PRECINCT

Preparedness and **R**esilience **E**nforcement for **C**ritical **IN**frastructure cascading **C**yberphysical **T**hreats and effects with focus on district or regional protection

www.precinct.info

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

PRECINCT

PRECINCT

WELCOME

Welcome to the PRECINCT brochure, which provides an overview of the project's goals, concept and innovations, the projects' partners, and it's geographical. Please, visit the PRECINCT website and follow us on social media.

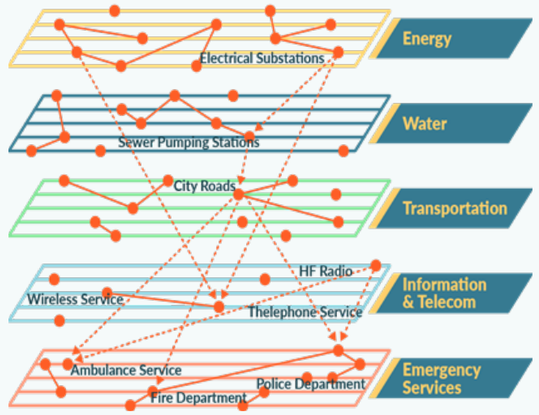
Enjoy reading!

Authors: PRECINCT consortium
Contact person: Jenny Rainbird (Inlecom Commercial Pathways), Project Manager
Contact details: PRECINCT_PM@inlecomsystems.com

Foreword

Critical Infrastructures are increasingly at risk from a variety of intentional cyber-physical attacks (malware, terrorist driven exploits, etc.) as well as risks from natural hazards (e.g. extreme weather, fires, earthquakes, disastrous consequences of global warming) and hybrid threats including fake news. However, managing the impact of cascading effects arising from the interdependencies between different types of critical infrastructures (e.g. related to energy, water, transport, communications) and their resilience towards enabling 'rapid recovery' is becoming more and more pertinent and is highly challenging, especially in the context of delimited geographical areas (e.g. districts, cities or regions). The vulnerability of urban centres points to the need for strong public-private coordination to mobilize a response from different sectors and improved level of protection for associated Critical Infrastructures.

The inter-dependencies between Critical Infrastructures (see Fig. 1.1), including their links to emergency services and smart city systems, need to be addressed in a more holistic way to increase the safety and security of citizens. Due to their high impact nature, the cascading effects in multi-hazard contexts have started to be recognized as a priority issue in legislation concerned with the control of major accident hazards. To address these issues, PRECINCT aims to connect private and public Critial Infrastructure stakeholders in a geographical area to a common cyber-physical security management approach which will yield a protected territory for citizens and infrastructures. Our ultimate ambition is a 'PRECINCT' that can be replicated efficiently and cost effectively for a safer Europe.



(Fig. 1.1 Interdependencies between Critical Infrastructures)

PRECINCT in a Nutshell

Project name

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

Type of action

Innovation Action

Call

H2020 – SU – INFRA – 2018 – 2019 – 2020
Protecting the infrastructure of Europe and the people in the European smart cities.

Duration

24 months (starts in October 2021)

Eu-funding

7.996.658,38 euro

Con-sortium

40 partners of excellence from 11 countries with very cross-cutting and complementary competencies.

Objectives

PRECINCT aims to connect private and public CI stakeholders in a geographical area to a common cyber-physical security management approach which will yield a protected territory for citizens and infrastructures. The ultimate ambition is that PRECINCT can be replicated efficiently and cost effectively for a safer Europe.

Expected impact

The involvement of 11 Critical Infrastructures representing the transport, water, energy and ICT sectors and 2 police organisations as active project partners, covering different type of Critical Infrastructures (private/public), size and geographical distribution. In 4 Living Labs and 3 Demonstrators more than 20 Critical Infrastructures and first responders, national authorities will participate creating a critical mass for adoption and providing evidence of what is working, and which components provide clear advantages.

The goal of the project

The goal of PRECINCT is to supervise and control complex interdependent networks and Cyber Physical Systems of Systems with distributed ownership and management structures.

