PRECINCT

# NEWSLETTER

November 2023
Issue #07

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 seventh and last newsletter and we are excited to share our last news with you all. These have been 24 intense months and lots of achievements have been accomplished by all the partners. Let's share with you some of them to conclude this project.



## Standardization - Supporting security and resilience of Critical Infrastructure

*By Jenny Rainbird & Loredana Mancini (Inlecom Commercial Pathways), Eftichia Georgiou, (Center for Security Studies (KEMEA), Hellenic Ministry of Citizen Protection) Sonia Fernandez Gonzalez (UNE-Asociación Española de Normalización, CEN/WS IPCI Secretariat)*

In the face of ever-evolving threats and unprecedented challenges to our modern way of life, safeguarding our critical infrastructure has become an ever more urgent priority. As the backbone of society, critical infrastructure which comprises of vital sectors such as energy, transportation, telecommunications and healthcare services, gives us the structure to support citizens and societies daily lives in Europe.

However, the interconnected and complex nature of these systems and the cascading effects of both physical and cyber-attacks, necessitate a comprehensive and unified approach to improve resilience.

Standardization can help to simplify complexity in Critical Infrastructure Protection by providing a consistent framework for operations, fostering interoperability, facilitating collaboration, optimizing security practices, ensuring compliance with regulations, and supporting scalability. By adopting standardized approaches, critical infrastructure entities can navigate the intricacies of their systems more effectively, ultimately leading to enhanced security and resilience.

In addition, common and adopted standards can be a booster for the European market, as they allow technology and solution providers to address market needs with products that are already shared and accepted by the user community. This helps to promote European products in worldwide market.

In collaboration with the STRATEGY project[1] as proposer of several standardization initiatives in CEN standardization, PRECINCT is participating in a CEN workshop on 'Improvement of information processing in crisis management of critical infrastructures for computer assisted data gathering, display and reporting' with more than 40 domain knowledge experts addressing the standardization of information and formats for improving the efficiency and accuracy of incident situational reporting for Critical Infrastructures.

Currently, in case of an emergency incident, there is no standardized type and content of information to be sent from a critical infrastructure to a nationally designated contact point for critical entities and the draft CEN Workshop Agreement (CEN/prCWA 18024) being draft, will cover this gap

The STRATEGY project has systematically identified and prioritised gaps in standardization, in crisis and disaster management in order to initiate several pre-standardization activities within its eight Streams and has compared and tested (though TTX and FSX) these draft documents (11 CWAs and 2 Technical Specifications) to the needs of end users and to available opportunities across a broad spectrum of disaster management activities.

1 Homepage - Strategy (strategy-project.eu) LinkedIn https://www.linkedin.com/newsletters/7079803171182628864/

PRECINCT has contributed to the workshop and the development of the Draft CEN Workshop Agreement prCWA 18024, and the documentation is available[2] on the CEN website. It is hoped that this will be useful for stakeholders such as security liaison officers of critical infrastructures, public administration, coordination centers, first responders' control rooms and first responders of a higher command level. The incident reporting form as developed in the specific CWA was demonstrated during the PRECINCT Athens LL demo and relevant feedback for the usability and usefulness for the form was collected by the participating end users.

The public consultation period for the draft CWA is completed and the final document will be available for free view and download from CEN/CENELEC website in short term.

STRATEGY
Interoperability for crisis management

2 https://www.cencenelec.eu/news-and-events/news/2023/workshop/2023-05-02-cwas-cen-ws-ipci/



# Artificial Intelligence based Complex Event Processing

*By Nicola Durante and Ilmija Asani, ENG*

Different kinds of interconnected service providers such as sensors, mobile phones, and household equipment generate a huge amount of data. When it is processed in a timely manner, the data collected can provide valuable information to better understand the status of their surroundings.

In PRECINCT, ENG developed the Artificial Intelligence based Complex Event Processing (AI-CEP) that analyzes and processed incoming data as simple events and can identify patterns that lead to complex events. The CEP pattern recognition uses predefined rules, written with the help of a domain expert, that describe the patter of simple events needed to produce a complex event.

