PRECINCT

NEWSLETTER

June 2023
Issue #06



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 sixth newsletter and we are excited to tell you all about the work that has been going on from February 2023 to April 2023. The next issue will present further PRECINCT developments, we will reveal the deliverables completed and the progress. We will also give the floor to consortium partners and will keep you informed on upcoming events.

Introduction

By Jenny Rainbird, Head of EU Projects Delivery, Inlecom Commercial Pathways

Disruptions to a city's critical infrastructure can result from several sources including natural hazards, physical and/or cyber-attacks on installations and their interconnected systems.

In recent years there have been an increase in the number and sophistication of combined physical and cyber-attacks on critical infrastructure due to part to their interdependencies.

Transport networks and public transport providers play a key role in evacuation, mobilization of first responders and post event recovery.

The European Commission are supporting a comprehensive approach to address these threats and secure existing and future, connected and interdependent Critical Infrastructure (CI) installations, plants and systems that is accurate, efficient and cost-effective and where possible automated that minimizes cascading effects.



Fig 1: Illustration of the interconnectivity of CI in a city

PRECINCT is one of the 8 projects which was funded under the SU-INFRA01-2018-2019-2020 Prevention, detection, response and mitigation of combined physical and cyber threats to CI in Europe call. Projects were asked to cover "forecast, assessment of physical and cyber risks, prevention, detection, response, and in case of failure, mitigation of consequences (including novel installation designs), and fast recovery after incidents, over the life span of the infrastructure, with a view to achieving the security and resilience of all functions performed by the installations, and of neighbouring populations and the environment".

PRECINCT is also a member of the ECSCI cluster which brings together the H2020 and Horizon Europe projects currently being funded by the European Commission aiming to address critical infrastructure protection and improve resilience in European cities.



Fig 2: ECSCI projects

PRECINCT is addressing the challenge of CI protection and acknowledges that CI operations are at increased risk of coordinated and sophisticated attacks and that these attacks or incidents can have a compounded effect due to interdependencies and non-obvious cascading attacks.

PRECINCT has a vision 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. Enabling interdependent CIs and First Responders / Public authorities to plan for, prevent, absorb, recover and adapt efficiently and effectively to the effects of cyber-physical and hybrid threats / attacks as well as impede their cascading effects. PRECINCT also has the vision of the creation of CIs Coordination Centres with associated collaboration and governance models that link CIs, first responders and other CI stakeholders harmonising CIs emergency processes with command structures and data sharing, thus enabling the quantification and management of resilience via identification and implementation of measures that minimise the impact of cascading effects arising from the interdependencies between different types of critical infrastructures.

PRECINCT has 4 Living Labs (LLs) and three additional transferability demonstrators who have designed scenarios such as bomb/cyber attack, earthquake and physical attacks and against these scenarios will implement the PRECINCT approach to ascertain the benefits and quantify the improved resilience.

The image below shows the PRECINCT Living Lab implementation process which will culminate in the Living Lab demonstrators which will take place in June this year.

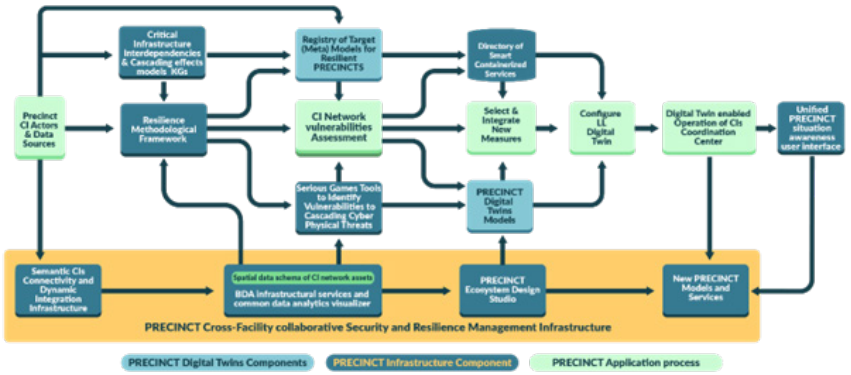


Fig 3: PRECINCT Implementation methodology for the Living Labs

We hope you enjoy this newsletter which contains some interesting updates on our recent developments and notices of forthcoming events.



Capacity building in PRECINCT

By Marisa Escalante Martinez, TCNL

To ensure a wide adoption of the PRECINCT cyber-physical security management platform and supporting tooling by first responders, police and CI stakeholders across the EU is one important objective inside PRECINCT. One of the activities planned during the project to fulfil this objective is to create a PRECINCT Capacity training programme.

