PROCRUSTES

RISK ASSESSMENT AND TREATMENT FRAMEWORK AND GUIDELINES

D5.1

JUNE, 2023

H.F.R.I. Hellenic Foundation for Research & Innovation

The Project PROCRUSTES has duration three years (23/12/2019-22/06/2023) and is funded by the Hellenic Foundation for Research and Innovation (H.F.R.I.) under the "First Call for H.F.R.I. Research Projects to support Faculty members and Researchers and the procurement of high-cost research equipment grant" (Project Number: HFRI-FM17-2918)

DELIVERABLE NUMBER	D5.1	**WORK PACKAGE**	WP5

DELIVERABLE TITLE

Risk Assessment and Treatment Framework and Guidelines

ABSTRACT

This deliverable reports the PROCRUSTES risk assessment and treatment framework and the associated platform. The PROCRUSTES platform inter alia aligns the overall processes with industry standards and the newest legislative provision of EU Directives that dictate the minimum required procedures of water utilities. The purpose of the risk assessment and treatment framework is to quantify risk (WP2), calculate risk impacts using the assembled toolkit (WP3) and propose suitable risk reduction measures from those screened using the RRKB and passed using the stress-testing platform (WP4). The capabilities of the semantically enriched platform are showcased through a series of use cases that demonstrate the multiple levels at which the PROCRUSTES platform supports decision-making at the tactical and strategic levels through contextualizing and harmonizing risk information.

DELIVERY DATE	DELIVERABLE AUTHORS
14/06/2023	**Georgios Moraitis** **Georgios Karavokiros** **Dionysios Nikolopoulos** **Ioannis Tsoukalas**

QUALITY ASSURANCE

19/06/2023	**Dimitrios Kalogeras (ICCS)**

DOCUMENT STATUS				APPROVED BY
DRAFT	☐	**FINAL**	☒	Christos Makropoulos – 22/06/2023

H.F.R.I. Hellenic Foundation for Research & Innovation

The Project PROCRUSTES has duration three years (23/12/2019-22/06/2023) and is funded by the Hellenic Foundation for Research and Innovation (H.F.R.I.) under the “First Call for H.F.R.I. Research Projects to support Faculty members and Researchers and the procurement of high-cost research equipment grant” (Project Number: HFRI-FM17-2918)

TABLE OF CONTENTS

The Project PROCRUSTES has duration three years (23/12/2019-22/12/2022) and is funded by the Hellenic Foundation for Research and Innovation (H.F.R.I.) under the “First Call for H.F.R.I. Research Projects to support Faculty members and Researchers and the procurement of high-cost research equipment grant” (Project Number: HFRI-FM17-2918)

LIST OF FIGURES

H.F.R.I. Hellenic Foundation for Research & Innovation

The Project PROCRUSTES has duration three years (23/12/2019-22/12/2022) and is funded by the Hellenic Foundation for Research and Innovation (H.F.R.I.) under the "First Call for H.F.R.I. Research Projects to support Faculty members and Researchers and the procurement of high-cost research equipment grant" (Project Number: HFRI-FM17-2918)

H.F.R.I. Hellenic Foundation for Research & Innovation

The Project PROCRUSTES has duration three years (23/12/2019-22/12/2022) and is funded by the Hellenic Foundation for Research and Innovation (H.F.R.I.) under the “First Call for H.F.R.I. Research Projects to support Faculty members and Researchers and the procurement of high-cost research equipment grant” (Project Number: HFRI-FM17-2918)

LIST OF TABLES

LIST OF ACRONYMS

HFRI	Hellenic Foundation for Research & Innovation
RRKB	Risk Reduction Knowledge-base
RRM	Risk reduction measure
ABM	Agent-based Model
CPS	Cyber-physical System
WP	Work package

1 Introduction

The current and future landscape of the water industry has been reshaped by the transformational power of digitalisation and the proliferation of IoT technologies. The emergent modus operandi of urban water systems builds on an integrated cyber-physical architecture and forthcoming information schemes (Makropoulos and Savić, 2019). These incorporate novel informatics and computer technologies, such as Big Data, IoT and Cloud computing, as well as innovations from the field of information and communication technologies (ICT), such as optical fibres and 5G cellular connectivity (Lu, 2017), along with hydraulic infrastructures. The operations of such cyber-physical systems (CPS) rely on a continuous information, computation and action loop between the associated cyber and physical layer devices that synthesise them (Rajkumar et al., 2017). In an urban water CPS, this loop employs sensors (e.g., pressure or water quality sensors) for on-site data collection, a wireless and/or wired data transmission network to pass information, and a set of computational decision systems to define actions and remotely control the operation of actuators in the field (e.g., valve settings) to regulate the system. A conceptual representation for the monitoring, transmission and actuation loop in a water CPS can be seen in Figure 1.

