



Security of Air Transport Infrastructures of Europe

D7.3 – Best practices for updating airport security standard and policies

Deliverable Number	D7.3
Author(s)	AIA, SEA, ZAG, KEMEA, DLR, DGS, ALS, ERI, INOV, IDE
Due/delivered Date	M30/2021-11-01
Reviewed by	ACS, KEMEA, DLR
Dissemination Level	PU
Version of template	1.083

Start Date of Project: 2019-05-01

Duration: 30 months

Grant agreement: 832969



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 832969

DISCLAIMER

Although the SATIE consortium members endeavour to deliver appropriate quality to the work in question, no guarantee can be given on the correctness or completeness of the content of this document and neither the European Commission, nor the SATIE consortium members are responsible or may be held accountable for inaccuracies or omissions or any direct, indirect, special, consequential or other losses or damages of any kind arising out of the reliance upon the content of this work.

The information and views set out in this report are those of the author(s) and do not necessarily reflect the official opinion of the European Union. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein. All intellectual property rights are owned by the SATIE consortium members and are protected by the applicable laws. Except where otherwise specified, all document contents are: “©SATIE Project - All rights reserved”. Reproduction is not authorised without prior written agreement.

Document contributors

No.	Name	Role (content contributor / reviewer / other)
1	Nikolaos Papagiannopoulos (AIA)	Content contributor
2	Eleni Maria Kalogeraki (AIA)	Content contributor
3	Tim Stelkens-Kobsch (DLR)	Content contributor
4	Nils Carstengerdes (DLR)	Content contributor
5	Angelo D’Andrea (SEA)	Content contributor
6	Elena Branchini (SEA)	Content contributor
7	Eftichia Georgiou (KEMEA)	Content contributor
8	Ilias Gkotsis (KEMEA)	Content contributor
9	Vasiliki Mantzana (KEMEA)	Content contributor
10	Kelly Burke (DGS)	Content contributor
11	Matteo Mangini (DGS)	Content contributor
12	Sebastien Clavert (IDE)	Content contributor
13	Thomas Mauger (IDE)	Content contributor
14	Kantharuban Samoogabalan (IDE)	Content contributor
15	Sven Hrastnik (ZAG)	Content contributor
16	Filipe Apolinário (INOV)	Content contributor
17	Éric Herve (ALS)	Content contributor
18	David Lancelin (ACS)	Technical Review
19	Vasileios Kazoukas (KEMEA)	Security Review

No.	Name	Role (content contributor / reviewer / other)
20	Meilin Schaper (DLR)	Quality Review
21	Andrei-Vlad Predescu (DLR)	Review

Document revisions

Revision	Date	Comment	Author
V0.01	2020-12-18	Initial draft	Nikolaos Papagiannopoulos
V0.02	2021-03-17	Content added to section 2.1.2	Kelly Burke
V0.03	2021-05-01	Content added to section 2.2	Sven Hrastnik
V0.04	2021-05-10	Content added to section 2.2	Filipe Apolinário
V0.04	2021-05-10	Content added to section 2.2	Éric Herve
V0.05	2021-05-10	Content added to section 2.4 and to the List of Acronyms	Eleni Maria Kalogeraki
V0.06	2021-05-17	Content added to section 2.4 and to the List of Acronyms.	Eleni Maria Kalogeraki
V0.07	2021-05-17	Content added to section 2.3 and list of the Acronyms	Angelo D'Andrea Elena Branchini
V0.08	2021-05-30	Content of D7.3 moved to the newest template of deliverables	Eleni Maria Kalogeraki
V0.09	2021-06-01	Address comments in sections 2.4 and 2.6	Vasiliki Mantzana
V0.10	2021-06-04	Review and comments	Meilin Schaper
V0.10	2021-06-17	Content added to section 2.2	Filipe Apolinário
V0.10	2021-06-21	Address comments in section 2.3.1	Elena Branchini, Angelo D'Andrea
V0.11	2021-06-28	Add content to section 2.3.2	Elena Branchini Angelo D'Andrea
V0.12	2021-06-29	Address comments in section 2.2	Sven Hrastnik
V0.12	2021-06-29	Address comments in section 2.4.2	Clavert Sebastien
V0.12	2021-06-29	Address comments in section 2.4.3	Thomas Mauger
V0.12	2021-06-29	Address comments in section 2.6	Eftichia Georgiou
V0.12	2021-06-29	Integrate content to chapter 2	Eleni Maria Kalogeraki

Revision	Date	Comment	Author
V0.13	2021-07-06	Content added in chapter 2, acronyms added in the list of acronyms	Eleni Maria Kalogeraki
V0.14	2021-07-07	Clean version prepared for review process	Eleni Maria Kalogeraki
V0.14	2021-07-08	Technical check and approval for sending the created report to standardization bodies	David Lancelin, Technical Manager
V0.14	2021-07-09	Security check and approval for sending the created report to standardization bodies	Vasileios Kazoukas, Project Security Officer
V0.14	2021-07-13	Quality check and approval for sending the created report to standardization bodies	Meilin Schaper, Quality Manager
V0.15	2021-10-06	Content added to sections 3.2.2 and 3.3.2	Eftichia Georgiou
V0.15	2021-10-07	Content added to sections 3.2.2 and 3.3.2	Sven Hrastnik
V0.16	2021-10-18	Comments added and corrections/improvements made in section 2 according to the feedback received from standardization bodies and policy makers.	Eleni Maria Kalogeraki
V0.17	2021-10-19	Corrections and amendments added a in section 2.5 to address the feedback gained from standardization bodies and policy makers	Tim Stelkens-Kobsch
V0.17	2021-10-20	Added section 3.3.2.3 – Satie Practitioner’s Workshop – MXP	Elena Branchini, Angelo D’Andrea, Marco Albertario, Biagio Tarantino
V0.17	2021-10-21	Corrections and amendments added in section 2.4.2.1 and 2.4.2.2 to address the comments received from standardization bodies and policy makers	Sebastien Clavert, Kantharuban Samoogabalan
V0.17	2021-10-22	Content added to sections 3.3.1 and 3.3.3	Eleni Maria Kalogeraki
V0.17	2021-10-22	Corrections and amendments added in section 2.4 and 2.6 to address the comments received from standardization bodies and policy makers	Eftichia Georgiou
V0.17	2021-10-23	Corrections and amendments added a in section 2.1 and 2.3 to address the feedback gained from standardization bodies and policy makers	Matteo Mangini
V0.17	2021-10-24	Corrections and amendments added in section 2.2 to address the comments	Filipo Apolinario

Revision	Date	Comment	Author
		received from standardization bodies and policy makers	
V0.17	2021-10-24	Corrections and amendments added in section 2.2 to address the comments received from standardization bodies and policy makers	Sven Hrastnik
V0.18	2021-10-25	Content added to section 3.2.1, section 3.2.2 and Annexes	Eleni Maria Kalogeraki
V0.19	2021-10-25	Content added to section 2.2	Éric Herve
V0.19	2021-10-25	Modifications made in section 3.3.2.3, Content added in the Annexes	Elena Branchini
V0.20	2021-10-26	Content added to section 1, section 4 and section 5. Last modifications made in the entire document and formatting issues fixed. Clean version prepared ready for review.	Eleni Maria Kalogeraki
V0.21	2021-10-27	Review	Andrei-Vlad Predescu
V0.21	2021-11-01	Final security check and approval for submission	Vasileios Kazoukas, Project Security Officer
V1.0	2021-11-01	Final quality check and approval for submission	Meilin Schaper, Quality Manager

Executive summary

The current deliverable reflects the outcome of T7.3. Its ultimate purpose is to report on best practices and recommendations for updating airport security standards and policies, as a result of the lessons learnt from the SATIE outcomes and as a consequence of the knowledge gained from open communication channels established between the SATIE consortium and standardization bodies, policy makers or other relevant external groups of aviation security. On top of that, D7.3 aims to present all other activities related to standardisation and interactions with airport stakeholders and practitioners of the three SATIE airport demonstrators (AIA, ZAG, SEA), undertaken to refine the impact of the SATIE Solution towards their internal existing security environment. Evaluation results on the SATIE findings derived from these procedures are herein reported as well.

This deliverable is aligned with the outcome of T2.3 regarding the harmonization of processes and approaches to build a holistic security management cycle. Moreover, it is related to T7.2 in terms of using its results (D7.2 - Training Handbook (1)) to train security practitioners that fostered the adoption of the SATIE results, upon which the SATIE best practices have been developed.

Table of Content

1	Introduction.....	14
1.1	Scope of the deliverable	14
1.2	Work packages and tasks related to the deliverable.....	15
2	Airport security: Recommendations, best practices and lessons learnt from SATIE	16
2.1	Guidance for airports - Novel cyber-physical risk assessment.....	16
2.1.1	Novel cyber-physical risk assessment methodology related to airport security	16
2.1.2	Updated cyber-physical risk analysis with defensive strategies	18
2.2	Best practices - Improving the cyber-physical security of the Baggage Handling System ..	22
2.2.1	BHS security regulations.....	22
2.2.2	Industrial Control System best practices.....	23
2.2.3	Recommendations for handling cyber-physical threats.....	24
2.3	Best practices - Improving the cyber-physical security of the Airport Operations Centre ..	25
2.3.1	Improving AOC practices in general.....	25
2.3.2	Improving AOC practices based on what has been learned in SATIE	27
2.4	Best practices - Improving anomaly detection on cyber-physical threats including passenger data	28
2.4.1	Recommendations of anomaly detection technological improvements on passenger data protection	29
2.4.2	Recommendations for airports employees biometric access control deployment	30
2.5	Best practices - Security of the digital services and voice communication systems of air traffic management services	31
2.6	Best practices - Airport crisis management and decision support.....	34
2.6.1	Operation and security regulatory framework.....	34
2.6.2	Physical and cybersecurity measures and security operation centres.....	35
2.6.3	Crisis management process and involved stakeholders.....	39
2.6.4	CIs security management gaps and best practices	41
2.6.5	Proposed holistic crisis management process	42
3	Standardization activities	45
3.1	Survey strategy and setup.....	45
3.2	Participation to standardization activities and workshops.....	45
3.2.1	SATIE's Awareness Events with stakeholders	46
3.2.2	Organization of the SATIE Practitioners' Workshop.....	47
3.3	Evaluation feedback.....	50
3.3.1	Evaluation results of the SATIE Practitioners' Workshop	50
3.3.2	Evaluation results gained from the national sessions of the SATIE Practitioners' Workshop	57

3.3.3	Feedback gained from standardization bodies.....	60
4	Conclusion	64
5	References	65
6	Annexes	68
	Annex 1 – Current regulatory framework and standards related to anomaly detection on cyber-physical threats, including passenger data	68
	Annex 2 – Evaluation questionnaire of Security Practitioners’ Workshop.....	73
	Annex 3 – Questionnaire for round table discussions of Security Practitioners’ Workshop	82
	Annex 4 – State-of-the-art in Italian cybersecurity rules and regulations.....	85

List of Figures

Figure 2.1: Common and holistic security and safety agenda.....	44
Figure 3.1: Screenshot from the SATIE Awareness Event	47
Figure 3.2: Screenshot from the joint session of SATIE Practitioners’ Workshop	48
Figure 3.3: Screenshot during a demonstrator’s national breakout session of the SATIE Practitioners’ Workshop	49
Figure 3.4: National Cyber Security Perimeter and fulfilments required by the Prime Ministerial Decree n. 81/2021 - security measures	58
Figure 6.1: Cybersecurity regulatory evolution	86
Figure 6.2: Provisions related to the Law Decree 105/2019 currently in force and upcoming Decrees implementing the Law Decree no. 105/2019.....	87

List of Tables

Table 2.1: Security standards for digital services and voice communication systems in ATM	32
Table 2.2: Best practices for airport physical security measures and technology solutions	37
Table 3.1: Results of the responders to questions related to actions considered necessary to enhance the resilience of airports and CIs	51
Table 3.2: Endorsements by the responders on the SATIE IEs	51
Table 3.3: Additional endorsements by the responders on the SATIE Solution.....	52
Table 3.4: Evaluation questionnaire statements overview	54
Table 3.5: Standardization bodies/policy makers list reviewed the SATIE report.....	60
Table 3.6: Feedback obtained from standardization bodies/policy makers for SATIE “Best Practices and Recommendations” on airports security standards and policies	61
Table 6.1: Additional biometric standards	72

List of Acronyms

Acronym	Definition
AACS	Automated Access Control System
AAIASB	Aviation Safety Board
ABC	Automated Border Control
ADO	Airport Duty Officer
ADPR	Anomaly Detection on Passenger Records
AI	Artificial Intelligence
ALCAD	Application Layer Cyber Attack Detection
ANSP	Air Navigation Service Provider
AOC	Airport Operation Centre
AODB	Airport Operations Database
API	Advanced Passenger Information
API	Application Programming Interface
ATC	Air Traffic Control
ATM	Air Traffic Management
BHS	Baggage Handling System
BIA	Business Impact Assessment
BIR	Biometric Information Record
BoD	Board of Directors
BP-IDS	Business Process Intrusion Detection System
CAA	Civil Aviation Authority
CAS	Crisis Alerting System
CBEFF	Common Biometric Exchange Formats Framework
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CIRA	Centro Italiano Ricerche Aerospaziali
CISR	Comitato interministeriale per la sicurezza della Repubblica (Interministerial Committee for the Security of the Republic)
CMC	Crisis Management Centre

Acronym	Definition
CMT	Crisis Management Team
CSDP	Common Security and Defense Policy
CSIRT	Computer Security Incident Response Team
C-UAS	Counter Unmanned Aircraft Systems
CVE	Common Vulnerabilities and Exposures
DCS	Departure Control System
DFS	Deutsche Flugsicherung
DG-CNECT	Directorate-General of the European Commission for Communications Networks
DG-HOME	The Directorate-General of the European Commission for Migration and Home Affairs
DIS	Dipartimento delle informazioni per la sicurezza (Security Intelligence Department)
DMZ	Demilitarized Zone
DPO	Data Protection Officer
EASA	The European Union Aviation Safety Agency
ECI	European Critical Infrastructure
EDA	European Defence Agency
EDS	Explosive Detection System
eMRTD	Electronic Machine Readable Travel Document
EOC	Emergency Operations Centre
EOT	Emergency Operations Team
EPCIP	European Programme for Critical Infrastructure Protection
ETD	Explosive Trace Detection
EU	European Union
EUROCONTROL	European Organisation for the Safety of Air Navigation
FIR	Flight Information Regions
GLPI	Gestion Libre de Parc Informatique
HHMTD	Hand-Held Metal Detection
HMI	Human Machine Interface
HSOC	Holistic Security Operation Centre
iAPI	interactive Advance Passenger Information

Acronym	Definition
IATA	International Air Transport Association
ICAO	International Civil Aviation Organization
ICS	Industrial Control System
ICT	Information Communication Technology
IDS	Intrusion Detection Software
IE	Innovation Element
IMP	Incident Management Portal
IPS	Impact Propagation Simulation
ISA	International Society of Automation
ISMS	Information Security Management Systems
IT	Information Technology
JTC	Joint Technical Committee
KEMEA	Center for Security Studies
LEA	Law Enforcement Agency
LDS	Logical Data Structure
MDR	Managed Detection and Response
MFA	Multifactor Authentication
MROTD	Machine Readable Official Travel Documents
MRP	Machine Readable Passport
MRTD	Machine Readable Travel Document
MRV	Machine Readable Visa
MRZ	Machine Readable Zone
NCSA	National Cyber Security Authority
NDR	Network Detection and Response
NG SIEM	Next Generation Security Information Event Management
NIS	Network and Information Security Directive
NIST	National Institute of Standards and Technology
OCR	Optical Character Recognition
OSDP	Open Supervised Device Protocol
OT	Operational Technology

Acronym	Definition
PAD	Presentation Attack Detection
PLC	Programmable Logic Controller
PNR	Passenger Name Record
PNRR	Piano Nazionale di Ripresa e Resilienza (National Recovery and Resilience Plan)
QSN	Quadro Strategico Nazionale (National Strategic Framework)
RIS	Risk Integrated Service
SARPs	Standards and Recommended Practices
SCADA	Supervisory Control and Data Acquisition
SES	Single European Sky
SMS-I	Investigation Tool
SOAR	Security Orchestration Automation Response
SOC	Security Operation Centre
SPI	Service Provider Interface
SWAL	Software Assurance Levels
TIP	Threat Intelligence Platforms
TLS	Transport Layer Security
TraMICS	Traffic Management Intrusion and Compliance System
UEBA	User Entity Behaviour Analytics
VIP	Vulnerability Intelligence Platform
WCO	Worlds Customs Organisation
WTMD	Walk-Through Metal Detection

1 Introduction

1.1 Scope of the deliverable

This deliverable resides in Work Package 7 (WP7), “Exploitation and Dissemination” and it is the result of the activities carried out in task 7.3 (T7.3) “Best practices for updating airport security standards and policies”.

The aim of this task is to produce and propose best practices and provide recommendations and guidelines that will facilitate airports and their stakeholders to update their security policies in terms of maintaining a secure environment of their Critical Infrastructures (CIs) (ensuring the secure design and operation of the existing and future airport IT/control systems infrastructure). In this respect, the current task is focused on the thorough analysis of the existing security standards and good practices related to airport security towards the scrutiny of the security specificities of airport CIs, i.e. Operational Technology (OT) systems, Air Traffic Management (ATM) systems, etc., to identify open security issues, current challenges and unbridged security gaps. Taken into account the SATIE results and the experience obtained from the lessons learnt within the project lifespan along with the continuous and strong collaboration with SATIE airport demonstrators (AIA, ZAG, SEA) to ascertain that all technical and operational domain-specific processes are captured, the current deliverable aims at developing recommendations related to:

- Cyber-Physical Risk Analysis and Risk Assessment (Section 2.1)
- Cyber-Physical Security of Baggage Handling System (BHS) (Section 2.2)
- Cyber-Physical Security of Airport Operations Centre (AOC) (Section 2.3)
- Anomaly Detection of Cyber-Physical Threats (including topics on passenger data) (Section 2.4)
- Security of Digital Services and Voice Communication Systems of ATM services (Section 2.5)
- Crisis Management and Decision Support (Section 2.6)

In addition, this task activities promote the establishment of relationship between the SATIE consortium and standardisation bodies that has a twofold purpose:

- i) to provide proposals and recommendations to the standardization bodies that could be fruitful for future actions and policy developments;
- ii) to retrieve feedback and comments that may be gained from the standardization bodies and policy makers recipients relevant knowledge and experience for improving the SATIE proposed recommendations on updating airport security standards and policies.

In order to retrieve feedback from the standardisation bodies, policy makers and other relevant airport stakeholders that will be utilized to improve the SATIE proposed best practices, a survey strategy was conducted (Section 3.1). The strategy underlined the development of a report of the SATIE proposed recommendations which was communicated to standardisation bodies and a considerable number of them responded providing valuable comments (Section 3.3) for potential enhancements and future improvements and supported strongly the SATIE effort which were taken into consideration in the final update of this deliverable.

Moreover, another goal of this survey strategy was to gather additional input from airport stakeholders to refine the impact of SATIE in relation to their internal policies, investigate whether the SATIE Solution can be used to leverage their policies and identify areas of interest for improving security. To accomplish this, a security practitioners’ workshop was conducted (section 3.2.2) which

aimed at retrieving such feedback from the three airport demonstrators stakeholders (e.g. first responders). The delivered feedback was further analysed and reported in this final version of D7.3.

Eventually, the current document aims to report additional activities related to standardisation and project's dissemination. In the context of T7.3, a second SATIE awareness event was conducted to promote the SATIE outcomes on airport stakeholders which is presented in this deliverable (section 3.2.1).

Due to COVID-19 related issues, both the SATIE Practitioners' Event and the SATIE Awareness Event were performed virtually.

1.2 Work packages and tasks related to the deliverable

This deliverable is supported by the activities of T2.3 of WP2 "Cyber-physical risk assessment and airports' requirements" as the harmonization of processes and approaches tailored to develop a holistic security management cycle.

Furthermore, the deliverable is related to T7.2 "Training materials for the airport security practitioners", as the training material produced from this task was used to train end-users who had a key-role for the adoption of the SATIE results, which served as a basis to generate the current best practices of SATIE.

2 Airport security: Recommendations, best practices and lessons learnt from SATIE

The scope of this section is to provide best practices and recommendations for the security of airports' critical infrastructures and aviation systems taking into account our experience from the SATIE project. In particular, several recommendations and lessons learnt from the Airport Operations Centre side will be provided.

2.1 Guidance for airports - Novel cyber-physical risk assessment

Among the most important guides that can be provided to airports with a view to improving their security and safety parameters, SATIE proposes an innovative methodology for conducting risk assessments.

2.1.1 Novel cyber-physical risk assessment methodology related to airport security

A novel cyber-physical risk assessment method was developed throughout the course of this project (see SATIE "D7.9 - Cyber-physical risk analysis" (2)) to best address the needs of the airport end-users. There were multiple crucial aspects that needed to be addressed to create an innovative approach: both physical and cyber threats needed to be included, the safety and security risks to human lives needed to go into the calculations of risk and new threats and new vulnerabilities specific to the airport environment needed to be included. These reconfigurations were addressed thoroughly in D7.9 (2), which focused on the cyber-physical risk assessment methodology and results. However, a summary has been included in the following subsections.

2.1.1.1 Asset inventory and asset criticality evaluation

In order to accommodate some of the unique assets found in an airport environment not covered by off-the-shelf risk assessments normally, new asset classes were created such as police officers, large equipment (e.g. conveyor belts), and airplanes among others. In this way, all relevant assets could be represented and included in the analysis.

More significantly, the way in which asset criticality is evaluated was reconfigured. The default approach is to use confidentiality, integrity or availability (CIA). This CIA triad is typically used in the IT-world; however, it partially addresses human assets and for this reason also the safety and security aspects of the impact have been introduced in the evaluation. Because one of the major aims of the SATIE project is to protect human life, when performing a risk assessment process, the criticality of personnel and passengers need to be accurately evaluated with respect to all the threats which may affect the entire airport environment. Therefore, a new business category and asset category were created, related to safety and security to human life so that all assets could be evaluated according to their impacts on the safety and security to humans (not just business operations), and human assets could be evaluated according to if their safety and security were lost (not just CIA). By including both of these, the criticality of all assets could properly be evaluated as well as their impacts on the airport.

2.1.1.2 Cyber and physical threats specific to the airport

RIS was already well-adapted for both cyber and physical threats; however, some threats specific to the airport environment were added to the Threat Catalogue used by the solution. This included threats such as hijacking, compromised personnel with high security clearance and a vehicle-ramming attack to name a few. These threats were associated with newly-included vulnerabilities as well. This means different kind of vulnerabilities, from the corruption of an employee, to an inadequate number of personnel at security-controlled areas, until an insufficient monitoring of the litter bins, just to name

a few examples. By adding these airport-specific threats and vulnerabilities, a broad and structured risk assessment could be performed.

