PRECINCT

NEWSLETTER

February 2023
Issue #05

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

WELCOME TO PRECINCT

Welcome to our quarterly Newsletter.

It is our fifth newsletter and we are excited to tell you all about the work that has been going on from October 2022 to February 2023. The next issue planned for July 2023 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

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 critical infrastructure (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 took on this challenge and particularly considered 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, as illustrated in the figure below.

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 process that the Living Labs are implementing.

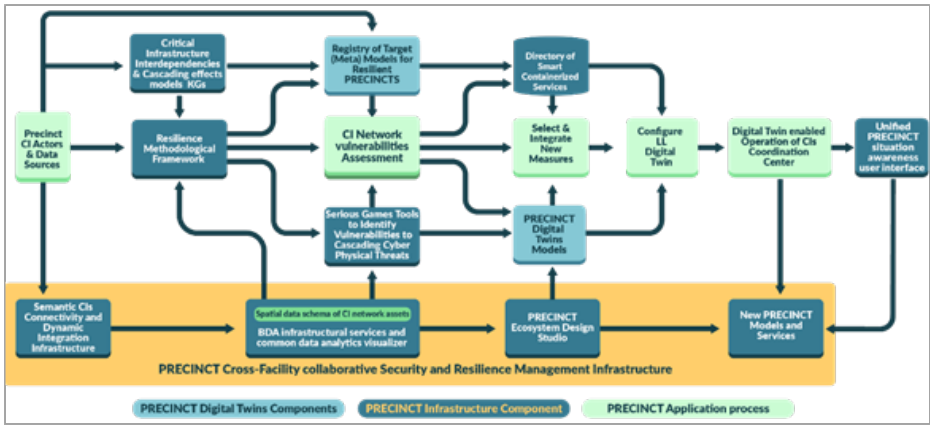


Fig 1: PRECINCT methodology for the Living Labs

Step one which is complete and aims to finalise the Ecosystem participants and the threat scenarios which will be investigated and the associated data sources which will be used. With this in place an initial Ecosystem has been set up using the Semantic CIs Connectivity and Dynamic Integration Tools.

The Living Labs have then moved on to model the Critical Infrastructure interdependencies and develop the Resilience Framework and Serious Games to perform Vulnerability Assessments both at individual CI level and at the coordination level.

In the next phase of the project short and long-term measures that enhance resilience will be identified and sourced either by configuring a PRECINCT CIP Blueprint or procuring additional control by the CI. Then the DT will be configured with the LL specific Solution Accelerators. All participants have access to the situation awareness picture and a number of feedback loops are used. The measurement are obtained to calculate actual KPIs and to feed into Return on Investment economic models.

The image below sums up the key first year results that have been achieved in the project, which is due to finish in September 2023.

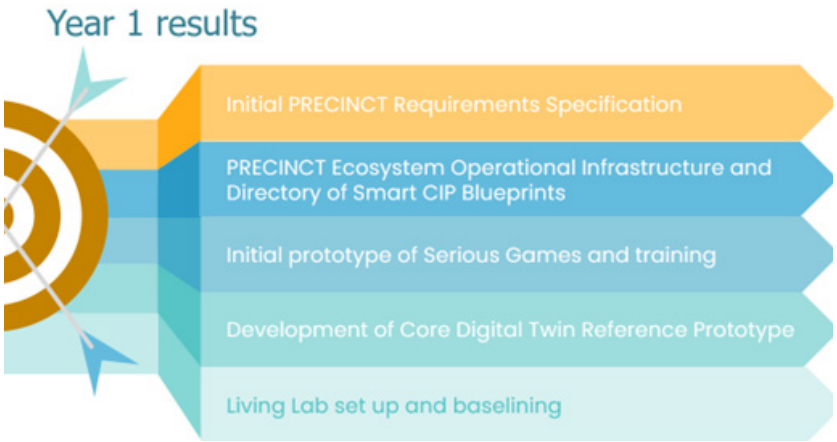


Fig 2: PRECINCT Year 1 highlights

PRECINCT Stakeholders Workshop

By Giovanni Nisato, Innovation and Commercialisation Consultant, Inlecom Commercial Pathways

On November 22nd, 2022, the PRECINCT and PRAETORIAN projects organised a stakeholders' meeting in Brussels. During this event, several PRECINCT partners presented a vision of the future of critical infrastructure protection based on real cases and work being done in the PRECINCT project.