PRECINCT project exploits the Digital Twin concept to model the current and future behaviour of territory-based interdependent Critical Infrastructures in a variety of conditions and configurations, to anticipate threats, to detect anomalies, and to incentivise optimised command structure and coordinated responses between Critical Infrastructures and first responders, thereby enhancing the resilience of the PRECINCT. Digital Twins will work in parallel with real-life operations supporting the design-operation continuum of interdependent Critical Infrastructures by modelling, and simulating, both the supervision and control of Cyber Physical Systems functions/components. In PRECINCT, vulnerabilities to previously unanticipated combinations of threats or cascading effects will be identified through a novel Serious Games approach. The ingenuity of people (Gamers) will be exploited by data mining and Machine Learning (reinforcement learning) of Serious Games' records to pre-empt the potential for successful attacks and inform defence strategies. Along with the Digital Twin concept, the Serious Game in PRECINCT will provide a means of testing and validating new detection and mitigation approaches in present day real-life contexts.

Importantly, the complexity of interrelated effects from interconnected Critical Infrastructures (Critical Infrastructures) exposes the limits of traditional risk assessment and risk mitigation approaches, when focused only on known risk event probabilities and associated consequence reductions. Therefore, resilience strategies become essential in minimising the impact of such threats and to ensure service restoration and continuity in the aftermath of destructive events, especially in cases when these cannot be predicted and/or avoided (such as natural hazards), and proactive and preventive measures to mitigate them are desirable.

Moving from traditional risk analysis to resilience analysis and management allows for resilience-driven risk control by taking appropriate measures in all security and resilience management phases: preparation and prevention (risk probability reduction), protection (consequence impact reduction), attack detection and identification response and recovery (linked to mitigation and fast recovery).

Technical objective of the project

The overall project's technical objective is to establish an Ecosystem Platform for connecting stakeholders of interdependent Critical Infrastructures 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 will provide 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.

PRECINCT concept

In full alignment with EU policy, particularly the pillars of the new EU Security Union Strategy for the period 2020 to 2025 , PRECINCT is addressing cascading effects in Critial Infrastructure system of systems (Multi-Modal Transport, Energy, ICT/Telecoms, Water) and focuses on both resilience and 'rapid recovery'. The PRECINCT concept is designed to consolidate and extend knowledge and assets from Reference Projects into a Framework and a Directory of PRECINCT CIP Blueprints supporting Critial Infrastructure Communities to design and operate ecosystems integrating their own systems with Digital Twins to enable coordinated security and resilience management incorporating improved "installation-specific" security solutions. Serious Games will be used as an innovative vulnerability assessment tool for the complex multi-system cascading effects in the Living Labs, thereby supporting focused development of new resilience enhancement services.

PRECINCT stakeholders

"The actions carried out in project will impact on and be affected by a wide range of stakeholders, from industry and technology companies, to infrastructure providers, cities, and policymakers."

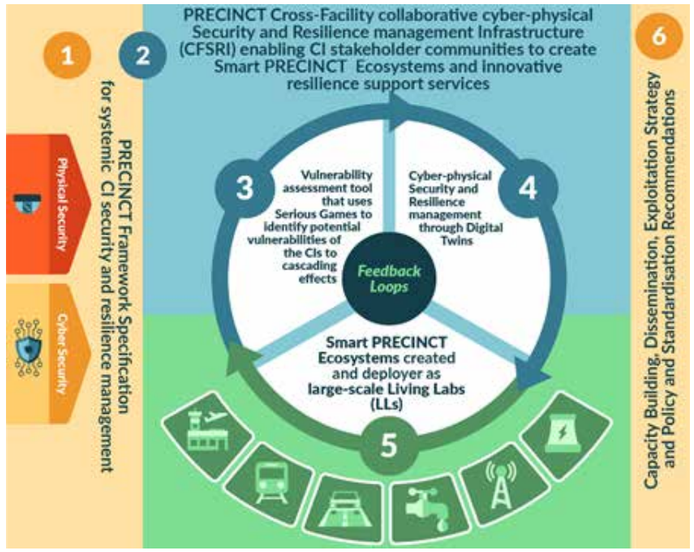
Local Level: Local law enforcement authorities; local first responders; local Critial Infrastructure protection actors.

