PRECINCT

NEWSLETTER

July 2022
Issue #03

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 third newsletter and we are excited to tell you all about the work that has been going on from April to July 2022. The next issue planned for December 2022 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.

Opening word from the management team

Mrs Jenny Rainbird, Head of EU Project Delivery at Inlecom Commercial Pathways and PRECINCT Project Manager

As we reflect on the PRECINCT project to date, we can be truly proud of our achievements. In only 9 short months, the 40 strong partnership has worked hard together to achieve all expectations with regards to milestones and deliverables and has been actively promoting the project through numerous international events.

The team have been actively engaged with Critical Infrastructure stakeholders over the period and concluded much of the work related to stakeholder requirements gathering including completing the stakeholder needs analysis and capturing the multiple Critical Infrastructure cascading cyber-physical threats scenarios. The team have also worked on capturing the stakeholder's technical requirements, analysing the standardisation potential of the project and understanding stakeholders' business requirements which you can read more about in this edition.

Indeed, the work that has been carried out with the stakeholders to finalise the PRECINCT Digital Twins architecture and defining the User-Story mapping in each of the project Living Labs is almost complete.

Planning for the PRECINCT living labs is well underway, with the baseline measurements activity in progress and the kick off of the LL1 Operation Ljubljana and LL2 Operation Antwerp in progress.

This newsletter will provide insights into some of the technical work that has been underway including development of the Resilience Methodological Framework, integration of Knowledge Graphs, a systemic approach for Information System Security Risk Management supported by Enterprise Architecture Management and the concept of self-protection strategies for cyber threats.

I hope you enjoy this newsletter and join me in congratulation the team on their achievements so far.

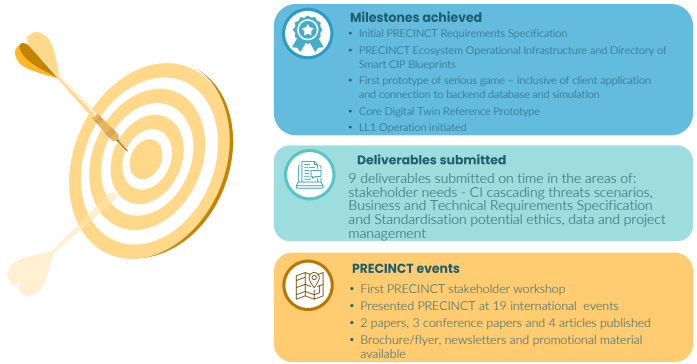

Fig 1: PRECINCT achievement highlights.

Resilience Methodological Framework

Lorcan Connolly, Associate, Research Driven Solutions

The PRECINCT Resilience Methodological Framework provides a quantitative measure of resilience for multimodal CI systems exposed to cyberphysical threats. The approach will be used to quantify resilience in each of the four project Living Labs. The consideration of a single measure of resilience across multiple CIs is a complex concept. Within PRECINCT, resilience is measured in terms of the service provided by each CI within the system. Examples of measures of service are theoretically unbounded, but some examples include the passenger miles carried by a railway network, availability of 50MB broadband by a telecoms network, or supply of electrical power in kWh. Measures of service related to safety and cost of interventions after hazards are also included. All measures of service must be quantified in monetary terms to allow cross consideration of the resilience. This is not a trivial matter and all key stakeholders should be engaged within the context gathering phase.

The PRECINCT Cascading Effects and Interdependency Graphs are an integral part of the Resilience Methodological Framework. In the first instance, interdependency graphs for the CI provide the context for the problem. Subsequently, when quantifying the baseline service, the interdependencies in services are quantified. When quantifying the resilience of the CI system to various cyber physical hazards, resilience indicators are used to describe the resilience relevant parts of the system. At this stage the interdependency graph is used to quantify the relative impact (weight) of each indicator on the overall measure of service.

The final step involves the setting of resilience targets based on stakeholder issues, legal requirements and Cost Benefit Analysis (CBA). CBA requires the calculation not only of the cost of resilience enhancements, but also the impact in terms of the savings made in the event of a hazard occurring. This is achieved by examining the probabilistic damage states within the cascading effects simulation, given a hazard of specific magnitude.

Resilience indicators can impact the Absorb phase (how an asset will react during a disruptive event) or the Recovery phase (Consequences after a disruptive event). Once resilience enhancements have been put in place, it is essential that ongoing monitoring records the service measures and resilience calculation over time, before, during and after subsequent disruptive events. The PRECINCT Resilience Methodological Framework was built from the foundation of the CEN CWA publication “Guidelines for the assessment of resilience of transport infrastructure to potentially disruptive events” but was enhanced to consider the interdependent impacts of cyber-physical cascading effects on interdependent CIs.

