



# PRECINCT

## Preparedness and Resilience Enforcement for Critical Infrastructure Cascading Cyber-Physical Threats

### D6.5 Impact assessment and Policy and Standardisation recommendations

#### Document Summary Information

<b>Grant Agreement No</b>	101021668	<b>Acronym</b>	PRECINCT
<b>Full Title</b>	Preparedness and Resilience Enforcement for Critical Infrastructure Cascading Cyber-Physical Threats		
<b>Project URL</b>	<a href="https://www.precinct.info">https://www.precinct.info</a>		
<b>Start Date</b>	01.10.21	<b>Duration</b>	24 months
<b>Deliverable</b>	D6.5	<b>Work Package</b>	WP6
<b>Contractual due date</b>	30.09.23	<b>Actual submission date</b>	28.09.23
<b>Nature</b>	Report	<b>Dissemination Level</b>	Public
<b>Lead Beneficiary</b>	EOS		
<b>Responsible Author</b>	Vincent Perez de Leon-Huet		



### **Disclaimer**

The content of this document reflects only the author's view. Neither the European Commission nor the REA are responsible for any use that may be made of the information it contains.

While the information contained in the documents is believed to be accurate, the authors(s) or any other participant in the PRECINCT consortium make no warranty of any kind with regard to this material including, but not limited to the implied warranties of merchantability and fitness for a particular purpose.

Neither the PRECINCT Consortium nor any of its members, their officers, employees or agents shall be responsible or liable in negligence or otherwise howsoever in respect of any inaccuracy or omission herein.

Without derogating from the generality of the foregoing neither the PRECINCT Consortium nor any of its members, their officers, employees or agents shall be liable for any direct or indirect or consequential loss or damage caused by or arising from any information advice or inaccuracy or omission herein.

### **Copyright**

© PRECINCT Consortium. This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both. Reproduction is authorised provided the source is acknowledged.

**Contributors**

Name	Name (organisation)
Jenny Rainbird	Inlecom Commercial Pathways (ICP)
Giacomo Bianchi	European Organisation for Security (EOS)
Vincent Perez de Leon Huet	European Organisation for Security (EOS)
Georgios Sakkas	KEMEA (STRATEGY Project)
Tamara Hadjina	Koncar (PRAETORIAN Project)
Gabriele Giunta	Engineering Ingegneria Informatica SPA (ENG)
Efstathios Zavvos	VLTN (VLTN)
Vinh La	Montimage (MON)
Carmela Canonico	International Association of Public Transport (UITP)
Maria Jose Bustos	Inlecom Commercial Pathways (ICP)

**Quality Control (including ethics, peer & quality control reviewing)**

Date	Role	Name (organisation)
20.09.23.09.2023	SAB Review	Denis Caleta (ICS)
20.09.23.09.2023	SAB Review	Loredana Mancini (ICP)
22.09.2023	Peer Review	Mircea Iacob (IMEC)
26.09.2023	Peer Review	Marusa Benkic (CORTE)
22.09.2023	QAM Review	Mark Miller/Victoria Menezes Miller (CPT)
22.09.2023	Ethics Review	Vagelis Papakonstantinou (VUB), (LSTS)
28.09.2023	Final QA Review	Mark Miller/Victoria Menezes Miller (CPT)
28.09.2023	PM Review	Jenny Rainbird (ICP)

**Revision history**

Version	Issue Date	% Complete	Changes	Contributor(s)
v1.0		5%	Initial Deliverable Structure	Jenny Rainbird (ICP)
V2.0	13.04.2023	20%	Initial text provided in sections 4-8	Jenny Rainbird (ICP)
V3.0	20.04.2023	30%	Contribution to section 5	Giacomo Bianchi (EOS)
V4.0	24.04.2023	35%	Contribution to section 4	Giacomo Bianchi (EOS)
V5.0	11.05.2023	40%	Contribution to section 9	Georgios Sakkas (STRATEGY)
V6.0	11.05.2023	45%	Contribution to section 9	Tamara Hadjina (PRAETORIAN)
V7.0	05.06.2023	50%	Contribution to section 7	Vincent Perez de Leon-Huet (EOS)
V7.1	10.07.2023	55%	Contribution to section 5.5	Gabriele Giunta (ENG)
V7.5	13.07.2023	60%	Contributions to sections 1-4	Efstathios Zavvos (VLTN)

<b>Version</b>	<b>Issue Date</b>	<b>% Complete</b>	<b>Changes</b>	<b>Contributor(s)</b>
V8.0	01.08.2023	65%	Contribution to sections 3.13,	Carmela Canonico (UITP)
V8.5	24.08.2023	70%	Contributions to various sections, mainly 8.9 and 9.2	Eftichia Georgiou (KEMEA)
V9.0	31.08.2023	80%	Contributions and editing to all sections	Vincent Perez de Leon-Huet (EOS)
V9.5	15.09.2023	90%	Integrating final contributions	Vincent Perez de Leon-Huet (EOS)
V10.0	26.09.2023	100%	Integrating review comments	Vincent Perez de Leon-Huet (EOS)



## Table of Contents

1	Executive Summary .....	9
2	Introduction.....	10
2.1	Mapping PRECINCT Outputs .....	10
2.2	Deliverable Overview and Report Structure .....	12
3	PRECINCT Impact.....	13
3.1	Security-relevant Scenarios Addressed in PRECINCT .....	13
3.2	PRECINCT Capabilities.....	13
3.3	Modelling Cascading Effects to Interdependent Critical Infrastructures for Enhanced Resilience. ....	14
3.4	Digital Twins in Facilitating Cognitive Decision Support CPSoS Capabilities.....	14
3.5	Risk Assessment and Mitigation Using AI & BDA Infrastructure .....	15
3.6	AI-based Services Component for Early and Zero-day Attack Detection.....	15
3.7	Target Impact Model.....	16
3.8	Societal Impacts .....	16
3.9	Impacts on the Academic Sector.....	16
3.10	Business Impact and Sustainability .....	17
3.11	CIP Market Sector Relevance and Impact .....	17
3.12	Impacts on the EU CI Community .....	18
3.12.1	PRECINCT Living Labs .....	18
3.13	Impacts on the Transport and Logistics Community .....	23
3.13.1	Fortified Cybersecurity Measures.....	23
3.13.2	Improved Incident Response and Recovery .....	23
3.13.3	Strengthening Inter-Agency Collaboration.....	23
3.13.4	Technological Innovations for Resilience .....	24
3.13.5	Public Confidence and Trust .....	24
3.14	Impact on Municipalities.....	24
3.14.1	City of Ljubljana .....	24
3.14.2	City of Antwerp.....	26
3.14.3	City of Athens.....	27
3.14.4	City of Bologna.....	27
4	Standardisation.....	29
4.1	Standards and Standardisation Bodies .....	29
4.2	PRECINCT Standardisation Landscape .....	31
4.2.1	Technical Committees .....	31
4.2.2	Standardization Questionnaire.....	33
4.2.3	Horizon Results Booster and Recommendations .....	34
5	Standards related to Digital Twins .....	36
5.1	Definition of Digital Twin .....	36
5.2	Application of Digital Twins in PRECINCT.....	36
5.3	5.3 Key standards related to DT applications such as those in PRECINCT .....	36
5.3.1	ISO DT standards.....	36
5.4	Best Practice.....	37
5.5	Standardisation Barriers to adoption of DTs.....	37
6	Standards related to Serious Games .....	39
6.1	Definition of Serious Game .....	39
6.2	Application of Serious Games in PRECINCT .....	40
6.3	Key standards related to SG applications such as those in PRECINCT .....	40
6.4	Standardisation Barriers to the Adoption of SGs.....	41
7	Standards related to artificial intelligence .....	43

7.1	Definition of artificial intelligence.....	43
7.2	Application of artificial intelligence in PRECINCT.....	43
7.3	Key standards related to artificial intelligence in critical infrastructure protection.....	44
7.4	Potential challenges.....	44
7.5	Artificial intelligence management procedures.....	45
8	Regulatory and policy relevance.....	46
8.1	Critical Infrastructure Policy directives.....	46
8.2	Foundation legislation.....	46
8.3	Evolution of the EC directive for CIP.....	46
8.4	Current legislation.....	47
8.5	Policy relevant to Critical Infrastructure.....	49
8.6	Agencies, Groups and Networks relevant to Critical Infrastructure.....	50
8.7	PRECINCT Relevance to the Current EU Policies & Policy Recommendations.....	50
8.8	PRECINCT Relevance to Current EU Policies.....	50
8.9	PRECINCT Policy Recommendations.....	52
9	Technical Committees.....	55
9.1	PRECINCT contribution to CEN/WS IPCI.....	56
9.2	PRECINCT application of STRATEGY standard in Athens LL3.....	57
10	Contributions.....	59
10.1	STRATEGY Project.....	59
10.2	PRAETORIAN Project.....	60
10.2.1	About PRAETORIAN.....	60
10.2.2	Use case scenarios.....	61
10.2.3	10.2.3 Validation Exercises.....	62
10.2.4	Validation exercises concerning standardisation.....	63
11	Conclusions.....	64
	References.....	65

## List of Figures

Figure 5-1: Standards code exposition.....	31
--	----

## List of Tables

Table 2-1: Adherence to PRECINCT's GA Deliverable & Tasks Descriptions.....	10
Table 3-1: Living Labs Thematic Focus, CIs and Stakeholders.....	19
Table 3-2: Transferability Demonstrators Thematic Focus, CIs and Stakeholders.....	19
Table 4-1: International and European Standards Bodies.....	29
Table 4-2: Features of standardisation documents.....	30
Table 4-3: Technical Committees Description.....	31

## Glossary of terms and abbreviations used

Abbreviation / Term	Description
ACM	Association for Computer Machinery
AI	Artificial Intelligence
BD	Big Data
BDA	Big Data Analysis
CA	Consortium Agreement
CEN	European Committee for Standardisation
CENELEC	European Committee for Electrotechnical Standardisation
CEPT	European Conference of Postal and Telecommunications Administrations
CER	Critical Entities Resilience
CI	Critical Infrastructure
CICC	Critical Infrastructure Coordination Centers
CIP	Critical Infrastructure Protection
CPSoS	Cyber-Physical CI Systems-of Systems
CSIRT	Computer Security Incident Response Team
DC	Data Capture
DMP	Data Management Plan
DT	Digital Twins
Dx.x	Deliverable x.x
EC	European Commission
ESO	European Standards Organisation
ETSI	European Telecommunications Standards Institute
EU	European Union
GA	Grant Agreement
HPP	Hydropower Plant
IEC	International Electrotechnical Commission
IEEE-SA	The Institute of Electrical and Electronics Engineers Standards Association
IGDA	International Game Developers Association
ISO	International Standards Organisation
JTC	Joint Technical Committee
KER	Key Exploitable Results
KG	Knowledge Graph
LIST	Luxembourg Institute of Science and Technology
LL	Living Labs
ML	Machine Learning
MS	Member State
NC	National Committee
NLP	Natural Language Processing
PEP	PRECINCT Ecosystem Platform
PSA	Physical Situation Awareness
RMF	Resilience Methodological Framework
RI	Resilience Index

<b>Abbreviation / Term</b>	<b>Description</b>
SC	Subcommittee
SG	Serious Games
SIGGRAPH	The Special Interest Group on Computer Graphics and Interactive Techniques
TC	Technical Committee
TDs	Transferability Demonstrators
TX.X	Task X.X
UNSCC	United Nations Standards Coordinating Committee
VA	Vienna Agreement
WG	Working Group
WKSP	Workshop
WPx	Work Package x

# 1 Executive Summary

PRECINCT has carried out extensive work in modelling and assessing the potential cascade effects of harmful events that occur to Critical Infrastructures (CIs) and has developed a framework for leveraging this information to improve the management and resilience of CIs as well as the precognition and associated planning for said cascade effects.

The aim of the present deliverable is to analyse and assess the potential impacts (in Chapter 3) of the work carried out by the PRECINCT consortium partners and resulting project outputs. To do this, first, we analyse the security scenarios PRECINCT has examined, and the capabilities developed by the partners in addressing these. We demonstrate here that PRECINCT is expected to project several impacts spread across multiple levels from societal impacts, to impacts affecting the industry and academia, the business and sustainability sectors, the market sector, as well as the European Union (EU) Critical Infrastructure (CI) and transport & logistics communities, and the municipality sector.

PRECINCT is further involved with a variety of standards in association with the methodologies and technologies employed. This deliverable explains these in detail in Chapter 4 – Standardisation. Regarding the Digital Twins (DTs) and Serious Games (SGs) (two major components of the project), these are discussed separately in Chapters 5 and 6. In discussing so, we identify several best practices, barriers / challenges and opportunities related to the adoption of standards in these two topics. A further chapter (Chapter 7) explores these same ideas in the domain of Artificial Intelligence (AI), which was extremely relevant to the project, as many of the tools were AI-enabled.

This deliverable will also present an extensive discussion around policies and legislation related to Critical Infrastructure Protection. The PRECINCT consortium has evaluated these in relation to outputs of the project, and is proposing several relevant recommendations for improving policies (in Chapter 8). These discussions and recommendations remained mainly at the EU level, mainly due to the European or transborder nature of the project, as well as the two newest and most relevant pieces of legislation related to critical infrastructure protection (the NIS2 and the CER Directives) were released in December 2022, and PRECINCT offers many ways to allow for operators and members states to comply. Additionally, further advances in the relevant policy area would further allow PRECINCT's results to be further exploited and increase the resilience of critical infrastructures across Europe.

## 2 Introduction

Standardisation and Policy Recommendations are an important output of European Research Projects. The research conducted can provide insights to policy makers that will allow them to fill the gaps, avoid duplications, highlight best practices or put structures in place that are currently missing. PRECINCT is a highly technical project and includes various scientific fields joining together to increase critical infrastructure protection, such as Engineering, Computer Science, Data Science, and more, leading to many opportunities for standardization and policy recommendations. Although the task focusing on standardization and policy recommendations (T6.5) only started in M12 of the project, PRECINCT partners engaged in the work from the beginning to identify as many opportunities as possible to contribute to standardization efforts and develop meaningful policy recommendations.

The purpose of this deliverable is to provide a comprehensive report defining a roadmap for the implementation of the PRECINCT methodology approaches and tools. The ambition of this report is also to deliver policy recommendations and best practices in support of relevant EU strategies, Security Research Strategy and the Industry for Security. The deliverables is structured to deliver these outputs with a separate White Paper provided at the end of this report.

### 2.1 Mapping PRECINCT Outputs

The table below provides an overview of the tasks related to D6.5 and maps the activities with the document structure to provide a justification as to how the document addresses the respective outputs and work performed.

Table 2-1: Adherence to PRECINCT's GA Deliverable & Tasks Descriptions

PRECINCT GA Component Title	PRECINCT GA Component Outline	Respective Document Chapter(s)	Justification
<b>DELIVERABLE</b>			
D6.5 Policy and Standardisation Recommendations	<i>PRECINCT White Paper defining roadmap, policy recommendations and best practice in support of relevant EU strategies, Security Research Strategy and the Industry for Security.</i>	Chapters 8, 12	<i>Chapter 8 describes the EU policies relevant to PRECINCT and policy recommendations developed by the project. The White Paper makes up chapter 12, which includes the roadmap and condenses the Project Ideas surrounding Policy and Standardisation Recommendations</i>
<b>TASKS</b>			
<i>Task 6.5 Policy and Standardisation recommendations</i>	<i>The main aim of this task is to provide a Target Impact Model, to assess the potential impact of the PRECINCT Platform and its key components both from an economic and social perspective and provide input to T7.2.</i>	Chapter 3	<i>Target Impact Model to assess PRECINCT Platform impact across various stakeholder communities</i>

	PRECINCT will analyze existing policies, standard and best practices relevant to CI protection, to provide a set of policy recommendations for targeted audiences based on the project outputs and to support the standardisation and broad application of the proposed methodologies and supporting tools.	<i>Chapters 4, 5, 6, 7, 8</i>	Existing policies are analysed in Chapter 8 Existing standards are analysed in chapters 4, 5, 6 and 7 as well as any best practices Policy recommendations are given in Chapter 8
	The main output will be a White Paper which defines a roadmap of required actions and a set of key policy recommendations and best practices with the aim of maximising the impact of the PRECINCT project in support of relevant EC strategies, the Security Research Strategy and the Industry for Security Strategy.	<i>Annex 1</i>	The white paper developed by the project is attached in Annex 1 of this Deliverable
	PRECINCT also aims to establish an Ecosystem Infrastructure for connecting stakeholders of interdependent CIs and Emergency Services to collaboratively and efficiently manage CI security and resilience as well as validating new detection and mitigation models and associated services in a real-time real-life context.		PRECINCT Ecosystem infrastructure (reported in deliverable D2.3)
	This task will also assess the societal impact of the research work conducted in the project which endeavours to address threats to society such as crime, terrorism, pandemic, natural and man-made disasters, etc.	<i>Chapter 3</i>	Societal impact is discussed in Chapter 3

	and will deliver a Societal Impact report.		
	Input from standardization groups and all the relevant stakeholder community will be considered to inform CI stakeholders and decision makers about how the PRECINCT results can help them to achieve their aims as well as how to integrate the project's outputs within their own internal cyber security roadmaps.	<i>Chapter 4</i>	Engagement with standardisation groups is outlined in Chapter 4

## 2.2 Deliverable Overview and Report Structure

Deliverable D6.5 is structured on three main pillars: an impact assessment, standardization activities and policy recommendations. Apart from Chapters 1 and 2 which are the introductory chapters, the rest of the deliverable is structured as follows:

- Chapter 3 summarises the key impacts that the PRECINCT project has in a number of key areas. The chapter summarises key technologies and then discusses impact in areas including, societal, industry and market impacts.
- Chapter 4 explores themes of standardisation, looking at relevant standardisation bodies and the standardisation landscape relevant to the PRECINCT project. The next two chapters focus on two specific standardization areas related to PRECINCT, as they were two of the main components of the project.
- Chapter 5 explores standardisation related to Digital Twins.
- Chapter 6 explores standardisation related to Serious Games and outlines any barriers to standardization.
- Chapter 7 explores standardisation related to Artificial Intelligence and outlines any barriers to standardization as well as opportunities.
- Chapter 8: analyses the PRECINCT project relevance to policy.
- Chapter 9: describes the PRECINCT contribution to standards related to CEN workshop agreements.
- Chapter 10: describes a summary of sister project contributions to standards, including the STRATEGY and PREATORIAN projects.
- Chapter 11 concludes the deliverable; however, a white paper is added at the end of Chapter 12 to provide a condensed report on the ideas developed during the project, as well as the roadmap of required actions and policy recommendations and best practices with the aim of maximising the impact of the PRECINCT.



### 3 PRECINCT Impact

As with any research project, one of the main goals is to have an impact in the field in which the research, in this case critical infrastructure protection regarding cyberphysical threats. This section will outline the various aspects of PRECINCT and assess the various impacts they have had or will have by the end of PRECINCT.

#### 3.1 Security-relevant Scenarios Addressed in PRECINCT

PRECINCT is focused on improving the resilience of Critical Infrastructures to physical, cyber and hybrid threats, by addressing the interconnectivity of Critical Infrastructures within a geographical location. The approach helps acknowledge the cascading effects of an attack or an event on one or more critical infrastructures and the impact this has on the infrastructure in the region as a whole.

The scenarios that PRECINCT addressed are (i) management of intentional or malevolent events, such as attacks by terrorists who want to exploit the properties of Critical Infrastructure for their own ends; and (ii) non-intentional events such as natural disasters, or accidents.

Relevant to a broad range of physical, cyber and hybrid threats, the project is focused on a number of Multimodal Transport, Energy, Water and ICT/Telecommunications threat scenarios that validate the approach and tools for a range of Critical Infrastructure stakeholders, which are representative of the broader industry within a geographical area. The scenarios can be summarised as:

##### (a) Intentional/malevolent threats:

- Combined attack on access control systems of airport resulting in fatalities, services disruption and physical damage to the infrastructure with cascading effects on local metro, rail and road transport.
- Combined bomb and a cyber-attack with simultaneous denial of service attacks to critical parts of the Industrial Control Systems of the electricity and communication operators, which provide important services for business continuity of the transport mobility hub resulting in damage and disruption of services and resulting casualties.

##### (b) Unintentional threats:

- Severe localised flooding with cascading effects on water critical infrastructure with cascading impacts on transport and traffic critical infrastructure in the region resulting in damage, service disruption and casualties.
- Earthquake disaster resulting in damage to communications and energy infrastructure with impact on first responders and transport resulting in damage and disruption of services and resulting casualties.
- Severe weather-related disaster resulting in damage and disruption to transport and traffic related infrastructure.
- An Industrial accident resulting in physical damage to rail and communications infrastructure resulting in damage and disruption of services.

#### 3.2 PRECINCT Capabilities

PRECINCT is establishing an Ecosystem Platform for connecting stakeholders of interdependent CIs and Emergency Services to collaboratively and efficiently manage security and resilience by sharing data, Critical Infrastructure Protection models and related new resilience services encapsulated in Digital Twins. In connection with the Digital Twins, the Serious Game approach in PRECINCT provides a means of identifying vulnerabilities as well as testing and validating new detection and mitigation models and associated services in a real-time real-life context.

The main project outputs are:

1. A PRECINCT Framework Specification for systematic Critical Infrastructure security and resilience management, fulfilling industry requirements and integrating new insights from reference EU projects.
2. A Cross-Facility collaborative cyber-physical Security and Resilience management platform enabling CI stakeholders to develop AI-enabled Smart PRECINCT Ecosystems and enhanced resilience support services.
3. A vulnerability assessment tool that uses Serious Games to identify potential vulnerabilities of the Critical Infrastructures to cascading effects, resilience enhancements and coordinated mitigation measures.
4. PRECINCT's Digital Twins to represent the Critical Infrastructures network topology and metadata. Closed-loop Machine Learning is used to detect potential anomalies and alert CI stakeholders timely based on alert conditions. This also facilitates the activation of suitable response and mitigation measures based on the expected cascading effects.
5. Deployment of the Smart PRECINCT Ecosystems in four large-scale Living Labs (LLs) and in transferability validation demonstrators to provide measurement-based evidence of the targeted advantages.
6. Capacity Building activities including Dissemination, Exploitation and Resilience Strategy, as well as Policy and Standardisation Recommendations.

In more detail, PRECINCT improves upon the state of the art in the areas described in the remainder of this Section.

### **3.3 Modelling Cascading Effects to Interdependent Critical Infrastructures for Enhanced Resilience.**

Instantiating detailed mathematical models is always complex and resource intensive, and most of those models are not able to include the intrinsic uncertainty inherent to critical infrastructure networks. To address this, PRECINCT has developed an interdependency graph approach, which as a basis for a cascading effects simulation framework. An automaton model describes the operational states of critical infrastructures the model is instantiated in a straightforward way incorporating the intrinsic uncertainty and randomness of cascading effects into the simulation. The simulation results serve as an input for the quantification of resilience measures via the resilience methodological framework and the serious games approach. The cascading effects simulation and interdependency graph approaches are further described in Deliverable 1.2 "Critical Infrastructure Interdependencies and Cascading Effects interdependency Graphs".

### **3.4 Digital Twins in Facilitating Cognitive Decision Support CPSoS Capabilities**

Cyber-Physical CI Systems-of Systems consist of spatially distributed Cyber Physical Systems communicating through a network infrastructure that enables their interoperability and the interaction with human operators. At design time, the Cyber Physical Systems behaviour can be modelled using hybrid systems, a mathematical framework and the decision logic that combines discrete transition systems capturing the computational behaviour of the software component with continuous ordinary differential equations describing the behaviour of the physical substratum with which the software component is deeply intertwined.

In PRECINCT (discrete-event) modelling of the CIs interdependency behavioural aspects (particularly resilience) are enriched to consider reconfiguration of components or systems. Supervisors will be synthesized based on discrete event models of CI Network subsystems and of the (security and resilience) requirements that the complete system should satisfy. Description of the behaviour of the relevant actors in the LL CPSoS will be used for building "Digital Twins" in support of achieving cognitive decision-support CPSoS capabilities. New components/systems that arrive (as an evolution) will need to identify their behavioural capabilities (possible behaviour they have to offer to the CI CPSoS) and requirements (necessary architectural, temporal and behavioural restrictions) such that the Digital Twin may do the synthesis online (during system operation) to

guarantee a resilient and safely operation. PRECINCT will utilise hardware accelerated Fast-Bayes or Bayesian Neural Nets or Reinforcement Learning algorithms for global optimisation and to update models and ground truths. A more thorough description of the Digital Twins can be found in the following deliverables: D4.1 “User story maps, architecture blueprint, and Digital Twin design guidelines report”, D4.2 “Tools to support the development of PRECINCT DTs” and D4.3 “A PRECINCT Digital Twin Instantiation (software)”.

### **3.5 Risk Assessment and Mitigation Using AI & BDA Infrastructure**

Visualization interfaces and solutions need to integrate computational modules and be compatible with advanced Big Data analytics frameworks which create limitations in BDA (Big Data analytics) applications associated with unconnected CIs. Further limitations arise from gathering all required geo-distributed data in a specific DC to process them, which is a costly operation in terms of resources and time.

In PRECINCT the Visualization Engine includes cross-platform visual and analytics tools, supporting the provision of interactive visualizations, including generic and custom components, combining visual analytics and augmented reality. A graph module structure defines the connections between different application modules and orchestrates both new resilience workflows and response actions. NLP toolboxes for threat prediction integrate Service Agents representing CI services creating new capabilities for predicting risk levels.

### **3.6 AI-based Services Component for Early and Zero-day Attack Detection.**

Anomaly detection has been applied successfully to numerous domains to identify unknown attacks. However, there are existing issues such as high error rates or large dimensionality of data that make its deployment difficult in real-life scenarios.

In PRECINCT, semi-supervised and unsupervised machine learning techniques are applied to detecting anomalies and attack patterns to CIs in a holistic way. (i.e. not only considering their normal behaviour but also possible impacts on other stakeholders of the related value chain or geographical area of influence). Furthermore, a novel computational intelligence technique, inspired by immunology, called Artificial Immune System (AIS), has emerged as a candidate to identify anomalous behaviour in a network and has achieved excellent results in anomaly detection and intrusion detection systems. AIS algorithms were fully exploited in PRECINCT Digital Twins.

Expected KPI improvements are:

- At least 2 new scenarios per LL and 3 new vulnerabilities from cascading effects identified compared with the present number of previously unanticipated (Unknown) attack scenarios and vulnerabilities identified through game play of the individual CIs participating in the Ljubljana Antwerp, Athens and Bologna LL’s.
- At least 1 person per CI participating in LLs achieving Serious Game training qualifications in the defence of cascading effects from CI interdependencies.
- The delivery of 6 Innovative Resilience Service Models at both CI level and coordination level developed by the end of the project.
- At least 20 CIs involved in living labs and demonstrators.
- Up to 10 customised dashboards per user organisation/role
- Between 4-10 Services Blueprints used per living lab
- Up to 10 coordinated response services to mitigate cascading effects and enhance resilience tested.
- 6 modelled disaster scenarios in the initial prototype
- Up to 3 new models/controls produced per living lab as a result of the Serious Games mechanisms
- 30% increase in improved capabilities of end users to manage cyber-physical threats more efficiently against baseline KPIs

- Integration of up to 10 heterogeneous models and tools to capture system-wide properties for resilience management per LL
- 15% improved operational resilience in the LLs regions as a result of benchmarking the PRECINCT Ecosystem against baseline KPIs
- Up to 4 member states demonstrating the replication scenarios
- 20% increase in improved accuracy in cyber-physical threats detection against baseline KPIs
- 20% increase in “Resilience Index” against baseline KPIs
- 10% increased speed in mitigation and reaction against baseline KPIs
- 20% increased ROI estimated by economic models for specific CI types against baseline KPIs

### **3.7 Target Impact Model**

The Target Impact Model is one of the main pillars of Task 6.5 “Policy and Standardisation Recommendations” and will outline the different areas in which PRECINCT will have an impact and assess the extent of said impact. Various social, economic and sectoral aspects will be considered, also highlighting specific outputs that are potentially more relevant than others by sector.

### **3.8 Societal Impacts**

In order to fully be able to understand the societal impact that the PRECINCT project will have, a separate large research study would be warranted. Instead, by increasing the resilience of the critical infrastructures of a geographical area, the main societal impact is greater physical security and societal resilience. In societies equipped with PRECINCT developed tools, the ability to respond to man-made and natural threats would be greater. Additionally, we get an initial understanding of how societies may be impacted by PRECINCT by looking at the impact the project had on the Living Labs and Transferability Demonstrators that were able to implement some or all of the PRECINCT tools.

### **3.9 Impacts on the Academic Sector**

PRECINCT produced various scientific articles that have helped to disseminate the results of the project to the scientific and academic community. While it is too early to truly measure the impact that this will have on the academic community, as it will take some time before papers are written using the knowledge generated by PRECINCT, it is foreseen that PRECINCT concept and tools will continue to be used in academic research, including in future Horizon Europe (and successor programmes). The PRECINCT project also has significant impact to academic sector through the understanding of a new complexity of critical infrastructure protection processes. Interdependences and possible cascading effects should be an important focus also for further research and academic activities in the future. One of the most important points about the transferability of PRECINCT results into academic sector is that the project provides proper integration through these new understandings of complexity of Critical infrastructure protection processes in academic curriculum. New experts who are in the educational process need to better understand this necessity for the comprehensive approach for protecting critical infrastructure as one of the important factors for normal operation of whole societies. The second important point is that just one academic discipline is not in the position any more that with research inside this domain could find proper solutions and approaches for upgrading systemic approach to protecting critical infrastructure. It is critical that also in the academic area we start to work outside of silos approach. The PRECINCT project is a great example how complex and diverse should be approaches for proper protecting a critical infrastructure.

