PRECINCT

NEWSLETTER

April 2022
Issue #02

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

Dr. Takis Katsoulakos, Managing Director, PRECINCT Project Coordinator – Inlecom

As PRECINCT moves into the second quarter of our first year, the project design team have been working together to build the foundations of the PRECINCT project architecture, bringing together baseline assets/components and state of the art research from recent reference projects, and pulling these together into a clear vision of the PRECINCT architecture with Digital Twins at its center.

In addition, the team have been working on the development of a generic Use Case for early deployment in the PRECINCT Living Labs. The Use Case will allow the Critical Infrastructure providers from the Living Labs to carry out the steps necessary to understand and quantify their resilience to cyber or physical attacks. This is the first step and an essential baseline activity before the project can move on to model the interdependencies between the Critical Infrastructures in the Living Lab regions of Antwerp, Athens, Bologna and Ljubljana. PRECINCT will then move on to implement Serious Games to perform Vulnerability Assessments both at individual Critical Infrastructure and at the 'command' coordination level.

The project timeline shows some of the key milestones that we aim to achieve in the delivery of the project.

Fig. 1 – PRECINCT project timeline.

Interdepency Graphs and Cascading Effects

Dr. Sandra König, Scientist; Dr. Stefan Schauer, Senior Scientist – Austrian Institute of Technology

Understanding the manifold effects of an incident such as a flood not only requires knowledge about the threat, but also about the area and infrastructures that will be affected. Today's critical infrastructures (CIs) are strongly interconnected and reduced operation of one or more may affect others. Therefore, a profound analysis of a threat includes awareness of the relevant CIs and their interdependencies. In PRECINCT, these interdependencies are modelled through a graph where nodes represent CIs (or relevant parts of CIs) and edges represent dependencies, such as exchange of resources or providing services.

A generic example of such a dependency graph is shown in Fig. 2. Several components of a water utility, telecommunication provider, power provider, hospital, traffic, and emergency services are shown with the dependencies between them. A threat may affect these CIs, and therefore indirectly also people living in the area, which is a core aspect of the analysis.

In PRECINCT, workshops carried out with experts from the Living Labs (LLs) will be the base for the development of scenario specific dependency graphs.

The dependency graph does not only rise awareness of potential indirect dependencies, but it also enables simulation of how an incident may affect such a network. The degree to which a component is affected by a threat is represented through an abstract state, which can be interpreted as level of functionality or availability of the respective CI. Knowing the local reaction to a threat, i.e., how the state changes in the light of a specific threat, the simulation allows an estimation of the global reaction of the entire network. The simulation results can be visualized through a map where nodes are coloured according to their state, e.g., green for normal operation, yellow for problems and red for not operating nodes.

An important goal in PRECINCT is to find synergies between different frameworks that focus on various parts of security of CI networks. The dependency graphs can benefit from and provide input to both the resilience framework developed by RDS and the serious game model developed by UCD. Information from the resilience framework may influence the local reaction to a threat (and therefore affect the global reaction). The simulation of cascading effects offers an additional source of information used for the design of the resilience framework, since different scenarios can be evaluated. Similarly, the dependency graph may provide input to the serious games from UCD. The empirical results of the game plays may in turn be valuable feedback to the modelling and can provide deeper insights into the dependencies among CIs.