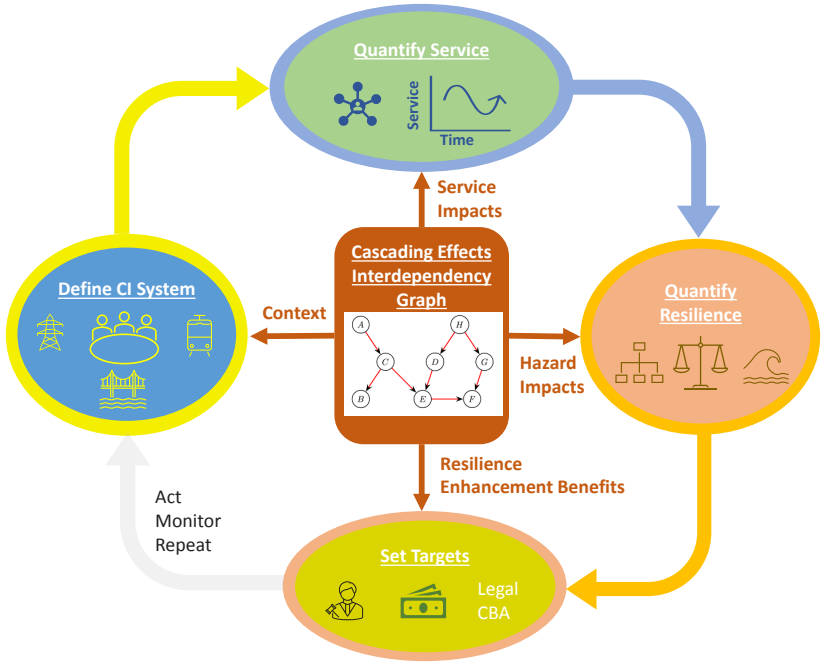

Fig 2: Resilience Methodological Framework.

What do Users want from Critical Infrastructure Protection solutions?

Mark Bennett, Senior Innovation and Commercialisation Consultant, Inlecom commercial Pathways (ICP)

The PRECINCT project was initiated on the premise that there was an unmet need amongst users of Critical Infrastructure Protection (CIP) solutions for a suite of tools that would bring clarity in a complex world of combined cyber physical threats and cascading effects between critical infrastructure assets.

Inlecom Commercial Pathways (ICP) tested that assumption early in the project by engaging with customers/users – initially through a questionnaire and then through a series of workshops. The aim was to try to understand what users saw as their key business requirements and then to prioritise what the project should focus on to meet those needs. Some of the most interesting results from the questionnaire are shown below:

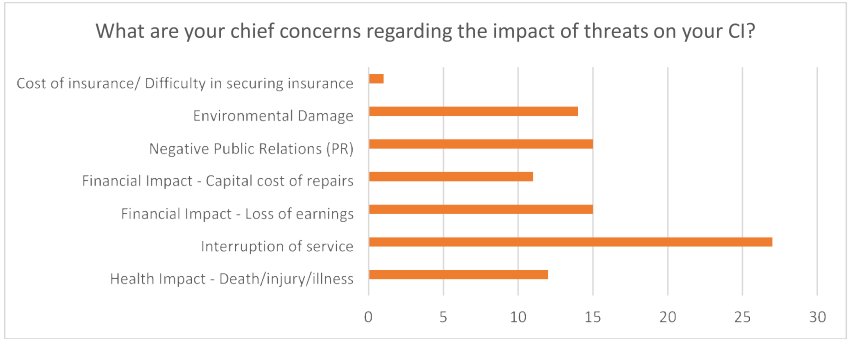

Fig 3: Concerns regarding impact of threats on CI.

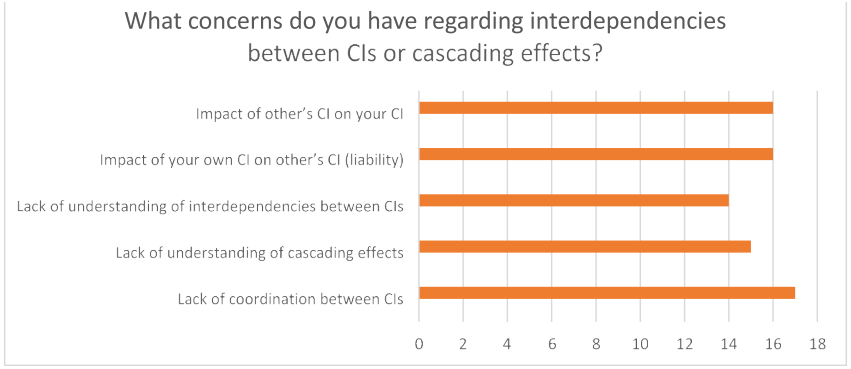

Fig 4: Concerns regarding interdependencies.