This programme covers two main objectives:

1. to present the PRECINCT's concepts, innovation and tooling of the project to a wide audience and
2. to get feedback from the stakeholders that attend the training.

This capacity training programme has been designed in different training blocks, that cover the main technologies and tooling provided in PRECINCT. This approach is due to the different audience for each tool, not all the tool and technologies are for people with the same knowledge or role.

The first session of this training programme was organized inside session inside the 2nd PRECINCT stakeholder workshop hold on November 22nd 2022 at Brussels. During this session a combined training with three training blocks was held.

These training blocks were:
i) Cascading effects and interdependency graphs,
ii) Resilience Methodological Framework and integration with graphs and
iii) Serious games & Serious game storyboard.

The main objectives of this first session were:

- Familiarize audience with the technology: Cascading effects and interdependency graphs; Resilience Methodological Framework and Serious games
- Present an LL Scenario: City impacted by a flood hazard
- Allow trainees to suggest enhancements to the scenario
- Show them the impact of their strategy
- Show them which strategies work and which ones don't
- Obtain feedback of the PRECINCT Results presented

The session was organized as a hybrid session. There were around 60 participants (online and in person). The trainees for this training were Lorcan Connolly from Research Driven Solutions Limited (RDS), Sandra König from AIT (Austrian Institute of Technology), Meisam Gordan from University College Dublin and Marisa Escalante from TECNALIA as moderator. At the end of the training session and the following days, the attendees received a form to get their feedback, in order to analyze it and provide improvements for the coming sessions. The following figures show the overall rate for the training (Figure 4) and how the training was useful for the participants (Figure 5).

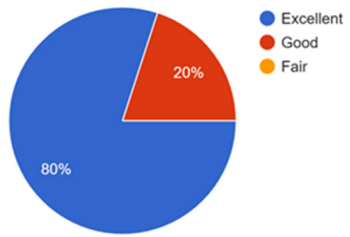


Fig 4: PRECINCT Training Session - Overall rate

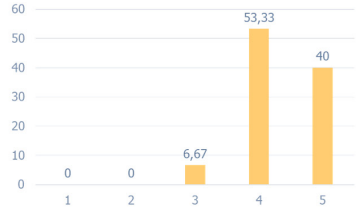


Fig 5: PRECINCT Training Session - Usefulness

The best rated aspects were the interactive/ practical session in the training, the clarity of the presentation, despite the complexity of the content and tools demos and Use Cases demonstration of the tools. Also, some improvements were identified: more time in order to deep more in the examples, show more examples of usage, provide the training material in advance.

The second training programme session was held in Brussels on the 16th and 17th of May 2023. For this next session, it is planned to create other training blocks of the different technologies and tools like: Root Cause Analysis, Complex Event processing, Digital twin and so on.



Railway infrastructure in Bologna

By Emiliano Altobelli, FST

Europe's Critical Infrastructures are nowadays extremely interrelated due to the advanced technological level that allows them to share information and to be connected. However, the high interdependence makes them at the same time highly vulnerable. In fact, if unforeseen events lead to the disruption of one or more infrastructure components the effects ripple out to the interconnected infrastructures, according to a model of cascading effects.

In this context the PRECINCT project aims to identify cyber-physical criticalities by detecting the possible solutions that can be adopted in the real environment and to connect interdependent European Critical Infrastructures with emergency services to manage the security and resilience of Infrastructures collaboratively and efficiently by sharing data, protection models and related new resilience services through Digital Twins models.

FSTechnology represents the railway infrastructure and it has an active role in the Bologna Living Lab. Since September 2022 we have been working together with Living Lab partners to identify physical and cyber criticalities that threaten the main infrastructures characterizing the framework of Bologna. Through the conceptualization and the structuring of the Digital Twins, we are setting up a virtual model in which we can simulate different events (natural hazards, cyber-physical attacks, etc.) and how these events affect the services provided, allowing us to draw important lessons to be exploited in the real world.



Fig 6: PRECINCT Training Session - Usefulness



EOS Considerations on Security of Critical Infrastructure

By Paolo Venturoni, Vincent Perez de Leon-Huet & Giacomo Bianchi, EOS

Recent acts of sabotage against undersea and rail infrastructure represent a wake-up call for Europe. As the international geopolitical situation deteriorates, a greater effort is needed at European Union level to increase the protection of European infrastructure not only against cyber but also physical attacks.

A forward-looking approach based on robust research and innovation funding, leading to targeted programs, is now necessary to increase the level of cyber-physical security of critical assets.

