SATIE

Security of Air Transport Infrastructures of Europe

D7.6 - SoA about airports security and expected improvements

Deliverable Number	D7.6
Author(s)	NIS, AIA, KEMEA, SEA, ZAG, DLR, TLB, FQS, ISEP, ALS, INOV, SAV
Due/delivered Date	M24/2021-04-30
Reviewed by	ACS, KEMEA, DLR
Dissemination Level	PU
Version of template	1.7

Start Date of Project: 2019-05-01

Duration: 30 months

Grant agreement: 832969

This project has received funding from the European Union's 7th Framework Programme for Research, Technological Development and Demonstration under Grant Agreement (GA) N° # 832969

DISCLAIMER
The opinion stated in this report reflects the opinion of the authors and not the opinion of the European Commission.
All intellectual property rights are owned by the SATIE consortium members and are protected by the applicable laws. Reproduction is not authorised without prior written agreement. The commercial use of any information contained in this document may require a license from the owner of that information.
All SATIE consortium members are also committed to publish accurate and up to date information and take the greatest care to do so. However, the SATIE consortium members cannot accept liability for any inaccuracies or omissions nor do they accept liability for any direct, indirect, special, consequential or other losses or damages of any kind arising out of the use of this information.

Document contributors

No.	Name	Role (content contributor/reviewer/other)
1	Nikolaos Papagiannopoulos (AIA)	Content Contributor
2.	Matteo Mangini (NIS)	Content Contributor
3.	Kelly Burke (NIS)	Content Contributor
4.	Filipe Apolinario (INOV)	Content Contributor
5	Eva Maia (ISEP)	Content Contributor
6	Eftichia Georgiou (KEM)	Content Contributor
7	Eleni - Maria Kalogeraki (AIA)	Content Contributor
8	Filippos Komninos (AIA)	Content Contributor
9	Vasilis Kontothanasis (AIA)	Content Contributor
10	Anastasios Nikas (AIA)	Content Contributor
11	Ioanna Varvitsioti (AIA)	Content Contributor
12	Spyridon Papastergiou (AIA)	Content Contributor
13	Elena Branchini (SEA)	Content Contributor
14	Paolo Previtali (SEA)	Content Contributor
15	Marcella Scuccimarra (SEA)	Content Contributor
16	Italo D'Ascoli (SEA)	Content Contributor
17	Angelo D'Andrea (SEA)	Content Contributor
18	Biagio Tarantino (SEA)	Content Contributor
19	Sven Hrastnik (ZAG)	Content Contributor
20	David Lancelin (ACS)	Reviewer
21	Vasileios Kazoukas (KEMEA)	Reviewer
22	Meilin Schaper (DLR)	Reviewer

Document revisions

Revision	Date	Comment	Author
V0.1	2021-03-29	Initial draft – updating D2.2	Nikolaos Papagiannopoulos
V0.1	2021-04-13	Initial security check and change requests	Vasileios Kazoukas, Project Security Officer
V0.2	2021-04-29	Adressing review comments	Nikolaos Papagiannopoulos Filipe Apolinario
V0.2	2021-04-30	Final security check and approval for submission	Vasileios Kazoukas, Project Security Officer
V1.0	2021-04-30	Final quality check and approval for submission	Meilin Schaper, Quality Manager

Executive summary

The main goal of the SATIE project is to protect critical air transport infrastructures against combined cyber and physical threats in terms of improving the interoperability between existing systems and enhanced security solutions to ensure resilience and sustainability across airport infrastructures and provide safety to the populations within the airport and in the adjacent environment. A stepping stone to find ways to encounter or mitigate the cascading effects of a sophisticated attack on airports' infrastructures is to have a complete understanding of the existing cyber and physical airports' security environment.

Deliverable 7.6 provides a state-of-the-art analysis about airport security and expected improvements. In this regard, current standards, guidelines, crisis management aspects together with their societal impact and security solutions applied on air transport infrastructures are presented in the context of SATIE and critical ICS/SCADA airport systems, such as the Baggage Handling System are described reflecting security concerns.

During this task, the consortium in collaboration with the end users has managed to analyse the current security measures and controls, the legal background and the crisis and disaster management practices applied in the three SATIE demonstration airports following a specific systematic approach that addresses the SATIE attack scenarios requirements and the assets/operations involved.

The deliverable's purpose is to build a reliable state-of-the-art and gap analysis about physical and cybersecurity in airports and analyse the requirements, in order to identify the main areas of security improvements. To this aim, an extensive gap analysis is presented upon which the expected improvements from SATIE are defined.

Table of Content

List of Figures

List of Tables

List of Acronyms

Acronym	Definition
AA	Airport Authority
ACC	Area Control Centre
AI	Artificial Intelligence
AIRAC	Aeronautical Information Regulation And Control
AIA	Athens International Airport
AIP	Aeronautical Information Publications
AISS	Aeronautical Information Security System
AMS	Apron Management Service
ANSSI	National Cybersecurity Agency of France
ANSV	Agenzia Nazionale per la Sicurezza del Volo (National Agency for Air Safety)
AOC	Airport operations control
API	Advanced Passenger Information
APOC	Airport Operations Centers
APP	Approach Control
ARINC	Aeronautical Radio, Incorporated
ARP	Airport (or Aerodrome) Reference Point
ATC	Air Traffic Control
ATM	Air Traffic Management
ATR	Automated Tag Reader
BHS	Baggage Handling System
BP-IDS	Business Process based Intrusion Detection System
BYOD	Bring Your Own Device
CBRN	Chemical, biological, radiological, and nuclear
CANSO	Civil Air Navigation Services Organisation
CARATS	Collaborative Actions for Renovation of Air Traffic Systems
CCS	Centralized control system
CCS	Cassidian Cybersecurity SAS
CCTV	Closed-Circuit Television

CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CIS	Common Information Space
CMC	Crisis Management Center
COE	Centro Operativo per l'Emergenza (Emergency Operations Centre)
COEU 118	Emergency Operations Centre 118
CPA	Cybersecurity Program Assessment
CPSRA	Critical Part of Security Restricted Areas
CSIRT	Computer Security Incident Response Team
CU	User Committee (Association Of Airline Companies and airport operators)
DCS	Distributed control system
DCS	Departure Control Systems
EBIOS	Expression of Needs and Identification of Security Objectives
ED	EUROCAE Documents
EDS	Explosive Detection System
EMCR	Emergency Message Content Router
ENAC	Ente Nazionale Aviazione Civile (the Italian Civil Aviation Authority)
ENAV	Ente Nazionale Assistenza al Volo (the Italian Air Navigation Services
ENISA	European Network and Information Security Agency
EOC	Emergency Operations Centre
EPIC	Emergency Procedures Information Center
ETD	Explosive and chemical trace detection systems
ETD	Explosive trace detection equipment
EU	European Union
EUROCAE	European Organisation for Civil Aviation Equipment
FIC	Flight Information Center
FIDS	Flight Information Display System
FTP	File Transfer Protocol
GLPI	Gestionnaire Libre de Parc Informatique
GUI	Graphical User Interface
HBS	Hold Baggage Screening

HF	High Frequency
HHMD	Hand-Held Metal Detection
HMI	Human-machine interface
ICAO	International Civil Aviation Organization
ICS	Industrial Control System
ICT	Information Communication Technology
ID	Identity
IDS	Intrusion Detection Systems
IEC	International Electrotechnical Commission
IED	Intelligent embedded devices
IoT	Internet of Things
IPS	Intrusion Prevention Systems
IPS/IDS	Intrusion Prevention Systems / Intrusion Detection Systems
ISG	Information Security Governance
ISMS	Information Security Management System
ISO/ IEC	International Organization for Standardization / International Electrotechnical Commission
IT	Information Technology
ITMS	Intelligent Traffic Management System
KGFC	Know, Get in, Find, and Control
LEDS	Liquid Explosive Detection System
MRZ	Machine Readable Zone
MSS	Managed Security Service
MVC	Model-vie-controller
NIS	Network and Information Security
NIS	Network Integration & Solutions
NIST	National Institute of Standards and Technology
NOTAM	Notice to Airmen
OT	Operational Technology
PAC	Programmable Automation Controller
PAS	Public Address System
PLC	Programmable Logic Controller

PNR	Passenger Name Record
PNS	National Security Program
RFID	Radio-frequency identification
RIS	Risk assessment platform
ROS	Rescue Operations Supervisor
RTCA DO	RTCA Document
RTCA	Radio Technical Commission for Aeronautics
RTU	Remote Terminal Unit
SAMD	Shoe Analyzer Metal Detectors
SCADA	Supervisory Control and Data Acquisition
SEA	SEA Società per Azioni Esercizi Aeroportuali
SESAR	Single European Sky ATM Research
SGSI	Sistema di Gestione della Sicurezza delle Informazioni (an Information Security Management System)
SOC	Security Operations Centre
SSUEM	Servizio Sanitario di Urgenza ed Emergenza Medica
SWIM	System Wide Information Management
TraMICS	Traffic Management Intrusion and Compliance System
TWR	Control Tower (Torre di Controllo)
UFIDS	Unique Across All Possible Distributed File Systems
UPS	Uninterrupted power supply
VHF	Very High Frequency
VPN/SSH	Virtual Private Network / Secure Shell
Wi-Fi	Wireless Fidelity
WTMD	Walk-Through Metal Detection
ZAG	Franjo Tuđman Airport of Zagreb (ZAG)

1 Introduction

SATIE project aims to provide a security solution to protect critical air transport infrastructures in terms of combined cyber and physical threats. A stepping stone on this way is to concentrate on the identification and mitigation of cyber-physical attacks on airports. To determine how to abate any cascading effects of an attack within the airport environment, the first task is to identify all current and expected physical- and cyber-security measures.

In this deliverable the results of the Task 2.1 “State-of-the-art about airport security and expected improvements” relevant to a thorough state-of-the-art analysis about security controls in airport infrastructures and to a comprehensive report on how SATIE is expected to provide improvements are documented in detail. It should be noted that this deliverable is the public version of document D2.2.

This deliverable aims to offer a clear and accurate understanding of the current measures in place so that future, well-defined strategies can be developed. To this intent, an analysis on the relationships between security solutions and the assets and airport operations involved in the context of SATIE is carried out. The results outlined here were used to harmonize the security and management strategies across the three airports in deliverable D7.7.

Moreover, chapter 2 presents the background information on the current security measures regarding the air transport infrastructures. In particular, the chapter i) describes indicative current Standards and Guidelines about Security techniques, risk management, information security controls, considered most relevant in the context of SATIE project requirements, activities and areas of interest, ii) presents a state-of-the-art analysis about relevant crisis management aspects along with their societal impacts, iii) refers to security solutions deployed in Airport infrastructures, such as the detection and screening of passengers and their baggage bringing up information sharing and Air Traffic Management (ATM) security concerns and iv) reports on the existing ICS/SCADA systems in the airports and provides a description of the Baggage Handling System (BHS) commonly used in airports.

Chapter 3 provides a brief overview of the existing security solutions that are extant and relevant for the hypothetical attacks outlined in the context of SATIE. To this extent, the current document reflects the SATIE project partners’ collaborative work to collect the security solutions data regarding the cyber and physical security controls that are undertaken by the three SATIE demonstration airports, tailored by the abovementioned systematic approach. The international standards followed by the end-users, which are relevant to this project, along with nation-specific and airport-specific measures in use are presented in the current report as well. Additionally, the crisis management approaches of the three demonstration airports and their societal impact are extensively described.

Finally, chapter 4 illustrates the study about the expected improvements from SATIE containing an in-depth gap analysis that takes into account the security gaps that have been identified by ENISA (1) and CONCEPTIVITY (2). The described gap analysis will allow the identification of the expected improvements from SATIE, which is furthermore documented.

2 Background information

2.1 Current standards and guidelines to be considered in the context of SATIE

This section aims in providing a comprehensive outline of existing standards/guidelines that are in effect in the field under study. In this regard, Table 2.1 indicatives Standards and Guidelines are considered to be relevant to the security techniques, requirements, risk management, information security controls in the context of SATIE and will be further studied. This is not an exhaustive list of all available standards but a refined selection of those considered to best suit the needs of the projects' activities and areas of interest.

Table 2.1: Current cyber standards and guidelines to be considered in the context of SATIE

Title	Description
ISO/IEC 27001:2013 (3) Information technology	This International Standard has been prepared to provide **requirements** for establishing, implementing, maintaining and continually improving an information security management system
ISO 31000:2018 (4) Risk management - Guidelines	The specific Standard can be used by any public, private or community enterprise, association, group or individual. Therefore, it is not specific to any industry or sector. ISO 31000:2018 **provides guidelines on managing risk faced by organizations.** The application of these guidelines can be customized to any organization and its context. ISO 31000:2018 can be used throughout the life of the organization and can be applied to a wide range of activities, including strategies and decision making, operations, processes, functions, services and assets. This International Standard provides principles and generic guidelines on risk management. It can be applied to any type of risk, whatever its nature, whether having positive or negative consequences.
ISO 27005:2018 (5) Information technology -- Security techniques -- Information security risk management	This document provides guidelines for **information security risk management**. This document supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach. Knowledge of the concepts, models, processes and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is important for a complete understanding of this document. This document is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) which intend to manage risks that can compromise the organization's information security.

Title	Description
ISO/IEC 27002:2013 (6) Information technology — Security techniques — Code of practice for information security controls	This International Standard is designed for organizations to use as a reference for selecting controls within the process of implementing an Information Security Management System (ISMS) based on ISO/IEC 27001 or as a guidance document for organizations implementing commonly accepted information security controls. This standard is also intended for use in developing industry- and organization-specific information security management guidelines, taking into consideration their specific information security risk environment(s).
ISO/IEC 27033:2015 (7)- IT network security standard.	The purpose of ISO/IEC 27033 is to provide detailed guidance on the security aspects of the management, operation and use of information system networks, and their inter-connections.
ISO 22301:2012 (8)- Societal security	It specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise.
CANSO (2014) (9) CANSO Position Paper on Cyber security	The CANSO Cyber Security and Risk Assessment Guide provides Members with an introduction to cybersecurity in ATM
ARINC 811 Commercial aircraft information security concepts of operations and process framework	This document describes a security process framework involving a three-step risk-based approach, which considers existing airline operations and impacts of new information security measures, especially regarding asset management.
EUROCAE ED-201 – 204 Aeronautical Information Security System (AISS) Framework	These documents describe the overall context of the AISS, covering all aspects of civil aviation, including airworthiness security process specification, airworthiness security methods and considerations, and information security guidance for continuing airworthiness.
RTCA DO-326 Airworthiness security process specifications	This guideline is intended to augment current guidance in how to handle cybersecurity threat to aircraft safety, adding data requirements and compliance objectives.
EU NIS Directive (10)	This EU-wide cybersecurity directive applies to all EU member states and specifies certain national cybersecurity improvements, that they must collaborate cross-borders, and that they must supervise the cybersecurity within their country including ex-ante and ex-post supervision.
NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (2018)	This document suggested a risk management framework with standards, guidelines, and best practices to mitigate cybersecurity risks.