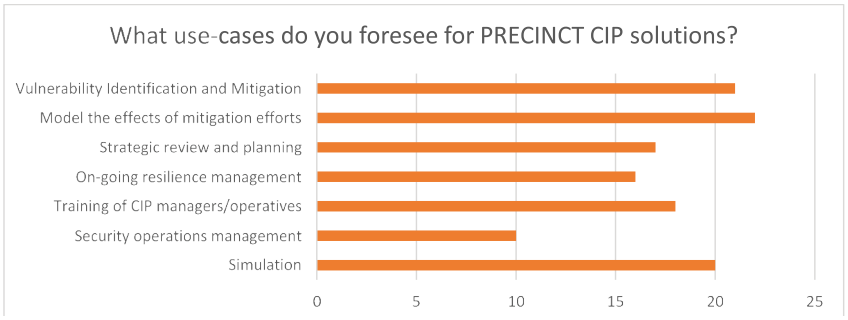

Fig 5: Use cases Precinct solutions..

To get a clear understanding of the different types of Users and their different requirements, ICP:

- analysed the CIP value chain,
- identified three distinct User Groups: 1) Critical Infrastructure Operators, 2) Emergency Services Managers and 3) Regional/National response coordinators, and then
- developed Value Proposition Canvases for each of those User Groups based on the User feedback. An example of one of these canvases – a visual means of representing user needs and how solutions may meet these needs - is shown below:

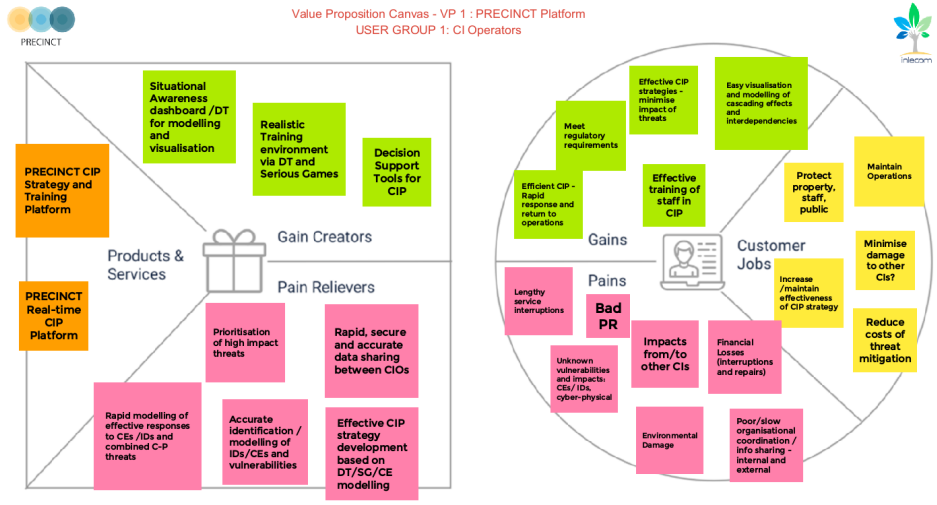

Fig 6: Value proposition canvas.

From the user feedback and value proposition analysis, ICP developed a detailed set of Business Requirements. Having reviewed the priorities expressed by the users, it was recommended that PRECINCT should focus its development efforts to meet those needs by:

1. Developing a predictive, strategic CIP tool in the first instance that enables CIP professionals to plan for measures to increase their resilience to potential complex threats.
2. Development of a user-friendly interface that both radically simplifies the visualisation of complex cyber-physical threats and serves as a CIP Decision Support Tool to enable CIP users to optimise decision making to increase resilience.
3. Development of tools that enhance understanding and awareness of CEs/IDs and enable coordination across organisations to increase resilience to such threats.
4. Developing the capability to identify mitigations that result in a swift return to operations and/or identify other prioritised impacts.

This assessment should be seen as an initial baseline of the business requirements of Users and will be reviewed and updated as we progress through the project and test the PRECINCT solutions in the Living Labs.

Are you a user? What do you think? We also would like to invite other users to give their feedback. Please contact us at: mark.bennett@inlecomsystems.com.