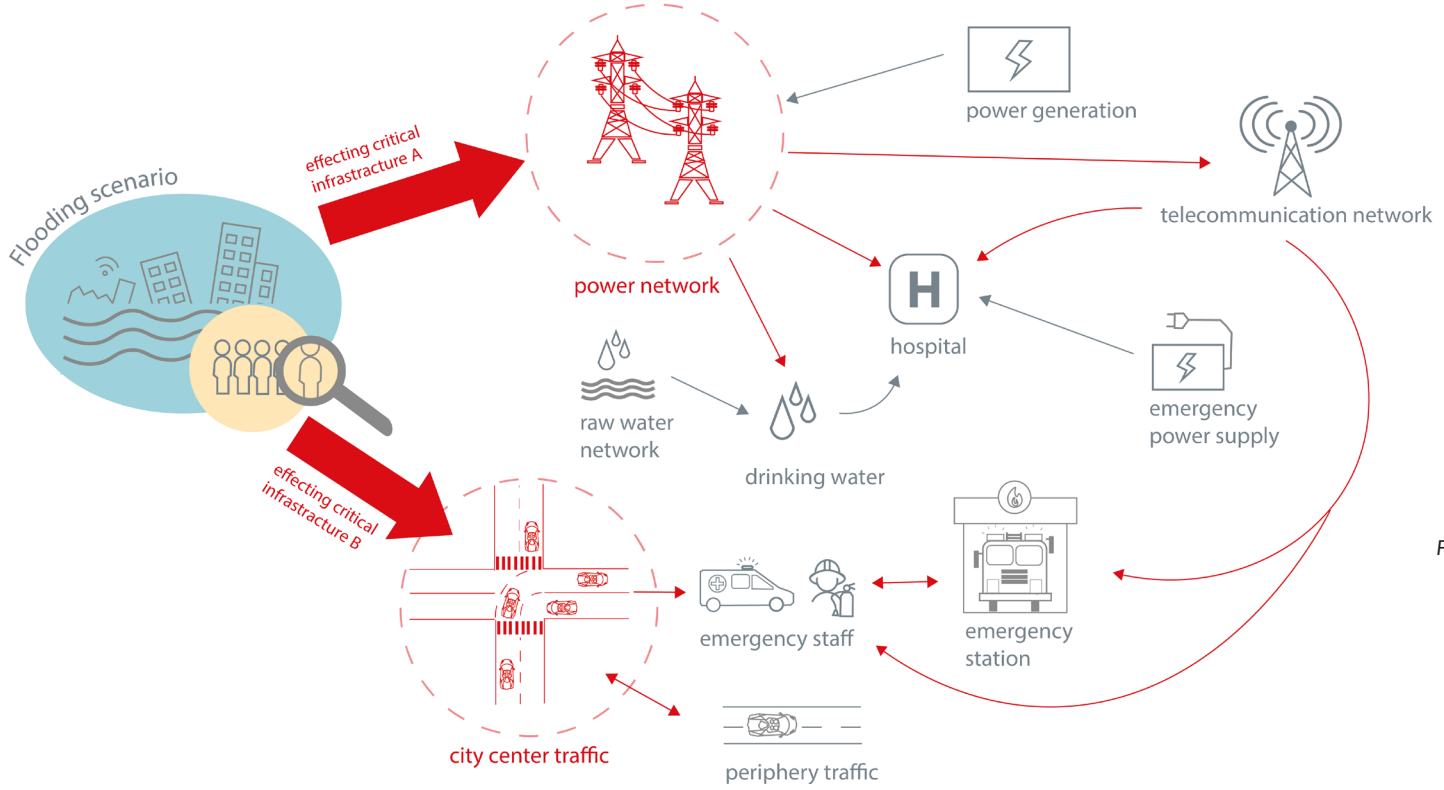


Fig. 2 – Dependency Graph.

Technologies for Message Exchange and Big Data Analytics

Gabriele Giunta, Senior Researcher, Francesco Durante, Researcher– ENGINEERING

ENGINEERING has been working to develop a full end-to-end encryption mechanism for message exchanges between federated systems on existing critical infrastructures. At an early stage, it was made an analysis of the state-of-the-art and cutting-edge Pub-Subs solutions. Among the others, Apache Kafka, RabbitMQ, Rocket MQ, ActiveMQ, Apache Pulsar, were duly analyzed, describing their pros and cons. In addition, a performance study based on throughput and latency was carried out.

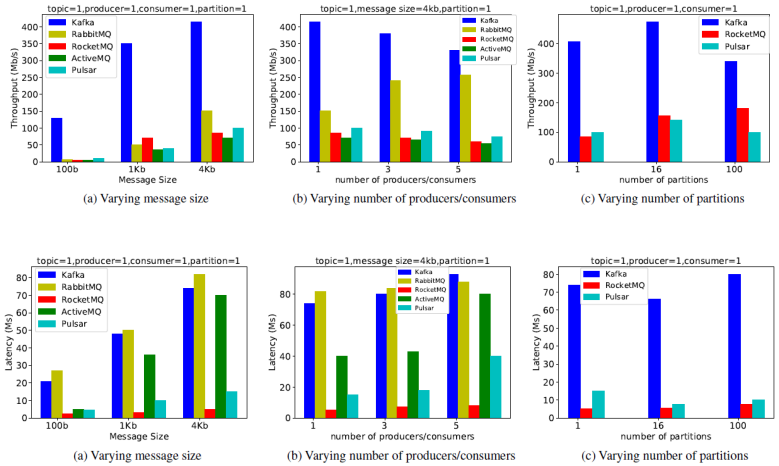
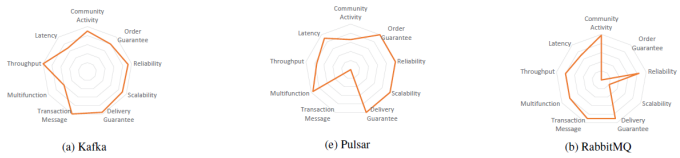


Fig. 3: communication method.

Finally, all the results from the previous analysis were aggregated to provide a comparative view showing as Apache Kafka appears to be the most balanced and more appropriate solution compared to its competitors. It doesn't require complex routing to deliver messages to consumers, adopting a simple and scalable architecture.



This work continues and the AI and BDA Infrastructural Services and Common Data Analytics Visualizer are being developed by ENGINEERING as the main technical reference, where the two key architectures supporting Big Data Analytics (BDS) and machine learning processes are devised. The main user of these technologies is the System Administrator who want to adopt such a solution to build up and reproduce the BDA service stack both in the cloud and on-premise infrastructure. It is worth noticing that all the components and sub-components will embrace the cloud-native principles to offer the highest degree of portability, and to be suitable for elastic environments and multi-cloud environments.