Title	Description
NIST SP 800-30 Rev.1 (2012) Guide for Conducting Risk Assessments	This Special Publication aims to provide guidance for conducting risk assessments of federal information systems and organizations, amplifying the guidance in Special Publication 800-39. Risk assessments, carried out at all three tiers in the risk management hierarchy, are part of an overall risk management process, providing senior leaders/executives with the required information to determine appropriate courses of action in response to identified risks.
NIST SP 800-37 Rev. 2 (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy	This publication describes the Risk Management Framework (RMF) and provides guidelines for applying the RMF to information systems and organizations. The RMF provides a disciplined, structured, and flexible process for managing security and privacy risk that includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring.
NIST SP 800-53 Rev.5 Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans.	This document provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks.

Table 2.2: Current physical standards and guidelines to be considered in the context of SATIE

Title	Description
ICAO Aviation Security Manual – Document 8973 (Restricted Access)	This manual assists member states on implementing Annex 17 of the Chicago Convention. It is regularly reviewed and amended as new threats and technological developments are identified and it provides guidance on how to apply its Standards and Recommended Practices.
ICAO's Annex 17 Security - Safeguarding International Civil Aviation Against Acts of Unlawful Interference	The specific annex contains recommendations, guidelines including the response to an act of unlawful interference, the International Cooperation, the national Organization and Training, the contingency Planning and Exercises, the architectural and infrastructure requirements, the implementation of aviation security measures and the exchange of information and reporting, etc.
Attachment to Annex 17 from ICAO's Annex 2 "Rules of the Air"	It refers to aspects of notification to Air Traffic System (ATS) and broadcast warnings on the VHF emergency frequency.
ECAC (European Civil Aviation Conference) Document 30	Provides recommendations aimed at ensuring: - the correct application of Annex 17 within the EU, - a higher level of Security in air transport.
Attachment from ICAO's Annex 9 "Facilitation"	It refers to aspects of valid passports or other acceptable from of identify; approved custom offices, imported

Title	Description
	security equipment - ground equipment; satisfactory facilities and services; specialized communication equipment, etc.
Attachment from ICAO's Annex 10 "Aeronautical Telecommunications"	It refers to aspects of reply codes (aircrafts), etc.
Attachment from ICAO's Annex 11 "Air Traffic Services	It refers to aspects of service to aircraft in the event of an emergency, alerting service, notification of rescue coordination centres, information to the operator, information to aircraft operating in the vicinity of an aircraft in a state of emergency, etc.
Attachment from ICAO's Annex 14 "AERODROMES"	It refers to aspects of isolate aircraft parking position, lights/security lighting, secondary power supply, fencing/patrolling, aerodrome emergency planning, aerodrome emergency exercise, etc.
Attachment from ICAO's Annex 18 "The Safe Transport of Dangerous goods by Air"	It refers to aspects of dangerous goods technical instructions, establishment of training programs, etc.
EU Regulation 300/2008	Common rules and basic standards on aviation security and procedures to monitor the implementation of the common rules and standards.
Eu Regulation Commission implementing Regulation 1998/2015	Sets detailed procedures concerning Civil Aviation safety fundamental rules. It refers to aspects of airport planning requirements, access control, screening of persons other than passengers, examination of vehicles, surveillance, patrols and other physical controls, aircraft security, passenger and cabin baggage screening, screening of hold baggage, cargo security, air-mail security, in-flight supplies, airport supplies, security during flight, staff recruitment and training, security equipment, etc.
Eu Regulation Commission Decision 8005/2015	Sets detailed provisions for the implementation of the common basic standards on Aviation Security containing the information referred to in Article 18, letter a) of Regulation (EC) no. 300/2008 ("EU classified information").
National Civil Aviation Security Regulation AND Security Technical Directives (Technical Directive No. 1, Technical Directive No. 2)	It refers to aspects of airport security measures, demarcated airport areas, aircraft security, passenger and cabin baggage screening, screening of hold baggage, cargo security - air-mail security, flight supplies, airport supplies, security during flight staff recruitment and training, security equipment, general aviation, etc.
National Civil Aviation Training Program	Describes the National Policy on the Basic, Advanced and Aviation Security Training Courses Implemented by the Hellenic Civil Aviation Authority.
National Civil Aviation Security Audits and Inspections	Describes the methodology and the protocols for auditing / inspecting / testing the Airport Security System.

Title	Description
Airport Security Program	It refers to aspects of airport security measures, demarcated airport areas, aircraft security, passenger and cabin baggage screening, screening of hold baggage, cargo security - air-mail security, flight supplies, airport supplies, security during flight staff recruitment and training, security equipment, general aviation, special categories of passengers, weapons and ammunitions, handling of security threats and incidents, etc.
Hellenic National Level National Aviation Security Programme containing the following documents: 1. National Aviation Security Regulations, 2. Technical Aviation Security Directive No1, 3. Technical Aviation Security Directive No2, 4. National Programme for Aviation Security Surveys and Inspections, 5. National Aviation Security Training Programme	Each country has to implement the international standards, taking into account national laws introducing another level of refinement, which makes the rules more precise and more constrained, and guides the design and processes of the airports.
Airport Level ATHENS Airport Security Programme	Document harmonised with the National Aviation Security Programme.
Italian National Level Ministerial Decree 29 January 1999, N°85	Entrustment under concession to the Airport Operator of: a) control of departing and transit passengers; b) X-ray inspection, or with other types of equipment, of passengers' baggage; X-ray inspection, or with other types of equipment, of hold baggage, cargo and express couriers' parcels.
Italian National Level Law-Decree 31 August 2013, N°101, Coordinated with the Conversion Law 30 October 2013, N°125	In compliance with EU Regulations, the following services are entrusted in concession to the Airport Operator by ENAC (national Civil Aviation Authority): a) control of airport staff and airline crews accessing security restricted areas through the checkpoints inside passenger terminals. The control is extended to the objects transported and to the verification of the possession of the necessary authorizations; b) control of airport staff and any other person who, through the checkpoints other than those inside the passenger terminals, access the security restricted areas. The control is extended to the objects transported and to the verification of possession of the

Title	Description
	necessary authorizations. Control of vehicles entering the sterile restricted area of the Airport which can be accessed exclusively with the necessary authorizations and only after carrying out specific checks.
Italian National Level ENAC – National Civil Aviation Authority National Aviation Security Programme	Sets the standard security measures concerning the controls, the procedures, the resources of airports and their operators. It has two objectives: the definition of responsibilities for the implementation of the common basic standard rules and the specification of the obligations required for this purpose to operators and other subjects to which it applies. Given the primary rules (i.e.: Regulation 1998/2015 and Decision 8005/2015), ENAC integrates them in the National Aviation Security Programme with specific methodological and procedural, supplementary or specific provisions.
Italian National Level ENAC – National Civil Aviation Authority NQCP - National Civil Aviation Security Quality Control Programme	The Program aims at establishing the organizational structure, skills, resources, procedures and methodologies that must be applied to obtain an effective monitoring which aim is twofold: on the one hand, the verification of the effective and correct application of the measures of civil aviation security, on the other hand it aims to control, through compliance control activities, their level of conformity with the provisions of EU Regulation n.1998 / 2015 and subsequent amendments. and of the National Civil Aviation Security Programme.
Italian National Level ENAC – National Civil Aviation Authority Security Training Manual	It sets guidelines for: a) the development of initial and periodic training programs for 16 professional categories, b) minimum duration of courses, c) methods of provision and use of technical support (Computer Based Training).
Airport Level Airport Operator Airport Security Program	The Program, besides including the Security Procedures applied in a specific Airport, also includes provisions related to internal quality control describing how the Airport Operator must monitor the compliance with these methods and procedures. The Airport Security Program is submitted to the competent authority (ENAC – National Civil Aviation Authority) for the final approval.
ISO 55001:2014 (11) Asset Management System Requirements	This standard indicates the framework and best practices for asset management, including how to optimize value while ensuring that assets meet necessary safety and performance requirements. This framework is for the whole lifecycle of assets, from acquisition to decommission.

Title	Description
International Civil Aviation Organization (ICAO) DOC. 8973 Security Manual for Safeguarding Against Acts of Unlawful Interference	This manual assists member states on implementing Annex 17 of the Chicago Convention. It is regularly reviewed and amended as new threats and technological developments are identified and it provides guidance on how to apply its Standards and Recommended Practices. It provides States and Air Carriers with details and information to guide them in creating / implementing their security programs
National Level CROATIA	National Civil Aviation Security Programme
Airport Level ZAGREB	Airport Security Programme
Airport emergency plan	Main goal of emergency plan is to save lives and eliminate dangers and threats to people, property and environment. Airport adopts this plan in order to define an organized and coordinated transition from normal activities to functioning during an extraordinary event.
Evacuation and rescue plan for the passenger terminal	With this plan, airport determines the organization, procedures and security measures to ensure quick and efficient evacuation and rescue activities. It refers to events that may endanger the safety and health of workers, passengers and other persons present in the premises of the new passenger terminal .
Safety policy	As airport's first priority, safety is a key pillar of the efficiency of the operations for all employees from all companies and stakeholders working at the airport. Goal is to be a safe, smoothly-functioning airport which is compliant with the international standards, national and EU legislation.
Book of measures against Covid-19	Airport prepared this book with a description of the measures in order to provide adequate health and safety instructions. This document is a summary of National public health institute (HZJZ), European Union Aviation Safety Agency (EASA), Airport Council International (ACI) and World health organization (WHO) based on available information about Covid-19 disease.

2.2 Crisis Management and Societal Impacts

Crisis Management is "the process by which an organization deals with a major event that threatens to harm the organization, its stakeholders, or the general public (12). In contrast to risk management, which involves assessing potential threats and finding the best ways to avoid those threats, Crisis Management involves dealing with threats **before, during, and after** they have occurred.

The process of Crisis and Disaster Management is often visualized in form of a life-cycle, as depicted in Figure 2.1.

Figure 2.1: Crisis Management life-cycle

The process comprises four phases with the following main goals:

- Prevention phase:
  - Building knowledge about potential risks
  - Risk mitigation
- Preparation phase:
  - Being prepared to react
- Reaction phase:
  - Minimizing the impact
- Recovery phase:
  - Working on getting back to normality

A more detailed picture, showing working methods and related information per phase is provided in Figure 2.2.

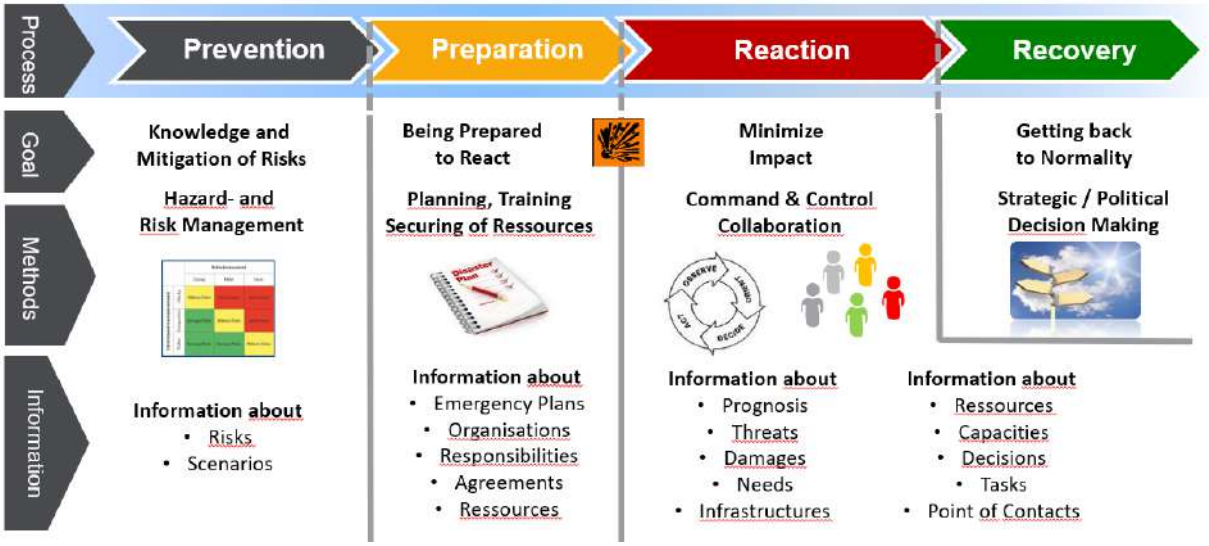

Figure 2.2: Linear presentation of the Crisis Management life-cycle, showing Goal, Processes and involved Information for each Phase

During the time-critical Reaction phase within a crisis or disaster management action, cross-organizational collaboration and the related information management today is still mostly based on face-to-face meetings, telephone calls, fax transmissions, email messages, paper charts, whiteboards, and proprietary electronic systems. As a consequence, situation awareness is hampered by a

fragmentation of relevant information into pieces held by different stakeholders. Within the highly collaborative scenarios of the civil crisis management operations such as for example in case of a flood, a forest fire, or an earthquake this fragmentation causes uncertainty whether the information base for critical decisions is up-to-date, comprehensive and valid. Figure 2.3. shows an example for fragmentation in the context of typical stakeholders.

Figure 2.3: Fragmentation of Information between Stakeholders

Although the nature of crises mentioned as examples above may be different from crises envisioned in the airport context in the scope of the SATIE project, the principles and the challenges of crisis management remain the same. Decision making based on a comprehensive picture of the situation requires exchange, verification and integration of all the different pieces of information provided by the stakeholders with their organizational and cultural background (13). At the same time a common understanding of the situation is also a basic prerequisite for successful collaboration (14).

A number of projects within the public safety domain focus on solutions for a Common Information Space (CIS). The U.S. XChangeCore programme and the European Research projects EPISECC (15), SecInCoRe, REDIRNET, SECTOR, IDIRA (16) and DRIVER have been identified as relevant projects or initiatives, respectively. All these projects implement a CIS (17). The CIS interconnects technical systems and applications of different organisations in order to support information sharing (see Figure 2.4). The Common Information Space is a data sharing platform, but not a data repository. The ownership of the data stays with the applications. The validation, interpretation and processing of the transported data is part of the applications.

The exchanged data need to be converted since the different applications usually use owner-specific taxonomies, data formats, and protocols. In order to avoid the necessity of N-to-N conversions the concepts are based on standard protocols, data formats and reference taxonomies. This allows implementing N-to-1-to-N conversion models based on application specific adaptors which depend on the individual external application itself.

Figure 2.4: Common Information Space (CIS)

In the aviation area, the European Aviation Crisis Coordination Cell (EACCC) has been established. It is actively engaged in an improved level of preparedness in Europe for any kind of crisis, including security breaches (18) .