The purpose was to showcase to prospective users a plausible contemporary scenario of cascading CI effects and what the future could look like once PRECINCT solutions are deployed (individually and in combination). This vision was developed within the context of the exploitation of the project results coordinated by Giovanni Nisato (ICP).

Isabel Verwee (Vias) opened the floor with a vision of the imaginary city of "Numenor", in northern Europe. While the city is imaginary, the case is based on work performed in the context of PRECINCT actual Living Labs. The city experiences a flood, which severely stresses several critical infrastructures (transportation, health), triggers a series of cascading events including opportunistic cyberattacks. The city is unprepared and faces a major disaster, from which it takes a lot of time to recover.

The presentation then switched to the future of the same city, in which several solutions were implemented after the disaster, sending "postcards from the future".

Stefan Schauer (AIT) showed that at first each CI can be modelled at high level, their relationships can be captured in an interdependency graph, and by using expert information and data digital twins of individual CI can be built. This modelling enables simulations of cascading effects.

Lorcan Connolly (RDS) then introduced the resilience methodological framework leading to Resilience Index (RI) and Return on Investment (ROI) metrics, which are based on the (economic) service-value provided by the CI. The metrics provide ways to optimise investment and resilience to decisions makers, building on the output from the cascading effects models produced by AIT. The results can be used to examine strategies which are well corelated in terms of both resilience enhancement and investment.

Mircea Iacob (IMEC) explained how a Digital Twin will enable users to better "see" what is happening in real-time, retrospectively, and with some trusted predictions of for example flood or 'what-if' scenarios performed on critical infrastructure nodes. The proposed mitigation actions enable, among others, emergency managers in Multidisciplinary Emergency Operational Command Post (CP-OPS) as well as CI and emergency planners to manage their resources more effectively and efficiently.

Vinh-Hoa La (MON) showed how cybersecurity resilience is increased by a test-and-simulation tool which records real-time data from IoT and telecom networks, simulates their response to realistic cyber-attacks, and tests the boundaries of the devices and services.

Nicola Durante (ENG) presented a Unified Situational Awareness User Interface, including a general dashboard enabling a global view, based on layers, of multiple CIs and their state, providing users access to specific events, in real time and their history, with more granularity.

This "unified" dashboard combines several PRECINCT tools and enables first-responders and emergency managers to have a single landing point to assess the status of the CIs and access its different components.

Ili Ko (UCD) introduced how "serious games" can be used to immerse users in realistic and dynamic simulations of CI in which they can experience "attack" or disaster scenarios and how their responses affect the unfolding of the situations. This increases their effectiveness in case of real emergencies, but also allows stakeholders to uncover un-expected relationships.

Finally, Benoît Baurens (AKKODIS) presented the concept of "blue-prints". These are not physical plans, but rather human and machine-readable IT-templates formally describing the tools deployed, their configuration, their inputs/outputs, and the hosting systems (e.g., on-premises, cloud, hybrid). This can facilitate the deployment, scaling and exploitation of (many of) the PRECINCT digital solutions, enabling the reuse, exploitation, maintenance and sharing of best practices, e.g., from one city or set of connected CI to another that wishes to gain time and experience.

The PRECINCT partners will continue to collaborate to explore how this vision of the future can be realised through the commercialisation both of individual tools and integrated suites of tools developed in the project.

Fig 3: City of Numenor - flooding (Vias)

Fig 4: City of Numenor – CI cascading effects (Vias)

Living Lab Operation: From theory to practice

By Dr. Isabel Verwee, Knowledge Group Manager – Road Safety & Security, and Shirley Delannoy, Researcher, Vias institute

Coordination and overall planning

At the second stakeholders workshop the Work package of the Living Lab operation was explored: from theory to practice.

Within this Work Package the set-up and the coordination of the overall planning of the Living Labs is central. This contains the:

1. Development and implementation of a permanent monitoring learning system.
2. Organization of four Living Labs in Ljubljana, Antwerp, Athens and Bologna.
3. Organization of Transferability Validation Demonstrators (Luxemburg, Dublin & Tallinn)
4. Development and implementation of a measurement and validation system.

Within the PRECINCT project, the Living Lab methodology is implemented.

A Living Lab methodology

A Living Lab (LL), in contrast to a traditional laboratory, operates in real-life context with a user-centric and multi-methods research approach. Within the LL methodology, the users and stakeholders from public-private domains are involved and play a key role in the development and innovation research, based on the principle of co-creation. These interdisciplinary experts are brought together to develop, deploy and test technologies in the LL. This user centered-research methodology is used for the development, implementation, monitoring and evaluation of the PRECINCT Ecosystem. This research methodology of Living Labs is about integrating research and innovation into daily practice and regularly adapting it to its daily practice.