The proposed technologies are based on ALIDA, a research prototype by ENGINEERING coming from previous and ongoing research activities. ALIDA is a micro-service based platform for the design, deployment optimization, execution and monitoring of Big Data Analytics workflows (ingestion, preparation, analysis, visualization). ALIDA is designed and developed on top of the most cutting-edge Open Source Big Data technologies and frameworks. It goes beyond Data Science and Machine Learning (DSML) platforms, making BDA design and development "closer" to target applications and towards augmented analytics (https://home.alidalab.it/).

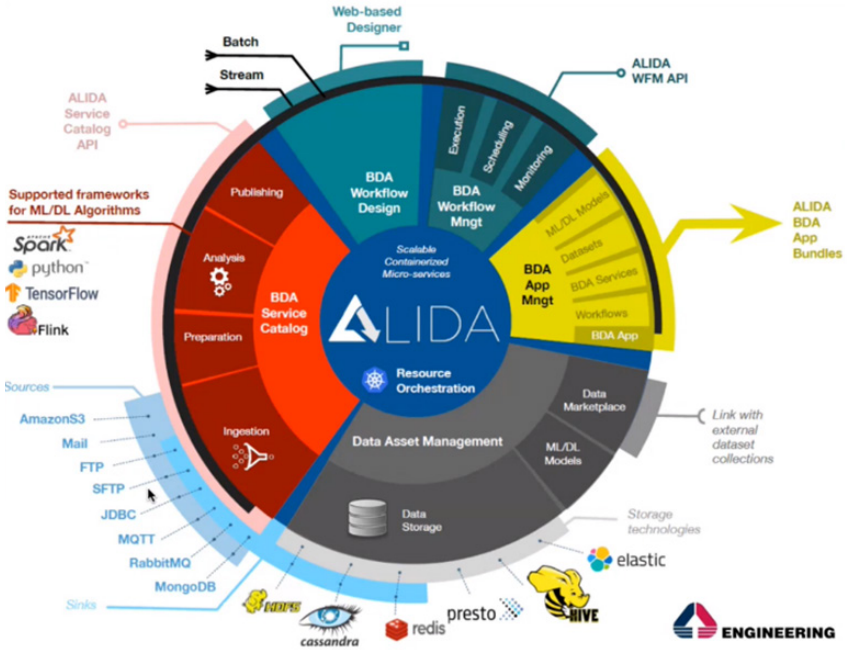


Fig. 4: ALIDA platform.

Digital Twins to enhance resilience in case of cyber-physical incidents

Luca Mariorenzi, Program Manager, Emiliano Altobelli, Program Manager - FSTechnology

Cyber-attacks represent a big threat on the correct functioning of all transport mode services; railways can also be the target of physical or cyber-attacks, which is why many studies and related tests aim at strengthening and improving the resilience of such critical infrastructure to external threats. Thanks to PRECINCT's outcomes, FSTechnology (FST) security strategy will be supported with the creation of a complete view and management of the combined risks and incidents of Italian Railway network and the local public transports infrastructure (including other critical infrastructures).

FST is involved in the Living Lab Operation Bologna, whose main objective is to establish a 'dependencies and cascading threat's model' for the main actors involved in the LL which, besides FST, are Lepida, Bologna Airport and Marconi Express.

An initial PRECINCT Ecosystem Platform will be deployed by Lepida to support LL development. As main output, PRECINCT system will stress on the Critical Infrastructure Cascading effects in order to identify which are the possible and suitable solution in a real life situation by testing new scenarios never tested before. FST's role is crucial since it is able to provide useful data sources in order to identify key scenarios in the interdependencies context and, in parallel, will be able to contribute in developing the Digital Twin concept, which will be exploited by the project.

Currently, we are working on the threat scenarios definition together with the Italian Living Lab partners, this activity is the first step required to be able to identify the most vulnerable points within the Living Lab area. Next upcoming tasks will include the starting of Living Lab operations activities and support to the Digital Twins Architecture and user story mapping.

Railway network.

Multi-agent deep reinforcement learning to optimise the normal operation of the critical infrastructure Digital Twin

Dr. Jose Carlos Carrasco-Jimenez, Senior Researcher - Barcelona Supercomputing Center

Timely and correct response to threats is key for the correct operation of a Critical Infrastructure network. As part of the PRECINCT project, we seek to develop a decision support tool enhanced with artificial intelligence to provide end-users with a long-term policy (i.e. list of actions) to optimise the operation of the digital twins (DTs) instantiated for each living lab. The optimisation process seeks to improve the resilience of the DT while minimising the cost of business interruption.

Our approach is based on the intersection of different state-of-the-art techniques, including advances in multi-agent systems and reinforcement learning. A multi-agent system describes multiple distributed systems (agents) which take decisions autonomously and interact with a shared environment[1]. Reinforcement Learning, on the other hand, is a machine learning technique which involves learning by taking actions in a trial-and-error manner.