Next to the direct consequences for the air transport system related to the crisis management, also the societal impacts are an issue which has to be considered (see Figure 2.5). The most obvious societal impacts result from the disruptions which are result of the attack:

1. Delays
   affect the whole air transport system, i.e. the stakeholders like airlines, airport authorities, ground handlers or air navigation service providers but also the passengers. Delay can still be seen as daily business due to several reasons like weather or technical issues. But each additional delay factor increases the negative impacts of delay. Especially high delay causes high cost for passenger (19). This cost is lost for the economy.
2. Cancellations
   have two main aggrieved parties, the airlines and the passengers. While the airlines may have high cost due to passenger compensations (depending on the applicable law) and adaption of operation scheduling. Associated services like ground handlers or fuel service have to reschedule their processes. Passengers themselves have cost due to missed meetings or bookings. In addition the above described delay cost occurs due to change of flight or transportation mean.
3. Rerouting
   has attributes from both of the above mentioned impacts. All affected stakeholders have to reschedule their processes. The airline has additional cost of transferring the passengers to their desired destination. The passengers lose a lot of time with the aforementioned cost. In addition, this can also lead to delays and even cancellations in case other airports' capabilities are exhausted.
4. Accidents
   are the most feared consequences of security breaches, as they have a high risk for fatalities. In a second stage they have a high impact on the trust in the air transportation system. Also air transportation is the safest traffic mean, one accident can significantly impact the travel behaviour.

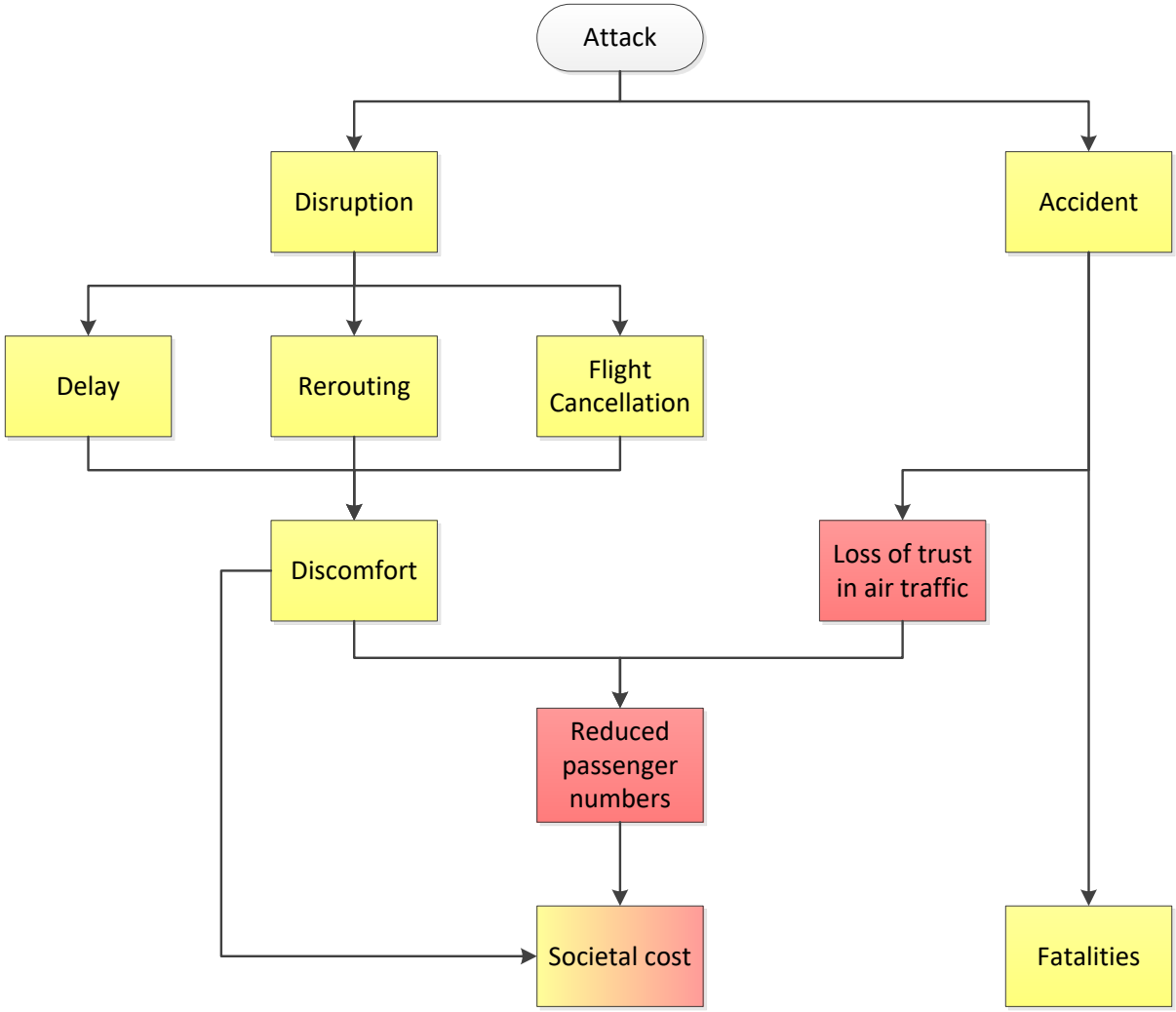

Figure 2.5: Societal impacts of security breaches (yellow: short term; red: long term)

To avoid the above mentioned consequences, high effort is put on the security of the air transportation system and especially in the prevention. Reaction and recovery are extremely challenging in this very complex environment and in case of an accident impossible. However, all these crises management measures impose additional costs, either directly by e.g. in installing new facilities or indirectly by e.g. increased process times. These costs contribute to the ticket price and so to the competitive ability of the air transport system.

The most prominent and dreadful event is the September 11 attacks in the year 2001. In the aftermath of this attack a significant drop in worldwide air travel was observed (20). Such a reduction occurred only twice so far with the financial crisis 2009 being the other event (see Figure 2.6). This example shows the sensitivity of air traffic to a security breach.

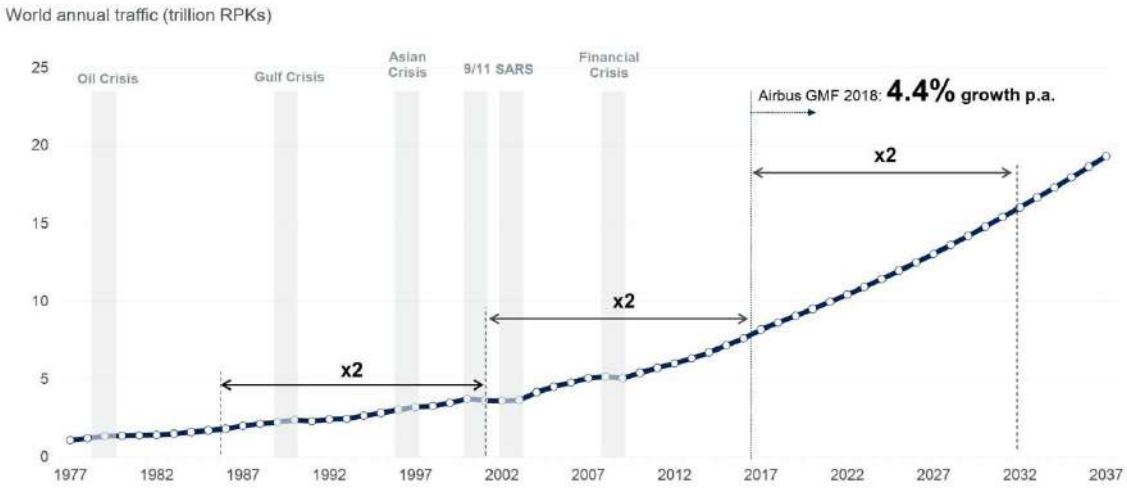

Figure 2.6: Air Traffic Demand (Source: Airbus Global Market Forecast 2018)

2.3 Security solutions deployed in airport infrastructures

Security is a multi-faceted issue in the context of airports and the security measures for passenger travel and cargo are quite different. A key aim of aviation security is to protect airport infrastructure, controlling the access of people's movements through surveillance and possible intelligent video surveillance using biometric tools to verify employee identify and access rights to particular buildings or areas.

A well-known implemented security solution is the detection and screening of passengers and their baggage. This can come in the form of X-ray screening, X-ray based explosive detection systems (EDS), explosive and chemical trace detection systems (ETD), neutron beam technology, and body scanners. Many types are often used in the same context, but the cost-benefit analysis has to be done carefully before adding a further method of scanning. While most of the publicity has been given to passenger screening, cargo screening is also important and there is a need to strengthen conventional detection systems. Current, average cargo screening technologies are limited and in light of liquid explosives and the use of CBRN (chemical, biological, radiological, and nuclear) materials, there is an increasing need while maintaining a low false positive rate. Importantly, baggage screening technology does not operate independently, but is controlled and managed by an industrial control system (ICS). These ICSs come in various forms, each offering their own types of security and risks, as will be discussed in section 2.3.1.

Information sharing has to occur about passengers, particularly between the EU and the US. While data privacy concerns are an issue, an agreement was reached so that 19 pieces of information about passengers may be shared. This ensures that the presence of any potentially dangerous people are reported for detection across many countries.

The Air Traffic Management (ATM) has its own unique set of security threats because attacks may occur on the system itself or on assets involved in its operation and there are increasingly more cyber threats to ATM systems. The Single European Sky ATM Research (SESAR) initiative aimed to address some of the ATM security concerns and encourages the move towards System Wide Information Management (SWIM) and other standardizations and regulations.

2.3.1 Analysis on existing ICS/SCADA systems in the airports and particularly on the BHS

Airport infrastructures (21), (22) like other industrial organizations, are generally comprised of two main classes of assets: physical assets and technological assets. The realm of airport physical assets (like control towers, hangars, terminals, baggage conveyors, etc.) is the core business of these transportation infrastructures and deliver a broad type of services (air traffic control, ground control, baggage and passenger boarding, etc.) to end-users that rely on the activities of these organizations (e.g., passengers, airline companies) (23). On the other hand, the technological assets that comprise the airport infrastructure monitor and control the organizations' physical assets and allow airport staff to have technologic tools to manage and supervise the work performed on the airport physical assets and automate the scheduling of the several tasks required to deliver airport services.

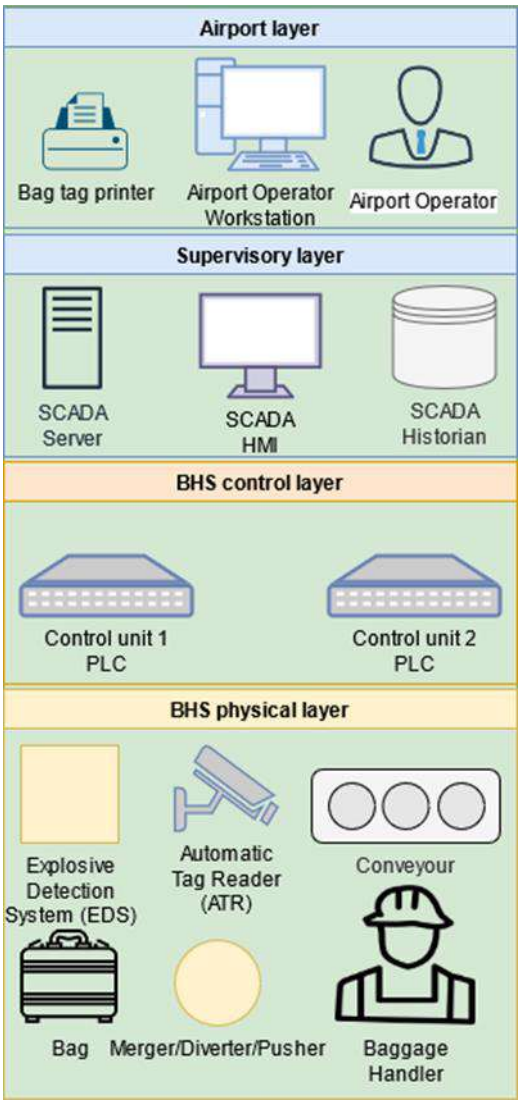

Figure 2.7: Example of ICS airport infrastructure architecture

Figure 2.7 provides a representation of an ICS airport infrastructure architecture, presenting the main components of the baggage handling system (BHS) commonly used in airports. Like other industry organizations (transportation, energy supply and distribution, manufacturing, etc.), airports typically follow industrial control system (ICS) architecture (24) where physical assets connect to technological assets using four main classes of technological devices:

1. Modular units – are intelligent embedded devices (IED) (24), (25) that serve as interface between physical and digital assets of the ICS organization. With the possibility of functioning

as sensors or actuators, these technology components are directly connected to physical assets (wired) and can: collect information about the asset physical state (acting as sensor); and, manipulate them according to certain events received from ICS control units (acting as actuator).

2. Control units – which are logical computing devices[1] connected to the modular units that decide, based on the input information gathered from modular sensor units, the actions that should be carried out by the actuator units to guarantee one or more airport services. Such decision capabilities are loaded as low computational programs[2] (26) each implementing one or more airport service. Moreover, contrary to modular units that are only communicate with one control unit, control units can also be connected[3] to a wide range of IT devices present in the ICS network (27) and this way collaborate by exchanging high-level information of the services provided by the airport. The level of collaboration between control units and other IT devices allows airport ICS to be classified into two categories:
    a. Centralized control systems (CCS) – In this case, only one central control unit is used to provide all airport services. All modular units are connected to this one control unit that decides reads input from all the sensors in the system and decides which actions should be performed to guarantee all the ensure all airport services. A representation of a CCS system is illustrated in Figure 2.7 in the box “Service A control layer”.
    b. Distributed control systems (DCS) - In this case, more than one central control unit is used to provide all airport services. All modular units are distributed between control units according on the airport services control unit is responsible for the decision making. Control units, then interact between each other, by exchanging the necessary high-level information and include these external data sources as input for decision making. Since most airports offer a wide range of services, and are comprised by wide variety of assets, it is very common for airports to use DCS architecture (e.g., several control units that exchange information and control specific assets: one or more control units that provide baggage handling services by controlling baggage handling assets; others for providing ground control services by controlling ground control assets; etc.). As described in (27), there are several ways for control unit interaction to take place, either one can use a multicast communication channel (also known as, multi-drop) where control units communicate freely, or a master-slave approach (also known as, series or series-star) where a main control unit sends information to the remainder control units. A representation of a master-slave DCS system is illustrated in Figure 2.7 in the box “BHS control layer”.
3. Human-machine interface (HMI) (28) – that are IT devices that serve as entry points for airport staff to interact to the ICS system. These components are network connected with control units and are responsible for:
    a. Gathering control unit information about the organization services and convert it to human understandable data representation format.

[1] Three examples of control units used in airport ICS are Programmable Logic Controller (PLC), Remote Terminal Unit (RTU), Programmable Automation Controller (PAC)

[2] Most control unit programs are developed in IEC 1131 or IEC 1499 programing languages (first one is used for centralized control unit, while the other one is used for distributed control units).