The CEP has four types of rules, each one is interpreted by a specialized agent able to carry out a procedure on the event:

- The validation process allows to identify inconsistencies in the received event and tries to solve them when it is possible.
- The enrichment process tries to enrich validated simple events with pertinent information. It is driven by a set of enrichment rules that provide the set of information about the types of enrichment to apply and the characteristic of the events to which these enrichment operations must be applied.
- The aggregation process identifies a set of already processed enriched simple events belonging to the same category and that are timely-spatially correlated with the current one, and that can be aggregated in a single event. The condition to be satisfied to proceed with the aggregation is provided through the rules.
- The fusion process continuously tries to identify patterns of aggregated events that are related to specific threats. These events are fused together by producing a new complex event. The event patterns are provided by a set of "Fusion Rules" that provide the patterns to match along with the characteristics of the event that will be produced by the fusion process when the pattern will match.

The traditional approach to CEP rule creation still requires an extensive and sometimes unattainable understanding of the relationships between events by the domain experts that write the rules. This operation can be problematic since it lowers the system's reliability and limits the complexity of the patterns that can be found.

In the PRECINCT scope, ENG developed a machine learning extension able to create CEP rules which, starting from a set of events, can write rules automatically and post them to the CEP APIs to activate them. This process analyzes the events happened during a time period and produces a decision tree that represents the new rules. The decision tree is then converted in the format that the CEP expects and finally, the domain expert is asked to review the rules before they are sent to the CEP.

The representation of correlated cyber-physical threats, produced by the CEP and illustrated in Figure 1, empowers users of the PRECINCT platform to acquire deeper insights into potential threats emerging within the network of Critical Infrastructures (CI). This improved understanding enhances their awareness and can contribute to the improvement of the system's overall resilience.

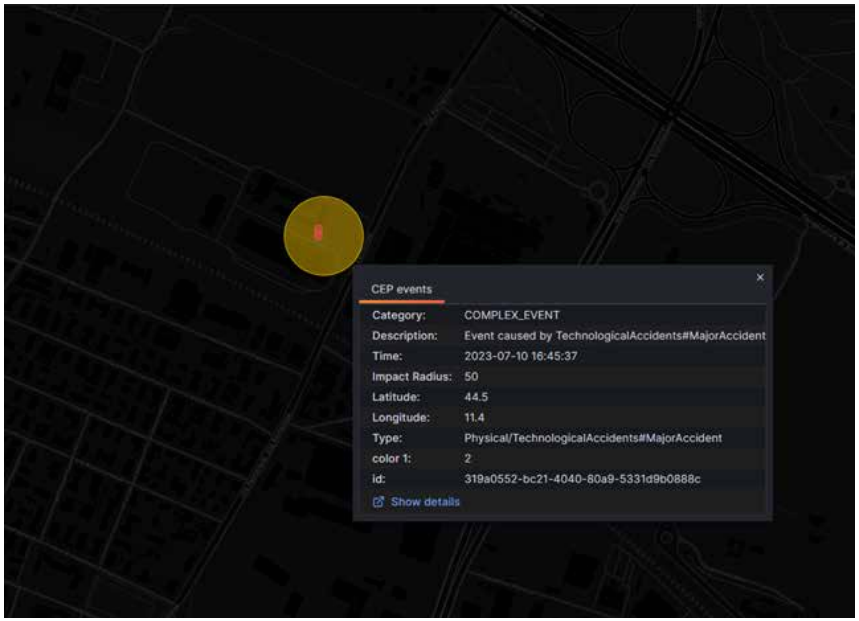


*Fig 1: Visualization of CEP events.*



# The PRECINCT Digital Twin and Serious Game deployed in LL2 Operation Antwerp

*By Shirley Delannoy, Researcher, Vias institute*

*"June 26, 2023, 8:47 am: Antwerp CP-OPS is established, the crisis management team is gathered, the LL Operation Antwerp demonstration session is about to start."*

After 20 months of intense collaboration, meetings and brainstorms, and several trainings and preparatory sessions, here we are. This is our final achievement: the LL2 Antwerp PRECINCT tools are demonstrated. We could not have dreamt of a better opportunity to test and assess the PRECINCT tools and components than a CP-OPS training. And this is what the LL2 partners and stakeholders did.

