PRECINCT

Preparedness and Resilience Enforcement for Critical INfrastructure Cascading Cyber-Physical Threats

D6.1 PRECINCT CyberPhysical Security Stakeholder Needs Knowledge Base - Liaison and cooperation

Document Summary Information

Grant Agreement No	101021668	**Acronym**	PRECINCT
Full Title	Preparedness and Resilience Enforcement for Critical Infrastructure Cascading Cyber-Physical Threats		
Project URL	https://www.precinct.info		
Start Date	01:10:21	**Duration**	24 months
Deliverable	D6.1	**Work Package**	WP6
Contractual due date	30:09:23	**Actual submission date**	26:09:23
Nature	Report	**Dissemination Level**	Public
Lead Beneficiary	European Organisation for Security (EOS)		
Responsible Author	Vincent Perez de Leon-Huet (EOS)		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 101021668

Disclaimer

Copyright

Contributors

Name	Name (organisation)
Vincent Perez de Leon-Huet	European Organisation for Security (EOS)
Cristina Pedrini	European Organisation for Security (EOS)
Jenny Rainbird	Inlecom Commercial Pathways (ICP)
Luca Simone	The Institute for Transport and Logistics (ITL)
Shirley Delannoy	VIAS Institute (VIAS)

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

Date	Role	Name (organisation)
2.08.2023	Peer Review	Denis Čaleta (ICS)
28.08.2023	Quality Assurance Review	Mark Miller/Victoria Menezes Miller (CPT)
29.08.2023	Quality Manager	Mark Miller (CPT)
01.09.2023	Internal Peer Reviewer	Eleni Maria Kalogeraki (AIA)
25.09.2023	Final Quality Review	Mark Miller/Victoria Menezes Miller (CPT)
26.09.2023	Final PM Review	Jenny Rainbird (ICP)

Revision history

Version	Issue Date	% Complete	Changes	Contributor(s)
V0.0	26-06-2023	5%	Table of Contents	Vincent Perez de Leon-Huet (EOS)
V1.0	12-07-2023	80%	Content to all sections added.	Vincent Perez de Leon-Huet (EOS)
V1.1	24-07-2023	90%	Content to stakeholder identification added.	Cristina Pedrini (EOS)
V1.2	01-08-2023	91%	Corrections and Comments added for implementation	Jenny Rainbird (ICP)
V2	17-08-2023	92%	Corrections and comments from SAB implemented	Vincent Perez de Leon-Huet (EOS)
V3	30-08-2023	99%	Corrections and comments from peer review implemented	Vincent Perez de Leon-Huet (EOS)
V4	07-09-2023	99%	Corrections and comments from peer review implemented	Vincent Perez de Leon-Huet (EOS)
V5	25-09-2023	100%	Final Content added to Section 4.4 regarding the final event	Vincent Perez de Leon-Huet (EOS)

Table of Contents

List of Figures

List of Tables

Glossary of terms and abbreviations used

Abbreviation / Term	Description
CEN-CENELEC	The European Committee for Standardization - the European Committee for Electrotechnical Standardization
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
EU	European Union
ECSCI	European Cluster for Securing Critical Infrastructure
GA	Grant Agreement
KPI	Key Performance Indicator
SEW	Stakeholder Engagement Workshop
LEAs	Law Enforcement Agencies
LL	Living Labs
SEW	Stakeholder Engagement Workshop
WP	Work Package

1 Executive Summary

This deliverable describes the activities carried out by the various PRECINCT partners in regards to PRECINCT's CyberPhysical Security Stakeholder Needs Knowledge Base, as well as all liaison and cooperation activities undertaken throughout the project.

The report starts by describing the context of PRECINCTs Stakeholder Landscape, followed by the activities that PRECINCT partners undertook to engage with said stakeholders and provide them with knowledge created within the project. Additionally, the forums in which this knowledge is hosted, also known as. the Stakeholder Needs Knowledge Base, is described in full detail.

The complementary actions of liaison and cooperation activities which furthered the outreach of PRECINCT are also outlined. Eventually, the deliverable concludes by assessing whether its goals were reached. In this case, the assessment determined that PRECINCT met its objective of sharing the project findings to a large group of relevant Critical Infrastructure (CI) stakeholders across the EU.

2 Introduction

Stakeholders play a vital role in research projects as they help to define the user needs, validate results, and in many cases they are the end-users of the developed solution developed, among other things. In order to maximise the impact of PRECINCT towards its stakeholders and vice versa, the project worked on developing a Stakeholder Needs Knowledge Base, which allows stakeholders to learn and benefit from the knowledge created by the project. Over the course of two years, PRECINCT partners undertook many outreach activities, as well, to interact with industry CI stakeholders, through organizing its own events, attending external events, publishing various materials and more in order to create the Stakeholder Needs Knowledge Base. The current deliverable aims to outline these activities, describe the Stakeholder Needs Knowledge Base for stakeholders and define the project's stakeholders. In addition, the document describes the liaison and cooperation activities of PRECINCT throughout the project's lifespan, which complimented the stakeholder activities and boosted the outreach of the project.

2.1 Mapping PRECINCT Outputs

This section aims at mapping PRECINCT's Grant Agreement (GA) commitments, both within the formal Deliverable and respective Task description, against the project's outputs and work performed.

Table 1 : Adherence to PRECINCT's GA, Deliverables and Task descriptions

PRECINCT GA Component Title	PRECINCT GA Component Outline	Respective Document Chapter(s)	Justification
DELIVERABLE			
D6.1	PRECINCT Cyber-Physical Security Stakeholder Needs Knowledge Base - Liaison and cooperation (R, PU, M24) (EOS) Stakeholder workshops, Collaboration meetings and commercial event report.	*Chapter 4; Chapter 5; Chapter 6*	These chapters report the activities undertaken during the PRECINCT events and discuss the Stakeholder Needs Knowledge Base

TASKS			
T6.1 PRECINCT Cyber-Physical Security Stakeholder Needs Knowledge Base - Liaison and cooperation	This task will guide PRECINCT's awareness events, knowledge base and open access library with the central goal of sharing the project findings to a large and relevant CI stakeholders across EU.	*Chapter 4;* *Chapter 5;* *Chapter 6*	
	Our aim is to consolidate and present the main outputs of PRECINCT and to ensure a strong interaction with industry CI stakeholders, end-users, citizens, solutions providers, and broad CI academia interest groups.	*Chapter 3;* *Chapter 4;* *Chapter 5*	
	Two prominent stakeholder workshops will be organised in Brussels in M7, M14.	*Chapter 4*	
	Clustering activities with other relevant EU CI projects to ensure synergies will is also planned.	*Chapter 5*	
	This task will also take care of the organization of a commercial event (final event of the project) where all open tools and assets will be presented to a broad CI audience at M24.	*Chapter 4*	

2.2 Document Overview and Report Structure

As mentioned above, the document reports all actions and activities carried out during the course of the PRECINCT project undertaken in its Task 6.1 – "CyberPhysical Security Stakeholder Needs Knowledge Base, Liaison and cooperation". In addition, an assessment for each activity is conducted to determine whether the actions were sufficient in reaching the goals or objectives outlined in the GA. The document is structured as follows:

- Chapter 3 defines the PRECINCT stakeholders, and the PRECINCT stakeholder landscape. In addition, it describes how PRECINCT identified and chose the stakeholders invited to events, demos, and sent dissemination materials.

- Chapter 4 covers the 4 PRECINCT-led events that were part of the core of T6.1. After describing each event and their objectives, it is further assessed if the events were successful, not only in execution but also in furthering the Stakeholder Needs Knowledge Base and liaison and cooperation tasks.

- Chapter 5 covers the liaison and cooperation tasks under the project.

- Chapter 6 discusses the actual output of T6.1, i.e., the knowledge base itself. The knowledge base consists of three parts. The section describes each of the three parts respectively. Afterwards, a general assessment of the knowledge base is conducted and presented.

- Finally, Chapter 7 concludes the document with some observations regarding the overall assessment of the task and lessons learned.

3 PRECINCT Stakeholder Landscape

The PRECINCT stakeholders are simply defined as the entities/parties that could or will be affected by the work of the PRECINCT project and are or could be interested in the outcome of the project. They were first identified in the early stages of the project. The stakeholders were depicted in the GA, as seen in the figure below, and constitute First Responders, Critical Infrastructure Operators, Industry & Technology Providers, Standardization Bodies, Policy & Decision-makers, Academia & Research and other relevant networks and Citizens.

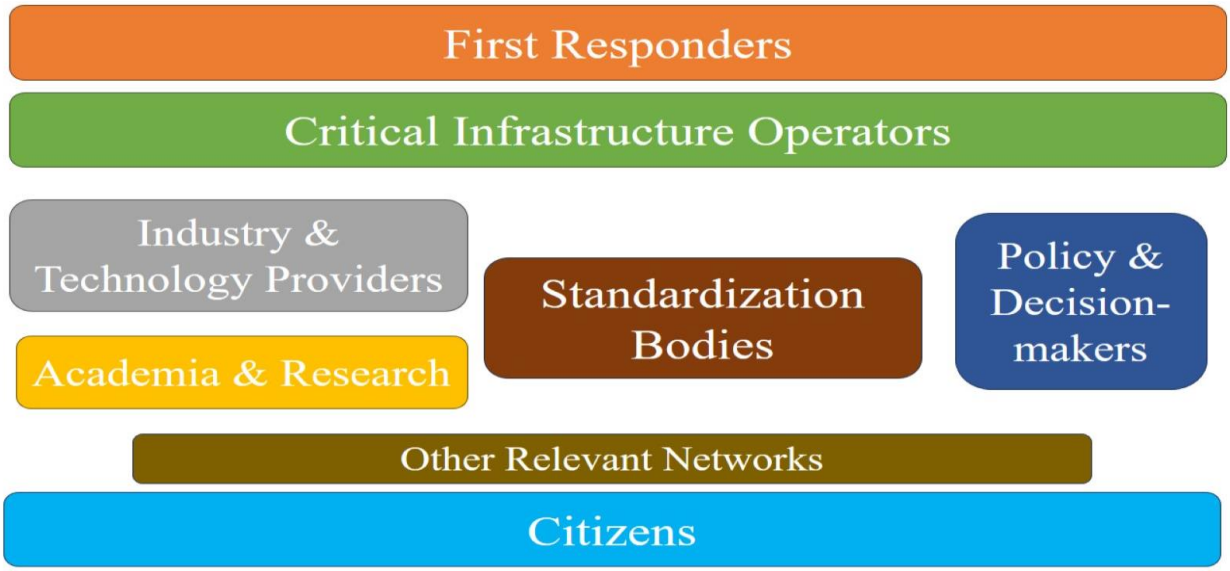


Figure 3-1: PRECINCT Stakeholders

First responders are identified as one of the key stakeholders for the PRECINCT ecosystem due to the role they play as the initial actors in the event of a CI failure. By inviting them to stakeholder workshops and identifying their needs and collecting feedback on tools (e.g., cyber-physical security management platform), PRECINCT Partners could ensure the tools were relevant and increase the chance of successful uptake. To further enhance PRECINCT's impact and relevance, it was important to engage with stakeholders at all levels; therefore, there were first responders targeted at the local level, national level, and European level. The same approach followed for all stakeholder groups as well. **Critical Infrastructure Operators** are vitally important to the PRECINCT project, considered as the end-users of the technologies provided by PRECINCT and will benefit by early identification of potential cascading effects among different infrastructures. Since there are mostly national Critical Infrastructure Operators, they represent the main entities targeted by PRECINCT. Nevertheless, whenever possible, local level entities were also contacted together with European associations that represented the CI Operators. **Industry & technology providers** and **Academia & Research** as stakeholders worked together with the PRECINCT partners to further develop the technological aspects of the project (e.g., modelling simulation), communicate their needs and feedback at PRECINCT events, and maximise exploitation. **Policy makers, decision makers and Standards Developing Organisations** would mainly be concerned with the policy recommendations and standardization tasks in the PRECINCT project, benefitting from recommendations representing an actual picture of the potential cascading effects and how to minimise their occurrence and damages through policy changes and standardization opportunities. In addition, these stakeholders were heavily engaged in both PRECINCT and non-PRECINCT events. The high level of concern for this stakeholder group is European, as the European Union (EU) lays out the framework for national entities to then implement in terms of Critical Infrastructure Protection (CIP), and the competent standardization bodies in Europe are the European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (CENELEC). **Other Relevant Networks** were expected to be directly impacted by the project activities and results; nonetheless, as main targets of the liaison and cooperation activities, they were beneficial to PRECINCT in terms of expanding relationships with related