Fig. 4depicts a high-level overview of the Multi-Agent Deep Reinforcement Learning model. The solution model follows a master-slave paradigm and is composed of three main components: 1) master agent, 2) slave agents, and 3) environment. The master agent reacts in the presence of a disruptive event and triggers the corresponding slave agent to compute the policy, that is, the list of actions to perform in order to mitigate the effects of the disruptive event. Slave agents specialize in a single type of disruptive event, suggesting a set of actions specific for the type of incident. Furthermore, all the slave agents interact with a shared environment, which is consists of a CI simulation module and a reward model. The CI simulation provides the mechanism to estimate the impact of a disruptive event on the CI network, while the reward model seeks to provide the optimization agent (slave) with clues to reinforce good actions that improve the operation of the CI network.

1. Adams, Julie A.. "Multiagent Systems: A Modern Approach to Distributed Artificial Intelligence." AI Mag. 22 (2001): 105-108.

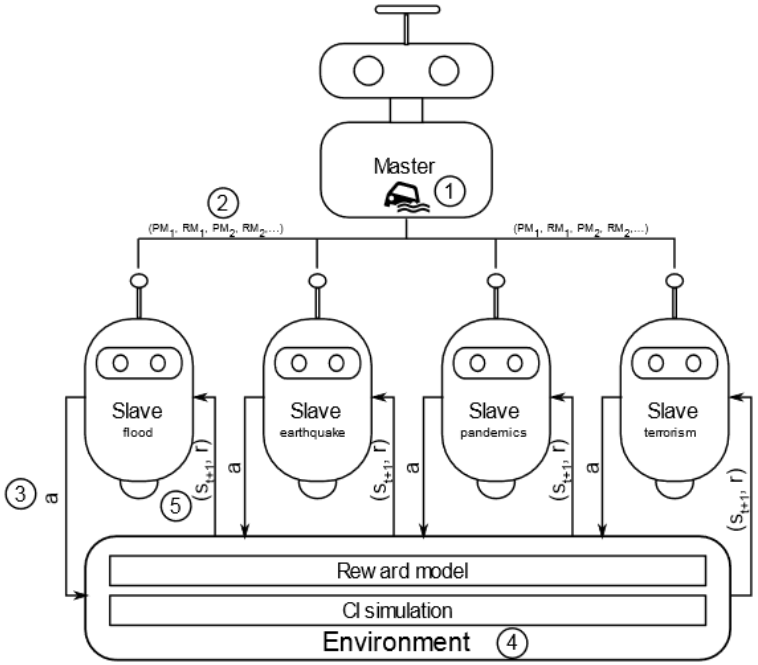


Fig.. 5: Overview of the Multi-Agent Deep Reinforcement Learning Model.

The interaction process can be summarised as follows (step numbers correspond to the numbers in the high-level diagram of Fig. 1):

1. Master agent identifies the type of disruptive event and triggers the corresponding slave agent
2. Master agent sends the location of the affected nodes of the CI network along with the corresponding operational capacity level
3. The corresponding slave agent is triggered and sends and action to the environment. Each slave agent has a specific set of actions to cope with the corresponding disruptive event
4. The slave agent will interact with the Environment (provided by the Serious Game module) which will execute the action provided by the slave agent and compute the next state and a reward value
5. The environment returns a reward value and the new state after executing the action.

Steps 3 to 5 are executed until a long-term policy is learnt by the corresponding slave agent, resulting in an optimal sequence of actions to improve the operation of the DT.

Experiential learning and training tool for improving cyber security competences

Dr. Cristina Regueiro, Senior Researcher, Angel Lopez, Senior Researcher, Marisa Escalante, Project Manager - TECNALIA Research and Innovation (TCNL)

Train the cyber security experts to support them to react as quickly as possible when a cyberattack occurs is one of the mitigation actions to CIs cybersecurity enhancement.

The cyber-ranges are a key tool for cyber security training. Cyber-range is an infrastructure that allows the simulation of real operating environments for the training of professionals as well as the experimentation, testing and validation of new cyber-security and cyber-defence concepts, technologies, techniques, and tactics. They can be employed by different types of users like students, security professionals, educators, companies, researchers etc. and for multiple purposes such as security research, security training, cybersecurity assurance.

TECNALIA owns a Cyber-range laboratory composed by the following elements:

- **Master room with 10 stations for participants in which the exercises take place, with all the hacking tools needed to solve the exercises and connected to the simulated infrastructure created for the exercise deployed in the CPD**
- **Security Operations Centre (SOC): Operations centre from which TECNALIA´s team monitors the conduct of the exercise for the smooth operation of the execution. It has tools to observe what is happening in the room, to give support to participants and to maintain the technical infrastructure.**
- **Data center where the infrastructure and tools required for executing the exercises are deployed.**

The design and implementation of cyber-exercises are a strong tool to support the enhancement of the knowledge of both offensive and defensive cybersecurity. They contribute to obtaining professionals who are better prepared to face the attacks and challenges they will encounter in their day-to-day work, who are more qualified and knowledgeable about the real cybersecurity problems faced by IT and OT systems. TECNALIA's cybersecurity team has been working in the last years in designing and implementing cyber exercise scenarios in both IT networks and OT networks given the new cybersecurity needs introduced by Industry 4.0, as well as hybrid networks in which there is communication between the IT and OT worlds.