[3] Central units can connect to other IT devices using two types of network protocols: fieldbus protocols; and ethernet protocols. Most common fieldbus protocols are: Modbus; Controlnet; profibus. Most common ethernet protocols are: profinet; ethernet/IP; etherCAT.

   b. Receiving human commands for control unit interaction, converting and transmitting those commands in communication formats understandable by those control units.
4. Supervisory Control and Data Acquisition (SCADA) – which are IT devices that supervise the work performed by the control units that comprise the ICS. SCADA is responsible for: acquire the necessary data from those units for assessing the quality of service; triggering control unit actions whenever it is time to apply the necessary operations of a service; and to warn organization staff (typically using system alarms) whenever corrective measures are needed to be applied to the control units for restoring quality of service.

The overall network topology of an airport ICS network is geographically dispersed throughout the airport facilities and is organized in three layers organization layers: the supervisory layer; control layer; and physical layer. The supervisory layer contains the high-level monitoring tools of the ICS network, SCADA and HMI, and it is typically centralized in one location, the airport operation centre (APOC) (29) which is responsible for managing and applying concrete measures to guarantee airport quality of service. The supervisory layer is typically the only layer that has internet connection (24). The other layers, control layer (that contains control units of the system) and physical layer (physical assets and modular units), are geographically dispersed throughout the airport infrastructure depending where the physical assets are located. Information is exchanged from the supervisory layer to the control layer and then communicated to the physical layer.

In the remainder of this section we explore in detail the existing airport SCADA (section 2.3.1.1) and provide an in-depth overview on the baggage handling system (BHS) deployed on airports (section 2.3.1.2).

2.3.1.1 Supervisory Control and Data Acquisition (SCADA)

In order to supervise the work performed by the control layer and trigger the necessary actions for ensuring airport services, the SCADA system (27), (30) deployed in this type of infrastructures is responsible for: acquiring the necessary data from those units for assessing the quality of service; provide to airport operator the necessary information for decision making and trigger alarms whenever quality of service is in jeopardy. To do so, such systems typically follow a model-view-controller (MVC) approach comprised of three components: the SCADA Server (also known as, Master Terminal Unit); the SCADA Database (also known as, data historian); and the human machine interface.

SCADA Server is the controller of the system, provides real-time monitoring of the ICS network and issues operations to control units to assure airport services. This component continuously polls the several control units that comprise the ICS network, and collects from those units the status of the infrastructure physical assets. The information collected is then analysed and evaluated to assess the status and quality of the services offered by the airport. As result of this real-time assessment, the server sends operation requests to the control units to assure service continuity and generates notifies airport operators (through alarms) when upon detecting any incident related with: physical assets (e.g., malfunctions); airport service quality drop (e.g., baggage flight sortation problems); or security/safety (e.g., explosive detection).

SCADA Database is the model of the system, this component stores the complete registry of the assessment conducted by the SCADA server. Namely, stores the data collected from the control units of the system, through a data model that provides information about the status of every physical and technical asset of the ICS network; stores the status of every airport service at the time of the analysis conducted by the SCADA server; and stores the registry of the incidents that occur in the infrastructure.

SCADA HMI is the view of the system, display to the airport operator a complete view of the analysis conducted by the SCADA server. This HMI is connected to the SCADA database and presents the model of the system in the most suitable human representation, normally contains: graphical overview of the ICS network assets and status of the airport services; real-time notification with

graphical representations of alarms (sometimes with other human attention capturing methods, like sound and vibration) for increasing incident awareness and response; detailed vistas for airport operators to access SCADA database and analyse the assessments and actions performed by the SCADA server. This HMI also allows airport operators to interact with the SCADA server and select service operations to be performed by the control units of this ICS infrastructure.

Currently, airport SCADA is mostly used to supervise the operations of air traffic control (31), (32) and baggage handling system (33), (34). In terms of air traffic control, the SCADA system provides real-time status and operative controls over: runway lighting systems, radar systems, UPS and genset controllers. In terms of baggage handling these systems can provide real-time status about: conveyor, diverter/pusher, fire and security door, and X-ray equipment.

2.3.1.2 Airport Baggage Handling System (BHS)

As illustrated in Figure 2.7, baggage handling systems are ICS mechanisms deployed in airports that ensure all the necessary operations to guarantee baggage dropped on airport check-in areas are delivered securely to the destination planes (also known as baggage handling lifecycle).

The services offered by BHS include: baggage tracking (that monitors the route taken by each baggage from check-in to destination plane); baggage sortation (which separates baggage received on BHS according to the destination flight, in order to allow easy distribution of baggage by plane); baggage screening (which checks baggage authorizations to be onboarded on the assigned plane, and identifies potential evidences of explosive material objects inside the baggage). BHS services are accomplished, by deploying one or more control units (usually PLC that implements the aforementioned service operations) combined with modular units and a physical infrastructure that includes four main physical assets: conveyor; diverter/pusher/merger; automatic tag reader; baggage weight scale; and explosive detection systems (EDS) (25).

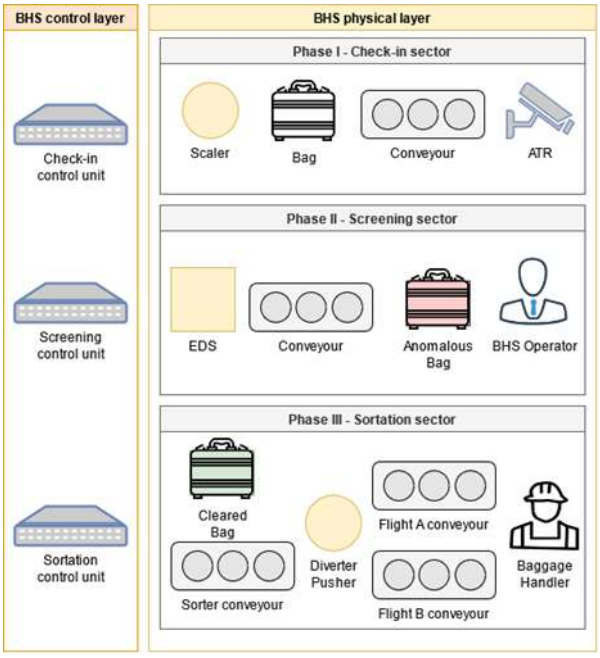

Figure 2.8: Example of BHS Distributed Control system

As can be seen in Figure 2.8, the BHS baggage transportation line path is composed of three main areas (25): (1) starting point of the BHS which is the airline check-in areas (where ATR and baggage weight scale are located), (2) then baggage are routed to the two BHS sectors: (2.1) security screening (where the EDS is located) and (2.2) baggage sortation (where diverters and pushers move the baggage to different conveyors in order distinguish them according to the destination flight); (3) and forward them to the flight makeup area for baggage collection and airplane onboarding (this

section includes ATR to provide baggage handlers the necessary information for flight onboarding). The behaviour of the BHS is typically implemented as follows:

1. Passengers check-in their baggage in the airlines check-in counters. Baggage is weighted using a weight scaler, and if authorized, a physical tag is attributed to the baggage with information about passenger (identification and name) and flight ticket (ticket number, plane identifier).
2. Baggage is put in the BHS entry conveyor, tag is scanned by the ATR and communicated to the BHS control unit. The BHS control unit decides whether the baggage is authorized based on information received by the supervisory layer (about the flight and passenger), and if authorized: starts the tracking of the baggage (by CCTV cameras and monitoring the speed of the baggage in the conveyor to ensure baggage is not manipulated); and forwards baggage to the screening area.
3. The screening area receives baggage and checks, using EDS devices, that no explosives are inside. The screening is typically composed of four conveyors (35) each representing a threat security level. All the bags are checked by EDS scanning devices classified into a specific threat security profile and they are treated accordingly..
4. The sortation area receives the baggage, scans it with the ATR and waits for the control unit decision. If the tracking system validates the baggage lifecycle, and explosive validation the baggage is then authorized for sortation and control unit sends baggage routing information. The sortation can be done manually by the baggage handler or automatically, using pushers and diverters, that forward the baggage to different conveyor lanes.

3 Overview of existing security solutions

3.1 Methodology

Airports have many security solutions and procedures in place. However, we needed to identify those which are extant and relevant for the hypothetical attacks outlined in this project. To this end, we followed the same systematic approach used in the methodology described in deliverable D2.1 sections 3.1 and 4.1 on the identification of critical assets and their vulnerabilities. The five scenarios, or attacks, include multiple steps which can each include a physical and/or cyber sub-attack. These sub-attacks were then analysed according to Know, Get in, Find, and Control: what kind of knowledge is required for the attacker, how they can physically or digitally gain access, how they can find what asset they are in search of, and how they can gain control of the targeted asset? This approach is based on the EBIOS risk analysis approach (35) used by ANSSI (the National Cybersecurity Agency of France), which is ISO 27001-, 27005- and 31000-compliant.

Using this same approach for security solutions as for asset identification and threat identification means that the results are consistent and closely connected. A particular sub-attack involves a particular asset, which in turn is involved in one or more airport operations, which are overseen by and/or follow certain security solutions. By identifying the individual assets involved in the sub-attack, such as a muster station or an internal network, we identified the surveillance cameras or cybersecurity standards directly related to those assets. The identification of the security teams involved in the threats management, lead to the identification of the security measures they are using to face the dangerous and/or emergency situations. This was performed for every sub-attack, therefore resulting in an exhaustive list of the security solutions used in each airport, and which assets and operations they involve, as shown in Figure 3.1.

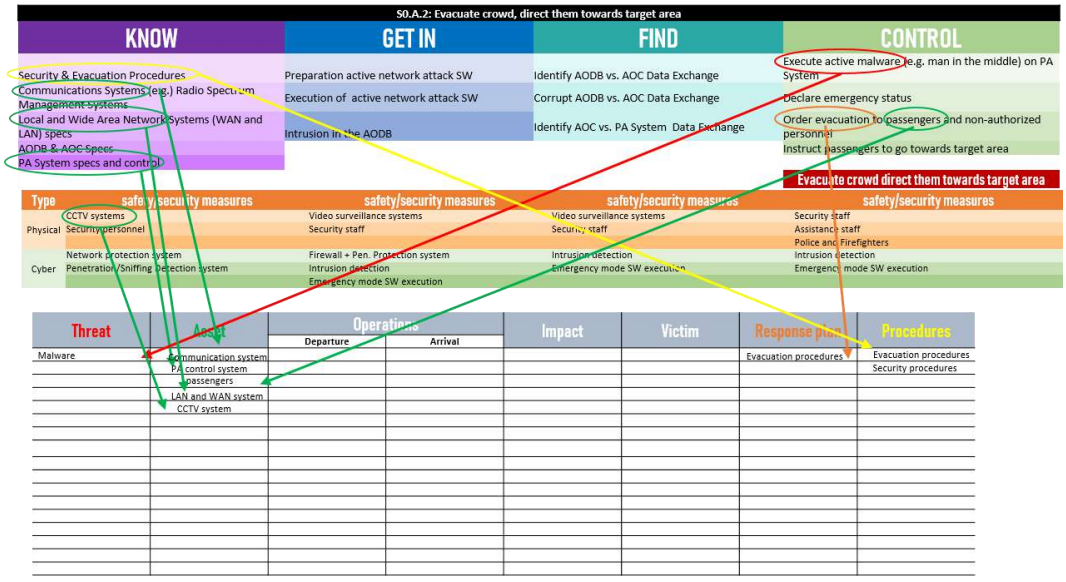

Figure 3.1: The elements in the Know, Get in, Find, and Control (KGFC) chart are translated into threats, assets, operations, impacts, victims, response plans, and procedures. This incomplete example demonstrates that each KGFC element may also involve more than one category.

3.2 Data collection and analysis of security controls in airport infrastructures

The collection of security solutions data started at the physical meeting in Athens (July 11-12, 2019) where almost all partners were present. Everyone was informed of the above-described methodology (Section 3.1) and worked together to this end. The primary goal of that meeting was to collect the relevant information for SATIE deliverable D2.1 (36) and therefore the work with security measures was later completed at the physical meeting in Zagreb (September 10-11, 2019). End-users agreed on which international standards they follow (and which are relevant for this project), along with nation-specific and airport-specific measures in use. All end-users verified with legal parties their ability to share this security information before information release.

The following sections present the physical and cybersecurity controls in the three SATIE demonstration airports (Athens International Airport, Franjo Tuđman Airport of Zagreb and Milan Airport).

3.2.1 Physical security controls in airport infrastructures

3.2.1.1 Physical security controls in Athens Airport

The physical security controls along with the physical security standards and legal background currently applied in the Athens International Airport (AIA) are described in the following.

3.2.1.1.1 AIA's applied physical security controls

This section describes the physical security controls applied by AIA for protecting the Company's information and technology resources from physical and environmental threats in order to reduce the risk of loss, theft, damage, or unauthorized access to those resources.

These controls establish a sound framework for the physical and environmental protection of AIA's facilities and system, in order to ensure the protection of its employees and passengers as well as to guarantee the confidentiality, integrity and availability of its information. Physical security controls of AIA have three types: organizational, procedural and technical. Organizational controls refer to constructive, structural policies performed vertically at the organizational level, procedural contain standards and internal instructions and guidelines to support organizational parts and technical controls involve policies regarding the physical security equipment.

The security equipment associated with the applied physical security controls in the Athens Airport is divided into three categories: electronic, responsive and structural.

- The electronic security equipment of Athens Airport are electronic systems or devices that support control operations or provide surveillance services and they fall in the following categories: (i) *Metal objects detection gates*. *Portable metal objects detector*; (ii) *X-ray machines*; (iii) *Explosive Detection Systems (EDS)*; (iv) *Explosive trace detection equipment (ETD)*; (v) *Long range cameras and other CCTV systems*; and (vi) *Perimeter detection - alarm systems.*
- Responsive security controls are considered forces capable of supporting the prevention of security events and the ensurance of safety within the airport.
- Structural security controls are measures designed to deny unauthorized access within the Airport.

3.2.1.1.2 Current security standards and legal background on Athens Airport physical security

The Athens International Airport applies a number of standards and regulations with regards to the *physical security controls* at international, EU, national and Airport Industry level. Indicatively, the following are listed:

- Annex 17 “Security - Safeguarding International Civil Aviation against Acts of Unlawful Interference” (37)
- Annex 9 “Facilitation” (38)
- Regulation (EC) N°300/2008. Most recent version: Commission implementing Regulation (EC) N° 2015/1998 (39)

3.2.1.2 Physical security controls in Milan Airports

The physical security controls along with the physical security standards and legal background currently applied in Milan Airports are described in the following sections.

3.2.1.2.1 Legal background on Milan Airports physical security

In Italy, the main point of reference for Civil Aviation security is the Ministry of Infrastructure and Transport which has delegated to ENAC (National Civil Aviation Authority) the administrative and operational functions relating to the Civil Aviation security.

With the Ministerial Decree of 21 July 2009, in fact, the Ministry has designated ENAC as a "Competent Authority" responsible for the coordination and monitoring of the implementation of the common basic rules on Civil Aviation security, according to the provisions of Art. 9 Reg. CE n. 300/2008.

The National Civil Aviation Security Program (PNS) of civil aviation described in Art. 10 Reg. CE n.300 / 2008 is drawn up by ENAC and defines the measures and requirements to be adopted for the protection of the security, the regularity and the national and international efficiency of the Civil Aviation in Italy, by providing dispositions and procedures tailored to prevent the execution of acts of illicit interference and the introduction of articles prohibited in areas potentially at risk. At the same time they regulate the response processes in case such events occur.