associations and stakeholders. Finally, **Citizens**, identified as stakeholders, they directly benefit from an increased protection of CI. However, the technical and restrictive nature of the project indicated that they could not be engaged in a meaningful way and were not the focus of the activities carried out over the course of the project.

Overall, PRECINCT touches a wide variety of stakeholders at different levels of governance. Below is a representation of the stakeholders PRECINCT targets classified by relevance and at which levels. Based on this classification, stakeholders were identified and then contacted by PRECINCT partners.

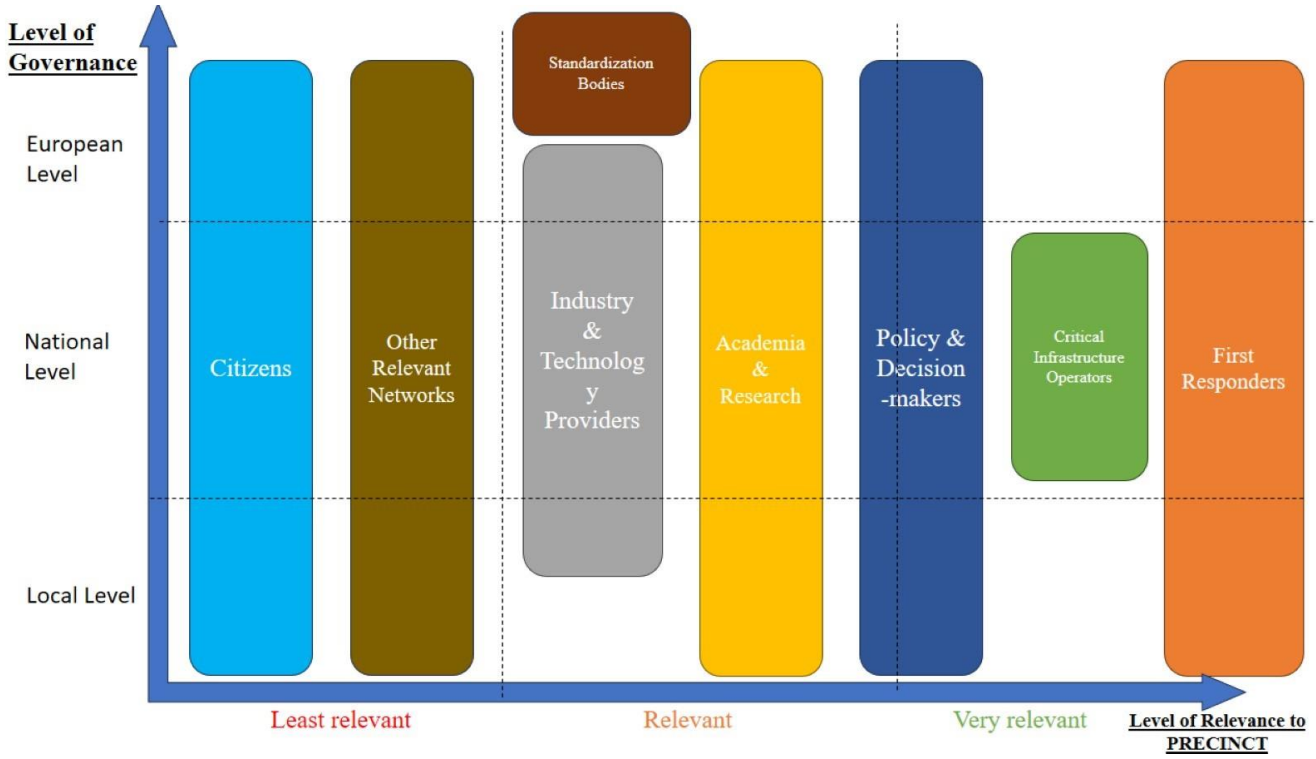


Figure 3-2: PRECINCT Stakeholders by level and relevance

3.1 Methodology for Selecting Stakeholders

The methodology for selecting stakeholders was quite simple, yet effective. Based on the categories described in the GA, EOS conducted desk research to identify stakeholders that would fit in the categories on the levels relevant to the PRECINCT project, as shown figure 3.2. Once the stakeholders were selected, they were enlisted in a file with contacts to be invited to the PRECINCT events. In addition, networks of PRECINCT partners, including stakeholders, were exploited for PRECINCT activities. For instance, EOS, shared the PRECINCT project invitations and information with its members highly interested in cyber-physical security. POLIS used its large network of municipalities to further disseminate the project results. UITP leveraged its network of public transport entities to discuss the PRECINCT project in the context of protecting public transport in the PRECINCT Conference and the UITP Global Public Transport Summit. Finally, stakeholders who signed letters of support and directly shared project results, such as the Emilia-Romagna region and the city and commune of Bologna, are also included in the list below.

3.2 Identification of Relevant Stakeholders[1]

Section 3.2 will list the stakeholders that were identified by PRECINCT partners via its stakeholder mapping exercise, as well as any other stakeholders identified afterwards by various partners.

3.2.1 First Responders

Table 3-1: List of First Responder Stakeholders

Name of Stakeholder	Country	Level
DG European Commission Humanitarian Aid & Civil Protection (ECHO)	Belgium	European/International
Police Federale/Federale Politie	Belgium	National
Les sapeurs-pompiers de Belgique	Belgium	National
Les secours médicaux, sanitaires et psychosociaux	Belgium	National
La Protection Civile	Belgium	National
Carabinieri	Italy	National
Polizia di Stato	Italy	National
Corpo Nazionale dei Vigili del Fuoco	Italy	National
Protezione Civile	Italy	National
Police nationale	France	National
Gendarmerie nationale	France	National
Brigade des sapeurs-pompiers de Paris	France	Local
Bataillon de marins-pompiers de Marseille	France	Local
Fédération nationale de protection civile	France	National
Policía Nacional	Spain	National
Bomberos de Barcelona	Spain	Local
Cuerpo de bomberos de la Comunidad de Madrid	Spain	Local
Bomberos de la Generalidad de Cataluña	Spain	Local
Cuerpo de Bomberos de Las Palmas de Gran Canaria	Spain	Local
Protección Civil	Spain	National
Bundespolizei	Germany	National
Bundeskriminalamt	Germany	National
Feuerwehr	Germany	National
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe	Germany	National
Korps Nationale Politie	Netherlands	National
Koninklijke Marechaussee	Netherlands	National
Brandweer Nederland	Netherlands	National
Hellenic Police - Ελληνική Αστυνομία	Greece	National
Hellenic Fire Service - Πυροσβεστικό Σώμα	Greece	National
Policja	Poland	National
Państwowa Straż Pożarna	Poland	National
Guarda Nacional Republicana	Portugal	National

[1] Citizens were omitted from identification, as this is a cross-cutting and large group and any attempt at identification could pose privacy issues.

Name of Stakeholder	Country	Level
Polícia de Segurança Pública	Portugal	National
Bombeiros de Portugal	Portugal	National
Autoridade Nacional de Emergência e Proteção Cívil	Portugal	National
Poliția Română	Romania	National
Jandarmeria Română	Romania	National
Inspectoratul General pentru Situaţii de Urgenţă - IGSU	Romania	National
Rendőrség	Hungary	National
Tűzoltóság	Hungary	National
Polgári védelem	Hungary	National
Bundespolizei	Austria	National
Landesfeuerwehrverband Oberösterreich	Austria	Local
Landesfeuerwehrverband Salzburg	Austria	Local
Landesfeuerwehrverband Tirol	Austria	Local
Politsei- ja Piirivalveamet	Estonia	National
GIGN	France	National
Emergency Response Coordination Centre	EU	European/International
Slovenian Police	Slovenia	National
Fire Brigade Ljubljana	Slovenia	Local
Municipality Police Ljubljana	Slovenia	Local

3.2.2 Critical Infrastructure Operators

Table 3-2: List of Critical Infrastructure Operators Stakeholders

Name of Stakeholder	Country	Level
Group ADP	France	National
Avinor	Norway	National
STIB/MVIB	Belgium	Local
DeLijn	Belgium	Local
RATP	France	Local
Transports Metropolitans de Barcelona	Spain	Local
Empresa Municipal de Transportes de Madrid	Spain	Local
Deutsche Bahn	Germany	National
SNCB	Belgium	National
SNCF	France	National
Irish Water	Ireland	National
ACCIONA	Spain	National
FN Motol	Czechia	National
The Fondazione Policlinico Universitario Agostino Gemelli	Italy	National
Hôpitaux universitaires de Genève - HUG	Switzerland	National
Universitätsklinikum Freiburg	Germany	National

