3, 4 and 5.

Recommendations for industry representatives

8.7 Collaborate with key stakeholders in the development of specific standards for cyber security products and solutions

Industry representatives should actively collaborate with airport operators and relevant European and international organisations (e.g.., ETSI, CEN, CENELEC, ENISA, DG MOVE, IATA and ICAO) in the development of security standards and specifications tailored to Smart airports' products and solutions. This will lead to coordinated efforts to strengthen cyber security for Smart airports, while reducing market fragmentation for cyber security products. This recommendation directly addresses gap 1 and 3.

8.8 Work with airport operators to develop products and/or solutions that are aligned to their cyber security requirements

Airport manufacturers and providers should work closely with airport operators to align their solutions and/or products to the cyber security requirements, needs and affordability-levels of airport operators. Solutions should be specifically tailored to address both existing gaps and the specific needs of airport operators (for instance working together to develop advanced interdependent threat analysis tools, and technologies that enable security in a multi-stakeholder environment). Products should also be developed by employing a security-by-design approach. This recommendation directly addresses gap 4, 5 and 7.

9. Annexes

9.1 Example of information security incidents impacting airports operations

DATE	COUNTRY	DESCRIPTION
August 2016	US	Thousands of air passengers around the world were left stranded after a power cut forced the US airline Delta to suspend flights.[146] The overnight power failure took place in Atlanta, near Delta's headquarters, causing computer systems to crash. Airport check-in systems, passenger advisory screens, the airline's website and smartphone apps were all affected by the system failure.
July 2016	Vietnam	Attackers successfully attacked Vietnam's two largest airports and the nation's flag carrier, Vietnam Airlines[147]. The attackers briefly hijacked flight information screens and sound systems inside the two airports. Instead of departure and arrival details, the airports' flight screens and speakers broadcasted what local media described as anti-Vietnamese and Philippines slogans, in turn prompting authorities to shut down both systems. Vietnam Airlines' website, meanwhile, was also seized and transferred to a malicious website abroad, while passenger data pertaining to an undisclosed number of its frequent flyers was published online as well. As a result of this attack Vietnamese authorities will carry out a comprehensive check on Chinese devices and technology to ensure information security at the Vietnamese airports since it is feared that the Chinese hacker group 1937cn might be responsible for the attacks.[148]
July 2016	IT	A third party failure at Rome's Fiumicino airport caused the shutdown of the automated passenger check-in system, which in turn caused two hours' delays for the passenger checking operation.[149] The failure was related to the internet connection (Fastweb) that the

[146] Delta: Power cut strands thousands of passengers, http://www.bbc.co.uk/news/world-us-canada-37007908.

[147] Cyberattack claims multiple airports in Vietnam, http://www.washingtontimes.com/news/2016/jul/29/cyberattack-claims-multiple-airports-vietnam-airli/.

[148] Vietnam to inspect use of Chinese technology following cyberattacks on airports, http://tuoitrenews.vn/society/36329/vietnam-to-inspect-use-of-chinese-technology-following-cyberattacks-on-airports.

[149] Aeroporto di Fiumicino, ore di stop e code al check in per un guasto alla connessione, http://roma.repubblica.it/cronaca/2016/07/18/news/fiumicino_problema_tecnico_al_t3_code_per_i_controlli_arrivano_in_strada-144357812/?ref=HREC1-6.

		automated passenger check–in at the airport uses for accessing and processing passenger data.
April 2016	UK	After landing, the pilot of a British Airways flight from Geneva reported a collision with a drone while approaching the London Heathrow airport on the 17th April.[150] The incident highlighted the issues faced with regard to drones. While the threat of bird strikes has been well researched, there is still little data about how much damage a drone could cause to an airplane.[151]
April 2016	Worldwide	The civil aircraft manufacturer Airbus Group is hit by up to 12 cyber-attacks per year, mostly in the form of ransomware and hostile actions carried out by state-sponsored attackers.[152] Airbus' chief information security officer cited an instance of ransomware compromising a computer, used by an employee offsite, which then (after the computer was connected to the company's intranet) spread over Airbus' corporate network, encrypting the contents stored on the hard drives of several machines.
November 2015	France	In November 2015, a bug due to obsolete versions of the operating systems in use caused disruptions at the Paris Orly airport.[153] The failure affected a system known as DÉCOR, which is used by air traffic controllers to communicate weather information to pilots who usually rely on such a system when weather conditions are poor. DÉCOR runs on Windows 3.1, released in 1992.[154]
June 2015	Poland	In June 2015, around 1,400 passengers were delayed at Warsaw's Chopin airport when the flight plan system went offline after its servers were overloaded by fraudulent information requests as part of a Distributed Denial of Service (DDoS) attack.[155] As a result the airport was not able to create flight plans and outbound flights were not able to depart.[156] This resulted in a 5-hour

[150] 'Drone' hits British Airways plane approaching Heathrow, with no damage caused, http://www.airportwatch.org.uk/2016/04/drone-hits-british-airways-plane-approaching-heathrow-with-no-damage-caused/.

[151] 'Drone' hits British Airways plane approaching Heathrow Airport, http://www.bbc.co.uk/news/uk-36067591.

[152] How Airbus defends against 12 big cyber attacks each year, http://www.itnews.com.au/news/how-airbus-defends-against-12-big-cyber-attacks-each-year-418131.

[153] Planes grounded at Paris Orly airport thanks to Windows 3.1 error, http://www.itpro.co.uk/security/25597/planes-grounded-at-paris-orly-airport-thanks-to-windows-31-error.

[154] Windows 3.1 Is Still Alive, And It Just Killed a French Airport, https://news.vice.com/article/windows-31-is-still-alive-and-it-just-killed-a-french-airport.

[155] Polish Airport Hack a Reminder that Airlines are at Risk for Cyber Attacks, http://www.thetelecomblog.com/2015/06/23/polish-airport-hack-a-reminder-that-airlines-are-at-risk-for-cyber-attacks/.

[156] Today afternoon LOT encountered IT attack, that affected our ground operation systems, http://corporate.lot.com/pl/en/press-news?article=772922.

		recovery time with 10 cancelled flights and around 15 delayed flights.[157]
June 2015	USA	In June 2015, about 400,000 United Airlines passengers were delayed in the US due to a problem with a network router. [158] [159] [160] Blaming network connectivity issues, the company ordered a ground stop to its domestic flights, as well as those flown by its regional United Express partners. [161]
May 2015	Belgium	In May 2015, the Belgian airspace was closed after technical problems escalated up to the shutdown of air traffic control systems, causing hundreds of flights to be cancelled and diverted around Europe.[162] [163] The incident has been attributed to a power outage and a malfunctioning emergency generator.[164]
December 2014	UK	In December 2014, a major computer failure at the main air traffic control centre in London caused massive disruptions to flights in and out of the global travel hub.[165] [166] [167] [168] [169]
July 2013	Turkey	In July 2013, an alleged cyber-attack led to the shutdown of the passport control systems at the departure terminals at Istanbul Atatürk and Sabiha Gökçen airports in Turkey causing many flights to be delayed.[170] [171] [172]

[157] Hack attack leaves 1,400 airline passengers grounded, http://www.cnbc.com/2015/06/22/hack-attack-leaves-1400-passengers-of-polish-airline-lot-grounded.html.

[158] United Airlines Grounds Flights, Citing Computer Problems, http://www.nytimes.com/2015/07/09/business/united-airlines-grounds-flights-citing-computer-glitch.html?_r=0.

[159] Computer glitch halts United Airlines flights for two hours, http://www.reuters.com/article/us-ual-flights-idUSKCN0PI1IX20150708.

[160] United Airlines flights restored after worldwide groundstop, http://www.cnbc.com/2015/07/08/all-united-airlines-flights-in-us-grounded-due-to-computer-system-glitch.html.

[161] Glitches freeze United Airlines, NYSE temporarily on Wednesday, http://www.chicagotribune.com/news/local/breaking/ct-united-grounds-flights-nationwide-because-of-automation-issues-20150708-story.html

[162] Belgian airspace closed: Air traffic control failure grounds all flights causing 'chaos' at Brussels airport and diversions around Europe, http://www.independent.co.uk/travel/news-and-advice/belgian-airspace-closed-air-traffic-control-failure-grounds-all-flights-causing-chaos-at-brussels-10278525.html.

[163] Travel chaos in Belgium as flights in and out of the country are halted due to power failure at air traffic control centre, http://www.dailymail.co.uk/travel/travel_news/article-3098915/Travel-chaos-Belgium-flights-country-halted-power-failure-air-traffic-control-centre.html.

[164] Air traffic back at 75%; 35,000 still stranded, http://deredactie.be/cm/vrtnieuws.english/News/1.2351961.