### 3.10 Business Impact and Sustainability

PRECINCT aims to provide pre-commercial tools by the end of the project, ready for potential commercialisation in open markets. The first stage of the commercial development during the project and in the short term after project end will be to build a community around the PRECINCT outputs and drive usage across as many customer segments as possible. To support this, the initial outputs from the project will be provided free of charge to users (upon registering basic user details) and PRECINCT will deliver a range of open-source products for those stakeholders who will adapt the relevant PRECINCT outputs e.g. the PRECINCT Blueprint directory, PRECINCT E-learning Module. However, the business plan will further outline how consortium members or other third parties can expand the initial “Community offering” to deliver a long-term, commercially viable business (For more details on the market analysis and Exploitation plan, see D6.4 “Business Model Market Analysis and Exploitation Plan”).

### 3.11 CIP Market Sector Relevance and Impact

PRECINCT is developing a number of commercial solutions aimed to manage the physical/virtual security of critical infrastructures in the face of physical or cyber incidents/threats as well as potential cascading effects between critical infrastructures, instead of focusing on isolated critical infrastructures as most of competing alternatives do. For this reason, PRECINCT’s related market is not one but rather a number of segments in several security-related markets (Critical Infrastructure Protection, Cybersecurity, Security Operation Centres and Homeland Security & Emergency Management markets). This adds complexity when analysing the impact that PRECINCT may have on these markets; however, the most closely related market is the critical infrastructure protection (CIP) market and the one that will be more benefitted from PRECINCT’s key exploitable results.

Currently, the CIP market differentiates between hardware tools to prevent physical events and software tools to cover cyber threats/attacks, with both types of solutions centred on protection of isolated critical infrastructures. There is still no market segment that includes solutions such as the one proposed by PRECINCT, because the project is aimed to address both physical and virtual sides as well as related cascading effects between critical infrastructures, while fostering collaboration between stakeholders at different levels of the CIP value chain, providing a holistic approach that is not feasible with current commercial alternatives. The lack of an integral view of interconnected critical infrastructures is reflected by the fact that there are still few or no coordinated CIP centres. This situation can be changed with the commercial launch of the PRECINCT’s tools, as they will facilitate the setup of these centres as new end users.

The CIP market and other markets related to precinct share some common challenges; one of the most prominent is their high complexity and fragmentation due to the high number of interdependencies between critical infrastructures and also because of the heterogeneity in regulations between geographical areas. While this is a clear barrier for new market entrants, it may be an opportunity for PRECINCT’s solutions: cloud-based AI tools (i.e. digital twins, cascading effects simulation, etc.) may help simplify this underlying complexity by pinpointing potential areas of friction, favouring collaboration between stakeholders during crises and, overall, contributing towards a more efficient management of interconnected critical infrastructures during a crisis. This increased efficiency will help raise awareness on the importance of integral tools and collaboration among key stakeholders, boosting adoption rates.

PRECINCT’s solutions (like serious games, digital twins, cascading effects simulator, etc.) can also help represent the critical infrastructure ecosystem and simulate its response to physical or cyber incidents with high accuracy. End-users can test new security protocols and approaches in a risk-free environment for better management. If properly quantified, this enhanced efficiency will serve to improve acceptance from key decision makers and increase adoption rates of the technologies.

PRECINCT's simulation capabilities will also allow to ease the training process of emergency response units and other operators. This way, the sector will become more attractive to younger people, creating new employment opportunities that will ultimately lead to lowering unemployment rates and reducing staff shortages in the sector.

Initially, it is expected that the markets most impacted by the commercial launch of the project's KERs are those where the living labs were performed, namely Slovenia (LL1), Belgium (LL2), Greece (LL3) and Italy (LL4), expanding shortly afterwards to the rest of Europe where the consortium partners are based. The living labs will also help position the KERs in terms of verticals where they are first demonstrated and validated, improving market share of the Transport & Logistics, Government, Defense and Telecom verticals. Together, these verticals are expected to be worth approximately USD 46.6 billion globally by 2026.

The markets related to security in general and to critical infrastructure protection in particular, are still emerging and highly fragmented with numerous market players – there are a few large and well-established companies (such as Lockheed Martin, Honeywell, IBM or Samsung) with a somewhat limited market share, while smaller, lesser-known companies hold the greatest share. These conditions can make it easier for PRECINCT's partners to enter the market successfully.

In summary, PRECINCT's solutions will streamline the management of critical infrastructures through a better view of interconnections between infrastructures, increased collaboration between stakeholders, and improved simulation/testing capabilities. These features will contribute to highlight the importance of an integral approach in the protection of critical infrastructures, raising awareness among key stakeholders and ultimately paving the way to the creation of regional/national coordinated centres. This will create new opportunities in the CIP market, and even favour the creation of a new segment within the CIP market to serve these new end users. The initial impact will be more prominent in the verticals related to PRECINCT's living labs and on European markets, as these are where the consortium partners are based and are more experienced with, expanding shortly afterwards to other markets such as the US.

## **3.12 Impacts on the EU CI Community**

### **3.12.1 PRECINCT Living Labs**

PRECINCT has deployed four Living Labs and three Transferability Demonstrators. The Living Labs have each dedicated threat scenarios and Critical Infrastructures focus. Within their operations, the Living Labs have set up their stakeholders community in order to implement the co-creation principle and the user-centred approach. The LLs stakeholders have played a crucial role all along the project phases and PRECINCT ecosystem components development and testing stages. Each LL has its own direct stakeholders, from public and private domain, and represented as consortium partners in the project:

- Energy Providers
- Telecoms companies operators
- Water distribution providers
- Road infrastructure providers
- Rail, Metro and bus infrastructure providers and operators
- Airports and Ports operators
- Regional administrations, councils
- and Police first responders.

In addition to the direct stakeholders, some “indirect” stakeholders were also participating in the activities. Not directly involved as partners of the project consortium, those indirect stakeholders were also from the private

and public domains and have been consulted at different moments of the Living Lab activities (electricity providers, first responders – fire department, medical services, etc.).

Four Living Labs were implemented and operated within the WP5. These four LLs aim to provide measurement-based validation of KPIs improvement across multiple axes of instrumentation aligned to the project's objectives to affirm that these objectives are satisfactory.

Each LL has specific focus in terms of CIs, stakeholders, thematic, and threat scenarios, summarized in Table 3-1:

Table 3-1: Living Labs Thematic Focus, CIs and Stakeholders

'LL	Thematic Focus	CIs & Stakeholders
Ljubljana	Multi-CI Coordination Centre for major city Transport Hub	National rail and City bus transport, Electricity (DSO), Telecommunication infrastructure) and Municipality Police
Antwerp	Early warning system to prevent the impact of flooding Emergency Services coordinated CIs through city level Digital Twin	Police Zone Antwerp, Multidisciplinary Emergency Operational Command Post (CP-OPS), All territory CIs linked to Police, Water Management
Athens	Increased resilience against cyber-physical incidents affecting urban transport	Athens Airport, Metro, Motorway
Bologna	Region level Digital Twin linking multiple CIs with city ICT and IoT systems	Region's ICT provider, Airport, Railway

The following sections (3.12.1.1 to 3.12.1.7 and 3.14) of this report provide an overview of the PRECINCT Living Labs and transferability demonstrators as to the impacts of the PRECINCT ecosystem platform within the Living Lab stakeholder communities.

In addition to the Living Lab Operations and their stakeholders, three Transferability Demonstrators had the challenging mission to follow the LLs planning and monitoring activities so that they could transfer insights into their own demonstrators to obtain maximum value and contribute to the knowledge of 'packaging' outputs for maximum impact and commercialisation potential. Translated into an implementation roadmap, the activities carried out in T5.7 demonstrated the replication of the PRECINCT concept and the actionable KER coming out from the PRECINCT activities.

The three demonstrators focused on the following CIs and thematises, as given in Table 3-2:

Table 3-2: Transferability Demonstrators Thematic Focus, CIs and Stakeholders

Transferability Demonstrator	Thematics investigated	CIs
Luxemburg - Luxembourg	Flood Severe weather Electricity blackout Network disturbance	Traffic and Mobility (at national, regional, and local levels) <ul style="list-style-type: none"> <li>• Airport</li> <li>• Bus</li> <li>• Bikes</li> <li>• Tramway</li> <li>• Funicular</li> <li>• Etc.</li> </ul>

Ireland - Dublin	Cyber attack	Traffic and EVs charging infrastructures
Estonia - Tallinn	Physical attack Cyber attack Natural hazard	Water supply Services CIs (hospitals, Social welfare institutions, emergency services, schools) Emergency services Ports

### 3.12.1.1 PRECINCT Living Lab 1 – Ljubljana, Slovenia

Living Lab 1 Operation Ljubljana research the usage of PRECINCT innovative tools from the given “toolbox”. LL1 stakeholders had the opportunity to:

- explore new tools and technologies, help develop and deploy the solutions relevant to their critical infrastructure needs and resilience.
- upgrade the understanding and importance of interdependence and impacts, which in certain crisis situations events bring cascading effects.
- increase early detection of threats and improved response procedures.
- upgrade the awareness that they are in real interdependence with other critical infrastructures when ensuring the operation of their critical infrastructure.
- manage better situational awareness, faster reaction and more effective communication and coordination at all levels of operation.

### 3.12.1.2 PRECINCT Living Lab 2 – Antwerp, Belgium

Living Lab 2 Operation Antwerp investigated a natural hazard (a flood) impacting the Traffic and Water management CIs. Thanks to the PRECINCT innovative approach, the LL2 CIs operators and the Antwerp police had the opportunity to:

- Investigate a flood event and assess its cascading effects on their CIs;
- Identify the vulnerabilities and map the interdependencies;
- Assess the LL2 DT designed and developed to interconnect the flood model prediction and the water and traffic CIs. Thanks to the user interface, the LL2 DT provides an early warning system to detect the flood threat, and visualisation of the dependencies and CIs on the Antwerp city map, and the flood prediction and probabilities on this map.
- Assess the PRECINCT Serious Games (SG) specifying the threat scenario cascading effects and identifying the vulnerabilities. This tool enhances the resilience tactical and strategic options for the CP-OPS disciplines and crisis management team of the city. Primarily used to training purposes, the SG is an experiential learning tool where the collaboration and interaction of the players enable to collect a deeper understanding of the actions and decisions undertaken in the game.
- Participate to workshops organised with the CP-OPS disciplines and the CIs representatives to share knowledge, experiences, needs and practices.

### 3.12.1.3 PRECINCT Living Lab 3 – Athens, Greece

Through Living Lab 3 operations, as well as the usage of PRECINCT innovative tools LL3, CIs operators had the opportunity to:

- Investigate new tools and technologies, as well as assist in the development of solutions relevant to their critical infrastructure needs and resilience.



- LL3 CIs infrastructure operators have identified interdependencies with their infrastructures and among others operating in the same geographical area. Finally, through utilizing project simulation techniques they were able to assess the impact of various threats and study the impact of contingencies plans, helping them to consider or design more efficient action plan.
- Through dedicated workshops and visits on CIs operations centers to exchange knowledge and exercises of crisis management from past events as well as processes and best practices from other critical infrastructure operators.

Finally, PRECINCT has provided to LL3 CIs operation a DT solution for fostering collaboration, enhancing communication, and promoting proactive crisis management strategies through threat and cascading effects simulations. The project also enables LL3 critical infrastructure operators to design and study the dynamics of various threats and mitigation strategies for managing crises through simulations.

#### *3.12.1.4 PRECINCT Living Lab 4 – Bologna, Italy*

Thanks to the activities carried out by the LL4 partners within the PRECINCT project, the following main objectives have been achieved:

- The creation of a Digital Twin that allows the integrated management of the critical infrastructures of the Bologna Living Lab, allowing the interaction of the different operators of the CIs. The Digital Twin contains dashboards dedicated to the critical infrastructures of Bologna, allowing to have both an overview of the operating status of the CIs, and a specific vision for each critical infrastructure involved;
- The creation of new synergies within LL4, in which partners have made themselves available and collaborated continuously to create digital solutions that cover the needs of all actors involved. Given that the LL4 scenario involves a cyber-physical threat, it was essential to outline all the aspects that the Digital Twin had to manage, correlating threats to provide specific calculations on the mitigation actions to be taken;
- Opportunities for discussion between partners, direct and indirect stakeholders. The LL4 partners have created different moments of restitution, directly involving transport operators, regulatory figures and the municipality of Bologna. For example, at the Brussels Conference held in May 2023, LL4 involved Marcomi Express (people mover service provider, TPER (UMP) and SRM (public transport authority) to present the main results obtained so far within the PRECINCT project. Also for this reason the Bologna Living Lab took the opportunity to host directly in Bologna the final event of PRECINCT, which also allowed the project partners to experience the events and CIs described in the LL4 scenario.

The project activities related to Living Lab 4 has been carried out with a view to a future exploitation of the project outputs, so the Living Lab 4 partners will continue to work together thanks to the synergies created within the PRECINCT project.

#### *3.12.1.5 Transferability Demonstrator – Luxembourg*

Luxembourg's role as a transferability demonstrator (TD) in the PRECINCT project allowed the city to develop valuable insights and practical knowledge. The main work done with this TD was implementing the PRECINCT Ecosystem Platform (PEP) components within Luxembourg. After checking the compatibility of Luxembourg's stakeholders, critical infrastructure operators, emergency services, and city administrations to comprehend the specific characteristics and challenges of the country's critical infrastructure systems, LIST worked towards incorporating achievements made at the 4 European Living Labs which were made with participation from emergency services and city administrations for each of their corresponding services or layers. Findings and insights from these living labs fed back into the ongoing planning and development done within LIST. LIST emphasized the sustainability of the project outcomes by focusing on capacity building, dissemination, and

exploitation. LIST engaged in trainings, workshops, and knowledge-sharing activities to ensure the effective understanding and transferability of the PRECINCT project's findings and solutions. This aimed at aligning with Luxembourg's commitment to sustainability to extend and influence the broader landscape of critical infrastructure protection and resilience. The country and LIST's active engagement in adapting the project's framework and conducting experiments and tests and real-world data ensures the applicability and effectiveness of the developed solutions. The dedication to knowledge transfer and sustainability further solidifies their positions as partners in advancing preparedness and resilience in critical infrastructure, both within the country and on a broader scale. Additionally, LIST designed its DT which will help it to produce trainings and real-life scenarios to increase the resilience of the cities' critical infrastructures.

#### *3.12.1.6 Transferability Demonstrator – Estonia*

Involvement in the PRECINCT project is strategically coherent with Tallinn's priorities and ambitions to enhance data-based decision making and policy development, enhance critical infrastructure resilience and situational awareness. The gained experience and developed models can be used to test out other scenarios and raise interest in using this kind of modelling for other fields critical to the city. The developed digital twin and simulation tools can be modified for different scenarios and the process used as a model for developing models for other kind of data and scenarios.

The utilities digital twin model developed will be connected to the city's general digital twin and also be used as a prototype for including other utilities and simulation options in the digital twin. Taking part of the project gives an opportunity to test out suitable data formats and digital twin, modelling and simulation software, which is a valuable input for developing the city's digital twin.

In parallel with the development of DT, work continues increasing the crisis preparedness of the city's institutions and practicing cooperation.

1. **Tallinna Children's Home** does not currently have a risk analysis of operations. Since the Social Insurance Board is also mapping the continuity of child welfare institutions, there was a plan to meet and map risks at the end of July, after that another risk analysis and action plan could be conducted (completion date no later than 30.09.2023).
2. **Iru Nursing Home.** Today, both the Board of Health and the Social Insurance Board manage nursing homes. Iru is involved in both working groups. The result is to review the operational assessment guide and then also the risk mitigation. It would be good to hear more about this project, as an analysis of our own performance has been conducted, also in relation to a possible water cut, and in addition to a cut in heat and electricity supply. The city will also install the generator that is required to ensure water pressure, and there is also a backup plan for the mobile installation of Tallinna Vee's water tanks, which was also put into practice last summer.
3. Business continuity risk analysis pilot project at Municipal Police. Based on the pilot project, legislation is being developed at the state level.

#### *3.12.1.7 Transferability Demonstrator – Ireland*

As a local authority, Dún Laoghaire-Rathdown County Council has a fundamental obligation to provide access to training for its staff. This obligation stems from the council's commitment to efficient and effective governance, as well as its responsibility to serve the best interests of the community it represents. By offering continual professional development and training opportunities the council ensures that its staff stay up to date with the latest advancements and best practices in their respective fields and are equipped with the tools necessary to carry out their duties effectively.

The collaboration with the PRECINCT project provided a unique opportunity for the council to stay at the forefront of innovation and leverage state-of-the-art tools and methodologies in its operations, specifically in

relation to the emerging utility of digital twins across public sector services. To facilitate this, the council implemented a training program with a number of internal expert staff that utilised video presentations from workshops conducted as part of the project.

The video presentations served as a useful resource for internal expert staff, offering in-depth insights into the functionalities and applications of the PRECINCT tools. The presentations were used to provide a guide on how to effectively employ a digital twin for infrastructure deployment within the county. The presentations capture key concepts and methodologies relating to aspects relevant for staff such as data integration, system simulation, scenario analysis, and decision-making support. As the council is generally responsible for providing hands-on training for all its employees, further training would need to provide a more structured learning experience to cater to the diverse skill levels and backgrounds among internal staff.

Digital Twins will also be used to represent traffic light states as well as simulate future states based on traffic analysis. Another Digital Twin will be used to represent EV charger and EV charging network. Where DT will be used to predict EV charger use and energy grid load.

### **3.13 Impacts on the Transport and Logistics Community**

Public transport assumes a pivotal role in strengthening the resilience of critical infrastructure. It helps maintaining the seamless functioning of essential services during times of crisis or disruption. By providing efficient mobility solutions, public transport can ensure that personnel, including emergency responders and maintenance crews, can access critical infrastructure facilities promptly. At the same time, public transport systems act as a resilient backup during infrastructure disruptions, providing alternative transportation routes and options for both passengers and infrastructure operators. Moreover, public transport plays a decisive role in swift and organized emergency evacuations, extending a vital lifeline to communities in distress. Its strategic integration with critical infrastructure enhances the overall resilience of urban systems, contributing to the safety, security, sustainability, and well-being of cities and regions.

PRECINCT addresses the preparedness and resilience of critical infrastructure against cascading cyber-physical threats, with the following potential impacts on the public transport and logistics community.

#### **3.13.1 Fortified Cybersecurity Measures**

The project's new approaches to address cascading cyber-physical threats will reinforce cybersecurity measures within the public transport domains. This enhanced security approach will create a shield against potential cyber-physical attacks, safeguarding critical systems, sensitive data, and passenger information.

#### **3.13.2 Improved Incident Response and Recovery**

The emphasis on preparedness and resilience will lead to improved incident response and recovery capabilities in the face of cyber-physical threats. The project's research outcomes and best practices will inform the development of public transport robust incident response plans and recovery strategies tailored to the unique needs of critical infrastructures.

#### **3.13.3 Strengthening Inter-Agency Collaboration**

The collaborative nature of the PRECINCT project, involving multiple stakeholders from diverse sectors, will foster stronger inter-agency cooperation within the public transport and other authorities. By sharing expertise and insights on cyber-physical threats and resilience measures, different entities can forge partnerships that enhance collective security. This cross-sector collaboration will facilitate knowledge exchange, joint exercises, and

information-sharing, leading to a more robust defence against cyber-physical threats, also via the digital twin solution developed in the project.

### **3.13.4 Technological Innovations for Resilience**

The PRECINCT project's research includes the development and integration of advanced cybersecurity tools, such as the digital twin and serious games. As these technologies gain market uptake, public transport networks and logistics supply chains can proactively contribute to the resilience of critical infrastructure against sophisticated cyber and physical threats. This technology can also be integrated in their operations to protect their assets as well.

### **3.13.5 Public Confidence and Trust**

As the PRECINCT project strengthens cybersecurity and resilience of the critical infrastructure also via an efficient and reliable public transport, it will also contribute to fostering public confidence and trust. Passengers and clients alike will perceive these assets and industries as secure and dependable, further encouraging the use of public transport services.

In conclusion, as the PRECINCT project's focus on CI preparedness and resilience against cascading cyber-physical threats, it allows for a great contribution of the public transport and logistics community. By fortifying cybersecurity measures, improving incident response, fostering and promoting inter-agency collaboration, the project empowers the prompt response of the Public Transport in contributing to the resilience of CI. As stakeholders embrace the insights and outcomes of the PRECINCT project, they pave the way for a more secure, resilient, and trustworthy future for CI, with a substantial contribution to its resilience from public transport.

## **3.14 Impact on Municipalities**

The municipalities involved in the Living Labs were asked to assess the impact that the PRECINCT project had in this domain. The following sections go more in detail about the impact the project and the activities listed in section 3.12 had on the municipalities.

### **3.14.1 City of Ljubljana**

To maintain Ljubljana's reputation as a safe city, prevention is essential. PRECINCT was an EU project designed to increase the resilience of critical infrastructure (CI), which is necessary for society's smooth functioning and needs to be protected against the increasing frequency of cyber and physical threats. In the LL Ljubljana, the scenarios focused on a physical threat to the transport-mobility hub. Additionally, the scenario included simultaneous DDoS attacks on electricity and communication operators. While the current situation is safe, the above threats must not be ignored and the CI must prepare.

PRECINCT had many significant impacts on the City of Ljubljana, was mainly about understanding the current state of preparedness for cascading events. It also included the possibilities of further development and cooperation between different services. The most significant impacts are summarized below.

- The project gave the City of Ljubljana an excellent opportunity to overview the current state of preparedness of city services and CI on cascading events. It also gave it the opportunity to improve it. An insight into the operation of city services, responsible for CI (water, gas, heat pipe, sewerage, and public and traffic areas) and interconnectedness was gained. It must be pointed out that networking, cooperation and information exchange were extremely significant, which went very well during the project. Also, a working group consisting of key departments from the City of Ljubljana, which met

regularly, was informed of PRECINCT's activities. It was, therefore, possible to obtain very accurate information and connections with the city's services.

- There were discoveries made between "interconnectedness" within the city and between the city and private sector (national rail and city bus transport, electricity distribution system and telecommunications infrastructure) and the City of Ljubljana, particularly the Municipal Constabulary Department, with its connection to city services and first responders. Aside from getting to know each service, understanding the operation of each service and its mutual interdependence was beneficial.
- Information on CI status is crucial. The concept of a 3C coordination centre represents a good starting point for possible further work and development in the direction of the exchange of information between the public and private sectors with the aim of immediate detection of the event, engagement and response to urgently needed services and, consequently, improvement of both detection and intervention in case of cascading events.
- Increasing awareness and learning about physical and cyber threats and responding to them needs to be pointed out. On the city webpage, we published a few news related to the project.
- In addition to LL Ljubljana, the other PRECINCT three living labs abroad provided a valuable insight and experience. They also provided additional knowledge to the City of Ljubljana related to other scenarios discussed within the project.
- The results of serious games offered an opportunity to improve the resilience of the city's CI. This included preventive actions, response, and upgrading the intervention of the services.
- Ljubljana gained valuable knowledge by testing PRECINCT technology solutions that can be used in the city for implementing preventive measures and shaping the response. Besides, currently, the city's digital platform is being prepared, so we an opportunity to integrate PRECINCT's tools into the digital platform can be envisaged. Nevertheless, within the project, the SOC (security control centre) of the City of Ljubljana and its role have already been included. SOC is currently being tested and developed at the city level and PRECINCT provided the City of Ljubljana with some insights and ideas on how it should look.
- Municipal Constabulary Department of the City of Ljubljana (Municipality police) coordinated the PRECINCT project in the City of Ljubljana, which meant coordinating the city's services and cooperating with Slovenian and foreign partners, thereby gaining new experience and contacts that will be useful in further work.
- For the purposes of implementing the project, the coordinator was employed so the city gained a new co-worker.
- Since PRECINCT is an international project, it was beneficial for the City of Ljubljana to benefit from gained promotion, by which it became visible that both the city and the Municipal Constabulary department were able to successfully participate in EU projects.
- Besides, it showed that the priorities of the City of Ljubljana, which are also defined in the sustainable development guidelines, are related to ensuring a higher level of security.
- Finally, and more importantly, the project also coincided with the vision of smart cities and digitization.

### 3.14.2 City of Antwerp

With climate change, an increase in the frequency and severity of extreme weather conditions, such as increased precipitation resulting in rain, river, and coastal flooding, is expected and Belgium will not be spared from these climatic disturbances. The consequences of such precipitation and flooding have devastating effects on cities, as witnessed by the latest floods in Wallonia in the summer of 2021, and in other European cities in 2023. To cope with flooding events, the LL2 Operation, carried out within PRECINCT project, has applied the living lab approach by using a public-private partnership between the city of Antwerp and its crisis management team and CP-OPS disciplines, and the research and technology actors, and the CIs Operators.

The LL2 threat scenario focused on a flood event and its cascading effects on the emergency planning disciplines and CIs, on traffic infrastructures (including tunnels and subways) and on the water management CIs. The deployment of the PRECINCT Ecosystem components, and the co-creation process to identify the needs and practices of the first responders and disaster management team, has provided to the city of Antwerp two actionable tools to support the decision-making process of the first responders and mapping the vulnerabilities and cascading effects of a flood event on the city CIs (traffic, electricity and water).

The deployment of the PRECINCT ecosystem has impacted at the different levels the city of Antwerp. The major impacts identified during the LL2 demonstration and the PRECINCT components evaluation are:

- The project provided the City of Antwerp with an excellent opportunity to overview the current state of preparedness of city emergency services and cascading effects of a flood event on its CIs. Moreover, thanks to the identification of the current state of the needs and practices, the project enabled actionable solutions to be provided in order to improve the preparedness of the emergency services.
- By mapping the cascading effects on the CIs, and identifying the impacted CIs, the project enabled the city to collect mitigation actions to prevent flood impacts on the CIs. In addition, the crisis management team identified that, in the current situation, they had to undertake actions to identify CIs persons of contact to improve their prevention.
- The interdependencies map and the resilience approach also gave the opportunity of providing mitigation actions to improve the resilience level of the CIs, and by consequences, of the city.
- The interconnectedness of the city and the CIs operators (mainly the traffic, water management and energy distribution) has been updated and mapped. The process is helping both parties, the city and the CIs operators, to be better prepared for flood events.
- The integrated early warning detection system of the LL2 DT is an impactful tool developed for and by the first responders and crisis management team of the city of Antwerp. This early warning system enabled (and still enables) the emergency and crisis teams to detect floods threatening the city of Antwerp and improve the mitigation actions that could be undertaken to prevent cascading effects.
- Increased awareness and learnings regarding natural threats and addressed mitigation actions improved the decision-making process of the emergency services and of the city crisis teams.
- The Serious game, one of the actionable tools developed within the PRECINCT project, was identified as an exploitable training tool by the crisis management tool, at the strategic level (how to determine the best decision to improve resilience) and the tactical level (how to train the emergency disciplines to undertake actions to mitigate the threat effects on the citizens and CIs).
- The LL2 Digital Twin is the other actionable tool developed within LL2 Operation. Still running at the time of writing down this contribution, this tool offered the integrated early warning system (see above), a visualisation of the dependencies and CIs on the Antwerp city map, and the flood prediction and probabilities on this map. For the city of Antwerp, this tool is one of the key components to prevent flood threat and enables the emergency services to anticipate actions.
- By participating to this European Project, the city of Antwerp also gained in notoriety at the European level and became one of the key player of innovative city.

And finally, to recall and conclude with the words provided by the Police of Antwerp, a partner of the project: *“PZA is a firm believer in data-driven approaches to risk analysis and operational decision-making. It is certain that this will only become more important in the future. The models provide guidance for decision-making, and the decisions will have an impact on the further development of the models. If the police force uses these computer models with the other Antwerp emergency services during a flood caused by heavy rain, they will be better able to assess the consequences of operational decisions. The models may even encourage 'intelligent' operational decisions. In this way, a disaster can be coordinated in a more controlled way and possibly resolved more quickly. A data-driven approach also enables the PZA to function even better during a multidisciplinary disaster or incident command (CP-OPS). The ultimate aim is always for all the disciplines to work together, each in its own specialism, to control and resolve a disaster”* (Delannoy, Verwee, & Witvrouw, 2023).

### 3.14.3 City of Athens

Living Lab 3 consists of three transport Critical infrastructure operators providing mainly transport related services to thousands citizen in the broader Attika area daily. Although the municipality of Athens is not a member of LL3, according to LL3 CIs operator’s views increasing the resilience and faster coordination in case of unforeseen events among CIs operators can have profound impacts on the municipality of Athens. Therefore, studying and developing, evaluating strategies for enhancing LL3 CIs resilience, done as part of the work of undertaken in Living Lab 3 operations, can benefit the city in plethora of ways such as:

- In times of crisis, either from natural disasters or malevolent attacks efficient communications among stakeholders can potentially reduce their negative impact and cascading effects, recover faster and ensuring the safe evacuation of people during emergencies.
- In terms of City reputation and safety for the residents/visitors of the city, which is crucial in a densely populated or cities rely on tourism such as is Athens.
- Economic development where a resilient and efficient transportation network is essential for businesses, commerce, and transportation of goods and people on a daily basis.