Name of Stakeholder	Country	Level
University Medical Center Ljubljana	Slovenia	National
UZ Leuven Gasthuisberg Campus	Belgium	National
Heidelberg University Hospital	Germany	National
Oslo University Hospital	Norway	National
Clinic Klagenfurt am Woerthersee	Austria	National
Universitätsklinikum Essen	Germany	National
Hospital General Universitario Gregorio Marañón	Spain	National
L'HÔPITAL UNIVERSITAIRE PITIÉ SALPÊTRIÈRE	France	National
Academisch Medisch Centrum	Netherlands	National
General Hospital Ioanninon Chatzikosta	Greece	National
ING	Netherlands	International
AXA	France	International
Allianz	Germany	International
BNP Paribas	France	International
Santander	Spain	International
Assicurazioni Generali	Italy	International
HSBC	United Kingdom	International
Crédit Agricole Group	France	International
Munich RE	Germany	International
Zurich Insurance Group	Switzerland	International
Dexia	Belgium	National
Nordea	Finland	International
KBC Group	Belgium	International
Deutsche Bank	Germany	International
Barclays	United Kingdom	International
Osterreichs Energie	Austria	National
Febeg	Belgium	National
Electric Authority of Cyprus	Cyprus	National
Czech Association of Energy Sector Employers	Czechia	National
Green Power Denmark	Denmark	National
Eesti Elektritoostuse Liit	Estonia	National
Finnish Energy	Finland	National
Union Francaise de l'electricite	France	National
BDEW	Germany	National
Public Power Corporation of Greece	Greece	National
Samorka	Iceland	National
Electricity Association of Ireland	Ireland	National
Elettricita Futura	Italy	National
LEEA	Latvia	National
Nacionaline Lietuvos Energetikos Asociacija	Lithuania	National
LuxEnergie	Luxembourg	National
LeoEnergie	Luxembourg	National

Name of Stakeholder	Country	Level
Enemalta	Malta	National
Energie Nederland	Netherlands	National
Netbeheer Nederland	Netherlands	National
Energi Norge	Norway	National
Polish Electricity Association	Poland	National
Elecpor	Portugal	National
Institutul Național Român pentru Studiul Amenajării și Folosirii Surselor de Energie	Romania	National
Zväz zamestnávateľov energetiky Slovenska	Slovakia	National
EZS	Slovenia	National
Aelec	Spain	National
Energiföretagen	Sweden	National
AES	Switzerland	National
Turkiyte Elektrik Sanayi Birligi	Turkey	National
Energy Networks Association	United Kingdom/Ireland	International
EnergyUK	United Kingdom	National
Association Francaise du Gaz	France	National
Federaţia Asociaţiilor Companiilor de Utilităţi din Energie	Romania	National
CEPSA	Spain	National
Cheniere	United Kingdom	National
Deutsche Telekom	Germany	International
Vodafone Group	United Kingdom	International
Orange SA	France	International
Telefonica SA	Spain	International
Bouygues	France	International
Centre de Crise National	Belgium	National
Agence nationale de la sécurité des systèmes d'information	France	National
Secretariat General de la Defense et de le Securite Nationale	France	National
ELES	Slovenian	National

3.2.3 Policy & Decision-Makers

Table 3-3: List of Policy & Decision-Makers Stakeholders

Name of Stakeholder	Country	Level
SPF Mobilitée et Transports	Belgium	National
Stockholm International Water Institute (SIWI)	Sweden	National
Siseministeerium	Estonia	National
Ministère de l'Intérieur et des Outre-mer	France	National
The Ministry of Transport and Communications of Finland	Finland	National
Ministero del Interno	Italy	National
DG Justice & Home Affairs (HOME)	Belgium	European/International

Name of Stakeholder	Country	Level
DG Mobility & Transport (MOVE)	Belgium	European/International
DG European Commission Humanitarian Aid & Civil Protection (ECHO)	Belgium	European/International
Ministry for Infrastructure	Slovenia	National
Ministry for Citizen Protection	Greece	National
Agenzia per la Cybersicurezza Nazionale	Italy	National
SPF Interieur	Belgium	National
Emilia-Romagna Region	Italy	Local
Bologna Municipality (Comune di Bologna)	Italy	Local
Metropolitan City of Bologna	Italy	Local
SRM – Reti e Mobilità S.r.l.	Italy	Local
Antwerp city authorities	Belgium	Local
Swedish Civil Contingencies Agency	Sweden	National
ENISA	EU	European/International
Agenzia per la Cybersicurezza Nazionale	Italy	National
Ministry for Energy	Slovenia	National

3.2.4 Academia & Research

Table 3-4: List of Academia & Research Stakeholders

Name of Stakeholder	Country	Level
Federal Highway Research Institute	Germany	National
IHE-HELP Centre at the University of Dundee	Scotland	National
SINTEF	Norway	National
IWW Water Centre	Germany	National
WiCE	Germany	National
EIP (European Innovation Partnership) Water	Belgium	International
Allied Waters	Netherlands	International
Water and Energy Intelligence	Netherlands	National
WETSUS	Netherlands	National
Universita Cattolica del Sacre Cuore	Italy	National
Energy Management Institute	Bulgaria	National
FREE ICT EUROPE (FIE)	Netherlands	International
The European Gas Research Group	Belgium	International
EU-HYBNET	N/A	International
PRAETORIAN	N/A	International
7SHIELD	N/A	International
STRATEGY	N/A	International
Institute Jozef Stefan	Slovenia	National
The Forum of European Road Safety Research Institutes (FERSI)	N/A	International
Securegas	N/A	International
INFRARISK (ended 2016)	N/A	International
IMPROVER (ended 2018)	N/A	International
SAURON (ended 2020)	N/A	International
DEFENDER (ended 2020)	N/A	International
SmartResilience (2019)	N/A	International

Name of Stakeholder	Country	Level
CyberSANE	N/A	International
CyberSEAS	N/A	International
FINSEC (ended 2021)	N/A	International
ATENA (ended 2019)	N/A	International
Snowball (ended 2017)	N/A	International
LISA institute	N/A	International
GEA College	Slovenia	National
Faculty for Security Studies	Slovenia	National
Faculty for Governmental and European Studies	Slovenia	National

3.2.5 Industry & Technology Providers

Table 3-5: List of Industry & Technology Providers Stakeholders

Name of Stakeholder	Country	Level
ACI Europe	Belgium	European/International
Aquarius IT LTD.	United Kingdom	National
Aigües de Barcelona	Spain	National
De Watergroep	Belgium	National
Hessenwasser	Germany	National
Xylem Vue	US/EU	International
SUEZ en France	France	National
ACQUAINT	Netherlands	National
Czech Gas Association	Czechia	National
DCBrain	France	National
INOV	Portugal	National
Internet Society (ISOC)	Switzerland	International
ORGALIM	Belgium	International
Eurelectric	Belgium	International
Eurogas	Belgium	International
ENTSO-E	Belgium	International
SNEP	Slovenia	National
AQUA Consultancy	Netherlands	International
BUSINESSEUROPE	Belgium	International
DIGITALEUROPE	Belgium	International
EUROSMART	Belgium	International
OpenForum Europe AISBL	Belgium	International
Water Europe	Belgium	International
ISKRA	Slovenia	National
INFORMATIKA	Slovenia	National

3.2.6 Standardisation Bodies

Table 3-6: List of Standardisation Bodies Stakeholders

Name of Stakeholder	Country	Level
CEN	Belgium	European/ International
CENELEC	Belgium	European/ International

Name of Stakeholder	Country	Level
The Institute of Electrical and Electronics Engineers	Belgium	European/International
International Electrotechnical Commission	Switzerland	National
Slovenian Institute for Standardization	Slovenia	National

3.2.7 Other Relevant Networks

Table 3-7: List of Other Relevant Network Stakeholders

Name of Stakeholder	Country	Level
ECSCI	N/A	European/ International
UIC	France	European/International
International Association of CIP Professionals	N/A	European/International
Slovenian Association for Corporate Security	Slovenia	National
European Hospital and Healthcare Federation	Belgium	European/ International

3.3 Assessment of the PRECINCT Stakeholders

PRECINCT affects a wide variety of stakeholders, as one of its main objectives is to increase critical infrastructure resilience across Europe via its tools, assets, and approach. By assessing stakeholders at various levels involved in Critical Infrastructure Protection (CIP) and/or affected by cyber-physical threats and their cascading effects, PRECINCT has managed to identify a great number of stakeholders. This allowed PRECINCT to exploit a diverse network of technical knowledge for feedback and communicate its results. In addition, it helped to improve the potential uptake of the PRECINCT tools, as a wide variety of stakeholders were identified to participate in the development process of the tools and provided suggestions to increase their usability, according to stakeholders' needs.

As outlined in the early stages of the project, the PRECINCT Stakeholder Landscape comprises First Responders and Critical Infrastructure Operators. As the primary beneficiaries of the project and potential end-users, these stakeholders were prioritized as targets of the PRECINCT events among other stakeholders. Additionally, the Other Relevant Networks were useful in identifying more relevant stakeholders, as previously established networks, such as the European Cluster for Securing Critical Infrastructures (ECSCI) cluster, brought with them stakeholders for PRECINCT to exploit.

3.4 Engagement Strategy of Stakeholders

Once the stakeholders identified, the next step was to engage them to take part in the PRECINCT project. The main forum for engaging these stakeholders was the events organized by PRECINCT, in which the main outputs of the project were presented which gave them the opportunity to provide feedback to the PRECINCT partners.

Before each event, stakeholders were either contacted directly via their email or indirectly through social media, such as Twitter and LinkedIn and invited to take part in these events. Promotional materials, such as save the dates, invitations, and agendas were sent out to encourage stakeholders to join the events either online or in-person. Additionally, reminders were sent periodically to external stakeholders regarding the event, and EOS encouraged and reminded PRECINCT partners to further share the event materials with their networks and relevant stakeholders.

4 PRECINCT-organized Events

In the scope of T6.1 "PRECINCT Cyber-Physical Security Stakeholder Needs Knowledge Base", the PRECINCT consortium organised 4 events: 2 stakeholder engagement workshops, a Conference, and a final commercial event. These events acted as the primary contact points between the PRECINCT project and its stakeholders and allowed stakeholders not only to be updated on the progress of the project, but also to provide feedback to the consortium regarding specific topics, namely the tools developed and the business exploitation, policy recommendation & standardisation, and training aspects.

4.1 1st Stakeholder Engagement Workshop

The 1st Stakeholder Engagement Workshop (SEW) was organized in Brussels on May 5th, 2022, and acted as the first PRECINCT organised event open to external participants. As the project had only started in September 2021, the first event was mainly focused on raising awareness of the project and its objectives, as well as presenting some initial findings and work. Additionally, this event was the first engagement that PRECINCT had with stakeholders. In total, the event was able to bring together 75 participants (out of 103 registered). During the event, despite the exception of a presentation conducted by the EU-HYBNET project, PRECINCT partners presented the work undertaken in each work package (WP), the WP overall objective, and the project's vision. A full recording of the workshop was uploaded to YouTube on May 25th, 2022, for stakeholders access, and the full deck of the presentations were uploaded to the Zenodo community.