[165] Flights disrupted after computer failure at UK control centre, http://www.bbc.com/news/uk-30454240.

[166] London airspace shuts after 'computer failure', http://www.independent.co.uk/news/uk/home-news/london-flights-disrupted-after-computer-failure-9921436.html.

[167] London airspace shuts after 'computer failure' , http://www.independent.co.uk/news/uk/home-news/london-flights-disrupted-after-computer-failure-9921436.html.

[168] Flights disrupted as computer failure causes chaos at UK airports, http://www.theguardian.com/uk-news/2014/dec/12/heathrow-london-air-space-closed-computer-failure.

[169] London flights disrupted after a computer failure at air traffic control centre, http://www.abc.net.au/news/2014-12-13/computer-failure-causes-massive-flight-disruption-in-london/5965084.

[170] Virus attack strikes at both Istanbul airports, http://www.hurriyetdailynews.com/virus-attack-strikes-at-both-istanbul-airports.aspx?pageID=238&nID=51449&NewsCatID=341

[171] Cyber attack hits Istanbul airport passport control system, http://thehackernews.com/2013/07/Istanbul-airport-cyber-attack-virus.html

[172] We need to talk about cyber-security, http://www.airport-business.com/2014/06/need-talk-cyber-security/

2013	USA	In 2013, a phishing scam seeking to breach US commercial aviation networks targeted 75 US airports.[173] [174] [175]
August 2012	USA	In August 2012, according to the Boston-based digital security firm Trusteer, malware hidden in the private network of a major non-U.S. international airport was found.[176] [177] [178] [179] The Citadel Trojan (which can be inadvertently installed by a user by simply clicking on a web link) was discovered during a routine security sweep of computers protected by Trusteer's software. The Citadel Trojan typically uses sophisticated techniques to steal credentials, such as employees who logged in remotely to the airport's VPN.
June 2011	India	In June 2011, a failure of the Common Use Passengers Processing System (CUPPS) at the Indira Gandhi International (IGI) Airport caused the delay of 50 flights, with their passengers that had to be boarded following manual procedures.[180] [181] [182]
February 2009	USA	In February 2009, The Federal Aviation Administration's (FAA) Air-Traffic Networks were breached by attackers who obtained access to personal information (including social security numbers) on 48,000 past and present FAA employees.[183] [184] [185] [186]
July 2008	Canada	E-ticketing kiosks at Toronto airport, using credit card authentication, were tampered with in order to steal passengers' credit card details.[187]

[173] Phishing Scam Targeted 75 US Airports, http://www.informationweek.com/government/cybersecurity/phishing-scam-targeted-75-us-airports/d/d-id/1278762

[174] Nation State-sponsored Attackers Hacked Two Airports, Report Says, http://www.nextgov.com/cybersecurity/2014/06/nation-state-sponsored-attackers-hacked-two-airports-report-says/86812/

[175] Airports, Other Critical Infrastructure Present Lucrative Attacker Target, https://www.entrust.com/airports-critical-infrastructures-present-lucrative-attacker-target/

[176] Cyberwars Reach a New Frontier: the Airport, http://www.businessweek.com/articles/2012-08-15/cyber-wars-reach-a-new-frontier-the-airport

[177] Man-in-the-Browser: Citadel Trojan Targets Airport Employees With VPN Attack, https://securityintelligence.com/man-browser-citadel-trojan-targets-airport-employees-vpn-attack/

[178] Citadel Trojan Linked to Attacks on VPN at International Airport, http://www.securityweek.com/citadel-trojan-linked-attacks-vpn-international-airport

[179] Airport VPN hacked using Citadel malware, http://www.scmagazine.com/airport-vpn-hacked-using-citadel-malware/article/254604/

[180] CBI believes cyber attack led to IGI airport's technical problems in June, http://www.zdnet.com/blog/india/cbi-believes-cyber-attack-led-to-igi-airports-technical-problems-in-june/710

[181] Over 50 flights delayed at IGI airport, http://www.thehindu.com/news/cities/delhi/article2144227.ece

[182] Solution for cash crunch! What are micro-ATMs and how do they function?, http://archive.financialexpress.com/news/cyber-attack-led-to-igi-shutdown/851365/0

[183] Hackers breach US air traffic control computers, http://phys.org/news/2009-05-attackers-breach-air-traffic.html

[184] FAA's Air-Traffic Networks Breached by Hackers, http://www.wsj.com/articles/SB124165272826193727

[185] Thoughts on Critical Infrastructure Protection, http://www.nartv.org/2009/12/13/thoughts-on-critical-infrastructure-protection/

[186] Report: Hackers broke into FAA air traffic control system, http://www.cnet.com/news/report-attackers-broke-into-faa-air-traffic-control-systems/

[187] Toronto airline kiosks breached, http://www.flyingpenguin.com/?p=1734

9.2 Key EU Legislation and relevant legislation affecting Smart airports

This table briefly describes the key EU regulations, directives and opinions that combine to form the *legal and regulatory environment* governing Smart airports at the EU level. Each legal instrument has been categorised according to whether its implementation effects: Air Traffic Management; Protection and Processing of Passenger Data; Technical Standards (including inspections); Minimum Standards on Basic Aviation Security; and/or Security Risk Management.

EU EXISTING LEGISLATION			
Title	**Domain(s)**	**Description**	**Impacts on Smart airports**
EU Network Information Security (NIS) Directive[188]	Security Risk Management; Air Traffic Management; Minimum Standards on Basic Aviation Security	It places a duty on operators of essential services (including airports) to *manage the risks posed to the security of networks and information systems which they control and use in their operations*. The broad aim of the proposed Directive is to again, ensure a common (high) level of network and information security across Member States that will require operators of essential services such as energy, transport, and key providers of information society services (e-commerce platforms, social networks, etc.), as well as public administrations to adopt appropriate steps to manage security risks and report serious incidents to the national competent authorities.	Imposes new network and information security requirements on operators of essential services including Smart airport operators and their third party providers, and digital service providers (DSPs). Those organisations are also required to report certain security incidents to competent authorities or Computer Security Incident Response Teams (CSIRTs). Each EU country must establish these teams, the Directive says. Different security and incident reporting rules will apply to operators of essential services than to DSPs, with a lighter touch framework applicable to DSPs.
Commission Implementing Regulation (EU) (EU) 2016/1377 of 4 August 2016 laying down common requirements for service providers and the oversight in air traffic management/air navigation services and other air traffic management	Air Traffic management	The Regulation 2016/1377 laying down common requirements for service providers and the oversight in ATM/ANS and other ATM network functions (repealing Regulation No 482/2008, Implementing Regulations No 1034/2011 and No 1035/2011 and amending Regulation No 677/2011) and its relevant Acceptable Means of Compliance (AMC) and Guidance Material (GM). It combines theory and practical exercises based on both ATM and non-ATM examples of	Set up common requirements for ATM and ANS providers and the declaration of political relevance of security in general, and especially the relevance of security as a key enabler of the (aeronautical) safety, which is paramount in the aviation context. Specifically , air navigation services and air traffic flow management providers and the Network Manager shall take the necessary measures to protect their systems, constituents in use and data and prevent compromising the network against information and cyber security threats which may have an unlawful

[188] Proposal for a directive of the European Parliament and of Council concerning measures to ensure a high common level of network and information security across the Union (COM/2013/048 final - 2013/0027 (COD)). http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52013PC0048.

EU EXISTING LEGISLATION			
network functions, repealing Regulation (EC) No 482/2008, Implementing Regulations (EU) No 1034/2011 and (EU) No 1035/2011 and amending Regulation (EU) No 677/2011		changes.	interference with the provision of their service.
Opinion 8/2014 on the Recent Developments on the Internet of Things (IOT) [189]	Protection and processing of passenger data	Privacy and security risks in IOT in general, social implications, contribution to uniform legal application across IOT, including main data protection risks.	Practical recommendations for OS and device manufacturers, and application developers, that facilitate the exercise of rights of access, modification and deletion of personal information and data, following a 'privacy by design' approach that minimizes the amount of data required to run the passenger service.
Commission Regulation (EU) No 677/2011 of 7 July 2011 laying down detailed rules for the implementation of ATM network functions	Air Traffic Management	Established the role of the role of European Network Manager	This Regulation defines detailed rules for the implementation of air traffic management (ATM) network functions in Europe in order to allow optimum use of airspace in the SES area and ensure that airspace users can operate preferred trajectories, while allowing maximum access to airspaces and air navigation services. The Regulation applies to Member States, European Aviation Safety Agency, airspace users, air navigation service providers, airport operators, airport slot coordinators and operating organisations, at national or functional airspace block (FAB) level.

[189] Opinion 8/2014 on the on Recent Developments on the Internet of Things, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.