2.1.1.3 Security measures

Through the security measures' evaluation, RIS allows to identify the relevant ones for the scope of the assessment (e.g. in a typical IT environment, ISO 27002 would be included), and then questions are submitted to a group of referents to evaluate how well those measures are being enforced in each operation of the organization. With this approach, RIS is thus flexible and able to include security measures tailored on the scope of the assessment, analysing both cyber and physical aspects. This allowed the end-users in this project to identify the relevant security measures that all airports must abide by. In this way, the identification of the level of application of the security controls allows an assessment of the vulnerabilities that may derive from a lack or poor application of the airport-pertinent security measures envisaged.

Together with the end-users, it was decided to include a list of regulations and standards in the risk assessment:

- ISO/IEC 27002:2013 (3): This standard was created by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) to create a best practice framework for Information Security Management Systems (ISMS), reducing information security and data protection risks to organizations. This standard contains a long annex with all of the controls and objectives covering human resources, access control, operations security, supplier relationships, asset management, information security policies, and compliance, among others;
- Convention on International Civil Aviation (ICAO), standards and recommended practices, Annex 9, Annex 17: ICAO was created to be in charge of the principles and techniques of international air navigation. The ICAO annexes - Annex 9, Annex 17, Annex 17 update – cover facilitation of entry and departure of people and baggage, security against unlawful interference from unauthorized people, vehicles or cargo, and detailed measures on aviation cybersecurity. By including these standards, the risk assessment covers the security measures and standards applicable in the airport environment, which are relevant for the SATIE threat scenarios, and in particular covering physical aspects specific to airports. The compliance to these standards ensures the observance of airport-specific requirements which off-the-shelf risk assessment methods cannot cover;
- Agence nationale de la sécurité des systèmes d'information (ANSSI), REGULATION (EC) No 300/2008, Annex: Common basic standards for safeguarding civil aviation against acts of unlawful interference. As part of the NIS Directive (4), the ANSSI created a Directive with 23 specific laws, covering the governance of the security, protection and defence of information systems as well as their resilience. These standards ensure proper coverage of current cybersecurity laws in airports, particularly as cybersecurity is a key aspect of the project.

Overall, this resulted in a risk assessment which was configured specifically to address airport security by including airport-specific assets with their airport-specific threats and vulnerabilities. The assets criticalities were identified by taking into consideration also impacts to human life, and by measuring risks according to airport-relevant security measures. This represented the basis for directing possible actions in terms of security policies, procedures and controls in order to improve the overall level of security of the organization.

2.1.2 Updated cyber-physical risk analysis with defensive strategies

Given that the project involves airports as critical infrastructures, this means that they are considered an essential asset for society, and for the economy to function. As the name implies, it is critical that they function properly, but it is of utmost importance that they operate safely. The air transport world handles billions of passengers a year on average, passing through airports worldwide, whose lives are in the hands of the air transport industry. This means maintaining the safety and security of airports has huge ramifications beyond the doors of an individual airport.

The first step to improve the safety and security within an airport is to understand the current situation, which should be done through an exhaustive cyber and physical risk analysis.

Often, standard risk analyses in organizations concentrate on IT aspects (e.g. through ISO 27001 certification); however, for an airport the physical threats are just as crucial as cyber threats, and similarly, protecting physical assets are just as important as cyber assets. Therefore, when selecting which type of risk analysis to perform, critical infrastructures like airports should choose one which can handle both cyber and physical aspects (applicable to assets, threats and vulnerabilities). There are various methodologies to risk assessment and given that airports are systems of systems, often with very complex infrastructure and governance, it is highly recommended to use a risk analysis which can handle subdivisions of operations (e.g. check-in, baggage handling system, airport operation center, third-party personnel management), because they are often managed separately or according to different regulations. Overall, the risk analysis should evaluate threats arising from both intentional acts (e.g. man-in-the-middle attack, tailgating through access control) as well as unintentional (e.g. maintenance error, lightning strike).

Risk analyses offer airports a thorough understanding of where the greatest risks lie within the organization, to better understand where more concerted efforts and funds should be directed to reduce exposure to vulnerabilities. The first major recommendation to defend against the threats is to implement and require a regularly-scheduled (e.g. annual) risk assessment. Nevertheless, it is extremely important that the risk reassessment process is also triggered by events deemed relevant in terms of impact on the security and safety of the organization (e.g. system changes, change to regulations, post-incident). In this way, any changes in adopted security measures or changes in management over time can be understood from a security point-of-view to understand the implications and any improvements made.

Regulations and security measures in place are what ultimately can reduce the risks. There are binding pieces of legislation, which are mandatory for all European airports, whereas there is a group of recommendations. While these were elaborated on in D2.4 and D7.7 (5) (public version of D2.4), a brief list of the cybersecurity and physical security regulations, relevant standards and practices (both recommended and binding) is included below.

Cybersecurity related standards and best practices:

- Security Smart Airports (report published by ENISA);
- NIST framework for improving Critical Infrastructure CyberSecurity;
- ISO/IEC 27001:2013 Information Technology;
- ISO 31000:2018 Risk management – Guidelines;
- ISO/IEC 27005:2018 Information technology, security techniques, information security risk management;
- ISO/IEC 27002:2013 Information technology, security techniques, code of practice for information security controls.

Cybersecurity related regulations:

- EU NIS Directive 2016, EU NIS 2 Directive (6) under review proposal of 16.12.2020).

Physical security related regulations, standards, best practices and recommendations:

- ICAO Annex 17 “Security”;
- ICAO Annex 9 “Facilitation”;
- ICAO Annex 10 “Aeronautical Telecommunications”;
- ICAO Annex 11 “Air Traffic Services”;
- ICAO Annex 14 “Aerodromes”;
- ICAO Annex 18 “The Safe Transport of Dangerous Goods by Air”;
- European Commission Implementing Regulation on Aviation Security (EU) 2019/1583 (7);
- EU Regulation 300/2008 Annex: Common basic standards for safeguarding civil aviation against acts of unlawful interference;
- National Civil Aviation Security Regulation and Security Technical Directives;
- National Civil Aviation Training Program;
- National Civil Aviation Security Audits and Inspections;
- Airport Security Program.

2.1.2.1 Improving physical security

Because there is a long history of airports being targets of physical attacks, physical security measures have had to be developed from the beginning. However, as attackers become more innovative with cyber-attacks, they also have become more creative in physical attacks. Therefore, airports also need to improve measures in physical security and threat prevention. The aviation industry takes airport safety and security seriously, but this can also result in improved or enhanced security measures causing increased waiting times and thus frustration from passengers and ultimately lead to flight delays. Therefore, it is important to take advantage of technological advances to improve security while maintaining a smooth and fast airport experience for passengers. There are different ways that have been recently developed that can help airports accomplish this, and here some of them are reported:

1. Powerful body scanning technology: the ability to detect and recognize prohibited items on passengers without the need to remove clothing items or even stay still has been developed and is being tested in airports. It is based on technology developed for astronomy to detect light in the farthest reaches of the universe, and through machine learning can determine the difference between a potential prohibited item and something benign on an individual.
 - a. Terahertz screening (always in body scanning technologies): This technology uses harmless heat sensing from an individual’s body to visualize objects concealed under clothes, including drugs, weapons and explosives. It can be done at a distance and it does not utilize harmful radiation.
2. Facial recognition: Software that can recognize faces is now being applied to recognize when a passport is being scanned that the actual person matches the photo. This could eventually be developed to allow for free movement of people throughout the airport, without ever scanning a passport and being able to recognize individuals and allow them through security without having to stop.
3. E-passports: This has been one of the major large-scale airport security advances recently. E-passports, otherwise known as biometric passports, contain a chip that can be scanned, significantly reducing the amount of work to be carried out by personnel and eliminating issues in human error, to help airports run faster but also safer.
4. Countering drones: There have been incidents recently of unauthorized drones flying around airports and wreaking havoc, even with just one single drone. Therefore, this is a new avenue of security that needs to be improved to maintain airport safety and security. There is a variety of technologies that can be used to Counter Unmanned Aircraft Systems (C-UAS), such as Geo-fencing which is based on GPS, stopping any drones from entering particular restricted areas.

While these new advances in technology improve the safety and efficiency of airports, it is imperative to not overlook more traditional physical security measures. Continuously maintaining and improving fencing, CCTV quality, and access control to security restricted areas are also important. This especially

considering the constraints that new technologies often encounter in order to be applied: privacy concerns/regulations, Geofencing not reliable for rogue drones, etc. But together, these novel and traditional physical security measures aim to keep passengers and personnel safe at all times.

2.1.2.2 Improving cyber security

Airports have long been targets for those wanting to create high-profile disruption and damage, so airport operations have evolved to manage the complex environment against physical security challenges. However, this security maturity level is often not matched by cybersecurity approaches. Although there is growing recognition of its importance and thus the creation of regulations described above, operators have a long way to go to better protect the airports from cyber-attacks.

Cybersecurity needs to cover the traditional Information Technology (IT) infrastructure, meaning computers, servers, network components, and software, as well as Operational Technology (OT) systems, such as Industrial Control Systems (ICS) like airfield lighting, heating, ventilation, fuel distribution, power management, and baggage handling systems. Put together, these aspects cover almost all airport operations in the scope of this project from check-in to screening, which again emphasizes the need to perform cyber-physical risk analysis on all operations, as stressed above.

The increased use of IoT, especially but not exclusively in an airport environment, can include, among others, all the installations that monitor environmental factors (temperature, humidity, etc.), control flow of people, their vital functions through integration of wearables and facial recognition to improve security, etc. This led the airports to have become increasingly susceptible to cyber-attacks due to seven main reasons:

1. Increased technology use: technology now plays an integral role in airport operations and thus the reliance on technology and automation to meet business needs means that airports are now exposed to new risks and unknown threats. Even communication between the air traffic control tower and aircraft, which traditionally used radio, is increasingly being done through data-link technology. DataLink is still using the electromagnetic spectrum for the transport layer, IP-based protocols are used and there is a deeper integration into the ATC and aircraft systems, thus creating a larger attack surface.
2. Hyper-connectivity: to make the most of the information available, airports have become more centralized and connected, linking multiple systems together through various platforms, and bringing information into centralized databases. This is also reflected in passenger expectations, that they have access to high-speed internet and real-time information on flights. However, this hyper-connectivity, and thus inter-dependency between these systems, means it is more difficult to exert complete control over a system due to different stakeholders being responsible for the different systems, allowing for an even larger network that malicious users could exploit.
3. Data sharing obligations: along with connecting systems, the data on those systems is increasingly under pressure to be integrated and shared across systems. The data being shared can even be spread across various geographic regions, similarly increasing the potential attack surface that attackers can target and even move through.
4. Customer centricity: similar to other businesses, airports need to understand their customers to best meet their needs and offer a range of services. As retail business in airports is in decline, there has been increased effort on offering passengers services starting in their own home through airport-related apps and messaging services to help develop brand recognition. All of this means the airports hold more personal data related to customers which creates another potential target and must be protected.
5. IT/OT towers while traditionally IT and OT systems have been isolated, there is increased integration between the two to increase efficiency, allowing for real-time data gathering, processing and decision-making. This is often used to *increase* security in the airports, but again adds another potential target with the increased connectivity that can allow for a cyber-attack on an IT network to result in threats to physical assets controlled by OT systems.

6. Remote towers: with stakeholders facing growing pressure to reduce operating costs, there is increased interest in digital remote towers replacing the primary control tower. This offers a central location for engineers to oversee the status of multiple airport systems at a time and better scalability. However, these critical systems then become highly dependent on the data links to transmit information, making a cyber-attack or even physical attack potentially devastating to airport operations and impossible to manage airport traffic.
7. Mega hubs: as some airports have become hubs in the air transport network, providing services for particular airlines or regions, this brings a substantial increase in operational volume and the need for better integration. Collaborative decision-making and processes must be shared with more stakeholders. But as a culmination of all the above changes, this also increases the reliance on hyper-connectivity, further IT and OT automation, and data sharing which all make the airport a more tempting and higher profile target for potential attackers.

Taking all of the above into consideration, it is often people that create the largest vulnerabilities in the airport environment. Cybersecurity measures are affected by the person in charge, what their experience is and what kind of governance structure there is. Cybersecurity starts with management buy-in and it is crucial embedding awareness into the organization's culture; it is of no use to have best practices if they are not followed or not followed 100% of the time. Beyond management, the airport personnel have varying levels of security understanding and how they are able to influence the security as security maintenance is responsibility for everyone engaged in the airport environment. For example, it makes sense to expect airport personnel to attend a cybersecurity briefing which would include how to interact with the airport's Wi-Fi system, but no passengers will be required to attend such a briefing before gaining access to the Wi-Fi. Lastly but certainly not least, contractors and third parties offer a notably weak spot in cybersecurity because the airport organization is not in charge of the hiring or sometimes of their training and instead relies on trust of the third-party company. This creates additional "shared risks" in the context of aviation supply chain security, and a weak link which must be addressed.

Therefore, for airports to overcome these cybersecurity challenges, there are eight steps, including mandatory requirements (according to the proposal of NIS 2 Directive (7)) that should be implemented and some additional practices that are highly recommended, if not mandatory for airports that have been identified as Operators of Essential Services under the NIS Directive:

1. Establish strong and effective cybersecurity leadership and governance: implement a cybersecurity governance framework based on international standards, national standards and emerging best practices, understand the legal and regulatory requirements, and create single points of accountability at the leadership level for end-to-end cybersecurity.
2. Establish a strong cybersecurity culture within the organization: establish cybersecurity awareness and training programs from the beginning.
3. Take a holistic, organization-wide risk management approach: conduct a risk assessment of the whole organization from the beginning, identify critical assets and systems, and address cybersecurity across all business processes.
4. Ensure the airport is secure by design: develop a robust security architecture which is a part of a greater airport architecture, ensure cybersecurity requirements are also included in how systems should be operated to reduce the risk of unauthorized access or system misuse.
5. Adopt a life-cycle approach to cybersecurity: ensure that cybersecurity requirements are included in all procurements, design systems that are easy to maintain from a security perspective, and design compartmentalized systems to prevent propagation effects.
6. Align cybersecurity with physical and personnel security: ensure that cybersecurity is a part of the overall, holistic security plan.
7. Establish a security monitoring and incident response plan: obtain threat intelligence from internal and external sources including the government, and develop an incident investigation plan as well as forensics.

8. Identify and manage cybersecurity stakeholders: identify both internal and external stakeholders to understand who are all affected.

Overall, improving cyber-physical security, based on areas of weaknesses revealed from risk assessments is crucial in this ever-changing world. There are no EU standardized norms to regulate safety and security in an integrated manner, which makes it that much more important for all airports to voluntarily adopt the proposed measures. Increasing safety and security at one airport, not only ensures the safety of those passengers and personnel, but others at all other connecting airports. While the world is becoming ever-more connected, digitally and physically, the bar needs to be raised across all air transport infrastructures.

2.2 Best practices - Improving the cyber-physical security of the Baggage Handling System

Airport Baggage Handling Systems (BHSs) make sure bags placed in check-in counters reach the correct flight destinations. BHSs follow the International Air Transport Association (IATA), Recommended Practice 1745, and provide several baggage handling services. Such services include baggage screening, tracking and sorting and are accomplished using physical equipment. The baggage screening service is implemented using Explosive Detection Systems (EDS) that scan the baggage and decide if a bag is clear or suspect. The baggage tracking service is implemented by placing sensors on BHS conveyors and CCTV cameras that track the baggage positions. The sorting is implemented using automatic tag readers to scan bag tags, and pushers/diverters that route the bags to the flight carousels. To enforce such services, BHSs-specific software controls the physical equipment, and performs baggage routing decisions according to the check-in information obtained from Airport Operations Database (AODB). The usage of both digital and physical assets to accomplish BHS services, requires an enforcement of cyber-physical security measures. This section proposes some security best practices that can be applied to BHSs.

2.2.1 BHS security regulations

The baggage process is an integral part of any commercial airport, and the efficiency of an airport is largely dependent on this process. Several different sub-processes interact with each other and cause domino effects because of the interconnectivity of systems and procedures (for example we can take check-in process which includes several different procedures and rules related to passenger and baggage handling, both with strict security regulations included). Cyber-physical attacks can exploit different sectors of the infrastructure, even physically or logically far away from the threat entry point.

A key aim of aviation security is to ensure safety of passengers, crew, ground personnel and the general public in all matters related to safeguarding against acts of unlawful interference with civil aviation (ICAO, Annex 17 (8)). On this account, it is important to protect airport infrastructure, control the access of people's movements through CCTV surveillance and access control rights using biometric tools to verify the employee's identification and access rights to particular buildings or areas. A well-known implemented security solution is the screening of passengers and their baggage to detect prohibited items. This can come in the form of X-ray screening, X-ray based explosive detection systems (EDS), explosive and chemical trace detection systems (ETD), and body scanners.

The BHS area is located on the airside with limited and restricted access rights: this means that everyone is subject to screening (e.g. metal detector doors and x-ray check) of personal belongings at each entry or exit. All employees have permanent ID cards, while for others temporary accompanied person ID's are issued. This airside security check combined with issuing of ID cards provides very high level of certainty and no one is excluded. The airside part of the airport is covered by safety management, where all safety-related anomalies and incidents are reported in order to determine the

precursors of accidents or potential safety hazards. Examples of safety significant occurrences are listed in the airport's Safety management manual. Because of this and strict airside access control and security inspections of personnel, it is hard for the outside attacker to reach the BHS area.

Physical security controls of the BHS area consist of organizational procedures, implementation of relevant standards and technical controls. Training and security awareness represent an important consideration for all employees and professionals with BHS area access, so they are aware of their responsibilities and obligations. This does not mean that all ID card holders can go wherever they want – access control policy is implemented to authorise only persons according to operational needs.

Equipment intended and used to achieve those set physical security goals is diverse. Walk-through metal detection (WTMD) and hand-held metal detection (HHMD) equipment allow the security screening of persons in order to prevent prohibited articles from being introduced into the security restricted area. An explosive detection system is used for security screening of hold baggage in order to prevent prohibited articles from being introduced into the aircraft, and all of it is covered with long range cameras and other CCTV surveillance systems.

Everything mentioned above is subject to strictly defined rules which are enforced constantly to ensure that no unauthorized person enters restricted areas and that no prohibited articles can be introduced.

2.2.2 Industrial Control System best practices

Most Industrial Control Systems (ICSs) are designed by following standards such as the International Society of Automation (ISA)-99 (9) or the National Institute of Standards and Technology (NIST) 800-82 (10). ICSs that follow these standards, typically have their network topology geographically dispersed throughout the organization facilities and are organized in five layers: enterprise, operations, supervisory, control, and physical layers. These five layers are explained in the following:

- The **enterprise layer** contains all IT devices needed to perform all the operations related with management of the organization (e.g. financial systems);
- The **operations layer** contains the devices for optimizing workload and quality of service (QoS);
- The **supervisory layer** contains the high-level monitoring tools of the ICS network, SCADA, HMI and SCADA Historian Database. This control centre, which is typically centralized in one location is responsible for monitoring the QoS, alerting operators of service drops, keeping the history of operations and applying concrete measures to guarantee quality of service. The enterprise, supervisory and organization layers are typically the only layers that have internet connection;
- The **control layer** (that contains control units of the system);
- The **physical layer** (that contains the physical ICS components) have restricted accesses and are geographically dispersed throughout the 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. It is common practice for BHSs to follow an ICS architecture approach. BHSs have control layer devices, e.g. programmable logic controllers (PLCs) that interact with the BHS physical equipment. These control layer devices are commonly connected to supervisory equipment (e.g. SCADA system) to maintain the status of the BHS operation and perform maintenance of the physical equipment. The BHS control layer devices can also be connected to the supervisory layer sorting unit, which polls the BHS control unit equipment to identify baggage circulating in the BHS conveyors and issue sorting orders to the control unit, to move bags to their correct destinations. The BHS sorting unit gathers knowledge from operation layer, namely the AODB, to make informed sortation decisions. The sorting unit is responsible to provide an up-to-date status of all checked-in bags that pass through the BHS. BHSs can thus be regarded as ICSs that should comply with International Society of Automation (ISA)-99 (9) or the National Institute of Standards and Technology (NIST) 800-82 (10). For

this reason, BHS cyber-physical security can improve significantly by implementing ICS common practises. Those practices include (10):

- Security policies, awareness and training of ICS personnel;
- Risk analysis and mitigation considering the threat level;
- Implementing access restrictions to ICS devices present on operation layer networks, through firewalling, access control and demilitarized zone (DMZ) architectures. Physical access restrictions to ICS devices should also be implemented;
- Reducing ICS user privileges to ICS devices based on work needs and enforcing authenticity and legitimate use based on authentication mechanisms (smart cards, passwords, etc.);
- Implementing a monitoring and detection strategy based on mechanisms, such as intrusion detection software (IDSs) and antiviruses, that can inspect activities on ICS devices and communications and detect in real-time abnormal use of the ICS equipment. Such mechanisms are crucial to address in feasible time the effects of cyber-physical attacks;
- Deploying security patches after testing all patches under field conditions on a test system if possible, before installation on the ICS.

The SATIE Toolkit provides several tools that help to enforce ICS common practices. The Business Process Intrusion Detection System (BP-IDS) (11) provides an innovative way to monitor communications between BHS control unit, sortation units and SCADA devices, and detect abnormal operations conducted over the physical equipment that can compromise the baggage sorting services. The Incident Management Portal (IMP) provides a security operation centre that aggregates all security alerts in a graphical user interface understandable to practitioners. BP-IDS, the Malware Analyser and IMP can play an essential role for having an effective detection strategy. Business Impact Assessment (BIA) (12) aids during the risk analysis phase to assess the overall impact that a cyber threat can have to the BHS services, and determine which devices should be protected in order to reduce the risk level associated to that threat. The Malware Analyser monitors activities and detects malicious activities on ICS devices. Gestion Libre de Parc Informatique (GLPI) offers an automatic mechanism for the up-to-date asset inventory system of the BHS, which can be integrated with the Vulnerability Intelligence Platform (VIP) for obtaining a list of Common Vulnerabilities and Exposures (CVE) affecting the BHS. Both GLPI and VIP can help in identifying the best security patches to apply to the ICS equipment.

2.2.3 Recommendations for handling cyber-physical threats

Regarding the BHS area's physical access control, the main guidelines are mentioned in the sections above. The main reason this area is in the airside zone of the airport (except for the conditions and regulations of the baggage handling process) is a high degree of security provided by the strict control of the movement of persons. In this context:

- allowing entry only to persons with authorisation,
- the security screening of people and belongings without exception,
- the complete CCTV coverage and recording,

should be sufficient levels of risk mitigation. Additional awareness is provided by:

- periodical trainings for all personnel,
- occasional tests for security personnel and,
- random checks defined by the security management policy.

However, as this may keep outside attackers away from the BHS area, employees with malicious intent or coerced could find a way to bypass security controls. Therefore, it is important to respond to any suspicions and be aware at all times, especially when it comes to what may seem as everyday tasks, known people and standard routines.

As far as cyber threats are concerned, SATIE proved to be promising and a good solution in recognizing attacks through training and simulations. Since the replica of the real BHS is used, the same results are expected in reality and should be confirmed with scheduled demonstrations at the airports.