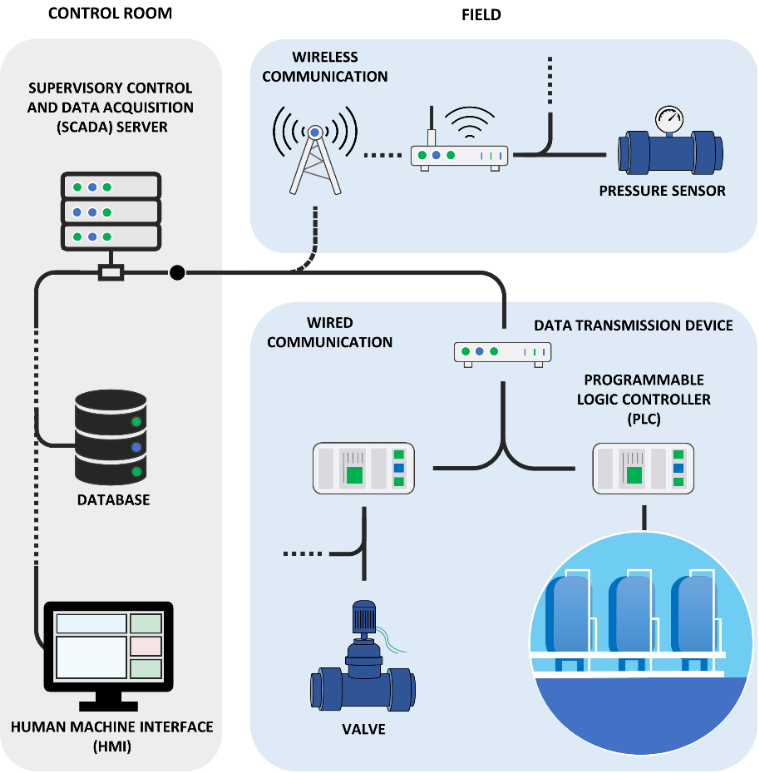

CONTROL ROOM
FIELD
SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) SERVER
WIRELESS COMMUNICATION
PRESSURE SENSOR
WIRED COMMUNICATION
DATA TRANSMISSION DEVICE
PROGRAMMABLE LOGIC CONTROLLER (PLC)
DATABASE
HUMAN MACHINE INTERFACE (HMI)
VALVE

Figure 1 Conceptual representation of a water CPS (monitoring/observation, transmission, computation and actuation components) (source: *Moraitis et al., 2023*).

Besides technical opportunities and merits associated with the transition of conventional systems into cyber-physical ones (Lee, 2015; Savić, 2021), the systems are also challenged by previously unknown and complex threats, stemming from the cyber domain (Loukas, 2015). In particular, the transition into CPS inevitably expands the previously available attack surface of the systems, as they inherit the vulnerabilities of the cyber layer and allow the implementation of the tactics, techniques and procedures (TTPs) of cyber-attackers (Johnson et al., 2016). In this emerging threat scene, the physical barriers are subordinated, and the potential attackers can leverage cyber access gates to infringe upon the system, gain control and eventually harm the system remotely. This has been the case for several recent attempts against the water sector world-wide, successful or otherwise. Examples of such incidents include the remote manipulation of a dosing system in Oldsmar's water treatment plant, that led to harmful concentration levels of sodium hydroxide (Robles and Perlroth, 2021), the 60-day PLC manipulations in the anonymised "Kemuri Water Company" that tampered with various asset settings and caused service disruptions (Verizon, 2016), as well as a series of allegedly state-affiliated cyber-physical attacks against Israel's water infrastructure (Cimpanu, 2020).