In conclusion, increasing the resilience of Athens Airport, the Athens Metro system, and the city's road network is a multifaceted and challenging endeavor with positive externalities which not only relate to the CIs per se, but also to the broader society and citizen’s daily using them.

### 3.14.4 City of Bologna

The LL4 involved transportation operators (partly partners and partly stakeholders) and the public TLC network Lepida who together provide interconnected services to several CIs, governmental bodies and to thousands of passengers travelling from the Bologna Airport: inhabitants of the Bologna metropolitan area, travelers from the entire Emilia Romagna region and also from neighbouring regions.

Although the Municipality of Bologna is not a member of LL4, according to the view of the LL4 CI operators in tight cooperation with stakeholders TPER (Urban Mobility Provider) and Marconi Express (People Mover operator) improving communication and faster coordination among CI operators in case of critical events can have significant effects on the Municipality of Bologna. Additional involvement of other emergency actors such as Civil protection, Fire brigades and in general Law Enforcement Agencies can bring a significant added value.

The activities carried out within the project to increase the resilience of LL4 CIs can benefit the entire city in multiple ways, such as:

- in emergency situations, whether due to extreme weather events or malicious attacks: efficient communication and information sharing among operators can reduce negative impacts and cascading

effects, restoring the operations of the involved CIs faster and ensuring integrative or substitutive public transport services to/from Bologna Airport and other relevant destinations in the city (i.e. Fairs, events, etc);

- in terms of the city's reputation and safety for the city's visitors, in a city such as Bologna that is a strongly growing destination for business travel and tourism;
- in terms of economic development: the efficient and resilient Airport-Railway Station connection is essential for business, commerce and passenger transport, in a regional significant transportation node such as Bologna.

In conclusion, increasing the resilience of the involved CIs, the connection Airport-Railway station and the TLC connectivity/monitoring provided by Lepida, is a challenging and complex activity, which through coordination actions, data-sharing, and dedicated technology tools such as the Digital Twin, generates positive externalities that affect not only the critical infrastructure itself, but also society at large, the citizens who use it on a daily basis (about 500 airport workers/day) and travelers (almost 10.000.000 passenger/year).



## 4 Standardisation

In the face of ever-evolving threats and unprecedented challenges to our modern way of life, safeguarding our critical infrastructure has become an ever more urgent priority. As the backbone of society, critical infrastructure which comprises vital sectors such as energy, transportation, telecommunications and healthcare services, provides the structure to support citizens and societies' daily lives in Europe.

However, the interconnected and complex nature of these systems and the cascading effects of both physical and cyber-attacks, necessitate a comprehensive and unified approach to improve resilience.

Standardization can help to simplify complexity in Critical Infrastructure Protection by providing a consistent framework for operations, fostering interoperability, facilitating collaboration, optimizing security practices, ensuring compliance with regulations, and supporting scalability. By adopting standardized approaches, critical infrastructure entities can navigate the intricacies of their systems more effectively, ultimately leading to enhanced security and resilience. In general, the process of standardisation describes the establishment of a set of rules governing the way people are supposed to govern and complete, within an organization, a dedicated task or sequence of tasks. Standards can help to improve interoperability between products or services, and they represent, in a certain sense, some knowledge through rules, regulations and guidelines. These rules, regulations and guidelines are documented and are accessible to everyone helping the direct interests to understand, react and act accordingly.

In addition, common and adopted standard can be a booster for the European market, as they allow technology and solution providers to address market needs with products that are already shared and accepted by the user community. This helps to promote European products in worldwide market.

This section of the report provides an overview of what was already mentioned in D1.5 "PRECINCT Business and Technical Requirements Specification and Standardisation potential" in regards to standardisation bodies and a literature evaluation of the standards that are of interest to PRECINCT.

### 4.1 Standards and Standardisation Bodies

Outlined in D1.5, there are various standards bodies that are of interest to PRECINCT on both and international and European level. Table 4-1 below provides an overview of these standards bodies.

Table 4-1: International and European Standards Bodies

Abbreviation	Name of Organization
ISO	The International Organization for Standardization
IEC	The International Electrotechnical Commission
IEEE-SA	The Institute of Electrical and Electronics Engineers Standards Association
CEN	The European Committee on Standardisation
CENELEC	The European Committee on Electrotechnical Standardization
ETSI	The European Telecommunications Standards Institute

The Standardisation Bodies operate at National (UNE, UNI, DIN, AFNOR, BSI), Regional (CEN, CENELEC, ETSI) or International (ISO, IEC, IEEE) level. Furthermore, there are different Standardisation Bodies at the same level covering different fields. This is the case of ISO (general), IEC (electrical) and ITU (telecommunications) at

international level, or CEN, CENELEC and ETSI at European level in the same way. Finally, the Standardisation Bodies such as ISO, IEC, CEN, DIN or UNE, consists of many Technical Committees (TC), which deal with different areas of interest, and each TC may have a few sub-committees (SC) or Working Groups (WG).

Table 4-2: Features of standardisation documents

Type	Standard	Technical Specification	Technical Report
<b>European Standard</b>	EN	CEN/TS CLC/TS	CEN/TR CLC/TR
<b>International Standard</b>	ISO IEC	ISO/TS IEC/TS	ISO/TR IEC/TR
<b>Main Features</b>	Elaboration: 3 years <ul style="list-style-type: none"> <li>• 2 steps of member approval</li> <li>• European: compulsory national adoption</li> <li>• Revision: every 5 years</li> </ul>	Elaboration: 21 months <ul style="list-style-type: none"> <li>• 1 step of member approval or internal approval in TC</li> <li>• European: optional national adoption</li> <li>• Revision: at 3 years (upgrading to EN or deletion)</li> </ul>	Elaboration: free timeframe <ul style="list-style-type: none"> <li>• Internal approval in TC</li> <li>• European: optional national adoption</li> <li>• No revision required</li> </ul>

The Technical Committees (TCs) are the key bodies of standardisation. It is a group responsible for the development and drafting of standards which are then ratified by European Standards Organisations. The most positive aspect, in this case, is that all stakeholders, that can be interested in the area or field of work, are entitled to participate during the draft phase, but without any rights in voting in the Technical Committee. This right indeed, is just of the representatives of the National Standardisation Bodies.<sup>1</sup> Further explanations of Technical Committees and Subcommittees (SC) can be found in D1.5

In addition to the TC and SC there are Working Group(s) (WGs). A Working Group, established by a TC or SC, has the duty to develop draft deliverables in the context of the scope and the sector and work programme of the parent body. A WG strictly follows defined policy guidelines given from the parent body. The WG members are individual experts, and they act in a personal capacity.<sup>2</sup>

Figure 4-1 below is an example of how a code of a potential standards is a combination of the relationship and cooperation between the standard bodies.

<sup>1</sup> <https://www.iso.org/technical-committees.html>

<sup>2</sup> <https://issanet.org/working-groups/standards/>

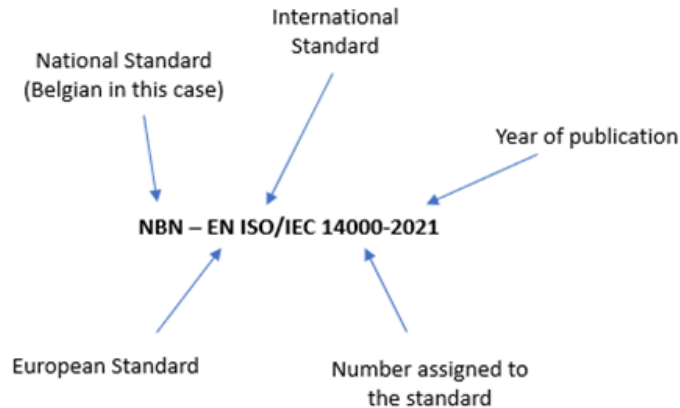


Figure 4-1: Standards code exposition

## 4.2 PRECINCT Standardisation Landscape

The purpose of this section is to describe the PRECINCT standardisation landscape identified in D1.5. In order to analyse the standardisation landscape and to identify the existing, or under development, standards, EOS proceeded with a research and literature of the processes and to set a sort of methodology to better understand the technical aspects of the project and to address them into identified standardization areas.

During the research and literature analysis carried out, both published standards and those still under development were considered. This was done for all the areas considered and for the technical committees identified. The standards developed by the main standardisation bodies were included in the research: the European Committee for Standardisation (CEN), the European Committee for Standardisation in the Electrical field (CENELEC), the International Electrotechnical Commission (IEC) and the international Organization for Standardisation (ISO). In order to outline an appropriate and relevant strategy and landscape, the in-depth study of the technical committees, subcommittees and working groups was done in a detailed manner. EOS identified 16 Technical Committees that will be presented in section 4.2.1

The standards are applicable to the PRECINCT project features and requirements, taking into consideration not only the technicalities of PRECINCT but also other aspects in the project Work Packages. The standards, listed in this chapter, have been classified taking into consideration both the released and underdevelopment ones, and they were used as a set of guidelines, remaining a recommendation and not a requirement.

### 4.2.1 Technical Committees

This section provides information regarding the relevant Technical Committees that have been identified during the research and literature phase. Table 4-3 provides a description of the Technical Committees.

Table 4-3: Technical Committees Description

Technical Committee	Sub-committee	Scope
<u>ISO/IEC JTC 1</u>	<u>X</u>	Standardisation in the field of information technology.
<u>ISO/IEC JTC 1</u>	<u>SC 2</u>	Standardisation of graphic character sets and their characteristics, including string ordering, associated control functions, their coded representation for

Technical Committee	Sub-committee	Scope
		information interchange and code extension techniques. Excluded: audio and picture coding.
<b><u>ISO/TC 184</u></b>	<b><u>SC 4</u></b>	Standardisation of the content, meaning, structure, representation and quality management of the information required to define an engineered product and its characteristics at any required level of detail at any part of its life cycle from conception through disposal, together with the interfaces required to deliver and collect the information necessary to support any business or technical process or service related to that engineered product during its life-cycle.
<b><u>ISO/IEC JTC 1</u></b>	<b><u>SC 6</u></b>	Since SC6 was established in 1964, SC6 has worked on standardisation in the field of telecommunications dealing with the exchange of information between open systems, including system functions, procedures, parameters as well as the conditions for their use. This standardisation encompasses protocols and services of lower layers including physical, data link, network, and transport as well as those of upper layers including but not limited to Directory and ASN.1: MFAN, NFC, PLC, Future Networks and OID.
<b><u>ISO/IEC JTC 1</u></b>	<b><u>SC 7</u></b>	Standardisation of processes, supporting tools and supporting technologies for the engineering of software products and systems.
<b><u>ISO/IEC JTC 1</u></b>	<b><u>SC 27</u></b>	The development of standards for the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as: Security requirements capture methodology, Management of information and ICT security; in particular information security management systems, security processes, and security controls and services, Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information, Security management support documentation including terminology, guidelines as well as procedures for the registration of security components, Security aspects of identity management, biometrics and privacy, Conformance assessment, accreditation and auditing requirements in the area of information security management systems, Security evaluation criteria and methodology.
<b><u>ISO/IEC JTC 1</u></b>	<b><u>SC 32</u></b>	Standards for data management within and among local and distributed information systems environments. SC 32 provides enabling technologies to promote harmonization of data management facilities across sector-specific areas. Specifically, SC 32 standards include: reference models and frameworks for the coordination of existing and emerging standards, definition of data domains, data types, and data structures, and their associated semantics, languages, services, and protocols for persistent storage, concurrent access, concurrent update, and interchange of data, methods, languages, services, and protocols to structure, organize, and register metadata and other information resources associated with sharing and interoperability, including electronic commerce.
<b><u>ISO/IEC JTC 1</u></b>	<b><u>SC 38</u></b>	Standardisation in the areas of Cloud Computing and Distributed Platforms including: Foundational concepts and technologies, Operational issues, and Interactions among Cloud Computing systems and with other distributed

Technical Committee	Sub-committee	Scope
		systems. SC 38 serves as the focus, proponent, and systems integration entity on Cloud Computing, Distributed Platforms, and the application of these technologies. SC 38 provides guidance to JTC 1, IEC, ISO and other entities.
<b><u>ISO/IEC JTC 1</u></b>	<b><u>SC 39</u></b>	Standardisation of assessment methods, design practices, operation and management aspects to support resource efficiency, resilience and environmental sustainability for and by information, data centres and other facilities and infrastructure necessary for service provisioning.
<b><u>ISO/IEC JTC 1</u></b>	<b><u>SC 40</u></b>	Standardisation of IT Service Management and IT Governance. Develop standards, tools, frameworks, best practices and related documents for IT Service Management and IT Governance, including areas of IT activity such as audit, digital forensics, governance, risk management, outsourcing, service operations and service maintenance, but excluding subject matter covered under the scope and existing work programs of JTC 1/SC 27 and JTC 1/SC 38.
<b><u>ISO/IEC JTC 1</u></b>	<b><u>SC 41</u></b>	Standardisation in the area of Internet of Things and related technologies: serve as the focus and proponent for JTC 1's standardization programme on the Internet of Things and Digital Twin, including their related technologies and provide guidance to JTC 1, IEC, ISO and other entities developing Internet of Things and Digital Twin related applications.
<b><u>ISO/IEC JTC 1</u></b>	<b><u>SC 42</u></b>	Standardisation in the area of Artificial Intelligence: serve as the focus and proponent for JTC 1's standardisation program on Artificial Intelligence and provide guidance to JTC 1, IEC, and ISO committees developing Artificial Intelligence applications.
<b><u>ISO/TC 279</u></b>	<b><u>X</u></b>	Standardisation of terminology tools and methods and interactions between relevant parties to enable innovation.
<b><u>ISO/TC 292</u></b>	<b><u>X</u></b>	Standardisation in the field of security to enhance the safety and resilience of society.
<b><u>ISO/TC 312</u></b>	<b><u>X</u></b>	Standardisation in the field of excellence in service

#### 4.2.2 Standardization Questionnaire

As part of T1.5, which also ties into T6.5, a questionnaire to better understand the standardisation processes inherent to the technical and business aspects of PRECINCT was sent around to PRECINCT partners in the early stages of the project. 140 standardisation processes and 15 different technical committees were collected from the initial construction of the questionnaire.

In the questionnaire<sup>3</sup> the author presented a deep set of questions composed by:

- Technical Committee
- Standard Name
- Standard Code
- Link of the standard, that can be easily consulted
- The detailed description of the Standard
- A closed questions to identify the specific area and sector of the standard

<sup>3</sup> The Standardisation Questionnaire shared with PRECINCT partners can be found in annex II of D1.5.

Partners were chosen for the feedback taking in consideration their affinity and relevance to the main topics, for the experience in working with standardisation processes.

#### 4.2.2.1 Questionnaire feedback

The questionnaire regarding the standardisation processes saw its continuation with a request for feedback from the technical partners of the project. This allowed partners to understand how the questionnaire could be developed, how it could be integrated with other relevant parts of the project and how the standards could be taken into account in the subsequent development phase of the project.

Thirteen project partners were contacted. The partners, both technical and non-technical, are representatives and exponents of different categories and different sectors, and their knowledge and expertise vary from one sector to another. This set of partners was preliminarily engaged with the request to provide their knowledge about those standardisation processes that could be useful for the project. A second activity, starting from January (M4) produced a draft of the questionnaire, and in April (M8) feedback from the responders was requested.

The feedback requested and received focused on three important technical aspects:

1. The identification of the standardisation processes under development and already developed
2. The evaluation of the processes already included in the questionnaire by answering if included between: Cyber, Physical, Response, Mitigation and Preparedness.
3. The possibility of including in the questionnaire, and therefore in the database that has been created, some standardisation processes that the partners know or utilise and which were not included in the first version.

For the tables listing the various feedbacks received, please refer to D1.5. The standardisation processes that were identified, both those already present in the initial questionnaire and those received via feedback from the project partners were taken into account for the technical aspects of the project, as well as activities carried out under T6.5 i.e. potential opportunities for PRECINCT to involve itself in ongoing standardisation processes. Additionally, this fed into the White Paper which defines a roadmap of actions and a set of key policy recommendations and best practices. Finally, the standardisation processes studied and researched will help maximise the impact of the PRECINCT project in support of relevant strategies of European Commission, the Security Research Strategy and the Industry for Security Strategy.

#### 4.2.3 Horizon Results Booster and Recommendations

As part of the work under T6.5, the PRECINCT project worked with the Horizon Results Booster (HRB) programme to further develop some of its exploitable results. PRECINCT and the HRB expert collaborated in the domain of standardisation, and recommendations were given to the project. The expert was assigned to PRECINCT almost at the end of the project but even if the project has reached its end, these recommendations would help standardisation efforts related to PRECINCT and are therefore presented in this section.

In the domain of digital twins, the recommendations are:

- At the **ISO/IEC level, active participation in SC41 and SC27** is recommended.
  - In SC41, the active participation of partners who are developing digital twins within the four living labs in WG6 is highly recommended. This involvement will enable society to leverage the knowledge and experience gained in the PRECINCT project.
- PRECINCT partners and other actors must **emphasize the need for Digital Twins standards at European level.**

- To achieve this, partners should contact their national standardization committees and propose the creation of a new TC or the creation a new WG related to digital twins, within the framework of CEN/CENELEC JTC 21 on Artificial Intelligence. The liaison of this new TC/WG with ISO/IEC JTC SC41 would be necessary.
- **Follow the path of other application domains.**
  - Examples like CEN/TC 442/WG 9 - Digital Twins in the AECOO sector could serve as an exemplary model or ISO 23247 Automation systems and integration - Digital twin framework for manufacturing can be used. Partners may consider tracking the process made to establish a dedicated working group on Digital Twins within other CEN/CENELEC groups, particularly in the context of cybersecurity or critical infrastructures.

In the specific domain of serious games:

- Considering the increasing application of serious games as effective educational and training tools and the absence of existing standards, **serious games are a strong candidate for inclusion as a subcommittee within any ISO/JTC/CEN SDO**. An initial recommendation of groups focused on software and systems engineering, are:
  - ISO/IEC JTC 1-information Technology, specifically SC7 related to software and systems engineering.
  - CEN/SS F12 - Information Processing Systems

In the cybersecurity domain:

- Currently, there is a substantial effort to promote standardization within the field of cybersecurity. As mentioned previously, numerous standards and initiatives are under development, making it difficult to recommend specific standards as it depends on the partners involved. The recommendations are mainly focused on the different working groups:
  - It is recommended to **promote cybersecurity in the frame of digital twins**, collaborating in the development of *PWI 27568 Security and privacy of digital twins*.
  - Partners must **pay attention to ISO/IEC 15408**, also known as "Common Criteria for Information Technology Security Evaluation". It establishes a global framework for the evaluation of the security of information technology products and systems including: Security Evaluation, Product Comparison, Security Requirements Establishment, Certification and Trust.
  - Once PRECINCT partners have identified and focused on relevant standards, the following **actions** are recommended **through their national standardization organization**:
    - Transfer the expertise gained in the PRECINCT project regarding cybersecurity in complex systems and the potential cascade effects of cyberthreats to CEN/CENELEC.
    - Actively participate and engage in various working groups, technical committees, and related forums to share their knowledge and contribute to enhancing the existing standards.
    - Advocate for the advancement of national recommendations, which can be further evaluated by CEN/CENELEC JTC 13 at the European level.
    - Encourage the examination of cybersecurity aspects within the context of cross-border emergencies affecting Critical Infrastructures.

PRECINCT partners can and should carry out these efforts as recommended by the Horizon Results Booster Expert (Tomás, 2023) after the end of the project; however, this may be difficult to do due to a lack of funding. In addition to the independent pursuit of these recommendations by PRECINCT partners, the European Commission could benefit from having these reflected in future research projects that deal with Serious Games, Digital Twins and Cybersecurity.

The next sections will further explore the standards in SGs, DTs and AI, as developed by PRECINCT partners.



## 5 Standards related to Digital Twins

### 5.1 Definition of Digital Twin

*"A Digital Twin is a virtual representation or digital replica of a physical asset, system, or process that captures and simulates its characteristics, behavior, and performance throughout its lifecycle. It encompasses the collection and analysis of real-time data from the physical asset, which is used to create a digital counterpart that can be monitored, analyzed, and manipulated to gain insights, optimize operations, and support decision-making." Glaessgen, E. H., & Stargel, D. S. (2012). The digital twin paradigm for future NASA and US Air Force vehicles. In 53rd AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics, and Materials Conference (p. 1821).*

Digital twins are often used in industries such as manufacturing, engineering, and healthcare to monitor, optimize and upgrade the performance of physical systems, predict maintenance needs, and troubleshoot problems. They are made by combining data from sensors, devices connected to the internet of things (IoT), and other sources of real-time data with sophisticated analytics and machine learning algorithms.

The idea of Digital Twins is also being used in other areas, like smart cities, where it can be used to improve city operations and simulate the behavior of entire urban systems.

### 5.2 Application of Digital Twins in PRECINCT

In the protection of critical infrastructure, the role of the Digital Twin has grown in importance. Operators are able to monitor the performance of the infrastructure in real time, identify potential issues before they become critical, and identify vulnerabilities that could be exploited by cyber attackers by creating a virtual replica of physical infrastructure such as power plants, water treatment facilities, transportation systems, and other critical infrastructure.

PRECINCT's Digital Twins aim to represent the Critical Infrastructure's network topology and metadata profiles, applying closed-loop Machine Learning techniques to detect violations and provide optimized response and mitigation measures and automated forensics.

### 5.3 Key standards related to DT applications such as those in PRECINCT

#### 5.3.1 ISO DT standards

- ISO/IEC AWI 30172: Digital twin - Use cases.<sup>4</sup> This is currently under development and at Stage 10.99 (Proposal) - now approved as a new project with a working draft under development.
- ISO/IEC AWI 30173: Digital twin - Concepts and terminology<sup>5</sup>. This is currently under development and at Stage 20 (Preparatory) - with a working draft already prepared, comments received and approved for registration as a Committee Draft.
- ISO/FDIS 23-247 - 1: Automation systems and integration - Digital Twin framework for manufacturing - Part 1: Overview and general principles<sup>6</sup>. This is currently under development and final text has been registered for approval. The additional parts to this standard include Part 2) Reference Architecture, Part

<sup>4</sup> <https://www.iso.org/standard/81578.html>

<sup>5</sup> <https://www.iso.org/standard/81442.html>

<sup>6</sup> <https://www.iso.org/standard/75066.html>



3) Digital representation of manufacturing elements and Part 4) Information exchange are also under development as well.

- ISO/IEC 27001: This international standard specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). It is relevant to digital twins as they often involve the processing, storage, and transmission of sensitive data related to critical infrastructure.
- ISO/IEC 27002: This standard provides best practice recommendations for information security controls within the context of an ISMS based on ISO/IEC 27001. It covers various aspects of information security relevant to digital twins, such as access control, data protection, and incident management.
- IEC 62443: This series of standards is specifically designed for industrial automation and control systems (IACS) security. Since digital twins are often integrated with IACS in critical infrastructure sectors, these standards are relevant for ensuring the cybersecurity of digital twin implementations.
- ISO/IEC 27032: This standard offers guidelines for cybersecurity, addressing various aspects such as risk management, incident management, and secure communications. It is relevant for organizations involved in critical infrastructure protection using digital twins.
- ISO 19650: This series of standards focuses on the organization and digitization of information about buildings and civil engineering works, including building information modeling (BIM). While not specifically focused on cybersecurity, these standards provide a framework for managing and exchanging digital information related to infrastructure assets, which can be relevant when implementing digital twins.
- ISO 55000: This series of standards focuses on asset management and provides a framework for the management of physical assets, including digital twins. While not specifically focused on cybersecurity, these standards can help organizations ensure the effective management and protection of digital twins as part of their overall asset management strategy.

## 5.4 Best Practice

In addition to these standards, organizations should also consider industry-specific guidelines, best practices, and recommendations for securing Digital Twins in critical infrastructure sectors. These may include guidelines from regulators, industry associations, or other authoritative sources. It is essential to stay up-to-date with the latest developments in digital twin technology and cybersecurity to ensure the effective protection of critical infrastructure assets.

## 5.5 Standardisation Barriers to adoption of DTs

The adoption of Digital Twins, which are virtual replicas of physical objects or systems, can be hindered by several standardization barriers. These barriers can impact the interoperability, compatibility, and overall effectiveness of digital twin implementations. Here are some common standardization barriers to the adoption of digital twins:

- **Lack of standardized data models:** Digital Twins require consistent data models to represent physical objects and systems accurately. However, the absence of standardized data models can lead to inconsistencies, making it difficult to exchange or integrate Digital Twin data across different platforms or organizations. Standardization efforts should focus on defining common data models that can be universally adopted across different industries and domains.
- **Data format and protocol fragmentation:** Digital Twin ecosystems typically involve various devices, sensors, and platforms that generate and consume data. In the absence of standardized data formats and communication protocols, interoperability challenges can arise. Different systems may use

incompatible formats or protocols, leading to data integration difficulties and limiting the scalability of Digital Twin solutions. Standardization can help establish common data formats (e.g., JSON, XML) and communication protocols (e.g., MQTT, RESTful APIs) to facilitate seamless data exchange.

- **Interoperability challenges:** Digital Twins often rely on data from diverse sources, including sensors, devices, and legacy systems. The lack of standardized interfaces and protocols can hinder the seamless integration of these disparate data sources, making it challenging to achieve comprehensive and real-time digital twin representations. Defining standardized interfaces, protocols, and data integration methodologies can enable seamless interoperability and promote the exchange of data between different digital twin platforms.
- **Security and privacy concerns:** Digital Twins deal with sensitive data related to physical objects and systems, such as operational information and performance data of physical assets. Ensuring the security and privacy of this data is paramount. Standardization efforts need to address security and privacy concerns adequately. Establishing common security protocols, encryption standards, and data access controls are crucial for building trust and ensuring the secure exchange of data within the digital twin ecosystem. This is an important aspects as it emerged from different input that trust in data sharing is one of the barriers in shared technology and process adoption
- **Lifecycle management and version control:** Digital Twins evolve over time, mirroring the changes in their physical counterparts. However, managing the lifecycle of Digital Twins and ensuring version control can be complex without standardized practices. Standardization efforts should focus on defining methodologies and frameworks for managing updates, versions, and changes to Digital Twin models, ensuring consistency and synchronization between the physical asset and its virtual representation.
- **Vendor lock-in and proprietary solutions:** Some vendors may offer proprietary Digital Twin solutions with limited interoperability or reliance on specific platforms or technologies. This can lead to vendor lock-in, where organizations become dependent on a particular vendor's ecosystem. Standardization can help mitigate vendor lock-in by promoting open and interoperable Digital Twin frameworks and technologies. Standardization efforts should promote open and interoperable Digital Twin frameworks, APIs, and data standards, allowing organizations to choose and integrate solutions from multiple vendors seamlessly.
- **Lack of industry-wide standards:** The absence of industry-wide standards for Digital Twins can impede their widespread adoption and interoperability across sectors. Collaborative efforts between industry stakeholders, organizations, and standardization bodies are necessary to establish common standards and best practices that span different sectors and domains. These standards can facilitate the seamless integration and exchange of Digital Twin data across sectors.
- **Legal and Regulatory Issues:** The adoption of Digital Twins may face legal and regulatory challenges, such as intellectual property rights, liability concerns, and compliance with industry-specific regulations. A lack of standardized guidelines in these areas can create uncertainty for organizations considering the implementation of Digital Twins.

Addressing these standardization barriers is crucial for the successful adoption and scalability of Digital Twins. Organizations can overcome interoperability challenges, enhance data exchange and integration, and foster the widespread adoption of Digital Twins across industries. Industry collaborations, the development of open and consensus-based standards and regulatory frameworks can help drive the standardization and trust efforts necessary for unlocking the full potential of Digital Twin technology.

## 6 Standards related to Serious Games

### 6.1 Definition of Serious Game

*"A Serious Game is a game or interactive application designed with the primary purpose of imparting knowledge, skills, or behaviors for a specific educational, training, or informational objective. It combines elements of entertainment and gameplay with educational content to engage users and facilitate learning in an interactive and immersive environment." Abt, C. C. (1970). Serious games. Viking Press.*

Serious games applied to critical infrastructure protection is an interdisciplinary field that involves computer science, security, and game design. The state of the art in this area is constantly evolving, but I can provide an overview of some recent developments.

One approach that has gained traction in recent years is the use of simulation-based serious games for training and assessing security personnel. These games can simulate real-world scenarios, allowing trainees to practice responding to cyber attacks or physical security breaches in a safe and controlled environment. By providing immediate feedback and tracking progress, serious games can help to identify skill gaps and improve overall readiness.

Another important trend is the integration of artificial intelligence and machine learning techniques into serious games. This can enable the creation of more realistic and dynamic simulations, as well as more personalized learning experiences. For example, AI algorithms can adapt the difficulty level of a game to match the skill level of the player, or generate new challenges based on the player's behavior.