2.3 Best practices - Improving the cyber-physical security of the Airport Operations Centre

The aim of improving the cyber-physical security of the airport's AOC, i.e. Airport Operations Centre, can be addressed on two fronts: by identifying how to improve its own functioning, through the widespread adoption of suggested measures and standards, and by applying what has been learned in SATIE specifically, including the correlation of cyber, physical and cyber-physical threats.

2.3.1 Improving AOC practices in general

According to the company objectives and the directives received in terms of strategy, the Accountable Management and Information Security Management functions share a plan that contains security measures and controls to be applied according to the results obtained from the risk analysis process (risk assessment).

The plan envisages the identification and classification of critical assets against which appropriate security measures must be taken and appropriate effectiveness controls established. With regard to the AOC entity, which represents the core institution for the execution and monitoring of airport operations, the highest attention must be paid in terms of safety to all the specificities that constitute it and make it operational, including human resources. With regard to human resources, they must be continuously trained and verified in relation to professional skills and knowledge with particular attention to aspects of safety, physical security and information security. Access to AOC areas must be strictly controlled and regulated according to the roles and responsibilities attributed to individual people.

2.3.1.1 Information Technology (IT) infrastructures

The AOC structure must be guaranteed electrical and climatic continuity measures (HVAC) and prevention from disastrous events (for example fire). All IT infrastructures (workstations and network connectivity) dedicated to the operation of the AOC must be electrically supported by uninterrupted power supply and the relevant technical rooms must be access-protected and only accessible according to defined and known criteria and procedures. When possible and feasible on the cost side, the AOC should be duplicated in an alternative area and distant from the primary one for contingency reasons, a timely crisis plan should be prepared to be used in cases of need. The workstations and monitoring stations must be accessed according to nominative identification, when possible using MFA (multifactor authentication). The ICT (Information Communication Technology) applications and services made available must be able to comprehensively represent and understand all the functions necessary for carrying out operations under the responsibility of the AOC.

2.3.1.2 Operational Technology (OT) infrastructure

The AOC may need to make use of additional monitoring platforms, relating to the automated and industrial systems of the OT (Operational Technology) area (for example ICS, i.e. Industrial Control System; SCADA, i.e. Supervisory Control and Data Acquisition), in order to be able to identify anomalies and correlate operational impacts to be managed procedurally. The systems, networks and infrastructures of the IT and OT type must be architecturally implemented according to resilience and persistence criteria in order to ensure adequate levels of continuity of the services essential for the proper functioning of the AOC.

2.3.1.3 Security Operation Centre (SOC)

In order to implement an efficient and effective system that can protect the AOC from cyber threats, according to the results deriving from the risk analysis, a technological architecture must be implemented (typically NG SIEM, i.e. next generation security information event management) and a cybersecurity organizational structure (typically defined SOC, i.e. Security Operation Center). The NG SIEM technological solution must be able to collect certain events from systems, networks and assets that are part of the ICT and OT infrastructures in order to be able to identify scenarios, states and behaviours that could determine anomalies with an impact on the management of airport operations. The peculiarity of the NG SIEM solution, now proposed by several brands on the market, is that of being able both to:

- integrate software components of the SOAR (Security Orchestration Automation Response), essential for the optimized management of incidents;
- include complementary elements of ICT analysis and sensors and OT cyber such as UEBA (i.e. User Entity Behaviour Analytics), MDR (i.e. Managed Detection and Response), NDR (i.e. Network Detection and Response) and TIP (i.e. Threat Intelligence Platforms) solutions.

The SOC structure, in which there are specialized figures of cybersecurity analysts, is in charge of verifying the content of the events and to classify their entity, up to establishing the critical state of any security incident and operating according to procedures also shared with the AOC structure. The SOC operates 24/7, in line with the service activities of an airport reality and must be able to guarantee its own detection and response processes with a responding organization, covered by IT certified specialist personnel, possibly located in at least two alternative locations. The effectiveness and efficiency of the service will have to be measured according to the timing of detection of a potential incident, response, impact mitigation and identification of its root causes. The cyber incident management procedure must include the actions approved for the management of the incident itself, which will involve multiple process owners of the business organization and, above all, the AOC structure.

2.3.1.4 NIS Directive

In relation to the requirements of the NIS directive, it is recommended to carry out the census of critical assets for the airport business and AOC operations and verify their maturity compliance with regard to cyber measures of the security framework model of NIS directive, inspired by the NIST standard. As contemplated by the European NIS directive, to protect critical operations carried out in the context of airport operations, of which AOC is an integral part, risk management processes must be activated at least once a year with the aim of identifying and analysing those risks potentially impacting on the ICT and OT infrastructures. However, other events can trigger the risk re-evaluation process, such as serious security incidents, regulatory changes, significant changes in systems, etc. The analysis will determine the appropriate technical and organizational measures that must be adopted.

2.3.1.5 ISO/IEC 27001 / IEC 62443

To protect information security, a further comparison with the ISO/IEC 27001 standard is also recommended in the context of IT, OT and business processes (for example AOC), in order to obtain appropriate certification and be able to monitor developments according to the continuous improvement. In addition, the industrial standard for communication networks IEC 62443 could be considered.

2.3.1.6 CISO / CSO

To ensure the protection and safeguarding of business processes, which as mentioned include the AOC, the company organization must consider the appointment of the CISO or CSO (Chief Information Security Officer or Chief Security Officer) who will have the duty to annually verify the effectiveness of the information security plan which will also include the resilience terms to guarantee business continuity.

2.3.2 Improving AOC practices based on what has been learned in SATIE

SATIE has helped to highlight the importance of improving security to physical threats, cyber threats, and combined cyber-physical threats which have the potential to affect many more airport systems and thus be catastrophic for AOC operations.

SATIE has contributed to highlighting the importance of improving the managing of those risk aspects deriving from cyber threats, having potential impacts on the safety of human life, physical security to facilities and IT infrastructures. This is done through the raising of alerts that refer to those events or incidents of a significant nature with regard to guaranteeing the security and safety of passengers and operators and the continuity of airport services. This risk is initially managed by the SOC which is operationally assisted by the AOC.

2.3.2.1 Events collection

The architectural components of cybersecurity event management which are part of the SATIE project, have in fact made it possible to demonstrate how the collection of anomalous technical or behavioural events can be inserted in a functional and operational context of the airport nature.

Within this context, IT security specialists and personnel assigned to the management and control of operations cooperate to identify and analyse the possible presence of uncommon states and take actions that are compliant to guarantee the correct functioning of the airport system through the application of adequate measures.

The effect of this synergy between the parties is to make the SATIE platform functional to detect complex situations or scenarios that are particularly critical to the regular exercise of airport activities, which often result affected on security and safety issues.

The cooperation between the parties involved in the management of the events collected by the SATIE platform has allowed greater effectiveness of applicability of the rules and improvement of the management chain of a potential security event or incident. This derives from a greater understanding of airport processes, from the standardization of the languages adopted by simplifying those that are too technical, and from the active involvement by the individual reference persons belonging to the SOC or AOC entities.

2.3.2.2 IT and OT technological assets

The identification of IT and OT technological assets, by the entities involved in the management of SOC and AOC security events, is to be considered an important scenario for the purposes of the applicability and maintenance of control rules within the SATIE platform and consequent application of the related protection measures.

As indicated, the SATIE functional tools for the purposes of managing anomalous security events lead to the deduction that it is necessary to identify the "surface of attack". This must be done in support of each implementation phase and shared in a synergic form between the parties involved. Moreover, the "management of cyber incidents" procedures must always be planned in advance and timely risk assessment sessions carried out, in order to minimize the impacts deriving from cyber threats.

An important part of maintaining the safety and security of the airport and all people involved (e.g. passengers, personnel, third-party personnel, etc.) means protecting the AOC from threats so that the AOC can maintain its operations, safeguarding the business and all involved people, which includes directing traffic on the apron and managing the flow of passengers throughout the airport. Threats can come in the form of physical and cyber-threats.

2.3.2.3 Addressing physical threats

Addressing physical threats to the AOC means protecting the personnel inside, protecting the building itself, not making possible unauthorized access of people, and keeping it well protected. Through the risk assessment performed in SATIE, it highlighted the need to securely protect the personnel inside, which means performing proper background checks when hiring staff, as well as having strict

requirements when selecting vendors or third-parties who will have access, though limited, to the AOC and its personnel. Protecting the building itself includes keeping it isolated from other areas of the airport where passengers and other unauthorized people may pass, incorporating seismic-resistant architectural design, as well as using blast and penetration resistant building materials. These measures can protect the AOC, its critical IT systems, and personnel protected from both natural disasters (e.g. earthquakes, lightning) and from intentional manmade disasters (e.g. bomb, vehicle-ramming attack). While these concepts are true in general and well-known in the air transport sector, these concepts were assessed, integrated and correlated into an overall view in the SATIE project which took into account the interactions between cyber and physical threats specifically in the airport environment.

2.3.2.4 Propagations of threats

The AOC houses critical airport systems, which are usually highly interconnected, to allow for faster and more efficient data flow and thus swift identification of problems. But this also lends itself vulnerable to cyber-attacks, especially if an attacker is able to enter from a weak point (e.g. Wi-Fi network, a workstation in the gate area connected to those critical systems) and navigate through the network to maximize their damage. Airports are strongly encouraged to adopt a regular risk assessment approach to understand where their largest vulnerabilities are, as discussed in section 2.1.2. Beyond that, it is ever-more increasingly important to understand potential impacts and propagations of threats throughout the assets within the AOC. This can be done by having an updated asset topology network, and using threat or impact propagation simulation software to better understand – before a threat occurs – how threats can propagate through the system and therefore help security personnel identify where better security is needed. No longer are attacks performing simple singular cyber-attacks, but they are becoming more complicated, and therefore, security preparation and mitigation efforts need to do the same.

A cyber threat cannot only transform into a different cyber threat through connected systems, but cyber threats can also transform into physical threats, and vice versa. The interconnectedness of cyber and physical assets has similarly increased with increasing advances in technology. For example, a cyber-attack altering passengers-related data, on a database found under the responsibility of an airline system, can result in allowing a terrorist to pass the authorities' passport controls as a legitimate passenger and board a flight, that otherwise it should have been forbidden. A cyber-attack into the AODB, altering flight gate information, could lead to congestion of passengers in a particular gate area, allowing for greater damage in a melee attack.

2.3.2.5 Combined cyber-physical security system

These examples emphasize the need for a combined cyber-physical security system such as SATIE so that the physical security personnel at an airport can cooperate with the IT security personnel so that they both have a full situation awareness and are able to understand more quickly when an incident is occurring, whether in the AOC or other areas in the airport. The measures adopted to mitigate or even eliminate the threat depends on the airport operator's understanding of the severity of the incident as well as their speed to contact and inform necessary airport entities to then react. This communication chain varies according to the procedures described by each airport's applicable regulations and manuals.

2.4 Best practices - Improving anomaly detection on cyber-physical threats including passenger data

The industry is deploying computer vision, machine learning and pattern recognition solutions, biometric technology that enables many automated passenger authentication and validation systems

at some of the world's largest airports. Most of the current solutions are developed through deep learning technology (13). Key products offered by the Industry in this field include among others:

- Biometric face recognition based on visible light images;
- Biometric face recognition based on infrared images captured using state-of-the-art cameras;
- Biometric face recognition where visible light images and infrared images can be compared;
- Facial recognition systems are powered by deep learning, a form of Artificial Intelligence (AI) that operates by passing inputs through multiple stacked layers of simulated neurons in order to process information;
- Predictive analytics to enable the digital twin of the airport to enhance operations management team performance;
- Bag-tag Optical Character Recognition (OCR) to read text from luggage labels to enhance read rates during sortation and act as a failsafe when barcode reading systems fail;
- Threat detection in images captured using x-rays or passive emissions;
- Facial image quality assessment (based on ICAO requirements);
- Automated queue monitoring;
- Passenger screening technologies;
- Behavioural Detection techniques.

There is a variety of current regulatory framework and standards related to anomaly detection on Cyber-physical threats embedding passenger data presented in “Annex 1 – Current regulatory framework and standards related to anomaly detection on cyber-physical threats, including passenger data”.

2.4.1 Recommendations of anomaly detection technological improvements on passenger data protection

Passenger data include sensitive information of people (i.e. name and IDs, contact details, payment information, etc). Passenger's travel details are provided by Passenger Name Records (PNRs) which illustrate the information required to enable reservations to be processed and controlled by the booking and participating air carriers for each journey arranged by or on behalf of any person, whether it is kept in reservation systems, departure control systems checking passengers onto flights or equivalent systems with similar functionalities (Specific system integrating both reservation and departure control functionalities). PNR data must include Advance Passenger Information (API) data whether collected by the air carriers, which are considered air passenger data captured at check-in or at the time of online check-in containing passenger biographic data retrieved from the Machine Readable Zone (MRZ) of their travel documents and passenger's flight data (full journey information, ticket number, pricing and taxes, passenger's contact information, etc.).

Given that, the number of countries utilizing PNR data and API data is gradually evolving in the last decades (over 50 countries already access PNR and over 90 countries utilize API data before the flight's arrival), the potential of such data leaks and information exposure can cause tremendous effects on people's personal life, safety and wealth as well. For instance, the February's 2021 data hack of IT operator Sita, which supports airlines including Singapore, Lufthansa and United, reported data breach revealing frequent flyer data where hundreds of thousands of Star Alliance passengers' details were stolen abusing people's privacy (14). To avoid such unwanted events and tackle malevolent activities against passenger data security and safety more good practices initiating advanced technologies and up-to-date techniques are needed to improve the protection of passenger data and thus citizen's personal rights while maintaining border integrity and facilitating passenger flow.

Within this framework, approaches that strengthen anomaly detection techniques could address this challenge. Based on the WCO/IATA/ICAO guidelines on passenger-related information (see Annex 1), the following recommendations aim to provide features and technology improvements that permit to

collect and analyse passenger information, providing security at each specific stage of the process (from the trip booking step (outside of the perimeter of SATIE), through the check-in, up to the border control) of the different parties involved in the process (i.e. airlines, custom, police, airport, travel agencies, etc). Recommendations on this process are presented in the following subsection.

2.4.1.1 Check-in step

Concerning the check-in step of the process, a baggage recognition solution is provided to enhance the current baggage check-in procedures by the airlines by bringing the photo capture capability and the features around it.

As for the capture of passenger data, the principle of security by design should be applied when deploying the system:

- Capture should have the best possible quality (avoid blur by always positioning the subject in the same position, put the capture device on a fixed standing point to keep the same point of view between captures);
- In case of multiple capture site, the capture process should use the same type of device and should be done in the same condition (exposure to light, color of ambient light, same type of background, same angle of view for the capture);
- Capture should take only information of the subject to avoid gathering unwanted information on other subject (protection of personal data by only capturing required data).

Those recommendations will ensure that the post event search will be the more efficient possible (to avoid false hit as much as possible) and could be reproduce for verification if required.

As a mandatory requirement, storage of the picture and transmission of the captured image shall be encrypted if not made in a separate network or if externals accesses are possible.

2.4.1.2 Border crossing step (gates)

Regarding the border crossing step of the process, an interactive API solution (iAPI) has been adapted to provide an efficient way to analyse passenger data.

The capture of passenger data from a MRZ of a travel document is a well-known technique that provides quality capture of information, so no specific additional recommendation is provided to improve the quality of the data.

For each data provider system that connect to the SATIE platform to send iAPI information, a signed certificate should be emitted specifically to identify both the data furnisher and its right to send data to the system. Those certificats should not be limitless and should have a lifespan corresponding to the expected time the data furnisher will send data to the system.

All others security recommendation to connect to the SATIE platform should also applies to any data furnisher that have to send iAPI data.

2.4.2 Recommendations for airports employees biometric access control deployment

When it comes to deployment of biometric solutions for access control, the following three main recommendations should be followed.

2.4.2.1 Accuracy of the solution

Accuracy of a biometric system is a key to a successful implementation as it will impact on both the security and the comfort of the end-users. Indeed, low accuracy system will increase considerably the chance to get false acceptance and/or false rejection. False acceptance which represent the fact to identify an individual by someone else from the database is a major security threat to airports and organizations as it means that somebody not allowed or even complete stranger to the organizations could get access to a restricted area. False rejection represents the fact to not being able to identify

an authorized person which result in an employee having to restart the identification process creating lot of frustrations. Thus, resulting in potential dismantlement of the solution of the frequency is too high among all employees.

Accuracy is not only about the results itself, but as well the means of enrolment and capture of the biometric are very important. The most secured identification solution has no value in access control if the process takes more than 5 seconds.

With the current context of COVID-19, it is recommended to opt for contactless solutions to avoid the spread of the pandemic across humans.

The Unified Access Control solution developed for SATIE (see SATIE D7.2 (1)) is the state-of-the-art solution to increase security for access control by combining both face and fingerprint identification while maintaining a great comfort of usage by providing contactless and frictionless identification.

2.4.2.2 GDPR compliance

Deployment of biometric identification for employees within the EU is subject to the GDPR and considered as a process of sensitive data by law (Article 9 of the GDPR (15)). Therefore, there is typically some main recommendations that should be followed for a deployment:

- Proportionality: The use of biometric data must be proportional to the negative impact of a potential threat. Only high security requirement area can justify the use of biometric data to protect their assets such as a Security Operation Center of an airport;
- Consent: Consent of the end user must be collected before any biometric processing;
- Possibility to opt-out: The system should offer the possibility to get access granted by other means than the biometric such as contactless card, pin code, magnetic card.

2.4.2.3 Secured implementation

The last aspect of the recommendations for safe deployment of biometric solutions for access control is to follow standard secured implementation such as:

- Access control devices and server should be encapsulated in a segregated network that with no open to external access;
- Databases and biometric templates should be encoded by non-reversible algorithms (i.e., apply hashes like SHA-256) and encrypted with state-of-the-art encryption and hashing function (e.g. AES 128, SHA 256);
- Communication between different systems should be secured via Transport Layer Security (TLS, which allows authentication between server and clients via digital certificates);
- Low-level protocol communication between devices and controller panel should be migrated from Wiegand (unsecured communication protocol) to Open Supervised Device Protocol (OSDP – encrypted communication protocol).

2.5 Best practices - Security of the digital services and voice communication systems of air traffic management services

When best practices in the area of Air Traffic Management (ATM) are concerned, it is needed to identify first the institutions providing the framework for the safe and secure set-up of the system. Thereafter, the rules which are in place to govern ATM need to be taken into consideration. Traffic management control operators are covered under the scope of the NIS Directive and the NIS 2 Directive proposal, including relevant requirements that address the cyber aspects. The main organisations in Europe administrating ATM are ICAO (which is on international level as well) and the European Union Aviation Safety Agency (EASA) for the European region. As traffic management control

operators are covered under the scope of the NIS Directive, the requirements therein are also relevant for the cyber aspects. In addition, there are respective national competent authorities.

The most prominent European regulation is currently the Regulation 551/2004 - Organisation and Use of the Airspace in Single European Sky (SES). The objective of the airspace regulation is to put an end to the fragmentation of EU airspace and to create an efficient and safe airspace without borders. The organisation and management of airspace should be improved by merging all the national Flight Information Regions (FIRs) into a single portion of airspace within which air traffic services will be provided according to the same rules and procedures.

Industry standards in any domain have already been set up to reflect good practice. In air traffic management and aviation, there is no difference. With respect to security in ATM, a specific number of standards and recommended practices stand as additional best practice to follow. The list of standards is presented in Table 2.1, where standards addressing digital services of ATM and voice communication systems are listed.

Table 2.1: Security standards for digital services and voice communication systems in ATM

Standard/Guidance documents	Brief description
ICAO Annex 17	Annex 17 is providing preventive security measures for all the aviation stakeholders involved in the ATM services, and not only. It safeguards civil aviation against unlawful interference, as it includes recommendations of critical information and communication system protection.
ICAO DOC 8973: Aviation Security Manual	ICAO Document 8973 was developed to assist Member States in implementing Annex 17. It provides guidance on the application of the Standards and Recommended Practices. Chapters such as chapter 18 provide assistance for communication systems security.
ICAO DOC 9985: ATM Security Manual	ICAO Document 9985 is a complement to Doc 8973 listed above. It is specifically targeting air traffic management and its components. It provides guidance on security issues and protection of ATM system infrastructure.
EUROCAE ED-201	The ED-201 document provides guidance not only to specific types of ATM stakeholders with respect to security, but it also puts accent on shared information risk resulting from the high level of interconnectivity between stakeholders, for example shared networks or information exchange.
EUROCAE ED-202A/RTCA DO-326A: Airworthiness Security Process Specification	ED-202A is built on top of ED-201 described above and proposes guidance for ensuring the airworthiness of security processes. Its focus is not primarily on the ATM digital services and voice communication systems, but rather on the aircraft systems. Nevertheless, these on-board systems are sharing connectivity with ATM systems which ensures the importance of this document.
EUROCAE ED-203A/RTCA DO-356A: Airworthiness Security Methods and Considerations	ED-203A is a complement to the ED-202A document. It provides guidance on methods of airworthiness security implementation.
EUROCAE ED-204/RTCA DO-355: Information	ED-204 is a guidance documents with the focus on preserving and continuing airworthiness related to information risks. This is a resource for ATM stakeholders to ensure for example that the information security risk

Standard/Guidance documents	Brief description
Security Guidance for Continuing Airworthiness	associated with the voice communication systems are within the acceptable boundaries.
ED-205: Process Specification for Security certification and declaration of ATM/ANS ground systems	ED-205 is a document focused on the security aspects of information through the entire data lifecycle. This document is targeting specifically the ATM digital services and voice communication systems, and the influence of the ground infrastructure systems on the safety of an aircraft.
ECAC DOC 30 - Chapter 14	ECAC Document 30 was developed to facilitate civil aviation. Chapter 14 from this document is concerned with cyber threats to civil aviation, which includes cyber security governance at national level and cyber security activities at organisational level.
ISO/IEC 27001: Information Security Management System (ISMS)	ISO/IEC 27001 is a standard concerning the general information security best practices. It specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system. Even though it is not an aviation specific standard, it is vastly adopted across other industries and it has the possibility to be tailored to the requirements in ATM digital services.
CEN - EN 16495: ATM – Information Security for organisations supporting civil aviation operations	CEN – EN 16495 document is providing guidance to organizations supporting air traffic management operations. This document is based on the ISO/IEC 27002 standard, which brings the security techniques and code of practice to the ATM world.
ISA/IEC 62443: Industrial Automation and Control Systems (IACS) security	ISA/IEC 62443 is a series of standards, technical reports, aimed at industrial communication networks. The ATM world comprises of both IT and OT systems, and this series are concerned with OT systems.
National Institute of Standards and Technology (NIST): Cyber Security Framework (CSF)	NIST CSF is a document providing policy framework for computer security guidance to minimizing security risks. It is widely adopted by private sector and governments and it was firstly designed for critical infrastructures. This allows the CSF to be among the best practices when considering the prevention, detection and response to cyber-attacks on the ATM infrastructures and voice communication systems.
NIST SP800-82: Operational technology security	SP800-32 document represents a guide, designed for ICS security. ATM and communication systems are composed of such systems, this guide can also be used to achieve the desired security level, as well as its risk management and assessment methodologies.