National level: national law enforcement authorities; national first responders; national Critial Infrastructure protection actors.

European level: ENLETS; European Network of Law Enforcement Technology Services; SENTER network; Network for Strengthening European Network Centres of Excellence in Cybercrime.

Four Living Labs

The project will demonstrate the concept of Smart Resilient PRECINCTs in 4 Living Labs. Cascading effects will be considered in Multimodal Transport, Energy, Water and ICT/ Telecommunications threat scenarios based on Critial Infrastructure interdependencies between these prominent and highly interconnected verticals covering cyber physical and hybrid threat scenarios. The requirements for a collaborative cyber-physical security management approach, including public-private partnerships, will be looked at from a nested-scales approach to achieve harmony between the social organization and economic development, finding the best balance between the risk, cost, and security & resilience requirements, as well as informing tactical and strategic territory investment options. For this, PRECINCT will build on recent and progressive Critical Infrastructures approaches in the 4 proposed LLs. The project will provide a model-driven collaborative and unifying cyber-physical security and resilience management platform for smart resilient PRECINCTs, leveraging advances from CIP and INFRA-01 projects, as well as the extensive body of work in Urban and Critical Infrastructure protection and resilience management (RESILENS, DRIVER, RESOLUTE) thus exploiting, evolving and embodying key outputs and knowledge gained into the PRECINCT models and services. The main project outputs depicted in Figure 1.2 are:



(Fig.1.2 : Overview - Rationale of the main project outputs)

PRECINCT key outputs

1. A PRECINCT Framework Specification for systematic Critical Infrastructures security and resilience management fulfilling industry requirements coming from stakeholders within the Living Labs and integrating new insights from other reference EU projects.
2. A Cross-Facility collaborative cyber-physical Security and Resilience management Platform enabling CI managers to develop AI-enabled PRECINCT Ecosystems and enhanced resilience support services.
3. A vulnerability assessment tool that uses Serious Games and includes cascading effects which will help to identify resilience enhancements for each CI and the measures which should be put in place to improve security.
4. Digital Twins that represent the Critical Infrastructures network topology and metadata which will apply closed-loop Machine Learning to detect anomalies and alerts to provide optimised activation of response and mitigation measures and automated forensics.
5. Smart PRECINCT Ecosystems, deployed in four large-scale Living Labs and in transferability validation demonstrators, will provide measurement-based evidence of the improvements delivered through the PRECINCT components.
6. Sustainability outputs including Capacity Building, Dissemination, Exploitation and Policy and Standardisation Recommendations.

Living Lab 1
Ljubljana (Slovenia)

Focus Area

Multi-CI coordination centre

LL1 will deploy and test the PRECINCT approach between four interconnected Critical Infrastructures (national rail and city bus transport, electricity distribution systems operator and telecommunications infrastructure) and the Municipality Police with connection to neighbouring city first responder services.

Threat scenario will focus on a physical threat (bomb) and a cyber-attack with simultaneous DDoS attacks to critical parts of the critical Industrial Control Systems (ICS) of the electricity and communication operators, which provide important services for business continuity of the transport mobility hub.

Living Lab Partners

- **Interconnected Critical Infrastructures**
- **The Slovenian National Railway Company and Traffic Institute**
- **The City of Ljubljana bus transport operator**
- **The Telekom Slovenije**
- **Elektro Ljubljana**
- **The City of Ljubljana's Municipality Police**
- **The Institute for Corporate Security Studies**
- **Support from the Information Security Administration of the Republic of Slovenia**

Living Lab 2
Antwerp (Belgium)

Focus Area

Emergency Services & coordinated Critical Infrastructures through city Digital Twin

LL2 will contribute to and utilize the PRECINCT Reference Framework models to establish a dependencies map between Critical Infrastructures in the Antwerp region using in the first place the Multidisciplinary Emergency Operational Command Post (CP-OPS).

Threat scenario will focus on flooding and disastrous consequences of global warming with cascading effects on the water CI and its impact on the traffic CI.