ENAC is divided into a central structure and local sections with Airport Districts (“Direzioni aeroportuali”), headed by a Director.

Every “Direzione Aeroportuale” ENAC coordinates, in normal situations, the application of the PNS measures, through a surveillance activity on the services given by the company managing the airport (as SEA), by the airlines and by the companies authorized to perform the security activities.

In emergency situations, collaboration with Police is envisaged to implement the necessary additional security measures. An essential role is played by the Border Police Office, which has a supervisory role to ensure the correct application of security measures and procedures and, in the event of disorders, in coordination with the Airport Management, assumes the direct management of the operations necessary to deal with them.

The provisions of the PNS, with reference to the regulation (EC) n. 300/2008, apply to:

1. Italian airports open to commercial air traffic;
2. airport operators;
3. air carriers;
4. subjects other than operators.

For other Italian airports not open to commercial air traffic, alternative security measures are applied, as allowed by regulation (EU) no. 1254/2009.

3.2.1.2.2 Milan Airports current security standards and applied physical security controls

With reference to Chapter 1 - AIRPORT SECURITY of the PNS, it is appropriate to specify that, in accordance with paragraph 2, letter h) of Art 705 of the Navigation Code, the company that manages the Airport (SEA SpA), without prejudice to the powers attributed to the state authorities regarding public order and security, civil defense, fire prevention and control, rescue and civil protection,

ensures security checks on passengers, baggage and cargo, in accordance with current regulations, as well as the management of lost and found items. SEA SpA responds to ENAC for the organization, preparation and performance of security services.

In order to efficiently manage a complex environment such as the airport, SEA applies a set of physical security controls to protect the organization from different kinds of threats. These controls embrace several aspects and areas including passengers and hand luggage check, hold baggage check, on-board supplies, airports supplies and cargo/mail security checks.

3.2.1.3 Physical security controls in Zagreb Airport

3.2.1.3.1 ZAG applied physical security controls

A variety of physical security controls (e.g. X-ray equipment and CCTV) are applied by Franjo Tuđman Airport Zagreb to protect the restricted areas of the airport. The main purpose of these controls is to ensure that no unauthorized person enters these areas and that no prohibited articles can be introduced into a critical part of security restricted areas or aircraft.

3.2.1.3.2 Current security standards and legal background on Zagreb Airport physical security

The Franjo Tuđman Airport Zagreb applies a list of standards and regulations at international, EU, national and Airport Operator level with regards to the physical security controls. In particular:
Annex 17 “Security - Safeguarding International Civil Aviation against Acts of Unlawful Interference”

- Doc 8973 - Aviation Security Manual
- Regulation (EC) N°300/2008
- Commission implementing Regulation (EC) N° 2015/1998
- Commission Implementing Decision of C(2015) 8005

3.2.2 Cybersecurity controls in airport infrastructures

3.2.2.1 Cybersecurity controls in Athens Airport

The following sections describe the proper Information Security Governance (ISG), the cybersecurity controls, the regulations and standards which are currently applied in the Athens International Airport.

3.2.2.1.1 AIA’s Information Security Governance

Athens International Airport’s assets and their effective utilization provide an organization with a competitive advantage, but it can also cause the destruction of the organization if misused or compromised. For this reason, it is imperative that all the important assets are protected adequately. Information security is the process whereby this objective is accomplished. The criticality of this process imposes that it should be an integral and transparent part of enterprise governance at AIA. In this context, AIA has adopted proper information security governance (ISG).

3.2.2.1.2 AIA’s applied cybersecurity controls

AIA has developed and adopted procedures and security controls that are proposed by the standard ISO 27001 as a combination of technical tools and management. The primary purpose of these controls is to ensure the protection of confidentiality, integrity, availability, accountability, authenticity and reliability of sensitive information stored or electronically transmitted and to ensure protection of company’s information technology resources.

3.2.2.1.3 Current security standards and legal background on Athens Airport cybersecurity

The Athens International Airport applies a set of cybersecurity standards and regulations at international and European level with regards to the *cybersecurity controls.* Bellow follows an indicative list of standards:

- ISO 27001:2013 (3) Information technology
- ISO 31000:2018 (4) Risk management - Guidelines
- ISO 27005:2018 (5) Information technology -Security techniques -Information security risk management
- ISO/IEC 27002:2013 (6) Information technology – Security techniques — Code of practice for information security controls
- NIST Framework for Improving Critical Infrastructure Cybersecurity
- ISO/IEC 27033 (2015) (7) IT network security standard.
- ICAO Annex 17 (37) - Aviation Security Manual – Document 8973
- EUROCAE ED-201 – 204 Aeronautical Information Security System (AISS) Framework
- ISA/IEC 62443 (40)
- EU NIS directive (10)

3.2.2.2 Cybersecurity controls in Milan Airport

3.2.2.2.1 Compliance with ISO 27001

As to SEA Milan Airports, in order to safeguard information security issues, in 2018-early 2019, an "IT Security Risk Assessment" activity and a consequent "Information Security Risk Management" have been performed, consistently with the recommendations indicated in ISO 27001, in order to consolidate corrective measures and IT security policies resulting from an appropriate risk assessment.

These activities have given rise to a baseline framework process, supported by a set of global policies and procedures aiming at mitigating the exposure to external and internal threats to the Company, in relation to information security risks.

3.2.2.2.2 Compliance with NIS Directive

The Directive 2016/1148 (41), the so-called NIS Directive, is a European Directive, stemming from this Directive, with the aim of defining the measures necessary to achieve a high level of security of its networks and IT systems, each Member State has given birth to its own Legislative Decree. In Italy it is the Legislative Decree 65 of 18 May 2018 (DL 65/2018).

As a consequence, in function of DL 65/2018, Italian Airports were summoned by Assareoporti to raise awareness on the NIS Directive. The cyber risk deserves full attention: it requires a deep awareness on the risks and requires necessary countermeasures to be identified for all the potential risks.

In turn, Italian Airports have independently completed a self-assessment process. In this context, SEA is verifying the compliance status of the measures active on its networks, systems, applications and data, with respect to the NIS Directive and DL 65/2018, with the aim of mapping the existing measures and those eventually to be implemented to strengthen the level of security of its networks and ICT systems.

3.2.2.2.3 Good practices against evolving cyber threats

The aviation community considers the security of smart airports and the preparedness against evolving cyber threats a top priority. The aviation system's resilience against attacks at different levels, the Identification of challenges posed by cyber threats, the risk assessment approaches and

guidelines to enhance cybersecurity, either in terms of high-level governance strategies or in terms of specific technological supports, are priorities currently tackled. In order to help Security Officers and actors involved in protecting smart airports against cyber-attacks, Operators, and asset owners, ENISA (1) has studied the current good practices. These practices represent what exists now and they are arranged according to the following three groups as suggested by ENISA: technical/tool-based, policies and standards, and organisational, people and processes.

3.2.2.3 Cybersecurity controls in Zagreb Airport

3.2.2.3.1 Objective

The objective is to define appropriate use of the ZAG Company Information system. The target is to prevent risky use of the ZAG Company Information system. The controls are applicable to all users of the ZAG Company Information system:

- ZAG Company Information system - includes all IT systems (all their software and hardware components; personal computers, servers, computer and network operative systems, network applications and maintenance), other IT resources and communication equipment, regardless of the location, types of connections and interconnections, which are used inside ZAG, as well as the IT property given for use to ZAG affiliated companies, but is under monitoring and management of the ZAG.
- User of the information system - employees of the ZAG and other companies, external partners, tenants and all other users who have permission to use the ZAG Information system, and in accordance with legal relations with this ZAG are obliged to observe the controls.
- Usage of ZAG Information system by the User of information system implies use of all parts of ZAG Information system owned by the ZAG or being in other form of owned property/usage in the ZAG.

3.2.2.3.2 ZAG cybersecurity controls

ZAG implemented security controls to ensure confidentiality, integrity, and availability of company information and systems. It should be noted that the controls are used internally but also are mandatory for suppliers which maintain parts of the information system of ZAG. In respect to cybersecurity law, controls are also important for alignment with demands specified in mentioned law.

3.3 Crisis Management and Societal Impacts in place

3.3.1 Crisis management and Societal Impacts at the Athens Airport

The Crisis Management Plan (CMP) of Athens International Airport is the general process by which the Airport Organization handles possible major events which threaten to harm its business continuity, the proper and safe operation of the airport's stakeholders, as well as the safe circulation of the general public within the airport's facilities.

Any incident or even occurrence could potentially be escalated into a crisis depending on the level of the professionalism at the very first reaction and of course on the degree of readiness in both human and material resources.

The CMP is AIA's form of preparedness that allows the involved agencies to deal with crisis more effectively than through ad hoc responses. Of course, the CMP alone does not guarantee that a

particular crisis will not occur, but it does signal the intent of the involved to respond forcefully to any contingency that may develop. While the definition of a crisis can vary, each event covered by the CMP is included in specific categories of crisis, which can be arisen and be escalated as a domino effect from even a simple/daily/operative incident caused by either cyber or physical attack against the normal and smooth operation of the airport.

3.3.2 Crisis management and Societal Impacts at the Milan Airports

The **ENAC Advisory Circular APT 18th** "Airport emergency plan - plane crash" (42), specifies that ENAC has adopted the "Regulation for the construction and operation of airports", which formally incorporated into the national regulatory framework the standards and recommended practices contained in ICAO - Annex 14 (43). The Regulation, in introducing the Certification of the Airport, has provided that, for each airport, plans are prepared for the management of the various types of emergencies that may occur and in particular for those arising from aircraft accidents affecting the airport or its immediate vicinity.
The Regulation also establishes that the Airport Operator prepares the parts of its responsibility for the Emergency Plan and submits them to ENAC for evaluation.

With the Regulation (EU) n. 139 dated 12 February 2014 (44) , which entered into force on 6 March 2014, the European Commission adopted and published the Implementation Regulation (IRs) of the Basic Regulation (Regulation (EC) No. 216/2008).
The recipients of **Regulation (EU) n. 139/2014** are:

- The competent Authority or Authorities for the certification and surveillance of certified airports
- Airport Operators
- Suppliers of apron management services (Apron Management Service (AMS))

The Regulation (EU) n. 139/2014 of 12 February 2014, establishes the technical requirements and administrative procedures relating to the airports pursuant to Regulation (EC) n. 216/2008 of the European Parliament and of the Council.
The new Reg. (EU) n. 139/2014 introduces a set of articles (from art. 1 to art. 11) intended for Member States and, attached, a series of IRs, collected in three distinct Parts (Parts), named respectively:

- Part ADR.AR (Part Authority Requirements, for the competent Civil Aviation Authority);
- Part ADR.OR (Part Organization Requirements, for Aerodrome Operators);
- Part ADR.OPS (Part Operation Requirements, for airport operations).

The EU139 / 2014 Regulation - Annex III - Chapter D “Management” - ADR.OR.D.005 “Management system” - part b (10) - states that “the management system must include the coordination of the safety management system with the airport emergency plan and coordination of the airport plan with the emergency plans of the organizations with which the safety management system must interface during the provision of airport services".
The EU139 / 2014 Regulation - Annex IV - Chapter B: "Airport operational services, plants and installations - ADR.OPS.B.005 - Emergency planning for the airport” also provides that “The airport manager has and implements an Emergency Plan for the airport that:

a. Is commensurate with the operations of the aircraft and other activities carried out at the airport.
b. Provides for the coordination of appropriate organizations in response to an emergency occurring at or near an airport.
c. Contains procedures for periodically verifying the adequacy of the plan and for reviewing the results in order to improve their effectiveness.IT 14.2.2014 Official Journal of the European Union L 44/31”.

The Airport Manual, as foreseen by EU Regulation 139/2014 - Annex III - Chapter E: "Airport Manual and related documentation" - ADR.OR.E.005, must be prepared by the Airport Operator.
It describes the procedures used by the Airport Operator for defining the contents of the parts of the Emergency Plan of its own competence, for monitoring the adequacy of such contents over time, for the qualification of the personnel involved in the activities related to emergencies, as well as the allocation of responsibilities for these activities.
It is useful to specify that it is not useful for the Manual to include "parts" of the Emergency Plan, but it is advisable that correct procedures are defined for the connection between the normal activity of the operator and the emergency.

3.3.3 Crisis Management and Societal Impacts at the Zagreb Airport

The first and main objective of emergency interventions is to save lives, and prevent the danger and threats to people, property and the environment.
ZAG adopts this plan for the purpose of defining an organized and coordinated transition from normal activities to a functioning state. This plan defines the types of emergencies, alerting, activation of the coordination and command units, procedures, main tasks and responsibilities, and key personnels.
The ZAG will, within the limits of its capabilities, take all necessary measures and engage available resources in order to minimize the consequences of an emergency, and prevent its escalation. ZAG will, in cooperation with relevant stakeholders, endeavour as soon as possible, depending on the type and scale of the particular emergency, to ensure the safe functioning of the airport and continued aircraft operations.

4 A study about expected improvements from SATIE

Gap analysis is based on taking a critical look at the current position of an area in order to implement specific improvements. The first step, then, in performing a gap analysis is to define where we want to go using terms as specific as possible. In this way, it will be possible to build an effective information security program that helps to minimize risk exposure and ensure a clear strategy for handling incidents while maintaining a continuous improvement and monitoring process.

To develop a gap analysis, the following four key steps (45) were used:

1. Seek an understanding of the environment surrounding the project.
2. Take a holistic view of the environment to gain a complete understanding.
3. Determine what framework your team will use for project assessment.
4. Make sure to provide data supporting the analysis performed.

Thus, in the next section, keeping these four steps in mind, the gap analysis of SATIE project will be developed. Subsequently, by using the gap analysis as a basis, the expected improvements from SATIE project will be presented.

4.1 Gap analysis

Airports are complex infrastructures where three dimensions co-exist: Landside, with the security and ground staff, Airside, with the needs of both internal and external coordination, and the Terminal, with the IT infrastructure, passengers coordination and buildings. As already outlined in the previous sections, there are many current standards and several different guidelines for risk management. A lot of security tools are used in airport infrastructure to maintain the physical and cybersecurity at airports, however, there are still some gaps, in particular the need to face more complex attacks, resulting from the combination of cyber and physical breaches, that are very representative of today's challenges in cyber and physical security of the airports. Taking into consideration all these current regulations, standards and daily challenges faced by the airports, the following security gaps have been identified (1), (2), (46):

1. **Security Convergence.** Security convergence has become a critical factor in airport cybersecurity and risk management. Security convergence refers to the convergence of two historically distinct security functions – physical security and information security – within infrastructures. Both are integral parts of any coherent risk management plan. It is important because control systems, physical security and IT security are now converging on an incredibly regular basis. For many organisations, increasing their security means changing their cultural concerns around it. Some difficulties arise from cultural changes, like the perception that physical security personnel are more blue collar, while the IT security industry is considered more white collar is one that needs to be overcome. There is a need to bridge the gap between physical and IT security and look upon it as one entity.