2.6 Best practices - Airport crisis management and decision support

The EC 114/2008 directive defines Critical Infrastructure (CI) as the assets, systems, and networks located in Member States which are essential to maintain vital economic and social functions such as health, food, transport, energy, information systems, financial services, etc. The EC recognizes that these infrastructures must be protected from disruption by natural disasters and man-made threats, and as such has launched the European Programme for Critical Infrastructure Protection (EPCIP). The importance of physical and cyber security in CIs has never been more explicit. CIs in general, and especially in transport, energy and health sectors are exposed to various physical threats (i.e. terrorism, technological accidents, natural disasters, etc.) and cyber-attacks which are emerging especially with the increasing use of information systems. Now more than ever, CIs must be vigilant in establishing safeguards against physical and cyber threats, as it is imperative to have a solid understanding of the risks, vulnerabilities, security processes and technologies available. In addition, it is of paramount importance for CIs to establish a standardized crisis management process to deal with attacks that threaten to harm the organisation and stakeholders.

The aim of this section is to describe a common cyber-physical crisis management process encompassing the involved stakeholders. Moreover, gaps and best practices related to security issues are analysed and a global approach for airports' cyber, physical and cyber-physical security management and joint coordination is proposed. This approach recommends the adoption of a Holistic Security Operations Centre (HSOC), which will facilitate the communication and cooperation/coordination between internal stakeholders for cyber and physical incidents, and the Airport Operations Center (AOC) that will facilitate the communication/coordination between the HSOC and the external stakeholders. The AOC will also support the communication and cooperation/coordination between the different CI operators and stakeholders, in case of an incident that has cascading effects to interconnected Infrastructures (16).

2.6.1 Operation and security regulatory framework

The first official effort for the preparation of a strategy to protect CIs was initiated by the European Council in 2004. In 2006, EU set the parameters for the implementation of the EPCIP (17). In 2008, the European Council Directive 2008/114/EC (evaluated on 2019 through public consultation and pending to be revised) established a procedure for the identification of and designation of European critical infrastructures (ECIs), focusing on the Energy and Transport sector, and the assessment of the need to improve their protection (18). In accordance with the Regulation (EU) 2016/679, organisations including CIs must protect natural persons while processing personal data and exchanging of such data. The principles of the EU Directive 2016/1148 (NIS Directive) concerning "measures of a high common level of security of network and information systems across the Union" are also applicable to CIs (4).

In the context of airports and additionally to the aforementioned, one year after the September 11 attacks, EU adopted a set of aviation safety and security rules based on Regulation (EC) No 1592/2002 and Regulation (EC) No 2320/2002 (19) (20). In 2008, the EU extended the safety rules in order to cover the aircraft operations and aircrew licensing and training (Regulation (EC) No 216/2008), while in 2009 the extended Regulation (EC) No 1108/2009 covered the safety aspects of aerodromes, air traffic management and air navigation services. Currently, EC regulation 300/2008, which repeals regulation (EC) No 2320/2002, establishes common rules in the EU to protect civil aviation against acts of unlawful interference, which pertain to the screening of passengers, cabin baggage and hold baggage, the airport security (access control, surveillance), the aircraft security checks and searches, the screening of cargo, mail, airport supplies and the personnel recruitment and training. In addition, a national authority for aviation security must be appointed while establishing a national civil aviation security and quality programme. The detailed measures for the implementation of the common basic standards on aviation security are updated in "Commission implementing Regulation (EC) N°

2015/1998” (21), an amendment to EC 300/2008 regulation which is still in force. Moreover, ICAO works with Member States and industry groups to reach consensus on international civil aviation Standards and Recommended Practices (SARPs) and policies. The regulations and policies suggested by ICAO are adopted by the ICAO Member States to ensure that their local civil aviation operations and regulations conform to the suggested norms, to ensure safety and security. ICAO Annex 17 sets the preventive security measures relating to access control, screening of aircraft passengers and their cabin baggage, screening of hold baggage, screening of cargo and mail, measures for handling special categories of passengers, for protecting Information Systems, etc.

2.6.2 Physical and cybersecurity measures and security operation centres

The physical security and cybersecurity measures as well as the relevant regulations, policies, standards adopted by the airports have been described in detail in the SATIE deliverables, D7.6 SoA about airports security and expected improvements (22) and D7.7 Specification of a holistic security management cycle (5).

Aviation safety and security is a combination of human and material resources to safeguard civil aviation against unlawful interference. Currently, regulation (EC) No 300/2008 of the European Parliament and of the Council and its amendments establish common rules in the European Union to protect civil aviation against acts of unlawful interference. Unlawful interference includes acts such as terrorism, bombing, sabotage to aircraft or airport facilities, hijacking, communication of false threat, which can cause chaos at the airport, and aircraft accidents etc. The Regulation's provisions apply to all airports, all operators that provide services at the airports, all entities located inside or outside airport premises providing services to airports. ICAO's Annexes 9 to 11, 14 and 17-18, along with nation-specific and airport-specific regulations establishing standards and recommended practices, concerning air navigation, flight inspection, prevention of unlawful interference, training, communication equipment, emergency planning, air accident investigation, etc. (Table 2.2).

Provided the aforementioned institutional framework, airports implement several security measures and technology solutions to deter, detect and react to physical attacks (8) (23) (24) (25). More specifically:

- **Access control** should rely on a combination of physical elements (perimeter protection, physical barriers/bollards, guards, portals, security lighting, alarm systems, intrusion detection systems, audio and video surveillance systems, etc.) and policies (asset classification, identification, authentication, authorization, access groups, credentials and credentialing, entry control techniques, such as password, pin, biometric identifiers etc.) to properly operate;
- Each airport operator should clearly **define the airport's boundaries** to enable the appropriate security measures to be taken in each of those areas. To this end, boundaries are set between landside, airside, security restricted areas, critical parts, and demarcated areas. In most cases, physical barriers, clearly defined, separate the different areas;
- **Physical barriers** include any objects that prevent access into a restricted area or through an entry portal. There are two common categories of physical barriers - admission control and perimeter control:
 - **The admission control barriers** are those used at entry points to selectively allow people to pass through. The most common admission control barriers are swing doors, turnstiles, etc. that might be operated mechanically or electronically in conjunction with electromagnetic door locks, keypads, or other entry-point screening mechanisms;
 - **Perimeter control barriers** establish a secure physical boundary around an area, and limit access to and from that area to admission control points (e.g. fences, doors, gates, etc.). They can be constructed from a variety of material, while a common and effective type of physical barrier for perimeter control is chain-link fencing with barbed wire;

- Consequently, the airport operators should ensure that the access to the different areas at airports is controlled to prevent unauthorized entry. The crossing of the barriers by persons or vehicles is established by the airport operator in collaboration with the relevant Civil Aviation Authority and the airport's security department which is a good practice to support airport's security. Access control measures for controlling entry to the secured areas must ensure that: (a) only those individuals authorized to have unescorted access to the secured area are able to gain entry, including visitors provided they are escorted; (b) an individual is immediately denied entry to a secured area when that person's access authority to the area is withdrawn, and; (c) provide a means to differentiate between individuals authorized access to an entire secured area and individuals authorized access to only a particular portion of a secured area;
- Measures for the **screening of persons other than passengers and the examination of vehicles** (vehicles entering critical parts or security restricted areas other than critical parts) should also be defined. Barriers that are not combined with intrusion detection equipment may be vulnerable to attack and unauthorized access if it is not under constant surveillance by security personnel. The suggested measures include among others:
 - Surveillance and patrols;
 - , and other controls including technology using alarms and/or CCTV systems, lighting, sensors to detect climbers or cutting actions, and/or security force personnel such as personnel dedicated to carry out surveillance activities are some indicative measures;
- The **aircraft security check** is the responsibility of the owners or operators. Based on ICAO, each Contracting State shall ensure that aircraft security checks of originating aircraft engaged in commercial air transport movements are performed or an aircraft security search is carried out. A thorough inspection of the interior and exterior of the aircraft for the purpose of discovering suspicious objects, weapons, explosives or other dangerous devices, articles or substances is needed to be conducted;
- Each airport operator should also ensure that the **passengers and their cabin baggage are screened prior to boarding an aircraft departing from a security restricted area**. Airport operators need to address the risk from weapons, explosives in liquid, aerosol or gel form, or any other dangerous devices, articles or substances, which may be used to commit an act of unlawful interference, from being introduced on board an aircraft engaged in civil aviation by implementing the restrictions and the associated measures recommended by ICAO. In addition to this, the commercial air transport operator is normally responsible for ensuring that only items of hold baggage which have been individually identified as accompanied or unaccompanied screened to the appropriate standard and accepted for carriage on that flight by the air carrier, are transported. This type of baggage should be recorded as meeting these criteria and authorized for carriage on the flight. Also, all cargo, mail, and other consumables and supplies must be physically screened before being loaded onto an aircraft. The means of screening include among others
 - security scanners;
 - shoe explosive detection, shoe metal detection;
 - explosive trace detection equipment;
 - x-ray equipment;
 - hand-held metal detectors;
 - walk-through metal detectors;
 - physical searches;
 - advanced cabin baggage x-ray;
 - liquid explosive detection systems;
 - remote explosive scent tracing and free running explosive detection dogs;
 - cargo x-ray screening equipment, etc.
- The security personnel provide all basic security services and **their role is of paramount importance to maintain the best quality of security services**. Their role includes among others

the hold baggage screening, the security screening of all departing passengers and their baggage, the CCTV monitoring, the reporting of incidents, the patrolling of the different airport's areas (e.g. apron, aircraft parking areas, etc.), the control of access to areas at airports in order to prevent unauthorized entry, the response to alarms or unauthorized entry, the initiation of the communications with emergency response personnel in case that it is needed. To that end, their training should be continuous and motivational;

- A **security awareness program** shall be developed for security personnel and for airport employees. A hiring policy should be defined and as such background investigations shall be conducted for new hires and periodic updates for current employees should also be implemented (especially for those with access to secure areas). The security personnel and fast response teams shall have the right equipment at their disposal. For example, a real-time communication system and emergency evacuation and protection systems shall be provided to security personnel to assist them to protect the passengers and employees;
- The measures for handling **special categories of passengers** include among others the requests to allow armed personnel to travel, the measures and procedures to be taken in order to ensure safety on board when passengers subject of judicial or administrative proceedings are obliged to travel, the handling of disabled passengers and patients, etc.

In addition to the aforementioned, an airport like any other CI must provide the required levels of physical security in order to protect people, data, equipment, systems, facilities and company assets in the case of any natural disaster, accidental event, explosion or sabotage. The methods must include among others, the appropriate site design and layout, analysis of environmental components, established physical security program, emergency response readiness, specialized and continuous training, power and fire protection systems, physical controls (e.g. perimeter security, motion detectors, etc.), technical controls (e.g. smart cards for access control, physical security intrusion detection systems, etc.), business continuity or disaster recovery plans to reduce business interruption, suppression systems in order to extinguish heat, oxygen, fuel, chemical reaction, etc. (26). The following Table 2.2 summarises the most common measures discussed in the previous paragraphs.

Table 2.2: Best practices for airport physical security measures and technology solutions

Category	Measures/Actions
Physical (nontechnology) measures	Guards, port gates, fences, barriers, turnstiles, vehicle barriers doors and locks, speed bumps, roadway design, increased gate visibility/detection, perimeter reflectivity and signage, law enforcement or contract personnel continuously patrolling the airports' perimeters and areas, security buffer zones, clear zones for perimeter, inner/outer perimeter roads, name/nomenclature for areas of the perimeter, etc.
Physical (technology) measures	CCTV, video analytics, automated gate barriers, thermal imaging video, radar systems, light detection and ranging systems, passive infrared area sensors, physical and remote sensors, remote power/communications technology, alarms, perimeter intrusion detection systems, access control systems like the mantrap, biometric readers (fingerprint, iris scanners, etc.), fire detection systems/sensors, anti-piggybacking systems, mobile surveillance towers, lighting, badge readers, verification of authenticity by embedding specific technology to badges

Category	Measures/Actions
	(guard against the use of fraudulent credentials), doors with access controls, etc.
Screening of passengers/employees, cabin baggage, hold baggage, cargo, in-flight catering, and supplies	Security scanners, shoe explosive detection, shoe metal detection, explosive trace detection equipment, x-ray equipment, hand-held metal detectors, walk-through metal detectors, physical searches, advanced cabin baggage x-ray, liquid explosive detection systems, remote explosive scent tracing and free running explosive detection dogs, cargo x-ray screening equipment, etc.
Operational efforts	Police presence (either stationed or patrols), K-9 teams (police dogs) anti-terrorism teams (covert and overt elements), mobile explosives detection screening teams, visible intermodal prevention and response teams, security awareness (e.g. training, exercises), unpredictable police patrols, routine security inspections, routine patrols (by the asset owner), monitor security cameras, security drills and exercises, etc.
	Aviation security personnel and airport employees need to be carefully selected and properly trained and supervised to ensure that they are consistently able to carry out their duties in a highly proficient manner. Pre-employment background checks are needed, and specific security training of aviation security personnel should be in place. Airport operators should develop, execute, and perform routine training and security awareness programs for their personnel, including methods for the identification of suspicious persons, awareness of their responsibilities, the security procedures, and the relevant contacts.
	An airport security programme (ASP) must, among other things, provide for the safety and security of persons and property on an aircraft against an act of criminal violence, aircraft piracy, and the introduction of an unauthorized weapon, explosive, or incendiary device onto an aircraft. Airports need to implement and maintain quality controls in their airport security programme to determine compliance with and to validate the effectiveness of the programme.

In order for airports, and CIs in general, to (a) prevent or at least reduce unauthorized access, use, disruption, information deletion, personnel and data corruption etc.; (b) respond effectively, timely and efficiently and; (c) minimize the impact of cyber-attacks to their network, information technology and systems, it is important to take both organisational and technical measures, as analysed below:

- **Organisational measures** might include (a) the assessment of cyber risks, which is used to identify, estimate, and prioritize risk to organisational operations, organisational assets, individuals, other organizations, and the Nation, resulting from the operation and use of information systems (27); (b) development and adoption of both generic and case specific

laws, standards, plans and policies that outline cybersecurity measures and crisis management procedures, and; (c) personnel training on cybersecurity protection and crisis management issues, standards, plans and protocols;

- **Technical measures** adopted, include among others the following: authentication, access control (authorization), data confidentiality and integrity, backup, tracing systems, log files, communication security, firewalls, traffic monitoring systems, etc. A security by design approach should complete the aforementioned countermeasures, focusing on the cybersecurity aspects for new devices or systems that need to be planned and implemented already from the beginning, meaning the procurement, design, development and maintenance phases. For securing networked devices and assets inventories should be created and maintained, as they can ensure a sound understanding of the systems and their components; support configuration and automated remediation management processes (28) and software should be regularly patched and updated. In addition, it is also crucial to have a clear understanding of actual cybersecurity strategies and controls implemented at targeted infrastructures, such as the passenger data records, flight display system, etc.

Airports, based on their functionalities and regulatory frameworks (as explained above), adopt several security related operations centres, given that any damage to their infrastructure, its destruction or disruption by natural disasters, manmade events or technological accidents, may have a significant negative impact for the security of the EU and the well-being of its citizens. In addition to the previous and in order to deal with security issues on an organisational and technical level, airports have different operation centres incorporated in their facilities to safeguard them in their daily routine. The Security Operation Centre (SOC) is a generic term describing part of or the whole platform whose purpose is to provide detection and reaction services to security incidents (29). SOC monitors the security level of an organisation on an ongoing basis and comprises a security team using various technological solutions in order to oversee security operations and to collect data and syslog to detect, identify, analyse, investigate and report cybersecurity incidents. SOC architecture models can differ based on airport's needs and preferences. There are dedicated or internal SOC (team within organisation), virtual SOC (team works remotely), and co-managed SOC (internal IT collaborating with outsourcing vendor). The Emergency Operations Centre (EOC) is a facility operating to manage disaster emergencies. It is the place where information management, allocation and coordination of resources, and recovery actions take place. The Network Operations Centre (NOC) manages, controls, monitors and maintains the network functionality and operations across various platforms, media and communication channels (internal or external). The AOC incorporates a selection of the centres (including the previous ones) based on the operational needs of each airport. AOC constitutes an operational management structure that allows a common operational view to airport stakeholders in order to communicate, collaborate, coordinate and decide on the progress of airport operations.

In case of a physical, cyber, cyber-physical security incident the SOC operators should detect the security incident and immediately inform the AOC which is the focal point for information collection and sharing once an incident is declared. Depending on the nature of the attack, the required stakeholders are determined, and the response and recovery measures are decided.

2.6.3 Crisis management process and involved stakeholders

Crisis management has been defined as “the developed capability of an organisation to prepare for, anticipate, respond to and recover from crises” (30). The full cycle of crisis management can be described in four phases (preparedness, response, recovery, mitigation), each with several steps following (see 2.6.5). The steps have been presented in detail in deliverable D7.7 “Specification of a holistic security management cycle” (5), and have been linked with the different internal and external airport stakeholders and the security coordination and operational centres. Within these steps, the several internal and external stakeholders involved, have different needs and requirements, trying to

cooperate, respond and recover from the crisis. Security stakeholders can be categorized according to their involvement and perceived proximity to the organisation into internal and external. Based on a literature review and information collected from the participating airports, the internal stakeholders and their role have been described in detail in D7.7 and are the following:

- Board of Directors (BoD);
- Data Protection Officer (DPO);
- Crisis Management Team (CMT);
- emergency response team;
- physical security manager/personnel;
- IT security manager/personnel;
- technical manager/personnel;
- health and safety manager;
- Airport Duty Officer (ADO);
- Crisis Management Centre (CMC);
- AOC;
- EOC/Emergency Operations Team (EOT);
- SOC /security services department;
- media centre;
- friends and relatives' assistance centre.

The external stakeholders' category includes individuals or groups outside the organisation who can affect or can be affected by a security incident in the airport, as they are conjoint into an interdependent relationship, namely:

- Law Enforcement Agencies (LEAs);
- fire brigade;
- emergency medical services;
- civil protection;
- national authorities (prefectures, municipalities, etc.);
- ministries (e.g. energy, transport, health, etc.) together with respective divisions, such as the National Cyber Security Authority (NSCA) of the Ministry of Digital Governance in Greece;
- national intelligence agency;
- national data protection authority;
- interconnected/interdependent CIs (e.g. power, communication, surface transportation);
- Computer Emergency Response Team (CERT);
- Computer Security Incident Response Team (CSIRT);
- International and EU Organisations (e.g. ICAO, EASA, EUROCONTROL);
- Air Accident Investigation and Aviation Safety Board (AAIASB);
- Civil Aviation Authority (CAA)/Aviation Authority;
- Air Traffic Control (ATC) (e.g. ENAV);
- information security service providers;
- passengers;
- telecommunication providers;
- airlines, ground handlers;
- cargo, concessionaires, etc.

2.6.4 CIs security management gaps and best practices

Standardization of safety and security procedures has followed a sectoral approach while its maturity varies according to the criticality of the services provided. Thus, security management in the airports complies with international guidelines and standards (e.g. ICAO).

The European Commission paved the way to integrate the management of the security of the ECIs through the EC Directive 114/2008, which was transferred to the national legislation of the member states since 2010. However, this directive addressed only the transport and energy sector and focused mainly to the threat of terrorism. Furthermore, the interconnection and interdependencies of the infrastructures have not been included at all as a systemic element of CI protection. Most of these challenges are planned to be addressed in the new relative directive, currently under elaboration.

Based on the work conducted in SATIE, reports on security management and the relevant experience of the Center for the Security Studies (KEMEA) in the field of CI protection as the national contact point in Greece regarding European CIs the following gaps have been identified with regards to the management of crisis and security as a whole:

Gap #1. Different physical, cyber and/or physical-cyber security solutions implemented in different infrastructures: Among airports, there is a lack of uniformity in the adoption and implementation of solutions that can support and enhance crisis management processes. This can trigger many inconsistencies and problems during a crisis that demands the cooperation among different infrastructures.

Gap #2. Decentralised control and collection of information: According to current standard practices, multiple decentralised information gathering processes 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.

Gap #3. Lack of fast communication and information dissemination: Airports, 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 among interconnected CIs.

Gap #4. Underestimating the complexity of predicting the potential impact of an incident: a) within the airport (i.e. fire propagation, terrorist attacks, plum dispersion, impact of toxic chemicals, radioactivity etc.), and b) among interconnected CIs, as disruptions in one sector can have cascading effects in other sectors, including cross-border.

Gap #5. Crisis management process understanding: Although the crisis management process is well analysed in the literature there is a need for airports to better understand the process, as well as to identify the involved stakeholders.

Gap #6. Lack of training and exercising in crisis management: Although continuous training is needed to enhance readiness and cooperation to respond to any type of complex incidents and emergencies, there is a lack of common continuous training of all involved stakeholders.

Gap #7. Different or no security plans within each airport: Standards and guidelines for the implementation of comprehensive plans for the security of an airport are needed at a national level (and if possible per CI sector) in order to build a common ground for all airports and CIs. 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 operations and business continuity management.

Despite the presented gaps, it appears that there are some **best practices** applied and used by the airports, as follows: (a) Airports have regulatory authorities/bodies that work with Member States and industry groups to reach consensus at international Standards and Recommended Practices (SARPs)

and policies in security issues **(related to Gap #5, #6 and #7)** (see deliverables D7.6 (22) and D7.7 (5)); (b) Airports use advanced physical and cyber integrated security solutions (e.g. metal detectors, x-ray, etc.) **(related to Gap #1, #2 and #3)** (see deliverables D7.6 (22) and D7.7 (5)) and; (c) In order to deal with security issues, airports have incorporated in their structure different operation centres, e.g. AOC, SOC, in more structured and detailed way than other CIs (e.g. hospitals) **(related to Gap #2, #3, #4 and #5)** (also see SATIE deliverable D7.7 (5)).

2.6.5 Proposed holistic crisis management process

Based on the consideration of the airports' security related issues, the gaps, the respective existing regulation (i.e. NIS Directive and NIS 2 Directive proposal) and best practices described in the previous paragraphs, the following mandatory requirement and additional recommendations are presented that are capable of enhancing airports' crisis management process, but also security as a whole:

Requirement. Airports need to develop security plans and implement integrated cyber and physical security solutions (at a minimum common level depending on their needs) to protect their critical assets across their infrastructure **(related to Gap #1 and #7)**.

Recommendation #1. Airports should integrate in their organisational structure a Holistic Security Operation Centre (HSOC) to detect, analyse, and manage cyber and physical attacks and to efficiently coordinate processes, people and technologies. Thus, a common operational picture will be achieved, and efficient information sharing will be facilitated, in order to alert operators and involved stakeholders to any potential threats or incidents **(related to Gap #2 and #3)**.

Recommendation #2. A common cyber-physical crisis management process should be established and followed within each CI and at Member States level **(related to Gap #5)**. In the following subsection, a global cyber-physical security management approach that addresses the aforementioned challenges, is presented. The proposed approach will facilitate the communication and cooperation between the different airport operators and stakeholders, in case of an incident, and enhance security of CIs.

2.6.5.1 Global cyber-physical crisis management process

As already discussed, a cyber, physical and cyber-physical crisis management process should be established and followed within each airport and at Member States level. This process consists of four phases (preparedness, response, recovery, mitigation), with several steps (see Figure 2.1). More detailed description of the process is presented in (16).