PRECINCT self-protection from cyber threats

Edgardo Montes de Oca, CEO, Manh-Dung Nguyen, Research Engineer, Vinh Hoa La, Research Engineer - Montimage

Today's critical infrastructures (CIs) are strongly interconnected and reduced operation of one or more may affect others. CIs are increasingly at risk from natural hazards and cyber-physical attacks. Security and resilience are therefore principal concerns for the design and construction of modern CIs. Self-protection is becoming increasingly important and has been identified as one of the essential properties of self-management for CIs. Combined with Digital Twins (DT), self-protection, like other self-* properties (i.e., self-optimization, self-healing, self-configuration), allows CIs to adapt to the changing environment without human intervention, and thus become responsive, cost effective with a high degree of security.

In PRECINCT, Montimage contributes to define and implement self-protection strategies that can be deployed in the real system to improve the management of the security and resiliency. Firstly, it is important to establish a definition of self-protection property to clarify what we have considered to be self-protecting CIs in this project. Secondly, as different Living Labs (LLs) have different requirements and needs, we should develop a generic self-protection solution to identify, analyse and cope with various cyber-physical threats scenarios in an autonomous manner. To sum up, self-protection strategies will allow PRECINCT's DT representing the CIs network topology and metadata to detect violations and provide optimised response and mitigation measures.

Self-protection strategies can take many diverse forms depending on the protection system. Self-protection can be characterised from two perspectives[1]. From a reactive perspective, the system automatically defends against malicious cyber-physical threats or cascading failure. From a proactive perspective, the system should have the capability for dealing with similar attacks in the future and applying corresponding mitigation actions. We therefore need to enhance the security and resilience of CIs by equipping them with both proactive and reactive self-protection capabilities. A well-known reference model for self-* system is the MAPE-K model[2] proposed by IBM. Following this reference model, a self-protection system can be logically structured into two principal elements: the system logic (a.k.a., the managed element) and the self-protection logic (a.k.a., the automatic manager). The MAPE-K Loop, which consists of four main conceptual components (Monitor, Analyse, Plan, Execute), distributes the tasks to each component in a loop manner and leverages a common knowledge base to characterise the self-protection property. We then use the basic concepts introduced in the MAPE-K loop to illustrate our proposed self-protection approach.

1. Yuan, Eric, Naeem Esfahani, and Sam Malek. "A systematic survey of self-protecting software systems." ACM Transactions on Autonomous and Adaptive Systems (TAAS) 8.4 (2014): 1-41.
2. J. O. Kephart and D. M. Chess, "The vision of autonomic computing," Computer, vol. 36, January 2003, pp. 41–50, doi:10.1109/MC.2003.1160055.

Fig. 7 shows an overview of our proposed self-protection architecture based on the MAPE-K loop. We map different tools that will be designed and developed by different partners with those principal components in the MAPE-K loop as follows.

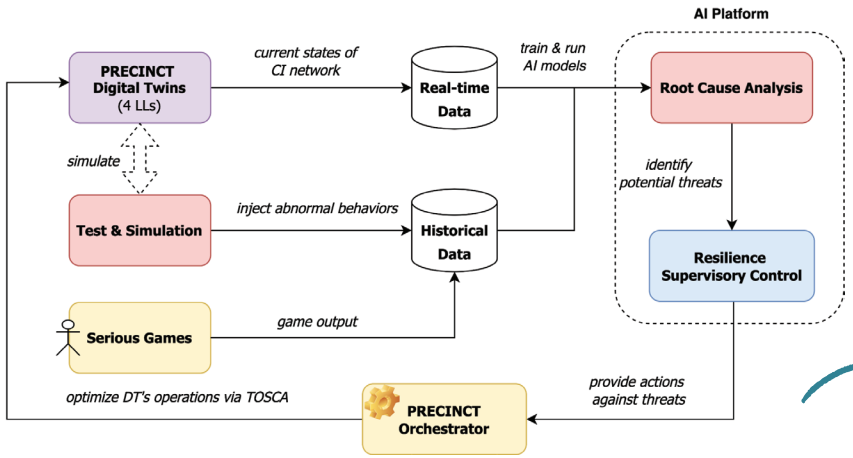

Fig. 7: PRECINCT self-protection architecture

Monitor. Apart from the current states of CI network and game play output produced by Serious Games, our MMT-TaS (MMT's Test and Simulation module) provides another solution to produce data for pre-training our AI models in the Analysis phase. It simulates PRECINCT DTs and injects abnormal behaviours representing potential cyber-physical attacks in the LLs. MMT-TaS provides the possibility to test the IoT system based on test scenarios using pre-prepared datasets and stress the boundaries of the testing scenarios to detect potential problems, such as denial of service (DoS) attacks or low battery conditions in an IoT device.