Virtual and augmented reality technologies are also being used to create more immersive and engaging serious games. These technologies can provide a more realistic experience, allowing trainees to practice skills in a highly realistic virtual environment.

Finally, there is growing interest in the use of serious games for public awareness and education. Games can be a powerful tool for communicating complex security concepts to the general public, and can help to increase awareness of potential threats and best practices for protecting critical infrastructure.

Overall, the state of the art in serious games applied to critical infrastructure protection is focused on creating more realistic, dynamic, and engaging simulations that can improve the skills and readiness of security personnel, as well as increase public awareness of security issues.

State-of-the-art developments in serious games applied to critical infrastructure protection:

- Serious games that utilize gamification techniques such as point systems, leaderboards, and rewards to incentivize players to learn and improve their skills.
- Use of serious games to develop and test new security technologies, such as intrusion detection systems, firewalls, and anti-virus software.
- Integration of serious games into broader security training programs, such as tabletop exercises and live simulations.
- Development of serious games that can be played remotely, allowing trainees to practice skills and scenarios from anywhere in the world.
- Creation of serious games that incorporate social networking and collaboration features, enabling trainees to work together to solve complex security challenges.

- Serious games that utilize virtual reality to simulate real-world scenarios and improve situational awareness and decision-making skills.
- Integration of serious games into broader risk management strategies, such as risk assessments and threat modeling.
- Serious games that utilize big data and analytics to provide real-time feedback and analysis of trainee performance, enabling more targeted and personalized training programs.

## 6.2 Application of Serious Games in PRECINCT

Serious Games provide an interactive user interface that integrates and communicates with simulations on the back end through an interactive decision support system and scenario specification/building process. In PRECINCT, the SG will provide an experiential learning environment for understanding the cascading impacts of cyber-physical threats to critical infrastructure networks and the associated vulnerabilities. In addition, it will enable emergency personnel and critical infrastructure operators to devise better approaches solutions to mitigate the cascading effects and as a result increase their preparedness for such events. The SGs will be applied in the LLs via the deployment of executable files (.exe), whereby groups of personnel can play the game together to work as a team/group to decide on the best approach/decision to make give the in game circumstances.

## 6.3 Key standards related to SG applications such as those in PRECINCT

- ISO/IEC 25000: This standard provides a framework for the evaluation of software quality, including serious games. It covers characteristics such as functionality, reliability, usability, and performance.
- NIST SP 800-53: This publication provides a catalog of security and privacy controls for federal information systems and organizations, including serious games used in critical infrastructure protection. It outlines a range of security controls that can be applied to protect against threats to information and systems.
- IEEE 1484.1: This standard provides guidelines for the development and implementation of learning technology systems, including serious games used for training and education. It covers aspects such as instructional design, assessment, and accessibility.
- NICE Cybersecurity Workforce Framework: This framework provides a standard taxonomy and common language for cybersecurity roles and skills, including those related to critical infrastructure protection. It can be used to identify the skills and knowledge needed for serious game developers and security personnel.
- STPA-Sec: This is a safety and security analysis method that can be applied to serious games used in critical infrastructure protection. It involves a systematic process for identifying and analyzing potential hazards and security threats.

These standards provide a basis for ensuring that serious games used in critical infrastructure protection are developed, implemented, and evaluated in a structured and secure manner, and can help to ensure that they meet the needs of users and stakeholders.

Additional standards include:

- NISTIR 7864: This publication provides guidance for designing and evaluating effective security awareness training programs, including those that use serious games. It covers topics such as program planning, delivery, and evaluation.
- SCORM: The Sharable Content Object Reference Model (SCORM) is a set of technical standards for e-learning, including serious games used in critical infrastructure protection. It provides guidelines for creating interoperable content that can be reused across different learning management systems.

- IEC 62443: This is a series of standards for industrial automation and control systems security, including those used in critical infrastructure protection. It covers aspects such as network security, access control, and incident response.
- OWASP: The Open Web Application Security Project (OWASP) provides a set of guidelines and best practices for application security, including serious games used in critical infrastructure protection. It covers topics such as authentication, input validation, and security testing.
- GSE-GAM: The Gamification Standardization and Evaluation (GSE-GAM) project is an initiative to develop standards and guidelines for gamification, including serious games used in critical infrastructure protection. It covers topics such as game design, player engagement, and user experience.
- IEEE 730-2014: This is a standard for software quality assurance, including serious games used in critical infrastructure protection. It covers topics such as planning, implementation, and evaluation of quality assurance activities.
- ISO/IEC 27001: This is a standard for information security management systems, including those used in critical infrastructure protection. It provides a framework for implementing security controls and managing security risks.
- NISTIR 8144: This publication provides guidelines for developing secure mobile applications, including those that use serious games for critical infrastructure protection. It covers topics such as secure coding practices, data protection, and app deployment.
- ENISA: The European Union Agency for Cybersecurity (ENISA) provides guidance and best practices for cybersecurity, including those related to serious games used in critical infrastructure protection. It covers topics such as risk management, incident response, and threat intelligence.

There are several technical committees and organizations that are relevant in the area of serious games applied to critical infrastructure protection. Here are some of the most important:

- IEEE Computer Society Games Technical Committee: This committee focuses on research and development related to games and gamification, including serious games used in critical infrastructure protection. It covers topics such as game design, player experience, and game engines.
- ACM SIGGRAPH: The Special Interest Group on Computer Graphics and Interactive Techniques (SIGGRAPH) focuses on computer graphics and interactive techniques, including those used in serious games. It covers topics such as computer animation, virtual reality, and human-computer interaction.
- International Game Developers Association (IGDA): The IGDA is a professional association for game developers, including those involved in serious games used in critical infrastructure protection. It provides networking opportunities, education, and resources for game developers.
- Simulation Interoperability Standards Organization (SISO): The SISO develops standards for simulation interoperability, including those related to serious games used in critical infrastructure protection. It covers topics such as simulation architecture, data exchange, and model representation.
- Association for Computing Machinery (ACM): The ACM is a professional organization for computing professionals, including those involved in serious games used in critical infrastructure protection. It provides publications, conferences, and networking opportunities for its members.
- International Association of Computer Science and Information Technology (IACSIT): The IACSIT is a professional organization for computer science and information technology professionals, including those involved in serious games used in critical infrastructure protection. It provides a forum for researchers, educators, and practitioners to exchange ideas and share knowledge.

## 6.4 Standardisation Barriers to the Adoption of SGs

Standardization barriers to the adoption of Serious Games (SGs) include:

- Content Quality: Lack of industry-wide standards for educational or therapeutic efficacy.
- Technical Interoperability: Inconsistent formats and platforms make integration into existing systems difficult.
- User Experience: Lack of standard guidelines for ensuring an engaging and intuitive user experience.
- Data Security and Privacy: No unified standard for handling user data securely and ethically.
- Assessment Metrics: No universally accepted metrics to evaluate performance and outcomes.
- Cost: Development and implementation can be expensive, discouraging adoption.
- Regulatory Approval: Especially in healthcare or educational sectors, lack of standardized guidelines can impede regulatory approval.
- Intellectual Property: Varied licensing models and proprietary technologies can hinder standardization.

## 7 Standards related to artificial intelligence

### 7.1 Definition of artificial intelligence

Artificial intelligence seeks to mimic the ability to perform tasks that are commonly associated with human intelligence such as abstracting and generalizing. There is a common interaction between an agent, which is programmed to act “rationally”, the environment, which is where the agent navigates to find solutions, rewards, which guides the agent towards achieving what is good to its end (this is what is called “acting rationally” and is commonly modeled as a mathematical function), and the interactions between them.

### 7.2 Application of artificial intelligence in PRECINCT

The reluctance to adopt AI across major critical infrastructure systems can be overcome if AI is understood within a realistic frame of what it is, and what is not. The usefulness of an artificial intelligence is measured in terms of its ability to reach an objective, which is usually associated with the optimization of a mathematical function that, with all its limitations, tries to model the world. Thus, the aim of such agents is not to substitute human intelligence, but to cooperate by informing human intuition and his ability to make decisions. Artificial intelligence cannot replace human intuition and common sense in the decision-making process; however, this does not make artificial intelligence useless. Acting rationally, for an artificial agent, would mean that, given the right information, the agent is able to reach its goal, which is specified by the operators.

The goal of an artificial agent depends on the problem at hand. In PRECINCT, AI is used to identify possible threats in the critical infrastructure network. In this case, the goal is to identify observations that deviate from what is considered normal patterns. For this agent, acting rationally would mean identifying threats with high accuracy. Identification of risks and cyberattacks is another problem that requires observations of previously recorded attacks. This problem is solved by exploiting supervised learning algorithms which, given a set of labeled observations, can learn to detect possible cyberattacks from previous experience. The rationality of an act for this agent would be to correctly label a new observation as a cyberattack. Furthermore, AI is also used to plan a sequence of actions that would improve the operational state of the critical infrastructures network in the presence of disruptive events. The artificial intelligence agents, in this case, are said to act rationally when the sequence of actions suggested improves the operational state of the network, thus improving its overall capacity. Lastly, AI is also used to identify vulnerabilities from play records obtained from the Serious Game developed in the project. Here, the agent is said to act rationally if it uncovers patterns from play records that help the operators identify new vulnerabilities in the systems.

In conclusion, artificial intelligence in PRECINCT seeks to provide critical infrastructure operators with timely information, derived from facts, also called data, that guides human judgement in the decision-making process, including predictive maintenance, what-if scenarios, anticipating any incident and plan its correction. Identifying patterns that help operators bring critical infrastructure assets to their optimal state also translates into a return of investment. Artificial intelligence improves the decision-making process by uncovering patterns that are unseen by the human brain. Despite the number of benefits, AI can also be misused to do the opposite of what we seek to do in PRECINCT, that is, to affect the operations of critical infrastructures. For example, an artificial intelligence chatbot, called ChatGPT, based on supervised and reinforcement learning, has helped to write code to exploit vulnerabilities in industrial systems. This is just one example of the challenges posed when artificial intelligence is used (or misused) which, coupled with a misunderstanding, and sometimes conceptually unrealistic goals, may be the cause for the appearance of reluctant actors in critical infrastructure protection.



### 7.3 Key standards related to artificial intelligence in critical infrastructure protection

- AI for Natural Disaster Management: This text “capitalizes on the growing interest and novelty of AI in the field of natural disaster management to help lay the groundwork for best practices in the use of AI for: assisting with data collection and handling, improving modelling across spatiotemporal scales, and providing effective communication.”
- AI and Internet of Things for Digital Agriculture: The document seeks to “explore the potential of emerging technologies including AI and IoT in supporting data acquisition and handling, improving modelling from a growing volume of agricultural and geospatial data, and providing effective communication for interventions related to the optimization of agricultural production processes.”
- AI for Autonomous and Assisted Driving: The document “supports standardization activities for services and applications enabled by AI systems in autonomous and assisted driving.”
- Machine Learning for Future Networks including 5G: This document aims at drafting “technical specifications for machine learning (ML) for future networks, including interfaces, network architectures, protocols, algorithms and data formats.”
- AI for Health: This text seeks “to establish a standardized assessment framework for the evaluation of AI-based methods for health, diagnosis, triage or treatment decisions.”
- EU guidelines on ethics in artificial intelligence: Context and implementation: “This paper aims to shed some light on the ethical rules that are now recommended when designing, developing, deploying, implementing, or using AI products and services in the EU.”

### 7.4 Potential challenges

Potential disruptive impacts of artificial intelligence are expected to challenge the design, implementation, and adoption of AI-based products in CIP and other fields. The first challenge commonly found is the digitization of processes of CI operations. Digital transformation is a required first step that clears the path to the adoption of AI solutions, demanding from CI operators an investment in the adoption of technologies that provide the foundation on top of which AI-based products are to be developed. In the presence of digitized processes, other challenges may arise, including data management and data security and privacy, which refer not only to the storage and management of data, but also to the transmission and exchange of data.

As large datasets are available, some questions may come up regarding the comprehensiveness and accuracy of the data. Large volumes of data do not necessarily translate into accurate and useful data; furthermore, some AI algorithms require labelled datasets, which in many cases, especially in large datasets, are most of the time unavailable.

AI algorithms also pose some challenges that include biases that can be introduced as a result of insufficient or inaccurate datasets, in this area cybersecurity should be considered as well as there is the possibility to introduce poisoned data if the dataset is not well structured and protected, as well as human factors that affect the training of the models. Some types of algorithms, especially those based on artificial neural networks, do not follow processes typical of explainable artificial intelligence algorithms that allows human users to comprehend and trust the results created by the algorithm. Model transparency is another factor that is often underestimated, and sometimes misunderstood. Transparency should be introduced in every step of the workflow, starting at the data collection process, where detailed methodology of the data collection process should be provided, as well as the selection of the AI algorithm, and what was done to reduce the effect of bias in the model.

Modern AI-enhanced systems exhibit a challenge when it comes to integration with legacy systems. The deployment of AI models is not always a straightforward task, especially when models need to be maintained and updated due to the evolving condition of datasets used to train the models.



Declaring the ownership of AI-based products is also a commonly debated topic that confronts the different actors involved in the development of AI-based products. Should the partners that implement the algorithm hold the ownership, or does it belong to the partners that provide the data? Misusing AI-enabled technologies is often a topic in the radar of ethic committees, especially when the presence of AI is ubiquitous.

## **7.5 Artificial intelligence management procedures**

The Artificial Intelligence Management Procedures: Standard and Recommendation Guidelines is the result of a collaboration among PRECINCT project partners with the aim of standardizing the adoption, implementation, and integration of artificial intelligence (AI) technologies in the protection of critical infrastructures. The document can be found in Annex III: Artificial Intelligence Management Procedures: Standard and Recommendation Guidelines

## 8 Regulatory and policy relevance

### 8.1 Critical Infrastructure Policy directives

Critical Infrastructure protection is an integral part of the EU Security Union Strategy, published in July 2020, and falling under one of the four key strategic priorities for action at the EU Level: A future-proof security environment. Under this key strategic priority, the European Commission (EC) aimed to put forward new EU rules on the protection and resilience of critical infrastructures.

The output of the aforementioned were two directives to cover the physical and cyber domains of critical infrastructure protection. The NIS2 directive (an output of the review of the NIS Directive) and the CER Directive entered into force January 2023 and will be further discussed in Section 8.4

Directives, as defined by the European Union, are “legislative act(s) that sets out a goal that all EU countries must achieve. However, it is up to the individual countries to devise their own laws on how to reach these goals. One example is the EU single-use plastics directive, which reduces the impact of certain single-use plastics on the environment, for example by reducing or even banning the use of single-use plastics such as plates, straws and cups for beverages.” (European Commission, 2023).

### 8.2 Foundation legislation

The founding legislation for the EU’s legislation on Critical Infrastructure was a direct response to the Madrid and London attacks that occurred in 2004 and 2005, respectively. The Council asked the EC for a strategy to protect critical infrastructures, and on October 2004 the EC adopted a communication on protecting critical infrastructures from future terrorist attacks, focusing on prevention, preparedness and response. In December 2005, the Justice and Home Affairs Council called upon the EC to make a proposal for a European programme for critical infrastructure protection (‘EPCIP’) based on an all hazards approach while countering threats from terrorism as a priority. Under this approach, man-made, technological threats and natural disasters would be taken into account in the CI protection process, but the threat of terrorism was to be given priority. In April 2007, the Council adopted conclusions on the EPCIP, here the Council reiterated that it was the ultimate responsibility of the Member States to manage arrangements for the protection of CI within their national borders while welcoming the efforts of the EC to develop a European procedure for the identification and designation of European critical infrastructures (‘ECIs’) and the assessment of the need to improve their protection. The resulting directive after the years of work done by the Council and the EC was **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 (ECI Directive)**. The directive established an EU-wide procedure for identifying and designating critical infrastructures and an EU-wide approach to assess how the needs to improve protections from threats; however, this only covered two sectors: energy and transport.

### 8.3 Evolution of the EC directive for CIP

The first review of the ECI Directive took place in 2012 and identified a number of limitations. Namely, there were different levels of maturity across the CIP programmes in member states, and some needed significant resources in order to ensure national parliamentary oversight of compliance with the directive. Additionally, member states with already mature CIP programmes did not find an added value by the directive. There were also sector specific gaps, such as the disparity in security measures in transport sub-sectors. After the 2012 review, it became clear that the ECI Directive, and the general approach, needed to be changed in order to fulfill the protection of Europe’s critical infrastructure. The following year, the EC published a new approach to the EPCIP. As part of this new approach to CIP, the EC decided to look at the interdependencies between critical infrastructures, and between critical infrastructures and other actors (industry, civil society, state actors, etc.). Additionally, the new approach attempted to develop a cross-sectoral approach to EPCIP, to help account for the

aforementioned shortcomings of the EPCIP. It is important to note that Critical Infrastructure Protection projects were mentioned, and highlighted key outputs of some of the projects. Following this new approach, the EC decided to undertake a review of the ECI directive. The 2018-2019 evaluation concluded that the 2008 Directive held little relevance, mainly due to the changes in societal, technological, economic, political and environmental factors. It also concluded that the 2008 directive did not reflect the new EPCIP approach, and therefore recommended the EC to assess the opportunity to extend the sectoral scope of the ECI Directive, strengthen the monitoring and evaluation framework in order to support future decision-making processes, and to streamline the EU CIP legislative framework and trigger synergies at the national level, among others. It is in this context that the EC published **DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC**, also known as the CER Directive, which entered into force in January 2023 (further discussed below). Over the 20 years of European CIP policy, it became clear that critical infrastructures operate with complex interdependencies and the initial 2008 Directive did not reflect this reality. Furthermore, EU legislation continued to evolve, such as the NIS and NIS 2 Directive, creating overlap and gaps in regard to the ECI Directive. Finally, there was also a shift in mentality in regard to CIP with the focus favoring resilience over protection. All of these factors shaped how the EU viewed EU policy towards CIP and the subsequent CER Directive.

## 8.4 Current legislation

There are two main legislations for the protection of critical infrastructures in Europe, the Critical Entities Resilience Directive (CER) and the Directive on Security of Network and Information Systems 2 (NIS2).

The Critical Entities Resilience Directive (CER) (full name "**DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance)**") was published in December 2022 replacing the European Critical Infrastructure Directive of 2008. The objectives of this directive are to ensure the smooth provision of services in the internal market that are essential for the maintenance of society and economic activities, and to enhance the resilience of the entities providing these services. As previously mentioned, this directive shifts the focus way from protection, favoring instead a focus on resilience, while opting for a risk-based approach (risks are all relevant non-cyber man-made and natural risks that may affect essential services e.g. natural disasters, accidents, public health emergencies and antagonistic threats), expanding the sectors from two to eleven, enhancing the cooperation mechanism(s) and identifying critical entities at the national level instead of cross-border designation. The CER Directive is built on 5 pillars (two obligations and 3 support activities respectively):

- Obligation for Member States to come up with a national framework on the resilience of critical entities including a strategy, risk assessment, identification of critical entities based on common criteria, establishing a single point of contact, supervision and enforcement.
- Obligations for identified critical entities, including conducting risk assessments; implementing technical, security and organisational resilience measures; incident notifications; appointing a liaison officer.
- Establishment of a Critical Entities Resilience Group to facilitate Member State cooperation.
- Commission support to both Member States and critical entities, by developing a Union-level overview of cross-border and cross-sectoral risks, best practices, methodologies, cross-border training activities and exercises to test the resilience of critical entities, among others.
- Advisory missions to critical entities of particular European significance which will assess resilience measures put by the entity and communicate actions for improvement.

The criteria for identifying a critical entity, found in the annexes of the CER Directive, dictates that a critical entity is an entity of a category and in a sector listed in the annex of the CER Directive that provides one or more essential services for the maintenance of society and economic activities; the entity is located in the territory of the members state conducting the identification; and an incident would have significant disruptive effects on the

provision of one or more essential services (in the sectors in scope of the directive). Once an entity is identified to be critical, they will then have certain obligations to fill, such as a risk assessment (assessing relevant risks that may disrupt essential services and take into account sectoral dependencies), resilience measures (take appropriate technical, security and organizational measures to ensure resilience, apply a resilience plan, etc.) and incident notification (inform without undue delay the competent authorities of incidents, provide follow-up reports, etc.) Member states have by the 17<sup>th</sup> of October 2023 to transpose the CER Directive into national law (and repeal the ECI Directive), by the 17<sup>th</sup> of January 2026 for a strategy to enhance resilience of critical entities and conduct risk assessments and by the 17<sup>th</sup> of July 2026 to identify their critical entities. 10 months after critical entities are notified of their identification as a critical entities, obligations (mentioned above) will apply.

In regards to the obligations for a strategy to enhance the resilience of critical entities, the strategy needs to include the following:

- a) strategic objectives and priorities for the purposes of enhancing the overall resilience of critical entities, taking into account cross-border and cross-sectoral dependencies and interdependencies;
- b) a governance framework to achieve the strategic objectives and priorities, including a description of the roles and responsibilities of the different authorities, critical entities and other parties involved in the implementation of the strategy;
- c) a description of measures necessary to enhance the overall resilience of critical entities, including a description of the risk assessment;
- d) a description of the process by which critical entities are identified;
- e) a description of the process supporting critical entities, including measures to enhance cooperation between the public sector, the private sector and public and private entities;
- f) a list of the main authorities and relevant stakeholders, other than critical entities, involved in the implementation of the strategy;
- g) a policy framework for coordination between the competent authorities for the purposes of information sharing on cybersecurity risks, cyber threats and cyber incidents and non-cyber risks, threats and incidents and the exercise of supervisory tasks;
- h) a description of measures already in place which aim to facilitate the implementation of obligations by small and medium-sized enterprises.

Member States were instructed to update their strategies at least every four years and communicate their strategies, and substantial updates to the EC within three months of their adoption.

**The Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148**, also known as the NIS 2 Directive, was also published in December 2022, alongside the CER Directive. The newest version of the NIS was brought about by potential cascading effects and an expanded threat landscape that demonstrated certain limitations in its predecessor. The main challenge and limitation of the first NIS was that not all sectors that may be considered critical were in the scope. Additionally, there were inconsistencies and gaps due to the NIS Scope being de facto defined by MS (detriment to the internal market), diverging security requirements across Member States (MS) (eg. Reporting requirements for cyber incidents) and incident notification requirements, ineffective supervision and limited enforcement, and finally voluntary and ad-hoc cooperation and information sharing between MS and between operators. The NIS 2 is built on 3 pillars:

- Member State Capabilities, focusing on national authorities, more robust national strategies, coordinated vulnerability disclosure (CVD) frameworks and crisis management frameworks.
- Risk Management & Reporting including accountability for top management non-compliance, entities being required to take cybersecurity risk management measures, and the obligation for entities to notify incidents (not just major but also cyber threats).

- Cooperation and information exchange via an NIS Cooperation Group, the previously established CSIRTs network, CyCLONe, a CVD and European vulnerability database, peer-reviews that will reflect the state of play for cybersecurity in the EU, and a biennial ENISA cybersecurity report.

And further divided into two regulatory regimes: essential vs. important. The essential entities include the original scope of the 1<sup>st</sup> NIS with the additional of certain new sectors, while the important entities include mostly new sectors designated by the Directive. Both entities must comply with the same security measures (risk based security obligations, accountability of top management, jurisdiction, etc.); however, only the essential entities will be supervised continuously, while important entities will only be monitored after an incident of non-compliance is reported. Similarly to the CER Directive, the entities covered by the Directive are operators of an essential service; however, the scope of the directive is also based on size. Identification under NIS 1 has proven inefficient, and there was a difficulty in identifying consistent thresholds. Size is a clear-cut benchmark (all companies which are medium sized or larger and a proxy for importance with the exceptions of electronic communications, trust services, TLD registries, and public administration. MS are able to add operators below the size threshold if:

- They are the sole providers of a service.
- Potential disruption of a service provided by the entity could have an impact on public safety public security and public health.
- Potential disruption of a service could induce a systemic risks.
- Entities with specific importance at regional or national level.

Ultimately, the NIS 2 strengthens security and reporting requirements for companies by imposing a risk management approach, which provides a minimum list of basic security elements that have to be applied (risk analysis and information systems security policies, incident handling, supply chain security, business continuity and crisis management, security in network and infosystems acquisitions, development and maintenance) and clarifies incident reporting (three stages, two mandatory: initial notification, intermediate report upon request of CA or CSIRT, final report after one month of incident). Member states have by the 17 October 2024 to transpose the NIS2 Directive into national law (and repeal the NIS 1), by the 15 April 2025 establish a list of essential and important entities (and notify the EC and Cooperation Group of the number of essential and important entities for each sector every two years). By the 17 October 2027 The European Commission will review the directive to assess its functioning.

## 8.5 Policy relevant to Critical Infrastructure

- European Programme for Critical Infrastructure Protection (EPCIP): EPCIP is a policy framework that aims to improve the protection of critical infrastructure in European Union Member States. It establishes a set of principles and guidelines for identifying, assessing, and managing risks to critical infrastructure.
- European Union Cybersecurity Strategy: The EU Cybersecurity Strategy outlines a comprehensive vision for ensuring cybersecurity and enhancing digital resilience across the EU. It includes measures for critical infrastructure protection, such as strengthening incident response capabilities, developing certification schemes, and fostering cooperation among EU Member States.

## 8.6 Agencies, Groups and Networks relevant to Critical Infrastructure

- NIS Cooperation Group: Established under the NIS Directive, the NIS Cooperation Group promotes strategic cooperation and information exchange among EU Member States on network and information system security. This includes sharing best practices and guidance on critical infrastructure protection.
- European Critical Infrastructure Warning Information Network (CIWIN): CIWIN is an information-sharing platform that facilitates the exchange of best practices, alerts, and warnings among EU Member States related to critical infrastructure protection. It aims to improve situational awareness and strengthen the resilience of European critical infrastructures.
- European Union Agency for Cybersecurity (ENISA): ENISA is an EU agency that plays a key role in enhancing cybersecurity across Europe, including critical infrastructure protection. It provides expertise, support, and guidance to EU Member States, developing guidelines, best practices, and recommendations to strengthen cybersecurity in various sectors.
- Public-Private Partnerships (PPPs) for critical infrastructure protection: The EU promotes PPPs as a means to enhance collaboration between the public and private sectors in critical infrastructure protection. These partnerships facilitate information sharing, risk management, and the development of innovative solutions to address security challenges.
- Cross-border and regional cooperation: The EU encourages cross-border and regional cooperation to enhance critical infrastructure protection. This includes initiatives like the Baltic Sea Region Energy Cooperation (BASREC) and the European Critical Infrastructure Protection Forum (ECIPF), which foster cooperation among Member States and neighbouring countries to address shared critical infrastructure challenges.
- These policy interests, along with national policies and strategies, contribute to a comprehensive approach to critical infrastructure protection in Europe. By engaging with these policies and initiatives, organizations can stay informed about the latest developments in critical infrastructure protection and contribute to the overall security and resilience of Europe's critical systems and services

## 8.7 PRECINCT Relevance to the Current EU Policies & Policy Recommendations

As part of PRECINCT's main objective to increase resilience in critical infrastructures in a geographical setting, in a manner that is replicable across Europe, it is important to place PRECINCT in the current policy landscape. By doing so, PRECINCT can highlight where it already helps answer the obligations laid out in the two European Union Directives, as well as offer some policy recommendations that will help improve critical infrastructure protection.

## 8.8 PRECINCT Relevance to Current EU Policies

In summary, the CER will require EU Member States to, following a risk assessment, identify critical entities that provide services that are essential for the maintenance of functions vital to society, economic activities, public health and safety or the environment, and identify cases in which an incident would have significant disruptive effects on these essential services. This touches most CIs, apart from those in the banking, financial market infrastructure and digital infrastructure sectors. MS will then be obligated to support the identified critical entities in enhancing their resilience, ensure that national authorities have the powers, resources and means to

carry out their supervisory tasks, etc. Critical entities will then be obligated to carry out risk assessments of their own to identify risks that could disrupt their ability to provide essential services, take technical, security and organisational measures to enhance their resilience, and notify significant disruptive incidents to the national authorities.

In regards to the NIS2 Directive, medium-sized and large entities operating in the sectors of high criticality as discussed previously, will mostly be concerned. Every MS must adopt a national strategy to achieve and maintain a high level of cybersecurity in the critical sectors, including:

- a governance framework clarifying the roles and responsibilities for relevant stakeholders at the national level;
- policy addressing the security of supply chains;
- policy on managing vulnerabilities;
- policy on promoting and developing education and training on cybersecurity; and measures to improve cybersecurity awareness among citizens.
- Computer security incident response teams (CSIRTS)

The CSIRTS will be tasked with monitoring and analysing cyber threats, vulnerabilities, and incidents at the national level; providing early warnings, alerts, announcements and information to the entities concerned and to other stakeholders on cyber threats, vulnerabilities and incidents, if possible in near-real time; responding to incidents and providing assistance where applicable; collecting and analysing forensic data and providing dynamic risk and incident analysis and situational awareness on cybersecurity; and providing, on request, proactive network and information system scanning to detect vulnerabilities with a potential significant impact.