Preparedness: The aim of this phase is to prepare airports and CIs and develop general capabilities that will enable them to deliver an appropriate response in any crisis. It is a continuous cycle of planning, organizing, training, equipping, exercising, evaluating, and taking corrective actions that internal and external stakeholders should follow closely to ensure readiness. In this sense, it is important for an airport to know which assets are vital for conducting their core activities, the potential threats against these assets, as well as their vulnerabilities. For this phase, appropriate institutional structures, supported by comprehensive policies, plans and legislation and the allocation of resources for all these capacities through regular budgets are also instrumental for thorough preparedness to crisis **(Step 1 – Develop plans)**. To improve the efficiency of the CI the appropriate tools must be in place **(Step 2 – Organise and equip)**. Training and exercising are the cornerstones of preparedness which focus on readiness of all involved stakeholders **(Step 3 – Train and exercise)**.

Response: Response initiates when an incident is detected by an internal or external stakeholder or the Holistic Security Operation Centre (HSOC for physical and cyber incidents), in a manual or automated way (e.g. monitoring networks and early-warning systems, public authorities, citizens, media, private sector, etc.) **(Step 4 – Incident detection)**. Depending on the type of the incident (cyber and/or physical) different stakeholders will collect the information needed for further investigation. **(Step 5 – Information gathering)**. The information should be collected and assessed by the CMT in

cooperation with relevant stakeholders that identified the incident (**Step 6 – Incident assessment**). The CMT should assess the extent of the crisis, evaluate the situation, determine, and define which response plan(s) should be activated (e.g. evacuation plan, etc.), inform the HSOC, which in its turn will communicate it to internal stakeholders and through the AOC to external stakeholders. Based on the activated plans, response processes and procedures are executed, co-ordinated and adapted (**Step 7 – Determine plan**). It is also crucial to know the availability and current status of resources, in order to allocate them efficiently (**Step 8 – Resource management**). HSOC is also responsible for communicating in timely and accurate manner information to internal stakeholders and to the AOC (**Steps 9 - Communication & 10 – Decision implementation**). The aforementioned steps could be repeated, until processes and assets return to business as usual or to another accepted status (demobilization) and the crisis is terminated. Demobilisation will be communicated by BoD and CMT coordinator to HSOC, which in its turn will communicate it to internal and external stakeholders (**Step 11 - Demobilisation**).

Recovery: When crisis occurs, airports must be able to carry on with their tasks during crisis, while simultaneously planning on how they will recover from the damage the crisis caused. Undeniably, required actions to return to normal operations and limit damage to the infrastructure and involved stakeholders continue after the incident or crisis. The CMT should decide the recovery actions to be taken (based on recovery plans), by cooperating closely with the HSOC, AOC, as well as internal and external stakeholders (**Step 12 – Recovery actions**). The CMT should collect and analyse evidence from the incident (**Step 13 – Collect and analyse**); and then should create an evidence report (**Step 14 – Create evidence report**). The CMT in cooperation with its coordinator should share relative information with all internal (**Step 15 – Share relative information with internal stakeholders**) and external stakeholders (e.g. Ministries, LEAs, fire brigade, interconnected CIs). Moreover, related investigations should be assisted (**Step 16 – Share relative information with external stakeholders**). As a crisis serves as a major learning opportunity, stakeholders should review the overall process as well as plans, procedures, tools, facilities etc., and identify areas for improvement (**Step 17 – Review incidence response**). Following the evaluation, lessons learnt should be identified (**Step 18 - Debriefing**) and recommendations/revisions should be made to relevant plans, and processes (**Step 19 – Update plans**).

Mitigation: Mitigation refers to the process of reducing or eliminating future loss of life/injuries, assets and operations resulting from threats/risks through short and long-term activities. The results of the evaluation of the response actions should lead to recommendations for change, responsibilities allocation and relevant timelines in order to ensure that it will be carried out (**Step 20 – Take mitigation measures**).

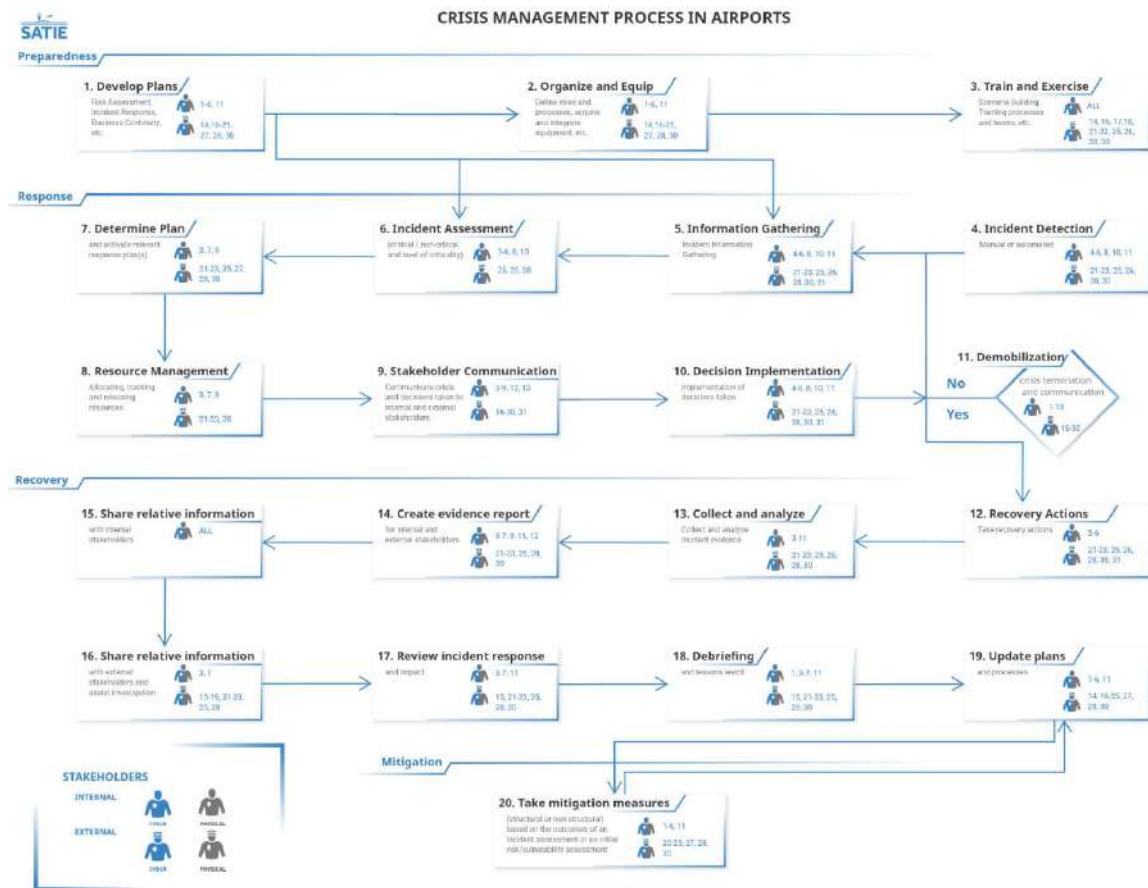


Figure 2.1: Common and holistic security and safety agenda

3 Standardization activities

In the previous chapter 2, best practices and recommendations for improving airport security standards and policies have been identified and proposed considering the project's lessons learnt from technical, operational and organisational perspectives. To ensure that all relevant aspects are covered:

- the SATIE consortium should establish relationships with standardisation bodies to foster knowledge exchange and promote the SATIE results;
- the SATIE demonstrators (AIA, ZAG, SEA) should further scrutinize their internal security policies towards the produced risk results and the emerging security challenges on airports CIs.

As part of collecting feedback from the standardization activities, the SATIE consortium prepared a report on the main outcomes of the projects, their innovative aspects and characteristics and a set of recommendations, guidelines and lessons learnt for improving aviation security which was submitted to a number of standardization bodies, policy makers and other external groups.

As regards the exploration and analysis of the SATIE impact on airports stakeholders' internal policies and operations, the SATIE consortium conducted a Practitioners' Workshop engaging airport demonstrators' stakeholders. In addition, dissemination activities among policy makers and airport stakeholders were organised to enhance the SATIE promotion.

Section 3.1 describes the survey strategy that was adopted to capture feedback from the standardisation bodies, policy makers and some external groups. Section 3.2 reports all the activities implemented to establish communication channels with standardisation bodies and retrieve security knowledge (SATIE Practitioners' Workshop) and all activities carried out to expand SATIE dissemination (SATIE Awareness Events). Section 3.3 presents the evaluation results gained from the SATIE Practitioners' Workshop and the feedback retrieved from the standardisation bodies.

3.1 Survey strategy and setup

The strategy of collecting feedback about SATIE results from the standardisation bodies and NIS stakeholders, other external groups and communities, as well as European airports and relevant security practitioners, have followed the steps proposed below:

- A. Feedback from the standardization bodies (steps 1 and 2):
 1. The initial draft of the D7.3 has been provided to standardization bodies;
 2. The received input from the standardization bodies was included in the second iteration of D7.3;
- B. Second draft of D7.3 and survey (steps 3 and 4):
 3. The provided input (item 2.) was used to setup the survey strategy (decision about method: survey vs. guided interview), as well as specific questions, based on the second draft of D7.3;
 4. The updated version of D7.3 was sent to security practitioners;
- C. Dissemination (steps 5, 6 and 7):
 5. Workshop with security practitioners was held;
 6. Survey with security practitioners was conducted during the workshop;
 7. The results were analysed and incorporated into this final version of D7.3.

3.2 Participation to standardization activities and workshops

SATIE partners (AIA, ZAG and SEA) organized multiple events with airport stakeholders (e.g. airports, police, firefighters, red-cross and other first responders) to refine the impact of the new security solution on their internal security policies and disseminate the SATIE Solution to airports stakeholders.

The current section enlists these workshop/event procedures and additional activities carried out by the consortium partners in the field of airport and aviation security as a means of establishing communication channels with Standardization Bodies and other external groups.

3.2.1 SATIE's Awareness Events with stakeholders

Close to the end of the year 2020, the SATIE Consortium has organized its first Awareness Event. The goal of this event was to introduce the SATIE Solution to the industry and regulatory bodies, and engage in open discussion with them. This represented an opportunity to demonstrate the solution in action, highlighting its benefits for airports across Europe. Some of the tools available for the SOC operators were shortly introduced by their developers, and afterwards exemplified with the help of two dedicated SATIE scenarios videos.

This event gathered more than 70 professionals in total. Among these, guests from EDA, EASA, ENISA, DG JRC, DG HOME, DG Connect, EUROCONTROL, SESAR JU, and many other stakeholders were present. With such an extensive number of experts, the discussion was highly valuable for all the participants. The involved parties have expressed challenges, concerns and advantages of developing, integrating and using such a solution to help at securing the critical air transportation infrastructure of Europe. This represented the initial step in integrating the feedback received into the development of the SATIE Solution.

On the 23th September 2021, the SATIE Consortium conducted the second Awareness Event. It aimed at gathering entities external to the project, directly or indirectly linked with the airport's environment, engaged professionals from different areas of expertise (e.g. management/operational/security background, etc.) to open discussions about the strong need for cyber-physical security improvement on CIs and exhibit the SATIE Solution and its Innovation Elements (IEs) to raise the audience awareness about the approach that SATIE undertakes and the way forward.

The 2nd Awareness Event was an all-day event undertaken entirely online due to COVID-19 related issues. It was attended by more than 55 people online. The event was chaired by the Project Coordinator from DLR. During the Awareness Event, an overview of the SATIE Solution was presented, and the motivation behind the SATIE project was highlighted. Moreover, the SATIE innovations achieved so far were showcased, highlighting the progress that had successively been made for the SATIE cyber-physical toolbox through the project's lifespan.

The latter Awareness Event was a great opportunity to discuss the technical aspects of the SATIE Solution and the corresponding applied technologies under the scope of enhancing the exploitation and uptake of the project. In this regard, representatives from other European projects as well as external security stakeholders attended and contributed to the discussions communicating their knowledge. Furthermore, the SATIE demonstration activities were illustrated through a representative video performance for each airport scenario which underlined how the SATIE Solution can be beneficial to the European airports. The conduction of the second Awareness Event a month before the end of the project gave SATIE the chance to disseminate the project results at their last stage and expanded stakeholders' knowledge on security solutions for airport CIs protection. Figure 3.1 illustrates an indicative screen of the SATIE Awareness Event.

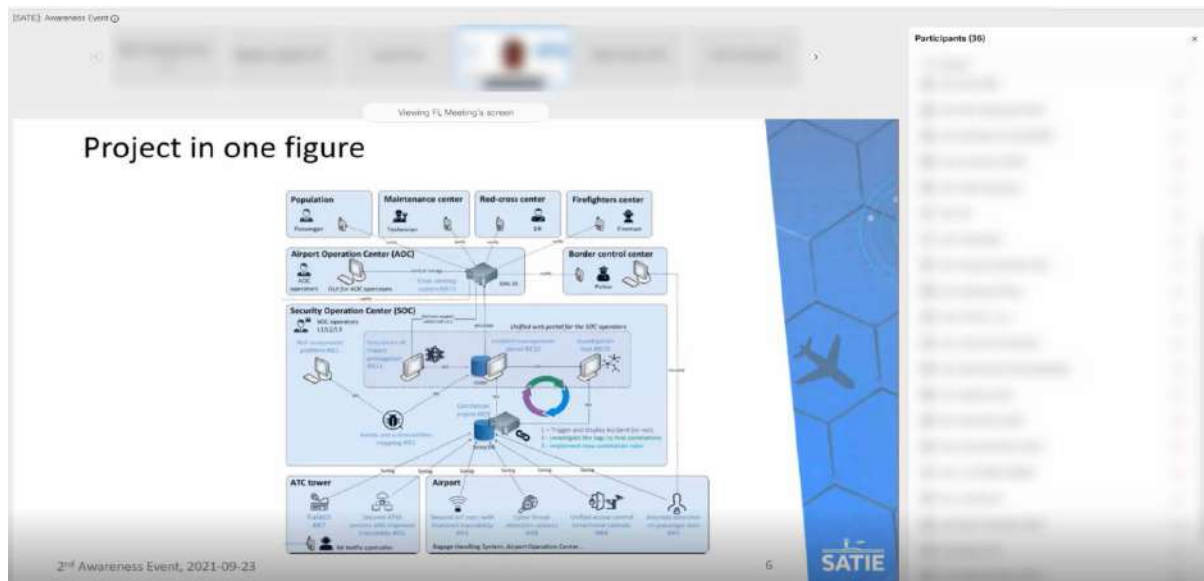


Figure 3.1: Screenshot from the SATIE Awareness Event

3.2.2 Organization of the SATIE Practitioners' Workshop

On the 24th September 2021, the SATIE Consortium organized an all-day virtual workshop (as a result of COVID-19 associated issues) which was dedicated to practitioners of the three airport demonstrators AIA, ZAG and SEA (i.e. first responders, such as airports, police, red-cross, fire brigade, civil protection, etc). The workshop was chaired by the Project Coordinator from DLR. It was attended by 41 people during the entire duration of the event. The ultimate scope of this workshop was to refine the impact of SATIE Solution, and its state-of-the-art IEs on the practitioners' internal security policies.

With this purpose, the workshop was divided into two parts: a joint session and a breakout session. During the joint session, the SATIE project was introduced and the SATIE Solution was demonstrated to raise the awareness of the audience on SATIE. In this respect, a short description of the SATIE demonstration scenarios was undertaken. It illustrated how the SATIE IEs have been involved in each scenario and triggered the audience attention with challenging test cases to show SATIE Solution's applicability in real airport environments and its capability to tackle attacks, detect, respond and mitigate threats to the protection of CIs and people's safety. The following Figure 3.2 depicts a screenshot from the SATIE Practitioners' Workshop.

[SATIE] Practitioner's Workshop

Viewing FL Meeting's screen

Agenda for today (Times are given in CEST)

Time	Item	Lead
09:45 – 10:00	Welcome	
10:00 – 10:10	SATIE project at a glance	DLR
10:10 – 10:30	SATIE Solution as a whole	DGS
10:30 – 11:30	SATIE Demonstration Scenarios	DLR
11:30 – 11:45	Coffee Break	
11:45 – 12:45	SATIE Solution demonstration	AIA / ACS / All technical partners
12:45 – 13:00	SATIE Questionnaire	Online
13:00 – 14:00	Lunch break	
14:00 – 15:00	Round Table discussions in native language	
15:00 – 15:15	Break	AIA / KEMEA / SEA / ZAG
15:15 – 15:45	Debrief & Evaluation	
15:45 – 16:00	Wrap up – Closing	DLR / all partners

Figure 3.2: Screenshot from the joint session of SATIE Practitioners' Workshop

The breakout session targeted into initiating national round tables discussions of the three SATIE demonstrators in their native language with a mission to:

- Discuss the SATIE Solution towards cyber and physical security in their daily work;
- Receive practitioner individuals' feedback against the need to improve security (recognize areas of interest);
- Identify gaps and vulnerabilities in their daily systems, processes and operations;
- Delve into the SATIE Solution and its accompanying tools and express their opinion and further argue whether they can assist to fill the perceived gaps and limit the identified vulnerabilities.

To better drive the national discussions on the above topics, a questionnaire template for all national practitioners was prepared and translated into the three demonstrators' native languages: Greek, Croatian, Italian. This questionnaire enabled the performance of semi-structured guided interviews to the practitioners, to gather more easily input concerning their technical environments and security specificities in their normal operations. Figure 3.3 below, displays a screenshot from the national round table discussions operated during the workshop's breakout session.

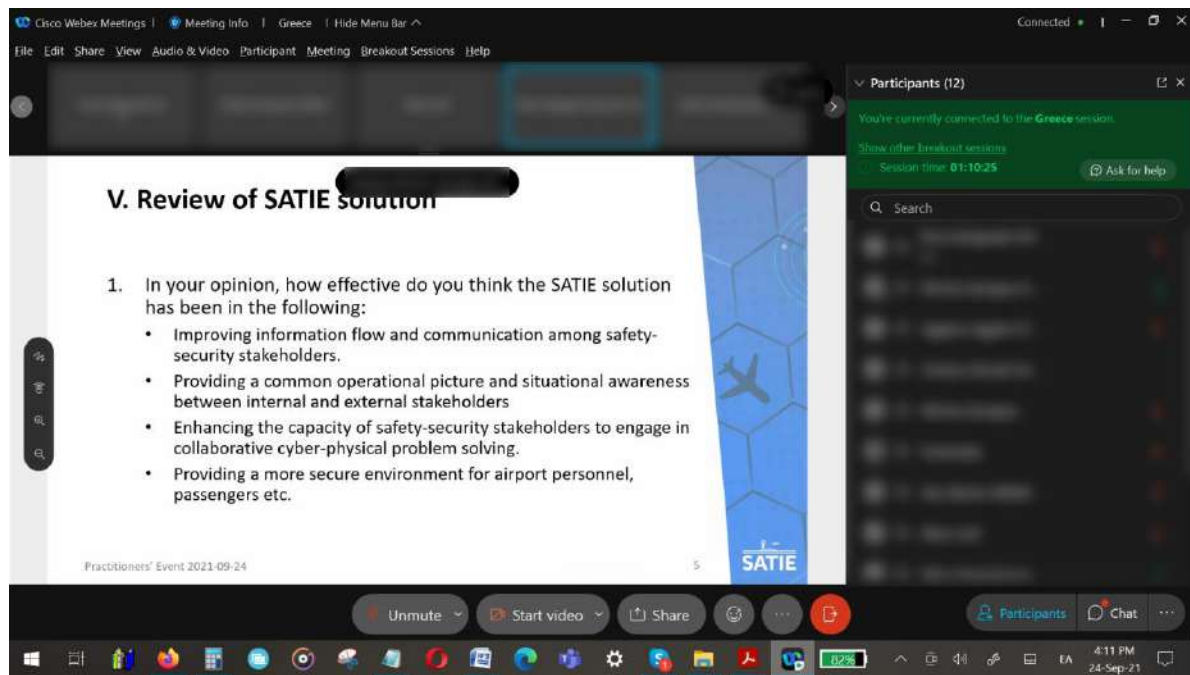


Figure 3.3: Screenshot during a demonstrator's national breakout session of the SATIE Practitioners' Workshop

Concerning the Greek airport's invitees, KEMEA communicated the Practitioners Workshop event to a considerable number of end-users (i.e. police, fire brigade, civil protection, Red Cross, Hellenic Cyber Security Incident Response Team - CSIRT) and motivated them to participate in the workshop. Representatives from the aforementioned organisations participated in the event. In particular, AIA and KEMEA conducted a Greek round table discussion with thirteen participants upon whom five were security practitioners or other airport stakeholders. During this national discussion several topics were raised, such as the importance of impact assessment results interpretation on operational level, the need to enhance crisis management procedures with proposed run books, action plans and guidelines and respective flowcharts to boost the user's efficiency when implementing allocated tasks, etc. The discussed topics are further analysed in section 3.3.2.1.

With the aim of presenting the SATIE project to professionals and getting valuable feedback from them, ZAG invited eighteen esteemed colleagues to the Practitioners Workshop. Although it was not an easy task to organize such an all-day event, six of them found the time to connect and participate as much as possible. This can be considered as a good response given that, as is well-known, airports are extremely dynamic environments where day-to-day business comes as a priority.

They had the opportunity to talk to airport's security compliance manager and security operators, Fire-Fighting unit commander, Safety Manager and IT security officer. Informal interviews were subsequently conducted with medical experts from airport's ambulance, subcontracted physical and technical protection service provider, police shift manager and airport operations director. The data thus collected was combined with feedback received during the actual workshop, which gave the event wider meaning and became complete. Further details are presented in section 3.3.2.2

SEA coordinated the Italian round table discussion. There were close to fourteen both internal and external people, with key-role participants in the airport's security environment (e.g. member from Malpensa Users Committee, the Head of Security, etc.). Within the Italian session, a set of topics were discussed in relation to the practitioner's questionnaire. For instance, the importance of utilizing AI-based mechanisms in threat detection to allow real-time reaction in an automated manner to the occurrence of threats in accordance with SATIE valuable response in terms of collecting and correlating events in real-time. Further topics discussed are described in detail in section 3.3.2.3.

At the end of these national breakout sessions, there was a final debrief and evaluation session where project demonstrators' representatives summarized what were the main findings from these prosperous discussions.

3.3 Evaluation feedback

During the SATIE Practitioner's Workshop, a survey was conducted with the security practitioners and evaluation results provided by the workshop attendees' evaluation questionnaire responds from and by semi-structured guided interviews that were taken over during the national breakout sessions of the three airport demonstrators. Section 3.3.1 presents and analyses the evaluation results arising from the filled evaluation questionnaires, whereas section 3.3.2 reflects in detail the results obtained from the national sessions of the SATIE Practitioner's Workshop.