Analyse. Our MMT-RCA (MMT's Root Cause Analysis module) employs the similarity-based machine learning technique to analyse the data (e.g., statistics extracted from the logs, metrics, network traffic, and any data that helps identify the system's state) collected during the Monitor phase and perform deep analysis to assess the similarity of a newly observed event reflecting the current status of the CIs and each learned one saved in the historical database. MMT-RCA will be trained and executed in the PRECINCT AI platform to identify potential cyber-physical threats.

Plan. After the Analysis phase, Resilience Supervisory Control (RSC) receives alerts concerning potential cyber-physical threats in the LLs. The RSC component then provides corresponding mitigation actions against detected threats.

Execute. Tools developed in the self-protection tool set will be deployed and orchestrated through the PRECINCT Orchestrator.

Knowledge. Both real-time and historical data will be stored in a database for training AI models and further analysis. Specifically, we need to clean, pre-process, and convert input data collected from different sources into a suitable format for different tools in the AI Platform.

Integration of Knowledge Graphs

Dr. Stéphane Kündig, project manager, Konnecta Systems, Dr. Efstathios Zavvos, Head of Artificial Intelligence, VLTN

Konnecta and VLTN have been working closely together towards the integration of Knowledge Graphs (KGs) for Critical Infrastructures (Cis), as part of the PRECINCT data operations between the relevant subsystems. A Knowledge Graph of a CI can be constructed in a manual or semi-manual manner from domain experts and knowledge engineers, and then enriched and augmented with data using automated techniques. By further interconnecting the relevant CIs, a unified PRECINCT KG can be created capturing the specific schema within each CI as well as the inter-CI associations, providing a global overview of the system (Fig.8). In the PRECINCT KG, new knowledge can be deducted and introduced in the KG via i) ingesting new data, ii) processing the available data for implicit info, and iii) identifying properties of objects and relationships not previously evident.

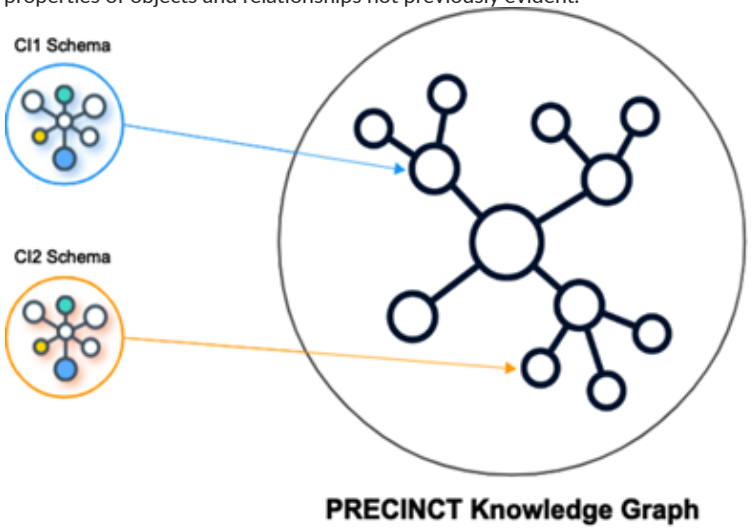

Figure 8. The PRECINCT Knowledge Graph

A crucial matter in that process is that new data, acquired from CI information systems, sensors, and other monitoring devices, must be semantically validated before they can be integrated into the KG. This is of paramount importance in order i) to achieve accurate knowledge extraction, as well as ii) to maintain efficient utilization of resources which will allow for seamless scaling up of the PRECINCT KG as the number of integrated Cis increases. The above is achieved using a semantic data component (Fig. 9), a tool that is being developed for the project purposes which utilizes the Shapes Constraint Language (SHACL) to perform semantic data validation. The semantic data component intercepts the incoming data and, given the prescribed constraints, creates emergent, validated KG instances that can be integrated in the PRECINCT KG, as well as be used to semantically annotate messages forwarded to relevant data subscribers.

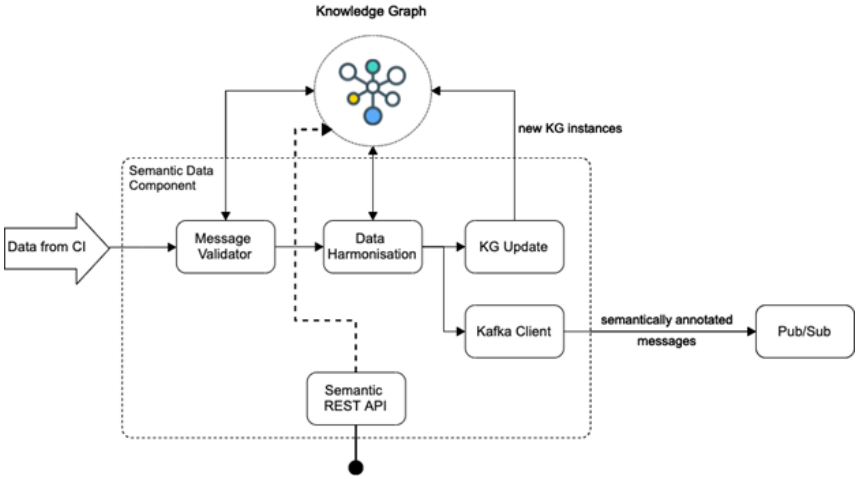

Figure 9. PRECINCT semantic data component.