PRECINCT has developed many tools and assets which will help Critical Entities (and MS) meet the requirements in an efficient and interoperable way. **The PRECINCT Framework**, developed to facilitate the modelling of dynamic interdependencies and cascading effects in complex networks of CI, as well as to quantify resilience and identify short-term and long-term resilience enhancement measures, facilitates the representation of multiple hazards and their resulting risks across interdependent sectors. The output of which can be employed to prepare and adapt to multiple hazard processes. The framework is adaptable and allows CI communities of different size and make-up, operating at various scales within a member state, to integrate the specifics of their system of CIs. This enables different systems of interconnected CIs to coordinate during the risk assessment obligation to identify cases in which an incident would have significant disruptive effects on their essential services and identify how the MS can help them enhance their resilience.

Additionally, PRECINCT used **Digital Twins** to investigate cascading effects on interconnected CI in the four living labs. This allowed for certain scenarios to be played out in real time and see the cascading effects it would have on those specific cities. The use of Digital Twins, as done in PRECINCT, could be replicated to better understand the necessary response measures to be implemented in order to quickly and efficiently respond to scenarios. Paired with the **Serious Game** developed by PRECINCT, which is a vulnerability assessment tool used to train operators in the living labs on how to respond to scenarios affecting interdependent Critical Infrastructures, both tools would allow for cost effective trainings that would help CI fulfill the obligation to take technical, security and organisational measures to enhance their resilience. The tools could also be used by Member States and CSIRTS to fulfill their obligations of conducting risk assessments, analysing cyber threats, and increasing both cyber and non-cyber resilience in general.

## 8.9 PRECINCT Policy Recommendations

In addition to developing tools that will allow for Critical Entities to efficiently follow the obligations laid out in the two directives, PRECINCT has also developed policy recommendations that will help drive critical infrastructure protection to higher levels, and plug certain gaps that are foreseen by the project. The policy recommendations are as follows:

- I. **Legal Requirement for the Creation of Centralised Critical Infrastructure Coordination Centers (CICC):** Legal requirements can be a main driver of increasing resilience for critical infrastructure protection, whether it be needing to comply with new technical requirements or the new obligations for risk assessments under the CER directive. In this case, the PRECINCT project recommends the legal obligation for MS to create Centralised Critical Infrastructure Coordination Centers (CICCs). CICCs can help increase resilience and a better understanding of cascading effects by continually analysing interconnected CIs at a strategic level and developing training scenarios to better prepare Critical Infrastructure Actors for scenarios that may occur. These CICCs must be defined at an EU level so that all MS create their CICC with the same framework and with the same objectives. These CICCs can also be involved in the next policy recommendation.
  
- II. **The development of a European Resilience Competence Centre:** With the creation of the European Cybersecurity Competence Centre in 2021 (Regulation EU 2021/887), the EU has its first executive agency to coordinate and collaborate with National Coordination Centers (and the Network of National Coordination Centers [NCCs]). The ECCC is tasked with developing objectives for cybersecurity research projects and facilitate collaboration and the sharing of expertise and capacities among all relevant stakeholders. While this is a step forward for improving CIP across the whole EU, it only focuses on cybersecurity. The PRECINCT project recommends that a similar centre is created for critical infrastructure protection focusing on resilience, a sort of European Resilience Competence Center (ERCC). Critical infrastructure Coordination Centres can play an important role in enabling communication between interdependent Critical Infrastructures, and a European Executive Agency that helps foster this collaboration and communication will only help to increase resilience around the EU and ensure that varying levels of critical infrastructure protection across MS are avoided. The tasks that could be entrusted to this ERCC are the following:
  - a. Bring networks of coordination centers focus on CIP together to discuss best practices, information sharing and standardization opportunities.
  - b. Produce research objectives and policy recommendations for the European Commission to consider when drafting policy related to non-cyber CIP
  - c. House a repository of standards for Critical Infrastructure Operators to easily find, while also being at the forefront of the creation of any new standards related to CIP.
  - d. Develop and provide trainings for CIP regarding cross-border cooperation and the risk of cascading effects
  - e. Provide a test-bed for new and developing technologies for CIP, including those being developed part of the Horizon Europe or other funding programmes.

While a Critical Entities Resilience Group is already established under the CER Directive (Article 19) with the mission to facilitate cooperation among Member States, including sharing information and good practices, an executive agency instead of a Commission expert group, could be better equipped to promote best practices. The ERCC could also host the CERG in order to make it easier for national coordination centers and critical infrastructure operators to know where to find the relevant expertise.

- III. **Close the ICT Gap in NIS2 and CER:** Currently, ICT operators are subject to the NIS2 and not the CER. Not including the ICT sector in the CER directive could lead to some increase in risks, this class of infrastructures should be subject to increased security measures. Such proposition is justified due to the



fact that ICT networks may be used as a mean to attack other infrastructures subject to the CER. For this reason, the same approach and level of protection should be applied with consistency.

- IV. **Develop policies indicating cybersecurity assessment processes on CIIIs that consider and evaluate the criticality of their cyberdependencies across the CIIIs collaborative network, to identify and mitigate risks:** The NIS 2 directive identifies operators of essential and important services. Research from PRECINCT, other projects (both ongoing and completed) and current available literature has shown that transport industries, such as aviation, engage heterogeneous, complex cyberphysical interdependent infrastructures composed by IT/OT architectures. PRECINCT identified and illustrated such interdependencies among CIIIs upon developing interdependency graphs towards such CIIIs. The EU authorities need to delve into their security specificities and identify sector-specific approaches addressing security assurance requirements on such infrastructures considering their dependencies and develop focused methods to be addressed (expanding NIS 2 and CER Directives). Moreover, EU regulation could promote best practices at EU level that guide CIIIs how to specifically assess risks and threats in collaborative CIIIs environments, such as supply chains. Furthermore, to consider digital relations between CIIIs (cyberdependencies) in the calculation of CIIIs' cyber risks, estimate the cascading effects among CIIIs networks and promote solutions for collaborative risk treatment. To identify sectorial solutions.
- V. **A Unified Standardised Approach Indicating Collaborative Incident Response Procedures:** Based on the research and findings of PRECINCT, it is considered that a unified standardized approach indicating collaborative incident response procedures among interconnected CIIIs (e.g., such as transport CIIIs, i.e., metro, road transport, aviation) within the EU is needed (e.g., based on related acknowledged international standards, such as infosec ISO/IEC 27035). The definition of crisis management protocols could rely on the CIP related directives (i.e. NIS 2 Directive, CER Directive). Currently, there are international policies and practices, addressing crisis management at sectorial/industry level, such as ICAO Annex-es 14,17 and other respective Docs (e.g., 8973, 9137, 9973, 9998). Within the EU, there is basically the EU Regulation no 996/2010 of the European Parliament and of the council "on the investigation and prevention of accidents and incidents in civil aviation" associated with Aviation crisis management procedures. It should be noted that the EU has already authorized a Group of Chief Scientific Advisors to work on a coherent, comprehensive, cross-sectoral EU strategic policy and operational framework for crisis management, which PRECINCT welcomes.
- VI. **Focus on the Integration of Cybersecurity and Privacy Processes:** Considering the gap of integrating privacy and cybersecurity processes suggested previously, the EU could further invest in R&D projects and other initiatives to focus their research on integrating cybersecurity and privacy processes on CIIIs. The ultimate purpose of research could be focused on i) protecting personal data from the perspective of applying cybersecurity risk assessment techniques on assets and processes that concern personal data handling to strengthen their level of privacy protection by implementing appropriate organisational and technical measures that eliminate the potential of data compromise and simultaneously ii) investigate whether cybersecurity risk assessment and risk treatment techniques are GDPR compliant, explore if involved data subjects satisfy privacy needs and rights to ensure transparency between data controllers and data subject services. For example, since Air Transport operators are considered operators of essential services with significant effect to the EU economy the potential of such service disruption, EU best practices and recommendations could guide in those areas the aviation security and indicate with specific directives how to be compliant with Critical Infra-structure directives (NIS2 Directive, CER Directive) and GDPR regulation.
- VII. **Increased funding for SMEs to keep European Innovation and Standardisation Efforts Strong:** SMEs are unequivocally one of the driving forces in Europe in regards to innovations, including in the CIP domain.

The EU should encourage SMEs to keep producing innovations and ensure that participation of the SME community in research and standardization is high. One way to do this is to evaluate the funding mechanisms, such as Horizon Europe. Funding rates for Innovation Actions are 70% which is prohibitive for SMEs to contribute effectively and should perhaps be re-evaluated. Additionally, research initiatives like StandICT “Supporting European Experts Presence in International Standardisation Activities in ICT” which allows SMEs and individuals take part in standardization efforts, should continue to be funded. PRECINCT welcomes the continuation of StandICT into 2026.

While the above recommendations will not close all of the gaps in Critical Infrastructure Protection, these actions and measures could help increase resilience across Europe by implementing structures to allow for better coordination, innovative tools to be used, and allow for more CIP research to be conducted. The main message of these recommendations is to ensure that a common approach continues to be the way forward when it comes to CIP, and to ensure that certain discrepancies do not go unnoticed e.g. NIS2 vs. CER, SME participation vs. big firm participation, Aviation Management procedures vs. other CI management procedures, etc.

## 9 Technical Committees

Various technical committees are involved in the development of standards, guidelines, and best practices in the area of critical infrastructure protection with a focus on security. Some of the most relevant technical committees include:

- ISO/IEC JTC 1/SC 27 - IT Security techniques: This joint technical committee is responsible for the development of standards for information security management systems (ISMS), cybersecurity, and privacy protection. The committee oversees the development of important standards like ISO/IEC 27001 and ISO/IEC 27002, which are relevant to critical infrastructure protection.
- IEC TC 65 and its subcommittee SC 65C - Industrial-process measurement, control, and automation: IEC TC 65 is responsible for developing standards related to industrial-process measurement, control, and automation systems. Its subcommittee, SC 65C, focuses on industrial networks and has developed the IEC 62443 series of standards for industrial automation and control systems (IACS) security.
- ISO/TC 292 - Security and resilience: This technical committee is responsible for developing standards that address security, emergency management, and business continuity. The standards produced by this committee, such as ISO 22301 and ISO 31000, are relevant to critical infrastructure protection and security.
- ISO/TC 268 - Sustainable cities and communities: While not solely focused on security, ISO/TC 268 is responsible for developing standards and guidance for sustainable and smart cities, which can include aspects of critical infrastructure protection. The work of this committee can contribute to the resilience and security of urban infrastructure.
- CEN-CENELEC Sector Forum on Security (SF-SEC): The SF-SEC is a European forum that coordinates and harmonizes standardization activities related to security, including critical infrastructure protection. This forum ensures cooperation between the various technical committees under the European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (CENELEC).
- ETSI TC CYBER - Cybersecurity: The ETSI Technical Committee on Cybersecurity is responsible for developing standards and technical reports related to cybersecurity, including those relevant to critical infrastructure protection in the telecommunications sector.
- NIST Cybersecurity and Privacy Advisory Committee (CPAC): While not a standardization body, CPAC is an advisory committee that provides input on cybersecurity and privacy issues to the National Institute of Standards and Technology (NIST). The committee's work is often influential in shaping standards and guidelines in critical infrastructure protection and security.

These technical committees, among others, play a crucial role in shaping the standards, guidelines, and best practices for critical infrastructure protection with a focus on security. By participating in or following the work of these committees, organizations can ensure they stay up-to-date with the latest developments in security and resilience for critical infrastructure.

Here are additional technical committees and groups involved in the area of critical infrastructure protection with a focus on security:

- IEC TC 57 - Power systems management and associated information exchange: This technical committee is responsible for developing international standards for information exchange and management related to power systems, including cybersecurity aspects for the energy sector.
- ISO/IEC JTC 1/SC 6 - Telecommunications and information exchange between systems: This subcommittee focuses on developing standards for information exchange between telecommunication systems, which can have implications for the security and protection of critical telecommunications infrastructure.

- ISO/IEC JTC 1/SC 31 - Automatic identification and data capture (AIDC) techniques: This subcommittee is responsible for developing standards related to AIDC techniques, which are relevant for secure identification and tracking of physical assets in critical infrastructure.
- CEN/TC 391 - Societal and Citizen Security: This technical committee works on standardization in the field of societal security, including aspects of critical infrastructure protection. It develops European Standards that contribute to security, resilience, and crisis management.
- ETSI TC ITS - Intelligent Transport Systems: This technical committee focuses on standardization for intelligent transport systems, including aspects related to the security and resilience of transport infrastructure, such as communication networks, sensors, and control systems.
- ETSI ISG SAI - Industry Specification Group on Securing Artificial Intelligence: This group develops guidelines and best practices for securing AI systems, which can be relevant to critical infrastructure protection as AI technologies are increasingly integrated into infrastructure systems.
- NIST Smart Grid Interoperability Panel (SGIP): This panel works on identifying, prioritizing, and addressing the requirements for smart grid cybersecurity. It brings together various stakeholders to develop guidelines and best practices for securing the smart grid, a critical component of modern energy infrastructure.
- European Network and Information Security Agency (ENISA) Working Groups: ENISA, an EU agency, often establishes working groups to address specific cybersecurity topics, including critical infrastructure protection. These working groups contribute to the development of guidelines, best practices, and recommendations to strengthen cybersecurity across Europe.

These technical committees, working groups, and panels, along with those mentioned previously, play a significant role in shaping the standards, guidelines, and best practices for critical infrastructure protection with a focus on security. By engaging with these groups, organizations can ensure they stay informed about the latest developments in security and resilience for critical infrastructure.

## 9.1 PRECINCT contribution to CEN/WS IPCI

In their role within the [H2020 STRATEGY project](#), PRECINCT partner #19, KEMEA was the proposer and writer of a CEN workshop Agreements (CWA) on the 'Improvement of information processing in crisis management of critical infrastructures for computer assisted data gathering, display and reporting'.

Currently, in case of an emergency incident, there is no standardised type and content of information that is sent from a critical infrastructure operator to a nationally designated contact point for critical entities.

The STRATEGY project has been working on this issue and has systematically identified and prioritised gaps in standardization in crisis and disaster management and has compared them to the needs of end users and to available opportunities across a broad spectrum of disaster management activities. This work has fed into the development of a proposed standard "Improvement of information processing in crisis management of critical infrastructures for computer assisted data gathering, display and reporting".

Through the synergy developed between the PRECINCT and STRATEGY projects, PRECINCT was invited to join the CEN workshop to contribute to the development of this standard and to support the validation of the standard related to "fields for PRECINCT incident reporting activities" within the PRECINCT Living Lab (LL) in Athens. As such and on behalf of the PRECINCT consortium a NDA was signed by Inlecom Commercial Pathways (ICP), the project coordinator.

Through this agreement, PRECINCT contributed to the workshop meetings and the development of the Draft CEN Workshop Agreement. The documentation from the workshop is available<sup>[2]</sup> on the CEN website. It is hoped

that this will be useful for stakeholders such as security liaison officers of critical infrastructures, public administration, coordination centers, first responders' control rooms and first responders of a higher command level. In addition to participation and contribution to the workshop meetings, the incident reporting form developed in the specific CWA was demonstrated in the PRECINCT Athens Living Lab relevant feedback for the usability and usefulness of the form, was collected by the participating end users and fed back to STRATEGY. The public consultation period on the CWA is now complete and the final documentation will be freely downloadable from [CEN/CENELEC website](#).

## 9.2 PRECINCT application of STRATEGY standard in Athens LL3

The Center for Security Studies / Ministry of Citizen Protection, pursuant to P.D. 39/2011 (Greek Government Gazette A'-104/ 6-5-2011), which harmonized the EC Directive 114/2008 in the Greek Legislation, has been nominated as the national contact point for the protection of the National Characterized European Critical Infrastructure (NCECI) located within the Greek territory (Article 10, par. 1 P.D. 39/2011). In this framework, KEMEA coordinates the examination of issues on Critical Infrastructure Protection (CIP) within the Greek territory in line with the competent authorities of the other Member States and the EC. The project "Targeted Actions for enhancing the protection of National Characterized European Critical Infrastructure – NCECI"<sup>7</sup> includes a series of actions and deliverables that are being developed to provide the background for a commonly acceptable level of safety and protection for the NCECI. To this end, it is critical to ensure the systematic cooperation of the bodies that are responsible for the safety and protection of citizens with the operators and in particular the Security Managers of the Infrastructures. Its main goal is to define a framework of synergies between those involved in security, protection and the sound operation of infrastructures that will contribute to the strengthening of the resilience of society, for the smooth operation of which, critical infrastructure constitute a key pillar.

To that end, KEMEA within its current Action and related activities in the field of Critical Infrastructure Protection is developing the pilot Coordination Center for Critical Infrastructure Protection (H3CIP) in its premises, following the supply of equipment and cut-edge GIS software. The main objective of the Center is the possibility of exchanging information among the crisis management agencies and first responders and the operators and managers of Critical Infrastructures in security-related topics.

The national platform for national CIs and the under-development information system aims at the systematic information of the infrastructure operators for their level of risk after analysis of natural and technological risks and anthropogenic threats. In addition, infrastructure operators are requested to provide pilot reporting of emergency safety and security incidents exceeding the limits of their Infrastructure, through a secure online application, in order to inform the competent authorities and to contribute to the register of security incidents. The scientific elaboration of the latter, in collaboration with the infrastructure and the operational bodies, is done for reasons of improvement of the infrastructure protection plan at national level. The Center and its operations are developed according to the standards of European CIWIN and ERNCIP.

The H3CIP manages any risk / threat that may have an impact on the operation of infrastructure and has a spatial dimension and can be defined with geographical coordinates. The way hazards / threats information is managed by the H3CIP is the same, regardless of the type of risk (all hazards approach). The purposes of the H3CIP are:

- Strengthening public-private sector partnership and communication on security issues
- Continuous exchange of views and good practices for improving the level of infrastructure security
- The ability to exchange information and information between:
  - the National Authorities
  - the Emergency Response Agencies involved; and
  - the operators / managers of the Critical Infrastructures.

---

<sup>7</sup> <http://www.ciprotection.gr/index.php/en/coordination-center>

H3CIP was demonstrated in the Athens Region Transport Resilience Living Lab with the goal of providing a common operational picture in near-real time to all stakeholders connected to the H3CIP platform; supporting the exchange of information among participating EMETRO (formerly AMETRO), AIA, ATTIKES DIADROMES operators during an incident; and facilitating coordination among the involved stakeholders during a crisis.

As already discussed, KEMEA led the CEN workshop addressing the efficiency and accuracy of Incident Situational Reporting for Critical Infrastructures in the context of STRATEGY project as a continuation of KEMEA's activities in the field of Critical Infrastructure Protection and development of the H3CIP.

The incident reporting form produced in the specific CWA was presented during the PRECINCT Athens LL demo as part of the H3CIP demo, and the incident fields filled out through the form based on the Athens threat scenario were visualized through the H3CIP. The functionality of the H3CIP as well as the incident reporting form were evaluated by the system's intended end users, and relevant feedback for the usability and usefulness for the form was collected by the participating end users.

## 10 Contributions

### 10.1 STRATEGY Project

Effective and response crisis management highly relies on information sharing, requiring efficient coordination and interoperability. The latter can be better achieved through standardization of operations, technological tools and other aspects that govern crisis management. In this respect, STRATEGY<sup>8</sup> aims to contribute to the EU (pre-) standardization process through streamlining, testing and validating (in realistic environments) interoperability-related standardization items in systems and procedures addressing the operational needs of practitioners involved with Crisis Management (across a set of 8 thematical domains encompassing the protection of Critical Infrastructure Protection - CIP).

Considering the above, (pre-)standards facilitate the enhancement of interoperability at organizational, semantic and technical level, supported by instruments of legal interoperability. This common language, common processes and common specifications are established, allowing for the creation of processes commonly understood by a wide variety of first responders, civil protection agencies as well as CI operators. In this respect, interoperability is the tool to facilitate collaboration between organizations and nations and consequently to save lives and protect assets (Sakkas et al., 2022).

STRATEGY, during the initial phase of its implementation, focused on mapping the “as is” situation with regards to the standardization universe relevant to (among others) the Critical Infrastructure Protection sphere. The effort has taken in consideration existing and ongoing (at the time) standardization work against a) the specific Disaster Management Phase being referred to, b) the Hazard Type being targeted, as well as c) individual end user needs as collected past and or-going research effort<sup>9</sup>. Processing on collected data, has been based on the cross-correlation of completed and under-development standardization activity against user needs towards identifying interoperability related gaps that hinder the efficiency of crisis management when it comes to protecting critical infrastructures (Sakkas et al., 2020).

The aforementioned work has led to the identification of a list of 15 primary gaps. Indicatively, a significant area of gaps in need of addressing, deals with the standardization of the format of the Decision Support Systems integrated in a Coordination Center for Critical Infrastructures, considering the variety of existing tools and the need for them to interoperate during crises (as by definition information exchange among stakeholders is deemed as critical for a successful response). This situation usually refers to a complex environment, with multiple interfaces, as well as resources and data formats.

Other important shortages with respect to existing standardization activity include a) the Exchange of information among CI operators by means of pre-selected communication tools and standardized data format and content, b) common Standard Operating Procedures for interconnected critical infrastructures as well as c) standardised procedures for secure registration, authentication, and authorization. Based on the gaps identified with respect to CIP as part of the methodological approach described above, STRATEGY has been engaged in a prioritization process taking into consideration the operational perspective of end-user communities for a) validating the produced outcomes I the latest operational practices and tools and b) selecting the gaps with the highest impact for promoting to (pre-)standards.

This prioritization led to the proposal of two new CEN Workshop Agreements aiming to close some of the above-mentioned gaps. These are the two following:

---

<sup>8</sup> <https://cordis.europa.eu/project/id/883520>

<sup>9</sup> Examples include DRIVER+, FIRE-IN, IDIRA, IN-PREP,MEDEA, RECONASS, ResiStand, SAYSO,RESISTAND and ZONeSEC projects

- CWA IPCI 1 ‘Semantic layer definition and suitability of EDXL-CAP+EDXL-SitRep standards for crisis management in Critical Infrastructures’.
- CWA IPCI 2 ‘Emergency management – Incident situational reporting for Critical Infrastructures’.

The first one (CWA IPCI 1) provides the formal definition of a semantic layer containing the list of field names to be used in the messages transmitted during a crisis. In cases of crisis, especially when data or alerts are transmitted through systems and sensors to a central system, the type of the data transmitted is not necessarily to the machine. Moreover, the proposed CWA evaluates the suitability of two existing standards for the automatic collection of the information of crisis in CIs (OASIS EDXL-CAP)) as well as the automatic generation of a situation report based on the information collected through the system and their delivery to strategic command levels (OASIS EDXL-SitRep).

The second one (CWA IPCI 2) focuses on the provision of requirements and recommendations in order to standardize the set of information to be sent from a critical infrastructure to a national competent authority in case of an incident. This CWA targets the higher command levels and not to be used by the force so the field. The CWA supports the implementation of the new CER 2022/2557 related to incident reporting and notification. In addition, recommendations for presenting the incident report on a paper format or a pc screen. The CWA could be used even in a real-time, near real-time basis in order to support and create an enhanced situational awareness picture or even for simply statistical purposes. It is compatible with other standards and more specifically with the OASIS EDXL-SitRep, the M/ETHANE and ISO/TR 22351. The CWA is not a technical schema.

Both of the (pre-) standardization items mentioned above have been progressively evaluated, at various stages of their elaboration process, by primarily end-users. In this respect, the operational application of the concepts of the CWA in consideration have been demonstrated, used and discussed during a series of Tabletop Exercises and Full-Scale Exercise, participated by (among others) first responders and critical infrastructure operators. Based on fictional scenarios, during the said exercises’, stakeholders had the chance to be engaged in hypothetical situations whereby though making use of the concepts of the said pre-standardisation items, they were able to experience the interoperability benefit that stems from their operation exploitation. Feedback provided through the above events was fed back in the documents elaboration process towards their finalization, for ensuring the development of a practical document – intended to be as mature as possible for end-users to exploit operationally.

## 10.2 PRAETORIAN Project

### 10.2.1 About PRAETORIAN

PRAETORIAN<sup>10</sup> strategic goal is to increase the security and resilience of European CIs, facilitating the coordinated protection of interrelated CI against combined physical and cyber threats. The project provides a multidimensional (economical, technological, policy, societal) yet installation-specific toolset comprising: (i) a Physical Situation Awareness system (PSA), (ii) a Cyber Situation Awareness (CSA) system; (iii) a Hybrid Situation Awareness system (HSA), which include digital twins of the infrastructure under protection; and (iv) a Coordinated Response (CR) system. The PRAETORIAN toolset supports the security managers of Critical Infrastructures (CI) in their decision making to anticipate and withstand potential cyber, physical or combined security threats to their own infrastructures and other interrelated CIs that could have a severe impact on their performance and/or the security of the population in their vicinity.

---

<sup>10</sup> <https://cordis.europa.eu/project/id/101021274>



The project addresses how an attack or incident in a specific CI can jeopardise the normal operation of other neighbouring/interrelated CIs, and how to make all of them more resilient, by predicting cascading effects and proposing a unified response among CIs and assisting First Responder teams.

PRAETORIAN is a CI-led, user-driven project, which will demonstrate its results in three international pilot clusters, Spain, France and cross border Croatian-Austrian, involving 9 critical infrastructures: 2 international airports, 2 ports, 3 hospitals and 2 power plants. The demonstration focuses around four attack scenarios developed by the project and described in the following section.

## **10.2.2 Use case scenarios**

### **10.2.2.1 CR-AUT (#1)**

Hydropower plant (HPP) security centre is alerted by the authorities about potential attack on the HPP. Triggered by this information a temporary counter unmanned aerial vehicle (C-UAV) system is contracted and deployed to reinforce the physical security of the HPP. In preparation of the attack, the terrorist intelligence team has obtained administrator credentials of HPPs industrial control system and used drones to collect aerial images of the HPP restricted area. Attackers then initiate a cyber-attack on the HPP industrial control system with the intention to impact power production. A coordinated physical attack includes entering HPP restricted area, manually destroying flood gates hydraulic mechanism and dam destruction.

Another group of attackers seizes opportunity to carry out a cyberattack on a hospital which is located in the area affected by flood and power blackout caused by the attack on the HPP. They execute a zero-day ransomware attack with the intention to get access to the central data hub of the hospital and steal patients' data.

### **10.2.2.2 French (#2)**

A corrupted power plant employee connects a USB key containing a malware into the PACS (Physical Access Control System). The same person creates 5 access badges for the attackers. The terrorists use the badges to access the transformer station and place several bombs in strategic locations. Additionally, they access the turbine area and connect a PC to the electrical cabinet in order to disrupt the industrial process. During night the time-triggered bombs detonate one by one, causing fire and a huge smoke screen. The time-triggered dormant malware wakes up and disables all badges. The power plant employees try to get out of the facility but discover that the exit buttons do not work. As a last resort, they use the emergency buttons, which overflows the PACS with alerts coming from the emergency buttons.

Attackers perform malicious acts at the radar stations at the entry of the port estuary to prevent the harbour master from overlooking the navigation in the estuary. The attackers also set up a signal jammer to jam broadcasts from ships. Later, attackers use drones to take pictures of the oil terminal. The port management team issues instructions to extend the perimeter of drone detection system (C-UAV) to the entire site. The drones loaded with explosives fly towards the oil terminals area, one of them succeed to hit an oil terminal and a ship setting them on fire.

### **10.2.2.3 Spanish (#3)**

The port of Valencia has been alerted to raise the security level due to potential attacks detected on social networks targeting European critical infrastructures. It is the Mediterranean cruise high season, and the cruise terminal is operating at full capacity having big cruises docked at the port with more than 6,000 persons on board.

One day, an unauthenticated drone is flying over the port and takes pictures. The drone) is detected by PRAETORIAN tools. Since there is a cruise in the terminal, and the HSA indicates that the area can be potentially compromised, the port authority decides that an underwater drone will do an inspection.

Later on, a cyber-attack on the port IT system has started. The cyber-attack is successful, hackers take control of the access control system in the port and an attackers' vehicle is allowed to enter in the port restricted area and move through the port towards the cruise area.

As PRAETORIAN detects the hacking of the access control system, members of the Port Police get alerted and head towards the cruise area in order to intercept the car. A new drone flying over the port provides images of the attack to guide the terrorists. The Port Police reaches the terrorists and fight them.

The terrorists manage to detonate several bombs and cause damage to the cruise. One of the explosives detonated is a dirty bomb and radioactive particles are disseminated, affecting also the people in the area. It is necessary to evacuate people in the area near the explosion.

Finally, while the terrorist attack on the port is taking place, another drone is detected in the vicinity of the airport. It is unknown if it is related or not, but upon learning that something has happened at the port, the airport activates the alarms and procedures to prevent something happening similar to the port.

#### **10.2.2.4 CR-AUT #4**

A biosafety level 3 laboratory is targeted by a group of terrorists. In preparation of the attack, they find the laboratory blueprints on the dark web, and using social engineering obtain a copy of employee's ID card and the entrance code. A terrorist uses this information to enter the laboratory, steal a bio-sample and insert a malicious USB into the laboratory computer. A terrorist is joined by one team member and both are headed towards the biggest airport in the region. In the meantime, when a legitimate user logs in to the laboratory computer a malware is launched from the malicious USB aiming to destroy laboratory database.

While preparing the scene at the airport a corrupted airport employee, collaborating with the terrorists, disables the check in systems which creates crowd at the airport. The attackers approach the airport carrying the bioweapon, one of them enters the check in area and the other one flies a drone towards the airport.

### **10.2.3 10.2.3 Validation Exercises**

During the validation activities, the aim was to ensure that the PRAETORIAN solution serves its intended purpose and meets operational requirements.