EU EXISTING LEGISLATION			
Regulation (EC) no 216/2008 of the European Parliament and the Council of 20 February 2008 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency. [190]	Minimum Standards on Basic Aviation Security; Technical Standards; Air Traffic Management	Established European Aviation Security Agency (EASA)	Establishes the EASA, tasked with: a) the certification and approval of products in fields where EASA has exclusive competence (e.g. airworthiness); b) Provide oversight and support to Member States on Air Operations and Air Traffic Management; c) Promote the use of European standards; and d) Co-operate with international actors in order to achieve the highest safety level for EU citizens e.g. EU safety list and Third Country Operator Authorisations. Proposals to repeal Regulation (EC) No 216/2008 of the European Parliament and of the Council and to implement proposals outlined in COM/2015/0613 final - 2015/0277 (COD)[191]. The main change as compared to Regulation (EC) No 216/2008 concerns clarification that cyber security aspects are to be taken into account in the design of the aircraft (1.3.5). Furthermore, experience gained through the practical implementation of that Regulation is reflected and the concept of non-installed equipment is introduced (including essential requirements for non-installed equipment). Annex VIII also proposes to have cyber security aspects added in the essential requirements dealing with aeronautical information and data (Point 2.1.3) and system and constituent integrity (Point 3.3). Under the present initiative a limited number of specific areas are proposed to be added to this overall Union aviation safety framework, namely unmanned aircraft, safety of ground handling services and security aspects of aircraft and aviation systems' design, including cyber security."[192]
Regulation (EC) No 1108/2009, amending Regulation (EC) No 216/2008 {in	Minimum Standards on Basic Aviation Security; Technical	Amendments, extending the tasks of EASA towards a "total system approach" to extend	This new responsibility mandated the Agency to prepare draft safety rules for aerodromes as well as common rules for certification and oversight by the

[190] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:079:0001:0049:EN:PDF.
[191] http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2015:0613:FIN
[192] Ibid.

EU EXISTING LEGISLATION			
the field of aerodromes, air traffic management and air navigation services and repealing Directive 2006/23/EC[193]	Standards; Air Traffic Management	EASA activities to include aerodromes.	National Aviation Authorities (NAAs) in support of the European Commission. Proposed Implementing Rules contain the conditions for the issuing of certificates, the obligations and privileges of certificate holders, and sanctions in case of non-compliance.
Commission Regulation (EU) No 18/2010 of 8 January 2010 amending Regulation (EC) No 300/2008 of the European Parliament and of the Council as far as specifications for national quality control programmes in the field of civil aviation security are concerned[194]	Minimum Standards on Basic Aviation Security	Necessity of developing a harmonised way of reporting on the quality control measures. National measures should be based on best practices, and those best practices should be shared with the Commission. Adds an Annex II to 300/3008/EC on Common specifications for the national quality control programme to be implemented by each Member State in the field of civil aviation security.	The objectives of the national quality control programme are to verify that aviation security measures are effectively and properly implemented and to determine the level of compliance with the provisions of this Regulation and the national civil aviation security programme, by means of compliance monitoring activities. - Includes requirements and definitions of a security audit, inspections, tests and reporting requirements.
Commission Regulation (EU) No 72/2010 of 26 January 2010 laying down procedures for conducting Commission inspections in the field of aviation security (Text with EEA relevance)[195]	Minimum Standards on Basic Aviation Security	It focuses on aviation security.	This Regulation lays down procedures for conducting Commission inspections to monitor the application by Member States of Regulation (EC) No 300/2008. Commission inspections shall cover appropriate authorities of Member States and selected airports, operators and entities applying aviation security standards. The inspections shall be conducted in a transparent, effective, harmonised and consistent manner.
Commission Implementing Regulation (EU) No 1035/2011 laying down common requirements for the provision of air navigation services and amending Regulations (EC) No 482/2008 and (EU) No 691/2010.	Requirements for air navigation security	It establishes requirements for air space security, personal security, computer network system security and cyber security.	European Commission Implementing Regulation (EU) 2016/1377 of 4 August 2016 laying down common requirements for service providers and the oversight in air traffic management/air navigation services and other air traffic management network functions, repealing Regulation (EC) 482/2008, Implementing Regulations (EU) 1034/2011 and (EU) 1035/2011 and amending Regulation (EU) 677/2011, was published in the Official Journal on 19 August 2016.
Commission Implementing Regulation (EU)	Aviation security	Sets out the detailed measures for the implementation of the common basic standards for	This contains requirements around secured areas, access control, identification cards, screening of

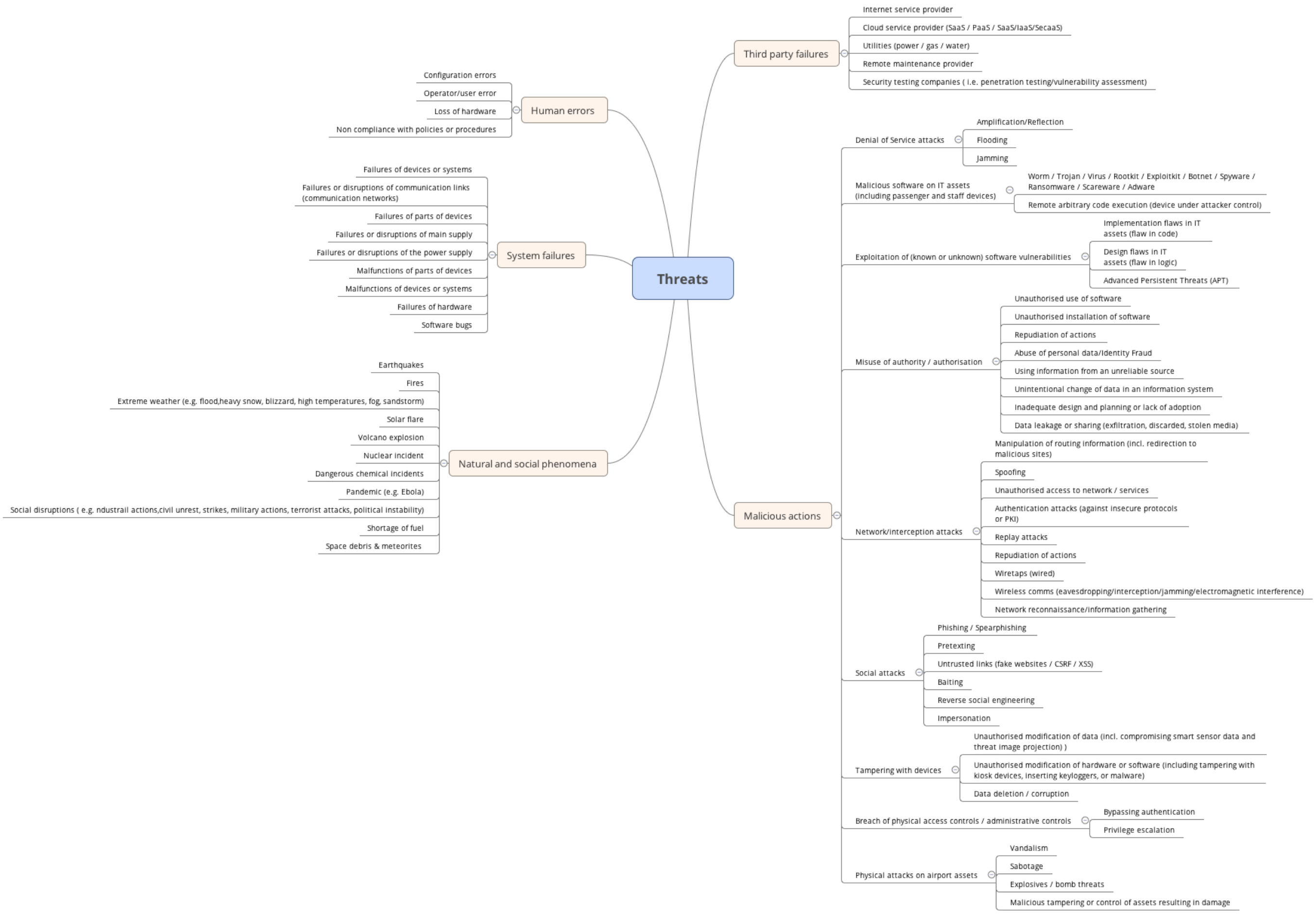
[193] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:309:0051:0070:EN:PDF.
[194] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32010R0018
[195] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:023:0001:0005:EN:PDF.