By applying the user-centred approach of the Living Lab, the activities carried out throughout the LL2 Operation Antwerp lifecycle aimed to contribute to and utilise the PRECINCT Reference Framework models to establish a dependencies map between CIs in the Antwerp region. This dependencies maps identifies the different interdependencies and effects the flood event could have on the CIs and emergency services. This objective was reached thanks to the close collaboration and work carried out with the Police of Antwerp (PZA), and the representatives of the CP-OPS and the Crisis Management team of Antwerp (both, indirect stakeholders), and the PRECINCT partners. This collaboration enabled to identify the pertinent scenarios to be deployed in the LL2 Operation Antwerp, and to map the use cases, the needs, and the current practices of the Emergency responders and stakeholders of Antwerp if flooding occurs in the city.

The experimentation environment and innovation testbed established within the LL2 Operation Antwerp facilitated to evaluate and improve the enablement and empowerment of Antwerp CI communities to achieve tangible benefits from the connected CIs resilience approach. In using CP-OPS practices as a baseline, LL2 Operation Antwerp explored and mapped the options to identify the vulnerabilities and needs and improve the capabilities of the 2 major PRECINCT tools: the Digital Twin (DT) and the Serious Game (SG).

*Fig 2: CP-OPS training for the LL2 Operation Antwerp Demonstration.*

In setting the DT and the SG deployment and demonstration into a real CP-OPS training context, it enabled the end users to interact and assess the tools functionalities and benefits as they would do in their real practice. The end users are the CP-OPS disciplines (police, fire department, medical services, civil protection and crisis communication) and the City's crisis management team. During the demonstration session, the end users had the opportunity to interact directly with the LL2 DT prototype and use it as they would do if they were facing a flood threat. The participants were immersed into a flood event and went through a 6 steps iteration to assess the functionalities of the tool, such as the flood probabilities and prediction, the CIs typology and mapping, etc. The demonstration ended by showcasing what would have happened to Antwerp if they had to face the 2021 Walloons flood.

*Fig 3: City of Antwerp map and flooded areas. User Interface DT LL2, modelling of the Walloons flood.*

In addition to the DT, 3 disciplines (police, medical and fire departments) and the crisis management team have assessed the LL2 SG. Successful run, the SG demonstration has highlighted the training purposes addressed to the Emergency responders and tactical decision makers. Moreover, the crisis management team has stressed the concrete added value of the SG tool capabilities to enhance strategic resilience decision-making process.