The PRECINCT ecosystem is developed in close collaboration with the several public-private partnerships in the 4 Living Labs and with respect to the user needs.

In other words, A LL is a dynamic process in which developers, implementers and end-users are working in close interaction with each other.

Objective

Vias institute coordinates the Living Lab activities as a whole and the Living Lab of Antwerp in particular. The Precinct Ecosystem Platform connects stakeholders of interdependent CIs and Emergency Services to collaboratively manage security and resilience exploiting Digital Twin, Serious Games and AI technologies. The objective is to improve CI protection for specific installations from vulnerabilities arising from interdependencies and cascading effects.

The validation scenarios, based in four large scale Living Labs and three transferability demonstrators, will result in ready-to-use tools. Increased automation and accuracy in security and resilience management will reduce costs and increase efficiency for CI management. The main societal benefits include enhanced overall physical security and safety levels, as well as data protection for personal and organizational information.

Living labs

Fig 5: Map of the PRECINCT Living Labs

LL2 Antwerp – Resilience to flooding

By Helen Witvrouwen, Police Commissioner - Police Zone Antwerp, Nele Daels, Functional Analyst - Imec, Daan Buekenhout - KU Leuven, and Nico Dies, Teamleader Maintenance - WaterLink

Thematic focus: Emergency Services coordinated through CIs through city level Digital Twin

Key stakeholders: Police Zone Antwerp, Waterlink, IMEC, KULeuven, coordinated by Vias institute.

Vias institute coordinates the LL of Antwerp. The purpose is to align all Living Lab partners in order to execute the Living Lab focusing on flooding and disastrous consequences of global warming with cascading effects on the water CIs and its impact on other CIs.

Going from theory to practice in this Living Lab is achieved by a clear definition of the partner's roles. Significant time has been spent in the identification of the CP-OPS needs, data collection, and the modelling, and the implementation of the digital twin. The challenges are related to defining the scope of the threat, the flooded area, the impact of cascading effects (police and utility operators) and the scoring and prioritization of the used and combined data.

Concretely, the scenario is:

"Currently, when very high rainfall is forecast and there is a chance of flooding, certain departments of the city of Antwerp, the fire brigade and the police contact each other. Based on the forecasts, these organizations carry out contingency planning based on past experience with the limited data available. If a large number of these organizations engage and parts of the city are at risk of flooding, a CP-OPS will be established. Within this CP-OPS, representatives from 5 disciplines sit together (the group may be supplemented by experts). They will coordinate the response to the disaster. They will do this in a multidisciplinary way. This CP-OPS is directed by a DIR-CPs. He or she should have an overview of the situation and across disciplines. When we have tools to show us what the predictions are in the near future, we can tailor our decisions, accordingly, allowing for better and more efficient decisions. Better allocation of our people and resources is a huge asset at such a time. An overview will be created, making consequences for critical infrastructures clear.

During PRECINCT, we have already conducted a number of interviews with stakeholders. From the different disciplines, mostly the same benefits emerged or the same 'missing links' at the moment. We are convinced that with the help of this project, several 'missing links' could be solved. And in order to support the decision making process, the pedagogical approach offered by the Serious Games is of real added-value"

Within Living Lab Antwerp, **Imec** is responsible for the digital twin. The digital twin will, first visualize the flood forecasting model output in Antwerpen. The predicted flood water levels will be shown, but also the effects of the flood on certain critical infrastructure (CI) and the cascading impact of this on other critical points in Antwerp hence giving an earlier insight for the CP-OPS to react.

A second part of the digital twin gives the CP-OPS also the insight in the what-if scenarios. When there is no flood at the current moment, the digital twin gives the possibility to look at "what would happen" if a certain CI would be flooded, what would be the cascading effect and secondly, how could the resilience be improved of this critical infrastructure. The latter is done by calling another model (resilience supervisory control model) that calculates the mitigation actions on a certain CI that got impacted.

KUL is developing a pluvial flood hazard assessment and forecasting component for the digital twin. This component is based on a novel concept of surrogate and hybrid modelling. This surrogate modelling approach makes use of machine learning tools to quickly obtain pluvial flooded zones based on meteorological data. The model training is based on a large number of simulations with a detailed full hydrodynamic model for the urban water system of the city, considering a large variety of meteorological boundary conditions including extreme rainstorms for different occurrence frequencies. This detailed, yet slow, model is based on the hybrid concept where the one-dimensional underground pipe system is bidirectionally coupled with a two-dimensional surface inundation model for the above-ground system. It is validated based on crowdsourcing data and crisis interventions by the fire brigade during recent pluvial flood events.

