PRECINCT

# NEWSLETTER

January 2022
Issue #01

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

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

PRECINCT

# WELCOME TO PRECINCT

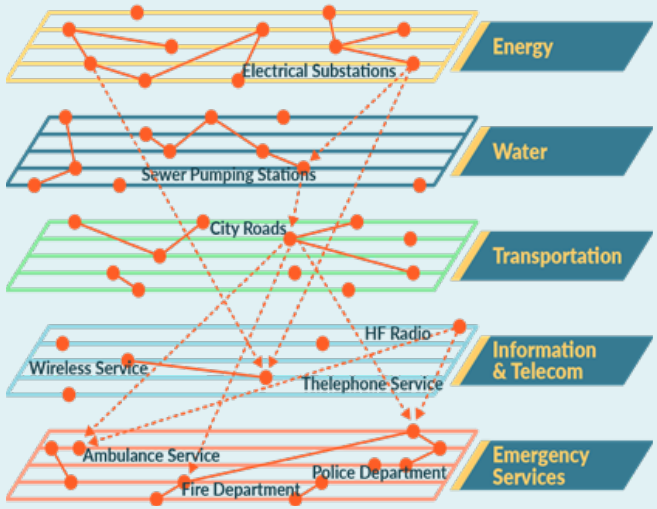
## Welcome to our quarterly Newsletter.

It is our first newsletter and we are excited to tell you all about the work that has been going on in the first few months since the project has started. This issue introduces the project, the team and partners. The next issue planned for April 2022 will present further PRECINCT developments, we will reveal the deliverables completed and the progress. We will also give a floor to consortium partners and will keep you informed on upcoming events.



## Challenge

Critical Infrastructure in Europe is at risk from a variety of natural disasters, physical and cyber attacks from malicious and terrorist groups and individuals. These problems are compounded by the inter-dependencies between Critical Infrastructures, including their links to emergency services and smart city systems.




CI threats associated with transport and energy create cascading risks that ripple through interconnected CI systems and pose life threatening conditions in affected areas. 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.

A comprehensive and holistic approach is needed to increase the safety and security of critical infrastructure for citizens.

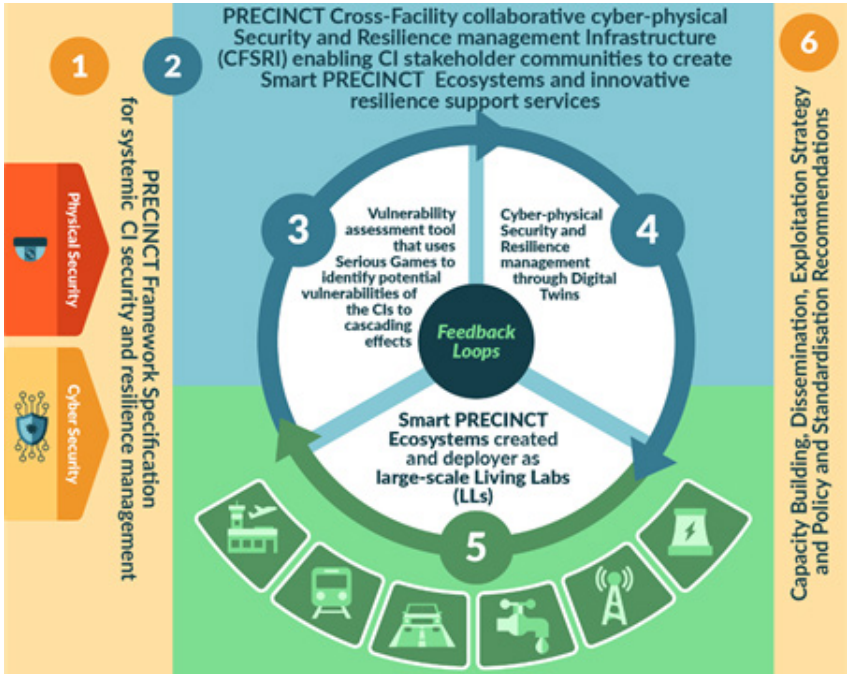
## Approach

In response to these challenges the EC raised a call from projects under the topic of «Prevention, detection, response and mitigation of combined physical and cyber threats for critical infrastructures in Europe". The PRECINCT project has been funded by the EC under this call and started in October 2021 and run for two years.

PRECINCT's technical objective is to establish an Ecosystem Platform for connecting interdependent CIs and Emergency Services so that they can collaboratively and efficiently manage security and resilience by sharing information such as Data, Critical Infrastructure Protection models and Resilience services.

PRECINCT will implement Digital Twins and a Serious Game approach to identify vulnerabilities and test or validate new detection and mitigation models and associated services in a real-time real-life context.

**PRECINCT has 6 key outputs which are:**




# PRECINCT key outputs

1. A PRECINCT Framework Specification for systematic CIs 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 CIs 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.