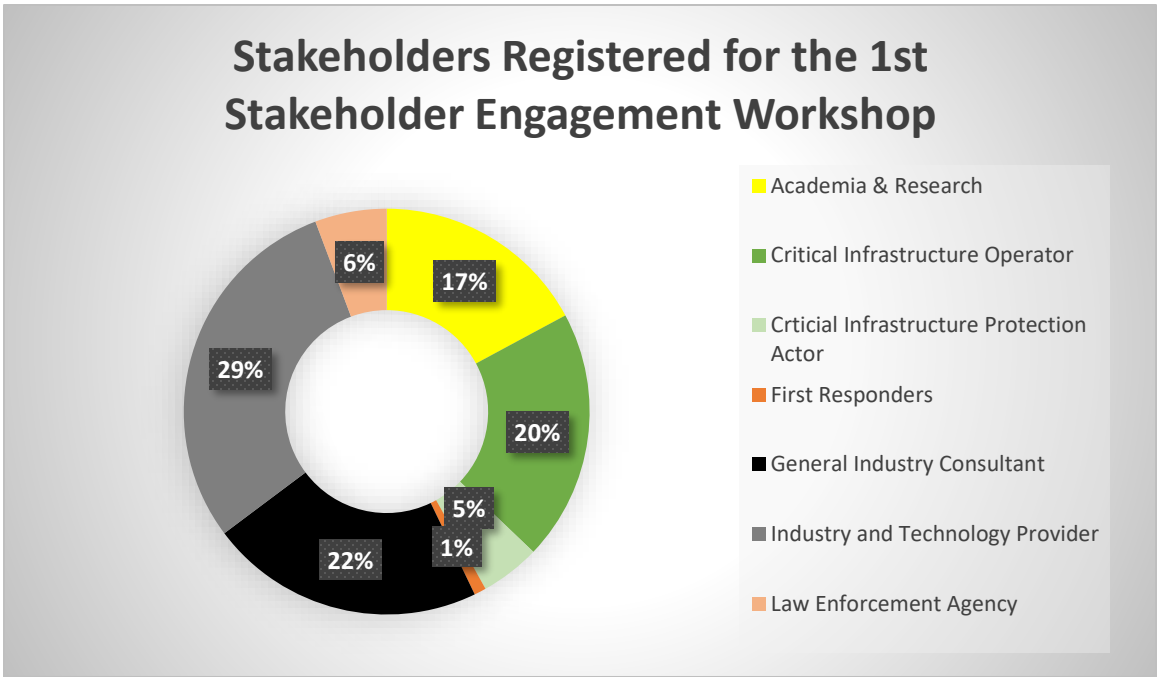


Figure 4-1: Stakeholders registered to the 1st SEW[2]

[2] The terms used for this registration form did not include PRECINCT Partners as an option, to differentiate external stakeholders. This graph includes PRECINCT partners.

Figure 4-2: Image from the 1st Stakeholder Engagement Workshop

4.1.1 Takeaways Learned

After the 1st SEW, it became clear that PRECINCT should and could reach a larger audience. Additionally, since the first event's content was mainly focused on presenting the initial work and objectives of the project tostakeholders, a more interactive approach for the next event was decided to have stakeholders more engaged. To increase the audience, and expand the liaison and cooperation activities, PRECINCT partners reached out to its sister project PRAETORIAN in order to co-organise the 2nd Stakeholder engagement workshop. This co-organisation allowed the projects to invite their stakeholder groups and increase their awareness. The partners involved also ensured that the planning of the next workshop would focus on having more interactive formats such as panels, working groups, etc. to raise stakeholders' active involvement in these engagement workshops.

4.2 2nd Stakeholder Engagement Workshop

The 2nd SEW was held 6 months after the first, in Brussels on November 22nd, 2022, and was co-organised with the PRAETORIAN project: a sister project of PRECINCT. This 2nd SEW aimed at build upon the first and bringing together the stakeholders of both projects to present how each project is approaching the same problem and update stakeholders on the PRECINCT work done since the last event. The event agenda (see section 8.2) also included working group sessions for the participants to further develop topics vital to the work of both projects (standardisation & policy recommendations and PRECINCT & PRAETORIAN training and capacity building programmes) and a general session on exploitation. The participation in this SEW increased from the last from 75 to 109, signaling a positive trend that allowed PRECINCT to further reach stakeholders.

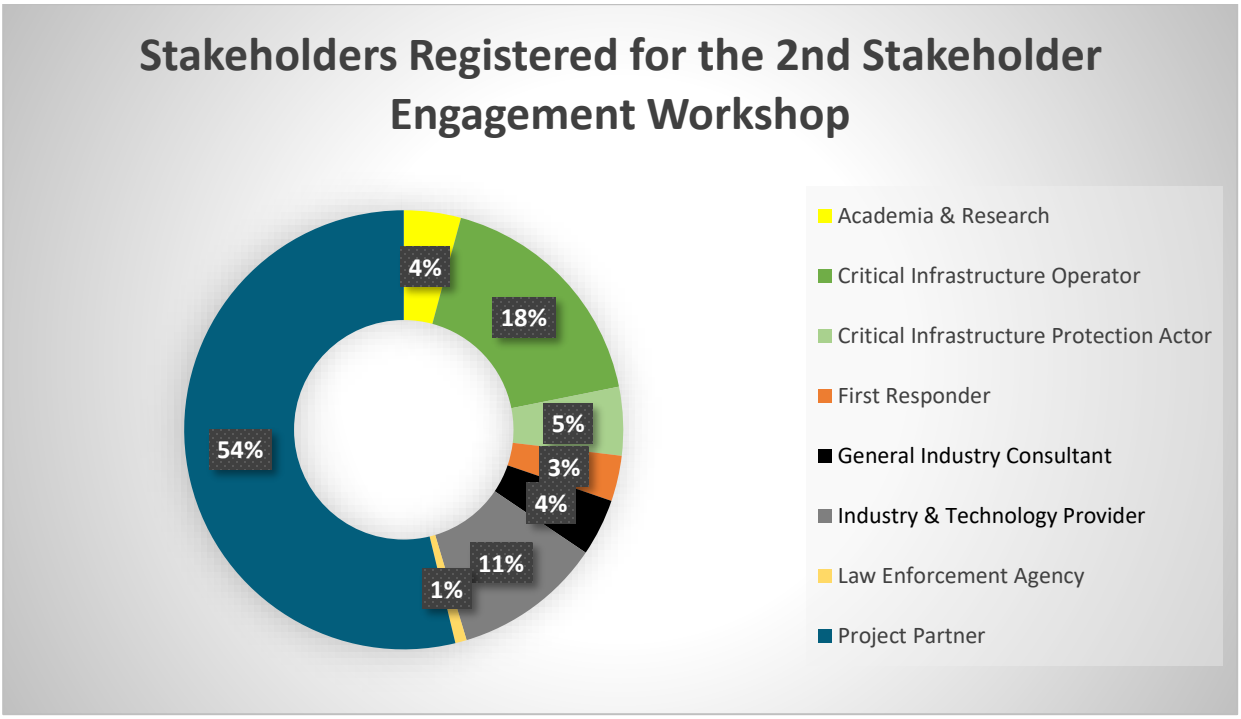


Figure 4-3: Stakeholders registered to the 2nd SEW

Figure 4-4: Image from the 2nd Stakeholder Engagement Workshop

4.2.1 Takeways Learned

The 2nd SEW demonstrated an improvement over the first, especially considering the increase in the number of participants in the workshop. Due to the ambitious Key Performance Indicator (KPI) that was attached to the PRECINCT Conference (180 participants), the goal was to continue this trend of increased participation. The success of this co-organisation paved the way not only to reach the liaison and cooperation activities outlined in the early stages of the project, but also to increase the engagement of stakeholders. Within this context, PRECINCT partners decided to continue the PRECINCT conference effort and reached out H2020/Europe projects relevant to PRECINCT and included them in the organisation process.

In terms of content, the interactive formats were kept, but the increased account of co-organising parties allowed them to organise their own parallel sessions.

4.3 PRECINCT Conference

The PRECINCT Conference took place in Brussels on May 16 and 17, 2023, and was organized with the participation of 7 other H2020 and Horizon Europe projects as follows:

- AI4CYBER
- EU-CIP
- EU-HYBNET
- PRAETORIAN
- DYNABIC
- STRATEGY
- SUNRISE.

The goal of the conference was to bring together a large audience of CI stakeholders, including researchers, industry, civil society, policy-makers, etc.. It was also the first PRECINCT organised event in the second year of the project and allowed partners to present an update of the work undertaken so far. To avoid duplication of the previous events, the Conference agenda focused on more high-level and cross-cutting issues, such as countering hybrid threats, innovation uptake and EU legislation/directives on protecting Critical Infrastructure (e.g. CER & NIS2), whereas it provided several follow-ups for some PRECINCT outputs, including the PRECINCT training and capacity building programme, the standardisation and policy recommendation activities, and the Living Labs (LLs). Moreover, some space was given to the participating projects in the form of break-out sessions or short presentations on topics related to PRECINCT. This approach provided various benefits, including a larger audience encompassing stakeholders from the other projects, a wider scope for the discussion, and an exchange of ideas and approaches. As with previous events, the PRECINCT Conference received positive feedback and a great number of registrants. At this event, there was a KPI of 180 participants, and there were 177 registrations before the event with various in-person registrations the day of. Overall, a great number of different stakeholders were involved, as depicted in figure 4.5. Even though a large portion of participants were PRECINCT partners, many other types of stakeholders took part in the event as well, such as Critical Infrastructure Operators, Academia & Research and Industry & Technology Providers.

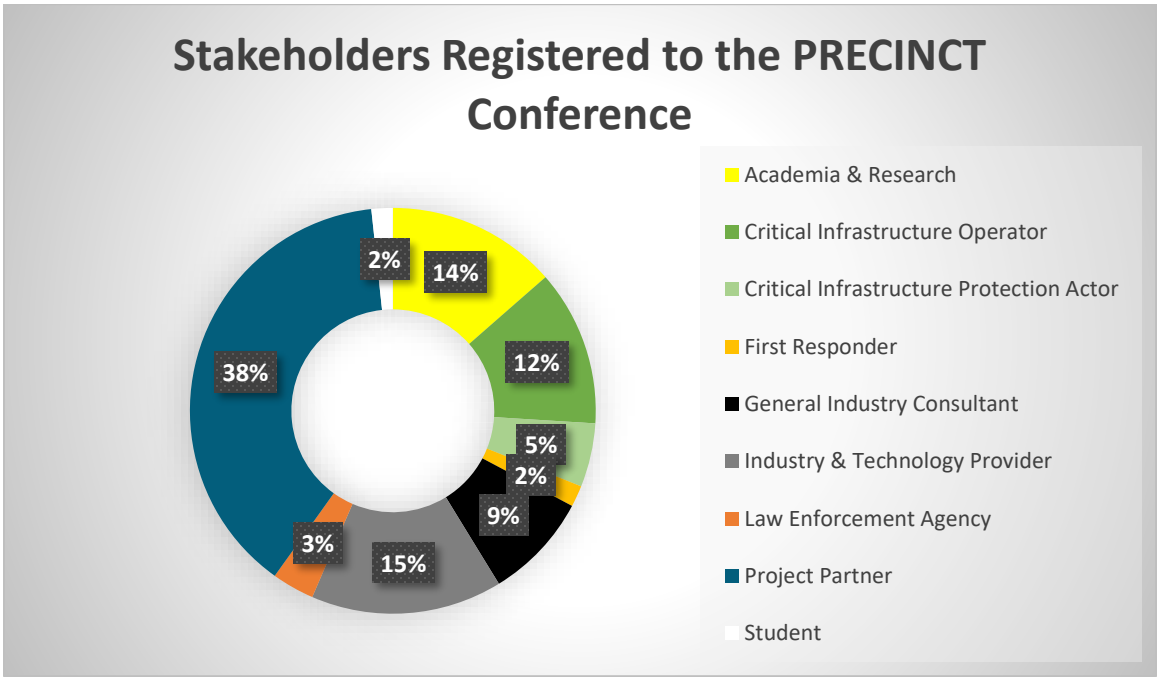


Figure 4-5: Stakeholders Registered to the PRECINCT Conference[3]

Figure 4-6: Image from the PRECINCT Conference

[3] Certain registrants selected multiple groups, only the first one selected was used

4.3.1 Takeaways Learned

The PRECINCT Conference further demonstrated the value of tying in the liaison and cooperation activities into the stakeholder events in order to increase engagement. The KPI of 180 participants was met, and the feedback received from participants at the conclusion of the event was very positive.