(a) (b) (c)

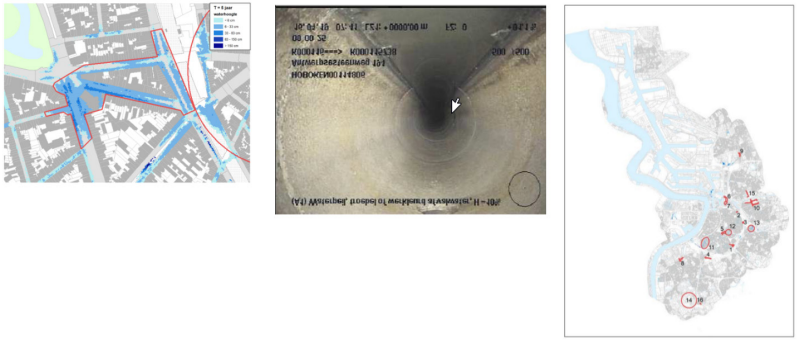


Fig 6: Sewer System and Water Cis in Antwerp. (a) Close up on Antwerp Street, blue color indicates inundated zones when lot of rain (b) Inspection inside a drain; (c) the 16 bottlenecks identified in Anwerp.

Waterlink will provide to the LL Antwerp information of the sewer system of the city of Antwerp based on their own GIS AQUAWARDS OPERATE.

Water-link is also sharing their real-life experience. This experience has helped identifying 16 bottlenecks for the city of Antwerp. In this way, the project team is able to compare the result of the digital twin with the real-life treats. Water-link hopes the digital twin will give extra insights to solve the problem of the 16 bottlenecks in the future.

The partners of the LL Antwerp stipulate as the biggest added value to gather new insights from the digital twin to prevent flooding in the city of Antwerp. Besides it will generate awareness of cascading effects and impact of flooding towards authorities and it offers and extra layer of data for the prioritization of new projects to optimize the sewer system for the future climate change.

Living Lab Athens – Objectives and Transport Resilience overview

By John Limaxis, Technical Project Manager, Inlecom Commercial Pathways

Thematic focus: Increased resilience against cyber-physical incidents affecting urban transport

Key stakeholders: Athens International Airport, Attiked Diadromes S.A, Attiko Metro S.A., KEMEA, coordinated by Inlecom

During PRECINCT 2nd Stakeholders Workshop Inlecom and KEMEA provided an overview of PRECINCT LL3- Athen's key objectives and activities so far. The presentation was kicked off by Inlecom, who is leading the coordination of PRECINCT LL3, by introducing the nature and expertise of LL3 Stakeholders and transport CIs. Following that, the Threat Scenarios developed by PRECINCT LL3 partners were introduced to the workshop's participants, along with the main challenges and problems identified by LL3 CIs operator in managing and mitigating such critical situations. Subsequently, the presentation focused on the implementation of PRECINCT project methodological framework and technological outputs by LL3. This included a presentation LL3 work for quantifying Athens Transportation Network Resilience Index and the vision for Athens Transportation network Knowledge Graph, aiming to ingest and interlink LL3 heterogeneous data and information for enabling CI's operators to respond faster or in automated ways.

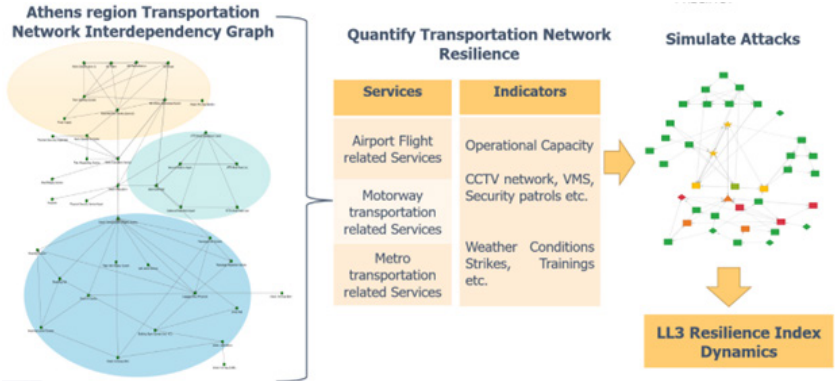


Fig 7: Living Lab Athens Interdependency graphs, KPIs indicators and Resilience index

KEMEA introduced the Hellenic Coordination Center for Critical Infrastructure Protection (H3CIP) in the second part of the presentation. H3CIP will be demonstrated in the Athens Region Transport Resilience Living Lab with the goal of providing a common operational picture in near-real time to all stakeholders connected to the 3HCIP platform; supporting the exchange of information among participating AMETRO, AIA, ATTIKES DIADROMES operators during an incident; and facilitating coordination among the involved stakeholders during a crisis.