One of the activities of the PRECINCT project is to design and develop a set of cyber exercises, one per each Living Lab with the objective of awareness of the cybersecurity relevance in the LLs and training to recognise potential cyberattacks that could be suffered and the mitigation techniques to avoid them.

The design of these cyber-exercises, that could be face-to-face or remote, follows these steps:

- **Identification of the cyber threats for the different scenarios defined in each LL.**
- **Definition of the Kill chain, this means to define how the vulnerabilities are going to be exploited or attacked.**
- **Design of the architecture of each exercise indicating which data and how are going to be collected from the LL or the DT, and also how are going to be presented to the trainees for their analyse.**
- **Creation of the story line for the exercise: Information to be provided to the trainees to support the understanding the objectives: what it is happening, context, trainee's role.**

TECNALIA´s cyber-range laboratory is where the cyber-exercises of the different PRECINCT LL's will be deployed and executed to train the LLs personnel about the cybersecurity threats of their infrastructures and the best actions to mitigate them.

Nowadays, TECNALIA is working together with each of the LLs to identify the potential cyberthreats that have been identified in each scenario and select the most suitable for training.

PRECINCT Digital Twins Architecture and user story mapping

David Vermeir, Operations lead, Dimitri Schuurmans, Innovation expert - Imec

Train The Trainer & User Story Mapping

Within the Train-the-Trainer sessions, imec is training the four PRECINT Living Labs (Ljubljana, Antwerp, Athens, Bologna) in the scoping process of the Digital Tin solutions. This process follows the FACTS-approach: FOCUS, ANALYSE, CO-CREATE, TEST and STUDY. Each phase lasts for two weeks and involves activities with the most important stakeholders and end-users of the different Living Lab cases. A threefold assessment is made regarding the use cases in order to maximize the potential impact of the resulting solution: feasability (is the solution technically possible), desirability (does the solution tackles the most important stakeholders' and users' needs) and sustainability (can the solution be implemented within a reasonable amount of time and budget).

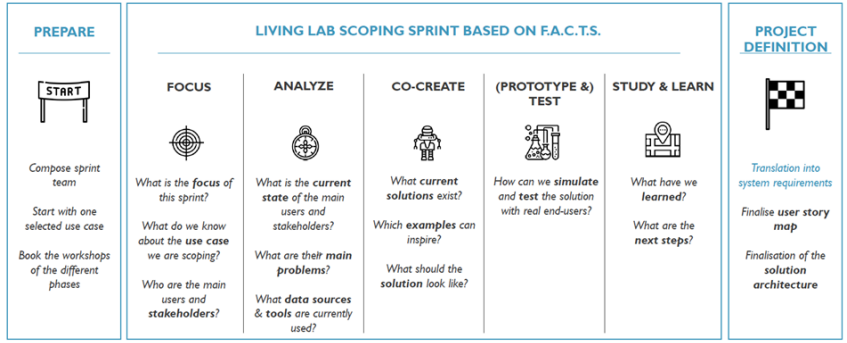


Fig. 6: Overview of Living Lab scopting print.

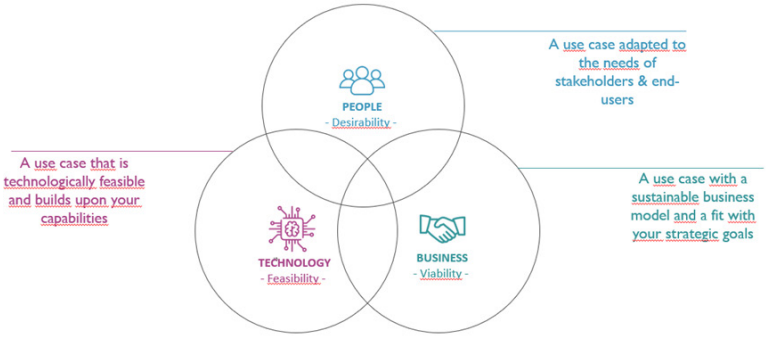
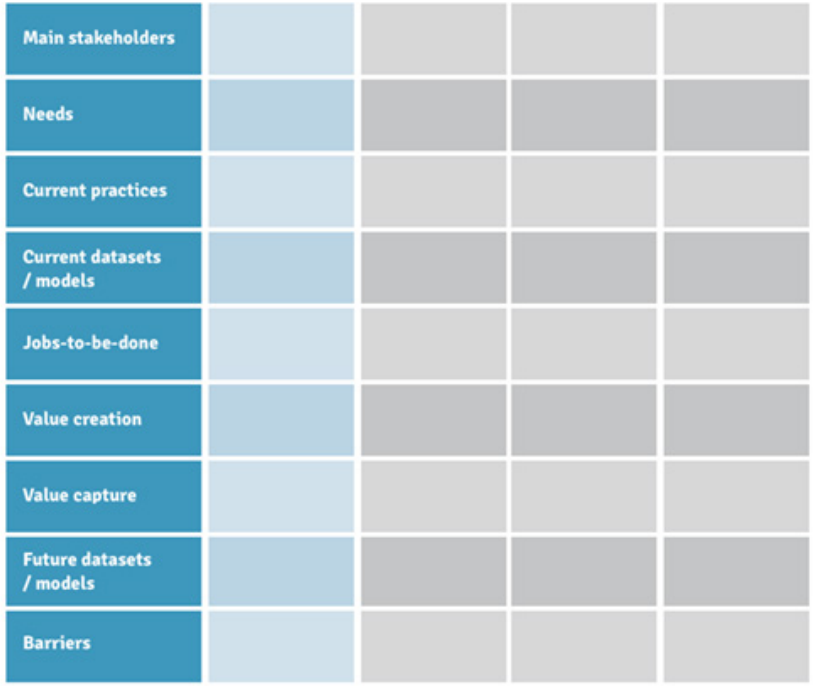