Such incidents have proven the capacity of the new attack vectors to cause deviations from the legal/regulatory levels of quality, quantity, continuity and pressure levels in supply systems (CEN-EN 15975-2, 2013), threaten the wellbeing of communities and possibly lead to severe reputational and/or financial damage for water utilities. Thus, being a force to be reckoned with, cyber-physical threats introduce a new challenge for the resilience of the sector while they push the boundaries of traditional risk assessment and the available tools and approaches. This is widely acknowledged by the sector as proven by a recent poll on 504 water utilities of the USA by the Water Sector Coordinating Council (WSCC). In their recently published report on the cybersecurity state of the sector and the challenges ahead (WSCC, 2021), the water utilities identified that the 2 major challenges for water utilities, and thus of high priority in years to come, are (a) business continuity and disaster recovery plans and (b) risk assessment and management of cyber threats. Moreover, the European Union Agency for Cybersecurity (ENISA), in its annual reports on cybersecurity and threats (ENISA, 2019; 2020; 2022), identifies a systematic increase in the frequency of attacks, while also acknowledges that assessing cyber-physical threats will be an ever more challenging task as a result of the increasing complexity of threats and the expansion of available vulnerabilities in cyber-physical systems. To this end, the EU published both the Directive (EU) 2022/2557 on the resilience of critical entities and the NIS2 Directive (EU) 2022/2555 on cybersecurity. Under the new EU legislative umbrella in force, member states and critical infrastructure stakeholders are asked to break the silos between cyber and physical risk management and follow a new path towards combined cyber-physical resilience of their critical systems and services. This transition, however, requires not only a shift in mentality of the engaged parties, but most importantly, a rethinking of the risk assessment practices and techniques that will help to overcome the challenges and limitations posed by the complexity and obscure nature of the emerging threat landscape.

2 The PROCRUSTES Risk Assessment & Treatment Framework

2.1 The PROCRUSTES Framework and supporting platform

The PROCRUSTES risk assessment and treatment framework is designed as a systematic and structured approach for identifying, analysing, and evaluating potential cyber-physical threats and uncertainties that may affect a utility's services and objectives, while also supporting the identification and evaluation of suitable risk reduction measures. At its core, PROCRUSTES is designed to accommodate the quantitative risk assessment of cyber-physical risks, to evaluate and quantify risks associated with the operations, security, and resilience of the system in hand. Utilising the developed quantitative risk assessment, utilities can gain a deeper understanding of their risks, prioritize mitigation efforts based on quantitative analysis of their efficiency, allocate resources more effectively, and make data-informed decisions. The processes, supported by the dedicated PROCRUSTES platform, involve the quantitative assessment of both the likelihood and the potential impact/consequences of cyber-physical threats, that synthesise the risk level. The framework also foresees the identification and prioritisation of threats at system and asset level, as well as the identification of critical assets against a given type of cyber-physical attack. The potential application of the framework also extends to the investigation of the periodic/seasonal changes in the risk level of utilities that service tourist destinations. The models can adjust to both seasonal demand conditions and the population changes that can affect the interest of attackers, to explore the variations in risk level that such utilities face during different periods, under the same cyber-security posture and system design.

The developed framework and the supporting platform are designed to serve the fundamental risk assessment and treatment steps, in accordance to international standards, such as the American Water Works Association J100-10 Standard (AWWA, 2010) for risk and resilience management of water and wastewater systems and the updated ISO 3100:2018 risk management principles and guidelines (ISO, 2018). The risk assessment framework processes can be summarised as:

- **Risk Identification:** The process of identifying and characterising potential threat events specific to the utility considering systems' design, dependencies, and cascade paths as well as the internal and external factors that may impact security and reliability (incl. existing cybersecurity and mitigation measures).

- **Risk Analysis:** The process of analysing identified threats and risk sources to quantitatively estimate the likelihood and the potential impact of potential threat events, considering existing measures and operational rules. This process should also assist the asset characterisation, i.e., to identify and prioritise the critical assets of a system that perform or support critical functions and operations.

- **Risk Evaluation:** The process of mapping and comparing the risk analysis results through suitable quantitative performance metrics that depict the severity of the identified threats, including the level of risk as the combination of consequences and likelihood, under the existing measures and operational rules. This step must consider both the risk criteria of the utility and any legislative or regulatory provisions to define if a threat is acceptable or exceeds the risk tolerance and needs to be mitigated.

- **Risk Treatment Analysis:** The process of identifying and analysing the performance of the system under new, suitable, and proportional measures for the threats that exceed the utility's risk tolerance. Those measures can include processes, operational rules, policies, practices, or devices which modify the risk in terms of likelihood, consequences, or both.