The more general focus of the Conference led to the discussions focusing on PRECINCT-related topics instead of only on the work of the project; therefore, for the final event, instead of inviting projects and stakeholders to be a part of the agenda, the decision was made to have them join as participants. This would allow for the Final Event to really focus on PRECINCT outputs and act as a commercial event, which is its main objective.

4.4 PRECINCT Final Event

On September 14th, 2023, the PRECINCT Final Event took place in Bologna at the headquarter of the Emilia-Romagna Region. The objective was to run a commercial event where all of the tools and assets developed within the project's lifespan were presented to a large and relevant CI stakeholder audience. 111 people participated, with around half participating online The event involved numerous partners of the PRECINCT project and some stakeholders directly involved in the project activities. The following stakeholders were present at the Final Event:

- Marconi Express (MEX) → MEX is the service provider of the connection between the airport and Bologna Centrale railway station. The people mover was central for the design of the LL4 and the tools of the PRECINCT Framework, so the CEO and the operative manager attended the Final Event to observe the project outputs;
- TPER → TPER is the urban mobility provider of numerous cities in the Emilia-Romagna region including the Metropolitan City of Bologna. TPER was also directly involved in the design of the LL4 and the Final Event was an opportunity to observe the outputs and possible future implementations within the LL4 PRECINCT Framework.
- Emilia-Romagna Region → It is the public body that deals with the management of the entire Region. The PRECINCT Final Event involved figures who deal with the management of the territory and transport within the regional territory, and who also deal with the monitoring and management of the security of the digital and physical infrastructures present in the region. For this reason, it was an opportunity of great interest to deepen the results of the PRECINCT Project.

The event received very positive feedback both during the course and at the end of the event. The aspects that were most successful were the contents presented, which retraced through the technical outputs two years of project, and the organization of the event, which allowed the presence of a large audience in presence and remotely throughout the course of the event. Overall, the PRECINCT Final Event was a special opportunity to visualize all the results obtained in two years of joint work and new synergies created, giving the opportunity to those who have not been directly involved in the project, to fully understand the objectives and results obtained by the PRECINCT Consortium.

Figure 4-7: Image from the PRECINCT Final Event

4.5 Assessment of the PRECINCT Events

The main objectives of the PRECINCT events were to consolidate and present the main outputs of PRECINCT and ensure a strong interaction with industry CI stakeholders, end-users, citizens, solutions providers, and broad CI academia interest groups. All events were organised to demonstrate to stakeholders the progress of the work undertaken duringthe project's lifespan and triggered feedback opportunities. The space between the different events allowed stakeholders to provide feedback at critical points of the project, maximising the impact they could have on the project and vice versa. Regarding the content, the feedback received about the events was always quite positive, with participants finding the content quite relevant and worth their time.

One of the main drawbacks of the PRECINCT events was the lack of consistency in the classification used for stakeholders in the registration form. The selections did not reflect the categories of stakeholders that were outlined in the Grant Agreement (GA) in a 1:1 way. Instead, Law Enforcement Agencies (LEAs) were divided into First Responders, Students from Academia and Research, and General Industry Consultants from Industry and Technology Providers, as described in a different section of the GA. This slightly affected the analysis of the present and most relevant stakeholders; nevertheless, it did not impact the project in a significant way as the main stakeholder groups were still represented (even if they were split). Additionally, this issue was rectified for the PRECINCT Final event registration form. In terms of external stakeholders, First Responders (including LEAs) covered on average 8% of participants in events, while Critical Infrastructure Operators and CIP protection actors covered on average 31% of participants. Despite not being ideal, as the targeted stakeholders did not represent the majority of stakeholders present, it is important to note that PRECINCT includes 40 partners, encompassing many First Responders and Critical Infrastructure Operators which increases the number of present targeted stakeholders within the events. In addition, the two stakeholder categories represent a great number of attendees. Eventually, it shall be noted that there was an increase in all events from stakeholders.

Overall, the PRECINCT events were quite successful, as there was a general increase in attendance for each event, and a wealth of knowledge created by the project was shared with stakeholders during the events' execution. Furthermore, the events attracted a wide range of relevant stakeholders, as shown in the previous figures' graphs, which was the main objective of these events. Additionally, these activities built a considerable part of the Stakeholder Needs Knowledge Base, as all of the events were recorded and uploaded on the PRECINCT YouTube channel. This will allow the events to continue to have an impact even after the PRECINCT project finishes.

5 Cyber-Physical Security Stakeholder Needs Knowledge Base

A main output of WP6 was to create a Stakeholder Needs Knowledge Base for stakeholders to be able to refer to after the conclusion of the PRECINCT events, and the project per se, for knowledge and outputs created by PRECINCT. There are three main repositories where stakeholders can refer to this PRECINCT knowledge: the PRECINCT website, the PRECINCT YouTube Channel, and a PRECINCT Zenodo Community. Together these make up the Stakeholder Needs Knowledge Base; however, the main knowledge base is considered the Zenodo community, as it hosts most of the PRECINCT's knowledge, including what can be found in the other two.

5.1 The PRECINCT Website

The PRECINCT website was created by VIAS in November 2021 (M3 of the project) and was the first PRECINCT knowledge repository. The website allowed for stakeholders to gain awareness about the project, learn of its objectives and stay up to date of further activities, including all of the events organised by PRECINCT.
Structured in seven sections, the website provides:

- A general presentation of the project scope and ambitions, and the milestones of the project. and the last updates.
- A presentation of the key outputs of the project and the (management) structure.
- An overview of the Consortium partners.
- A description of the four Living Labs, their scenario and CIs.
- PRECINCT publication material (videos, training session, articles, promotional material and newsletters).
- An overview of events organised by PRECINCT and third-party events and of the other projects in the European Cluster for Securing Critical Infrastructures.
- A contact form (redirecting to the project PM, ICP).

On the homepage, an insert is dedicated to the last updates of announcements about the project ("newsletter publication", "event subscription", …). VIAS is responsible of the website creation (content and layout) and the maintenance and updates. The website will be kept online minimum in the three months following the end of the project (and probably for the next three years). The website was submitted to ethics review at M3, and validated.

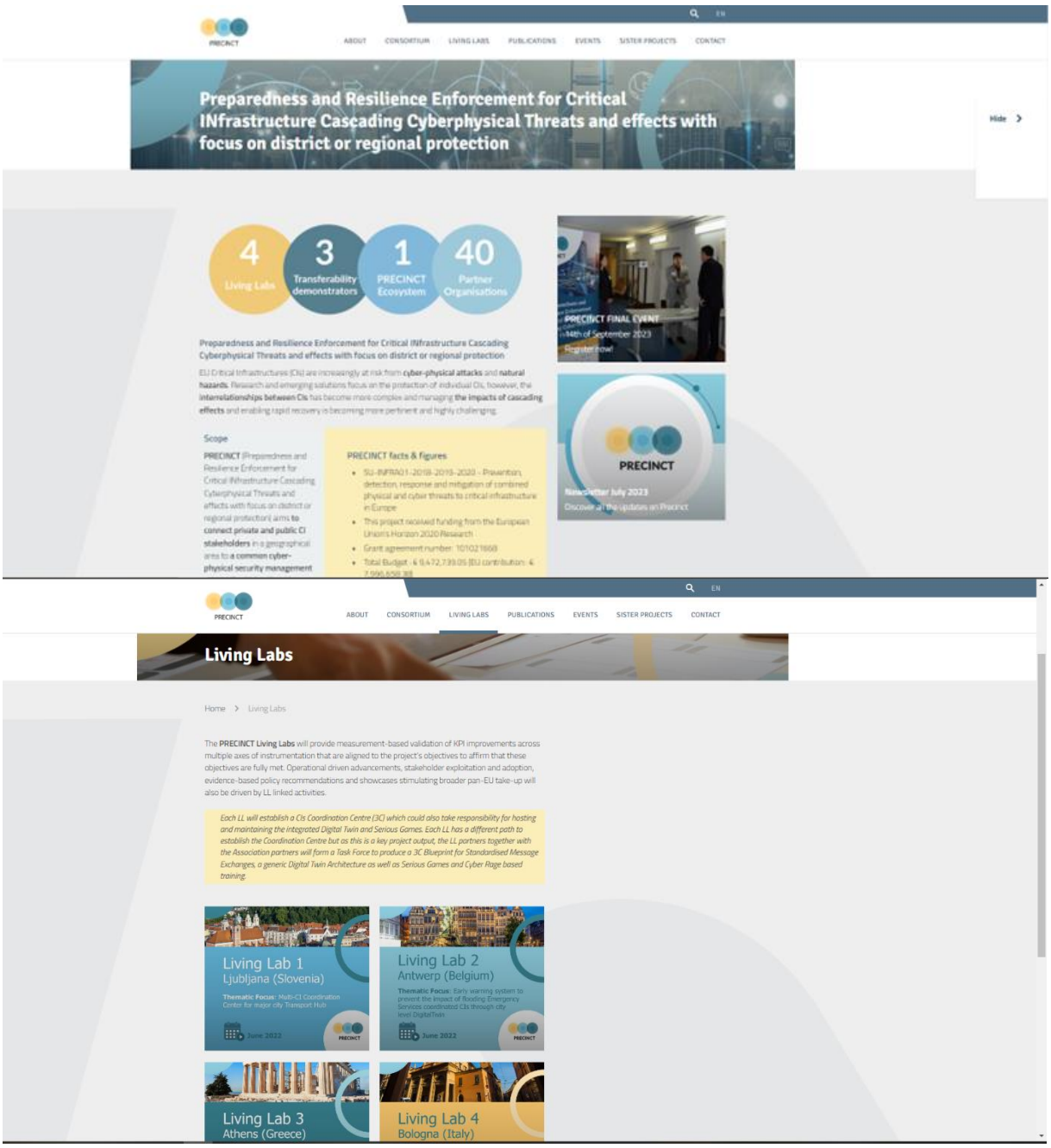


Figure 5-1: Overview of the website

5.2 The PRECINCT YouTube Channel

The PRECINCT YouTube channel was created by EOS in May 2022 following the conclusion of the 1st SEW, using the PRECINCT project email. The YouTube channel serves as a tool where stakeholders or project partners could watch or rewatch the PRECINCT workshops if they were unable to attend the workshop or missed certain parts. Following the uploading of the workshop, other videos were uploaded to the channel, such as an innovation lesson and the general project video, letting stakeholders engage with content outside of simply the PRECINCT events. At the time of writing the deliverable, PRECINCT has a total of 14 subscribers and 6 videos, with the most watched video being the 2nd SEW recording with 147 views. Below is a image from the YouTube Channel and its analytics.