Thanks to the semantic data component, the continuous enrichment of the KG with new data is ensured to happen in an efficient, automated manner, allowing for new logical inferences to be made about the interconnected CIs. Finally, several systems and services can be built around the KG to exploit the stored knowledge and the semantic interconnection of Cis. These can include simulation tools to evaluate resilience and to help determine appropriate responses to threats, services to determine and optimize CI operations, and real-time decision-making and decision assistance tools among others. Naturally, these will be the focus of the following stages of the project.

PRECINCT Ecosystem Platform, Blueprints and Orchestrator

Djibrilla Amadou Kountche, Project Manager, AKKA

AKKA and partners (MONTIMAGE, NUROGAMES, ENGINEERING, KONNECTA, AE SYN, ATHENS INTERNATIONAL AIRPORT, and LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY) delivered in Month 6 (March 2022) a major WP2 deliverable (D2.3) that documents the PRECINCT Ecosystem Platform, Blueprints and Orchestrator.

It shall support PRECINCT Blueprints by federated Critical Infrastructures (CI) systems to dynamically deploy new services, thereby facilitating the semi-automated integration of such services in PRECINCT Ecosystems (the LivingLabs) through Digital Twins.

This deliverable describes WP2 tools assembled under the term of PRECINCT Ecosystem Platform. This ecosystem is illustrated by the figure below. The illustration considers the deployment perspectives of the ecosystem, providing the reference architectures that can readily be translated into Blueprints.

AKKA leads the PRECINCT Ecosystem Operational Infrastructure and CIP Blueprints Directory in PRECINCT's WP2. Here is a reminder of the ambition of the WP2:

- Provide tools to connect CI systems that need to share data in collaboratively managing Vulnerabilities to Cascading Cyber-Physical Threats and integrate data in Serious Games and Digital Twins applying Federated Identity Access Management and Control (IAM).
- Provide tools for loading data from connected data sources and applying AI analytics to provide recipes/models that can be integrated into DTs and a Blockchain-based framework for coherent data and service distribution and data ingestion functions of the BDA infrastructural services, integrating with the IAM.
- Provide a Design studio for CIP software engineers to integrate existing CIP tools/services with the PRECINCT Blueprints Directory, providing abstractions over low-level concepts such as infrastructure, component-particular configuration, etc.
- Provide a Unified PRECINCT situation awareness user interface (UI) for all Ecosystem participant groups addressing LL requirements directly and utilizing IAM and Blockchain Framework (building on CHARIoT).

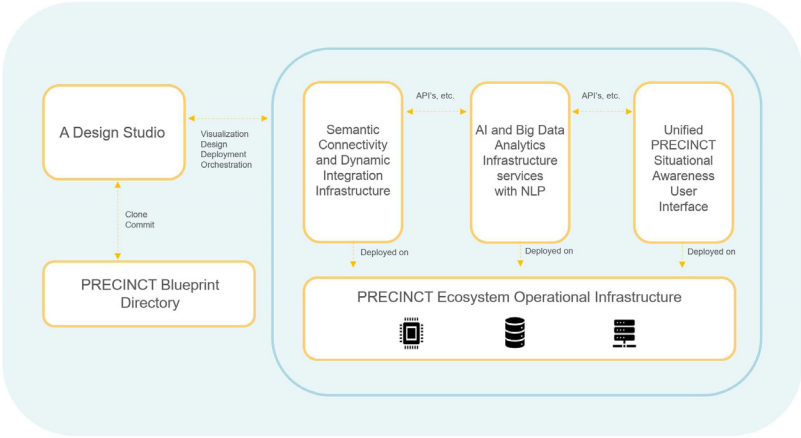

Fig 10: PRECINCT Ecosystem Operational Infrastructure.