Concluding, the ultimate purpose of LL3 operations is to utilize the PRECINCT ecosystem in order to leverage CIs security and enhance communication and coordination among the interconnected CIs and first responders in view of a major incident.

Living Lab Operation – Project KPIs baselining activities

Dr. Isabel Verwee, Knowledge Group Manager – Road Safety & Security, and Shirley Delannoy, Researcher, Vias institute

Within PRECINCT activities are dedicated to the performance evaluation of the PRECINCT components in the context of the four Living Labs considering the defined user requirements and KPIs and the project's strategic objectives.

In that context, one of the initial tasks was to obtain baseline measurements for the project KPIs, to evaluate their improvement at the final stage of the project. The KPIs that were measured at that stage were the ones more closely related to the PRECINCT technical infrastructure, since this made sense in order to evaluate the potential improvements.

In particular, these were:

1. Improved capabilities of end users to manage cyber-physical threats more efficiently
2. Improved operational resilience in the Living Labs regions (as a result of benchmarking the PRECINCT Ecosystem)
3. Improved accuracy in cyber-physical threats detection
4. Improved "Resilience Index"
5. Increased speed in mitigation and reaction
6. Increased ROI estimated by economic models for specific CI types

For each of these KPIs, a series of discussions between technical partners and LL stakeholders took place, in order to define a common approach for obtaining their baseline values in the Living Labs. Finally, after the baselining strategy was set, the LL technical partners applied it in each LL and the overall obtained measurements were consolidated and reported in one of the project deliverables.

Besides an evaluation of the PRECINCT framework in terms of user experience and the potential of acceptance based on structured interviews and standardized questionnaires is foreseen.

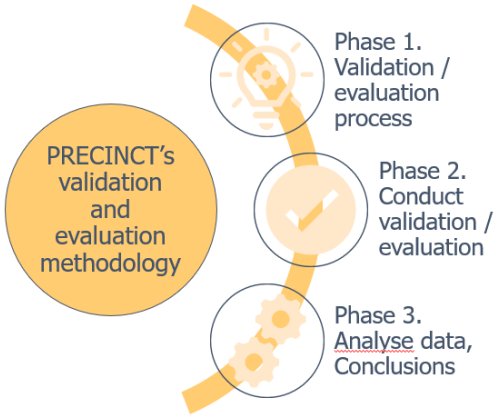
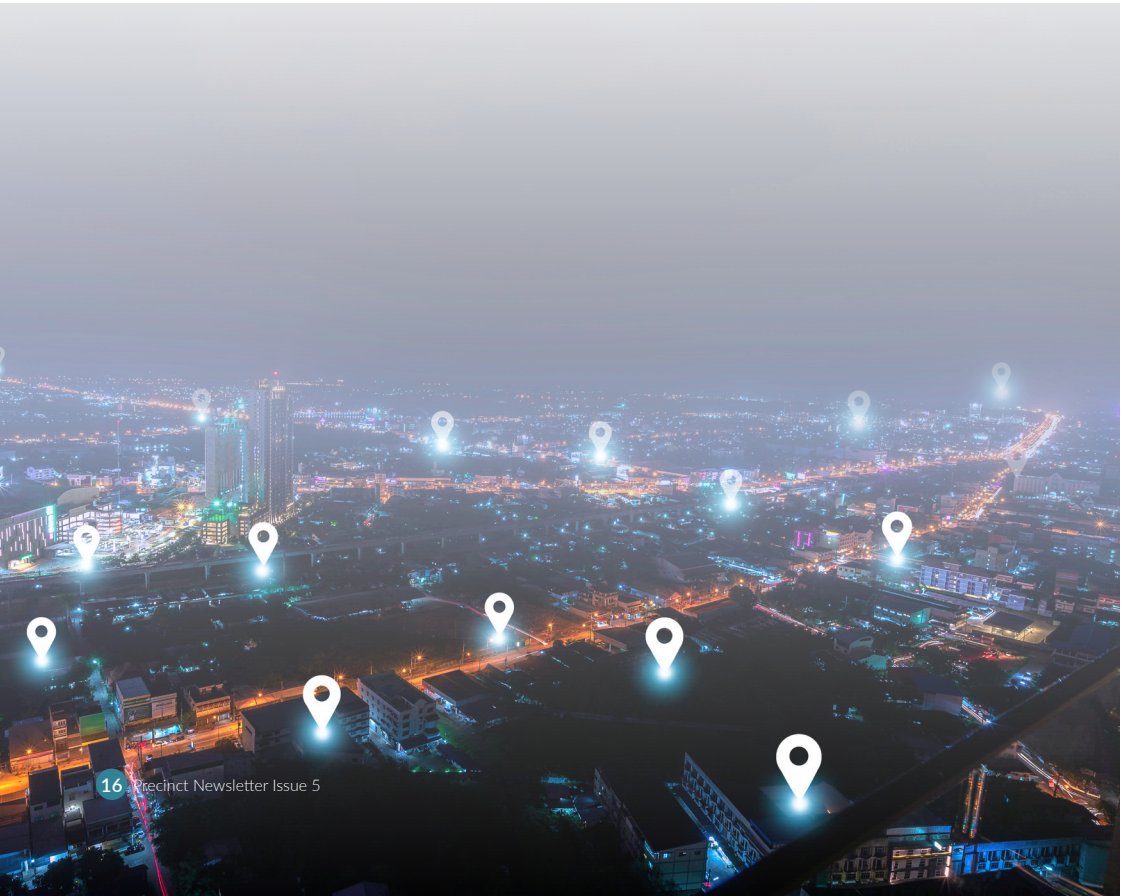