EU-funded programs can make it possible to defragment the security market, increase strategic autonomy, foster the development of a healthy fabric of small and medium enterprises, ensure a better uptake of research results, and facilitate the development of breakthrough solutions in critical areas such as cyber security and artificial intelligence.

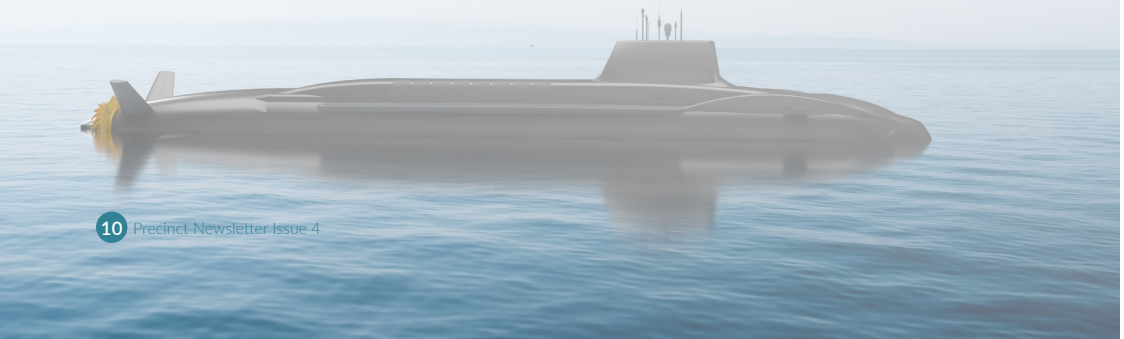
As international tensions increase, the risk of hybrid threats increases as well, in particular in the cyber and maritime domains where the attackers have the advantage of plausible deniability.

Infrastructure in the maritime domain is particularly at risk. Ports, offshore regassification facilities, undersea cables and pipelines, oil and gas rigs, all represent potential targets that need to be protected with cutting edge technological solutions.

Artificial intelligence-based systems must be developed and deployed to ensure the real-time protection of the infrastructure's digital components against cyber-attacks.

Unmanned underwater and aerial vehicles capable of autonomous navigation capabilities are needed to protect sensitive assets such as ports, drilling rigs, regassification facilities and undersea infrastructure.

Integrated command and control systems capable of leveraging satellite surveillance, artificial intelligence, cybersecurity and secure communications solutions, are needed to provide a precise operational picture, detect dangerous anomalies and respond to hostile actions.



What is artificial intelligence and why it matters in critical infrastructure protection?

By José Carlos Carrasco-Jiménez, Ph.D., Barcelona Supercomputing Center

What is intelligence

Artificial intelligence (AI), according to the Stanford Encyclopedia of Philosophy[1], is a discipline dedicated to building "artificial animals" or "artificial persons", or at least something that "appears" to be an animal or a person. In fact, current artificial agents are fundamentally inspired in nature, not only animals or humans; we call these agents bio-inspired intelligence.

But what is intelligence? Aristotle believed that every human being, as well as every object, has a telos, a Greek term that refers to his purpose, goal, end, or true final function. Thus, in achieving its function, goal, or end, a person or object can achieve goodness. For Aristotle, the good of a human being is acting in accordance with reason. This is one of the first references to something close to the idea of intelligence. In Muḥāsibī's theory of intelligence[2], intelligence refers to the ability to act in accordance with the knowledge of what is rational, and rationality demands consistency with the knowledge of Allah. For Thomas Aquinas[3], intelligence is inherent to the human person, and is defined as the act of apprehending something. Aquinas' view on intelligence is fundamentally consistent with Aristotle's idea of reason, but it transcends it by suggesting that "reason alone belongs to the human race, as intelligence alone belongs to God."

In the 1900s, Alfred Binet developed the first modern style intelligence tests. Binet, with a very deficient and limited concept, defines and measures intelligence as the ability to perform everyday tasks such as: naming parts of the body, comparing lengths and weights, counting coins, remembering digits and definitions of words. Further developments in the design of intelligence tests occurred in more recent years, however, what has changed is not the ancient definition of acting in accordance with reason, which is many times misunderstood, but the tasks that are evaluated, for example, basic arithmetic, comprehension, vocabulary, and short-term memory. Intelligence has also been studied from psychological observations, especially in the study of Alzheimer's disease[4] in which several disturbances are observed: disturbance of memory, thinking, orientation, comprehension, calculation, learning capacity, language, and judgement, which are usually associated with intelligence.