# ICS: PRECINCT TAKES SOME IMPORTANT STEPS IN MULTIPLE CI CASCADING CYBER-PHYSICAL THREATS 'SCENARIOS' ELABORATION

In the PRECINCT project, the partners perform a state-of-the-art analysis of physical / cyber risk scenarios for threats and hazards in different types of CI. The research was focused on CIs, which are covered in four Living Laboratories (LL), which represent an important focal point of the PRECINCT project research. Due to the proper understanding of the security environment, and especially the studies and solutions carried out so far in the field of identifying complex threat scenarios, the first logical step was taken in the direction of a thorough analysis of the current situation.

The analysis took into account any cyber and physical threat and natural / technological hazards, including threats to humans (e.g. social engineering), and evaluate and sort them out according to their relevance and severity for the LL CIs, particularly in a combined context. Identification of different levels of interdependencies and cascading effects in LLs was also an important step in the scope of the research. With this approach we attempted to identify and analyse the multiple levels of interdependencies and cascading effects, namely the combination of cyber and physical threats / hazards between the critical infrastructures included in the LLs. This analysis also included potential cascading effects (disaster escalation points), elements at risk (assets, installations, plants, employees, neighbouring populations, infrastructure, environmental qualities, etc.), disaster damage magnitude scale, as well as scales for the spatial and social effects from the disaster scenarios under consideration. As the last step of the analysis and findings, it was mainly focused on the specification of representative threat scenarios and related data sources focusing on LL CIs.

The essential findings that we could share with the public due to the sensitivity of the topic and sensitive data are that despite extensive research in this area, it is impossible to identify typical threat scenarios that would be fully applicable to any environment of different CI. Each case of CI due to specific different factors represents a unique example of the development of complex threat scenarios that requires detailed individual analysis. The development of complex threat scenarios is significantly influenced by several factors, such as the security environment (possible attack vectors), the evolutionary stage of the organization that operates CI (vulnerabilities staring points), the development of security processes and business continuity mechanisms, appropriate processes for providing security awareness of all stakeholders in this organizational environment, inter-organizational cooperation, and effective public-private partnership mechanisms with a clear understanding of responsibilities. All these factors play an important role in understanding interdependencies and limiting possible cascading effects in the event of an attack or accident in a particular CI. In a complex and dynamic environment, it is impossible to analyse a single CI capacity without implementing a comprehensive evaluation of impacts on the overall CI system operating in a single geographic entity, such as a city. These findings are particularly reflected in the analysis carried out in the complex LLs of the PRECINCT project. In any case, it is important for assessment to develop appropriate methodological approaches that help to comprehensively understand the situation in different CIs, which are in different forms of interdependence and corelation with each other. In this part, within the PRECINCT project, we continued the already conducted research of past INFRA 01 projects and upgraded new model approaches to threat scenario elaboration that will help in the further development of the planned project activities.

*Dr. Denis Caleta, Aljosa Kandzic, Institute for Corporative Security Studies (ICS)*

# UCD: workshop for Living Labs (LLs) and Serious Games (SGs)

A vulnerability assessment tool is being developed as part of the PRECINCT project in Work Package 3, that will employ Serious Games to identify potential vulnerabilities of the critical infrastructures (CI) to cascading effects and to identify resilience enhancements. The serious game will consist of a platform generating adaptive game scenarios for training and will be used as an experiential learning and training tool for staff involved in the defence of CIs interact and will communicate with back-end simulations & Digital Twins of region/city system of systems.

Stakeholder engagement has begun with living lab partners to determine the nature critical of infrastructure protection training that is currently in place and to communicate plans for the serious game. This exercise will guide the first development cycle of the serious game in preparation for the Beta/ prototype, therefore detailed feedback from the end-users is crucial to this process.

The conceptual design is also being created for the graphical user interface (GUI) and client application which will visualise the threat scenarios to the game players, as well as a various resilience metrics using GIS and a statistics dashboard.

The UCD team would also like to welcome the recruitment of Post-Doctoral researchers Dr. Ili Ko and Dr. Mona Soroudi to the PRECINCT project.

*Dr. Páraic Carroll, Assistant Professor in Transportation Engineering*

# Upcoming events

Participation of PRECINCT project's partners at conferences, exhibitions, seminars, workshops, roundtables  is a very important part of project's Dissemination and Communication strategy. For today we can confirm our participation (speaking, chairing the session, organising the event) in the following events:

**March 2022**

Critical Infrastructure Protection and Resilience Europe (15-17 March 2022, Bucharest, Romania) (project presentation ). Konstantinos Loupos "Preparedness and Resilience Enforcement for Critical INfrastructure Cascading Cyberphysical Threats and effects with focus on district or regional protection"

**April 2022**

2nd ECSCI (European Cluster for Securing Critical Infrastructures) workshop (presentations, chairing the sessions) Jenny Rainbird "PRECINCT: Cascading cyber-physical threats and effects"

**May 2022**

Workshop in Brussels (event organized by PRECINCT). The 1st Workshop should take place at the beginning of May. More details will be available later via PRECINCT communication

**May 2022**

European Security Week (May 2022, Liege Belgium) (project presentation) Lina Kolesnikova "PRECINCT – protecting the infrastructure of Europe and the people in the European smart cities".