Fig 8: PRECINCT validation and evaluation methodology (by KEMEA)



Framework of standardization in the sector of critical infrastructure

By Cristiano Passerini, CTO Emergency Response Division, and Sandra Mattarozzi, Senior Researcher & Project Manager, Lepida

The "physical" 2nd Stakeholder Engagement Workshop has been a strategically well-planned event to discuss and increase the awareness in the context of standardization opportunities stemming from the PRECINCT Project. Indeed, it was of great impact sharing with the colleagues of the "twin project" PRAETORIAN both the overall status and the views in the field of standardization.

The opportunity of joint presentations within a specifically tailored session event has paved the way to share a common language and lay down the basis for the understanding of what standards for critical infrastructures resilience improvement could be.

The focus point of Lepida presentation has been on the framework of standardization in the sector of critical infrastructure, the most recent approaches in this area and the perspective that are in the view of the European Union. But the main focus has been on the lesson learned in the first year of the PRECINCT Project.

Thus, it has been acknowledged that each of the partners involved in the Living Labs has its own understanding of what the critical flow are from their own standing point. Also, each partner has its own understanding of what the other partners flows represent. It has therefore been learned that crucial issue to address is that this second understanding may be biased, because of the own interpretation and the own specific knowledge of the partners' critical flows. Therefore, the great contribution arising from the two projects is to suggest to each LL partner to understand the relevance of the other partners data and flows in the correct terms that is the ones that the latter assign to them.

As a consequence, a peculiar approach about the needs of standardization has arisen from this picture. This approach relies in sharing a taxonomic description of the flows of data of concern to the parties of each LL. In concrete terms, the first standardization step appears to be the definition of meaning and the properties of data to be collected, as required by the partners of the Living Labs to improve their own processes. Specifically, each Chief Information Officer (CIO) must become aware that some data it doesn't care about must however be collected for the sake of more performing resilience of the other partners CIs. E.g., the measure of the number of long-term standing wifi devices connected to an access point might be a useful measure of queuing passengers unable to leave a site. That measure is of poor relevance for a telecommunication operator but could be possibly collected in order to improve the overall resilience of the ensemble of Critical Infrastructures.

As CIOs cooperate in the collection of data relevant to the other LL parties and stakeholders, the overlaying view of the concurrent CIOs aiming at an increased resilience in the Living Labs can be alternatively seen as a graph of the interactions among the CIOs to exchange the data collected by the other parties and the processes that lead to the use and analysis as well interpretation of those data in order to increase the resilience of the overall system.