There were four validation exercises in total, one per validation scenario. The sample comprised 24 participants overall. Participants were recruited from the CIs involved in the four validation scenarios. They were selected in a way to create a close match between participants' actual occupation and the role they would assume in the context of the validation scenario.

Participants received an overview of the PRAETORIAN solution, followed by more in-depth presentations of the CSA, PSA, HSA and CR systems.

This was followed by the scenario ployout: In each validation exercise, the respective validation scenario was presented. The course of each validation scenario was narrated and for each step of the scenario, relevant functionalities of the PRAETORIAN system were presented by tool developers. Alerts and notifications were simulated or played on the developed digital twins. Participants were asked questions about their current operations and their opinion on the PRAETORIAN system during the scenario ployout. These questions were

specific for each validation scenario. At the end of each validation scenario playout, participants were asked debriefing questions. Following this, participants were asked to fill in online questionnaires.

#### **10.2.4 Validation exercises concerning standardisation**

The feedback gathered from the validation participants was clustered around the project objectives and PRAETORIAN tool acceptance criteria (AC). Of particular interest for this Whitepaper is the following project objective and the associated acceptance criteria:

*Objective 3 - Improve the resilience of the CIs, their neighbouring population and environment and enable a coordinated response to an attack.*

*AC07 – PRAETORIAN enhances teamwork between the parties involved, e.g. operators and first responders*

While clustering the feedback the topic of standardization was assigned to AC\_07 because standardized systems or regulations and legislations could ease the cooperation between different parties. While some participants saw standardization as a chance or possible benefit associated with PRAETORIAN (in terms of early adopters' privilege), others viewed standardisation as a prerequisite for the implementation of PRAETORIAN tools. One of the challenges reported was the need to ensure interoperability between different CIs' systems.

The following debriefing questions were asked to all participants at the end of the scenario playout. This was done consistently in each validation exercise.

PRAETORIAN can share the information you received during the previous attacks with other Critical Infrastructures on a European scale.

1. *Which benefits do you see in this kind of cooperation?*
2. *Which obstacles do you see in this kind of cooperation?*

From the debriefing feedback, it becomes clear that participants saw several benefits related to communication, coordination or information exchange in PRAETORIAN. While standardization was seen as a possible chance of PRAETORIAN by some participants, others viewed this as a challenge for implementation, as well as ensuring interoperability between different CIs in terms of type of information shared and the communication channels. Other proposed improvements regarded the involvement of authorities and usage of a central point for inter-CI communication.

## 11 Conclusions

This deliverable describes all of the work carried out by PRECINCT partners under task 6.5 “Policy & Standardisation Recommendations”. More specifically, the deliverable discussed the potential impacts the work of the PRECINCT project could have on various sectors and parts of society, the standardization work undertaken by the project under the task, and made recommendations on EU policy, taking into account the current pieces of legislation most relevant to PRECINCT: The NIS2 and CER Directives.

While it remains difficult to assess the immediate impact PRECINCT has had, due to the nature of European Research Projects (finishing at a mid TRL, length of research, etc.), another impact assessment should be carried out either by the European Commission or future research projects to fully assess the impact, particularly in the living labs and transferability demonstrators. These geographical areas, or PRECINCTs, were the first to implement the tools and methods developed by the project; therefore, it stands to reason that measuring their resilience to see if it has increased in the mid to long term would be the best way to understand the full impact PRECINCT has had or can have.

A large part of the deliverable focused on standards and the process of standardization. As noted in the introduction to Chapter 4, standardization can help to simplify complexity by providing a consistent framework for operations, fostering interoperability, facilitating collaboration, optimizing security practices, ensuring compliance with regulations, and supporting scalability. In addition, common and adopted standards can be a booster for the European market, as they allow technology and solution providers to address market needs with products that are already shared and accepted by the user community, helping increase the chance of uptake. D6.5 identified the principal benefits and issues with the standard processes that are related to the technical aspects developed within PRECINCT while also going further by focusing on three areas highly important to the PRECINCT concept: Digital Twins, Serious Games, and Artificial Intelligence. Barriers and opportunities of standardisation in these areas were identified, hopefully serving to guide standardisation efforts in the future, either by standardisation bodies or EU funded projects such as the STRATEGY project.

Additionally, PRECINCT has developed policy recommendations that can help policy-makers develop new ideas to increase resilience of critical infrastructure across Europe. As seen with many other issues such as climate, migration and crime, a European approach can help foster innovation and eliminate varying levels of implementation, funding or resilience, which is at the core of the CER Directive specifically. EU legislation can be a powerful tool in motivating actors to adopt novel solutions such as the ones developed by PRECINCT. PRECINCT’s recommendations encourages the EU to go further in developing ideas such as the CERG group and ensuring that gaps between the NIS2 Directive and CER Directive do not materialize. In addition, mandates such as the creation of centralized coordination centers could help drive their development, leading to further levels of resilience and better responses to both natural and man-made threats.

Finally the PRECINCT project would like to extend its gratitude to the collaboration of other EU projects, such as the PRAETORIAN and STRATEGY projects. It is this spirit of collaboration that drives European Research and allows for European citizens to be protected from future threats.

## References

- 1) Article 16 January 2023 New stronger rules start to apply for the cyber and physical resilience of critical entities and networks EC Digital Strategy Press Release.
- 2) 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 (Text with EEA relevance) (OJ L 345 23.12.2008, p. 75, ELI: <http://data.europa.eu/eli/dir/2008/114/oj>)
- 3) Data Spaces: Governance, Regulations, Interoperability and Standards, BDVA <https://www.youtube.com/watch?v=ONSUIjAhZes>
- 4) Delannoy, S., Verwee, I., & Witvrouwen, H. (2023, March 8). La Police d'Anvers teste un Digital Twin et un Serious Game pour gérer et anticiper les effets en cascades suite à une inondation. *BlueConnect*.
- 5) DIGITAL TWINS AND STANDARDS, BDVA, Valencia Spain, November 22<sup>nd</sup> 2022 <https://european-big-data-value-forum.eu/session/digital-twins-and-standards/>
- 6) Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance) (OJ L 333 27.12.2022, p. 80, ELI: <http://data.europa.eu/eli/dir/2022/2555/oj>)
- 7) Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance) (OJ L 333 27.12.2022, p. 164, ELI: <http://data.europa.eu/eli/dir/2022/2557/oj>)
- 8) European Commission, Directorate-General for Migration and Home Affairs, Evaluation study of Council Directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection – Final report, Publications Office, 2020, <https://data.europa.eu/doi/10.2837/864404>
- 9) European Commission. (n.d.). Types of Legislation. Retrieved from European Union: [https://european-union.europa.eu/institutions-law-budget/law/types-legislation\\_en](https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en)
- 10) European Union: European Commission, Commission Staff Working Document: on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure, 28 August 2013, SWD(2013) 318, [https://energy.ec.europa.eu/publications/new-approach-epcip-swd-2013-318\\_en](https://energy.ec.europa.eu/publications/new-approach-epcip-swd-2013-318_en)
- 11) Introduction to Digital Twins and Standards, Arne Berre, Chief Scientist and Innovation Director at SINTEF and NorwAI <https://european-big-data-value-forum.eu/wp-content/uploads/2022/10/Digital-Twins-and-Standards-v-1-0.pdf> [3]
- 12) ISO/TR 22351:2015, Societal Security – Emergency management – Message structure for exchange of information.
- 13) JESIP M/ETHANE model. Joint Emergency Services Interoperability Programme.
- 14) OASIS Emergency Data Exchange Language Situation Reporting (EDXL-SitRep) Version 1.0.

- 15) Sakkas, G., Kazantzidou-Firtinidou, D., Tsaloukidis I., Skarlatos, E., Varela, V. (2022). Critical infrastructure protection: standardization and exercises. SafeThessaloniki 2022 Proceedings, 9<sup>th</sup> international Conference on Civil Protection 7 ne wTechnologies 29 September – 1 October. ISSN 2654-1823.
- 16) Sakkas, G., Tsaloukidis, I., Kazantzidou-Firtinidou, D. et al., 2020. Deliverable D1.1, Standardisation Landscape: Gaps and Opportunities, STRATEGY project.
- 17) Tomás, V. R. (2023). *PRECINCT Recommendations from Horizon Results Booster*. Horizon Results Booster.

## Annex I: White Paper

# PRECINCT

Preparedness and Resilience Enforcement  
for Critical Infrastructure cascading  
Cyberphysical Threats and effects with  
focus on district or regional protection



## Enhanced Resilience of Interdependent Critical Infrastructure

Perspective of the EU H2020 PRECINCT Research Project

Dr. Ronan Frizzell, Mrs. Jenny Rainbird, Dr. Giovanni Nisato, Mrs.  
Loredana Mancini, Inlecom Commercial Pathways



The project has received funding from the European Union's  
HORIZON 2020 research and innovation program under  
Grant Agreement No 101021668



**PRECINCT**



# 1. The Growing Interdependency of Critical Infrastructure

Governments around the world are enacting regulations that require critical infrastructure providers to implement security measures to protect their systems. This is in response to the growing trend of cyber-physical attacks, natural hazards and hybrid threats, which leave Critical Infrastructure (CI) increasingly at risk.

An examination of a recent CER Directive from the European Parliament and Council [1] highlights the indispensable role of CI in enabling essential societal and economic functions across the Union. The growing interdependency of the Union economy is highlighted in the directive, which emphasises the need for harmonised rules to help improve resilience of CI and provide associated supporting measures.

The essence of the directive centres on ensuring CI operators are in a stronger position to prevent and mitigate the effects of adverse incidents that could interrupt the provision of essential services. A key element of this directive that this paper would like to highlight is the recognition that protective measures for individual CI do not go far enough in preventing disruption to essential operations and the topic of interdependent CI must be considered.

This topic deserves further discussion due to the nature of how essential services are being provided within the Union, which, as the directive highlights, has become increasingly co-dependent and cross-border in nature. To support this point, Article 12.2 of the directive discusses how risk assessments for critical entities must consider their dependency on essential services in other sectors and the degree to which other critical entities depend on their services. This should also include considerations of cross-border dependencies.

This white paper is intended to support the discussion on this topic and present the perspective of the EU H2020 funded PRECINCT research project ([www.precinct.info](http://www.precinct.info)). This project investigated the complexities of interrelationships between CIs and how to manage the impacts of cascading effects as a result of hazardous events, with the goal of enabling rapid recovery. The project brought together a broad range of stakeholders from across the CI ecosystem, including industrial actors and research providing organisations. In this way, the project was able to gather varying perspectives and insights from this strong, cross-industry consortium on the topic of interconnected CI and develop meaningful technological solutions to address the associated challenges. This white paper aims to ensure the learnings from this project are shared with interested stakeholders across the community and considered when developing future policy and industry standards in relation to the protection of CI.

**In summary, it is the view of the project partners that interconnection of CIs should be considered an essential part of any related policy due to its importance, not only for individual CIs, but also for the collective resilience of the Union economy and citizens. In order to realise this improved resilience there is a need to develop an ecosystem where CI operators are both mandated and supported to engage collectively to mitigate risks of cascading effects associated with interdependent CI.**



## 2. Complexity of Interconnected CIs

With the increasing interdependence of various CIs across Europe and the associated risk of disruption caused by cascading effects, it is essential to understand and manage the dynamics of this extremely complex collection of heterogeneous yet interconnected systems in order to safeguard the interests of the Union.

The complexity of interconnected CIs can be understood when one considers the potential interactions between diverse verticals (for example: emergency services, electricity, food production, telecommunications, water infrastructure, supply chains, etc.), which ultimately results in a significantly broader threat canvas compared to the case of considering a single CI operating independently. The problem is compounded by the range of possible, unanticipated combinations of threats and actions that can affect whole cities, districts or regions.


Because of the complex nature of interactions between interdependent CI and the potential for broad impact across many jurisdictions, a holistic approach is required to ensure resilience of CI within and between member states. A further challenge arises when selecting the scale at which to analyse and manage the problem. This is because the dynamics of cascading effects can vary when one considers interdependent CIs at different scales across the member states. For example, the threat of cascading effects exists with interconnected CIs across different geographical areas, such as districts, cities or regions.

The problem is also not static in nature and the appropriate reaction and/or allocation of resources in response to an incident will depend on the specifics of the incident, size of the area affected and the organisations impacted. This interplay between interconnected CI can also lead to counterintuitive, or “nonlinear”, effects, further complicating decision making aimed at mitigating the consequences of cascading effects.

From this overview of the underlying issue, it follows that there is a need to supervise and manage / coordinate these complex interdependent networks and Cyber Physical Systems of Systems (CPSoS). However, this approach is inherently challenging since the CI ecosystem is characterised by distributed ownership and management structures.

Individual CIs have clear ownership over the protection of their services and understand well how to respond to protect those services. However, it is challenging to define ownership of the interaction between CIs in terms of mechanisms, processes, data sharing requirements, etc., all of which could be implemented to enhance resilience of interdependent CIs. The challenge here is understandable because the overall situation is extremely difficult to assess by individual CIs, as in many cases these only have a local view of their own infrastructure, rather than a wider “system-view”.

To compound this issue many existing critical infrastructure protection (CIP) systems were designed and implemented independently and according to different requirements and use cases. This can create interoperability issues when implementing CIP solutions that require integration with multiple systems. This, in turn, adds complexity and cost to enabling interactions between CIP solutions. Nevertheless, interdependency must be considered in



any risk analysis, including those focused on single CI entities. This is necessary, even in cases of the most secure CI entities, where exogenous factors can affect operations, and therefore these are viable risks that must be assessed.

Direction from policy makers is very important in this context, as they can drive the behaviour of countries and their citizens. The question for policy makers to address therefore centres on how interdependent CIs could be understood and managed, such that decisions can be made on the optimal resource investment for protecting against cascading effects in such complex systems. A clear statement from policy makers and consensus from within the industry on accountability is also required in relation to addressing the issues associated with cascading effects of connected infrastructure. In addition, due to the multi-scale nature of the problem, public-private collaboration solutions that apply across different districts, cities or regions will have to be devised and driven by policy decisions.

### 3. Critical Infrastructure Coordination Centre (CICC)

#### Increasing Preparedness and Awareness

Refining the systems and processes for understanding and mitigating the effects of cascading effects of interconnected CIs is important as it can minimise the need for reactive responses to incidents and lack of information leading to resource overallocation, the cost of which will most likely be borne by the public. On-going public-private planning and communications can lead to optimisation of resource allocation by promoting information sharing and development of best practices that will ultimately benefit all Member States.

It is the view of the PRECINCT project that Centralised Critical Infrastructure Coordination Centres (CICCs) can play an important role in enabling communication between interdependent CIs. Such centres can focus on continually simulating and assessing the probable consequences of related threats, an activity that can be replicated at different levels across each Member State to address threats to interconnected CI at district, city, regional levels, as required.

During the PRECINCT project, one of the core issues considered that drives the need for such centralised roles was the challenge of coordination between various stakeholders, such as government agencies, private organizations, and regulatory bodies. Poor communication and restricted exchange of data can lead to delays or inconsistencies in the response to attacks on CI, ultimately leading to delays in recovery. In some cases, there may be overlapping governance and competence areas that further complicate the adoption of effective mitigation strategies.

The importance of this type of centralised role is recognised by the CER Directive [1], which calls for the establishment of the Critical Entities Resilience Group (CERG). This group will enable information exchange between Member States in relation to CI protection, identify and exchange proposals on best practice, and will consider cross-border and cross-sectoral interdependencies.



The CERG will facilitate exchange of information at the Member State-level, which is a broad and necessary role. Other centralised coordination centres also exist within member states covering more limited pockets of the European CI (examples include: Safe.Brussels<sup>1</sup>, IAEMO<sup>2</sup>, Hellenic National Platform for Disaster Risk Reduction (HNP-DRR)<sup>3</sup>, Antwerp's Emergency Planning department<sup>4</sup>). However, considering the complex, multi-scale nature of the problem, it was found in the PRECINCT project that the extent to which such entities were clearly established and focused on interdependencies of CI was insufficient. This severely impacts the ability to offer widescale protection against cascading effects of interconnected European CI. It was also found that, despite the need for such CICC entities, there is a risk that such entities will not develop at a sufficient scale through natural market forces due to cost and complexity constraints, creating the need for governmental intervention at multiple scales through clear policy decisions. Directing the creation of such entities and their focus on interconnected CI through policy discussions is possibly a key role for the CERG.

### The Role of the CICC

PRECINCT investigated the role of CICC entities and this paper aims to communicate learnings from the project to be considered in the development of associated policy and governance schemes.

The core role of the CICC considered during the project was to continually analyse interconnected CI at strategic levels, enabling informed, evidence-based decisions to be made about CI interconnectedness, identification of critical risks, preparation of optimised response plans, and running of training simulations.

The key recommendation coming from the project is to ensure policy decisions specifically focus on cascading effects in CI protection by enabling the creation of CICC agencies and support them in gathering information at multiple scales across member states resulting in:

- **Creation / improvement of actionable plans for cascading events**
- **Creation / improvement of emergency response training for cascading events, which can expose (and test) the critical emergency responses in realistic simulation environments**
- **Identification of case studies to be funded, which develop the justification for resource allocation to protect against cascading effects**
- **Exposing unforeseen consequences of triggering events and preparing appropriate responses**

This information is primarily targeted at strategists / planners at different levels across a Member State (e.g. regional-level, city-level, district-level) to help in understanding interdependency issues. The overall goal is to increase preparedness and awareness, and enable the implementation of training scenarios that demonstrate benefits in terms of time / cost impact on CI due to hazardous events.

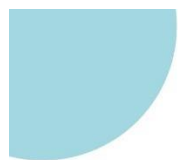
To make these CICC entities effective they will require a mandate and clear legal status within Member States to ensure adequate security of data, information sharing, participation from CI owners, while enabling it to perform a monitoring and audit role. To be widely effective

1. <https://safe.brussels/en>

2. <https://www.iaemo.ie/>

3. <https://www.preventionweb.net/national-platform/greece-national-platform>

4. <https://www.antwerpen.be/contact/dienst-noodplanning>



CICCs would need to be replicated at different levels across each MS and would be required to deliver information to oversight bodies (such as the CERG discussed earlier), which would in turn facilitate inter-MS communications and other centralised functions such as: sharing of best practice, defining of minimum standards, development of decision making tools.

The expected result of the approach described here is to combine the effects of 1) enhanced coordination during adverse events, 2) improved abilities to understand, anticipate and prepare for cascading effects, and 3) sharing of lessons learned / best practice across Member States to support interdependent CIs in going beyond resiliency to an “antifragile” state. This concept, introduced by [2], is centred on the premise that predicting all causes and effects of future adverse events is not possible. It is preferable to create adaptive systems, which learn how to better respond to future threats from past experiences, and thus benefit from adverse events [3][4].



The table below summaries some of the key distinctions between CICC and CERG entities:

CICC	CERG
Multiple instances across Member States covering different groupings of CI, providing localised and detailed views of interdependent CI.	Single entity that acts as an oversight body at EU-level.
Continually analyses interconnected CI at strategic levels, enabling informed, evidence-based decisions to be made about CI interconnectedness, identification of critical risks, preparation of optimised response plans, and running of training simulations.	Enables information exchange between Member States in relation to all types of CI protection, identifies and exchanges proposals on best practice, and considers cross-border and cross-sectoral interdependencies.
Key role is to gather information at multiple scales across member states.	Receives and assesses information from various CI-focused entities across all Member States, including the various CICC entities, to provide EU-level oversight and guidance on protection of CI within the Union.
All information and findings primarily targeted at strategists / planners at different levels across a Member State (e.g. regional-level, city-level, district-level) to help in understanding interdependency issues.	Could mandate Member States to create CICC entities through policy decisions.

### Building Trust with Stakeholders

The approach of implementing CICC at multiple levels across Europe is driven by the need for a systemic solution for the protection of interdependent CI. The core issue with this holistic approach is that widescale implementation relies on adoption and engagement by individual owners of CI elements.





Within the PRECINCT project, interactions with owners of CI elements highlighted barriers to this engagement, the main issue being related to data sharing. The issue is created by the security risk of disclosing vulnerabilities to ill-intentioned agents through sharing the information necessary to understand the interdependency of CIs. For any CICC to function effectively, it will be critical to convince owners of CI that the benefits of engaging outweigh the risks of data sharing.


Trust-building among stakeholders and decision makers is crucial in any sector. This is especially so for CI management, where data sharing can go against established CI risk management processes. This presents a clear dilemma for CI owners and results in a clear barrier for adoption of centralised solutions. To encourage willingness and trust to share data among CI operators, it will be necessary for policy makers to focus primarily on clearly articulated governance models outlining central data management processes that address data sovereignty and control.

This theme of trust also extends to the selection of technical solutions that support communication between CI entities. The security management and the appropriate communication of security measures related to the technical solutions should therefore also be high on the agenda for policy makers wishing to alleviate barriers to the mitigation of cascading effects.

Based on the above discussion it can be seen that demonstrating the benefits of multi-CI interactions is crucial for building and maintaining trust with CI operators. It is recommended that these benefits be communicated at both strategic / leadership and operational levels in CI organisations to garner support and engagement in CIP strategies and technologies. Such demonstrations could utilise simulation technologies, such as Digital Twins (DTs), to reproduce past critical situations and showcase the effectiveness of management solutions that consider the effects of interconnected CI. Such an approach will need to be carried out in a focused way as no city or region is the same, and metrics for understanding the effectiveness of different CI management interventions at city / regional levels will vary on a case-by-case basis. As such, any case studies funded to develop the justification / evidence for CI owner engagement to protect against cascading effects should involve direct interactions with all stakeholders from the early stages, ensuring the specifics of future users' needs are addressed during the design process.

Diversity is also an important consideration here because of the potentially widespread impact of CI cascading effects. Diversity can be integrated at the root of policy decisions when defining required stakeholder engagements and making provisions to ensure the full community of those impacted by services from CI are fully represented. In addition, diversity can help when deciding on technologies and processes to implement to ensure they are effective in reacting to and/or preventing cascading effects across broad communities.

For example, considering cognitive diversity that arises by gathering the perspectives of a variety of people (different genders, ages, professions, etc.), it follows that diversity is critical to broadening the solution space for enhancing interdependent CI resiliency. This is because bringing diverse groups of people together enables multiple points of view to emerge, reduces perception bias and group-thinking by providing a holistic view of highly complex situations,



helping to identify vulnerabilities. Diversity can also be considered in how reactions are planned and resources allocated to prevent cascading effects, ensuring equality of responses and resources across different communities of potentially impacted stakeholders.

### Unified Vocabulary and Metrics

As discussed, complexity is inherent to systems involving interconnected CI. The absence of a unified vocabulary and metrics to assess resilience in a qualitative or quantitative manner enhances the difficulty of effectively planning resource allocation and can lead to expensive, reactive approaches for mitigation of cascading effects.

It is envisaged that one of the key functions of any CICC will be to develop metrics and tools to understand how to optimally allocate resources within their area of influence to minimise adverse effects on supply of services due to the interconnection of CI entities. Such metrics provide a route for CI emergency planners to allocate their resources more effectively and efficiently. Essentially, meaningful metrics can be used to better understand how different choices of preventative measures can impact inter-CI resilience, leading to more optimal resource investment.

The choice of these metrics for evaluating CI resilience is challenging and will depend on the scenario being investigated. To ensure these metrics are meaningful, engaging with all affected stakeholders is important, and these should include regional authority personnel, operators of the CIs, and representatives from users groups. Based on this engagement, guidance could be provided by policy makers to clarify acceptable metrics or the characteristics of such metrics.



It has been discussed that sharing of data across CI is key for the implementation of solutions that tackle cascading effects. Along with the willingness and trust from CI operators to share data that was discussed earlier, this also requires **data interoperability** (a technical and organisational culture issue). The recommended approach to address this issue is to ensure the ecosystem can support the development of standardisation bodies that work to create industry-driven, standardised vocabularies (ontologies), and data exchange protocols that facilitate inter-CI collaboration and communication in the long term.

It is recognised that related activities are underway with recent efforts as part of the CEN Workshop Agreement [5]. Ensuring such standards facilitate understanding of interdependencies and interconnections between CIs will be important. In this way, the impact of failures in one CI entity could be understood by other CIs through standardised interfaces / data exchange.

### Cross-Border Issues

A number of inter-country issues became apparent during the PRECINCT project, which added to the complexity and resource requirements needed from CI operators to comply with regulatory requirements. This is because regulatory requirements tend to vary across different regions and countries, creating additional challenges for commercial organisations offering services and products across borders. Essentially, this is driven by how CI is defined and regulated in different countries, and this creates issues for CI networks spanning multiple





countries. These multiple layers of legislation and varying regulation compliance requirements, both local and international, may hinder the development of generic CIP solutions, which may need instead to be developed for specific local needs and contexts. Policy decisions should consider such complexities when mandating actions from CI organisations providing cross-border services, potentially providing supports through dedicated inter-Member State agencies that can work to harmonise regulation and foster improved resilience through smoother communications channels.

Semantic modelling (i.e., controlled vocabularies, taxonomies, ontologies) can be considered here to mitigate cross-border challenges. Such modelling approaches could be maintained centrally by the EU, upon which standards can be defined and implemented. The aim of such modelling and associated standards would be to enable 1) unified identification of infrastructure that could be considered critical, and 2) enhanced communication between Member States. On this second point, translation of CI-related terms and processes to the various languages that exist in the EU is essential, but must be done in such a way that ensures the same meaning is maintained across country borders.

### Cost Considerations


A significant challenge related to inter-CI resilience protection is covering the costs of enhanced protection against threats that are outside of the immediate responsibility of a particular CI operator. This calls for specific budgets allocated to measure and increase resilience of interconnected CIs. It is understood that such budgets do not yet exist, and support to unlock such funding would be necessary at the city council, regional or even national level. Existing budget lines would likely be needed initially to support developing metrics that demonstrate ROI and justify further investments by governmental agencies. The exploration / simulation activities discussed earlier to articulate the potential impact of cascading effects of interdependent CIs would be highly beneficial during budget allocation discussions and therefore a critical element in the required efforts to enhance resilience of CI.

It is noted that budget considerations would not just require the funding for analysis and justification but also require funding for implementing resilience enhancement strategies. Policy could consider the importance of these impact assessment activities in order to support financial planning at governmental levels.

### CIP Market Considerations

It is expected that as the public becomes more aware of the risks facing interconnected CI, there will be increased demand for solutions that defend CI from these risks. In anticipation of this, the Critical Infrastructure Protection (CIP) market needs to be ready to meet the resulting demand. Part of overcoming this issue is to ensure policy and standardisation are in place to support the developing ecosystem.

A comprehensive analysis of the CIP market was conducted as part of the PRECINCT project, which highlighted certain issues that can be considered during policy development. Overall, the CIP sector is a highly fragmented, complex, and global market. The market dynamics



in Europe have been found to be more complex than other regions, such as the US, with municipal, regional and national dimensions to consider and higher linguistic and cultural diversity. The EU is also introducing coordination directives, such as the recent CER and NIS-2 directives in 2022 [1][6][7], which are expected to influence the market dynamics in the medium term and provide incentives for adoption of coordinated CI risk management processes [8]. The competitive yet fragmented CIP market currently lacks integrated solution to identify, prevent and manage cascading effects across interconnected CI, which poses challenges for implementation of policy decision related to this topic.

It follows that compliance with new regulations will be a significant driver for adoption of advanced CIP solutions, but also a concern from a cost and administrative-load perspective. Any new technologies needed to communicate and coordinate between CI service providers will require additional funding for dedicated training, and adaptation within CI management procedures. Ensuring awareness within the market regarding policy developments and upcoming legislation will be important for enabling CI owners to have the time to prepare for legislative changes. This awareness within the market is also important to ensure time is provided to developers of CI protection services and digital solutions to create products and service offerings such that solutions can be deployed at scale. This helps ensure costs of compliance are minimised, which is particularly important within this cost-sensitive market. The time to develop solutions is also seen as critical due to the complex global market within the CIP sector, where systems and solutions will need to be specific in order to alleviate the challenges of different classes of CI actors.

Another challenge to consider concerning sustainable roll-out of technological solutions to support compliance with new legislation is the secrecy inherent to the CI management market. This is, of course, necessary to avoid exposing vulnerabilities, as discussed earlier, however, from a market development point-of-view, it can also hamper the rate at which the CIP solution market can grow due to restrictions on sharing implementation information and / or access to certain (potentially bespoke) solutions. To address these constraint, standardisation of CIP solutions should, where possible, prioritise solutions that balance robust security with the ability to scale solutions across the sector, with the overall aim to facilitate uptake at low cost.

Supporting this low-cost requirement is the adoption of cloud-based solutions, which is increasing across all sectors, including critical infrastructure. This presents an opportunity for companies that provide cloud-based CIP solutions, which can take advantage of cloud technologies to provide greater scalability, flexibility, and cost-effectiveness.

Certain considerations, particularly around security, are necessary when considering cloud-based solutions for CI. For these solutions, it is necessary to develop specific classes of contracts that apply to this market, along with robust certification and audit mechanisms. European-level initiatives are in place to address such issues, such as GAIA-X [9], where the goal is to link cloud services to share data across a trustworthy environment.