EU EXISTING LEGISLATION			
2015/1998 of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security (Text with EEA relevance) [196]		safeguarding civil aviation against acts of unlawful interference that jeopardise the security of civil aviation, referred to in Article 4(1) of Regulation (EC) No 300/2008, and the general measures supplementing those common basic standards, referred to in Article 4(2) of that Regulation	persons and vehicles, surveillance patrols and other physical controls, disruptive passengers, protection of aircraft, cargo and mail screening, regulated agents (any third party providing security controls), methods of screening using new technologies, standards for security scanners,
Commission Implementing Regulation (EU) 2015/2426 of 18 December 2015 amending Regulation (EU) 2015/1998 as regards third countries recognised as applying security standards equivalent to the common basic standards on civil aviation security (Text with EEA relevance)[197]	Minimum Standards on Basic Aviation Security	Extends the list of third countries that meet the basic or minimum requirements on aviation security apparatus.	Amends 2015/1998/EU (recognises Canada, USA, and Montenegro and others as meeting the basic standards)

[196] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015R1998.

[197] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R2426&from=EN.

9.3 Detailed Third Level Threat Taxonomy


Threats
Human errors
Configuration errors
Operator/user error
Loss of hardware
Non compliance with policies or procedures
System failures
Failures of devices or systems
Failures or disruptions of communication links (communication networks)
Failures of parts of devices
Failures or disruptions of main supply
Failures or disruptions of the power supply
Malfunctions of parts of devices
Malfunctions of devices or systems
Failures of hardware
Software bugs
Natural and social phenomena
Earthquakes
Fires
Extreme weather (e.g. flood,heavy snow, blizzard, high temperatures, fog, sandstorm)
Solar flare
Volcano explosion
Nuclear incident
Dangerous chemical incidents
Pandemic (e.g. Ebola)
Social disruptions (e.g. ndustrail actions,civil unrest, strikes, military actions, terrorist attacks, political instability)
Shortage of fuel
Space debris & meteorites
Third party failures
Internet service provider
Cloud service provider (SaaS / PaaS / SaaS/IaaS/SecaaS)
Utilities (power / gas / water)
Remote maintenance provider
Security testing companies (i.e. penetration testing/vulnerability assessment)
Malicious actions
Denial of Service attacks
Amplification/Reflection
Flooding
Jamming
Malicious software on IT assets (including passenger and staff devices)
Worm / Trojan / Virus / Rootkit / Exploitkit / Botnet / Spyware / Ransomware / Scareware / Adware
Remote arbitrary code execution (device under attacker control)
Exploitation of (known or unknown) software vulnerabilities
Implementation flaws in IT assets (flaw in code)
Design flaws in IT assets (flaw in logic)
Advanced Persistent Threats (APT)
Misuse of authority / authorisation
Unauthorised use of software
Unauthorised installation of software
Repudiation of actions
Abuse of personal data/Identity Fraud
Using information from an unreliable source
Unintentional change of data in an information system
Inadequate design and planning or lack of adoption
Data leakage or sharing (exfiltration, discarded, stolen media)
Network/interception attacks
Manipulation of routing information (incl. redirection to malicious sites)
Spoofing
Unauthorised access to network / services
Authentication attacks (against insecure protocols or PKI)
Replay attacks
Repudiation of actions
Wiretaps (wired)
Wireless comms (eavesdropping/interception/jamming/electromagnetic interference)
Network reconnaissance/information gathering
Social attacks
Phishing / Spearphishing
Pretexting
Untrusted links (fake websites / CSRF / XSS)
Baiting
Reverse social engineering
Impersonation
Tampering with devices
Unauthorised modification of data (incl. compromising smart sensor data and threat image projection))
Unauthorised modification of hardware or software (including tampering with kiosk devices, inserting keyloggers, or malware)
Data deletion / corruption
Breach of physical access controls / administrative controls
Bypassing authentication
Privilege escalation
Physical attacks on airport assets
Vandalism
Sabotage
Explosives / bomb threats
Malicious tampering or control of assets resulting in damage

9.4 Main Threats to Smart Airport and related affected assets

CATEGORY	THREAT	VARIANTS	ASSET GROUP AFFECTED	ASSETS AFFECTED
Malicious actions	Denial of Service attacks	Amplification / Reflection Flooding Jamming	**IT & Comms**	- Communication Systems - Global Positioning Systems - Cloud-based Data and Application Services - Network Security Management - Wide Area Networks - Air to Satellite Comms systems - Mobile Network and Apps
	Malicious software on airport IT assets	Worm / Trojan / Virus / Rootkit / Exploit kit / Botnet / Spyware / Ransomware / Scareware / Adware	**Customer Ancillary Sys.**	- Point of Sales Machines - Automatic Teller Machines
			Safety and Security	- Fire Fighting Services and System - Common-Use Passenger Processing Systems (CUPPS)
			Airline/Airside Operations	- Air Traffic Management, Navigation Aids and Approach - Flight Tracking Systems - Airline Gateway Server Systems
			IT & Comms	- Local Area Network (LAN) Systems and VPN - IT equipment (Hardware and Software) - Flight Information Display System and Management
			Passenger Management	- Kiosk Devices (E-ticketing) - Stationary Devices (desktops, laptops, ports) - Passenger Name Record (PNR) - Central Reservation Systems (CRS) - Passenger Check in- and Boarding
	Exploitation of (known or unknown) software vulnerabilities	Implementation flaws in IT assets Design flaws in IT assets	**Facilities and Maintenance**	- SCADA (Roads) - SCADA (Aprons, Ancillary Areas) - SCADA (Utilities) - Environmental Management Systems

			Passenger Management	- Way-finding Service - Stationary devices (desktops, laptops, ports)
			Airside Operations	- Airfield Lighting Control Systems and Runway Monitoring - Air Traffic Management (ATM), Navigation Aids and Approach - Flight Tracking Systems
			Landside Operations	- Airport Landside Operations Systems Control Centre
			IT & Comms	- IT Hardware and Software - Cloud-based Data and Application Services Mobile Network & Apps
	Misuse of authority / authorisation	Unauthorised use of software and admin tools Unauthorised installation of software Repudiation of actions Abuse of personal data / identity fraud Using information from an unreliable source Unintentional change of data in an information system Inadequate design and planning or lack of adoption Data leakage or sharing (exfiltration / discarded / stolen media)	**Staff Management**	- Staff Authentication Systems
			Airport Administration	- Human Resources Management System - Asset Inventory Management System - Enterprise Management Systems - Procurement Management Systems - Financial Management Systems - Policy Management Systems
			Landside Operations	- Landside Operations Systems Control Centre
			Passenger Management	- Central Reservation Systems (CRS) - Passenger name Record (PNR) - Passenger Check-in and Boarding
			Safety and Security	- Common-Use Passenger Processing Systems (CUPPS) - Baggage Screening Systems - Authentication systems - Access Control Systems - Passenger Screening Systems

	Network / interception attacks	Manipulation of routing information (incl. redirection to malicious sites / DNS attacks) Spoofing[198] Unauthorised access to network / services Authentication attacks (against insecure protocols or PKI) Replay attacks Repudiation of actions Wiretaps (wired) Wireless comms (eavesdropping / interception / jamming/electromagnetic interference Network reconnaissance / information gathering	**IT & Comms**	- LAN and VPN Systems - Air Traffic Management - Communication Systems - GPS/EGNOS/SBAS/GBAS - Cloud-based Data and Application Services - Network Security Management - Wide Area Networks (WAN) - Common Comms network - Passenger-Airline Comms - Air to Satellite Comms - Mobile Network & Apps
			Safety and Security	- Baggage Screening Systems - Baggage Handling - Passenger Screening Systems - Common-Use Passenger Processing Systems (CUPPS)
			Facilities and Maintenance	- SCADA
			Passenger Management	- Way-finding Services - Central Reservation Systems - Passenger Check-in Boarding
	Social attacks	Phishing Pretexting Untrusted links (fake websites / CSRF / XSS) Baiting Reverse social engineering Impersonation	**Passenger Management**	- Stationary Devices (desktops, laptops, ports)
			Airport Administration	- Enterprise Management System - Asset Inventory Management System Procurement Management System - Financial Management System
			IT & Comms	- IT Equipment
	Tampering with airport devices	Unauthorised modification of data (incl. compromising smart sensor data)	**IT & Comms**	- Stored data - IT equipment hardware and software. - Connected Internal and external IT Comms

[198] Spoofing an i-Beacon allows cloning and creating another beacon with the same ID. Also by sniffing out an i-Beacon profile you can implement the profile in your own app.