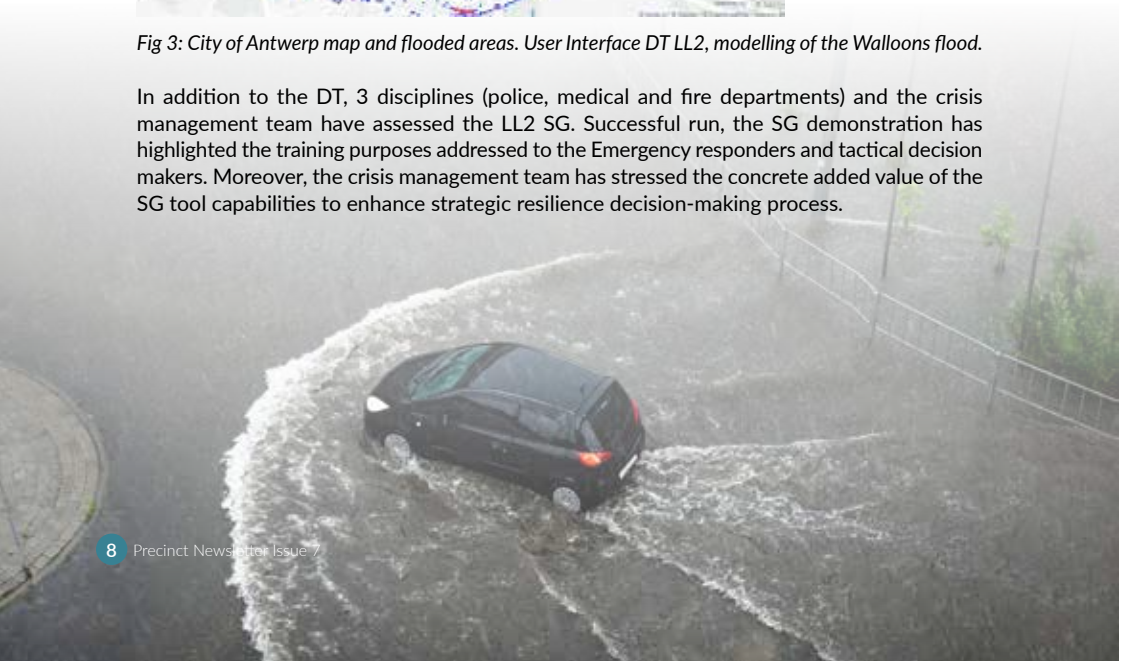



*Fig 4: Second Demonstration of LL2 SG (online - print screen).*

While this very ambitious and challenging project is touching to its end, it can be proudly stated that the user centred approach, the development process applying an iterative approach and the interactive demonstration have enabled to reach and meet the LL2 Operation Antwerp objectives:

- To represent the CIs network topology.
- To detect flood threat and alert flooding conditions.
- To visualise flood prediction and possible impacted areas.
- To provide an objective state of the situation.
- To provide mitigation actions.

The societal and decision-making process challenges PRECINCT project addressed are finding their echoes in the flood events European Cities faced in the first half of 2023. The cascading effects designed during the project and observed in past events (Wallonia in July 2021; Bologna in May 2023) shows the disastrous consequences a flood can have on a city, a region, a country. These societal challenges addressed by PRECINCT project and tools were also stressed out by the Emergency responders' representatives of LL2 who have identified the unpredicted evolutions a flood can have, and the catastrophic consequences previous decision taken had. By integrating the early warning system, the CIs interdependencies map and the flood prediction capabilities, the PRECINCT Digital Twin developed and deployed in LL2 Operation Antwerp aims to support the Emergency responders' decision-making and will benefit the citizen and CIs operators' resilience. This societal and strategic challenges are answering to the national Emergency services and crisis management team's current vulnerabilities and needs.

*N.B.: The LL2 Operation Antwerp task leader, VIAS institute, would like to sincerely thank the CP-OPS and crisis management team representatives for their commitment and participation, and the PRECINCT partners for the constructive collaboration.*

# Development of LL2 Digital Twin

*By Mircea Iacob, Architect & Project Lead, IMEC*

To make possible the development of the digital twin, we initiated the user story map as an innovation process to describe the interaction journey of the living lab. This user story map includes the interaction with the tools, systems, and data sources/models to support the decision-making process, and it is used as starting point of the LL2 Digital Twin (DT) prototype. This helped direct the DT architecture by the different technical providers of the components.

During the development of the Digital Twin, a lean and agile methodology was used. Concretely this means that every 2 weeks (a sprint) we focused on delivering value for the living lab. By delivering value and demo to the Living Lab every 2 weeks, feedback could be gathered at an early stage and questions for the next sprint could be more concrete to solve.

For a Digital Twin, the user interface (UI) is just the emerging part of the iceberg. We are now going to iterate over the integration of models/components delivered by the other partners.

In collaboration with the living lab, we identified the critical infrastructures to use for our use case, related with flooding in the city of Antwerp. There was chosen to take nodes in the centre of the city around the "stadspark" of Antwerp since this is known as an area that is sensitive to flood.