This can be thus seen as the aim of standardization, possibly to be analysed further in other projects: a taxonomic description of CIs data and a network-based description of data consumption by other CIOs cooperating in the joint scenario. In this perspective, the ground-breaking activity developed by the INSPIRE Directive poses EU in a prominent position in the development of such a taxonomic model specifically devoted to Critical Infrastructures

This can be thus seen as the aim of standardization, possibly to be analysed further in other projects: a taxonomic description of CIs data and a network-based description of data consumption by other CIOs cooperating in the joint scenario. In this perspective, the ground-breaking activity developed by the INSPIRE Directive poses EU in a prominent position in the development of such a taxonomic model specifically devoted to Critical Infrastructures.

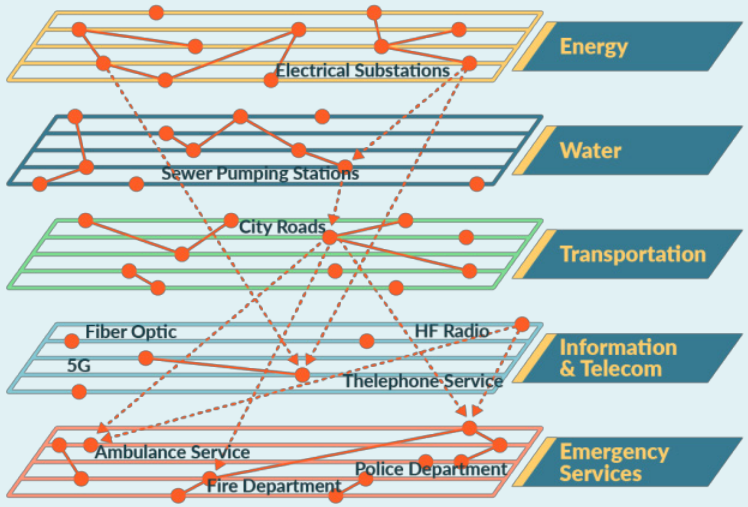


Fig 9: The CIs interconnect among each other at the specified nodes and exchange a set of taxonomically defined data as well as the rules of use and analysis. A superimposed networks then may be used to describe the flows of these data

Standardization within PRECINCT

By Giacomo Bianchi, Project Manager, EOS

During the second PRECINCT stakeholders' engagement workshop, a session concerning the topic of standardization was held. The session, which saw the participation and involvement of the EC funded projects STRATEGY and PRAETORIAN, as well as PRECINCT, is to be considered as the first appointment for discussion and confrontation on a very important and sensitive topic.

Moderated by Giacomo Bianchi of EOS, PRECINCT WP6 leader, the session had the honour of hosting three experts in the field:

- Cristiano Passerini from LEPIDA, PRECINCT project partner. Cristina held a PhD in Engineer in 1997, and he worked during the years in Radio Channel modelling for 3G systems, Radio Spectrum policies and management, EM Field measurements for public safety and international broadcasting coordination within CEPT and ITU.
- Tamara Hadjina from Končar-Digital, and PRAETORIAN project partner. Tamara is the manager of research projects in the field of cyber security of critical infrastructure at Končar-Digital. She participates in all development activities of Končar-Digital in the field of cyber security of industrial control systems. Tamara graduated and received her Phd from the Faculty of Electrical Engineering and Computing at the University of Zagreb. After completing her studies, she was employed at the faculty's Department of Control and Computer Engineering, where she worked as a research associate in the Laboratory for Renewable Energy Systems.
- Pertti Woitsch from Woitsch Consulting Ltd., and STRATEGY project partner. Mr. Pertti Woitsch is an experienced defense & security industry professional with wide experience in international sales, marketing, and business development with more than 40 years of business experience in a broad range of innovation driven industries. Pertti studied physics and computer science at the University of Helsinki. Pertti has a special interest towards standardization, having acted in various positions at CEN, CENELEC, ISO and IEC. He currently works as CEO at Woitsch Consulting Ltd., a Helsinki based advisory firm with focus on consulting services to the industry, national public authorities and the research community, including EU-funded research projects.

The standardization session has set itself goals to pursue, such as i) Analyse and discuss existing effort in standardisation in Critical Infrastructure; ii) Present activities carried on in EU funded projects involved in Critical; iii) Present standard under development in the Critical Infrastructure; iv) Analyse possibility of; v) Create the basis for standard improvement or creation of new ones in Critical Infrastructure areas.