		Unauthorised modification of hardware or software (including tampering with kiosk devices, inserting keyloggers, or malware) Data deletion / corruption		- Network Security Management
			Passenger Management	- Kiosk devices (E-Ticketing) - Stationary Devices (Ports/smart safe/USB devices) - Central Reservation System (CRS)
			Airside Operation	- Airport Operational Database (AODB)
			Safety and Security	- Smart Surveillance Systems - Common-Use Passenger Processing Systems (CUPPS)
	Breach of physical access controls / administrative controls	Bypassing authentication Privilege escalation	**Safety and Security**	- Access control systems - Authentication Systems - Perimeter Intrusion Detection Systems (PIDS)
			Staff Management	- Staff Authentication Systems
			Passenger Management	- Stationary devices (laptops, ports)
	Physical attacks on airport assets	Explosives / bomb threats Sabotage Vandalism Malicious tampering or control of assets resulting in damage	**Safety and Security**	- Improvised Explosive Devices (IEDs) Systems - Baggage Screening Systems
			IT & Comms	- GPS/EGNOS/SBAS/GBAS
			Airside Operations	- Air Traffic Management, Navigation and Approach, - Departure control systems (DCS)
			Facilities and Maintenance	- SCADA (Aprons, Ancillary Area) - SCADA (Roads) - SCADA (Utilities)
Human errors		Configuration errors Operator/user error Loss of hardware Non-compliance with policies or procedures	**IT and Comms**	- All
			Staff Management	- All
			Passenger Management	- All
			Facilities and Maintenance	- All
			Airport Administration	- All
			Airside Operations	- All
			Landside Operations	- All

			Safety and Security	- All
			Customer Ancillary Services	- All
System failures		Failures of devices or systems Failures or disruptions of communication links (communication networks) Failures of parts of devices Failures or disruptions of main supply Failures or disruptions of the power supply Malfunctions of parts of devices Malfunctions of devices or systems Failures of hardware Software bugs	**Customer Ancillary Sys.**	- Point of Sales Machines - Automatic Teller Machines - Commercial cross management services - Private, VIP and disable support
			IT & Comms	- LAN and VPN Systems - IT equipment (Hardware and Software) - Mobile Network & apps - Network Security Management - Wide Area Network - Common Communication Network - Passenger-Airline Communication Systems - Air to Satellite Communication Systems
			Airside Operations	- Air Traffic Management (ATM), Navigation, Aids and Approach - Flight Tracking Systems - Local DCS weight and balance - Meteorological Information systems - Departure Control Systems - De-icing Systems - Airfield Lighting Control Systems - Cargo Processing Systems - Aircraft Re-fuelling Systems - Portable Aircraft Data Loader
			Landside Operations	- All
			Safety and Security	- Access Control Systems - Authentication Systems - Badging Systems - Baggage Screening Systems - Smart Surveillance Systems - Improvised Explosive Detection Systems - Passenger Screening Systems - Perimeter Intrusion Detection Systems - Common-Use Passenger Processing Systems

				- Firefighting services and detections Systems
			Staff Management	- All
			Airport Administration	- All
			Facilities and Management	- All
			Passenger Management	- All
Natural and social phenomena		Earthquakes Fires Extreme weather Solar flare Volcano explosion Nuclear incidents Dangerous chemical incidents Pandemic Social disruptions Shortage of fuel Space debris & meteorites	**Facilities & Management**	- All
			Landside Operations	- All
			Safety and Security	- All
			Airport Administration	- All
			Customer Ancillary Services	- All
			Staff Management	- All
			Passenger Management	- All
			Airside Operations	- All
			IT & Comms	- All
Third party failures		Internet service provider Cloud service provider (SaaS / PaaS / SaaS/Iaas/SecaaS) Utilities (power / gas / water) Remote maintenance provider Security testing companies	**Staff Management**	- Staff Authentication Systems
			Safety and Security	- Firefighting Services and Detection Systems - Common-Use Passenger Processing Systems (CUPPS)
			Airport Administration	- HR Management - Asset Inventory Management - Enterprise Management Systems - Procurement Management Systems
			IT and Comms	- LAN and VPN - Mobile Network & apps - Cloud-based data and application services - Network Security Management - WAN

				- Common Communication Network
			Landside Operations	- Parking Management Systems - Public and non-public Transport Systems - Way-finding services
			Facilities and Maintenance	- Energy Management
			Passenger Management	- Way –finding Services

9.5 Detailed security good practices

9.5.1 Technical/Tool-based

CATEGORY	GOOD PRACTICE	THREAT GROUPS ADDRESSED
Employ appropriate cyber security and protection measures	**GP01 – Intrusion Detection Systems (IDS):** Refers to monitoring of both software and hardware devices over wired and wireless networks. IDS can be categorised as follows: • Network based intrusion detection systems focused on the analysis of network traffic and the detection of broader actions (i.e. network scan, vulnerability assessment, spoofing, etc.) either from outside or internal attackers • Host based intrusion detection systems which are able to analyse activities on the host (e.g., servers, workstations, embedded devices, etc.) and raise an alert in case of events such as unauthorised access to applications, escalation of privileges, modification of file systems, connection of peripherals, etc.). IDS alerts should be investigated and acted upon, e.g. via forensic investigation. IDS implementation should ensure compliance with relevant standards (e.g., ED-153).	**Malicious actions** -Denial of service attacks -Malicious software on airport IT assets -Exploitation of (known or unknown) software vulnerabilities -Network/interception attacks -Social attacks
	GP02 – Antimalware: Computers should run antimalware software (also known as antivirus) to detect and remove and/or quarantine malicious software. This includes but is not limited to: kiosk devices, IT equipment, Common-Use Passenger Processing Systems (CUPPS), SCADA, and Cloud-based data and application services, etc. It is also recommended to use multi-engine anti-virus solutions to check against maximum virus signatures in order to better protect available resources.	**Malicious actions** -Malicious software on airport IT assets -Tampering with airport devices -Misuse of authority/authorisation
	GP03 – Change default credentials of devices: Devices, connected to the airport network, such as routers, access points, IP-cameras and/or surveillance cameras connected to closer networks, should be properly configured and default user accounts should not be used, or should have the default password changed. In addition, when not required, remote access should be disabled to prevent cyber criminals from attempting remote connection to devices. For critical assets, password enforcement policy should be implemented, avoiding the adoption of computationally weak passwords.	**Malicious actions** -Misuse of authority / authorisation -Breach of physical access controls
	GP04 – Bring your own device (BYOD) controls: Airports should typically prevent employees from connecting their own personal devices to airport systems (including via Wi-Fi, Ethernet, or VPN), and where this is not appropriate apply effective technical controls to protect the airport and the network infrastructure from rouge or compromised devices. Due to the lack of control on BYOD mixed infrastructures, these appliances should be kept off the perimeter of relevant servers and services and network access of these devices should be regulated by individual credentials associated to the device (for example, using digital certificates). Wherever possible, these devices should operate under a policy based infrastructure while joining the airport	**Malicious actions** -Misuse of authority / authorisation -Breach of physical access controls -Malicious software on airport IT assets -Network/interception attacks

	IT domain, giving a more restricted environment (i.e. restriction of peripherals usage via group policy).	
	GP05 – Monitoring and auditing for malicious insiders: This includes: *A: Logging systems:* Log files should be managed and monitored to review system and user activity across airport systems. *B: Real-time monitoring:* Log files should be stored securely, and should enable non-repudiation. For example, a security information and event management (SIEM) software solution enables a centralised system for real-time analysis of recorded events including events correlation and alerting *B: Integrity management:* Integrity management solutions should be used to monitor systems for unauthorised changes: for example, modified software on a shared server. *C: Data Loss Prevention (DLP)*: DLP systems can be used to detect and/or prevent sensitive data at rest (such as an employee copying sensitive files onto a USB storage drive) or in-motion (being copied over a network). This can be combined with periodic, without notice, activity auditing of users. In order to prevent data leakage, a special attention to stenographic communication should be paid, due to this emerging approach in establishing covert channels in restricted environments. Networks should be scanned for rogue access points.	**Malicious actions** -Denial of service attacks -Exploitation of software vulnerabilities -Misuse of authority / authorisation -Breach of physical access controls -Malicious software on airport IT assets -Network/interception attacks -Tampering with airport devices
	GP06 – Software and hardware updates: Software should be regularly updated to avoid cyber criminals exploiting patched software vulnerabilities to get access to devices and related data storage. Therefore, the airport system administrator should plan a software update procedure to ensure systems are kept up-to date so mitigating the possibility of security attacks. The 'window of vulnerability' refers to the time taken for a vulnerability being introduced into the software (such as a programming mistake), its discovery, vendor fix, and eventual updates applied to systems to remove the vulnerability. Applying security patches is an important practice that reduces the exposure to known vulnerabilities. Disposal of obsolete hardware has to be done carefully to prevent access to specialised hardware and software (i.e. interfaces and software for baggage security scanning hardware interaction) or data (activity logs, stored credentials) from devices at their end of life. Physical or logical destruction of end-of-life hardware, software and data should be ensured.	**Malicious actions** -Malicious software on airport IT assets -Exploitation of software vulnerabilities -Misuse of authority/authorisation -Social attacks
Employ secure digital access controls to networks and data	**GP07 – Security hardening of systems:** Airports should reduce systems' surface of vulnerability (i.e. attack surface) by for instance disabling services, closing ports, restricting usage of external devices, regular patching of systems, etc. This is particularly relevant for systems in the demilitarised zone (DMZ)[199].Network devices should not have services enabled that are not required as this provides additional attack surface, which may be exploited by malicious users. For this reason, system administrators should disable those services that are not needed and also should close or block connections that are not required. External device access should be controlled and authorised only on explicit requests. Access to external peripherals (i.e. USB storage drives) should be denied wherever possible, in order to prevent data leakage or unauthorised introduction of software. Internet activity (i.e. web navigation, and social	**Malicious actions** -Denial of service attacks -Exploitation of software vulnerabilities -Tampering with airport devices