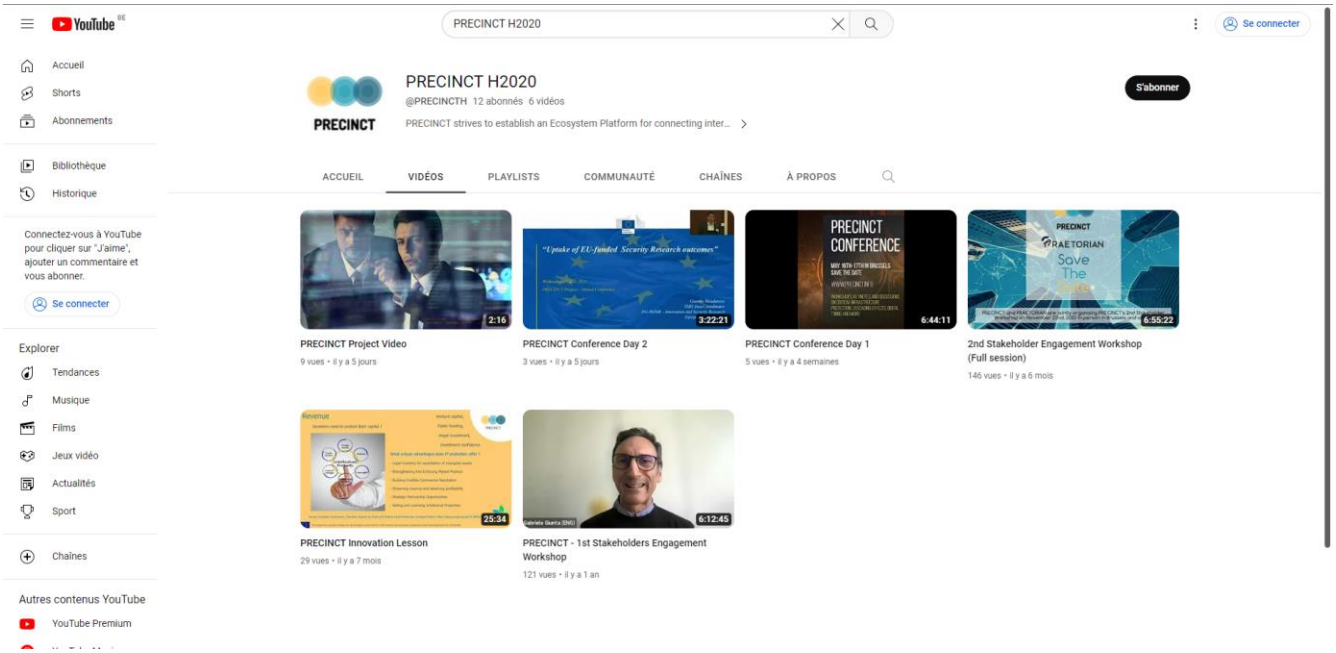


Figure 5-2: Youtube Channel Overview

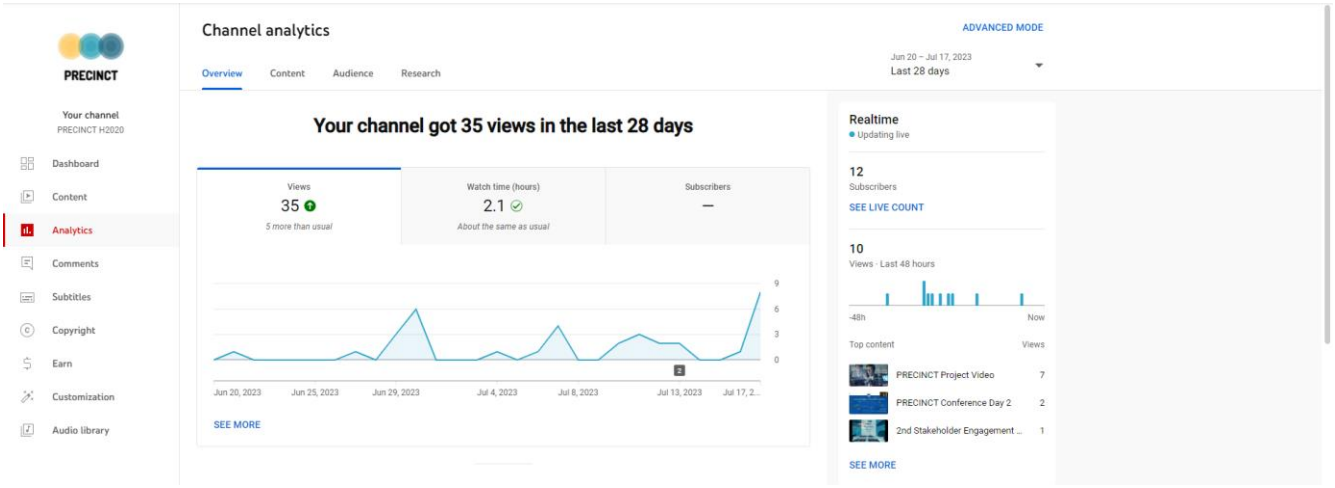


Figure 5-3: Youtube Channel Analytics

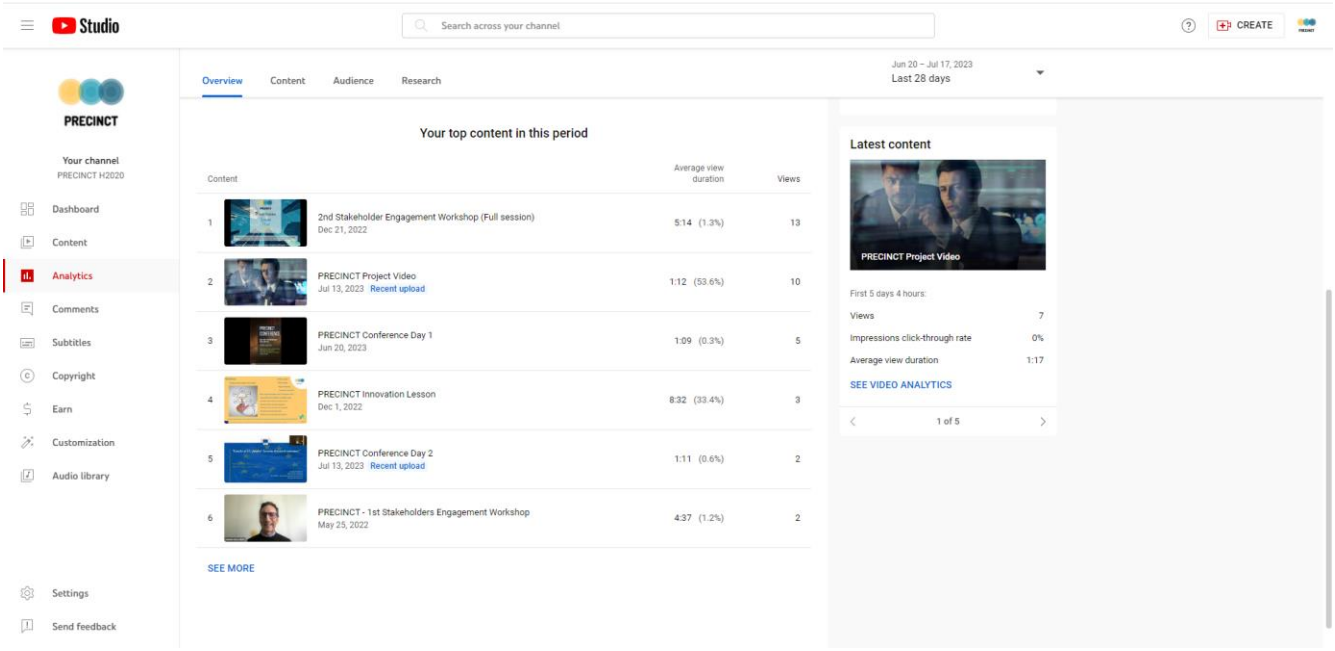


Figure 5-4: Youtube Channel Analytics (continued)

The analytics were taken from period of 20/06/2023-17/07/2023 and demonstrate that even in between periods of uploads there seems to be some level of engagement with the PRECINCT videos. Additionally, the average watch time is 2.1 hours, which indicates that viewers are spending a considerable amount of time watching the videos instead of clicking away immediately. After the conclusion of the project, the YouTube Channel will remain open for stakeholders to come back to rewatch the PRECINCT events and the innovation lesson to refresh themselves whenever needed, as there is no upkeep needed to maintain the channel.

5.3 The PRECINCT Zenodo Community

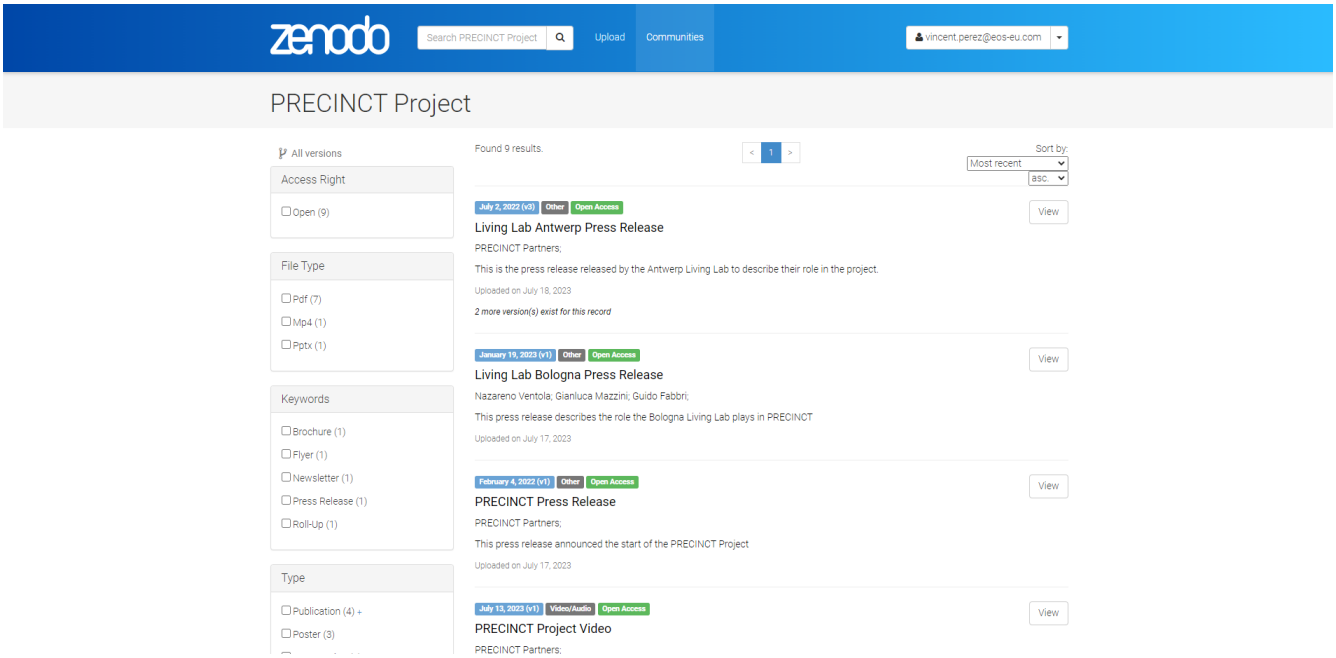


Figure 5-5: Overview of the Zenodo Community

Zenodo is a general-purpose open repository developed under the European OpenAIRE program and operated by CERN. It allows researchers to deposit research papers, data sets, research software, reports, and any other research. PRECINCT opened its own community in April, 2023 in order to start curating all of the mature tools, publications and other resources. Due to the very restrictive nature of the project, not many of the deliverables will be published in the Community; however, all of the public deliverables, scientific articles, videos, presentations, publications, etc. produced by the project will be considered. Namely, the Zenodo community will house most of the PRECINCT-produced content available to the public, including some of which is already found on the YouTube Channel and the website. Due to the open access of Zenodo, any type of stakeholder will be able to engage with the content, while it may potentially attract more academia and research stakeholders due to the research-oriented nature of the site. In addition, the longevity of the results will be guaranteed due to Zenodo's support from CERN and the European Union, guaranteeing that the impact will be long-lasting.