## 4. Technology To Support CICC

The purpose of this section is to share learnings from the PRECINCT project on specific technologies that have the potential to support the CI sector in better understanding the impact of interconnected CI and mitigation of related cascading effects.

From the discussion earlier it is clear the topic of interconnected CI is complex, however, there are technology-based solutions that can support enhanced resilience in these CI networks. Generally speaking, the development of emerging technologies, such as artificial intelligence (AI), digital twins, and blockchain, presents opportunities for CIP solutions that can leverage these technologies to provide more effective and efficient security solutions.


The PRECINCT project explored the potential of various tools and processes to mitigate the effects of cascading effects. These tools addressed some of the previously discussed challenges around understanding this complexity and helping users to enhance resilience and / or derive plans for rapid recovery following a disruption to services. The key requirements for this technology were **affordability, effectiveness, security, and transferability**, all of which were fundamental to allow solutions to be scaled to multiple levels across member states.

A focus of the technology explored in PRECINCT was to model the current and future behaviour of territory-based interdependent CIs in a variety of conditions and configurations, to anticipate threats, to detect anomalies, and understand dynamic interdependencies and cascading effects. This resulted in optimised command structures and coordinated responses between CIs and first responders, thereby enhancing the resilience of the territory analysed. Such a modelling approach has the potential to support previously discussed needs in the sector, such as developing the information required for buy-in from CI owners and justification of resources to protect against cascading effects of interdependent CI.

**The PRECINCT Framework** was key to the technologies explored in PRECINCT. This was developed to facilitate the modelling of dynamic interdependencies and cascading effects in complex networks of CI, as well as to quantify resilience (using a specific Resilience Index) and identify short-term and long-term resilience enhancement measures. To efficiently manage risks across Europe and to develop sustainable mitigation/adaptation strategies, the Framework facilitates the representation of multiple hazards, their potential spatial and temporal interrelations, their resulting risks across interdependent sectors, and how these risks may evolve over time. The output of this can be employed to prepare and adapt to multiple hazard processes, thus enhancing resiliency.

The framework is adaptable and allows CI communities of different size and make-up, operating at various scales within a Member State, to integrate the specifics of their system of CIs. This enables different systems of interconnected CIs to coordinate security and resilience management using the framework's modelling and assessment capabilities.

Central to the modelling capabilities explored in PRECINCT were **Digital Twins**, which combine data / IoT networks, AI and 3D visualisation. This technology has been proven in recent years as a promising decision support tool for various applications. Building on this, PRECINCT has



employed Digital Twins to investigate cascading effects within interconnected CI in the context of a specific region / city. The general idea is that Digital Twins link physical assets to virtual representations and facilitates a bi-directional communication link, supporting optimisation of resource allocation, control loops through sensing and actuation, and exploring “what-if?” scenarios. The tool can therefore be used in the context of training to explore how responses to adverse events can be handled using information from previous real scenarios or based on possible future attacks. For more information, see for example [10].

AI-based tools were key to the Digital Twins and are candidate technologies to identify anomalous behaviour in a network of CIs and has achieved excellent results in anomaly and intrusion detection systems. To enable such AI-based tools, semi- and unsupervised machine learning techniques can be used to detect anomalies and attack patterns within CI systems in a holistic way, characterising their normal / abnormal behaviour and investigating possible impacts on other interconnected stakeholders. In addition, machine learning algorithms can be applied to determine the optimal strategy for resilience enhancement.



A **Serious Games** approach was employed as an innovative vulnerability assessment tool for investigating cascading effects in complex multi-system living labs, where the aim was to support development of new resilience enhancement services. Serious Games are primarily used for training purposes as a form of experiential learning that employ simulation techniques as a cost-effective alternative to often high risk and costly real-life activities. Users are immersed in realistic and dynamic simulations of CI in which they can experience “attack” or disaster scenarios and observe how their responses affect the unfolding of the situations. The expectation is that the use of Serious Games will result in the identification of previously un-anticipated threat combinations involving cascading effects across multiple sectors. Another key outcome is increasing the resilience across an entire CI network by indicating the activities which allow faster recovery from an incident. Examples of the application of serious games from PRECINCT can be found in [11].

PRECINCT enabled various threat scenarios to be simulated and an understanding of the impact various mitigating effects can have on specific resilience measures. This approach is expected to be superior to traditional risk-based approaches since it can explore a very large number of potential enhancements and resulting outcomes, and is thus effective in meeting the complexity challenges highlighted earlier. Based on the simulation results expressed through the resilience scores, it is possible to estimate how strongly each CI entity is affected by given threats and to identify entities that are in danger. This information can be further used to identify protection measures, e.g., if a given CI entity turns out to be affected frequently and severely, it might be necessary to protect it better or to ready a backup in case it fails.

It is expected that tools such as these could form the basis of supporting the work of entities like the CICCAs discussed earlier, along with the Critical Entities Resilience Group, outlined in the CER Directive [1], particularly in activities related to “developing best practices, guidance materials and methodologies, and cross-border training activities and exercises to test the resilience of critical entities”, as described in that directive.

One of the core functionalities of the PRECINCT Ecosystem Platform was its ability to enable communication of data across CIs and distribute data for use in Digital Twins. The data





sources can be generalised IoT data from sensors and actuators, which are connected to a communications component that protects the data through blockchain-based key management techniques. This ensures total visibility across the entire system of interconnected CIs, providing a link between the physical security layer and computing infrastructure. Such approaches aim to mitigate challenges associated with siloed data sets, security by secrecy that lead to poor communication and coordination between interdependent CI entities. The key benefit from such secure communication channels is an ability for CI operators to be more objective in their decision making due to improved communication across key CI. This can lead to increased situational awareness, which facilitates improved resilience against cascading effects.

To enable this approach, the **PRECINCT Ecosystem Platform** integrated multiple scalable and often open-source components. These included, for example, AI-based and Big Data Analytics (BDA) infrastructural services, Semantic Connectivity and Dynamic Integration infrastructure, along with a situational awareness user interface / data analytics visualizer. This was coupled to the computational, networking and storage resources needed to deploy and interconnect the various tools.

Despite the benefits of these various technologies in enabling improved protection of interconnected CI, there were certain challenges highlighted through the PRECINCT project:

1. There is a potential for a lack of trust in new technological solutions, especially ones that involve predictive decision support capabilities. This acceptance issue is particularly evident when asking CI operators to accept decisions of non-human systems in critical situations.
2. Trust is also an issue between CI entities, both in terms of data sharing and in being confident that reactions to cascading effects made by one entity will be in the best interests of others.
3. The culture of the CI market has been found to be resistant to change, often demonstrating long and complex procurement cycles.
4. Regulatory compliance can also be a challenge, especially when considering cross-border interactions and data sharing. Technologies often do not inherently recognise borders and so inter-state data sharing issues will have to be managed during the solution design phase, enhancing the complexity of solutions.
5. Long development cycles for new technologies in the CI market are also a challenge. These are often driven by long periods where proof of concept solutions must run in parallel with older solutions, requiring additional resources from CI entities, which might not exist.

Further details of technology developed during the PRECINCT project can be found at: <https://www.precinct.info/en/publications/articles-press-releases/>.

## 5. Conclusions

With the growing interdependency of the Union economy the European Parliament and Council has emphasised the need for harmonised rules to help improve resilience of CI and provide associated supporting measures. This is driven by the indispensable role of CI in enabling essential societal and economic functions across the Union.

This white paper is intended to support the discussion happening at the EU-level on this topic [12] and present the perspective of the EU H2020 funded PRECINCT research project, which investigated the complexities of interrelationships between CIs. The white paper aims to ensure the learnings from this project are shared with interested stakeholders across the community and considered when developing future policy and industry standards in relation to the protection of CI.

In summary, it is the view of the project that interconnection of CIs should be considered an essential part of any related policy and development of industry standards due to its importance, not only for individual CIs, but also for the collective resilience of the Union economy and citizens. In order to realise this improved resilience there is a need to develop an ecosystem where CI operators are both mandated and supported to engage collectively to mitigate risks of cascading effects associated with interdependent CI.

The summary of key topics below is intended to assist the wider CI community (policy, standard, industry and research organisations) in effectively enhancing the reliance of interconnected CI:

Theme	Description
<b>A Holistic Approach</b>	Cascading effects among interdependent CI have the potential for broad impact across many jurisdictions, requiring a holistic approach to ensure resilience of CI within and between member states.
<b>Managing Complexity</b>	The dynamics of cascading effects vary depending on the specifics of the incident, size of the area affected and the organisations impacted. This leads to complexity in understanding system dynamics and determining optimal resource investment to protect CI. Regulations are needed to ensure CI owners share the required information to manage this complexity centrally but in such a way as not to be overburdened with monetary or administrative burdens.
<b>Accountability</b>	A clear statement from policy makers and consensus from within the industry on accountability is also required in relation to addressing issues related to cascading effects of connected infrastructure. Accountability and governance structures in this space are essential and need to be created where they do not exist.
<b>Multi-scale in Nature</b>	Due to the multi-scale nature of the problem, public-private collaboration solutions that apply across different districts, cities or regions will have to be devised and driven by policy decisions.



<b>Centralised Coordination</b>	Policy decisions should specifically focus on cascading effects in CI protection by enabling the creation of centralised coordination agencies with jurisdiction over groups of interdependent CI. Policy should support these entities to effectively gather the required information at multiple scales across their areas of influence.
<b>Trust</b>	To encourage willingness and trust to share data among CI operators, it will be necessary for policy makers to focus primarily on clearly articulated governance models outlining central data management processes that address data sovereignty and control.
<b>Security</b>	Security management and the appropriate communication of security measures related to the technical solutions should therefore also be high on the agenda for policy makers wishing to alleviate barriers to the mitigation of cascading effects.
<b>Diversity</b>	This topic can be integrated at the root of policy decisions when defining required stakeholder engagements and making provisions to ensure the full community of those impacted by services from CI are fully represented.
<b>Cross-Border Issues</b>	Regulatory requirements tend to vary across different countries and this creates compliance challenges / burdens for CI networks spanning adjacent countries. Such CI would benefit from harmonised regulation that fosters improved resilience through smoother cross-border communications channels. Semantic modelling (i.e., controlled vocabularies, taxonomies, ontologies) can be considered here to mitigate cross-border challenges. This can enable 1) unified identification of infrastructure that could be considered critical, 2) translation to the various languages of the EU, and 3) enhanced communication between Member States.
<b>Cost</b>	Covering the costs of enhanced protection against threats that are outside of the immediate responsibility of a particular CI operator is a significant challenge. This calls for specific budgets allocated to measure and increase resilience of interconnected CIs. Policy development can play a key role in highlighting the impact of interconnected CIs in order to support budget justification and financial planning at governmental levels. Resulting budgets need to be specific to the circumstances of the networks of CI examined and will depend on the area of influence and the nature of threats considered.
<b>Market Growth</b>	Compliance with new regulations will be a significant driver for adoption of advanced CIP solutions that addresses market needs related to interconnected CI. Ensuring awareness within the market regarding policy developments and upcoming legislation will be important for providing CIP solution / service providers the time to effectively prepare for legislative changes. In support of these efforts, standardisation of CIP solutions should, where possible, prioritise solutions that balance robust security with the ability to scale solutions across the sector, with the overall aim to facilitate uptake at low cost, which is a key consideration in the CIP market.

It is interesting to consider how the recommendations discussed here align with the recent CER Directive in terms of timeline and roadmap. The goal of this Directive is to ensure that CI are sufficiently resilient to the increasingly complex threat landscape that exists today (e.g. natural disasters, terrorism, sabotage, etc.) and is expected to develop with time [13]. The CER Directive has already come into force as of January 2023 and Member States have until October 2024 to ensure the requirements of the directive are implemented in national law. This is a relatively brief timeline, yet creates an opportunity to revise how CI protection is implemented, particularly in the area of interdependent CI. The recommendations and actions outlined in this white paper can therefore be considered during the development of CI protection strategies at European and national levels, which must now take place to meet the adoption deadline of January 2026.

The European Commission will assess each Member State's compliance with the CER Directive, which is mandated to happen by July 2027. Considering the discussion within this white paper, it seems appropriate that any such assessment should specifically address the extent to which provisions are made within each Member State's national laws to account for threats due to the increasingly interdependent nature of CI.

Finally, this paper presented an overview of specific technologies explored during that PRECINCT project. These have the potential to support the CI sector in better understanding the impact of interconnected CI and mitigation of related cascading effects.

The key requirements for this technology were affordability, effectiveness, security, and transferability, all of which were fundamental to allow solutions to be scaled to multiple levels across member states. A focus of the technology explored was to model the current and future behaviour of territory-based interdependent CIs in a variety of conditions and configurations, to anticipate threats, to detect anomalies, and understand dynamic interdependencies and cascading effects.

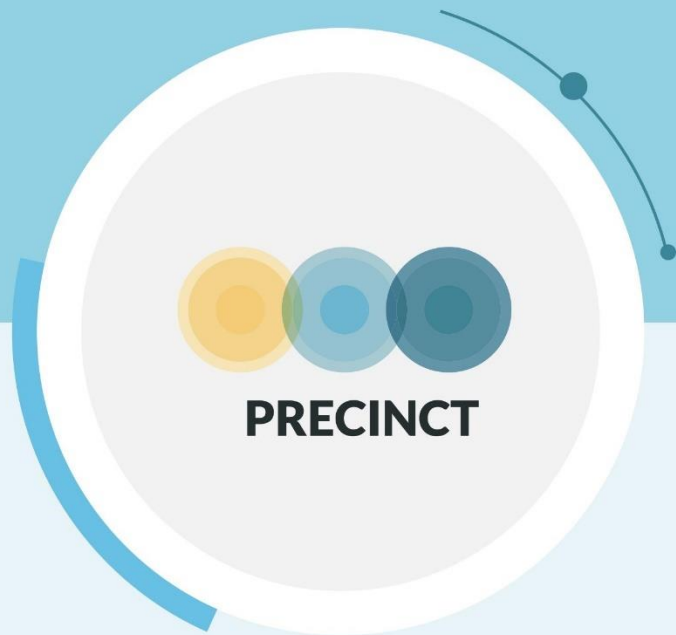
The technologies examined by PRECINCT aimed to provide insight on optimised responses to hazardous events, thereby enhancing the resilience of the territory analysed. The approaches examined have the potential to support previously discussed sectorial needs, such as developing evidence-based arguments required for buy-in from CI owners and justification of resources to protect against cascading effects of interdependent CI. This approach supports efforts to promote long-term benefits for the Union, including economic stability, public safety, and environmental sustainability.

Further information on the specifics of the PRECINCT project can be found at <https://www.precinct.info>.



## References

- [1] DIRECTIVE (EU) 2022/2557 Of The European Parliament and of the Council on the resilience of critical entities and repealing Council Directive 2008/114/EC. Online. Available: <https://eur-lex.europa.eu/eli/dir/2022/2557/oj>
- [2] Taleb, N. N. (2013). Antifragile. Penguin Books.
- [3] Bangui, H., Buhnova, B. and Rossi, B, 2022, Shifting towards Antifragile Critical Infrastructure Systems. In Proceedings of the 7th International Conference on Internet of Things, Big Data and Security (IoT BDS 2022), pages 78-87
- [4] Munoz, A., Billsberry, J. & Ambrosini, V. (2022) Resilience, robustness, and antifragility: Towards an appreciation of distinct organizational responses to adversity. *International Journal of Management Reviews*. 24: 181–187.
- [5] CEN Workshop Agreement (CWA 18023:2023) August 2023. Online. Available: <https://www.cenelec.eu/media/CEN-CENELEC/CWAs/RI/cwa18024.pdf>
- [6] European Commission, 2022, “CER and NIS-2 Directives enter into force to strengthen EU’s Resilience”. Online: Available: <https://ec.europa.eu/newsroom/cipr/items/764849/en>. (Accessed 08th September 2023).
- [7] NIS-2 directive Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Online. Available: <https://eur-lex.europa.eu/eli/dir/2022/2555>.
- [8] Critical Infrastructure Protection Market Size, Share, Revenue Forecast & Opportunities | Markets and Markets (2023). Available at: <https://www.marketsandmarkets.com/Market-Reports/critical-infrastructure-protection-cip-market-988.html> (Accessed: 30 May 2023).
- [9] Gaia-X, About Gaia-X. Online. Available: <https://gaia-x.eu/what-is-gaia-x/about-gaia-x/>
- [10] Nguyen, L., Segovia, M., Mallouli, W., Oca, E.M.d., Cavalli, A.R. (2022). Digital Twin for IoT Environments: A Testing and Simulation Tool. In: Vallecillo, A., Visser, J., Pérez-Castillo, R. (eds) *Quality of Information and Communications Technology. QUATIC 2022. Communications in Computer and Information Science*, vol 1621. Springer, Cham.
- [11] Meisam Gordan, ili Ko, Páraic Carroll, Daniel McCrum, Mona Soroudi, Sandra König, Stefan Schauer, Lorcan Connolly, A Serious Game Conceptual Approach to Protect Critical Infrastructure Resilience in Smart Cities, 14th International Conference on Applications of Statistics and Probability in Civil Engineering (ICASP14), Dublin, Ireland, 2023.
- [12] European Commission: 2022, “Critical Infrastructure: Commission accelerates work to build up European resilience”. Online. Available: [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_22\\_6238](https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6238).
- [13] Cyber Risk GmbH. “The Critical Entities Resilience Directive (CER)”. Online. Available: <https://www.critical-entities-resilience-directive.com/> (Accessed 08th September 2023).



**PRECINCT**

## PRECINCT COORDINATOR

### INLECOM COMMERCIAL PATHWAYS

**PRECINCT Project Coordinator**

Dr Takis Katsoulakos – Managing director

**PRECINCT Project Manager**

Jenny Rainbird - Head of EU Projects Delivery

Inlecom Commercial Pathways  
Room 12, Gateway Business Suites,  
The Reeks Gateway, Killarney, Co Kerry, V93 PPA0

PRECINCT\_PM@inlecomsystems.com

Please, follow us on LinkedIn or Twitter and keep up to date  
with our news items and downloadable content at [www.precinct.info](http://www.precinct.info)





## Annex II: Memorandum of Cooperation between PRECINCT and STRATEGY

### Editors

Name	Contact	Entity
Jenny Rainbird	Inlecom Commercial Pathways (ICP)	Edits to MOU objectives
Giannis Chasiotis	Satways Ltd.	Edits to MOU objectives

### Contributors

Name	Entity	Contribution
Jenny Rainbird	Inlecom Commercial Pathways (ICP)	PRECINCT project outline
Giannis Chasiotis	Satways Ltd.	STRATEGY project outline

### Document Changes Record

Edit./Rev.	Date	Chapters	Reason for change
1.00	01/11/2022	All	Original Document

## MEMORANDUM OF COOPERATION

### Executive Summary

The purpose of this Memorandum of Cooperation is to provide the framework for the envisioned synergy (and / or cooperation) of PRECINCT and STRATEGY projects (in alphabetical order) ultimately aiming at maximising the impact of results produced as part of the research activities delivered by both consortiums. Identifying a commonality with respect to Critical Infrastructure Protection and Standardization, in their research domains, the aforementioned projects agree to proceed to a synergy along a set of specific objectives that are described subsequently.

In this respect, considering the aforementioned areas of thematical relevance between the 2 projects, the synergy outlined through the document in discussion, foresees where possible to a) leverage on lessons learned, b) extend the validation process for all results produced and c) communicate the outcomes to an extended group of potential stakeholders building up on the communities approached by both projects up to this point of their implementation. As such, this synergy will expectedly allow both projects to reach wider target audiences via suitable communication channels, fostering the active interaction with relevant parties of the first responders' / standardisation domain(s).

Provided the above, this document, having the approval and signature of the coordinators of both projects, was created with the intention of documenting and formalizing the context of all subsequent

synergy activities planned to be carried out between PRECINCT and STRATEGY projects. As a starting point, a concise description of both projects is first provided followed by a brief analysis of the points this cooperation as identified at the time of signing this Memorandum of Cooperation.

- **PRECINCT Project Outline**

H2020-SU-INFRA-2020 – PRECINCT (Preparedness and Resilience Enforcement for Critical Infrastructure Cascading Cyberphysical Threats and effects with focus on district or regional protection) is an Innovation Action funded by the European Union under Horizon 2020 research and innovation programme via grant agreement no. 101021668

- SU-INFRA01-2018-2019-2020 topic: - Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe
- Duration: October 2021 – September 2023
- Overall budget: €9,472,739.05
- EU contribution: €7,996,658.38
- Requested funding: *funded as requested*
- Consortium: 40 partners across 12 European Countries
- Summary: PRECINCT will provide a model-driven collaborative and unifying cyber-physical security and resilience management platform for smart resilient ‘PRECINCT’s. Specifically, PRECINCT will develop the following: 1) A PRECINCT Framework Specification for systematic CIs security and resilience management fulfilling industry requirements. 2) A Cross-Facility collaborative cyber-physical Security and Resilience management Infrastructure enabling CI stakeholder communities to create AI-enabled PRECINCT Ecosystems and enhanced resilience support services. 3) A vulnerability assessment tool that uses Serious Games to identify potential vulnerabilities to cascading effects and to quantify resilience enhancement measures. 4) PRECINCT’s Digital Twins to represent the CIs network topology and metadata profiles, applying closed-loop Machine Learning techniques to detect violations and provide optimised response and mitigation measures and automated forensics. 5) Smart PRECINCT Ecosystems, deployed in four large-scale Living Labs and Transferability Validation Demonstrators, will provide measurement-based evidence of the targeted advantages and will realize Digital Twins corresponding to the CIs located therein, include active participation of emergency services and city administrations with results feeding back to the Digital Twins developments. 6) Sustainability related outputs including Capacity Building, Dissemination, Exploitation, Resilience Strategy, Policy/ Standardisation recommendations.

- **STRATEGY Project Outline**

H2020-SU-SEC-2019 – STRATEGY (Facilitating EU pre-Standardization process Through streamlining and validating interoperability in systems and procedures involved in the crisis management cycle) is an Innovation Action funded by the European Union under Horizon 2020 research and innovation programme via grant agreement no. 883520

- SU-DRS03-2019 topic: Pre-standardisation in crisis management (including natural hazard and CBRN-E emergencies)
- Duration: September 2020 – August 2023
- Overall budget: €6.833.075.00

- EU contribution: €5.997.293,25
- Requested funding: *funded as requested*
- Consortium: **23 partners** across 14 European Countries
- Summary: STRATEGY aims to contribute to the EU pre-standardization process through streamlining, testing and validating (in realistic environments) interoperability-related standardization items in systems and procedures addressing the operational needs of practitioners involved with Crisis Management across a set 8 thematic areas (1. Search and rescue, 2. Critical infrastructure protection, 3. Response planning, 4. Command and control, 5. Early warning and Rapid damage assessment, 6. CBRN-E, 7. Training and 8. Terminology/Symbology). Currently the project is in the process of elaborating 11 Pre-Standardization Items (i.e. CEN Workshop agreements – CWAs) and 2 Technical Specification (TSs) Documents along the aforementioned thematical areas.

### **Joint activities and cooperation**

#### **I. OBJECTIVES**

The objectives of this Memorandum of COOPERATION (MOC) between PRECINCT and STRATEGY include:

- 1) Working together, in joint activities and events towards, enhancing the extending results relevant to a) Critical Infrastructure Protection (CIP) and b) standardization and policy recommendations topics, in line to the activities specified in the PRECINCT & STRATEGY Grant Agreements respectively.

In this respect, both projects have agreed to take advantage of the validation processes being planned as part of PRECINCT, in order to encompass the validation of the pre-standardization items elaborated as part of STRATEGY in the CIP domain. More specifically the living labs that are to take place during the last quarter of PRECINCT will be investigated so as to include the validation of the CWA work on Incident situational reporting for Critical Infrastructures developed within STRATEGY. In this context the incident report structure that is addressed in the aforementioned CWA shall be incorporated in the testing environment of PRECINCT. Specific attention shall be given to the living lab of PRECINCT that is to be held in Athens that encompasses the scenario / technical set-up the is mostly applicable to the concept of the STRATEGY CWA. This will allow investigating the applicability of the said pre-standardization item concept by an extended end-user community providing feedback & recommendations towards its completion. In addition, the end-user community of PRECINCT will expand its testing basis on interconnected CIs in line with incident reporting approaches (in a practical manner) that are in the process of being pre-standardized - ultimately enhancing the impact of its results.

- 2) Exchanging information and knowledge (non-confidential and/or sensitive). In order to ensure the full accomplishment of their pre-set research objectives and also extend the impact of produced results, both projects may be engaged in discussing / exchanging non-confidential information that falls in line to their corresponding field of research, goals and activities. In this respect, each project may provide feedback to the approach and/or results as produced by their counterpart in this Memorandum of Cooperation. For optimally coordinating efforts in

the context of the above, a series of online meetings (and face to face meetings if budget allows) will be organized for the purposes of planning, monitoring and evaluating outcomes.

- 3) To create a synergy for dissemination and communication activities, and exploit networks and contacts created as part of each project to ensure the largest / widest outreach of all results. Specific consideration shall be paid to restrictions relating to sharing of personal information and GDPR national and EU guidelines and regulations.

Indicatively as part of this synergy the following action points are being planned and could be further enhanced as optimally identified until the end of the projects in discussion.

- STRATEGY to participate in the 2<sup>nd</sup> PRECINCT Workshop planned for November 22<sup>nd</sup> 2022 in Brussels. During the event STRATEGY shall deliver a presentation of its activities and in addition participate in a round-table discussion for clarifying standardization aspects – relevant to among others CIP.
- PRECINCT shall participate in the 1<sup>st</sup> Interoperability Event organized by STRATEGY on Rome on February 15<sup>th</sup> 2023. During the event PRECINCT shall deliver examples of research activities in the CIP domain that enhance / facilitate interoperability – as relevant to the corresponding theme of STRATEGY. In addition, PRECINCT’s participation during the 2<sup>nd</sup> Interoperability event shall also be assessed as per the progress status of the project close to the time of organization of the said event (approx. May 2023).
- STRATEGY shall investigate its participation to the PRECINCT could participate in events organized by STRATEGY. In this respect, organization of the 2 interoperability events were specifically mentioned for discussing interoperability-related aspects relevant to Critical Infrastructure Protection.
- Both projects will investigate the possibility of organizing a joint event approx. during the 3<sup>rd</sup> quarter of 2023.

## II. POINTS OF CONTACT

The points of contact for the Memorandum of Cooperation between PRECINCT and STRATEGY will be:

**PRECINCT Project Coordinator**

**STRATEGY Project Coordinator**

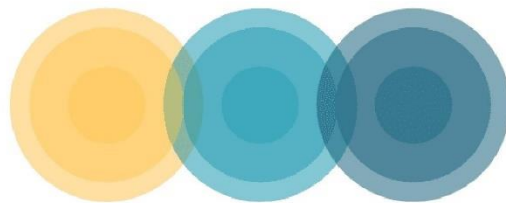
## III. DURATION OF THE AGREEMENT

This memorandum of cooperation is entered into effect.  
On the 1<sup>st</sup> of November in the year 2022

This memorandum shall remain in effect until the end of each of the respective projects (listed in clause I of this document), with the possibility of further cooperations and joint activities (such as workshops, conferences and others).

## **Annex III: Artificial Intelligence Management Procedures: Standard and Recommendation Guidelines**

# Artificial Intelligence Management Procedures



# **PRECINCT**

## Standard and Recommendation Guidelines

AI for Critical Infrastructure Protection – Guidance on the  
implementation of AI-based products

First version  
December 2022

**Keywords:** artificial intelligence, critical infrastructure protection, procedures

**Editors:** Removed in accordance with the  
Ethics Review

**Contributors:** Removed in accordance with the  
*(in alphabetic order)* Ethics Review

## Table of contents

<b>Foreword</b> .....	<b>4</b>
<b>Introduction</b> .....	<b>4</b>
1. Scope .....	4
2. Normative references .....	4
3. Abbreviations and acronyms .....	6
4. Potential challenges.....	6
<b>Data</b> .....	<b>7</b>
Data Management and Administration .....	7
Data Processing .....	9
Policy, Ethics, and Legal Considerations.....	10
<b>Modelling</b> .....	<b>11</b>
AI Algorithm Life Cycle.....	11
AI Algorithm Selection .....	12
AI Algorithm Tunning.....	13
<b>Evaluation</b> .....	<b>13</b>
Evaluation of AI Algorithms .....	13
Evaluation of AI-based Products.....	14
<b>Appendix 1: AI Management Checklist</b> .....	<b>15</b>
<b>Appendix 2: AI Management Report</b> .....	<b>19</b>

## Foreword

This document is the result of a collaboration among PRECINCT project partners with the aim of standardizing the adoption, implementation, and integration of artificial intelligence (AI) technologies in the protection of critical infrastructures.

## Introduction

The purpose of this document is to provide guidelines that improve the trustworthiness of AI-based products. Although it is mainly intended for critical infrastructure protection (CIP), the principles identified may apply to any AI-based products. The document describes many aspects around AI tool development including normative references, potential challenges, data management and processing, as well as policy, ethics, and legal considerations. This manual also defines several considerations in the modelling phase, including AI algorithm design, as well as criteria to evaluate AI algorithms and AI-based products. It concludes the description of the suggested templates for *AI Management Checklist* and *AI Management Report*.