[199] DMZ or demilitarised zone (sometimes referred to as a perimeter network) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a usually larger and untrusted network, usually the Internet.

network activities) should be subject to filtering, either for security scanning purposes or white/black listing.	
GP08 – Conduct security assessments and penetration tests: Airports should undergo various forms of security assessment, to detect security vulnerabilities and assess their impact. Vulnerability assessment involves an automated scan of connected systems; these scans should be regularly performed (potentially automated on a daily basis) to detect changes in the security posture of the airport network. Vulnerability management solutions make this potentially within the preview of airport system administrators. Each relevant segment of the airport infrastructure can be scanned in a distributed fashion, and credentialed scans can also improve scan accuracy. Penetration tests should be performed to provide a more thorough offensive assessment of the capabilities of a network, and such tests are typically required from the airport by external parties[200]. Other more advanced forms of security audit include threat modelling and architecture analysis, which can be applied to airport systems to identify otherwise difficult-to-identify weaknesses, such as modelling complex interactions between legacy systems and smart components. Additionally, periodic vulnerability scanning should be done in combination with hardening (see GP 07) to ensure systems are always updated and secure.	**Malicious actions** -Denial of service attacks -Exploitation of software vulnerabilities -Network attacks -Breach of physical access controls / administrative controls
GP09 – Least privilege and data classification: All users, processes, passengers, and airport employees should be granted the least level of privilege/authority necessary to enable them to perform their function. Airport data at rest should be classified to ensure that information is only accessible to those that need access and data classification should be part of any information security management system (see GP016). This can help to ensure data for airport use cannot trivially be made public. Security personnel should consider the use of access policies that define which users have access to the data, and enforcement mechanisms that protect on real-time the access of the data from unauthorised read. Access to sensitive data should be under mandatory access control (such as role-based-access-control, RBAC, policies), and should be reviewed and subject to external auditing on a regular basis. Access to data should be logged and logs should be stored in a secure location, to prevent unauthorised alteration. Furthermore, privacy impact assessment and privacy by design, based on the EU General Data Protection Regulation (GDPR), should be also followed for proper data and information management.	**Malicious actions** -Misuse of authority / authorisation **Human errors** -Operator/user error
GP10 – Data encryption: The use of encryption should be used to protect sensitive information exchanged in the network from eavesdroppers, and to protect data at rest. Insecure protocols, such as WEP and unencrypted Wi-Fi networks should be avoided. Encryption should be configured using peer-reviewed and academically sound standard solutions to protect data. The use of encryption, such as VPN, can enable employees to be remotely connected with the airport service keeping a high level of secrecy in the data exchanged. Critical devices that are unable to communicate over the network of encrypted channels should be connected via hardware security modules to implement secure data transfers across unsecure networks. Traffic encryption should occur at both endpoints of mainstream link from airport site and their counterpart at connectivity providers to ensure the privacy of data communications. Commercial off-the-shelf (COTS) hardware isolated execution environments should be used to do all cryptographic operations (e.g., secret key generation and encryption/decryption) to prevent sophisticated attacks (e.g., cold boot attack). Many modern PCs provide such	**Malicious actions** -Misuse of authority / authorisation -Network/interception attacks

[200] Helping Airports Understand the Payment Card Industry Data Security Standard (PCI DSS), http://onlinepubs.trb.org/onlinepubs/acrp/acrp_rrd_011.pdf.

	tamper-resistant capabilities. Encryption related to open and interoperable systems, such communication systems used by ATC, might require further developments both in technologies (e.g., non-cryptographic schemes and public key) and trust framework (see section on gaps and recommendations).	
	GP 11 – Firewalls, network segmentation, and defence in depth: The border of the airport network infrastructure should be protected by perimeter firewalls to block untrusted connections between networks, such as remote connections to airport systems. Firewalls should be configured to only allow access to required ports and services and for specific transportation protocols, like TCP or UDP. A defence in depth approach should be taken to improve network security by further restricting traffic between network segments and hosts: for example, using VLANs for traffic separation, firewalled segmentation, and end-point controls. Separation of airport functions communications should be enforced. Defence in depth is an important security concept, as it can limit the impact of a breach in a specific control: additional layers of communication security, such as authenticated secure communications (such as, HTTPS) should be employed, combined with the multitude of best practices, including least privilege.	**Malicious actions** -Denial of service attacks -Exploitation of software vulnerabilities -Social attacks
	GP 12 – Strong user authentication: IT services provided by airports should be protected by the use of authentication, such as username and password credentials. Moreover, sensitive or remote services should require access only via multifactor authentication, in which identity is verified via multiple forms of authentication, such as digital certificates, authentication tokens, One-Time Passwords (OTP), or trusted IP addresses. Biometric identifiers, such as fingerprints, facial image and iris-patterns can be introduced. Biometrics techniques are intended to be employed for traveller identification at border checks, as explored by the Smart Borders Pilot Project.[201] However, biometrics could play an increased role also as authentication support in Smart airport protection. Persistent failed authentication attempts should be blocked or rate limited. This will mitigate the risk of brute force or dictionary attacks.	**Malicious actions** -Misuse of authority / authorisation
Other	**GP13 – Integrate shutdown procedure / remote deactivation of capabilities for assets based on risk:** Compromised services or devices should be configured to foresee the presence of remote shutdown procedures that switch-off services or devices to avoid data loss. Airport operators should have the ability to remotely shut-down or deactivate certain capabilities/functionalities of these assets to minimise damage/loss and internal incident response capabilities should be established to avoid individual, panic driven, actions. However, a risk assessment should weight the advantage of enabling remote shut down (when hacked) against the disadvantage of opening up another hack-opportunity through the remote access itself.	**Malicious actions** -Denial of service attacks -Network/interception attacks -Social attacks -Tampering with airport devices
	GP 14 – Application security and secure design: All airport systems including bespoke websites and tools should be developed with security implications and best practices under consideration. Secure design should be part of System/Services/Technology Acquisition. It should be combined with airport assets under provisioning risk assessment, privacy by design principle, and security criteria requirements. Thorough testing, static code analysis and fuzzing can help to ensure security vulnerabilities are not introduced during development. A formal approach such as the Security Development Lifecycle (SDL), including threat modelling, provides rigour to development and ensure potential security issues are considered and mitigated. Websites should be	**Malicious actions** -Social attack --Exploitation of software vulnerabilities -Malicious software on airport IT assets

[201] Smart Borders, EU-LISA, http://www.eulisa.europa.eu/AboutUs/SmartBorders/Pages/FAQ.aspx.

	protected against common attacks, including reflected XSS, and clear signals to users to indicate they are interacting with the correct server (to reduce the chances of related phishing attacks).	
	GP 15 – Disaster recovery plans for IT assets: Technical procedures should be in place to restore the operation of critical IT assets in a Smart airport to an adequate level of service in case of an emergency, and therefore a disaster recovery plans must be carefully designed. Both technical and organisational aspects must be included in such a plan, and people involved in these operations must have a clear view of their roles, the sequence of actions to be performed, the actors involved and so on. The disaster recovery plan should be revised annually, or earlier, if major changes in IT infrastructure occur.	**Malicious actions** -Physical attacks on airport assets **Natural and social phenomena** -All **System failures** -All