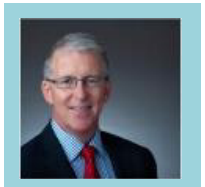
## Meet the project team

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*

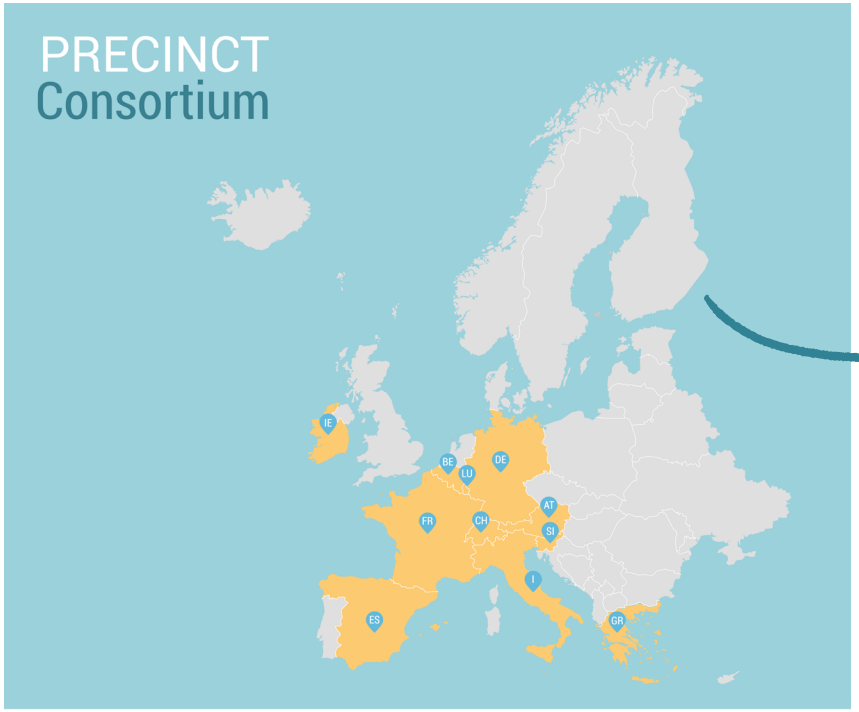
*Mr. Yash Chadha*
*ICP Financial Director*

*Mr. Gerasimos Kouloumbis INLE Innovation Delivery Department Leader*

*Mr. Ioannis Lymaxis*
*PRECINCT*
*LL3 & T1.5 Leader*

*Mrs. Vasiliki Konstantopoulou*
*PRECINCT*
*Technical Engineer*

## PRECINCT members of the consortium (logos of consortium members)




# PRECINCT Members

**Austria**
- AIT Austrian Institute of Technology

**Belgium**
- Vias institute
- VLTN BV
- KU leuven
- POLIS
- European Organisation for Security (EOS)
- CORTE
- IMEC
- Water-link
- Antwerp Police Department
- UITP Advancing Public Transport

**France**
- Montimage
- AKKA HIGH TECH
- Germany
- Nurogames GMBH

**Greece**
- Attikes diadromes s.a.
- KEMEA
- Attiko metro
- Athens International Airport
- Inlecom Innovation

**Italy**
- Fondazione Istituto sui Trasporti e la Logistica
- FSTechnology SPA
- Engineering Ingegneria Informatica S.p.A. (ENG)
- LEPIDA
- Bologna Airport (ABD)

**Ireland**
- Research Driven Solutions
- KONNECTA systems limited
- Inlecom Commercial Pathways
- University College Dublin
- DLR Dún Laoghaire-Rathdown County Council

**Luxembourg**
- Luxembourg Institute Of Science And Technology (List)

**Slovenia**
- Ljubljanski potniški promet d.o.o.
- Institute for Corporative Security Studies (ICS)
- Municipality of Ljubljana
- Slovenske železnice, d. O. O.
- Prometni institut Ljubljana d. O. O.
- Telekom

**Spain**
- Fundación tecnalia research & innovation
- Barcelona Supercomputing Center

**Switzerland**
- CONCEPTIVITY s.à.r.l.

We are eager to share with you our progress and achievements. We hope you enjoy reading about PRECINCT. Please follow us on LinkedIn or Twitter and keep up to date with our news items and downloadable content at www.precinct.info

# 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

## Con-sortium

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

## Type of action

Innovation Action

## Eu-funding

7.996.658,38 euro

## 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)

## Objec-tives

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

# PRECINCT

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

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