5.4 Assessment of the PRECINCT Stakeholder Needs Knowledge Base

The main objective of the Stakeholder Needs Knowledge Base is to share the project findings to a great number of relevant CI stakeholders across the EU. By collating almost all knowledge (the exception refers to the EU restricted materials) generated by PRECINCT and publishing them on an open-access repository like Zenodo, PRECINCT is ensuring that the knowledge will outlive the project itself. Additionally, it is important that the knowledge can be easily found and can be easily accessible to stakeholders in order to decrease any barriers to engagement. Thus, the Stakeholder Needs Knowledge Base of PRECINCT aims to be as open as possible and as simple as possible, by using well-known platforms and ensuring that the platforms complement each other. YouTube is one of the world's most recognizable video-hosting platforms, allowing stakeholders to easily interact with PRECINCT's video content and even sharing it to other stakeholders. In addition, the channel has been advertised on the website, social media channels and at the final event, thus, stakeholder awareness should be high. Zenodo is also well-known, especially in the European research community, as a knowledge repository. It is also quite easy to use, and once the PRECINCT community is located the content is enlisted by the date uploaded in an easy-to-read format. These two platforms are free for the PRECINCT project to use and maintain, meaning that the lifespan of these depends on the platform's existence (currently there is no foreseeable closing of either platform). Therefore, if the PRECINCT website becomes defunct, all knowledge will still remain on Zenodo and YouTube.

As it stands, the PRECINCT Stakeholder Needs Knowledge Base achieves its objective of providing stakeholders with an open access library that contains the projects' findings allowing them to enter after the conclusion of the project. The knowledge base has not only benefited the stakeholders by providing them with knowledge created by the PRECINCT research; it also benefits PRECINCT by continuously raising awareness of the project and by allowing stakeholders to hopefully exploit this knowledge to increase CIs resilience. Additionally, by using the knowledge of stakeholder needs gained through engagement with stakeholders in the PRECINCT events, the knowledge base and T6.3, the potential for uptake of PRECINCT tools and assets should increase as stakeholders understand the tools, how they work, and why they matter to protecting Europe's CI.

6 Liaison & Cooperation Activities

PRECINCT engaged in various Liaison and Cooperation Activities aiming to share and benefit from the knowledge of other projects and initiatives in the domain of CIP. The first and foremost activity in this domain was PRECINCT joining the European Cluster for Securing Critical Infrastructure (ECSCI) in 2021. This cluster creates synergies and fosters emerging disruptive solutions to security issues via cross-projects collaboration and innovation, while also highlighting the different approaches between the clustered projects and establishing tight and productive connections with closely related and complementary H2020 projects. PRECINCT was present at the second workshop organised on April 27-29, 2022 both presenting the project and coordinating a panel on standard in CI. This first step led to the stable participation of PRECINCT to the working group "Contribution to standards and regulations on the protection of Critical Infrastructures". PRECINCT was also present at the "1st annual conference on Critical Infrastructure Protection and ECSCI workshop" held on the 20th and 21st September in Brussels. PRECINCT also worked in collaboration with the ECSCI cluster and other projects in the CI area to organise a Workshop to be held on December 5, 2023 on "Collaborative Standardisation and Policy making for greater resilience in Europe". This workshop will be held after the completion of the PRECINCT project but it remains useful to be present with the aim to share results and lessons learned from the project. PRECINCT's participation in these events allowed the projectto further promote PRECINCT and disseminate its project results to stakeholders and invited the cluster to participate in each of its events. On top of the above participation PRECINCT has also worked closely with the EU-CIP project which will be transforming the ECSCI cluster into a an EU-wide knowledge network with advanced analytical and innovation support capabilities, of which PRECINCT envisages to be a part of.

Figure 6-1: Visualisation of the ECSCI

PRECINCT also cooperated directly with projects that were of close relevance to it, most notably its sister project PRAETORIAN and the STRATEGY Project. PRAETORIAN and STRATEGY have been involved in all PRECINCT events, with PRAETORIAN co-organising the 2nd Stakeholder Workshop and the PRECINCT Conference, and STRATEGY participating in the standardization and policy recommendations sessions for the SEWs, while also being co-organisers for the PRECINCT Conference. Furthermore, PRECINCT and STRATEGY signed a memorandum of cooperation (see Annex V) outlining the areas for further cooperation and the activities to be undertaken, including the use of a STRATEGY Standard in the Athens Living Lab. KEMEA led the CEN workshop addressing the efficiency and accuracy of Incident Situational Reporting for Critical Infrastructures in the context of the STRATEGY project as a continuation of KEMEA's activities in the field of Critical Infrastructure Protection and development of the pilot Coordination Center for Critical Infrastructure Protection. 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. More information regarding this cooperation can be found in D6.5 "Impact Assessment and Policy & Standardisation Recommendations"

7 Conclusions

Although the PRECINCT project did not develop a traditional Dissemination & Communication Plan, it managed to engage stakeholders throughout the project's lifespan. The main engagement was through its stakeholder knowledge base task (supplemented by dissemination communication tasks under T6.2) under which PRECINCT partners created the knowledge base repositories and organized the 4 main events to gather external stakeholders. As previously mentioned, the project events were at critical points of the project which delivered feedback that was considered during the project's development progress and continuously informing stakeholders for the corresponding updates.

In terms of meeting its objectives, the PRECINCT project managed to consolidate and present the main outputs of PRECINCT and to ensure a strong interaction with industry CI stakeholders, end-users, citizens, solutions providers, and broad CI academia interest groups, which was the central aim of Task 6.1. In addition, all events outlined in the Grant Agreement (GA) were held and managed to reach any KPI attached to them.

Finally, one of the main outputs of this task was a CyberPhysical Security Stakeholder Needs Knowledge Base that allows the PRECINCT generated knowledge to be easily accessible to stakeholders beyond the project's lifespan. This was achieved with the creation of the PRECINCT Zenodo community, which houses all publicly available PRECINCT information for free, complemented by the YouTube Channel and the website.

8 Annex

8.1 PRECINCT 1st SEW Agenda

PRECINCT

Agenda

PRECINCT's 1ST Stakeholders Engagement Workshop

Maison des Associations Internationales, Rue Washington 40, 1050 Brussels (Ixelles)

(On-Line, Zoom)

5th May 2022

08:30 – 09:00	*Welcome and Registration*	
09:00 – 09:10	Remarks	Jenny Rainbird, Project Coordinator (ICP)
09:10 – 09:25	Main Key Results and Roadmap	Gabriele Giunta (ENG)
09:25 – 09:50	BluePrints and Knowledge Graphs	Djibrilla Amadou-Kountche (AKKA), Stathis Zavvos (VLTN)
09:50 – 10:10	Serious Games	Daniel McCrum (UCD), Yash Shekhawat (NURO)
10:10 – 10:30	PRECINCT Architecture and Implementation	David Vermeir (IMEC)
10:30 – 10:45	Coffee Break	
10:45 – 11:00	PRECINCT Living Labs	Shirley Delannoy (VIAS)
11:00 – 11:15	Operation Athens	John Limaxis, Gerasimos Kouloumbis (ICP)
11:15 – 11:30	Operation Antwerp	Shirley Delannoy (VIAS)
11:30 – 11:45	Operation Ljubljana	Denis Čaleta (ICS)
11:45 – 12:00	Operation Bologna	Giuseppe Brancaccio (ITL)
12:00 – 12:40	Partners' feedback on the business requirements	Mark Bennett (ICP)
12:40 – 12:45	Morning Conclusion	Jenny Rainbird, Project Coordinator (ICP)
12:45 – 13:30	Lunch Break	
13:30 – 13:45	Critical Infrastructure Protection	Päivi Mattila, EU-HYBNET Project Coordinator (LAUREA)
13:45 – 15:15	PRECINCT's Future Technical Aspects	*Moderator*: Mark Miller (CPT) *Speakers*: Daniel McCrum (UCD), Stefan Lefever (IMEC), Stefan Schauer (AIT), Gabriele Giunta (ENG), Lorcan Connolly (RDS)
15:15 – 15:30	Coffee Break	
15:30 – 16:45	Drivers and Barriers for implementation of new CIP Solutions	*Moderator*: Mark Bennett (ICP) *Speakers*: Marisa Escalante Martinez (TCNL), Päivi Mattila (LAUREA), Vito Morreale (ENG), Benoit Baurens (AKKA), Denis Čaleta (ICS)
16:45 – 17:00	Conclusions	Jenny Rainbird, Project Coordinator (ICP)

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 101021668.