Fig. 7: The sweet spot of innovative data-driven solutions.

During this intense 2 month process, imec's Innovatrix digital Innovation Management platform is used to keep track of all assumptions and of the (in)validation of them during the scoping sprint phases. The Living Labs use the specifically developed Digital Twin Canvas to map the most critical elements of the current state and of the future state (= the digital twin solution). The canvas provides structure to describe, discover and validate stakeholder requirements.



At the end of the 2-month scoping process, each Living Lab should be able to specify and prioritize requirements for their Digital Twin as user stories.

Digital Twin Architecture

Besides user story Mapping imec is also responsible for the architecture of the PRECINCT Digital Twin. As the scoping of the specific solutions for each Living Lab is in progress, the architecture is created in two phases. The first phase creates a generic Digital Twin architecture living within the PRECINCT Ecosystem Platform. It covers generic use cases assumed to be critical for the operation of a Digital Twin as an important component within the ecosystem of Critical Infrastructure systems. To do this, we're using the C4 model for visualizing software architecture on 4 different levels (context, containers, components and code). The reference architecture only requires the first 3 levels as the 4th level is an implementation concern.

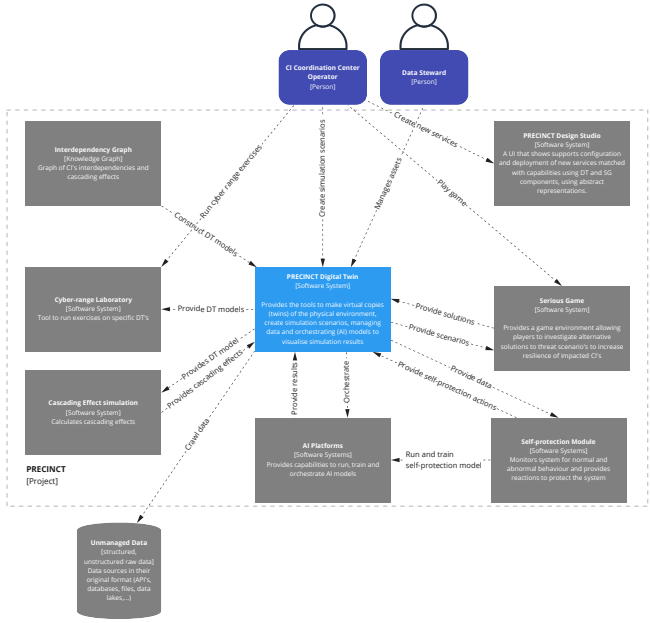


Fig. 8. PRECINCT DT System Context Diagram.

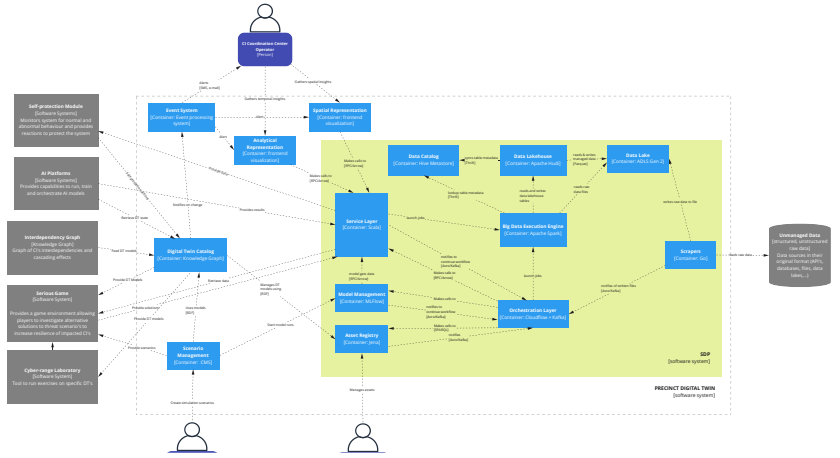


Fig. 9. PRECINCT DT Container Diagram.