9.5.2 Policies and Standards

CATEGORY	GOOD PRACTICE	THREAT GROUPS ADDRESSED
Information security management	**GP 16 – Set up an information security management system and implement international standards:** Airport and other organisations involved in air traffic management should implement existing international standards on information security management. Relevant standards on information security management include ISO/IEC 27001, which defines the technical specifications of an information security management system (ISMS), and ISO/IEC 27002, which provides guidelines concerning the selection, implementation and management of information security controls.	**Malicious actions** -All **Human errors** -All **System failures** -All
	GP 17 – Rely on an information security framework and external audits to assess maturity and demonstrate compliance: Organisations following international standards on information security management should rely on an information security framework (e.g. NIST Cyber Security Framework), as well as external audits, for measuring progress, identifying gaps and demonstrating compliance. To attest their contribution to supply chain security, organisations involved in air traffic management should get certified as compliant with the above-mentioned standards by a third-party institution.	**Malicious actions** -All **Human errors** -All **System failures** -All **Third party failures** -All
	GP 18 – Appoint an information security officer: A security officer should be appointed, with the mission and resources to coordinate, develop, implement and maintain an airport-wide information security program plan. The security officer should be an individual possessing the professional qualifications, including training and experience, required to administer the airport's information security program functions and should focus on security duties as his/her primary responsibility. Information security as a function should have the necessary resource to operate effectively and should be separated by IT so as to be independent. In formation security officer should report directly to C level executives or be high enough to be able to apply controls throughout the organisation.	**Malicious actions** -All **Human errors** -All **System failures** -All **Third party failures** -All
Programme management	**GP 19 – Establish an inventory of the information and information systems available:** An inventory of all the information collected and the information systems maintained across the airport should be developed. As a first step in the system security planning activity, the information and information systems collected or maintained should be categorised based on the objective of providing appropriate levels of information security according to impact.	**Malicious actions** -All **Human errors** -All **System failures** -All

CATEGORY	GOOD PRACTICE	THREAT GROUPS ADDRESSED
	GP 20 – Develop, monitor and report on the results of information security measures of performance: The performance of the airport's information security program and the security controls utilised to support the security program should be measured, monitored and reported. Measures of performance are outcome-based metrics employed for measuring the effectiveness or efficiency of the information security program and the security controls in place for supporting the program. Guidelines for the development and implementation of an information security measurement programme are provided in NIST's 'Performance Measurement Guide for Information Security'.	**Malicious actions** -All **Human errors** -All **System failures** -All
Risk assessment/ management	**GP 21 – Classify information systems according to information classification policy:** The aim of security categorisation is to describe the negative effects that may be suffered by airport operations, assets and individuals in case of damage to airport information and information systems. The results should be documented in the airport information system security plan, and be subject to review and approval by the authorising official or an authorising official's designated representative. The use of security categories should be combined with vulnerability and threat information for the purpose of assessing the risk to which the airport is exposed.	**Malicious actions** -All **Human errors** -All **System failures** -All
	GP 22 – Conduct risk assessments: Risk assessments include the determination of the likelihood and magnitude of harm resulting from the unauthorised access, use, disclosure, disruption, modification or destruction of the information system and the information being processed, stored or transmitted. Risk assessments take into account vulnerabilities, threat sources and security controls planned in order to evaluate the level of residual risk based on the operation of the information system. Formal methodologies currently in use for risk assessments related to airport information security include 'EBIOS' and 'MEHARI'. Guidance on how to carry out risk assessments may be found also in NIST's 'Guide for Conducting Risk Assessments'.	**Malicious actions** -All **Human errors** -All **System failures** -All **Natural and social phenomena** -All **Third party failures** -All
	GP 23 –Create a risk registry and monitor risks effectively: The results of the risk assessment process should be documented in the airport security risk registry/ plan and/or in a dedicated risk assessment report. The risk registry and its assessments should be subject to review and its results be updated on a pre-established frequency or when warranted by changes concerning the airport's information system, operational environment or other conditions relevant to security.	**Malicious actions** -All **Human errors** -All **System failures** -All **Natural phenomena** -All **Third party failures** -All

CATEGORY	GOOD PRACTICE	THREAT GROUPS ADDRESSED
	GP 24 – Perform continuous monitoring of information security: A 'continuous monitoring' strategy and program should be established and implemented across the airport. This should include a configuration management process for the airport's information system, a determination of the security impact of changes to the information system, a security control assessment on the monitoring strategy, a continuous reporting on the security state of the information system. Continuous and effective monitoring may be supported by the use of data gathering technologies such as: ○ Asset management tools, allowing to keep an inventory of all the hardware and software in use at the airport, track their life cycle and remotely handle single assets; ○ Network management tools, allowing to automate device configuration, ensure device compliance with pre-defined policies as well as detect unauthorised software/hardware on the network; ○ Information management tools, allowing for the monitoring of data coming from hardware and software equipment, mobile applications, stationary client devices, cloud-based data and application services as well as other relevant sources.	**Malicious actions** -All **Human errors** -All **System failures** -All **Natural and social phenomena** -All **Third party failures** -All
	GP 25 – Manage risk according to international standards and a methodological approach: Risk management should be carried out following a sound methodological approach and in line with existing international standards. Standard ISO 31000 provides a set of principles and generic guidelines for managing risk within an organisation and to incorporate risk management objectives into the organisation's strategic, management and operational tasks. 'Magerit' is a specific methodology used within the aviation sector for implementing the risk management framework defined by ISO 31000.	**Malicious actions** -All **Human errors** -All **System failures** -All
System & services acquisition	**GP 26 – Require that providers of external information system services comply with airport information security requirements and/or be certified against relevant standards:** An external information system service is a service that is used by the airport but it is not a part of the airport's information system. The responsibility for adequately mitigating risks arising from the use of external information system services rests with the authorising official, who requires that an appropriate chain of trust be established with external service providers when dealing with the many issues associated with information security. To enhance trust in the supply chain, accreditation (i.e. the process of obtaining formal approval by an authorising official) may be supported by certification against relevant standards. Standard CEN - EN16082 lays out a set of quality criteria for the delivery of civil aviation security services to public and private clients.	**Third party failures** -All
	GP 27 – Enforce explicit rules governing the installation of software: Airports should rely on software and associated documentation in accordance with contract agreements and copyright laws. They should employ tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution, and controlling and documenting the use of peer-to-peer file sharing technology to ensure that this capability is not used for unauthorised distribution. Specific rules should be established as to which types of software are permitted and which are prohibited. Such rules should be applied to users of stationary client devices (e.g. desktops, ports, workstations, etc.) but also to airport personnel using portable and mobile devices, thus improving the level of security of 'bring your own device'	**Malicious actions** -All **Human errors** -All **System failures** -All **Third party failures** -All

CATEGORY	GOOD PRACTICE	THREAT GROUPS ADDRESSED
	airport staff policies. Software policies can be enforced using trusted firmware and digital signatures.	
	GP 28 – Require developers/integrators to create and implement a security and privacy assessment and evaluation plan, combined with a verifiable flaw remediation process: Security test and evaluation process results are used whenever there have been security-relevant modifications to the information system subsequent to developer testing. A verifiable flaw remediation process should also be implemented to correct security and/or privacy-related weaknesses/deficiencies identified during the testing and evaluation process. In the evaluation phase, information security criteria must be completed by the vendors and software development should be carried out following systems development life cycle (SDLC). Airport components that may be subjected to security and privacy assessments include: hardware and software IT equipment, mobile applications, Web browsers and applications, database systems (e.g. human resources management, staff records management, etc.), authentication systems (e.g. badging systems, staff authentication systems) and intrusion detection devices (e.g. Perimeter Intrusion Detection Systems).	**Malicious actions** -All **Human errors** -All **System failures** -All **Third party failures** -All

9.5.3 Organisational, People and Processes

CATEGORY	GOOD PRACTICE	THREAT GROUPS ADDRESSED
Personnel security	**GP 29 – Screen individuals prior to authorising access to the airport's information system:** Individuals should be screened before being authorised to access the airport's information system and rescreened according to a specific list of conditions demanding rescreening, to preserve a high level of access security. Requiring airport employees to undergo biometric identification prior to being issued access credentials can be beneficial for mitigating the risk of identity fraud. Screening may be supported by enhanced CCTV surveillance and monitoring at critical areas and entry points.	**Malicious actions** -Misuse of authority/authorisation
	GP 30 – User access management: Logical and physical access authorisations to airport information systems/facilities should be reviewed for personnel. User access management and periodic review of user access rights should be established. In more mature organisations, an Identity Access Management System should be established to control effective provisioning of accesses to various systems. Additionally, Privileged Access Management can also be applied as technical control in order to monitor and protect privileged accounts. There are cases that privileged users are also Third Parties, therefore, such aforementioned controls are imperative to protect critical operations. To prevent unauthorised personnel from gaining access to restricted areas, policies and penalties may be put in place, directed at enforcing the requirement to immediately report employee separations as well as lost, stolen and unaccountable badges.	**Malicious actions** -Misuse of authority/authorisation