The PRECINCT Ecosystem Platform is composed of:

- The PRECINCT Ecosystem Operational Infrastructure
- The PRECINCT Blueprint Directory
- The PRECINCT Design Studio
- The PRECINCT Semantic Connectivity and Dynamic Integration Infrastructure
- The PRECINCT AI and Big Data Analytics Infrastructure services with NLP
- The PRECINCT Unified PRECINCT Situational Awareness user Interface

The standardized OASIS TOSCA is used as PRECINCT Blueprint Description Language. Node types, relationship types, and service templates, among others, are defined to allow the composition mechanism to be formalised and visualised using the PRECINCT Design Studio.

Orchestration tools such as Kubernetes and IT automatization tools such as Ansible will be used to deploy the PRECINCT Ecosystem Platform. Finally, the D2.3 deliverable will provide practitioners with recommendations on the usage of VMS, Unikernels, and Containers.

A systemic approach for Information System Security Risk Management (ISSRM) supported by Enterprise Architecture Management (EAM)

Jocelyn Aubert, Research and Technology Associate; Dr. Nicolas Mayer, Senior Research and Technology Associate – Luxembourg Institute of Science and Technology

In a context of increasing cyberattacks, it is essential to guarantee the resilience of critical infrastructures encompassing finance, energy, health, air transport, communication, gas, and water. All of us heard about these massive cyberattacks targeting essential services such as the one in Ukraine in 2015 on the power grid or the WannaCry ransomware having huge consequences especially in the healthcare sector. Therefore, there is nowadays a strong emphasis on the security of information systems and the management of cybersecurity risks for critical infrastructures. Furthermore, these critical infrastructures are more and more dependent one to the other (e.g., energy supply is necessary for telecommunications services, finance is largely based on telecommunications services for any transaction, etc.) leading to an increasing complexity and requiring considering sophisticated cyber-physical attacks.

It is today a complex challenge to analyse risks on a system composed by companies needing to keep confidential their IT architecture and their remaining vulnerabilities to the other organizations who are part of the supply chain. A promising approach to bridge this gap is to introduce a multi-layer dependency model dealing with both business dependencies and architectural dependencies. In such security and risk analysis of dependent companies, the business dependencies can in general be shared between the actors and are sometimes public (i.e., which company is using which kind of services provided by another one) but companies are reluctant to display and share their internal infrastructure and associated weaknesses.

Such a multi-layer approach is well-known and widely used by the Enterprise Engineering community and enabled by Enterprise Architecture Management (EAM) and associated modelling language such as Archimate. EAM has shown to be a valuable and engaging instrument to face enterprise complexity and the necessary enterprise transformation. It offers means to govern enterprises and make informed decisions: description of an existing situation, investigation and expression of strategic direction, analysis of gaps, planning at the tactical and operational level, selection of solutions, and architecture design.

Within PRECINCT, LIST is investigating how an EAM-ISSRM integrated model; a multi-layer approach to analyse risks and security of depending organizations; shown in Fig. 11; can be leveraged to enable risk cascading and ecosystem risk management following a 3-step approach as presented in Fig. 12.