We're mapping these capabilities to components, meaning we'll have a form of Digital Twin menu card which allows a Digital Twin user to identify which capabilities are required for his/her use case and which components provide the necessary capabilities. This can be configured into a PRECINCT Blueprint so there are ready-made Digital Twin solutions for often recurring use cases. The capabilities are shown as a periodic table, which provides a structured overview where they are grouped by similarity into families.

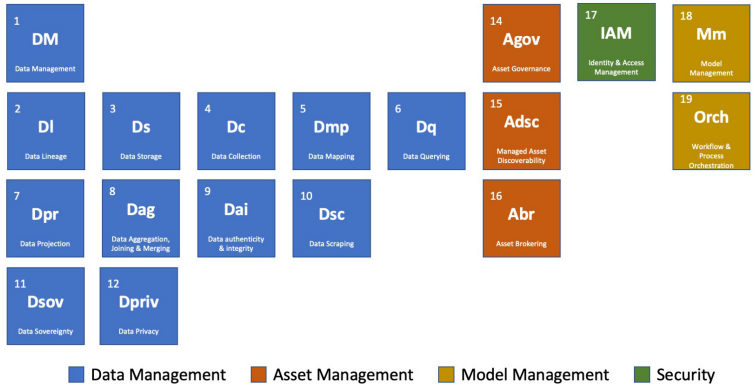


Fig. 10. PRECINCT Periodic Table of DT Capabilities (WIP).

Transport, logistic and technology

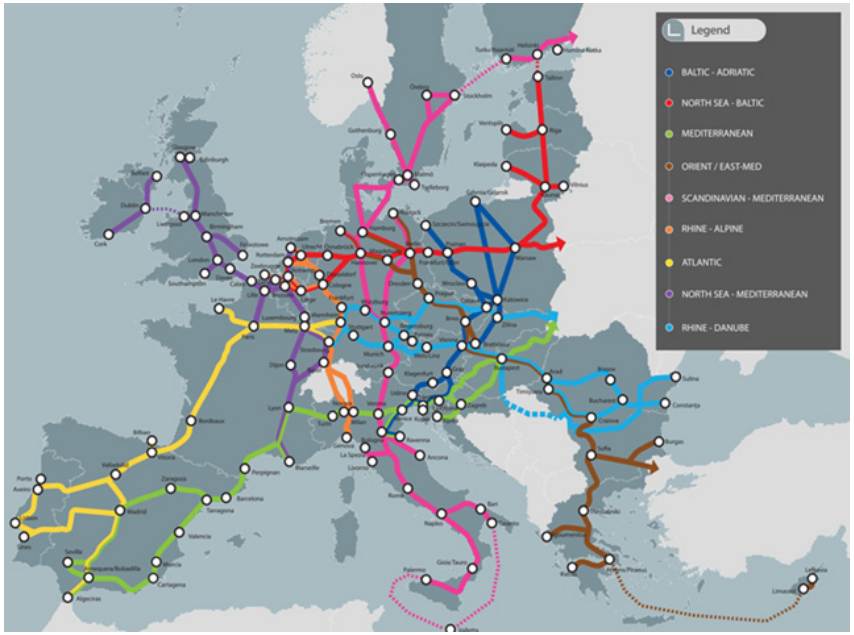
Guiseppe Brancaccio, Transport Engineer – Fondatzione ITL

The Institute for Transport and Logistics Foundation (ITL) is a no-profit public research body born in 2003 with the mission to contribute to develop and promote the transport and logistics system in Emilia-Romagna region (Italy), through research, consultancy and training activities. Environmental consciousness and technology diffusion are tightly coupled to ITL's technical background and represent two priorities for such a strategical Region, and a continuous dialogue with local authorities and stakeholders is the only way to pursuit them.

ITL is the coordinator of the Living Lab Operation Bologna, and will collaborate with FS Technology, Lepida, Airport of Bologna and with other stakeholders involved in the project activities such as the Marconi Express, Emilia-Romagna Region and local authorities.

ITL will also have the delicate role to discuss with local stakeholders the activities carried out from the Living Lab in Bologna and to finalize the reports at project level in a transnational environment. Besides the transversal skills in project management and geospatial analysis, ITL will also share with the rest of the LL of Bologna the transversal knowledge on transport, and in particular on the impact that critical infrastructure may have in the transport environment of the city of Bologna, of the Emilia-Romagna, and in general of the TEN-T Network.

After having identified the vulnerabilities of the assets in the study area and defined the threat scenarios and the cascading effects, the focus of the LL is now on the development of the Digital Twin that will be used by local stakeholders for monitoring and simulating many scenarios. As aforementioned, transport infrastructures are involved in this process, as well as the telecommunication network and the passenger flows at the airport, while the main vulnerabilities are related to natural and physical damages.



Events

December 2021

Jayant Sangwan, Innovation and Policy Mangerof CORTE presented PRECINCT to its members during the annual meeting held in December 2021, the audience included more than 100 representatives from road transport authorities, transport ministries, European transport associations, European Union and private sector entities. CORTE will continue to present updates from PRECINCT in working group meetings of its members.