Machine Intelligence[5]

From the reasoning of ancient philosophy to the advances in modern neuroscience, intelligence is fundamentally rooted in rationality. However, Stuart Russell and Peter Norvig[6] broadly categorize artificial intelligence into two categories: those based on human behavior and those based on rationality. This definition clearly disassociates rationality from what is human, as

1 https://plato.stanford.edu/entries/artificial-intelligence/
2 https://zoboko.com/text/0eg6wd35/with-the-heart-in-mind/9
3 https://www.newadvent.org/summa/1079.htm#article10
4 https://www.psychologytoday.com/us/blog/hide-and-seek/201811/what-is-intelligence
5 https://www.britannica.com/technology/artificial-intelligence
6 Stuart Russell and Peter Norvig. 2021. Artificial Intelligence: A Modern Approach (4th. ed.). Pearson Higher Ed, USA.

was previously perceived in classical philosophy. In fact, Russell and Norvig suggest that "an intelligent agent takes the best possible action in a situation," which is very suggestive of the disassociation that we have identified between the rational and the human; modern concepts of artificial intelligence are mostly developed from this disassociation. Such disassociation can be philosophically debated, however "acting rationally", as it is understood by Russell and Norvig, sufficiently captures the notion of artificial intelligence. A clear distinction should be made between a rational act for a human being, which is a lot more complex, and a rational act of an object, and in our case, a rational act of an artificial agent, which is measured in terms of a mathematical function. This distinction will help adopters to establish realistic expectations of AI's goals.

Human intelligence, as can be deduced, is too rich and complex to be fully modeled by artificial agents, thus, artificial intelligence cannot replace humans in the decision-making process, at the best, it can exploit computing power, that is, the ability to perform operations on numbers, to uncover patterns that are not evident to the human brain.

Machine intelligence, in other words, seeks to mimic the ability to perform tasks that are commonly associated with human intelligence such as abstracting and generalizing. There is a common interaction between the agent, which is programmed to act "rationally", the environment, which is where de agent navigates to find solutions, rewards, which guides the agent towards achieving what is good to its end (this is what is called "acting rationally" and is commonly modeled as a mathematical function), and the interactions between them (see Figure 7).

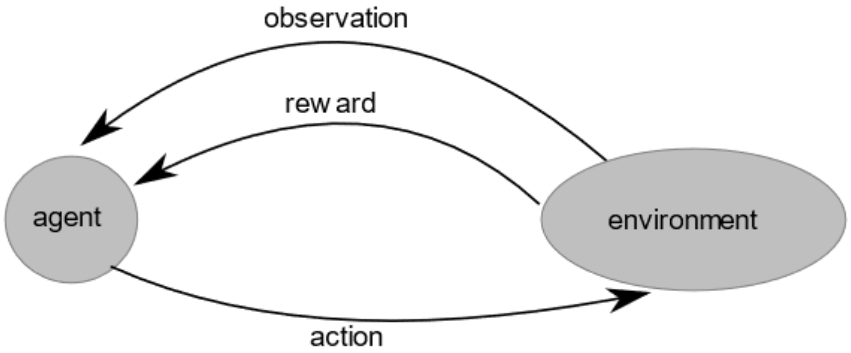


Fig 7: The agent and the environment interact by exchanging information.

Human intelligence, which is associated with rational acts, is also related to how the environment is perceived through the human senses that help us understand and perceive the world around us. Mimicking human rationality, machines have their means to acquire information about the environment (e.g. sensors) and to interact with the world (e.g. actuators).

Artificial intelligence in PRECINCT

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

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

In conclusion, artificial intelligence in PRECINCT seeks to provide critical infrastructure operators with timely information, derived from facts, also called data, that guides human judgement in the decision-making process, including predictive maintenance, what-if scenarios, anticipating any incident and plan its correction. Identifying patterns that help operators bring critical infrastructure assets to their optimal state also translates into a return of investment. Artificial intelligence improves the decision-making process by uncovering patterns that are unseen by the human brain. Despite the number of benefits, AI can also be misused to do the opposite of what we seek to do in PRECINCT, that is, to affect the operations of critical infrastructures. For example, an artificial intelligence chatbot, called ChatGPT, based on supervised and reinforcement learning, has helped to write code to exploit vulnerabilities in industrial systems[7]. This is just one example of the challenges posed when artificial intelligence is used (or misused) which, coupled with a misunderstanding, and sometimes conceptually unrealistic goals, may be the cause for the appearance of reluctant actors in critical infrastructure protection.