8.2 PRECNCT 2nd SEW Agenda

PRECINCT

PRECINCT's 2nd Stakeholder Engagement Workshop

Co-organized with the help of PRAETORIAN

AGENDA

Time	Topic	Room in the M.A.I
8:50 – 9:00	Welcome and Registration	**Berlin Room**
9:00 – 9:10	Opening of the Workshop	**Berlin Room**
9.10 – 9.20	PRECINCT: First Year Results & Highlight	**Berlin Room**
9.20 – 9.40	PRAETORIAN: First Year Results & Highlight	**Berlin Room**
9:40 – 10:30	Crisis Management: The Human Aspect of Critical Infrastructure Protection	**Berlin Room**
10:30 – 10:45	Coffee Break	
10:45 – 13.00	From Theory to Practice: Project Living Labs & Pilot Scenarios	**Berlin Room**
13.00 – 13.45	Lunch Break	
13.45 – 15.15	Working Group #1: Standardisation & Policy Recommendations	**Paris Room**
13.45 – 15.15	Working Group #2: PRECINCT Training & Capacity Building	**Berlin Room**
13.45 – 15.15	Working Group #3: PRAETORIAN Training & Capacity Building	**Roma Room**
15.15 – 15.30	Coffee Break	
15:30 – 16:00	Conclusions of the Working Groups	**Berlin Room**
16:00 – 17.00	PRECINCT: A Perspective in View of Exploitation (Q&A)	**Berlin Room**
17.00 – 17.15	Conclusions & Closing of the Workshop	**Berlin Room**

8.3 PRECINCT Conference Agenda

PRECINCT

PRECINCT Conference
on
Critical Infrastructure Protection, Cybersecurity and Crisis Management

Day 1 – May 16th

AGENDA

Time	Topic	Speaker
9:00 – 9:30	Welcome and Registration	**PRECINCT Consortium**
9:30 – 10:00	Opening of the Conference	**Ms. Natalja Miolato,** *Project Advisor at the Research Executive Agency*
10:00 – 11:00	Protecting Critical Infrastructures facing Hybrid Threats	Chair: **Dr. Stefan Schauer,** *Senior Researcher for Security & Communication Technologies at AIT* Speakers: • **Dr. Päivi Mattila,** *Director of Security Research Program & EU-HYBNET project coordinator* • **Gilda de Marco,** *R&D - European Projects at Insiel* • **Rafa Company,** *Director of Safety and Security at Valencia Port*
11:00 – 11:15	Audience Q&A	**Dr. Stefan Schauer,** *Senior Researcher for Security & Communication Technologies at AIT*
11:15 – 11:30	EU-CIP: a novel pan European knowledge network for Resilient Infrastructures.	**Dr. Gabriele Giunta,** *Head of the Smart Transport and Infrastructures Unit with the IS3 R&D Lab at ENGINEERING*
Coffee break		
11:45 – 12:45	Living Lab Methodology - Innovative Threat Response	**Mrs. Shirley Delannoy,** *Researcher, VIAS Institute* **Thomas de Meester,** *Innovation Specialist/Product Owner, IMEC*
12:45 – 13:00	Audience Q&A	**Mrs. Shirley Delannoy,** *Researcher, VIAS Institute*
Lunch break		
13:45 – 14:00	Practical Information on the Break-Out Sessions	**Dr. Giovanni Nisato,** *Managing Director & Founder of Innovation Horizons; Inlecom Commercial Pathways*

AI4CYBER EU-CIP PRAETORIAN EU-HYBNET DYNABIC STRATEGY SUNRISE

PRECINCT

14:00 – 15:30	**Break-out session #1**: *Cybersecurity Datasets: Challenges and Opportunities*	**Dr. Erkuden Rios,** *Director of Cybersecurity R&I projects at TECNALIA/Coordinator of AI4CYBER*
	Break-out session #2: *Critical Infrastructure Resilience through Public Transport*	**Mrs. Carmela Canonico,** *Safety & Security Manager at UITP*
	Break-out session #3: *PRECINCT's 2nd Training & Capacity Building Programme*	**Mrs. Marisa Escalante,** *Project Manager at TECNALIA*
Coffee break		
15:45 – 17:15	**Break-out session #4**: *Standardization in PRECINCT & STRATEGY and future policy recommendations*	**Mrs. Loredana Mancini,** *PRECINCT Impact Manager* **Dr. Georgios Sakkas,** *Research Associate at KEMEA*
	Break-out session #5: *Validation of security tools for CI protection*	**Mr. Tim Stelkens-Kobsch,** *Aviation Security Researcher at DLR,* **Mrs. Eva Muñoz Navarro,** *Project Manager at Grupo Etra*
	Break-out session #6: *PRECINCT's 2nd Training & Capacity Building Programme*	**Mrs. Marisa Escalante,** *Project Manager at TECNALIA*
17:15 – 17:30	Conclusions – End of Day 1	**Dr. Giovanni Nisato,** *Managing Director & Founder of Innovation Horizons; Inlecom Commercial Pathways*

Day 2 – May 17th

AGENDA

Time	**Topic**	**Partner Responsible**
8:30 – 9:00	Welcome and Registration	**PRECINCT Consortium**
9:00 – 9:15	Opening of Day 2	**Dr. Giovanni Nisato,** *Managing Director & Founder of Innovation Horizons; Inlecom Commercial Pathways*
9:15 – 9:30	Keynote speech	**Mr. Giannis Skiadaresis,** *Area Coordinator for Strengthened Security Research and Innovation (SSRI), DG HOME*
9:30 – 10:30	Panel Discussion on Innovation Uptake for Critical Infrastructure Protection	Chair: **Mr. Mark Miller**, *CEO of Conceptivity & Vice-Chair of EOS* Speakers: • **Mr. Giannis Skiadaresis,** *Area Coordinator for Strengthened Security Research and Innovation (SSRI), DG HOME*

AI4CYBER EU-CIP PRAETORIAN EU-HYBNET DYNABIC STRATEGY SUNRISE

		• **Dr. Takis Katsoulakos** *Managing Director for Inlecom Commercial Pathways* (TBC) • **Mr. Isto Mattila** *R&D Director at Laurea University of Applied Sciences & CEO of Dicitur Ltd* • **Dr. Giovanni Nisato** *Managing Director & Founder of Innovation Horizons; Inlecom Commercial Pathways*
10:30 – 10:45	Audience Q&A	**Mr. Mark Miller**, *CEO of Conceptivity & Vice-Chair of EOS*
Coffee Break		
10:45 – 11:45	The Resilience of Critical Entities: a New EC Directive	Chair: **Dr. Georgios Sakkas,** *Research Associate at KEMEA* • **Dr. Erkuden Rios,** *Director of Cybersecurity R&I projects at TECNALIA; Coordinator of AI4CYBER* • **Dr. Aikaterini Poustourli,** *Scientific Fellow of STRATEGY; Satways Ltd.)* • **Mr. Paolo Venturoni,** *CEO of the European Organisation for Security*
11:45 – 12:30	Resilience in Cybersecurity	**Dr. Sandra König,** *Scientist/Researcher in Safety and Security at AIT*
12:30 – 13:00	After PRECINCT, DYNABIC	**Dr. Erkuden Rios,** *Director of Cybersecurity R&I projects at TECNALIA*
13:00 – 13:10	Closing of the Conference	**Dr. Giovanni Nisato,** *Managing Director & Founder of Innovation Horizons*

8.4 PRECINCT Final Event Agenda

PRECINCT

PRECINCT Final Event

9:00 – 17:00 CEST, September 14th, 2023
Viale della Fiera, 8 - 40127, Bologna, Italy

AGENDA

Time	Topic	Speaker
8:30 – 9:00	Welcome and Registration	**The Institute for Transport and Logistics (ITL)**
9:00 – 9:10	Opening of the Final Event	**Mr. Guido Fabbri,** *President of ITL*
9:20 – 9:30	Objectives and ambitions of PRECINCT	**Mrs. Jenny Rainbird,** *Head of EU Project Delivery at ICP; PRECINCT Project Coordinator*
9:30 – 10:00	Quick Overview of PRECINCT's Achievements & Success stories	**Mr. Gabriele Giunta,** *Head of the Smart Transport and Infrastructures Unit at ENGINEERING*
10:00 – 10:45	Demonstration of the PRECINCT Tools & Assets: • Cascading Effects Simulation • Resilience Methodological Framework • Cyber Range	**Mr. Manuel Egger,** *Junior Research Engineer at AIT* **Mr. Lorcan Connolly,** *Director at Research Driven Solutions* **Mrs. Marisa Escalante,** *Project Manager at TECNALIA*
Coffee Break		
11:00 – 11:45	Demonstration of the PRECINCT Tools & Assets: • Serious Games • Supporting IT operation : Blueprints as guidelines and executable plans for mastering deployment, configuration and maintenance of PRECINCT Tools	**Dr. Páraic Carroll,** *Assistant Professor in Transport Engineering at UCD* **Dr. Djibrilla Amadou Kountche,** *R&D Project Manager at AKKODIS Research*
11:45 – 12:30	The Roadmap to Implementation: View from the Transferability Demonstrators	**Mrs. Shirley Delannoy,** *Researcher, VIAS Institute* **Mrs. Esther Linask,** *Geoinformatics specialist at Tallinn Strategic Management Office* **Dr. Seifeddine Bettaieb,** *Researcher at Luxembourg Institute of Science and Technology*
Lunch Break		

13:30 – 14:30	Bologna Living Lab – Experiences, Lessons Learned and What Next?: PRECINCT Analytics Dashboard and Digital Twin	**Mr. Nicola Durante,** *Research And Development Engineer at ENGINEERING*
14:30 – 14:45	Keynote Speech: Policy & Critical Infrastructure Protection	**Dr. Aikaterini Poustourli,** *Scientific Fellow of STRATEGY; Satways Ltd.)*
14:45 – 15:15	PRECINCT Recommendations: PRECINCT White Book; Policy Recommendations	**Mrs. Loredana Mancini,** *PRECINCT Impact Manager*
Coffee Break		
15:30 – 17:00	After PRECINCT: Upscaling Potential	Chair: **Dr. Giovanni Nisato,** *Managing Director & Founder of Innovation Horizons; Inlecom Commercial Pathways* **Dr. Cristiano Passerini,** *COO Digital Innovation Hub - Emilia-Romagna at Lepida ScpA* **Mr. Benoit Baurens,** *Head of Innovation Department and R&D Program Manager at AKKODIS* **Mr. Pedro Homem de Gouveia,** *Senior Policy and Project Manager, Governance & Integration + Safety & Security at Polis Network*
17:00 – 17:15	Conclusion of PRECINCT's Final Event	**Mrs. Jenny Rainbird,** *Head of EU Project Delivery at ICP; PRECINCT Project Coordinator*

8.5 Memorandum of Cooperation between PRECINCT & STRATGEY

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

1

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

2

- 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

4

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 2nd PRECINCT Workshop planned for November 22nd 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 1st Interoperability Event organized by STRATEGY on Rome on February 15th 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 2nd 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 3rd quarter of 2023.

5

II. POINTS OF CONTACT

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

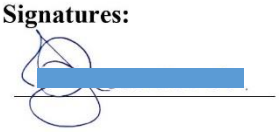
PRECINCT Project Coordinator	STRATEGY Project Coordinator
Mrs. Jenny Rainbird	**Mr. Giannis Chasiotis**

III. DURATION OF THE AGREEMENT

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

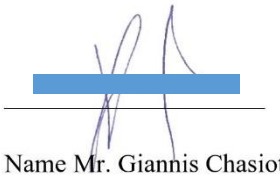
This memorandum shall remain in effect until the end of each of the respective projects (listed in clause I of this document), with the possibility of further cooperations and joint activities (such as workshops, conferences and others).

Signatures:



Name Mrs. Jenny Rainbird

Position: PRECINCT Project Coordinator



Name Mr. Giannis Chasiotis

Position: STRATEGY Project Coordinator

6