2. **Gaps in taking the best potential of AI and data analysis for enhanced safety and security.** Airports have no choice but to place AI (Artificial Intelligence) at the top of their priority lists, both for security solutions to better prevent, detect, respond and mitigate cyber and physical problems. The more operational data they can capture and centralise, the faster they can bring some certainty back to operations and rebuild passenger confidence. Current topics like COVID19

pandemics are good examples of the benefits these technologies can bring from the safety point of view and also in the convergence of safety and security.

3. **Disparity of physical-cyber security solutions implemented in airports.** There is not a common adoption level and implementation of physical-cyber solutions that can support and enhance crisis management processes. Especially with regards to the cybersecurity the existing guidelines are broad enough, meaning that each airport decides upon their understanding for the measures to be adopted. Threrefore, some airports have a very mature cybersecurity posture, however, due to several reasons, many other airports have limited capabilities or resources dedicated to cybersecurity. Moreover, even some simple best practices are not in place, for example, password reuse or sharing is common and a centralised centre for incident handling does not exist.

4. **Lack of integration between cybersecurity and privacy compliance**

   The General Data Protection Regulation (GDPR) applicable since May 25th 2018 is now the legal framework for the protection of personal data in Europe. So, cybersecurity processes must be well integrated with data protection processes in order to:

   - Ensure and to be able to demonstrate that processing is performed in accordance with the GDPR.
   - Satisfy data subject's privacy needs and rights.
   - Improve transparency between data controllers and data subject services.
   - Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing.
   - Find a trusted basis for risk calculation services in cyber sector.

   With the introduction of GDPR airports need to implement changes to ensure compliance with the new regulation. In addition, compliance with NIS Directives also requires some changes in the airport systems and infrastructure. However, airports are critical infrastructures where change is always difficult to happen, and therefore some airports do not fully comply with NIS directives or/and GDPR law.

5. **Lack of complex cyber-physical threats consideration in risk assessment definition**

   Airports, due to its critical and vulnerable infrastructure, are a profitable target for physical-cybercrime, since exploiting its vulnerabilities brings a huge potential for financial and political gain. Several physical and cyber assets can be used as the source of the attack. In order to have the desired impact, an attacker could prepare, during months or even years complex attacks involving some cyber and physical assets (cyber-physical attacks). Typically, these attacks are difficult to predict, since they are new and sophisticated to ensure they can achieve their goal. This difficulty in attack detection is due to the lack of harmonization between cyber and physical security, which hinders the correlation of suspicious and dangerous actions. Because of that, risk assessment methods often underestimate these complex cyber-physical attacks.

   Moreover, there is a lack in predicting the potential impact of such incidents within the Airport (i.e. fire propagation, terrorist attacks, plum dispersion, impact of toxic chemicals, radioactivity etc.), but also between interconnected CIs, as disruptions in one sector can have cascading effects in other sectors, including cross-border.

   However, it is crucial to fight against this principle since these attacks can destabilize large organizations, nations and unions. In doing this, there is a need from airports to better understand the crisis management process as well as the stakeholders involved in this. In addition to this in order to enhance readiness and cooperation of all involved stakeholders to

respond to any type of complex incidents and emergencies, continuous and specialised training is of paramount importance.

6. **Missing mapping between airport assets and airport operations**

   The first step of any cybersecurity program is the identification of the assets, operations, business practices and data flows within the organization. This inventory is necessary in order to implement useful protective measures and organize all the details necessary in case of attack. However, not only is its identification important, the way they are related is also crucial to understanding what might be affected by a successful physical and/or cyber attacks. Thus, it is indispensable to develop a clear mapping between airport assets and airport operations (e.g. business processes), in order to improve cyber-physical detection rules and impact propagation models.

7. **Command-control systems (like the Baggage Handling System) are not sufficiently secured**

   Command control systems cover several types of systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCSs), programmable logic controllers (PLCs), and general-purpose controllers (GPCs), such as airfield lighting control system, NAVAIDS, baggage handling system, Building Management System, Energies Management, etc. They perform various functions and exist at different stages of evolution throughout airport processes. Many of the systems used today were designed for availability and reliability during an era when security received low priority, and where they operated in isolated environments. In addition, they typically rely on proprietary software, hardware, and communications technologies. All these characteristics make control systems a good target for attackers. Today these systems are becoming increasingly interconnected and interdependent, which may introduce additional vectors of attack that can have a huge impact on operations, since they will compromise the availability and integrity of these systems.

   All these systems comprise several IT, OT, IoT and SCADA assets. However, not all assets are correctly inventoried and managed, which can introduce many vulnerabilities in the system. Moreover, IT and OT systems are very different, so we cannot fully transpose IT cybersecurity methods to OT. OT is about availability and integrity of cyber-physical systems, whereas IT is about management of information. These differences can lead to inappropriate measure or lack of cybersecurity. Therefore, it is important to implement appropriate cybersecurity measures, incorporating cybersecurity in the earliest stages of design. Also, legacy applications should be fully supported given the longevity of the technical airport facilities. These implementation needs should be justified and analyzed during the risk assessment process.

8. **Radio communication networks are insufficiently secured**

   Radio communications networks, such as Wi-Fi, support a lot of systems as baggage handling, aircraft gate, facilities maintenance, operation and security needs. Moreover, many airports offer public Wi-Fi internet connectivity to passengers. All of these networks, if not properly protected, are vulnerable to cyber threats in a different number of ways, e.g. laptops, wireless access points, smartphones, emails, etc. In recent years, not only the airport users, but even the airport personnel wish to bring their own devices into the workplace. However, if these devices interact with enterprise systems (such as e-mail and VPN access) they can potentially be used to secretly gather confidential information or introduce viruses. Similarly, the increasing use of mobile Wi-Fi hotspots can pose serious cyber threats since hardware options for mobile hotspots, such as Mi-Fi devices and USB Wi-Fi routers can be easily brought into airport premises (46). In addition, these potential cyber-attack sources can lead to the occurrence of physical threats, causing a bigger impact in airport security, which is not so easily detected. Therefore, it is crucial to implement countermeasures to reduce the likelihood of vulnerability to these threats.

9. **Novel System Wide Information Management (SWIM) services**

System-wide information management (SWIM) was developed to facilitate the sharing of essential information between all air traffic management (ATM) stakeholders. SWIM is essential for the modern ATM systems such as NextGen, Single European Sky, CARATS and others, facing new challenges inspired to safety, efficiency and resilience. The fundamental premise of SWIM requires complete information availability at multiple levels with a plurality of recipients and a degree of reliability consistent with the expected safety, security, affordability and availability requirements. This modern concept of aeronautical information must at every stage consider security as a main requirement, however, as any new system, it requires a new approach in terms of cybersecurity actions, learning from the safety approach and taking into account the similarities and differences. It can bring new attack vectors and keep some that already exist, but the important action is to analyse the potential effects of new information sharing paradigms, such as SWIM, and take the necessary countermeasures to prevent cyber-physical attacks (47).

10. **Voice communication attacks**

Voice communication is the primary means of communication between ATC and the aircraft. It is used to transmit all ATC instructions to the aircraft, which are acknowledged by the pilot, as well as pilots' reports and requests to ATC. Flight information services, weather reports, and airport information broadcasts can also be provided by voice communication. It is also used for operational communication between the airline operator and the aircraft, as far as the aircraft is in range of the operator's transmitter. Voice communication is conducted by analogue radio on VHF and HF (outside VHF range, e.g., over oceans) (48). Therefore, spamming and spoofing attacks (for example) on voice communication networks put both airside and landside operations at risk. A key element of security needs in these ATM critical communications is end-to-end encryption without compromising and violating strict requirements such as high-availability (network resiliency with full redundancy) as well as precise timing and very low delay, jitter and packet loss needs (49). However, physical security should not be forgotten or underestimated. Security measures should be implemented (if not already done) to avoid unwanted access to the ATC tower and other ANSP-facilities deserving protection to avoid subsequent risks.

11. **Breaches raised by lost baggage tags**

Baggage tags are more important than a passenger thinks. Passenger name, frequent flyer number, address and other personal information can all be accessed by using a barcode reader, which can be downloaded for free on the internet.Moreover, each traveller is identified by a six-digit code which is also the booking code (known as a PNR Locator) and is printed on boarding passes and baggage tags.

A passenger's last name and their PNR locator code is all that is needed to access a booking. Once logged in, an attacker can see details about the flight and all other passengers in the same booking. This includes full names and often email addresses, phone numbers, frequent flyer numbers, postal addresses and, for intercontinental flights, passport details and dates of birth. With most airlines, having the PNR code and passenger's last name means an attacker can cancel the flight, rebook it for another date, or change customer details in their frequent flyer account. Basically, an attacker could gain full control over passenger bookings and have access to a lot of sensitive information that could also be used to carry out identity theft and phishing attacks (50). Therefore, the link between passenger and baggage must be better managed through, for example, an extended passenger identity and enhanced video monitoring with picture recognition of passengers' baggage. Anomaly detection on passenger data is still frequent in the airports and need to be improved.

12. **Correlation between physical and cybersecurity events**

The integration of physical and digital worlds is helping airports to cope with new challenges. However, the correlation between physical and cybersecurity events is not easy to perform due to the lack of interoperability between physical and cybersecurity solutions (e.g. access control

systems, IDS, IPS, etc.). The existence of legacy systems and their lack of compatibility with smart technologies, the outdated policies and the insufficient experience make it difficult to establish a correlation between physical and cybersecurity events. This gap is a direct consequence of the lack of harmonization between cyber and physical security.

13. **Forensics investigation tools**

Forensics investigation tools remains notably under-developed especially due to lack of enough solid data that combines cyber and physical incidents and threats which can be very distant in time. Log files can be an important source of data, since they are the most likely of all files residing in a system that contain significant information. They can help to understand how, when and where an attack occurred and to reveal the malicious activities of the attacker. However, as mentioned before, the difficulty in correlating physical and cybersecurity events hinders the analysis of different data, reducing the efficiency and usefulness of the forensic investigation tools.

14. **Lack of structured and fast communication and harmonized procedures**

According to current usual practices, most airports, CIs and involved stakeholders during a crisis use multiple decentralised information gathering processes that run in parallel (potentially overlap). Usually, there is no single coordination point acquiring the complete set of collected data for feeding it to the interested parties. It is well known, that aiports, and CIs in general, need to effectively and efficiently manage and share information (incident detection, evolution, resource allocation and management etc.), in different layers: within the airport, between the airport and its response partners, between the airport and the public, as well as between inter-connected CIs. To that end, there is arguably the need for a collaborative platform for airports to share data with Airport Operation Centers, Security Operation Centers, local authorities, first-responders and maintenance teams. The lack of a real network to collaborate on specific issues of cyber and physical security has a negative impact on airport structures and security priorities within it.

Also, a data sharing platform would allow airports to share information on new attack vectors and early warning vulnerabilities in systems to provide continuous system improvements. Before being implemented, this need for communication and collaboration should be analyzed during the risk assessment process to check if the advantages of the use of the data sharing plataform outweight the risks of an attack.

15. **Lack of cost-effective solutions for cyber physical security**

It is difficult to show return on investment for physical-cyber risk programs, since the budget on airports side is very limited to cover security requirements defined by national and European authorities. Airport safety and security teams have a hard time demonstrating that the investments they are making are aligned with the actual risks they face. They must ask if they are making the appropriate investments in security, vigilance, and resilience, and whether those decisions are based on a realistic understanding of the specific risks their organisation faces – and the magnitude of impact that a physical and/or cyber-attack could have. The use of detailed risk assessments should help justify the use of such safecty and security plans, programs and measures, when potential incidents are identified.

16. **Different or no security plans within each airport**

As mentioned in Gap 1, each airport is individually responsible for developing its own physical-cybersecurity measures. There are several guidelines and standards addressing cybersecurity practices that need to be implemented, but its interpretation and adaptation to fit an airport context is done by each airport. Therefore, standards and guidelines for the implementation of comprehensive plans for the security of airports are needed at a national level in order to build a common ground for all airports. It is of high value to have a series of standardized plans (Risk and

Vulnerability Assessment, Security Operations, Crisis Management, Business Continuity) related to preventive planning, day-to-day operation and business continuity management. Therefore, despite the importance of having security guidelines and standards that can serve as a baseline level of security processes, it is also important to ensure the consistency of its application at airports.

In addition to the challenge of correcting the aforementioned gaps, there is also the additional challenges of combining them, and updating security policies in favour of a simplified change management. A common awareness to security as a whole shall be raised, together with harmonized roles, responsibilities and procedures, ensuring improved prevention, detection, response, mitigation and recovery against physical and cybersecurity threats and attacks. These changes in security approach and operations allow for the improvement of the synergy between cyber and physical security, which, in turn, should affect the risk assessments made. That is the number of potential incidents should diminish with the application of better cyber and physical security measures.

4.2 Identification of expected improvements from SATIE

The gap analysis allowed the identification of twelve key objectives that will support the development of the security toolkit to protect critical air transport infrastructures against combined cyber-physical threats. These objectives and the gaps to which they respond are presented in the Table 4.1.

Table 4.1: Key objectives

Ref	Objectives	Gap
O1	Identify main areas of security improvements in airport infrastructures	3
O2	Improve risk assessment methods to address complex attack scenarios	3,4
O3	Improve cyber threat prevention on airport assets and communications	3, 5,6,7
O4	Improve physical threat prevention and detection against access to critical areas and passenger control	3,9
O5	Improve cyber threat detection on airports IT and OT networks	3,5,7,8
O6	Improve correlation of cyber and physical threats to facilitate human analysis and decision-making	3,10
O7	Improve incident response and impact mitigation for a unified and fast response	3, 4,11,12
O8	Carry out operational demonstrations at TRL7 in real conditions at three different international airports	All
O9	Continuous improvement approach to dynamic airport security standards and to the harmonization of emergency and security-incident related approaches	12,14
O10	Disseminate project results to inform the pervasive service industry, and the scientific and business communities about the developments	All
O11	Provide efficient and cost effective solutions for airport security	13
O12	Ensure compliance with ethics, privacy and regulations	1,2,14

According to these objectives, it is possible to identify fourteen key innovation elements of SATIE project that will improve the state of the art by addressing the conceptual, technical, economic and social gaps already identified:

a) Risk assessment platform with cyber-physical threat analysis (RIS)

Existing risk management solutions are not able to combine and correlate cyber and physical threats in an integrated risk view. Usually, these solutions analyse the cyber and physical threats separately. Another issue of the current solutions is the use of predefined categories of threats and vulnerabilities that are limited and not dynamically updated to the current landscape, what makes difficult the prevention against not known attacks. This can be solved by a repeatable analysis to compare the threats in the course of time. However, this is not a easy task to current solutions due to its actual design. Also, risk treatment is almost never considered, what makes difficult to identify the high-priority domains where to invest resources.