7. https://www.wsj.com/articles/chatgpt-helped-win-a-hackathon-96332de4

Combined Cascading Effects Simulation and Resilience Quantification

By Sandra König, AIT

Current research in the protection of Critical Infrastructures (CIs) focuses on more and more on resilience. In PRECINCT, a Resilience Methodological Framework (RMF) has been developed that assesses the resilience of a network of connected CIs. The resilience quantification is supported by a probabilistic Cascading Effects Simulation (CES). The CES uses an interdependency graph that models how the involved CIs depend on each other in the sense that a problem in one CI, e.g., if a service is only partly available, may propagate to the other CI. Based on the knowledge of the local dynamics of each component the CES mimics the propagation through the entire network over time. The availability of a node is described through a state and the local dynamics then describes how this state changes. Information on the resilience may influence the local dynamics, so that the CES can also benefit from the RMF.

In more detail, a combination of CES and RMF yields the following benefits:

1. The interdependency graph provides context and supports quantification of services, which are key steps in the RMF. The simulation results, which estimate direct and indirect consequences of an incident, is relevant information for setting resilience targets.
2. The local dynamics of a node represented by the transition matrix may now depend on information about resilience, i.e., conditional transition probabilities can be used. The intuition behind this is that well protected nodes with increased resilience react less strong to incidents, i.e., the chance that they switch to a bad state is smaller if the resilience increases.

In the course of PRECINCT, the CES tool is extended to capture the described interaction with the RMF[1]. On one hand, all quantities relevant for the resilience computation are stored and collected and the resulting resilience is computed and returned as a result. On the other hand, the network may now contain indicator nodes that describe the resilience level of another (normal) node and hence influence its behaviour.

Figure 1 is an extract from an example from a PRECINCT Living Lab where the RMF uses an Indicator Tunnel to describe the resilience of the tunnel and the availability of resources to measure resilience of the emergency station. In Figure 1, these nodes are shown in red to represent the baseline situation. If resilience is increased, e.g., due to investments, these nodes become yellow or green to indicate that the node they refer to is better protected. Depending on the resilience indicator value, the transitions of the corresponding node changes.

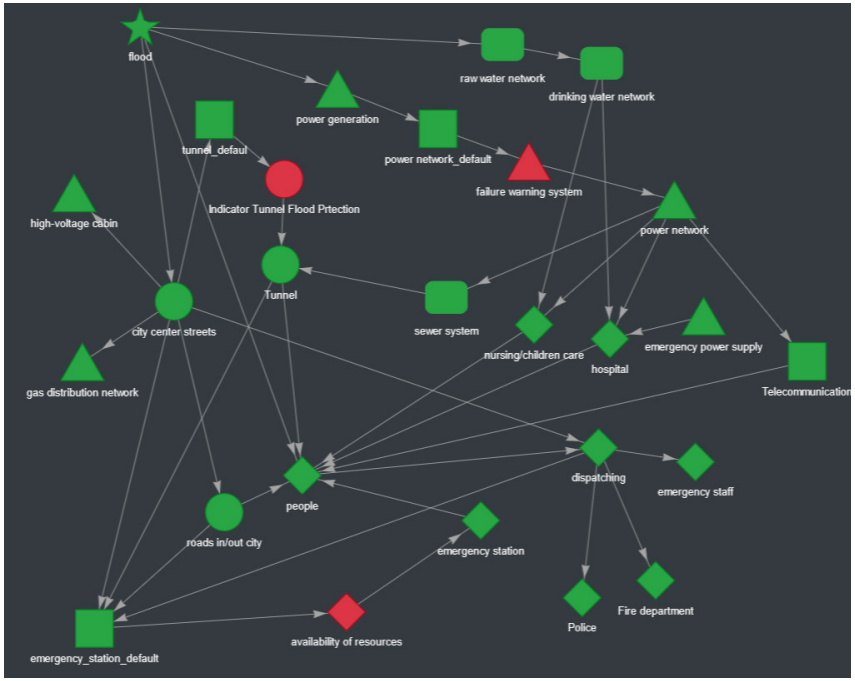


Fig 8: Interdependency graph with resilience indicator nodes (red)

1. https://risk-mgmt.ait.ac.at/prcnkt/#/network

Events

May 2023

On May 16th and 17th, PRECINCT Consortium held its 3rd conference at Brussels, bringing together Policy-Makers, Academia, Industry and CIs operators to discuss on critical infrastructure protection, cybersecurity and crisis management, with experts representing 8 EU projects in the domain. Thank you to the PRECINCT partners and to the representatives of PRAETORIAN, DYNABIC, STRATEGY, EU-CIP, AI4CYBER, EU-HYBNET and SUNRISE Projects.



Fig 9: Group picture of the participants



Fig 10: Shirley Delannoy, Researcher at Vias institute



Fig 11: Giovanni Nisato, Managing Director & Founder of Innovation Horizons; Inlecom Commercial Pathways

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