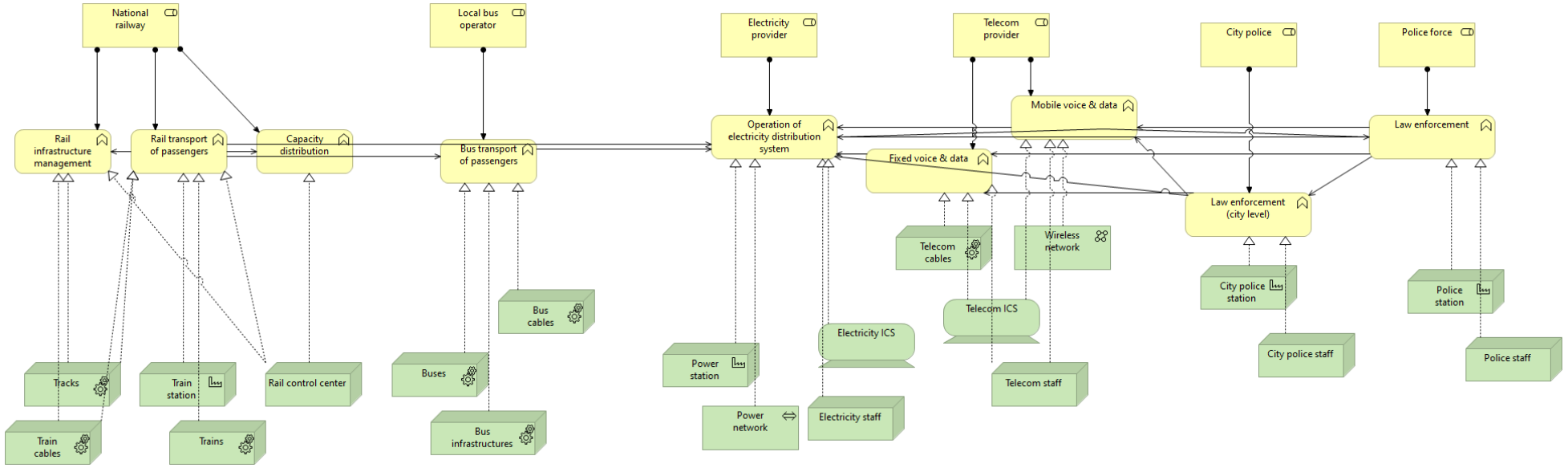

Fig. 11 - Example of modelling using EAM-ISSRM

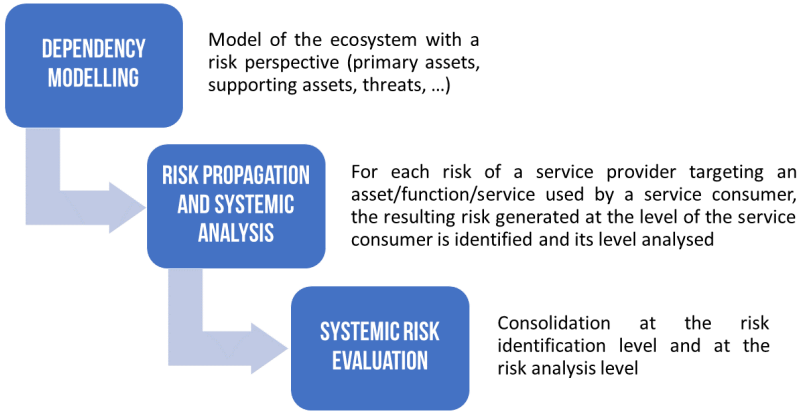

Fig. 12 - Risk cascading and ecosystem risk management.

Promotion of PRECINCT

Lottie Stainer, Communications Manager, UITP

UITP is investigating and analyzing stakeholder needs through the involvement of UITP members, particularly public transport and sustainable urban mobility operators, authorities and industries. In addition, through sharing the project activities and results, we are promoting the PRECINCT outreach and approach, transferability and industry take up to both members and the wider sustainable mobility sector. Recently, the PRECINCT project was presented during UITP's Security Committee meeting with 19 public transport operators and authorities interested in learning more about security-related solutions. As for the stakeholder workshop, held on 5 May, UITP shared information on their social media accounts to a wider audience and with two direct emailing to key members interested in the topic of security.

UITP is looking for opportunities to link the activities of PRECINCT to our global public transport events which will be taking place in the near future. We are also reach our audiences through news articles on the website related to our wider editorial topics, linking the projects to wider public transport news and linking to our European and security newsletters. During both these event and through member and external communications, UITP is working with EOS who are the task leaders for the "Stakeholder and need knowledge base" to ensure our communications are well-coordinated with the timeline of project activities such as surveys and workshops so as to promote the activities to key stakeholders wherever possible.

Events

May and June 2022

- Bologna Airport represented PRECINCT and Living Lab Bologna at the online E-Corridor Project Conference, where a talk was given about multimodal transport.
- Shirley Delannoy of Vias institute gave a presentation on “PRECINCT – case of living lab Antwerp” at the 13th International Conference “Days of Corporate Security 2022” in Slovenia.
- Dimitri Schuurman of IMEC presented “Scoping a Digital Twin for Disaster Management” and moderated a session on Digital Transformation in Living Labs at the ISPIM Innovation Conference in Copenhagen. During the session on Digital Transformation, Shirley Delannoy gave a talk on the theme “Living Labs for digital transformation in the public sector: Digital Twins for disaster management”.

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:

August 2022

- PCSCI workshop at the ARES conference, 17-20 August 2021, Online
- 16th International Conference on Availability, Reliability and Security, SBA Research & University of Vienna, Austria, 23 - 26 August 2021, Online
- PCSCI workshop at the ARES conference, 23-25 August 2022 Vienne, Austria, www.ares-conference.eu/workshops-eu-symposium/
- ESREL - European Safety and Reliability Conference, 28.08. – 01.09.2022 Dublin, Ireland, https://www.esrel2022.com/www.esrel2022.com

September 2022

- Sep-22 Turin, Italy, https://openlivinglabdays.com/

October 2022

- European Cluster for Securing Critical Infrastructures (ECSCI), 8 October 2021, Online , st.fbk.eu/events/CPS4CIP2021/
- Settimana della Bioarchitettura e Sostenimilita, 17-26 October 2021, TBD, www.settimanabioarchitettura.it

November 2022

- TRA Lisbon 2022, TRA 14-17 November 2022 Lisbon, traconference.eu/

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