Hereupon, SATIE project aims to develop a novel comprehensive and holistic cyber-physical security risk management platform considering all phases of risk management process, providing qualitative and quantitative risk analysis results. The methodology adopted for risk analysis will be in accordance with the principles of the ISO 31000 standard that provides guidelines for risk management process. Unifying the world of physical security and logical security in a single integrated risk scenario, the platform will help to prevent and cope with complex attacks (for example, attacks that exploit vulnerability typical of the ICT world to disable some checks and then put in place a physical threat). The platform will implement functions that allow the user to realize "what-if" scenarios of risk treatment in order to provide assistance for mitigation. Infrastructure owners will be able to evaluate different risk treatment plans, analyse them and choose the most effective one, balancing cost and benefits. The platform will be realized so that it can be used "as-a-service" in order to simplify its adoption in new generation airport SOCs. This way, the adoption of the platform can take place very quickly, even experimentally, from all those airports that are interested in adopting the holistic approach to risk carried out by the SATIE project. The modular nature of the platform and the fact that it can be used "as-a-service" can also facilitate the exchange of information between the various entities involved, sharing information about new threats, vulnerabilities, but also contingency and strategic plans for risk reduction.

b) Vulnerability management system for ICS and OT systems (GLPI)

The proprietary IT Service Management Systems (ITSM) solutions of the consortium partners manage an Information System containing desktops, servers and mobiles. However, they do not manage ICS/SCADA systems that are connected inside this Information System. No vulnerability management, connected with the Information System inventory, is provided, making this task complicated for the Information Systems' administrator. Automatic discovery of vulnerability is not yet integrated in the solution.

The platform developed will be integrated in single ITMS OT systems, ICS/SCADA systems as well as standard desktop and server systems, leveraging a unique database of all the IT components of the airport Information System. This database provides an inventory of all the components and will be automatically updated, delivering an up-to-date cartography of the airport's Information Systems: having an exhaustive and detailed inventory of an Information System is considered as a prerequisite for a security policy, but ITSM tools that are able to integrate standard desktops and servers as well as specialized systems such as OT or ICS/SCADA are missing. The centralized view of the airport IS provided by the platform will be accessible by the other components of the platform, in particular to the Incident Management Platform; based on this inventory, a vulnerabilities map will be established, showing the different levels of trust for all the IT/OT components in the airport. Using security evaluation rules as well as automatic discovery of vulnerabilities, a security ranking of the components of the airport IS will be delivered and automatically updated, delivering accurate input data for the risk assessment platform.

c) Encryption framework for secured IoT communications on Baggage Handling Systems (BHS)

Airports, formerly isolated in dedicated network with no connection to the IT or internet (air gapped), are continually being integrated into complex networks. New cybersecurity threats are emerging because of the interconnection of these highly connected IoT components with the traditionally segregated industrial control systems. Although several proposals exist for industrial control system (ICS) communication security, they are not widely adopted in systems like the BHS. IoT devices generally follow a different set of security protocols than the ones used in the ICS domain.

Under SATIE project, a communication security module will be developed in order to mitigate the risks of interconnection of an ICS, such as the Baggage Handling System, to the IoT ecosystem. This will be achieved by studying the vulnerabilities and threats that arise from this new type of interconnections, and the implementation of security communication modules for the two different interconnected domains: ICS and IoT. Although the BHS will be used as the reference application. The result might be reused for other IoT and ICS assets in the airports.

d) Unified access control system combined with video analytics

The most efficient existing access control systems are based on biometrics. They sometimes combine several biometrics (fingerprint, iris, face, etc.). However, even based on biometrics technologies, the current access control systems need human continuous monitoring. This fact limits the global capability of the airport security system and the Authorities to generate and to manage alerts. Therefore, combining access control technologies based on biometrics with video analytics will improve the prevention against physical threats and improve resilience and security response of the people and the airport infrastructure. Morpho Video and Image analytic platform (MVI – the software that enhances video analysis capabilities in daily security tasks and in criminal investigations) is the key component of the SATIE system to be implemented. MVI offers in depth post event analysis of video information from a range of sources. Investigators will benefit from real-time, or near real-time awareness of events both in live video feeds and in recorded videos.

e) Extended passenger identity with baggage tracking and data analysis for anomaly detection

All airports are equipped with check-in systems, able to collect API (Advanced Passenger Information) data (from “MRZ” Machine Readable Zone) of all passengers checked-in. However, only a very limited number of these systems all over the world are coupled with an API data analysis system. In the other hand, the baggage tracking by current BHS is based on baggage identification by means of tags.

Considering baggage as an extended passenger identity, it will be developed a complement to the BHS, which provides baggage identification functionalities as well as cross relations between passenger and baggage, by means of CNN (Convolutional Neural Network). This system aims at tracking lost or isolated untagged baggage. It identifies unusual characteristics of Passenger API data and related operational data, highlighting any potential cyber or physical threats (e.g. unusual changes to passenger records, unusual itineraries and unusual booking characteristics). It provides internal risk assessment to determine potential threats. Targeting is based on Watch-list matching and Profile matching. Risk Assessment is performed for all bookings and check-ins. It can be connected to national systems for verification against government watch-lists, and Interpol FIND/MIND if available. It applies maschine learning algorithms and predictive analytics to highlight outliers in Passenger Name Records, reduce the number of false positives, and infer potential threats based on past threats. It can import/export results of risk assessment and expected passenger movements from government systems. It can be connected to airports check-in systems for passenger identity control, travel document verification, and Passenger Name Record validity. Passport verification is based on MRZ or RFID reading for e-passports.

Verification may include: verification against lost or stolen passports, verification of e-passports certificates, and verification of cryptographic protection of Passenger Name Record.

f) Secured air traffic management data services with enhanced traceability

SWIM Technical Infrastructure and SWIM compliant services and applications are operating in an environment with complex threat scenarios that go beyond simple attacks using a singular attack vector. However, the current standard of securing SWIM services is based on authentication (access control), confidentiality (encryption) and integrity (verification) on data and service level. These protections assume a relatively low level of sophistication that focuses on one or a low number of technical aspects, like basic schema checks on data, or even assuming that data signed with the correct key is trustworthy.

Therefore, while security has been a focus in SWIM, validating and enhancing the SWIM security concepts are a key innovation on SATIE project. In order to provide guidance for retaining data and service integrity, and to secure the operational status of the air transportation infrastructure as a whole, complex and wide-ranging multi-pronged attack scenarios that include, but are not limited to cyber-attacks, will be evaluated and demonstrated.

g) Traffic Management Intrusion and Compliance System (TraMICS)

Conflict detection and conformance monitoring are elements already used in air traffic control systems for safety reasons. However, it is important to decrease detection time of security threats and support immediate decision about mitigation procedures. Thus, a Traffic Management Intrusion and Compliance System will be developed to monitor different indications and correlate them to a security threat indicator. To achieve this, TraMICS monitors voice communication and traffic situation with regard to command conformance and common behaviour patterns. Speaker authentication, speaker acute-stress detection and plausibility checks of ATC instructions/aircraft movements will be features of this innovative system. Also, information on the vocal effort will be provided, since, according to recent research, it significantly affects the reliability of the speaker authentication. The system will be setup in such a flexible way that the conditions of different application areas (e.g. ground control) can be considered.

h) Cyber threat detection on critical networks and business processes

Currently, the majority of tools countering cyber-attacks (in particular in the application layer) are either proprietary solutions that are shipped with commercial licences or require cloud-based deployment. Some of these tools are also functionally limited to a specific environment.

Thus, the data from various services and knowledge as well as the context retrieved from recent threat scenarios analysis, will be used to build a new anomaly and cyber-attacks detection system. In example, malfunctioning, infected or taken over by cybercriminal components of the system, usually act differently than normal (e.g. excessively communicating with unknown hosts over the internet). The normality model can be seamlessly extracted from the collected data using popular machine learning solutions such as unsupervised deep auto encoders, recurrent neural networks or stochastic models. Moreover, our ambition will be also to improve already developed anomaly and cyber-attack detection methods in the application layer. Particularly, we will aim at extending the capabilities of our method for automated signatures generation. Part of the objective will be to provide online-learning capabilities of used models/classifiers and to improve scalability and interoperability. Using data generated by the ICS systems as part of the control process, and taking into account the business process where the specific systems are used, a Business Process specification-based Intrusion Detection System (BP-IDS) will be used to detect anomalies on processes that depend of ICS systems. The cyber threat detection system will serve as additional probes that produce security related events to the correlation engine.

i) Correlation engine for cyber-physical threat detection

Many correlation systems are available on the market with a high maturity level. Most efficient solutions are owned by large US companies like Splunk or IBM (QRadar). These systems are cyber oriented, but they do not take into account physical security solutions like access control events. They are also big data oriented, very relevant for large interconnected networks. Moreover, annual licence costs are expensive and indexed on data load.

So, under the SATIE project a new correlation engine, based on an open-source framework which is more relevant for small segregated networks, will be developed. It will combine cyber and physical security events by gathering syslog data coming from various services and detection systems in order to store it and to process it in real time. Data processing includes threat signature detection based on deep packet inspection and file analysis as well as aviation specific rules in order to detect inconsistent information or combination of cyber and physical security events, also known as low signals. The correlation engine is accessible from the investigation engine in order to perform timeline analysis on a long-time frame and generate reports. It will include aviation specific rules related to anomaly detection on data exchanges related to passenger controls, baggage handling, and air traffic management. Finally, it will trigger real time alerts that are sent to the incident management system.

j) Data analytics for forensics investigation and fast recovery

There are no mature tools to address multi-dimensional analysis of data coming from both cyber and physical security monitoring. Today attacks are even more sophisticated, and it is known how physical vulnerabilities can be used to open the way for cyber intrusions, and vice-versa. A comprehensive analysis of both dimensions provide knowledge to enrich the context of incidents and to drive new correlation rules, where investigation can be used for fast recovery after detection and for prevention.

Therefore, based on the analysis of airports and the set of scenarios considered from state of the art and from the end-users in the consortium, a common information base will be delivered, describing physical and cybersecurity concepts. The model will be defined by means of ontology, that provides description logics, as an efficient way to express complex knowledge and to provide deductive and inductive reasoning, and that allows interoperability between heterogeneous systems. An Investigation tool will analyse syslog data and rules from the correlation engine and unify the physical security and logical security investigation. It will analyse additional security details, providing contextual and semantic data, to identify causes for security events and threats started by an alert, and feed the correlator with new and/or improved rules. The analytics engine will use hybrid learning to process and analyse multi-dimensional data, across multiple behavioural attributes, and to provide an updated threat intelligence context. The investigation tool will deliver an intelligent dashboard, to present and contextualizes threats and events in an intuitive web application. The dashboard will support SOC in optimizing the analysis of activity and threats timeline, as well as the way to define and/or customize correlation rules in a dynamic way.

k) Impact propagation simulation for anticipated impact assessment

Several models are used for analysing different aspects of systems. There are some models for delay estimation in airport services. It is known that failures in services may influence the functionality of other services. But there is no model, including all relevant services, for ensuring a fast response on cyber-physical incidents.

SATIE impact propagation simulation for anticipated impact assessment is based on a model which aims increasing the understanding of effects of combined cyber-physical attack and includes various aspects of impacts and their possible propagations. The model will be built based on an analysis of the airport services, which contains the dependencies between the

services. This analysis will contain the relevant services, and business processes as well as direct and indirect dependencies between these services and services and business processes. This analysis serves then as input for two types of models: a basic model for fast response and an extended model for a deep analysis and for increasing the preparedness. Based on these models, the understanding of the impact of cyber-physical incidents can be increased.

Once the model will be built, it will be integrated in a software tool. This software tool allows SOC and AOC operators to analyse the impact of cyber, physical and combined attacks and possible propagations of it through different services. This propagation will cover different aspects of the system as economic, cyber, physical and societal ones. The results of the impact propagation assessment can be used for a resilience assessment with cyber, physical, cyber-physical, economic and societal aspect.

l) Cyber-physical incident management portal for enhanced SOC awareness

There are several incident response systems available on the market with a high maturity level. Again, most efficient solutions are owned by large US companies like Splunk (Phantom) or IBM (Resilient). However, these solutions are not oriented towards cyber-physical awareness. They do not take into account geolocation of assets in the building and they do not provide impact assessment for a specific infrastructure. Moreover, their knowledge database is mostly focused on IT oriented systems.

Therefore, an incident management portal will be developed. It will be connected with the vulnerability management system and the correlation engine. From the first, it will get information about network topology and airport assets (type, IP address, Operating Systems, firmware, software versions, etc.). From the latter, it will collect security events in syslog format. Based on the top of a vulnerability intelligence platform, it retrieves the known vulnerabilities on these assets. By providing an overview about critical assets, known vulnerabilities and cyber-physical security events in near real time, it will improve the detection of insiders' attacks and it will reduce the time to respond.

It will also include a web portal that embeds several graphical widgets about forensics investigation and simulation of impact propagation and manages Single-Sign-On authentication. The web portal will also include a graphical framework that allows SOC operators to qualify security incidents and optimize decision making in case of complex scenarios of threat: visualize alerts, look for evidences on the syslog database, analyse airport networks in order to identify vulnerable assets to a specific threat, evaluate potential impacts on airport services in case of failure of a vulnerable asset. By unifying the navigation across the GUIs, the prioritization of the incidents according to the impact level will be improved, and the investigations in reaction to an unknown threat will be easier. Finally, the interconnection with the crisis alerting system will improve the communication between SOC and AOC operators.

m) Crisis alerting system for coordinated security and safety responses

Crisis Management System is quite new in the airport industry and the main available solutions in the market are provided by large US companies. Although most of them are providing some operational picture by integrating airport security and safety systems they do provide smart information sharing capabilities with other agencies, but just some predefined notifications.

The crisis management system performs two main functions. The first one is the generation of the operational picture by combining information from security and safety systems of the airport with information provided by the SOC and the impact propagation module. The second one is the smart notification and alerting service be based on the Emergency Message Content Router (EMCR). It enables information sharing among involved actors at every level of coordination, enabling collaborative response and at the same time can support multichannel alerting of passengers and adjusted possibly affected population with variable content according to their

location. The SATIE crisis management system will provide enhanced situation awareness by integrating information not only from the airport security and safety systems, but also from the EOC and the impact propagation module. In addition, the smart multichannel notification/alerting service will provide a unique capability to enable the proper information to reach the proper responder in due time and at the same time alert the public in the vicinity of the installations through many different communication channels.

EMCR is a software service which enables data messages to be routed according to their header information and in order to support cross platform interoperability, conforms to the Emergency Description Exchange Language (EDXL) of the OASIS standards organization. More specifically the EMCR routes messages conforming to the EDXL-DE (Distribution Element) via specific rules that can be based: on Roles (Role based communication), unique endpoints, geographical areas and even keywords. The payload of an EMCR message can be any format defined in the EDXL family of standards (e.g. CAP, TEP/TEC, RM, and SitRep) or any other well-defined message format. In the frame of SATIE, the EMCR will be further developed in order to support intelligent message content selection according to specific criteria (role, age, location etc.) and also to support various end devices such as social media, public announcement systems, IVR systems to inform fixed telephone users and SMS like messaging through mobile telephony cell broadcast service.

n) Emulation platform for improved cyber defence strategies

Emulation platforms can be used either to test systems before on-site integration, optimize cyber-defence strategies or to train the end-users. The objective is to avoid potential incidents on operational systems. Focusing on cybersecurity topic, this kind of emulation platform is also called CyberRange. CyberRange platforms are often limited to IT environment which is not sufficient to cover airports requirements, whereas ICS and OT systems are widely used. Moreover, CyberRange platforms often remain experimental initiatives which do not reach TRL 7.