The presentations of the three experts covered the role of standardization in their respective projects, underlining the activities, challenges and objectives set. The session showed how the topic of standardization, especially in crisis communication, is not only a topical issue, but a fundamental as common standards for emergency communication are still missing and a lack of testing and validating standards in organizational and technical interoperability in

realistic environments are still present. Common points and joint activities have been found and planned, in order to have a common approach to the theme for the continuation of the projects.

Fig 10: Standardisation panel at the PRECINCT workshop

Fig 11: Standardisation workshop, summary of next steps

The PRAETORIAN Project

By Tamara Hadjina, Research Project Manager, Končar-Digital

PRAETORIAN project strategic goal is to increase the security and resilience of European CIs, facilitating the **coordinated protection** of **interrelated CIs** against **combined physical and cyber threats**.

PRAETORIAN focuses standardisation activities on the standardisation of the solutions that are part of the developed PRAETORIAN platform:

- open architecture,
- components,
- interfaces,
- data exchange formats.

Fig 12: PRAETORIAN project standardisation objectives

Project partners are diligently following the activities of ISO TC 292 (Security and Resilience) WG3, WG5 and WG6 in order to find a way to provide input related to emergency management, community resilience and protective security.

PRAETORIAN (through participation of partner ETRA) was accepted to join the CEN Workshop Agreement on '**Improvement of information processing in crisis management of critical infrastructures for computer assisted data gathering, display and reporting**' which should have two outcomes:

- CWA 1- Semantic layer definition and suitability of EDXL-CAP+EDXL-SitRep standards for crisis management in Critical Infrastructures
    - Provides a formal definition of the parts that comprise the messages transmitted during a crisis. Those messages include data coming from sensors, but also other intelligent software modules. à Related to PRAETORIAN PSA, CR and IOP
- CWA 2- Emergency management – Incident situational reporting for Critical Infrastructures
    - Defines the information exchanged and a common template of reporting incidents of certain significance that affect Critical Infrastructures à Related to PRAETORIAN CR

PRAETORIAN partners have representatives in IEC TC 57, in the working groups responsible for developing IEC 62443 and IEC 62351 standards, both of which are industry standards dealing with automation and control systems cybersecurity. Through those representatives we plan to give our contribution to the development of new versions of the respective standards, all based on the experience and development carried out during the PRAETORIAN project.

PRAETORIAN Pilot scenarios

By Eva Muñoz Navarro, Project Manager, GRUPO ETRA

The PRAETORIAN toolset will support the security managers of Critical Infrastructures (CI) in their decision making to anticipate and withstand potential cyber, physical or combined security threats to their own infrastructures and other interrelated CIs.

The end users of the solutions developed in PRAETORIAN are the stakeholders who will be able both to operate PRAETORIAN technology and to understand it in a context of CIs facing cyber-physical threats and civil security protection applications: CI security practitioners, First responders and Law Enforcement Officers. PRAETORIAN is a CI-led, user-driven project, which will demonstrate its results in three international pilot clusters –some of them cross border– involving 9 outstanding critical infrastructures: 2 international airports, 2 ports, 3 hospitals and 2 power plants. Moreover, three FRs teams are also involved in different scenarios:

- **French scenario**: the Bordeaux Port, a major facilitator in supplying petrol and gas in the country, plays a key role since it is one of the strategic targets for attacks. In the same area near the port a power plant is located, that produces energy at full capacity and supplies the city of Bordeaux with electricity along with several Critical Infrastructures such as the hospital, the port itself, the airport, etc.
- **Spanish scenario**: it is the Mediterranean cruise high season, and the cruise terminal at the Valencia Port is operating at full capacity having big cruises docked at the port with more than 6.000 persons on board. A coordinated group of terrorists are planning a combined attack (cyber and physical) on the Valencia port to cause severe damage to the port facilities, kill the largest number of persons possible and provoke an economic crisis in the Valencia region. Both the Valencia airport and Hospital La Fé (largest hospital in the region) will be impacted by this attack.
- **Croatian scenario #1**: a Croatian Hydro Power Plant has stored a big amount of potential energy: the energy demand is lower than its usual level and water level in both the reservoir lake and the downstream water are high. A terrorist group, with the main purpose to unbalance the Croatian energy network, decides to act. The HPP is located higher along the same river as an Austrian hospital, which will be impacted due to a blackout produced in the whole region, and also by extensive rainfall provoking a flood.
- **Croatian scenario #2**: a Laboratory in Graz is targeted by a group of terrorists. They will be able to steal some samples they will use as bioweapon, and move with them to the Zagreb airport with the intention to use it both inside as well as using drones. Also a cyberattack in the lab will be produced.

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