These critical infrastructures and the dependencies between them have been modelled into an interdependency graph. More, this graph also contains the state (value from 1 to 5) and the threats/mitigation actions that apply to each node. The interdependency graph is part of the application programming interface of Cascading Effect Simulation Engine (CESE) allowing this last one to calculate the impact of an event onto the whole network of critical infrastructures.

Is the digital twin who orchestrates CESE to allow the user to perform simulations and so better understand the impact of a specific threat. To make this visible to the end user, there was provided in the Digital Twin UI an additional "what-if" section. On top of CESE, the Resilience Supervisory Control (RSC) model can be used to list the actions to be executed for improving the CI nodes state after a disruptive threat occurred.

*Fig 5: Interdependencies and CIs in LL2 DT.*

## Integration of the flood model

Due to the climate changes observed in the last years, we wanted to handle the use case of flash floodings. Therefore, DT orchestrates a flood model run every 5 minutes.

Since forecasting flooding includes uncertainty, this requires implementation of a stochastic rainfall forecast. By running the model multiple times with some random variations, we can improve the accuracy of the model and so the confidence in its prediction. This gives us an ensemble of multiple forecasts for each simulated timestamp.

Considering a model run gives prediction for future two hours, with a prediction every 5 minutes, the flood model outputs 24 ensembles (120 minutes divided by 5) that contain 20 predictions each. It ends with the digital twin that handles 480 files every 5 minutes, and it is important to make the output information easy to understand and smooth to display in the user interface.

To make these statistics better visible to the end user, there was chosen to make a slider and fix one of the two parameters:

- A first slider is the probability slider. The user can fix a certain probability (eg. "20%"). The map then visualizes the predicted flood height in the city that 20% (or 4 from the 20) models predict. The colours on the map then correspond to flood height in meters.
- A second slide is the height slider. The height slider allows the user to fix a certain flood height. The colours on the map then correspond to a certain probability that this height is predicted.

Height slider:


*Fig 6: Height slider in LL2 DT.*

DT also enables CP-OPS representatives to receive email alerts in case of flood detection. Every model output is analyzed in the DT and following some thresholds defined with the domain experts, email alerts are being fired. Following the receival of an alert, the stakeholders can connect to the DT UI and monitor closely any changes.

# PRECINCT LL3 Input

*By Ioannis Lymaxis, Research Project Manager, Inlecom Commcercial Pathways*

The PRECINCT Living Lab 3 – Operations Athens is nearing to completion. Over the past months, the collaborative efforts of LL3 and project's technical partners have been concentrated on the design and application of PRECINCT resilience methodological framework for the LL3 case, the development, and customizations of PRECINCT tools to LL3 end-user's requirements. These efforts culminated in three well-structured demonstrations, organized and moderated by INLECOM, on the following dates:

- June 12th – First Demonstration: LL3 Digital Twin and Execution of Threat Scenario
- June 26th – Second Demonstration: LL3 Cyber-range
- July 11th – Third Demonstration: LL3 Serious Game

During the first demonstration the LL3 Digital Twin solution was presented to LL3 CIs stakeholders. In addition, LL3 DT capabilities were showcased to LL3 audience through the execution of its main Threat scenario. It should be noted that over 40 people participated in this season from the various LL3 CIs departments, and with different backgrounds such as for example Crisis Planning Supervisors, Transport Engineers, Data Analysts, System and Information Security engineers etc. Finally, recognizing the diverse audience of LL3, a comprehensive series of training sessions were conducted, by the project technical partners, on the same day and prior to the scenario execution. This ensured that all stakeholders and end-users remained up to date about project outputs, the DT platform logic, and on how to use its components.