Living Lab Partners

- **Vias Institute is a coordinator**
- **Police Zone Antwerp**
- **Water-link**
- **IMEC - integrated CI models for flooding and traffic prediction**
- **KUL - city's flooding model and rainfall nowcasting**

Living Lab 3
Athens (Greece)

Focus Area

Transport reliance- Athens

LL3 will deploy and test the PRECINCT platform in terms of increasing the resilience of Critical Infrastructures (rail and road network along the Athens Airport/Attiki Odos corridor as well as along the urban rail/road network) in the case of various cyber-physical attack scenarios.

Threat scenario will focus on cyber-attack on the airport's Building Management System, underground and road communications. The scenario under a seismic event will be considered, as the Greater Urban Area of Athens has a moderate to high chance of earthquakes.

Living Lab Partners

- **Athens airport**
- **Attiko Metro**
- **Attikes Diadromes - will contribute to road/motorway-related data**
- **KEMEA - holistic PRECINCT security framework**

Living Lab 4
Bologna (Italy)

Focus Area

ICT Critical Infrastructure – Bologna

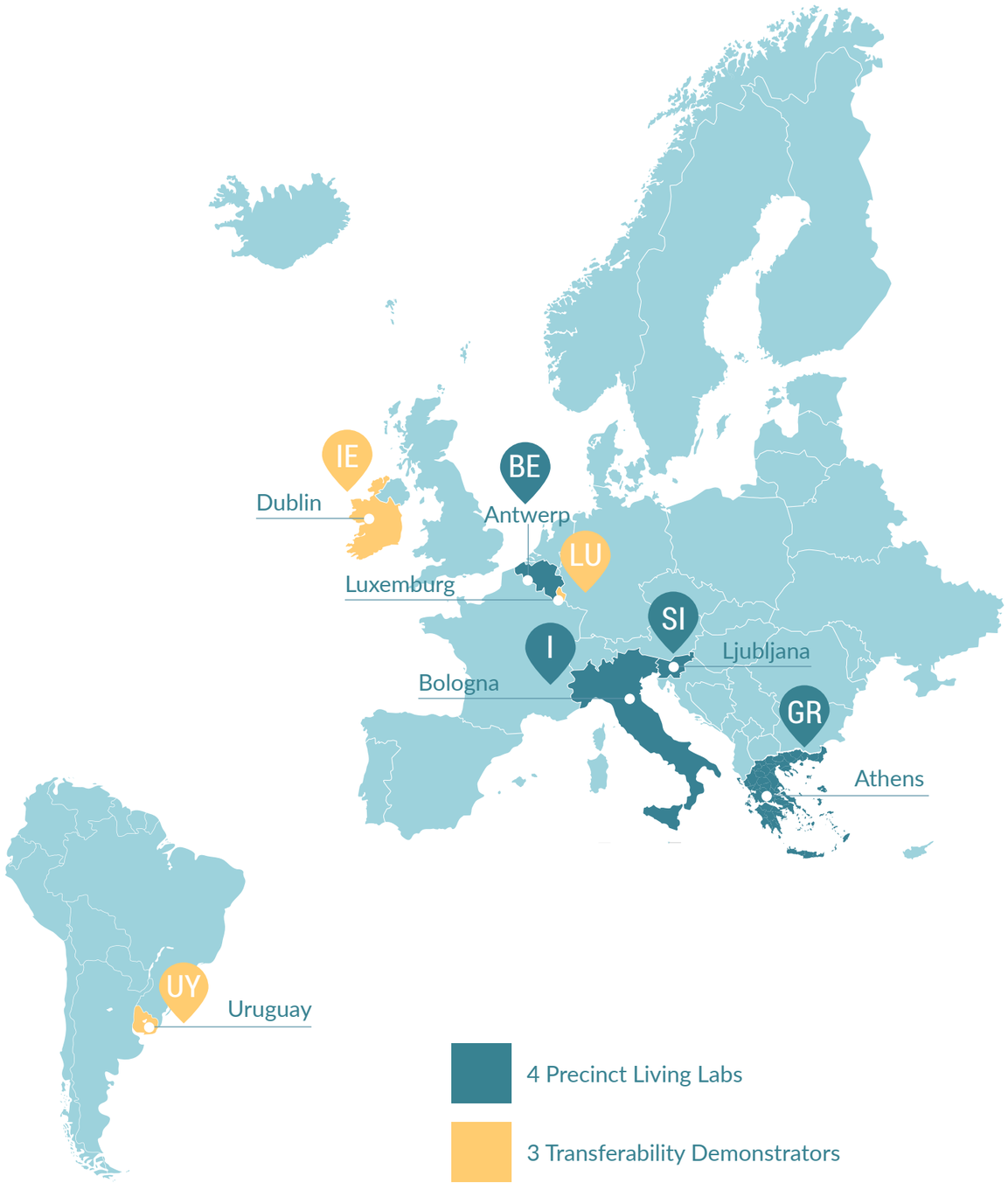
LL4 will contribute, deploy and test PRECINCT Framework and Critical Infrastructures coordinated security and resilience approach with a focus on the Lepida ICT CI and interdependencies/cascading effects of the full range regional transport Critical Infrastructures.