3.3.1 Evaluation results of the SATIE Practitioners' Workshop

This section aims to imprint the evaluation results derived from the questionnaires responders during the SATIE Practitioner's Workshop. In particular, an evaluation questionnaire was available online for security practitioners' attendees of the workshop during a respective session that was devoted within the workshop. The content of this evaluation addressed the SATIE Solution and its Innovation Elements (IEs), as well as additional questions, were raised in general subjected to airports CIs, airports' security requirements and security plans and policies that are either adopted or needed to enhance airports security and resilience. The ultimate purpose of this feedback was to evaluate the SATIE results, and to refine the impact of the SATIE Solution towards the specific implemented security policies of the airports' stakeholders.

The current evaluation questionnaire was an enhancement of the evaluation questionnaire that was disseminated during the airports' demonstrations, which results are reported in SATIE's demonstration report deliverables (D6.4 (31), D6.5 (32) and D6.6 (33)). This questionnaire's responders were totally different than the demonstration questionnaire participants, allowing us to ensure an un-biased opinion over the SATIE Solution. Questions pertinent to parts of the SATIE Solution not shown during the demonstration have been omitted from the questionnaire. During the event, only participants external to the project and with no connection to the SATIE project were asked to answer the questionnaires. More specifically, there were nine participants that filled the evaluation questionnaire, four of them deriving from the security industry domain, three of them were from Law Enforcement sector, one coming from the Emergency Management domain and one was a representant of the Operator Users' Committee.

The evaluation questionnaire incorporated the following topics:

- Actions considered necessarily to enhance the airports' resilience;
- Whether there are any endorsements to the SATIE Solution, including its IEs, and potential further comments;
- A statement-based list of questions addressing airports security requirements, security policies of airports' stakeholders, and the overall SATIE Solution feedback.

Further on, the tables reflecting the results from the answers gained from the nine participants according to the topics abovementioned are depicted.

Table 3.1: Results of the responders to questions related to actions considered necessary to enhance the resilience of airports and CIs

Question	"Which actions do you consider as necessary to enhance the resilience of airports / CIs?"
Pool of answers	No. of replies in agreement with the respective answer
Continuous training of personnel	9
Enhancement of cyber and physical measures combination	7
Additional exercises	5
Common security plans	5
Enhancement of physical measures	4
Enhancement of cyber measures	4

According to Table 3.1, actions to enhance the airports/CIs resilience: 9 out of 9 responders agreed that continuous training of personnel is required, 7 out of 9 responders positively replied that enhancement of cyber and physical measures combination should be provided, 5 out of 9 responders agreed with their answers that additional exercises are needed, 5 out of 9 responders positively replied that common security plans are required, 4 out of 9 responders agreed that enhancement of physical measures should be considered and 4 out of 9 responders agreed with their answers that enhancements of cyber measures should be undertaken. The default questions on actions to enhance the airports/CIs resilience, presented in Table 3.1, are ordered according to their importance for the responders. As it is shown from the results gained, the most important action unanimously answered from the responders to improve airports/CIs resilience is the continuous training of personnel, whereas enhancement of physical measures and cyber measures separately assessed as the less important.

Table 3.2: Endorsements by the responders on the SATIE IEs

Question	"Which of the Innovation Elements stood out for you and why?"	
Innovation Element	Frequency	Reasons
Incident Management Portal (IMP)	6	Integration from different tools; The direct information of this tool was very usefull.
Crisis Alerting System (CAS)	4	Innovatively easy to communicate with SOC.
Business Impact Assessment (BIA)	3	A blocked threat is a non-quantifiable gain.
Malware Analyser	3	
Anomaly Detection On Passenger Records (ADPR)	2	
Application Layer Cyber Attack Detection (ALCAD)	1	
Correlation Engine	1	Flexible usage for relegato alert about different threats.
CyberRange	1	
Investigation Tool (SMS-I)	1	
Traffic Management Intrusion and Compliance System (TraMICS)	1	

Table 3.3: Additional endorsements by the responders on the SATIE Solution

Question	"Is there anything else you would like to mention about the SATIE Solution?"
Comment	SATIE Solution could be deployed on other CI sectors already existing inside aviation domain (energy, cargo, Maintenance, etc.) or outside, but involved with it.

Table 3.2 and Table 3.3 highlight the endorsements provided by the responders on the overall SATIE Solution and the SATIE IEs respectively. One participant went beyond a simple answer and suggested that the "SATIE Solution could be deployed on other CI sectors that already exist either inside the aviation domain (such as energy, cargo and maintenance, etc.) or outside, but they are involved with it". Table 3.2 depicts the responders endorsements on the following SATIE IEs: Anomaly Detection on Passenger Records (ADPR), Traffic Management Intrusion and Compliance System (TraMICS), Malware Analyser, Application Layer Cyber Attack Detection (ALCAD), Correlation Engine, Investigation Tool (SMS-I), Business Impact Assessment (BIA), Incident Management Portal (IMP) and Crisis Alerting System (CAS), which are analytically presented in the SATIE Training Handbook, D7.2 (1). Table 3.2 depicts the SATIE IEs evaluation results in a hierarchical manner according to which SATIE IE stands out mostly for the airports stakeholders' responders. The results show that IMP is the most supported SATIE IE (with 6 out of 9 positive replies) that meets their needs, followed by CAS (with 4 out of 9 positive replies). The Malware Analyser and ADPR were equally supported (with 3 out of 9 positive replies), followed by ADPR (with 2 out of 9 positive replies). Eventually, the Correlation Engine, CyberRange, SMS-I and TraMICS were equally supported (with 1 out of 9 replies). Additional feedback was received from responders justifying their answers. Moreover, IMP was characterized that is on their highest priority as they find very useful the information delivered from this IE, which provides integration from different tools. CAS was commented to be innovatively easy to communicate with stakeholders. Regarding BIA, responders added as a comment that a blocked threat is a non-quantifiable gain. Concerning the Correlation Engine IE, responders stated that it has a flexible usage in presenting alerts raised on different threats. The free additional comments field was completed by one participant which encouraged the deployment and adaptation of the SATIE Solution to other Critical Infrastructures domains, positively strengthening the benefits and the added value this solution brings to the CIs protection.

Table 3.4 shows the results of questions asked to the practitioners. The participants had to agree or disagree to statements given to them with the option to omit answers. This resulted in different numbers of responders for each question (from N=7 to N=9).

The first questions dealt with the current status and shown satisfaction with the state-of-the-art. However, the results also showed the wish for a common cyber-physical crisis management process which should be established and followed within each airport/CI and at Member States level. Furthermore, statements about the ease of predicting the potential impact of incidents within the airport and among interconnected CIs received lower agreements than other statements. Additionally, a very high agreement to positive statements about the SATIE Solution have been received, proving that the SATIE Solution is really addressing the right issues. The questions asked during this workshop were an adapted and extended set of the ones presented to the simulation validation participants and to the participants at the Athens, Zagreb and Milan demonstrations. This offered the opportunity to compare the results and simultaneously enrich the gathered data by additional information. Even though the participants were different regarding their operational background and experience, the responses received were similar. The results from demonstrations, simulations and from this workshop were strikingly similar despite the different scenarios presented and the different participants. This strengthens the assumption of representativeness of the results and is an indication of the validity and reliability of the obtained results. Operational experts trained to use the novel SATIE Tools, and security experts just observing the demonstration attack scenarios and the actions of SATIE Tools

operators as well as the practitioners attending this workshop evaluated the SATIE Solution very positive. The similarities of answers and the positive feedback in the different groups of participants are an encouraging reinforcement of the SATIE Solution benefits.

Table 3.4: Evaluation questionnaire statements overview

Statement	Mean	SD ¹	N ²
The current design for the safety and protection of the airports/ CIs take into consideration the combination of cyber and physical threats.	5.56	2.07	9
The security plans should include integrated cyber- and physical-security solutions.	6.00	1.94	9
There is a need for a Holistic Security Operation Centre (HSOC) able to detect, analyse, and manage cyber and physical attacks.	1.94	1.94	9
A common cyber-physical crisis management process should be established and followed within each airport/CI and at Member States level.	6.33	1.66	9
The current security plans as well the crisis management process to be followed is well understood by the involved parties .	5.44	1.94	9
The roles and responsibilities of those involved during an incident are well defined.	5.67	1.87	9
During an incident there is a single coordination point acquiring the complete set of collected data for feeding it to internal and external stakeholders.	5.44	2.01	9
During an incident the information needed is effectively and efficiently managed and shared in different layers and between the internal and external stakeholders.	5.44	1.81	9
It is easy to predict the potential impact of an incident within the airport (i.e. fire propagation, terrorist attacks, plum dispersion, impact of toxic chemicals, radioactivity etc.)	4.56	2.07	9
It is easy to predict the potential impact of an incident among interconnected CIs	4.78	2.05	9
There is continuous training to enhance readiness and cooperation in order to respond to any type of complex incidents and emergencies.	5.67	1.50	9
The SATIE Solution is overall a significant improvement compared to current security-monitoring systems.	6.00	2.07	8
The SATIE Solution is an excellent way to monitor and raise security alerts.	6.13	1.73	8
The SATIE Solution provides all relevant information.	5.75	1.67	8
The SATIE Solution enables a faster detection of cyber threats compared to current systems.	5.75	2.05	8
The SATIE Solution enables a faster detection of physical threats compared to current systems.	5.88	2.10	8
The SATIE Solution enables a faster response to cyber threats compared to current systems.	6.13	2.10	8

¹ SD = Standard Deviation² N = Number of Participants answering the question about the respective statement

Statement	Mean	SD ¹	N ²
The SATIE Solution enables a faster response to physical threats compared to current systems.	6.00	1.69	8
The use of the SATIE Solution increases the efficiency compared to current systems.	5.63	2.00	8
I think that it will be easy to integrate the SATIE Solution with the necessary airport systems.	5.63	1.60	8
The SATIE Solution is innovative compared to others on the market.	5.60	2.07	5
I think the SATIE Solution will boost airports' revenues.	5.14	2.12	7
I think airports will like to secure their systems with the SATIE Solution.	5.29	1.98	7
I think that the shown scenario(s) were suitable to illustrate the SATIE Solution's capabilities.	5.78	1.86	9
The SATIE Solution has good usability.	6.00	1.94	9
It was easy to understand the structure and logic of the SATIE Solution.	5.33	1.73	9
By using the SATIE Solution I could become more productive.	5.89	1.54	9
The SATIE Solution has all the functions and capabilities I expect it to have in an overall security system.	5.56	1.51	9
Overall, I am satisfied with the SATIE Solution.	5.56	1.42	9
The SATIE Solution provides helpful visualization and interactive control of the working process as well as the reports.	5.67	1.80	9
The SATIE Solution provides important decision support.	5.44	1.74	9
Using the SATIE Solution, the user (i.e. as security operator) is able to collaborate in the identification and classification of the various incidents and threats.	5.78	1.56	9
The SATIE Solution provides important decision support for improving the organizations situation awareness.	5.56	1.81	9
The SATIE Solution facilitates the incident handling process.	5.67	1.87	9
I think SATIE could provide economic benefits to my organization.	5.14	1.86	7
I think SATIE could provide compliance benefits to my organization.	5.56	1.94	9
I think SATIE could provide security benefits to my organization.	5.56	1.94	9
Using The SATIE Solution, my organisation can reduce the expenses in handling security.	5.00	1.63	7

Statement	Mean	SD ¹	N ²
Useful monitoring procedures are implemented in the SATIE Solution that improve cyber threat detection on airports IT and OT networks.	5.56	1.81	9
Useful monitoring procedures are implemented in the SATIE Solution that improve physical threat detection on airports physical facilities.	5.67	1.80	9
Useful monitoring procedures are implemented in the SATIE Solution that improve incident response and impact mitigation.	5.67	1.80	9
Useful monitoring procedures are implemented in the SATIE Solution that reduces the response time to a security or safety incident and minimize the impact of a cyber or physical attack.	5.78	1.86	9
The SATIE Tools can be effective in improving information sharing and communication among internal and external stakeholders.	5.67	1.50	9
The SATIE Tools can be effective in providing a common operational picture and situational awareness to both internal and external stakeholders.	5.67	1.87	9
The SATIE Tools can be effective in supporting the engagement of internal and external stakeholders in collaborative cyber-physical problem solving	5.78	1.92	9
The SATIE Tools can be effective in addressing the challenges of cyber-physical security that the airport personnel, passengers, visitors etc. may face.	5.78	1.92	9
Summary	5.63	1.84	

3.3.2 Evaluation results gained from the national sessions of the SATIE Practitioners' Workshop

This section presents the evaluation results and feedback gained from the three airport demonstrators' AIA, ZAG and SEA national breakout sessions carried out during the second part of the SATIE Practitioners' Workshop.

For the needs of the SATIE Practitioners' Workshop, KEMEA prepared a questionnaire (Annex 3 – Questionnaire for round table discussions of Security Practitioners' Workshop), in order to collect input from the practitioners in a form of a structured interview in the three different round tables (Greece, Zagreb, Milan).

The following sections analyse the results gained from each round table discussion in native language of the demonstrators that took over within the breakout session.

3.3.2.1 SATIE Practitioners' Workshop - AIA

During the Greek round table discussions coordinated by AIA and KEMEA, the current situation in terms of cyber – physical security practices and how the different SATIE Tools could contribute in further improvements have been discussed. Based on the received answers the following main conclusions can be extracted:

1. There is a need for a Holistic Security Operation Centre (HSOC) able to detect, analyse, and manage cyber and physical attacks. Also, the security plans should include integrated cyber and physical security solutions.
2. The understanding of the crisis management process to be followed by the internal and external involved parties during an incident can be improved. In addition, a better understanding of the roles and responsibilities of the internal and the external stakeholders including the interconnected CIs involved during an incident is needed.
3. During an incident due to operational and legal limitations the level of detail of information collected is not always efficiently shared in different layers and between the internal and external stakeholders.
4. The practitioners' agreed that one of the more important pieces of information about an incident is the impact it has on the organization (impact assessment).
5. With regards to the SATIE adoption by the different CIs and the SATIE Solution's interoperability, one of the biggest challenges seems to be the existing legal framework among the different stakeholders and the Interconnected CIs.
6. One area for SATIE improvement is the communication among the SOC operators while handling an incident through the Incident Management Portal.
7. One future improvement of the SATIE Solution could be the integration of routine procedures and operations (run-book) that operators carry out during an incident in the Crisis Alerting System (CAS).
8. Overall, the participating practitioners stated that SATIE can improve the flow and the communication of information among the stakeholders as well as the provision of a common operational picture.

3.3.2.2 SATIE Practitioners' Workshop - ZAG

Round table discussion and subsequent conversations with end-users in Zagreb included analysis of the existing solution and identification of some potential gaps in order to find an opportunity for improvement. This resulted with very useful, mainly similar feedback, including positive reinforcement and encouragement. Based on that, the following conclusions were drawn:

1. Compared to the existing solution in cyber-threats detection and prevention, SATIE offers much more analysis of particular events. The operator is given insight into many details and additional data which can be checked at the first-level support already. Therefore, it is possible to eliminate certain events at the beginning without the need for further escalation.

2. It was not clear, as it was not planned as a part of SOC operators' scope of work, who should monitor the alarms and raise them accordingly. Although it makes sense for IT professionals to use it, their working hours are not covering airport's 24/7 needs. After the debate we have agreed that SOC operators make a logical choice, but some additional training and support from IT personnel must be provided.
3. Related to that, risk management and business impact analysis are very useful in the aftermath of an event, but are not needed so much for SOC or AOC operators. Those advantages are clear in incident prevention for the future, so that part will be addressed to security and risk managers at the airport.
4. When we talked about emergency situations, it was clear that communication between all users should not change. Special radio-channels are designated in airport's TETRA system for such purposes and represent the fastest way of communication between everyone involved.
5. The challenge will be to install SATIE Solution to the external users (police, ambulance, outsourced security company). The best way is to start using it at the airport only and over time present all the benefits and advantages to the others in order for them to accept that kind of solution as well.
6. It may represent a problem to interconnect SATIE Toolkit with the existing CCTV system at the airport, because this system is very isolated. But this seemed more like a technical issue which can be resolved in the future if needed, and SATIE offers so much even without it.

3.3.2.3 SATIE Practitioners' Workshop - MXP

The round table opened with the explanation of the complex regulatory framework related to Cyber Security, to understand the possible connections of SATIE with it. Due to the increased exposure to cyber threats, both nationally and internationally, it became necessary to impose the need to develop, in a short time, suitable and increasingly stringent protection mechanisms. For further information on the Italian cybersecurity regulatory framework, please refer to "Annex 4 – State-of-the-art in Italian cybersecurity rules and regulations".

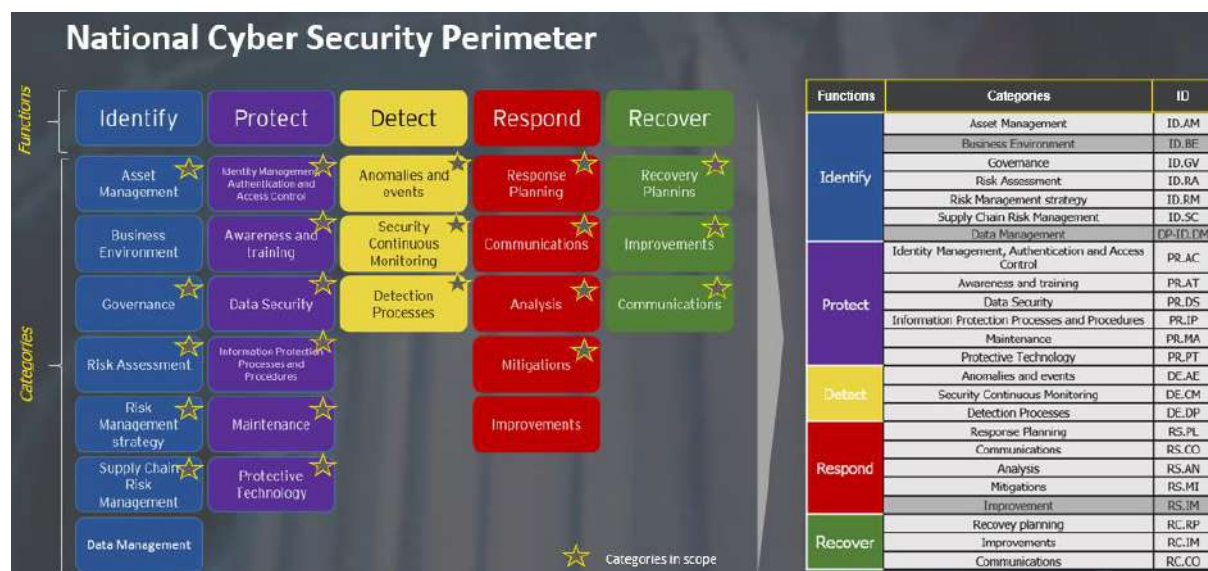


Figure 3.4: National Cyber Security Perimeter and fulfillments required by the Prime Ministerial Decree n. 81/2021 - security measures

The Figure 3.4 above is part of the National Cyber Security Perimeter which, referring to the national framework for cybersecurity and data protection (2019 edition), requires the individuals identified, according to criteria established by the Security Intelligence Department (DIS), to operate giving evidence for the purposes of compliance with the single Functions and Categories according to the timing as set out in the Prime Ministerial Decree no. 81/2021.

Trying to carry out a technical-functional mapping between the security measures required by the National Cyber Security Perimeter and what is satisfied in the context of the SATIE initiative, it is noted that some functions contemplated find correspondence as shown below:

- "Identification" -> through the RIS Tool;
- "Detection" -> through SOC tools (in both layers);
- "Response" and "Recover" -> through the Crisis Alerting System (CAS) and Impact Propagation Simulation (IPS).

The Malpensa Users Committee asks if SATIE is an Artificial Intelligence. For the moment SATIE is a "decision support tool" and SEA replies that if SATIE grows and interfaces with various airport systems, this will certainly involve the development of mechanisms (also based on AI) that will allow it to react in real-time in an automated way to the occurrence of threats.

In addition to cyber threats, SATIE also detects physical threats, so SEA's Head of Security compliance was requested to specify what measures apply at the airport. With regard to threats of a physical nature, the measures and procedures laid down by European, national and local (intended where the Airport is located) legislation apply. Measures and procedures applied concern the security of the airport, aircraft, passengers and baggage, goods, supplies, equipment used for security checks and the selection and training of personnel.

Although some changes have been made in recent years, the European relevant legislation is the EU Regulation no. 300/2008, the EU Regulation 1998/2015 and the Confidential Decision of the Commission no. 8005 of 2015, also taking into account the changes that have occurred in recent years.

The national legislation is essentially constituted by the National Program for Civil Aviation Safety which, in compliance with European legislation, establishes and specifies the procedures for the application of safety measures. At the airport level, in the event of a threat or illegal act in progress, the measures of the local Leonardo da Vinci Plan apply.

SEA highlighted the fact that reaching "0 risk" is almost impossible. SATIE, however, is useful because it collects events in real-time and puts them in correlation.

The cyber security consultant was asked for his opinion on how he sees SATIE in relation to critical infrastructures, both airport and external. He explained that the Essential Service Operators (Transport/Energy/Finance/Health) are public or private companies that have been recruited for national cyber defence in the strategic sectors they represent. Imagining a broader perspective, he explained that airport security already drops the fences that separate the various types of security: safety/security /ICT, placing them all under a single DNA. In this, SATIE highlights all the possible threats emerging from these different sectors and then brings them together for the purposes of decisions in a single concept of security of operations.

He then highlighted how SATIE, in addition to reaching the objective set by the National Security authority, also captures the weakest signals coming from complex realities such as airports as it offers the possibility of interfacing to other subjects, for example in the administrative field. The example of the "suppliers" was made: SATIE allows to check whether whoever is entering the security restricted area, or is in the airport perimeter, has an existing employment contract and is entitled to be present at the airport. SATIE correlates a series of information from databases that detect anomalies and highlight any type of illegal activity.

The SATIE Solution responds to every threat: it highlights significant anomalies with regard to Safety (potentially including fires), anomalies on the operating systems of all equipment, even those not related to the security risk.

Furthermore, SATIE, for the methods of collecting and cataloguing the reports, but also for the conservation of the same, in a certified and analytical manner, in addition to allowing to facilitate the Police Forces' investigation activities, immediate or subsequent, also allows the analyses of forensics

material on illegal activities carried out through unauthorized access to systems, data theft, their manipulation or damage, thus making it possible to secure any type of information useful for identifying the type of attack and those responsible for the illegal activity.

The head of the Malpensa Users Committee then reiterated (he had also pointed out during the Demo in Milan) that as with respect to the Cargo City, SATIE can be used to highlight critical situations to those appointed to intervene.

3.3.3 Feedback gained from standardization bodies

During the period between June 2021 and early July 2021, a report was prepared on SATIE's best practices and recommendations for updating airport security standards and airport security policies. The report relied upon the content of chapter 2 of this deliverable concerning recommendations, best practices and lessons learnt from SATIE on airport security according to a first consolidated draft version of the deliverable that was developed by that time. During that period, the consortium of the SATIE project established relationships with a group of standardization bodies aiming to promote the SATIE results within the international community and foster knowledge exchange pertaining to aviation security. On this account, between mid-July 2021 and early October 2021 the generated report was communicated to a number of standardization bodies, policy makers and relevant security practitioners aiming to strengthen knowledge transfer on aviation security and externalize SATIE outcome and, indeed, some recipients responded by providing valuable feedback. In particular, positive responses received from the following seven entities, depicted in Table 3.5.