March 2022

Carmela Canonico, Safety and Security Manager of UITP, presented PRECINCT to its SECCOM Member on March 2022. The Audience included representatives and experts from European transport associations (from Poland, Portugal, The Netherlands and Italy) and private sector entities.

April 2022

The ECSCI (European Cluster for Securing Critical Infrastructures) will hold its 2nd virtual workshop on April 27-29, 2022 on Critical Infrastructure Protection.

May 2022

The PRECINCT's 1st Stakeholder Engagement Workshop is now reality.

The Workshop will take place in Brussels on the 5th of May 2022 in hybrid format and will show the latest project results and focus on engaging with relevant stakeholders on the technical and business aspect of the project through presentations and roundtable discussions.

Engaging with Critical Infrastructure stakeholders, such as yourselves, is an essential part of PRECINCT, and we are excited to host you in our first organised event!

If you are interested in participating, please see below the agenda and a registration link. EUSurvey - Survey (europa.eu)

Agenda

1ST Stakeholders Engagement Workshop

Maison des Associations Internationales, Rue Washington 40, 1050 Brussels,

(On-Line, Zoom) 5th May 2022

08:30 – 09:00 Welcome and Registration

09:00 – 09:10 Remarks | Jenny Rainbird, Project Coordinator (ICP)

09:10 – 09:25 Main Key Results and Roadmap | Gabriele Giunta (ENG)

09:25 – 09:50 BluePrints and Knowledge Graphs | Djibrilla Amadou-Kountche (AKKA), Stathis Zavvos (VLTN)

09:50 – 10:10 Serious Games | Daniel McCrum (UCD), Yash Shekhawat (NURO)

10:10 – 10:30 PRECINCT Architecture and Implementation | David Vermeir (IMEC)

10:30 – 10:45 Coffee Break

10:45 – 11:00 PRECINCT Living Labs | Shirley Delannoy (VIAS)

11:00 – 11:15 Operation Athens | John Limaxis, Gerasimos Kouloumbis (ICP)

11:15 – 11:30 Operation Antwerp | Shirley Delannoy (VIAS)

11:30 – 11:45 Operation Ljubljana | Denis Čaleta (ICS)

11:45 – 12:00 Operation Bologna | Giuseppe Brancaccio (ITL)

12:00 – 12:40 Partners' feedback on the business requirements |Mark Bennett (ICP)

12:45 – 12:45 Morning Conclusion | Jenny Rainbird, Project Coordinator (ICP)

12:45 – 13:30 Lunch Break

13:30 – 13:45 Critical Infrastructure Protection | Päivi Mattila (LAUREA)

13:45 – 15:15 PRECINCT's Future Technical Aspects
Moderator: Mark Miller (CPT)
Speakers: Daniel McCrum (UCD), Stefan Lefever (IMEC), Stefan Schauer (AIT), Gabriele Giunta (ENG), Lorcan Connolly (RDS)

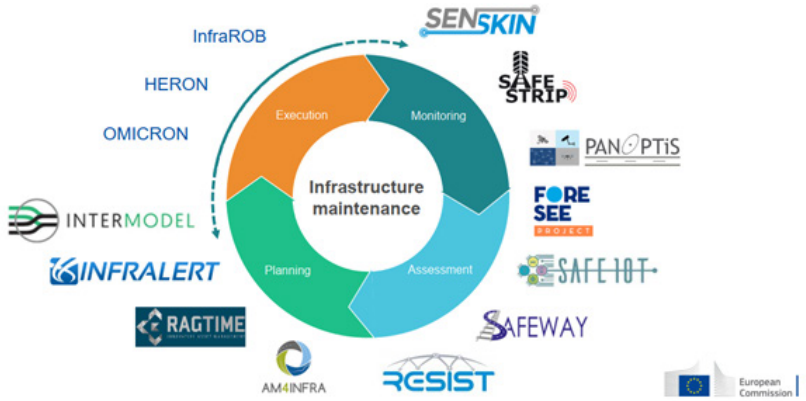
15:15 – 15:30 Coffee Break

15:30 – 16:45 Drivers and Barriers for implementation of new CIP Solutions
Moderator: Mark Bennett (ICP)
Speakers: Marisa Escalante Martinez (TCNL), Päivi Mattila (LAUREA), Vito Morreale (ENG), Benoit Baurens (AKKA), Denis Čaleta (ICS)

16:45 – 17:00 Conclusions | Jenny Rainbird, Project Coordinator (ICP)

Synergies

PRECINCT will be closely linked to and work with projects PANOPTIS and HERON, where the PRECINCT consortium partner CORTE is involved. Both PANOPTIS and HERON are part of a series of projects (see below) funded by the European Commission to develop new technologies for road infrastructure maintenance, security and safety. The work in these projects will draw upon the research under PRECINCT to further improve their outcomes. This collaboration will also facilitate involvement of key stakeholders in PRECINCT.



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