Threat scenario will focus on airport cyber-attack / cyber physical attacks on rail/ airport infrastructures combined with attack on the Lepida IT system reducing the ability of the Critical Infrastructures and authorities to communicate with the public and cascading effects on mobilisation of first responder services.

Living Lab Partners

- **Lepida - IT for the Regional Government**
- **Bologna airport**
- **Ferrovie dello Stato - data sources and threat scenarios**
- **The Institute for Transport & Logistics**
- **Emilia-Romagna Region Regional Government**
- **Bologna Metropolitan City**
- **Local emergency responders**
- **Police dept and traffic police.**
- **Local Health Authority of Bologna**
- **TPER (public transport operator)**
- **SRM Reti e Mobilità (Local Authority for Public Transport)**
- **Marconi Express - Bologna Int. Airport to city of Bologna transport link**
- **Port Authority of Ravenna**

Precinct Living Labs



Transferability Demonstrators

The precinct insights will be transferred into demonstrators to obtain maximum value. Moreover in:

Luxemburg (Energy Tele-communications focus) – investigation in integration of the PRECINT DT with the ongoing development of the Luxemburg National DT by LIST

Dublin Smart Sandyford/ Dún Laoghaire Rathdown County Council (Transport, Energy focus) and investigation of green transport city security/resilience implications.

Uruguay coordinated by the Secretaría de Inteligencia Estratégica del Estado (SIEE) (involving OSE (water), UTE (electricity) and ANTEL telecom Critical Infrastructures) and will explore the possibility of SIEE establishing a Digital Twin-enabled National Critical Infrastructures Coordination Centre.

Besides they will contribute to the knowledge of ‘packaging’ outputs for maximum impact and commercialization potential.

Partners

Our project team

PRECINCT is coordinated by Inlecom Commercial Pathways, which is the branch of Inlecom Group that supports commercialisation of products, solutions, assets and services, including guiding associated patents, and guiding market sector analyses/intelligence and business plans. ICP assumes the role of the Project Coordinator and Commercialisation Consultant for the project including project management and risk management led by PMI and Prince certified project management professionals with 20+ years of experience.

Dr Takis Katsoulakos
PRECINCT Coordinator

Mrs. Jenny Rainbird
PRECINCT Project Mgr

Dr Pat O'Sullivan
ICP CTO

Mr. Patrick Durkin
ICP Commercial Director

Mr. Mark Bennet
PRECINCT Commercial Lead

Mrs. Loredana Mancini
PRECINCT Impact Manager

Mr. Yash Chadha
ICP Financial Director

Mr. Gerasimos Kouloumbis INLE Innovation Delivery Department Leader

Mr. Ioannis Lymaxis
PRECINCT
LL3 & T1.5 Leader

Mrs. Vasiliki Konstantopoulou
PRECINCT
Technical Engineer

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
Core B, Block 71, The Plaza Park West, Dublin, Ireland

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**