Table 3.5: Standardization bodies/policy makers list reviewed the SATIE report

Standardization Body/Policy Maker	Type of entity	Description of entity
Directorate-General of the European Commission for Migration and Home Affairs (DG-HOME)	Directorate-General of the European Commission	The key-role is to ensure the EU's security, develop a common European Union (EU) migration and asylum policy, and encourage dialogue and boost cooperation with non-EU member states.
Directorate-General of the European Commission for Communications Networks, Content and Technology (DG-CNECT)	Directorate-General of the European Commission	It sets up and implements all the policies required to build a Digital Single Market.
European Union Aviation Safety Agency (EASA) (Department of Safety Intelligence & Performance)	EU Agency	It is responsible for ensuring civil aviation safety and environmental protection in air transport across Europe. It carries out certification, regulation and standardization, performs investigation and monitoring, capturing and analysing data related to safety legislation and coordinates with similar organizations on a global scale.
European Defence Agency (EDA)	EU Agency	It fosters integration between EU member states through the Common Security and Defense Policy (CSDP) of the EU.
European Organisation for the Safety of Air Navigation (EUROCONTROL)	European organisation	It aims to provide safe and seamless air traffic management across Europe.

Standardization Body/Policy Maker	Type of entity	Description of entity
(Civil-Military Coordination-DECMA/CMC Division)		
Deutsche Flugsicherung GmbH (DFS)	German certified Air Navigation Service Provider (ANSP)	It is responsible for the air traffic control in Germany.
Centro Italiano Ricerche Aerospaziali (CIRA) (Department of Reliability Availability Maintainability Safety & Security)	Italian Aerospace Research Centre	It promotes the advancement and success of the aerospace industry in Italy.

All these standardization bodies/policy makers positively commented and strongly supported the SATIE work and effort which was highly appreciated by the SATIE team. In particular, it was commented that SATIE Best Practices and Recommendations for updating airport security standards and airport security policies *“is coherent with its aim of providing best practices for a 360° protection of airports in the field of Security”* and that *“it represents a good basis to work upon for further steps”*. Moreover, the report was characterized as well-appreciated as it was expressed the difficulty in putting together all this information to a document.

In addition, four of these entities gave detailed and elaborated input on the SATIE report for improvements and possible further development. The major comments given by the standardization bodies/policy makers are displayed in Table 3.6.

Table 3.6: Feedback obtained from standardization bodies/policy makers for SATIE “Best Practices and Recommendations” on airports security standards and policies

Comment (C)	Description of comment
C#1	It provides a complete assessment in terms of list of reference standards.
C#2	Standards limitations and difficulties in application of harmonizing different aspects, sometimes conflicting could be highlighted.
C#3	It seems very focused on some specific systems and use cases of airport protection, specifically on current systems and how to improve them on a single basis, which is useful.
C#4	Possible conflicts among different airport assets and related control systems and governance should be addressed.
C#5	Little or nothing is said about Drones (intruders) or other more emerging threats.
C#6	The protection of different interdependent assets, represents a complex task also in terms of time constraints of the single processes running and time is critical. Thus, future steps in the focused systems will need the time dimension to rely upon.
C#7	The indications are qualitative, an estimate (quite general) of the expected improvements on the safety properties (KPI) is provided by adopting these practices. Furthermore, additional discussion could be given on monitoring the efficiency of the organization in relation to the security part (e.g. KPIs and metrics from all over), just to recall the concept of time dimension.
C#8	Additional information and proposed recommendations could be introduced on addressing the management of the unknown, specifically survivability in case of

Comment (C)	Description of comment
	attacks, such as indicate how to reorganize e.g. escape routes or to react dynamically to evolving scenarios.
C#9	Better clarify between mandatory requirements and recommendations in SATIE proposed steps for overcoming aviation's cybersecurity challenges in general.
C#10	Enhance SATIE cybersecurity recommendations on countering unauthorized drones entering particular restricted areas with references to relevant European Commission activities (including JRC) and other EU funded programs that concern Counter Unmanned Aerial Systems (C-UAS) – in addition, discussion on other emerging threats (apart from unauthorized drones) about air transport across Europe could be introduced.
C#11	Present more thoroughly relevance with NIS Directive.
C#12	Reduce the crisis management process costs as it is too extensive.
C#13	Regarding stakeholders' involvement in crisis management process it was indicated to include Computer Security Incident Response Teams (CSIRTs) as required by the NIS Directive.
C#14	The identified security management gap regarding different or no security plans within each airport should be reconsidered in line with the respective EU regulation that eliminates the gap: (i) Commission regulation (EC) 18-2010 on specifications for national quality control programmes for civil aviation security, (ii) Commission regulation (EC) 72-2010 on Commission inspection in aviation security.
C#15	Replace unnecessary detailed content with references or place some content in the Annexes to avoid exhaustive details that cause inconvenience to the reader.
C#16	Enhance the report's description with bullet-point structure and graphical representations.

According to Table 3.6, there were positive comments illustrating the coherent structure of the report on airport protection which is useful and the completeness of assessment regarding the existing related standards (C#13, C#3).

The comments provided for potential future amendments and improvements involve the harmonization of the different challenges deriving from standards limitations and difficulties in application (C#2), identify possible conflicts on different airport assets and address their governance (C#4). In addition, enhancements were proposed on SATIE recommendations addressing the challenges of unauthorized drones and other emerging threats and report on EU programmes and activities for Countering Unmanned Aerial Systems (C-UAS) (C#5, C#10), indications to initiate the concept of time dimension towards monitoring organizations efficiency on security and addressing the protection of multiple, heterogeneous, interdependent assets were delivered (C#6, C#7). Moreover, other suggested expansions refer to the promotion of the dynamic incident response dimension and the management of the unknown to achieve survivability in case of an attack (C#8).

The comments that raised the attention for current improvements are the following: enhance clarifications on the mandatory requirements regarding cybersecurity protection in aviation and SATIE recommendations (C#9), introduce thoroughly the NIS Directives and corresponding requirements (e.g. CSIRTs involvement in crisis management) (C#11, C#13). Furthermore, the crisis management process was indicated to shorten to avoid extensive reading (C#12), it was recommended the security gaps on different or no security plans within airports to be aligned with the respective EU regulation (C#14). Redundant contents of the report were suggested to be reduced (C#15) and eventually, bullet-points and graphical representations were proposed to improve the overall presentation (C#16).

As a result, the standardization bodies/policy makers confirmed and well-supported the SATIE outcomes and the feedback gained was very fruitful to increase the SATIE performance. The comments received from them were taken into account during the deliverable's updates.

To this end, the communication of the SATIE report to the standardization bodies and relevant parties proved to be a good evidence to inject gathered knowledge into standards and good practices and it additionally expanded the dissemination activity and promotion of the SATIE results.

4 Conclusion

The current deliverable has a very important role to the SATIE project findings, as it engages a set of best practices that airports in collaboration with their respective stakeholders can utilize to better monitor their security policies and thereby enhance the protection of their CIs. The produced best practices and recommendations were adopted based on the experience gained from the SATIE Project results (directly linked with T7.2, T2.3) throughout the project's lifespan and followed a continuous improvement approach by updating the delivered information with knowledge received from standardisation bodies, policy makers, airport stakeholders and security practitioners. It incorporates an extensive report on the existing regulation, standards, frameworks and guidelines in airport security (i.e. cybersecurity related and physical security related) as a result of a comprehensive analysis on the domain-specific infrastructures characteristics and their evolving security issues. More specifically, it provides guidance and recommendations on the general topics enlisted below:

- Improve airport security by utilizing the SATIE proposed innovative risk assessment methodology (advance cyber/physical security by utilizing a set of techniques);
- Improve security and set guidelines for BHS and relevant systems (i.e. exploring ICS system characteristics, e.g. SCADA, use SATIE IEs to reinforce ICS common best practices);
- Provide existing recommendations and best practices for improving the cyber/physical security of the AOC (e.g. compliance with NIS Directive, employ SATIE best practices);
- Introduce best practices for improving anomaly detection on cyber/physical threats, including passenger data (i.e. SATIE check-in step/border crossing step);
- Recommendations for airports employees biometric access control deployment (i.e. accuracy of solution, GDPR compliance, security implementation);
- Report on existing best practices related to the security of the digital services and voice communication systems of ATM services;
- Indicate best practices related to airport crisis management and decision support operation and report on relevant existing security regulation framework (i.e. identify security gaps/propose holistic crisis management process).

In addition, this deliverable reports on the performance of all the standardization and dissemination activities provided to communicate the SATIE Solution and IEs and expand the knowledge of stakeholders on how to protect their CIs (SATIE Awareness Event) and to foster knowledge from airport practitioners by exploring the SATIE impact towards their daily operations and normal processes (SATIE Practitioners' Workshop). This was achieved via the conduction of national round tables discussions carried out in native language and the generated outcome has been reported in the evaluation results of the current deliverable which is very promising (section 3.3.2). Indicatively, one of the most popular comments that was raised correspondingly by all airport demonstrators is the major importance of impact assessment and risk management and specifically estimating the impact of an incident to the overall organization. Whereas, a future improvement of the SATIE Solution could be, for instance, the integration of routine procedures and functions (run-book) that operators should perform during an incident when using CAS. The workshop's participants were requested to provide additional input on the SATIE Solution and its IEs by filling an online questionnaire presented in the respective section 3.3.1 which gives insights on the action points needed to ensure security and protection of airports environment and CIs and to assess the SATIE Solution and IEs towards their security needs. Once more, the input received was well commented endorsing SATIE. Eventually, the feedback received from the standardization bodies was positive as well, strongly supporting the SATIE work which is further analysed in section 3.3.3.

5 References

1. **SATIE project.** *D7.2 - Training Handbook.* 2021.
2. —. *D7.9 - Cyber-physical risk analysis.* 2021.
3. **ISO.** ISO/IEC 27002:2013. *Information technology — Security techniques — Code of practice for information security controls.* [Online] <https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en>.
4. **European Commission.** *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.* [Online] 2016. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148>.
5. **SATIE project.** *D7.7 - Specification of a holistic security management cycle.* 2020.
6. **European, Commission.** *COM/2020/823 Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148.* 2020.
7. **European Commission.** *Commission implementing regulation 2019/1583 amending Implementing Regulation (EU) 2015/1998 laying down detailed measures for the implementation of the common basic standards on aviation security, as regards cybersecurity measures.* 25.09.2019.
8. **ICAO.** *Security Manual for Safeguarding Civil Aviation Against Acts of Unlawful Interference.* [Online] <https://www.icao.int/Security/Pages/default.aspx>.
9. **ISA, ANSI.** *Security for industrial automation and control systems part 1 terminology, concepts, and models.* . s.l. : International Society for Automation, 2007. ISA-99.
10. **Stoffer, Keith, et al.** *Guide to Industrial Control Systems (ICS) Security.* s.l. : National Institute of Standards and Technology, 2015. Technical Report NIST Special Publication (SP) 800-82 Rev. 2.
11. **Lima, João, et al.** *BP-IDS: Using business process specification to leverage intrusion detection in critical infrastructures.* Coimbra : IEEE, 2020.
12. **Köpke, Corinna, et al.** *Impact Propagation in Airport Systems.* Guildford, United Kingdom : 1st International Workshop on Cyber-Physical Security for Critical Infrastructures Protection (CPS4CIP 2020), 2020. 14.-18.
13. **Aurora - AI.** *Artificial Intelligence (AI) Solutions using Deep Learning for automation and analysis.* [Online] 2021. [Cited: 05 10, 2021.] <https://www.airport-suppliers.com/supplier/aurora-ai/>.
14. **SITA.** *SITA statement about security incident.* [Online] 03 04, 2021. <https://www.sita.aero/pressroom/news-releases/sita-statement-about-security-incident/>.
15. **CNIL, European Union** /. <https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre2>. <https://www.cnil.fr>. [Online] 2018.
16. **Vasiliki Mantzana, Eftichia Georgiou, Anna Gazi, Ilias Gkotsis, Ioannis Chasiotis and Georgios Eftychidis.** *Towards a Global CIs' Cyber-Physical Security Management and Joint Coordination Approach.* s.l. : Cyber-Physical Security for Critical Infrastructures Protection, pp. 155 – 170, First International Workshop, CPS4CIP 2020, 2020.
17. **European Commission.** *European Commission. Communication from the Commission on a European Programme for Critical Infrastructure Protection.* [Online] 2006. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52006DC0786>.

18. **European Commission.** *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.* 2008.
19. **European Commission.** European Aviation Safety Rules. [Online] https://ec.europa.eu/transport/modes/air/safety/safety-rules_en.
20. **European Parliament.** Air transport: Civil aviation security. *Fact Sheets of the European Union.* [Online] https://www.europarl.europa.eu/factsheets/en/sheet/132/air-transport-civil-aviation-security#_ftn1.
21. **European Commission.** *Commission Implementing Regulation (EU) 2015/1998 of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security (Text with EEA relevance).* [Online] 2015. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015R1998>.
22. **SATIE project.** *D7.6 - SoA about airports security and expected improvements.* 2021.
23. **Alliance, National Safe Skies.** *PARAS. Recommended Security Guidelines for Airport Planning, Design, and Construction.* s.l. : National Safe Skies Alliance, Inc. Sponsored by the Federal Aviation Administration, 2017.
24. **Hutter, David.** *The Importance of Physical Security.* s.l. : The SANS Institute, 2016.
25. **PARAS.** *Airport Perimeter Breach Classification and Post-Incident Best Practices.* s.l. : National Safe Skies Alliance, Inc., 2016.
26. **Hutter, David.** *Physical Security and Why It Is Important.* s.l. : SANS Institute. Physical Security and Why It Is Important., 2016.
27. **NIST.** NIST - Digital Identity Guidelines. [Online] 2019. <https://pages.nist.gov/800-63-3/sp800-63-3.html#def-and-acr>.
28. **ENISA.** *Securing Hospitals: A research study and blueprint.* Independent Security Evaluators. [Online] 2016. https://www.securityevaluators.com/wp-content/uploads/2017/07/securing_hospitals.pdf.
29. **Bidou, Renaud.** *Security Operation Center Concepts & Implementation.* 2005.
30. **British Standard Institute (BSI).** *BS11200: Crisis Management – guidance and good practice .* s.l. : BSI, 2014.
31. **SATIE project.** *D6.4 - Report about demonstration and results in Zagreb airport.* 2021.
32. —. *D6.5 - Report about demonstration and results in Athens airport.* 2021.
33. —. *D6.6 - Report about demonstration and results in Milan airport.* 2021.
34. **ISO.** ISO/IEC 19794-5:2011. [Online] <https://www.iso.org/standard/50867.html>.
35. **ISO.** *Standards by ISO/IEC JTC 1/SC 17.* 2021.
36. **ISO.** ISO/IEC 18745-1:2018 - Part 1. [Online] <https://www.iso.org/standard/67800.html?browse=tc>.
37. **ICAO.** ICAO / Publications. [Online] <https://www.icao.int/publications/pages/publication.aspx?docnum=9303>.
38. **EU, Council of the.** *Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data.* s.l. : EU, 2004. pp. 24-27.
39. **ISO.** ISO/IEC 19784-1:2018. Information technology — Biometric application programming interface — Part 1: BioAPI specification. [Online]

40. **NIST.** Background on CBEFF Standards. *Background on CBEFF Standards*. [Online] <https://www.nist.gov/services-resources/software/biometric-testing-software/nistitl-conformance-test-suite-patron-0>.
41. **Fernando Podio, Jeffrey Dunn, Lawrence Reinert, Catherine Tilton, Bruno Struif, Fred Herr, James Russell.** Common Biometric Exchange Formats Framework (CBEFF). *NISTIR 6529-A*. [Online] 2004. <https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir6529-a.pdf>.
42. **ISO/IEC.** ISO/IEC 19785-1. *Information technology - Common Biometric Exchange Formats Framework - Part 1: Data element specification*. [Online] 2020. <https://webstore.iec.ch/publication/67653>.
43. —. ISO/IEC 19785-2:2006. *Information technology -- Common Biometric Exchange Formats Framework -- Part 2: Procedures for the operation of the Biometric Registration Authority*. [Online] 2006. <https://webstore.iec.ch/publication/10762>.
44. —. ISO/IEC 19785-3:2020. *Information technology -Common Biometric Exchange Formats Framework - Part 3: Information technology - Common Biometric Exchange Formats Framework - Part 3: Patron format specifications*. [Online] 2020. <https://webstore.iec.ch/publication/67654>.
45. **INCITS.** INCITS 385-2004[R2014]: Information technology - Face Recognition Format for Data Interchange . [Online] https://standards.incits.org/apps/group_public/project/details.php?project_id=876.
46. **NIST.** ANSI/NIST-ITL Standard History. [Online] <https://www.nist.gov/itl/iad/image-group/ansinist-itl-standard-history>.
47. **ANSI.** ANSI/NIST-CS1-1993. *American National Standard for Information Systems - Data Format for the Interchange of Fingerprint Information*. [Online] https://www.nist.gov/system/files/documents/2021/02/03/ansi-nist-csl_1-1993.pdf.
48. **NIST.** <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-290e3.pdf>. *ANSI/NIST-ITL 1-2011 Update:2015 Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information*. [Online] <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-290e3.pdf>.

6 Annexes

Annex 1 – Current regulatory framework and standards related to anomaly detection on cyber-physical threats, including passenger data

ISO / IEC 19794-5:2011 Standard

The **Part of the ISO/IEC 19794-5:2011** (34), Information technology - Biometric data interchange formats - Part 5: Face image data, 2011, which is mentioned in the **ICAO** (International Civil Aviation Organization) provided recommendations about the travel document, and defined the standard formats for digital images of faces in order to guarantee the correct execution of operations by specifying:

- a record format for storing, recording, and transmitting information from one or more facial images or a short video stream of facial images;
- scene constraints of the facial images;
- photographic properties of the facial images;
- digital image attributes of the facial images;
- best practices for the photography of faces.

ISO/IEC JTC 1/SC 27 - Information security, cybersecurity and privacy protection

This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as (a) Security requirements capture methodology; (b) Management of information and ICT security; in particular Information Security Management Systems (ISMS), security processes, security controls and services; (c) Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information; (d) Security aspects of identity management, biometrics and privacy etc.

ISO/IEC JTC 1/SC 37 - Biometrics

A major part of the international biometric standards work has been taking place in ISO/IEC Joint Technical Committee 1 (JTC 1), particularly in its Subcommittee 37 (SC 37) on 'Biometrics' established in June 2002. To date, more than 130 international standards related to biometrics have been published under the direct responsibility of this group. The areas of template protection, algorithm security and security evaluation are addressed outside SC 37, in SC 27 on 'IT Security techniques', and SC 17 deals with biometrics in 'Cards and personal identification'.

ISO/IEC JTC1/SC17 WG3

The current area of work of JTC 1/SC 17 pertains to the following fields:

- Identification and related documents;
- Cards;
- Security devices and tokens;
- And the interface associated with their use in inter-industry applications and international interchange.

The committee has published more than 103 ISO standards (35), and indicatively the following are relevant to test methods for machine readable travel documents (ISO/IEC 18745-1:2018), Part 1: Physical test methods for passport books (durability), and Part 2- Test methods for the contactless interface:

- ISO/IEC 18745-1:2018 (36). Test methods for machine readable travel documents (MRTD) and associated devices — Part 1: Physical test methods for passport books (durability). This document provides a set of instructions for evaluation of MRTDs which may incorporate contactless integrated circuits. This evaluation is an instrument to establish the ability in principle of a specific type of document to fulfil the requirements of use;
- ISO/IEC 18745-2:2016. Information technology — Test methods for machine readable travel documents (MRTD) and associated devices — Part 2: Test methods for the contactless interface. The document defines the test plan, based on ISO/IEC 10373-6, for the contactless interface of electronic MRTDs (eMRTDs) and eMRTD associated readers compliant with ICAO Doc 9303.

CEN/TS 16634:2014 - Personal identification - Recommendations for using biometrics in European Automated Border Control

This technical specification primarily focuses on biometric aspects of Automated Border Control (ABC) systems. Drawing on the first European and international ABC deployments, it aims to disseminate best practice experiences with a view to ensure consistent security levels in European ABC deployments. Furthermore, the best practice recommendations given here shall help make border control authorities' processes more efficient, speeding up border clearance, and delivering an improved experience to travellers. This technical specification amends the ISO standards with respect to special European conditions and constraints. The technical specification systematically discusses issues to be considered when planning and deploying biometric systems for ABC and gives best practice recommendations for those types of systems that are or will be in use in Europe.

CEN/TS 16921:2016 - Personal identification - Borders and law enforcement application profiles for mobile biometric identification systems

This technical specification primarily focuses on biometric aspects of portable verification and identification systems for law enforcement and border control authorities. The recommendations given here will balance the needs of security, ease of access and data protection. This technical specification extends the ISO standards by emphasizing specific European needs (for example EU data protection Directive 95/46/EC and European databases access). The technical specification systematically discusses issues to be considered when planning, deploying and using portable identity verification systems and gives recommendations for those types of systems that are or will be in use in Europe. Communication, infrastructure scalability and security aspects other than those related to biometrics are not considered. This document also does not consider hardware and security requirements of biometric equipment and does not recommend general identification procedures.

CEN/TS 17262:2018 - Personal identification - Robustness against biometric presentation attacks - Application to European Automated Border Control

This document provides requirements and recommendations for the implementation of ABC systems in Europe with Presentation Attack Detection (PAD) capability. This document covers the evaluation of countermeasures from the biometrics perspective as well as privacy, data protection and usability aspects. This document covers biometric impostor attacks and biometric concealer attacks in a watchlist scenario. This document addresses PAD for facial and fingerprint biometrics only.

CEN/TS 17261:2018 - Biometric authentication for critical infrastructure access control - Requirements and Evaluation

This document addresses biometric recognition systems that are used as part of an automated access control system (AACS) to provide a second and independent authentication factor of the individual using the AACS to access secured areas of critical infrastructure. This document specifies requirements for biometric recognition systems to be used as part of an AACS for critical infrastructure, and describes a methodology for the evaluation of biometric authentication for AACSs against the specified requirements.

CEN/TC 377 - Air Traffic Management / EN 16495:2019

This document provides guidance based on EN ISO/IEC 27002:2017 applied to organisations supporting civil aviation, with a focus on air traffic management operations. This includes, but is not limited to, airspace users, airports and air navigation service providers. The basis of all guidance in this document is trust and cooperation between the parties involved in air traffic management.

CEN/TS 16501:2013 - Air Traffic Management - Specification for software assurance levels

It specifies the technical, operational and maintenance requirements for Software Assurance Levels (SWAL) to support the demonstration of compliance with some elements of the Essential Requirements Safety and Principles governing the construction of systems of the Regulation (EC 552/2004) of the European Parliament and of the Council on the interoperability of the European air traffic network (the Interoperability regulation).