The SATIE emulation platform will replicate some parts of the airport information system related to passenger control, baggage handling, air traffic management services and airport operations management. It will be managed by the CyberRange system which provides the capacity to deploy airports assets on a virtual environment through a simple drag and drop, then to perform predefined cyber-attacks on demand. The main challenge is to package and embed new virtual instances, and to connect new hardware components that use specific communication protocols. Specific scenarios of threat exploiting target systems vulnerabilities will be implemented in order to highlight the efficiency of prevention, detection controls, as well as response including investigation and impact assessment.

In addition to all these innovation elements already presented, SATIE will also bring policy improvements. As mentioned in previous sections, there are several regulations in place but more have to be considered. Suitable solutions need to be developed also beyond the application of such regulations. This is needed to adequately protect professionals on duty in these areas as well as non-involved persons like passengers. SATIE will contribute by discussing roles and responsibilities in such a complex area where airport operators, integrators, IT solution providers and first responders are all part of the game. SATIE will also help in the emerging exploration of policy makers and other stakeholders in this field and its results will feed not only trade associations of cPPP but it is also the intention to propose elements to the European Parliament (Committee on Security and Defence, Committee on Terrorism and Committee on Transport and Tourism) and the Commission (DG TRANSPORT, DG HOME, DG CONNECT) to better tackle evolution in regulations for increased/updated security in and around airports.

5 Conclusion

Current report focuses on the identification of cyber-physical security improvements at airports relying on a state-of-the-art analysis of the current security measures applied on air transport infrastructures in the context of SATIE, resulting in the development of a gap analysis upon which the expected improvements from SATIE project are set up.

In this respect, relevant security standards and guidelines in the framework of the SATIE project have been presented, the principles and challenges of crisis management in airports along with their societal impacts have been described and existing solutions deployed in airport infrastructures have been highlighted and analysed in terms of existing ICS/SCADA airport systems and particularly on the Baggage Handling System (BHS).

Hence, in order to identify the security solutions that deal with the SATIE attack scenarios requirements, the methodology “Know, Get in, Find, and Control” of the EBIOS risk analysis approach (which has been already described in the deliverable D2.1 (36) for the identification of critical assets and their vulnerabilities) is adopted to analyse the sub-attacks of the five SATIE demonstration scenarios and produce an exhaustive list of the security solutions used per demonstration airport according to the assets/operations involved. Within this framework, a list of the physical and cybersecurity controls applied in the SATIE airports has been delivered. Additionally, the international, nation-specific and airport- specific measures followed by the demonstration airports in the context of SATIE and the airports crisis management and societal impact in place have been presented.

A brief analysis of the existing standards, guidelines and the security solutions applied on the airports CIs is provided in order to form a holistic view of the airports’ current cyber and physical security environment. The understanding of this environment helped to conduct a gap analysis, which findings were described in detail.

The identified security gaps were used as a basis, to specify the expected improvements from the SATIE project. In particular, twelve key objectives were addressed according to relevant security gaps and fourteen key innovation elements were identified in the context of SATIE that are valued to improve the state-of-the-art by responding to the conceptual, technical, economic and social nature of the identified gaps.

The overall purpose of this deliverable is to formalize knowledge about the current cyber and physical security status on airports and the existing security gaps and challenges, in order to predefine the prerequisites that will support the cyber-physical risk analysis of D2.3 and assist in the development of the security toolkit that will be capable of protecting the critical air transport infrastructures against combined cyber and physical threats.

6 References

1. **ENISA.** *Securing Smart Airports.* [Online] European Union Agency for Network and Information, December 2016. https://www.enisa.europa.eu/publications/securing-smart-airports.
2. **CONCEPTIVITY.** *Cybersecurity standard gap analysis.* s.l. : cyberwatching.eu consortium, 2019.
3. **ISO/IEC, 27001:2013.** *Information technology — Security techniques — Information security management systems — Requirements.* [Online] International Organization for Standardization, 2013. [Cited: 10 21, 2019.] https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en.
4. **ISO, 31000:2018.** *Risk management — Guidelines.* s.l. : International Organization for Standardization (ISO), 2018.
5. **ISO/IEC, 27005:2018.** *Information technology — Security techniques — Information security risk management.* [Online] International Organization for Standardization, 2018. https://www.iso.org/standard/75281.html.
6. **27002:2013, ISO/IEC.** *Information technology — Security techniques — Code of practice for information security controls.* [Online] International Organization for Standardization, 2013. https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en.
7. **27033:2015, ISO/IEC.** *Information technology — Security techniques — Network security.* [Online] International Organization for Standardization, 2015. https://www.iso27001security.com/html/27033.html.
8. **22301:2012, ISO.** *Societal security — Business continuity management systems — Requirements.* [Online] International Organization for Standardization, 2012. https://www.iso.org/standard/50038.html.
9. **CANSO.** *Cyber Security and Risk Assessment Guide.* [Online] Civil Air Navigation Services Organisation, 2014. https://www.canso.org/canso-cyber-security-and-risk-assessment-guide.
10. **ENISA.** *EU NIS Directive 2016/1148.* [Online] ENISA, 2016. https://www.enisa.europa.eu/topics/nis-directive.
11. **ISO, 55001:2014.** *Asset management — Management systems — Requirements.* [Online] International Organization for Standardization, 2014. https://www.iso.org/standard/55089.html.
12. *Crises and Crisis Management: Integration, Interpretation, and Research Development.* **Bundy, J., Pfarrer, M.D., Short, C.E., Coombs, W.T.** s.l. : SAGE, 2017, Journal of Management, Vol. 43(6), pp. 1661–1692.
13. *Governance of occasional multi-sector networks.* **Treuniet, W. et al. (2014).** University Park, Pennsylvania, USA, pp. 118 - 122. : Proceedings of the 11th International ISCRAM Conference.
14. *Unified Incident Command and Decision Support (UICDS): A Department of Homeland Security Initiative in Information Sharing.* **Morentz, J.W., (2008).** s.l. : Proceedings of the Conference on Technologies for Homeland Security, 2008. IEEE. pp. 321 - 326.
15. *Towards a Pan-European Information Space.* **Huebner et al., (2015).** Proceedings of the ISCRAM 2015 Conference : Kristiansand, Palen, Büscher, Comes & Hughes.
16. **Fraunhofer, (2015).** IDIRA Interoperability of data and procedures in large-scale multinational disaster response actions. *Final report.* [Online] [Cited: 6 08, 2015.] http://www.idira.eu/.
17. *Developing a Framework of Common Information Space (CIS): Grounded Theory Analysis of Airport CIS, in Collaboration and Technology.* **Selvaraj, N. and Fields, B (2010).** s.l. : Berlin Heidelberg, Springer,, 2010. pp. 281-296.
18. **EACCC, (2019).** *European Aviation Crisis Coordination Cell.* [Online] European Commission. [Cited: 9 24, 2019.] https://ec.europa.eu/transport/modes/air%20/.
19. *The Hidden Cost of Airline Unpunctuality.* **Cook, A., et al (2012).** s.l. : Journal of Transport Economics and Policy, Vol. 46(2), pp. 157-173.

20. **Schulz, Eric.** [Online] 2019. [Cited: 9 18, 2019.] https://www.airbus.com/content /dam/corporate-topics/publications/media-day/Presentation-Eric-Schulz-GMF-2018.pdf.
21. *Aviation Cyber–Physical Systems: Foundations for Future Aircraft and Air Transport.* **Poovendran, K. Sampigethaya and R.** s.l. : Proc. IEEE, Aug. 2013. vol. 101, no. 8, pp. 1834–1855.
22. **Falvo, M.C., Santi, F., Acri, E., Manzan, E., (2015).** *Sustainable airports and NZEB: The real case of Rome International Airport.* [Online] [Cited: 8 11, 2019.] https://ieeexplore.ieee.org/abstract/document/7165392.
23. *Extending the airport boundary: Connecting physical security and cybersecurity.* **Willemsen, Bert and Cadee, Menno, (2018).** s.l. : Henry Stewart Publications, Journal of Airport Management, Vol. 12(3), pp. 236-247.
24. **K. Stouffer, S. Lightman, V. Pillitteri, M. Abrams, and A. Hahn.** *Guide to Industrial Control Systems (ICS) Security.* NIST Special Publication (SP) 800-82 Rev. 2, Jun. 2015 : National Institute of Standards and Technology (NIST).
25. *Now That's Smart!* **Vyatkin, Valeriy, et al.** s.l. : IEEE Industrial Electronics Magazine, 2007, Vol. 1(4), pp. 17-29.
26. *Formal methods in PLC programming.* **Litz, G., Frey, L. (2000).** s.l. : in Smc 2000 conference proceedings ieee international conference on systems, man and cybernetics "cybernetics evolving to systems, humans, organizations, and their complex interactions". cat. no.0, 2000, vol. 4, pp. 2431–2436..
27. *Introduction to Industrial Control Networks.* **Hancke, B. Galloway and G. P., (2013).** s.l. : IEEE Commun. Surv. Tutor, Vol. 15(2) (Second 2013). pp. 860–880.
28. **DLR, Institute of Flight Guidance.** *A-HMI Advanced Human Machine Interface.* [Online] DLR Institute of Flight Guidance. https://www.dlr.de/fl/en/desktopdefault.aspx/tabid-1127/1591_read-3003/.
29. *OPERATIONAL CONCEPT FOR AN AIRPORT OPERATIONS CENTER TO ENABLE TOTAL AIRPORT MANAGEMENT.* **G. Spies, F. Piekert, A. Marsden, R. Suikat, C. Meier, and P. Eriksen, (2008).** s.l. : 26th International Congress of the Aeronautical Sciences. pp. 1-10.
30. *Providing SCADA network data sets for intrusion detection research.* **Fernandez, A., Lemay J. M., (2016).** s.l. : th Workshop on Cyber Security Experimentation and Test ({CSET} 16). p.8.
31. **Solutions, Airport SCADA.** *VTScada.* [Online] Trihedral's airport solutions. [Cited: 10 21, 2019.] https://www.vtscada.com/airport-solutions-overview/.
32. **S.p.A., Leonardo.** *Air Traffic Centres Increased automation & interoperability.* [Online] Leonardo S.p.A. [Cited: 8 11, 2019.] https://www.leonardocompany.com/en/land/air-traffic-control/air-traffic-centers.
33. **Systems, Integral.** *System of operating baggage handling complex IS-ABHS.* [Online] Integral Systems. [Cited: 8 11, 2019.] https://integral.lv/products/baggage_handling/bhs-control/.
34. **Limited., Glidepath.** *GlideView.* [Online] Glidepath Limited. [Cited: 8 11, 2019.] https://glidepathgroup.com/pages/bhs-glideview.
35. **LA MÉTHODE EBIOS RISK MANAGER.** LA MÉTHODE EBIOS RISK MANAGER. [Online] https://www.ssi.gouv.fr/administration/management-du-risque/la-methode-ebios-risk-manager/.
36. **SATIE project, (2019).** *D2.1 - Critical Systems and Vulnerabilities.*
37. **Organization, International Civil Aviation.** [Online] April 2017. https://www.icao.int/Security/SFP/Pages/Annex17.aspx.
38. **International Civil Aviation Organization, (ICAO).** *Annex9.* [Online] https://www.icao.int/Security/FAL/ANNEX9/Pages/default.aspx.
39. **Commission Regulation (EU), 2015/1998.** [Online] November 5, 2015. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02015R1998-20190201&from=EN.
40. **62443, ISA/IEC.** *security capabilities for control system components.* [Online] 2018. https://www.isa.org/intech/201810standards.
41. **2016/1148, DIRECTIVE (EU).** *Concerning measures for a high common level of security of network and information systems across the Union.* [Online] July 6, 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

42. **Ente Nazionale per l'Aviazione Civile Italian Civil Aviation Authority, (ENAC).** *Advisory Circular APT 18th.* [Online] 1 30, 2008. https://www.enac.gov.it/sites/default/files/allegati/2018-Mag/APT_18A.pdf.
43. **International Civil Aviation Organization, (ICAO).** *Annex 14 - to the Convention on International Civil Aviation, Aerodromes - Aerodrome Design and Operations.* [Online] Vol.1, 2009. https://www.icao.int/APAC/Meetings/2016%20ICAOPIS/3%20ICAO%20Annex%2014%20Standards%20and%20Aerodrome%20Certification.pdf.
44. **Official Journal of the European Union L. 44 of 14 February, (2014).** *COMMISSION REGULATION (EU) No 139/2014.* [Online] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0139&from=EN.
45. **Bowen, Ronda.** *Learn About Gap Analysis Methods: Which Are the Best?* [Online] Bright Hub PM, 08 22, 2019. https://www.brighthubpm.com/methods-strategies/75624-different-ways-to-approach-a-gap-analysis/.
46. *CYBER SECURITY FOR AIRPORTS.* **Gopalakrishnan, Kasthurirangan & Govindarasu, Manimaran & Jacobson, Douglas & M. Phares, Brent.** 2013, INTERNATIONAL JOURNAL FOR TRAFFIC AND TRANSPORT ENGINEERING, pp. 365-376.
47. *CYBER RESILIENCE IN THE SWIM CONCEPT.* **Civil Air Navigation Services Organisation, (CANSO).** Montréal, Canada : International Civil Aviation Organization, 2018. 13th Air Navigation Conference . pp. 1-4.
48. **Strohmeier, Martin, (2016).** *Security in Next Generation Air TrafficCommunication Networks.* Trinity : Phd Thesis, University of Oxford.
49. *Mission-critical Communications - Let's connect.* **ABB, (2019).** AIR TRAFFIC MANAGEMENT & AIRPORT COMMUNICATIONS.
50. **Wueest, Candid.** Airport boarding gate display leaks booking codes, puts passenger data at risk. *Symantec Official Blog.* [Online] 08 22, 2019. https://www.symantec.com/connect/blogs/airport-boarding-gate-display-leaks-booking-codes-puts-passenger-data-risk.
51. *Detecting Bombs in X-Ray Images of Hold Baggage: 2D Versus 3D Imaging.* **N. Hättenschwiler, M. Mendes, and A. Schwaninger, (2019).** s.l. : Human Factors, Vol. 61(2). pp. 305–321.
52. **ISO/IEC, 27001:2017.** [Online] Information Security Management System Auditing Guideline, 8 2, 2017. https://www.bsigroup.com/en-GB/iso-27001-information-security/BS-EN-ISO-IEC-27001-2017/.
53. **ISO, 9001:2015.** *Clause 7.5.3. Control of documented Information.* [Online] http://9001quality.com/7-5-3-control-documented-information/.