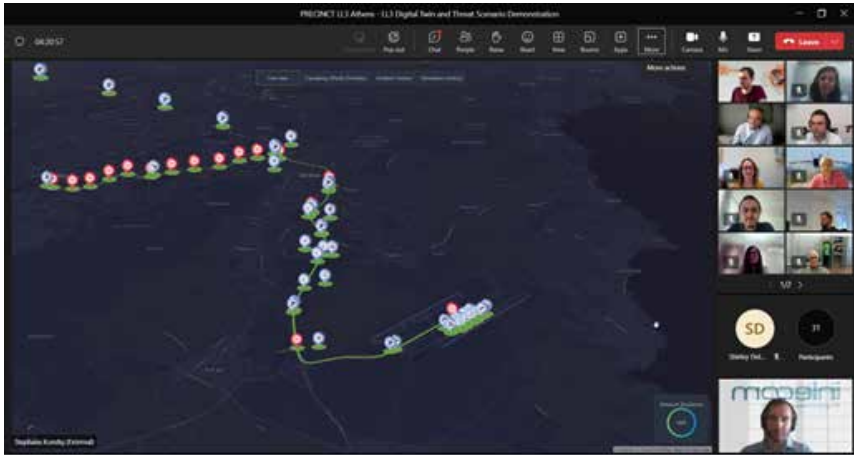

*Fig 7: PRECINCT LL3 – Digital Twin Demonstration Session.*

In the following weeks, the LL3 Cyber Range and Serious Game demonstration took place, respectively. In the former session, members from the Airport and ATTD Network Centre actively participated in a customized cyber exercise developed by TNCL. This exercise was tailored to LL3's Threat scenario and was executed in collaboration with Athens International Airport members. The cyber exercise was structured into three distinct stages or missions, were LL3 participants by answering various questions were trained in identifying cyber-attacks, draw from real-life cases and utilizing actual data sourced from LL3 CIs network infrastructures. Finally, the focus of the last demonstration was on the LL3 Serious Game and users defence strategies. The aim was to gather diverse choices and gameplay records from LL3 end-users in order to be analyzed, with the utter goal to identify the most effective choices and strategies for improving the resilience of the network.

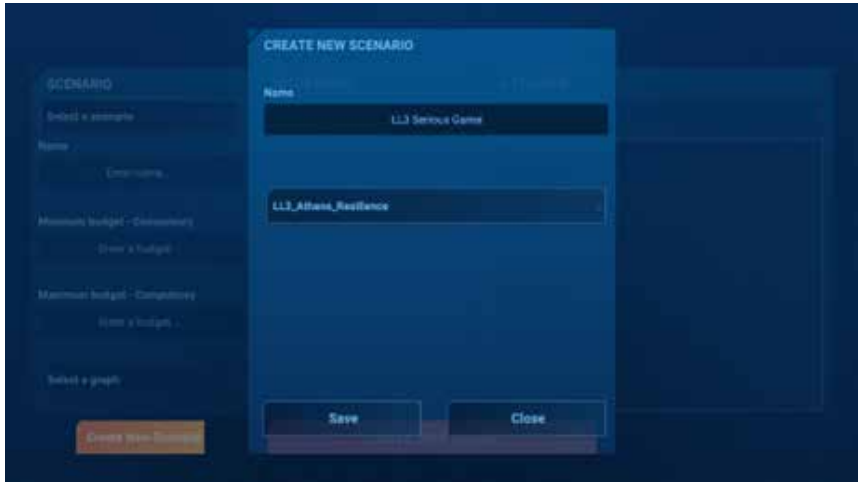


*Fig 8: PRECINCT LL3 Serious Game App Screenshot.*

In conclusion, the PRECINCT framework and solutions establish a comprehensive and unified approach to managing cyber-physical security. This approach aims to enhance the security of critical infrastructures against intricate cyber-physical threats. As per LL3 CIs end users' evaluation and positive feedback, the PRECINCT framework and DT have brought together the private and public stakeholders within LL3's geographical region. This achievement is materialized by the holistic situational awareness picture provided by the LL3 DT interface provides and its incident reporting capabilities. Furthermore, the DT solution can enhance communication and facilitate collaboration among the different stakeholders involved during a crisis compared to the current situation, according to LL3 CIs view. Finally, LL3 end-users also found that DT platform capabilities offered to them could improve the threat response and mitigation actions, consequently elevating the overall security and resilience of the CIs network.

# 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