ICAO Doc 9303 - Machine Readable Travel Documents (MRTD)

ICAO Doc 9303 (37) provides the basic functional specification for MRTD's and describes all relevant properties of MRTD's. The portrait printed on the ICAO compliant MRTD is an essential element of that document and one of the most important information carriers binding the document to the holder. A standardized portrait produced at a high quality helps issuing agencies to screen identity and border agencies to inspect the travel document manually or via automated processing. After the introduction of the digitally stored image in 2005, ABC systems have been introduced to perform automated comparison of the person and the electronically stored image. Those ABC systems compare, whether it is manually or automated the printed image and/or the electronically stored image and the image taken live while crossing a border. Parts of the document are based on **ISO/IEC 19794-5:2005 and ISO/IEC 19794-5:2011**. The content of these documents has been rearranged, consolidated, enriched, and improved within **ISO/IEC JTC1 SC17 WG3**. The ICAO Doc 9303 ICAO provides a set of specifications for three types of machine readable official Travel Documents (TDs); size 1 (TD1), size 2 (TD2) and size 3 (TD3) respectively in terms of the security of the design, manufacture and issuance of MRTDs. It consists of the 13 following parts:

- Part 1: Introduction;
- Part 2: Specifications for the security of the design, manufacture and issuance of MRTDs;
- Part 3: Specifications common to all MRTDs (Amendment for New Part B in page 28 and Part D in page 29);
- Part 4: Specifications for Machine Readable Passports (MRPs) and other TD3 size MRTDs;
- Part 5: Specifications for TD1 size Machine Readable Official Travel Documents (MROTDs);
- Part 6: Specifications for TD2 size Machine Readable Official Travel Documents (MROTDs);
- Part 7: Machine Readable Visas;
- Part 8: Emergency Travel Documents;
- Part 9: Deployment of Biometric Identification and Electronic Storage of Data in eMRTDs;
- Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC);
- Part 11: Security Mechanisms for MRTDs;
- Part 12: Public Key Infrastructure for MRTDs;
- Part 13: Visible Digital Seals.

Based on the ICAO Doc 9303 specifications the following requirements (translated to characteristics for algorithms) are extracted:

- ICAO08 (pixelation);
- ICAO10 (Eye Closed);
- ICAO13 (Flash Reflection on Skin);
- ICAO15 (shadow behind Head);

- ICAO17 (Dark Tinted lenses);
- ICAO18 (Flash Reflection on Lenses);
- ICAO22 (Veil over Face);
- ICAO02 (Blurred);
- ICAO04 (Ink Marked/Creased);
- ICAO05 (Unnatural Skin Tone);
- ICAO06 (Too Dark/Light);
- ICAO11 (Varied Background);
- ICAO14 (Red Eyes);
- ICAO19 (Frames too Heavy);
- ICAO20 (Frame Covering Eyes);
- ICAO23 (Mouth Open);
- ICAO01 (Eye Location);
- ICAO03 (Looking Away);
- ICAO07 (Washed Out);
- ICAO09 (Hair Across Eyes);
- ICAO12 (roll/pitch/yaw Greater than 8);
- ICAO16 (Shadow Across Face);
- ICAO21 (Hat/CAP);
- ICAO24 (Presence of other Faces or Toys too Close to Face).

Commision SWD Evaluation of the Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data (API Directive) (SWD175/8-9-2020)

This evaluation assesses Council Directive 2004/82/EC of 29 April 2004 (38) on the obligation of carriers to communicate passenger data (the 'API Directive') and its implementation in EU Member States and Schengen associated countries. It aims to improve border controls and combat illegal immigration through the transmission of Advanced Passenger Information (API) by air carriers to competent national authorities. In addition, it places the possibility to Member States to facilitate data for law enforcement purposes.

ICAO Annex 9 – “Facilitation” (SARPs 3.47 and 3.48)

A very important regulation function of ICAO is set by the formulation and adoption of Standards and Recommended Practices (SARPs) for international civil aviation. Annex 9 (Facilitation) to the Chicago Convention embodies the SARPs and guidance material related to the facilitation of landside formalities for clearance of aircraft and passengers, goods and material in line with the requirements of customs, immigration, public health and agriculture authorities. The standard 3.47 and recommended practice 3.48 of ICAO, Annex 9 provides the basic rules for the use of Advanced Passenger Information (API) and Passenger Name Record (PNR) respectively on a global level. Furthermore, regarding API, standard 3.47 obliges each Contracting State that engages an API system in its national legislation to adhere to international recognized standards for the transmission of Advance Passenger Information.

WCO/IATA/ICAO Management Summary on Passenger-related Information (Umbrella Document)

The “Umbrella Document” is a joint document, published by the International Civil Aviation Organisation (ICAO), the World Customs Organisation (WCO) and the International Air Transport Association (IATA) which gives a high-level executive brief on the different sources and systems for passenger-related information, such as specifying the PNR, Passenger information in a Departure Control System (DCS), Advance Passenger Information (API), interactive API iAPI) required to be provided by international aircraft operators to border control agencies. General aviation operations are excluded from the scope of the current document. Furthermore, the Umbrella Document gives

guidelines concerning passenger-related information secure utilization by immigration authorities and presents the electronic exchange process.

Additional Biometric standards for passenger data

Table 6.1 depicts some additional biometric standards, used in the field of the passenger anomaly detection.

Table 6.1: Additional biometric standards

Standard	Short description
BioAPI 2.0 (ISO/IEC 19784-1:2006) (Framework and Biometric Service Provider for Face Identification Engine) (39)	ISO/IEC 19784-1:2018 defines the Application Programming Interface (API) and Service Provider Interface (SPI) for standard interfaces within a biometric system that support the provision of that biometric system using components from multiple vendors. It provides interworking between such components through adherence to this and to other international standards.
CBEFF V1.2 (ANSI INCITS 398-2008) (Common Biometric Exchange Formats Framework) (40)	The Common Biometric Exchange Formats Framework (CBEFF) group of standards – developed by national and international standards development bodies – defines basic data structures and sets of abstract data elements and values that support the straightforward interchange of biometric data when used in conforming Biometric Information Records (BIRs). The original version of CBEFF was published as NISTIR 6529 (41). Three parts of the multi-part CBEFF international standard have been published as ISO/IEC standards: ISO/IEC 19785-1, Information technology — Common Biometric Exchange Formats Framework — Part 1: Data element specification (42), Part 2: Procedures for the operation of the Biometric Registration Authority (43), Part 3: Patron format specifications. (44)
ANSI/INCITS 385-2004 (Face Recognition Format for Data Interchange) (45)	Specifies definitions of photographic (environment, subject pose, focus, etc.) properties, digital image attributes and a face interchange format for relevant applications, including human examination and computer automated face recognition.
ANSI/NIST-CSL 1-1993 (Data Format for the Interchange of Fingerprint, Facial, & SMT Information) (46)	In 1993, ANSI approval was obtained for the "Data Format for the Interchange of Fingerprint Information" standard (ANSI/NIST-CSL 1-1993) (47). The standard specifies formats to be used for exchanging fingerprint and other image data. In 2013, the standard was updated to ANSI/NIST-ITL 1-2011: Update 2013. The "Forensic Dental and the Forensic and Investigatory Voice Supplements" were approved. In 2015, the standard was updated to ANSI/NIST-ITL 1-2011: Update 2015 (48).

Annex 2 – Evaluation questionnaire of Security Practitioners' Workshop

Welcome to the SATIE Workshop questionnaire. Please click "Next" to start.

Section A: Startpage

Please choose the type of organization you work at.

A1. Type of organization

Emergency Management Services ☐

Governmental Authority ☐

Law Enforcement ☐

Ministry ☐

Regulatory Authority ☐

Research/Academic ☐

Security Industry ☐

Other ☐

Other

Section B: Airport cyber-physical security current practices and identification of gaps

Please answer the following questions.

If you feel that you cannot answer a particular question, please check "not applicable".

B1.

	Completely disagree	Mostly disagree	Slightly disagree	Neither agree nor disagree	Slightly agree	Mostly agree	Completely agree	Not applicable
There is continuous training to enhance readiness and cooperation in order to respond to any type of complex incidents and emergencies.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
It is easy to predict the potential impact of an incident among interconnected CIs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

	Completely disagree	Mostly disagree	Slightly disagree	Neither agree nor disagree	Slightly agree	Mostly agree	Completely agree	Not applicable
It is easy to predict the potential impact of an incident within the airport (i.e. fire propagation, terrorist attacks, plum dispersion, impact of toxic chemicals, radioactivity etc.)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
During an incident the information needed is effectively and efficiently managed and shared in different layers and between the internal and external stakeholders.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
During an incident there is a single coordination point acquiring the complete set of collected data for feeding it to internal and external stakeholders.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The roles and responsibilities of those involved during an incident are well defined.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The current security plans as well the crisis management process to be followed is well understood by the involved parties .	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
A common cyber-physical crisis management process should be established and followed within each airport/CI and at Member States level.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
There is a need for a Holistic Security Operation Centre (HSOC) able to detect, analyse, and manage cyber and physical attacks.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The security plans should include integrated cyber- and physical security solutions.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The current design for the safety and protection of the airports/ CIs take into consideration the combination of cyber and physical threats.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

B2. Which actions do you consider as necessary to enhance the resilience of airports / CIs?

You are able to select more than one answer

Enhancement of cyber measures	<input type="checkbox"/>
Enhancement of cyber and physical measures combination	<input type="checkbox"/>
Continuous training of personnel	<input type="checkbox"/>
Additional exercises	<input type="checkbox"/>
Common security plans	<input type="checkbox"/>

Other ☐Enhancement of physical measures ☐**B3. You have chosen "Other". Would you like to specify your answer?**

Section C: General Questions

Please answer the following general questions about the SATIE Solution.

If you feel that you cannot answer a particular question, please check "not applicable".

C1.

	Completely disagree	Mostly disagree	Slightly disagree	Neither agree nor disagree	Slightly agree	Mostly agree	Completely agree	Not applicable
The SATIE Solution enables a faster detection of cyber threats compared to current systems.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The SATIE Solution provides all relevant information.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I think the SATIE Solution will boost airports' revenues.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The SATIE Solution is innovative compared to others on the market.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I think that it will be easy to integrate the SATIE Solution with the necessary airport systems.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The use of the SATIE Solution increases the efficiency compared to current systems.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The SATIE Solution enables a faster response to physical threats compared to current systems.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The SATIE Solution enables a faster response to cyber threats compared to current systems.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The SATIE Solution enables a faster detection of physical threats compared to current systems.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The SATIE tools can be effective in improving information sharing and communication among internal and external stakeholders.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

	Completely disagree	Mostly disagree	Slightly disagree	Neither agree nor disagree	Slightly agree	Mostly agree	Completely agree	Not applicable
The SATIE tools can be effective in providing a common operational picture and situational awareness to both internal and external stakeholders.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The SATIE tools can be effective in supporting the engagement of internal and external stakeholders in collaborative cyber-physical problem solving	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I think airports will like to secure their systems with the SATIE Solution.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Using the SATIE Solution, the user (i.e. as security operator) is able to collaborate in the identification and classification of the various incidents and threats.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The SATIE Solution provides important decision support for improving the organizations situation awareness.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The SATIE Solution facilitates the incident handling process.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I think SATIE could provide economic benefits to my organization.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I think SATIE could provide compliance benefits to my organization.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I think SATIE could provide security benefits to my organization.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Using The SATIE Solution, my organisation can reduce the expenses in handling security.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I think that the shown scenario(s) were suitable to illustrate the SATIE Solution's capabilities.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The SATIE Solution has good usability.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
It was easy to understand the structure and logic of the SATIE Solution.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
By using the SATIE Solution I could become more productive.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The SATIE Solution has all the functions and capabilities I expect it to have in an overall security system.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Overall, I am satisfied with the SATIE Solution.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The SATIE Solution is an excellent way to monitor and raise security alerts.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

	Completely disagree	Mostly disagree	Slightly disagree	Neither agree nor disagree	Slightly agree	Mostly agree	Completely agree	Not applicable
The SATIE Solution is overall a significant improvement compared to current security-monitoring systems.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The SATIE solution provides helpful visualization and interactive control of the working process as well as the reports.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The SATIE solution provides important decision support.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Useful monitoring procedures are implemented in the SATIE Solution that improve cyber threat detection on airports IT and OT networks.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Useful monitoring procedures are implemented in the SATIE solution that improve physical threat detection on airports physical facilities.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Useful monitoring procedures are implemented in the SATIE solution that improve incident response and impact mitigation.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Useful monitoring procedures are implemented in the SATIE solution that reduces the response time to a security or safety incident and minimize the impact of a cyber or physical attack.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The SATIE tools can be effective in addressing the challenges of cyber-physical security that the airport personnel, passengers, visitors etc. may face.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
C2. Please consider to briefly explain why you indicated that the monitoring procedures are not useful.								
<div style="border: 1px solid black; height: 100px; width: 100%;"></div>								

C3. Please consider to briefly explain why you think that the solution is not acceptable as a way to monitor and raise security alerts.

C4. You indicated that the solution does not provide you with all relevant information. What information do you feel is missing?

C5. You indicated that the SATIE Solution does not have all the functions and capabilities you expect it to have. Could you briefly explain what is missing?

Section D: General Questions 2

Please answer the following additional general questions about the SATIE Solution. If you feel that you cannot answer a particular question, please write "not applicable".

D1. Which of the Innovation Elements stood out for you and why? Please indicate our top three.

Application Layer Cyber Attack Detection (ALCAD)

☐

Comment

Malware Analyser

☐

Comment

Business Process-based Intrusion Detection System (BP-IDS)	<input type="checkbox"/>
Comment	<input type="text"/>
Traffic Management Intrusion and Compliance System (TraMICS)	<input type="checkbox"/>
Comment	<input type="text"/>
Secured ATM Services	<input type="checkbox"/>
Comment	<input type="text"/>
Anomaly Detection On Passenger Records (PAD)	<input type="checkbox"/>
Comment	<input type="text"/>
Unified Access Control (UAC)	<input type="checkbox"/>
Comment	<input type="text"/>
Secured Communication on the BHS (ComSEC)	<input type="checkbox"/>
Comment	<input type="text"/>
Gestion Libre de Parc Informatique (GLPI)	<input type="checkbox"/>
Comment	<input type="text"/>
Vulnerability Intelligence Platform (VIP)	<input type="checkbox"/>
Comment	<input type="text"/>
Risk Integrated Service (RIS)	<input type="checkbox"/>
Comment	<input type="text"/>

	Digital Twin of the Baggage Handling System (BHS)	<input type="checkbox"/>
Comment	<input type="text"/>	
	CyberRange	<input type="checkbox"/>
Comment	<input type="text"/>	
	Incident Management Portal (IMP)	<input type="checkbox"/>
Comment	<input type="text"/>	
	Business Impact Assessment (BIA)	<input type="checkbox"/>
Comment	<input type="text"/>	
	Investigation Tool (SMS-I)	<input type="checkbox"/>
Comment	<input type="text"/>	
	Correlation Engine	<input type="checkbox"/>
Comment	<input type="text"/>	
	Crisis Alerting System (CAS)	<input type="checkbox"/>
Comment	<input type="text"/>	
D2.	Is there anything else you would like to mention about the SATIE Solution?	
	<input type="text"/>	

Thank you for completing the SATIE Workshop questionnaire!

Annex 3 – Questionnaire for round table discussions of Security Practitioners' Workshop



SATIE

Security of Airport Transport Infrastructure of Europe

Round table discussion

AIA, Eftichia Georgiou (KEMEA)
Practitioners' Event, 2021-09-24, Remote



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement number 832969.




SATIE

I. Perceived purpose of SATIE

1. When you joined the practitioners' event, were there specific expectations or knowledge areas that you anticipated to be discussed?
2. When you joined the practitioners' event of SATIE, were you looking for a solution to a specific problem or were you more broadly interested in expanding your knowledge or expertise around the cyber-physical security topic?

Practitioners' Event 2021-09-24

1



SATIE

II. Airport cyber-physical security current practices and identification of gaps

1. Are the roles and responsibilities of those involved during an incident well defined?
2. During an incident, is there a single coordination point acquiring the complete set of collected data for feeding it to internal and external stakeholders?
3. During an incident, is the information needed effectively and efficiently managed and shared in different layers and between the internal and external stakeholders?

Practitioners' Event 2021-09-24

2



III. Airport cyber-physical security current practices and identification of gaps

4. In your opinion, are the current security plans as well as the crisis management process to be followed well understood by the involved parties?
5. In your opinion, should a common cyber-physical crisis management process be established and followed within each airport/CI and at Member States level?
6. Is there a need for a Holistic Security Operation Centre (HSOC) able to detect, analyse, and manage cyber and physical attacks?
7. In your opinion, should the security plans include integrated cyber and physical security solutions?

Practitioners' Event 2021-09-24

3



IV. Review of SATIE solution

- ☐ Following today's presentations of the SATIE solution and modules, kindly provide your feedback on the following questions:
1. In what way(s) has SATIE solution met your expectations and/or requirements?
 2. In what way(s) has SATIE solution failed to meet your expectations and/or requirements?

Practitioners' Event 2021-09-24

4



V. Review of SATIE solution

1. In your opinion, how effective do you think the SATIE solution has been in the following:
 - Improving information flow and communication among safety-security stakeholders.
 - Providing a common operational picture and situational awareness between internal and external stakeholders
 - Enhancing the capacity of safety-security stakeholders to engage in collaborative cyber-physical problem solving.
 - Providing a more secure environment for airport personnel, passengers etc.

Practitioners' Event 2021-09-24

5



VI. Review of SATIE solution

1. Did you identify any challenges or barriers (e.g., organizational challenges, technological challenges) during the presentation of the SATIE solution?
 - Can you think of anything that the SATIE solution could do differently to address the challenges or barriers mentioned?
2. Can you think of any other additional features/functionalities SATIE could have?

Practitioners' Event 2021-09-24

6



Further information and results can be found at <http://satie-h2020.eu/>

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 832969. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein.

Practitioners' Event 2021-09-23

7



Annex 4 – State-of-the-art in Italian cybersecurity rules and regulations

Cybersecurity is one of the interventions envisaged by the Italian National Recovery and Resilience Plan (PNRR) transmitted by the Government to the European Commission on 30 April 2021. At European Union level, Directive (EU) 2016/1148 of 6 July 2016 sets out measures for a high common level of security of networks and information systems in the Union (the so-called "NIS - Network and Information Security Directive") in order to achieve a "high level of security of the network and information systems at national level, helping to increase the common level of security in the European Union". The Directive was transposed into Italian law with Law Decree n. 65 of 18 May 2018, which

defines the measures to be adopted for the security of networks and information systems and identifies the competent subjects to implement the obligations established by the NIS directive.

In 2019, with the aim of ensuring a high level of security of the networks, information systems and IT services of public administrations, as well as of national, public and private entities and operators, the Law Decree no. 105 was adopted. Besides requiring the establishment of a national cyber security perimeter, the Law Decree no. 105 also required the definition of measures to guaranteeing the necessary security standards aimed at minimizing risks.

In addition, Regulation (EU) 1583/2019 was also issued with the purpose of providing new Community rules to protect data and fundamental information and communication technology systems from cyber-attacks that could compromise the security of civil aviation.

The Figure 6.1 below represents what has been indicated above in relation to directives and legislative provisions having the purpose of establishing guidelines and compliance rules related to the topic of cybersecurity.



Figure 6.1: Cybersecurity regulatory evolution

Hereafter, the declination of the NIS Directive is presented, implemented for the Italian legal system under the Law Decree 65/2018, in terms of objectives and identification of the potentially involved subjects.

The main objective of the **NIS Directive and Law Decree 65/2018** is to establish measures aimed at achieving a high level of network and information systems security at national level, helping to increase the common level of security in the European Union. To this end, a list of essential service operators is established, i.e. subjects that provide a service that is essential for the maintenance of fundamental social and / or economic activities and whose supply depends on the network and information systems.

Essential Service Operators have been identified in the following sectors:

- Energy;
- Transportation;
- Banking sector;
- Financial market infrastructures;
- Health sector;
- Supply and distribution of drinking water;
- Digital infrastructures.

Below, the declination of the cybersecurity perimeter within the Law Decree no. 105/2019, in terms of objectives and identification of the potentially involved subjects (Figure 6.2).

The main purpose of establishing the National Cyber Security Perimeter is to "ensure a high level of security of the networks, information systems and IT services of public administrations, public and private entities and operators based in the national territory from which the exercise of an essential function of the State depends or else the provision of an essential service for the maintenance of civil,

social or economic activities fundamental for the interests of the State and from which malfunction, interruption, even partial, or improper use may derive a prejudice to national security”.

Two categories of subjects are included in the National Cyber Security Perimeter through the implementation of the graduality criteria:

1. Subjects operating in the government sector connected to the activities of the CISR administrations (Interministerial Committee for the Security of the Republic);
2. Other subjects, public or private, operating in specific sectors, if not included in the government sector:
 - Interior;
 - Defence;
 - Space and Aerospace;
 - Energy;
 - Telecommunications;
 - Economics and Finance;
 - Transportation;
 - Digital Services;
 - Social Security / Labour Bodies;
 - Critical Technologies (art. 4 EU Reg. 2019/452).

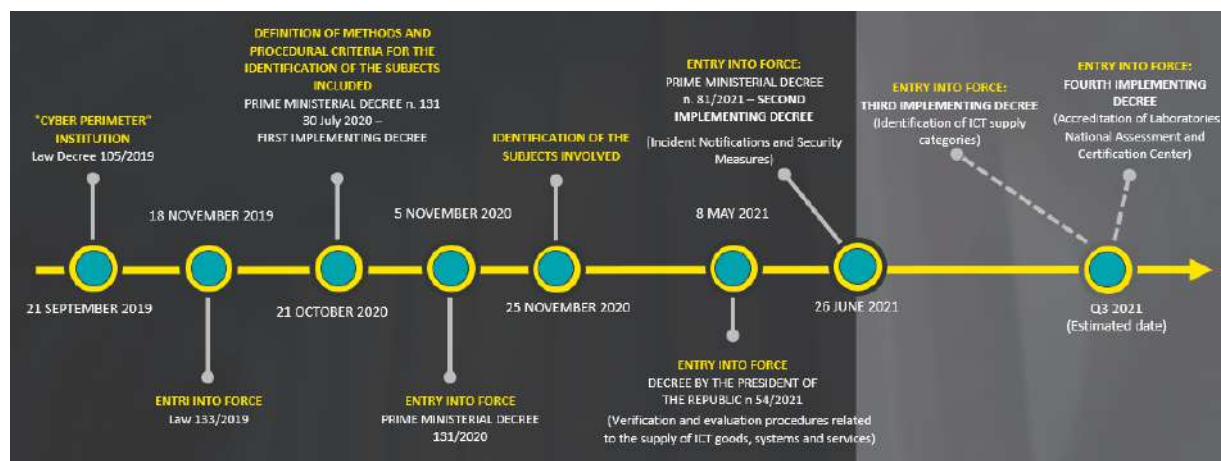


Figure 6.2: Provisions related to the Law Decree 105/2019 currently in force and upcoming Decrees implementing the Law Decree no. 105/2019

In light of the guidelines for cyber protection and information security indicated by the President of the Council of Ministers in his capacity as the top body of the national cyber architecture, the above is consistent with the National Plan for Cyber Protection and Information Security which identifies the operational guidelines, the objectives to be achieved and the lines of action to be put in place to concretely implement the National Strategic Framework for the security of the cyber space (QSN).