The policy, ethics and legal considerations are of significant importance given the nature of the problems that evolve around critical infrastructure protection, where sensitive data is at risk of being misused if not proper actions are taken to secure data exchange and communication channels.

### 1. Scope

The consortium of collaborating partners in PRECINCT project are exploring ways in which AI-based products/applications can benefit from standardised procedures and recommendation guidelines. This technical report describes key considerations that should guide the development of AI-based products including data management and administration, data pre and post-processing, policy, ethical and legal issues, as well as AI algorithm life cycle, and evaluation of AI-based products for critical infrastructure protection.

### 2. Normative references

Title	Description	Link
AI for Natural Disaster Management	This text “capitalizes on the growing interest and novelty of AI in the field of natural disaster management to help lay the groundwork for best practices in the use of AI for: assisting with data collection and handling, improving modelling across spatiotemporal scales, and providing effective communication.”	<a href="https://www.itu.int/en/ITU-T/focusgroups/ai4ndm/Pages/default.aspx">https://www.itu.int/en/ITU-T/focusgroups/ai4ndm/Pages/default.aspx</a>



AI and Internet of Things for Digital Agriculture	The document seeks to “explore the potential of emerging technologies including AI and IoT in supporting data acquisition and handling, improving modelling from a growing volume of agricultural and geospatial data, and providing effective communication for interventions related to the optimization of agricultural production processes.”	<a href="https://www.itu.int/en/ITU-T/focusgroups/ai4a/Pages/default.aspx">https://www.itu.int/en/ITU-T/focusgroups/ai4a/Pages/default.aspx</a>
AI for Autonomous and Assisted Driving	The document “supports standardization activities for services and applications enabled by AI systems in autonomous and assisted driving.”	<a href="https://www.itu.int/en/ITU-T/focusgroups/ai4ad/Pages/default.aspx">https://www.itu.int/en/ITU-T/focusgroups/ai4ad/Pages/default.aspx</a>
Machine Learning for Future Networks including 5G	This document aims at drafting “technical specifications for machine learning (ML) for future networks, including interfaces, network architectures, protocols, algorithms and data formats.”	<a href="https://www.itu.int/en/ITU-T/focusgroups/ml5g/Pages/default.aspx">https://www.itu.int/en/ITU-T/focusgroups/ml5g/Pages/default.aspx</a>
AI for Health	This text seeks “to establish a standardized assessment framework for the evaluation of AI-based methods for health, diagnosis, triage or treatment decisions.”	<a href="https://www.itu.int/en/ITU-T/focusgroups/ai4h/Pages/default.aspx">https://www.itu.int/en/ITU-T/focusgroups/ai4h/Pages/default.aspx</a>
EU guidelines on ethics in artificial intelligence: Context and implementation	“[T]his paper aims to shed some light on the ethical rules that are now recommended when designing, developing, deploying, implementing, or using AI products and services in the EU.”	<a href="https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/640163/EPRS_BRI(2019)640163_EN.pdf">https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/640163/EPRS_BRI(2019)640163_EN.pdf</a>

### 3. Abbreviations and acronyms

5V	Volume, Velocity, Variety, Veracity, Value
AI	Artificial Intelligence
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
DataOps	Data Operations
DL	Deep Learning
EDA	Exploratory Data Analysis
FGDC	Federal Geographic Data Committee
GDPR	General Data Protection Regulation
ISO	International Organization for Standardization
ML	Machine Learning
MLOps	Machine Learning Operations

### 4. Potential challenges

Potential disruptive impacts of artificial intelligence are expected to challenge the design, implementation, and adoption of AI-based products in CIP and other fields. The first challenge commonly found is the digitization of processes of CI operations. Digital transformation is a required first step that clears the path to the adoption of AI solutions, demanding from CI operators an investment in the adoption of technologies that provide the foundation on top of which AI-based products are to be developed. In the presence of digitized processes, other challenges may arise, including data management and data security and privacy, which refer not only to the storage and management of data, but also to the transmission and exchange of data.

As large datasets are available, some questions may come up regarding the comprehensiveness and accuracy of the data. Large volumes of data do not necessarily translate into accurate and useful data; furthermore, some AI algorithms require labelled datasets, which in many cases, especially in large datasets, are most of the time unavailable.

AI algorithms also pose some challenges that include biases that can be introduced as a result of insufficient or inaccurate datasets, as well as human factors that affect the training of the models. Some types of algorithms, especially those based on artificial neural networks, do not follow processes typical of explainable artificial intelligence algorithms that allows human users to comprehend and trust the results created by the algorithm. Model transparency is another factor that is often underestimated, and sometimes misunderstood. Transparency should be introduced in every step of the workflow, starting at the data collection process, where detailed methodology of the data collection process should be provided, as well as the selection of the AI algorithm, and what was done to reduce the effect of bias in the model.

Modern AI-enhanced systems exhibit a challenge when it comes to integration with legacy systems. The deployment of AI models is not always a straightforward task, especially when models need to be maintained and updated due to the evolving condition of datasets used to train the models.

Declaring the ownership of AI-based products is also a commonly debated topic that confronts the different actors involved in the development of AI-based products. Should the partners that implement the algorithm hold the ownership, or does it belong to the

partners that provide the data? Misusing AI-enabled technologies is often a topic in the radar of ethic committees, especially when the presence of AI is ubiquitous.

## Data

### Data Management and Administration

Data management and administration refers to the process of collecting, organizing, storing, and protecting data. The following concepts indicate a variety of considerations that should be acknowledged in the process of data handling in AI-based products. Some of these concepts are more relevant in CIP due to the nature of the problem at hand, for example, data security and privacy, along with data sharing restrictions are key concepts in datasets collected from critical infrastructures. However, all the concepts should be considered in the process of identifying the right datasets for training AI models.

<b>Data themes</b>	minimum set of concepts used to label datasets in order to enable interoperability between different groups, companies, organizations, and nations.
<b>Data provenance</b>	data provenance records information on how data sets were generated, where the data came from originally, where it has been, and who handled it.
<b>Data acquisition</b>	process of collecting new data, converting, or transforming legacy data, sharing data, and purchasing data.
<b>Data storage</b>	describes what type, where and how hardware and software stores, deletes, backs up, organizes, and secures information. This includes a description of temporary and permanent storage.
<b>Data elimination</b>	defines rules that can be set up in a system for the removal of data. It includes removal from data broker or database following a clear and traceable protocol.
<b>Data accessibility</b>	provides a bridge between available data and the ability to use it. Data accessibility refers to the process that makes the available data suitable for use. This process includes data cleansing, reformatting, and standardization of data sets, as well as the implementation of access controls.
<b>Data democratization</b>	describes rules that complement data access with a comprehensive method to make data available to all the users indistinctly of the degree of expertise.
<b>Data versioning</b>	refers to tracking data sets by registering changes on a particular set of data. This includes naïve approaches such as saving entire datasets under completely new name of file path or the use of timestamps or unique IDs.

<b>Metadata</b>	refers to data or information about data. It is helpful to understand the structure, nature, and context of the data.
<b>Data standards</b>	define documented agreements on data representation, format, definition, structuring, transmission, manipulation, and management of data. Data standards are used for creating, sharing, and integrating data (e.g. ISO, FGDC, etc.).
<b>File formats</b>	refer to standard ways in which data is encoded for storage in a computer file. Define supported file formats and rules for file format conversion.
<b>Data reusability</b>	refers to the idea of using the same data set in different applications or scenarios. Data reusability provides consistency, reduces errors, saves time, and resources, and simplifies application development.
<b>Data sharing restrictions</b>	refers to the definition of guidelines concerning classified data and data sharing rules based on the level of accessibility of the data. Typical categories include <i>“general data”</i> for non-confidential and unclassified data sets, and <i>“classified”</i> category which may include <i>“restricted use/sensitive unclassified”</i> or <i>“strictly classified/secret”</i> data sets.
<b>Data security</b>	protective measures used to protect data against unauthorized access, ensuring data integrity and availability.
<b>Data privacy</b>	procedures for handling of data, including consent, notice, and regulatory obligations.
<b>Data integrity</b>	refers to the accuracy, quality, and completeness of data, which should be preserved over time.
<b>Open Data</b>	can be freely used, re-used, and redistributed by anyone. It must be available and accessible in a convenient and modifiable format and must be available for use by everyone.
<b>Data validation</b>	Ensures high-quality data by analysing whether data was recorded correctly, reflects realistic values, relevant data has no missing entries, and whether data follows established structure and format.
<b>Data annotation</b>	categorization and labelling of data used mainly for AI/ML applications. It is particularly useful for model training.
<b>Data homogenization</b>	is the process of bringing all the data into a unified and common framework to ensure consistency of data, integrity of analysis, and validity of results.
<b>Data fusion</b>	is the process of combining data from multiple sources to create a more complete dataset. It is useful to improve accuracy in AI models.



<b>Synthetic data generation</b>	refers to annotated information generated by computer simulations or algorithms as an alternative to real-world data.
<b>Data bias</b>	occurs when the data source is skewed, providing results that are not fully representative of the phenomenon.

### Data Processing

The term data processing refers to the manipulation and transformation of digital data that can be used to deduce meaningful insights. Data processing covers a range of operations performed on data including manual or automated means.

<b>Data curation</b>	refers to the process of creating, organizing, and maintaining data sets by collecting from different sources and integrating them into repositories that are more valuable. The process involves collecting, structuring, indexing, and cataloguing data.
<b>Data types</b>	is an attribute from a piece of data that provides end-users with a specification on how to interact with the data.
<b>Changes to the number of decimal positions</b>	refers to the precision of a numeric value, which is important for the consistency of results in machine learning.
<b>Data quality</b>	measures the accuracy, completeness, validity, and consistency of data.
<b>Missing values</b>	occurs when an observation does not contain a value, either because it does not exist, or because it was lost due to errors in any part of the data management process.
<b>Change in data units</b>	refers to the use of different unit systems in the same dataset. This may cause inaccurate results in data analysis.
<b>Data normalization</b>	a way to rescale data so that each value falls between a range, usually between 0 and 1.
<b>Data standardization</b>	a way to rescale data so that each value is centered, and the unit is removed, usually using mean of 0 and standard deviation of 1.
<b>Data denoising</b>	refers to the process of smoothing data since data measured in engineering processes often contain different types and degrees of noise that may affect the accuracy of machine learning algorithms.
<b>Data labelling</b>	it is similar to data annotation. It is part of data pre-processing where raw data is contextualized with the addition of one or more labels. This is a necessary step for training supervised models.

<b>Temporal data handling</b>	refers to the process of managing data of moving things, events, or any observation that varies over time.
-------------------------------	--

#### Policy, Ethics, and Legal Considerations

In *EU guidelines on ethics in artificial intelligence: Context and implementation*<sup>1</sup>, as well as in the *General Data Protection Regulation*<sup>2</sup>, the European Union provides several key requirements for achieving trustworthy AI. The requirements include policy, ethics, and legal considerations that seek to protect the rights of end users to a proper use of automated data handling and processing in digital means.

<b>General Data Protection Regulation (GDPR)</b>	Europe's new data privacy and security law that provides regulatory points such as data protection principles, accountability, data security, data accessibility, and data consents.
<b>Ethical approach</b>	data ethics is a data-related practice that seeks to preserve the trust of persons that generate data, including users, patients, consumers, clients, employees, etc.
<b>Transparent design</b>	transparent data usage is key in the design of data products; it improves engagement from users.
<b>Trustworthiness</b>	criteria that measure the reliability of data to procure accurate AI models. The primary criteria to ensure trustworthiness includes credibility, confirmability, transferability, and dependability.
<b>Impact assessment</b>	data protection impact assessment is required under the GDPR, especially in projects that involve a "high-risk" to other people's personal information.
<b>Data sovereignty</b>	concept that describes the legal parameters that affect data, particularly the idea that data are subject to the laws and governance structures of the nation where they are collected.
<b>Government principles and guidelines</b>	guidelines, recommendations, and best practices to ensure appropriate and effective data protection by design by data exploiters.

<sup>1</sup> [https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/640163/EPRS\\_BRI\(2019\)640163\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/640163/EPRS_BRI(2019)640163_EN.pdf)

<sup>2</sup> [https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu\\_en](https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en)

## Modelling

### AI Algorithm Life Cycle

AI algorithm life cycle typically consists of three phases: design, development, and deployment. The phases include several stages that are iterative along the process. Deployment of AI models also requires continuous monitoring of performance since it tends to degrade as new information is available. The following considerations define the most common stages in the AI algorithm life cycle.

<b>Project objectives</b>	states the desired results of an AI project, including the motivation, direction, purpose, goals and deliverables.
<b>Exploratory Data Analysis</b>	a process that is used to understand data sets and summarize their main characteristics. It is a useful step that is required before any statistical analysis, and includes exploration, description, and summarizing data. This process ensures objectivity and interoperability. Typical steps in EDA include descriptive analysis, analysis of data types, missing values, outlier identification, correlations, identification of linear combinations, among others.
<b>Machine learning pipeline</b>	sequence of steps that the data must go through until it is effectively displayed to the end-users. Any ML project requires a minimum number of steps to prepare the data for the training of ML models and the postprocessing of the resulting output. Typical steps include data collection, data preparation, exploratory data analysis, training of the model, model evaluation, model deployment, and performance monitoring. These are the most basic steps of a ML pipeline.
<b>Data acquisition</b>	refers to the process of digitizing data from the context or environment for further storage and examination in a computer system.
<b>Data preparation</b>	refers to the process of cleaning, transforming, and restructuring data so that it can be used by ML/AI algorithms.
<b>Data modelling</b>	provides a common, consistent, and predictable way of defining and managing data resources across an organization. Data models may change.
<b>Dimensionality reduction</b>	is a pre-processing step that seeks to transform data into a more compact set of variables that maintaining the variance of the original data set. Dimensionality reduction is usually accomplished through unsupervised learning techniques.
<b>Feature selection</b>	is the process of reducing the number of input variables to a ML/AI model. The idea is to reduce computational

	cost as well as to improve the performance of the models.
<b>Cross-validation</b>	refers to a procedure commonly used to evaluate the true performance of learning models.
<b>Parameter optimization</b>	refers to the selection of parameters or hyper-parameters to improve the performance of a ML/AI model.
<b>Model versioning</b>	refers to the tracking and managing of changes in ML models over time.
<b>Reusable software environments</b>	refers to the development of reusable software components that can be used in the context of different software development lifecycles and architectural styles.
<b>Model governance</b>	e.g. who is publishing the model and when were models deployed, why changes are made, or when were de models used in production
<b>Model monitoring</b>	measures how well a ML model performs a task during training and in real-time deployment.
<b>Model testing</b>	ML model testing depends on software, but also on problem domain, datasets available, business context, and model selected.
<b>Deployment of AI models</b>	refers to the strategies for AI model deployment, which includes deployment on local machines, mobile devices, or cloud infrastructure.

#### AI Algorithm Selection

The selection of AI algorithms starts by identifying the category of the problem at hand and the objectives that have been defined by the users. The selection depends on a number of criteria, as described in the following definitions.

<b>Problem categorization</b>	categorizing the problem allows us to select the right algorithms to solve a problem. ML algorithms
<b>Identifying applicable algorithms</b>	algorithms can be broadly categorized into supervised (e.g. classification, regression) and unsupervised algorithms (e.g. clustering), transfer learning, reinforcement learning, deep learning.
<b>AI algorithm selection</b>	refers to the criteria to select the best AI algorithm. The selection depends on the problem at hand, available data, including quantity and quality of data. In other words, AI algorithm selection depends on the problem and the characteristics of the data.
<b>Supervised learning</b>	requires label datasets to train the ML models to classify observations or predict outcomes.
<b>Unsupervised learning</b>	ML algorithms capable of discovering hidden patterns without the need of labelled data or human intervention.



<b>Transfer learning</b>	refers to a technique that takes features learnt on a ML problem and leveraging it to a similar problem.
<b>Reinforcement learning</b>	an algorithm that follows a paradigm based on trial and error to solve problems. It is fundamentally rooted in the idea of learning the optimal behaviour in an environment to obtain a maximum reward.
<b>Deep learning</b>	refers to artificial neural networks that emulate the human brain to extract patterns hidden in a dataset. The term “deep” refers to artificial neural networks with three or more layers.

### AI Algorithm Tunning

Knowledge of the types of AI algorithms available is important, but hyperparameter tuning is crucial for exploiting the capability of AI algorithms to identify useful and meaningful insights, trends, and patterns from data.

<b>Hyperparameter optimization</b>	seeks to find well-performing hyperparameter configuration of a machine learning algorithm on a dataset.
<b>Ensemble learning</b>	refers to a combination of several machine learning models to improve the ability to exploit patterns in a dataset.
<b>Active learning</b>	refers to a special case of supervised machine learning that seek to train high-performance classifier while keeping the size of the training dataset to a minimum.
<b>Federated learning</b>	allows collaborative training of decentralized models without sharing data (e.g. confidential data). Models can be trained over remote devices (e.g. servers) while keeping data localized.

### Evaluation

#### Evaluation of AI Algorithms

Evaluation of performance of AI algorithms is a required stage in the AI algorithm life cycle that seeks to measure the trustworthiness of the results of the AI model. It considers some aspects such as time to build, train, and test, as well as other metrics related to accuracy, robustness in the presence of outliers, transparency, explainability, and interpretability.

<b>Model performance</b>	measures the accuracy and trustworthiness of a machine learning model (e.g. precision, accuracy, F1, etc.).
<b>Baseline model</b>	refers to a simple ML model that serves as a reference and as benchmarks for trained ML models. Baseline models can provide clues on future steps in a ML task.

<b>Complexity</b>	refers to properties of the machine learning algorithms that assess execution time and memory usage of a model.
<b>Time to build, train, and test</b>	refers to the time it takes to build, train, and test a machine learning algorithm.
<b>Execution time</b>	measures the efficiency of an algorithm in terms of execution time.
<b>Robustness</b>	refers to a type of metric that measures the reliability of a ML model. It measures the ability of a ML model to process new and independent observations.
<b>Transparency</b>	refers to a characteristic of ML models that allows an analyst to understand what the model is doing to the point of explaining it.
<b>Explainability</b>	refers to a set of techniques that describe the features that influence a prediction.
<b>Interpretability</b>	refers to a set of properties of a ML model that are useful to understand the outcome of the algorithm.
<b>Scalability</b>	refers to the ability of a ML model to handle varying loads of work, either due to a decrease or an increase of data observations.
<b>Reliability</b>	refers to any qualitative property (e.g. accuracy, availability, responsiveness) that assesses how well a ML model performs.

#### Evaluation of AI-based Products

Evaluation of AI-based products is complementary to evaluation of AI algorithms. On one hand, AI algorithms seek to exploit insights, trends, and patterns from datasets, thus, evaluating the performance of the algorithms gives an idea of the trustworthiness of the results. On the other hand, AI-based products refer to AI-enabled products where AI is a core component. Evaluation of AI-based products focuses more on the ethical use of AI models, the ownership, assuring the trustworthiness of the models by updating the AI models with new data.

<b>Ethical use of AI models</b>	<p>according to <i>Ethics By Design and Ethics of Use Approaches for Artificial Intelligence</i><sup>3</sup> published by the European Commission in 2021, AI-based systems/applications must preserve and promote:</p> <ul style="list-style-type: none"> <li>• respect for human agency</li> <li>• privacy, personal data protection and data governance</li> <li>• fairness</li> <li>• individual, social, and environmental well-being</li> <li>• transparency</li> </ul>
---------------------------------	---

<sup>3</sup> [https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-by-design-and-ethics-of-use-approaches-for-artificial-intelligence\\_he\\_en.pdf](https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-by-design-and-ethics-of-use-approaches-for-artificial-intelligence_he_en.pdf)

	<ul style="list-style-type: none"> <li>• accountability and oversight</li> </ul>
<b>Ownership of AI-based products</b>	refers to decision of whether to use a model built and owned by a vendor, or a model that is built and owned by the end-user. There are important considerations that influence the ownership of AI-based products such as governance, model accuracy, and asset value.
<b>Model documentation</b>	refers to pertinent, complete, and proper documentation of how AI models were selected, trained, and deployed.
<b>Track model performance</b>	refers to the techniques used to track the performance of models both on training and validation datasets to reduce the risk of the model not performing well in production.
<b>Model maintenance</b>	describes the procedures that should be followed in the post-deployment of the model. AI models tend to degrade over time, thus retraining the model to consider new observations is a task that must be performed periodically. The process of model maintenance requires direct communication between data scientists and MLOps.

### Appendix 1: AI Management Checklist

The AI management checklist serves as a tool to inspect the procedures followed in the development of AI-based products. The following checklist describes the suggested template to analyse the correct implementation of AI-based products.

<b>Partner:</b>	<b>Conducted on (date and time):</b>	<b>Inspected by:</b>	<b>Location:</b>
<b>Context of the organization</b>			

AI for Critical Infrastructure Protection		Auditor Name: José Carlos Carrasco Jiménez Date: 05-12-2022		
Data Management and Administration		Auditor		
Question	Response	Notes	Pass/Fail	Recommendations
Please provide details about the <b>data themes</b> used.				
Please provide details about <b>data provenance</b> (i.e. origin).				
Please provide details about the <b>data acquisition</b> process.				
Please provide details about the <b>data storage</b> process (i.e. how and where is data stored).				
Please provide details about the <b>data elimination</b> process.				
Please provide details about the <b>data accessibility</b> process (visibility + interoperability + usability).*				
Please provide details about the <b>data versioning</b> process.				
Please provide details about <b>metadata</b> (e.g. time of creation, definitions, annotations, etc.) and how it has been used.				
Please provide details about <b>standards</b> for creating, sharing, and integrating data (e.g. ISO, FGDC, etc.).				
Please provide details about conversion of <b>file formats</b> .				
Please provide details about <b>data reusability</b> (e.g. data formats, etc.).				
Please provide details about <b>data sharing</b> restrictions.				
Please provide details about the <b>data security</b> process.				
Please provide details about <b>data privacy</b> and how is sensitive data handled.				
Please provide details about <b>data integrity</b> assurance.				
Please provide details about <b>Open Data</b> sources used.				
Please provide details about the <b>data validation</b> process.				
If supervised learning was performed, please provide details about the <b>data annotation</b> process.				
Please provide details about the <b>data homogenization</b> process.				
Please provide details about the <b>data fusion</b> process.				
If sythetic data was used, please provide details about the <b>synthetic data</b> generation process.				
Please provide details about the <b>data bias</b> mitigation process.				

Data Processing		Auditor		
Question	Response	Notes	Pass/Fail	Recommendations
Please provide details about <b>data curation</b> procedures.				
Please provide details about changes of <b>data types</b> (e.g. numeric, date, character).				
Please provide details about changes to the <b>number of decimal positions</b> .				
Please provide details about <b>data quality</b> controls (e.g. outlier detection).				
Please provide details about <b>missing values</b> handling (e.g. completion, interpolation, deletion, imputation, etc.).				
Please provide details about change in <b>data units</b> .				
Please provide details about change in <b>unit system</b> (e.g. imperial vs metric).				
Please provide details about the <b>data normalization</b> process.				
Please provide details about the <b>data standardization</b> process.				
Please provide details about the <b>data denoising</b> process.				
Please provide details about the <b>data labeling</b> process.				

Policy, Ethics, and Legal Issues		Auditor		
Question	Response	Notes	Pass/Fail	Recommendations
Please provide details about the compliance with the General Data Protection Regulation ( <b>GDPR</b> ) of the datasets used.				
Please provide details about the <b>ethical approach</b> used to guarantee the correct use of data to train AI models.				
Please provide details about the <b>transparent design</b> of AI technologies.				
Please provide details about the <b>trustworthiness</b> of the AI models.				
Please provide details about the <b>impact assessment</b> performed on the AI models.				
Please provide details about <b>data sovereignty</b> procedures.				
Please provide details of local <b>government principles</b> and guidelines followed in the data handling process.				

AI for Critical Infrastructure Protection		Auditor Name: José Carlos Carrasco Jiménez Date: 05-12-2022		
AI Algorithm Life Cycle		Auditor		
Question	Response	Notes	Pass/Fail	Recommendations
Please provide details about the <b>project objectives</b> .			Pass	
Please provide details about the <b>machine learning pipeline</b> used? Is it reproducible?				
Please provide an overview of the <b>data acquisition and data preparation</b> process.			Fail	
Please provide an overview of the <b>model data</b> .				
Please provide details about the <b>dimensionality reduction</b> process.				
Please provide details about the <b>feature selection</b> process.				
Please provide an overview of the <b>parameter optimization</b> process.				

Please provide details about <b>model versioning</b> system.	RSC was deployed in a Docker container through microservices that provide the version of the module being called.			
Please provide details about <b>reusable software environments</b> (e.g. conda, etc).				
Please provide details about the <b>model governance</b> (e.g. who is publishing the model and when were models deployed, why changes are made, or when were de models used in production).				
Please provide details about the <b>model monitoring</b> process (e.g. comparison of model input and output, performance metrics).				
Please provide details about the <b>model testing environments</b> used.				

AI Algorithm Selection		Auditor		
Question	Response	Notes	Pass/Fail	Recommendations
Please provide the details about <b>problem categorization</b> .				
Please provide details about the process for identifying <b>applicable algorithms</b> .				
Please provide details about the data and <b>AI algorithm selection</b> .				
Did you use <b>supervised learning</b> ? Please provide details about the algorithm and labeled dataset.				
Did you use <b>unsupervised learning</b> ? Please provide details about the algorithm used.				
Did you use <b>transfer learning</b> ? Please provide details.				
Did you use <b>reinforcement learning</b> ? Please provide details.				
Did you use <b>deep learning</b> ? Please provide details about the algorithm and architecture used.				

AI Algorithm Tuning		Auditor		
Question	Response	Notes	Pass/Fail	Recommendations
Did you perform <b>hyperparameter optimization</b> ? Please provide details.				
Did you perform <b>ensemble learning</b> ? Please provide details.				
Did you use <b>active learning</b> paradigm? Please provide details.				
Did you do <b>federated learning</b> ? Please provide details.				

AI for Critical Infrastructure Protection		Auditor Name: José Carlos Carrasco Jiménez Date: 05-12-2022		
Evaluation of AI Algorithms		Auditor		
Question	Response	Notes	Pass/Fail	Recommendations
Please provide details about the metrics used to measure the <b>model performance</b> (e.g. precision, accuracy, F1, etc.).			Pass	
Did you train a <b>baseline model</b> ? Did you compare your model with the baseline model? Please provide details.				
Did you test for <b>complexity</b> ? Please provide details.				
Did you record the <b>times to build, train, and test</b> ? Please provide details.			Fail	
Did you record the <b>execution time</b> (i.e. time to make predictions or inferences)? Was execution time within reasonable time? Please provide details.				



Did you test for <b>robustness</b> ? Did you add noise and tested your algorithm to test for robustness? Please provide details.				
Did you test for <b>transparency</b> ? Please provide details.				
Did you test for <b>explainability</b> ? Please provide details.				
Did you test for <b>interpretability</b> ? Please provide details.				
Did you test for <b>scalability</b> ? Please provide details.				
Did you test for <b>reliability</b> ? Please provide details.				

Evaluation of AI-based products		Auditor		
Question	Response	Notes	Pass/Fail	Recommendations
Please provide details about the <b>ethical use</b> of AI models.				
Please provide details about <b>ownership</b> of AI-based products.				
Did you prepare <b>model documentation</b> . Please provide details.				
Did you <b>track model performance</b> when the model was deployed in production environments? Please provide details.				
Please provide details about the <b>model maintenance</b> procedures (e.g. is your AI model retrained? How often?).				
Please provide details about the <b>deployment</b> of AI models.				

## Appendix 2: AI Management Report

The AI management report template is an example of how the concluding remarks from the auditor could look like. The audit report includes information about the results of the inspection of AI-based products, the client, location, and date. It also highlights failed items that should be revised, along with some notes and recommendations that can be used by the client to improve the score of the audit.

<Client> | <Date> | <Auditor>

AI Management Checklist

Complete

Inspection score	Failed items	Due date
<b>92.6%</b>	<b>6</b>	<b>21-01-2023</b>

Client
<Client>
Conducted on
<Date> <Time>
Inspected by

<Auditor>
Location
Online

Failed items 4 failed

---

Data | Data Management and Administration

Please provide details about the data versioning process.	Fail
Notes	
Recommendations	

Please provide details about the data versioning process.	Fail
Notes	
Recommendations	

Please provide details about the data versioning process.	Fail
Notes	
Recommendations	

Audit 92.6%

---

Data | Data Management and Administration

Please provide details about the data themes used.	Pass

...

Data | Data Processing

Please provide details about data curation procedures.	Pass

...

Data | Policy, Ethics, and Legal Issues

Please provide details about the compliance with the General Data Protection Regulation (GDPR) of the datasets used.	Pass
--	------


Modelling | AI Algorithm Life Cycle

Please provide details about the project objectives.	Pass

...

Modelling | AI Algorithm Selection

Please provide the details about problem categorization.	Pass

...

Modelling | AI Algorithm Tunning

Please provide the details about problem categorization.	Pass
--	------


...

Evaluation | Evaluation of AI Algorithms

Please provide details about the metrics used to measure the model performance (e.g. precision, accuracy, F1, etc.).	Pass

...

Evaluation | Evaluation of AI-based products

Please provide details about the ethical use of AI models.	Pass

...

Recommendations	
Inspector's full name and signature	Date