CATEGORY	GOOD PRACTICE	THREAT GROUPS ADDRESSED
	GP 31 – Ensure that individuals requiring access to airport information and information systems sign appropriate access agreements prior to being granted access: Prior to being given access to airport information and information systems, individuals should sign appropriate access agreements (including nondisclosure agreements, acceptable use agreements, rules of behaviour, and conflict-of-interest agreements) ensuring that they have read, understood and agreed to abide by the constraints associated with the information system to which access is authorised.	**Human errors** -Non-compliance with policies or procedures
	GP 32 – Establish personnel security requirements also for third-party providers: Personnel security requirements, including security roles and responsibilities, should be defined also for third-party providers and their compliance with such requirements should be monitored. Third-party providers may include service bureaus, contractors and other organisations providing information system development, IT services, outsourced applications and network and security management.	**Third party failures** -All
Awareness and training	**GP 33 – Provide basic security awareness training to all information system users:** The content of security awareness training and security awareness techniques should be based on the specific requirements of the airport as well as the information systems which personnel have access to. Examples of security awareness techniques include displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organisational officials, displaying logon screen messages and conducting information security awareness events. Training should include recognising social engineering attacks.	**Malicious actions** -All **Human errors** -All
	GP 34 – Provide specialised information security training: The content of specialised information security training should be determined according to assigned roles and responsibilities, as well as the requirements of the airport and the information system which personnel have access to. Personnel should be provided with role-based security-related training before being granted authorised access to the information system and/or prior to carrying out their assigned duties. Specialised information security training should be provided also if significant changes to the system occur.	**Malicious actions** -All **Human errors** -All **System failures** -All
	GP 35 – Document and monitor security training activities: Individual security training activities, including basic security awareness training and information system specific training, should be documented and monitored. Individual training records of all personnel undergoing training should be retained depending on organisational needs.	**Malicious actions** -All **Human errors** -All **System failures** -All
	GP 36 – Maintain on-going contacts with security groups and associations: Ongoing contact with security groups and associations is of paramount importance in an environment of rapidly changing technologies and threats. Security groups and associations include, for example, special interest groups, forums, professional associations, news groups, and/or peer groups of security professionals in similar organisations. Organisations select groups and associations based on organisational missions/business functions. Organisations share threat, vulnerability, and incident information consistent with applicable laws, directives, policies, regulations, standards, and guidance.	**Malicious actions** -All **Human errors** -All **System failures** -All **Natural and social phenomena** -All

CATEGORY	GOOD PRACTICE	THREAT GROUPS ADDRESSED
		Third party failures -All
Contingency/ disaster recovery planning	**GP 37 – Develop a contingency plan:** The contingency plan should identify essential airport missions and functions and associated contingency requirements. It should also address contingency roles, responsibilities, assigned individuals with contact information as well as both information system restoration and implementation of alternative processes when systems are compromised. Copies of the contingency plan should be distributed and changes of the same be communicated to a list of key contingency personnel. Examples of actions to be addressed in contingency plans include: information system shutdown, fall back to a manual mode, alternate information flows or operating in a mode that is reserved solely for when the system is under attack.	**Malicious actions** -All **Human errors** -All **System failures** -All **Natural and social phenomena** -All **Third party failures** -All
	GP 38 – Develop a disaster recovery plan: The operation of critical IT assets is a crucial element in a Smart airport and the disaster recovery plan, aimed to establish an adequate level of service in case of an emergency, must be carefully designed. Both technical and organisational aspects must be included in such a plan, and people involved in these operations must have a clear view of their roles, the sequence of actions to be performed, the actors involved and so on. The disaster recovery plan should be revised annually or earlier if major changes in IT infrastructure occur.	**Malicious actions** -All **Human errors** -All **System failures** -All **Natural and social phenomena** -All **Third party failures** -All
	GP 39 – Train airport personnel in their contingency and disaster recovery roles: Airport personnel should be trained in their contingency and disaster recovery roles and responsibilities and be provided refresher training in order to ensure continuity of operations and address other security-related events resulting in a reduction in effectiveness, such as malicious attacks compromising the confidentiality or integrity of the information system.	**Malicious actions** -All **Human errors** -All **System failures** -All **Natural and social phenomena** -All **Third party failures** -All
	GP 40 – Test and assess the contingency and disaster recovery plans: The airport's contingency and disaster recovery plans should be tested and subject to continuous assessment according to ISO 22301 standards. Tests and assessments should determine the impact of contingency and disaster recovery operations carried out in accordance with the respective plans on airport operations, assets and individuals. Results should be used to evaluate the plans' effectiveness and the airport's readiness to implement them.	**Malicious actions** -All **Human errors** -All **System failures** -All **Natural and social phenomena**

CATEGORY	GOOD PRACTICE	THREAT GROUPS ADDRESSED
		-All **Third party failures** -All
Incident response/ reporting	**GP 41 – Provide incident response capabilities for airports:** The aviation community should establish rapid incident response capabilities with the specific task to enable airports to mitigate, respond and recover from cyber-attacks. Relevant examples and experience on successful implementation of such capabilities in other domains may be drawn from as a source of lessons learned. Cooperation between the public and private sector would be desirable towards the creation of effective incident response capabilities.	**Malicious actions** -All **Human errors** -All **System failures** -All **Natural and social phenomena** -All **Third party failures** -All
	GP 42 – Train airport personnel in their incident response roles with respect to the information system: Airport personnel should be trained in their incident response roles and responsibilities with respect to the information system and should be provided refresher training to handle the situation in a way that limits damage and reduces recovery time and costs when an incident occurs. Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources.	**Malicious actions** -All **Human errors** -All **System failures** -All **Natural and social phenomena** -All **Third party failures** -All
	GP 43 – Test and/or exercise the airport's incident response capability for the information system: The airport's incident response capability for the information system should be tested and/or exercised to determine incident response effectiveness and avoid a low level of incident response capability. The results obtained should be documented so as to ensure improvements in personnel training.	**Malicious actions** -All **Human errors** -All **System failures** -All **Natural and social phenomena** -All **Third party failures** -All
	GP 44 – Track and document information system security incidents: Security incidents affecting the airport's information system should be documented by maintaining records about each incident, the status of the incident and other pertinent information necessary for forensics, evaluating incident details, trends, handling and lessons learned. Incidents information can be obtained from a variety of sources including incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring and user/administrator reports.	**Malicious actions** -All **Human errors** -All **System failures** -All **Natural and social phenomena**

CATEGORY	GOOD PRACTICE	THREAT GROUPS ADDRESSED
		-All **Third party failures** -All

9.6 Glossary

ACARS	Aircraft Communications Addressing and Reporting System
ACRP	Airport Cooperative Research Program
ADS-B	Automated Dependent Surveillance-Broadcast
ANSPs	Air Navigation Service Providers
AODB	Airport Operational Data Base
AOP	Airport Operations Plan
ARINC	Aeronautical Radio, Incorporated
ATFCM	Air Traffic Flow and Capacity Management
ATM	Air Traffic Management
AVI	Automated Vehicle Identification
CAAs	Civil Aviation Authorities
CDM	Collaborative Decision Making
CERT	Computer Emergency Response Team
CISOs	Chief Information Security Officers
COTS	Commercial Off-the-Shelf
CPNI	Centre for the Protection of National Infrastructure
CRS	Central Reservation System
CSIRTs	Computer Security Incident Response Teams
CUPPS	Common-use passenger processing systems
DCS	Departure control systems
DDoS	Distributed denial of service
DoS	Denial of service
EC	European Commission
ECAC	European Civil Aviation Conference
EASA	European Aviation Safety Agency
FIDS	Flight Information Display System
GANP	Global Air Navigation Plan
GIS	Geographic Information Systems
GPS	Global Positioning System
IATA	International Air Transport Association
ICAO	International Civil Aviation Organisations
ICANN	Internet Corporation for Assigned Names and Numbers
ICS	Industrial Control Systems
IEDS	In-Line Explosive Devices Systems
IETF	Internet Engineering Task Force
ISMS	Information Security Management System
LAN	Local Area Network
NFC	Near Field Communication
NISD	Network and Information Security Directive
OTP	One-Time Password
PIDS	Perimeter Intrusion Detection Systems
POS	Point-of-Sales
PNR	Passenger Name Records
RBAC	Role-based-access-control
RFID	Radio-Frequency Identification
SCADA	Supervisory Control and Data Acquisition
SES	Single European Sky
SESAR	Single European Sky ATM Research

SITA	Société Internationale de Télécommunications Aéronautiques
SMC	System Monitoring and Control
SWIM	System-Wide Information Management
TAM	Total Airport Management
VLAN	Virtual LAN
VPN	Virtual Private Network
WAN	Wide Area Network

ENISA
European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vasislissis Sofias
Marousi 151 24, Athens, Greec

TP-07-16-070-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-185-4
DOI: 10.2824/865081