- **Risk Treatment Evaluation:** The process of mapping the risk treatment analysis results under the same criteria and metrics used for the risk analysis, to allow the comparison between the current risk and the modified risk characteristics, and ultimately derive the effectiveness of the selected measures and/or their combination to support the preparation of risk treatment plants.

In addition to the above-described quantitative risk assessment and treatment steps, PROCRUSTES also supports utilities in the subsequent risk management processes of:

- **Record and Report:** The process of creating and maintain records of the risk assessment processes including the identified risks, their analysis, evaluation, and treatment plans. Those records and derived reports can be used to communicate risk-related information to decision-makers, stakeholders, and any relevant authorities.

- **Communicate and Consult:** The process of establishing effective and direct communication channels to share risk information and promote awareness among stakeholders, in an interdepartmental manner. This process also allows the engagement and consultation of experts across the utility, to gather their insights, perspectives, and expertise and facilitate informed decision-making and improve the overall understanding of risks.

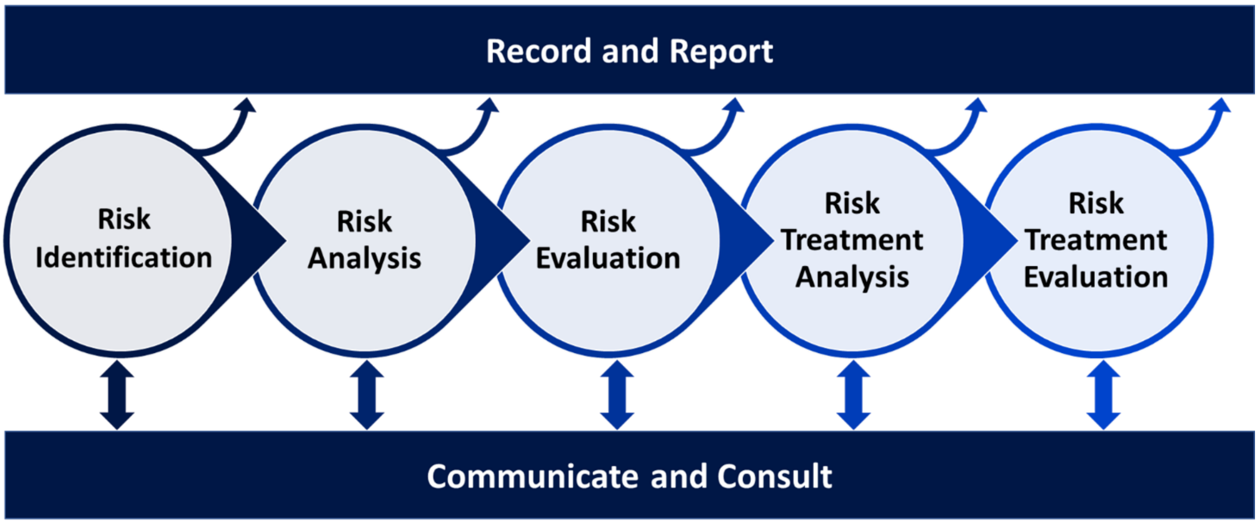


Figure 2 PROCRUSTES Risk Assessment and Treatment Framework processes

By conducting a risk assessment, organizations gain valuable insights into their current exposure to the surrounding cyber-physical threat landscape, i.e., the dynamic and evolving range of risks and vulnerabilities that can compromise the security and resilience of a water utility's cyber-physical infrastructure. By recognizing and comprehending these threats, water utilities can develop effective strategies to mitigate risks and protect their critical operations.

The PROCRUSTES framework allows water utilities to proactively identify vulnerabilities, assess and prioritise risks, detect critical assets and develop strategies to enhance the resilience of their cyber-physical systems, in accordance with the legal and regulatory provisions.

The overall PROCRUSTES approach is designed to support water utilities in respect to:

- **Proactive Risk Management:** Risk assessment enables organizations to identify potential risks and vulnerabilities before they materialize into actual incidents. By proactively assessing risks, organizations can develop strategies to prevent or mitigate potential threats, reducing the likelihood of costly disruptions to operations.
- **Strategic planning and resource allocation:** Risk assessment allows organizations to allocate resources effectively by prioritizing risks based on their potential impact and likelihood. This helps in optimizing resource allocation, ensuring that mitigation efforts are focused on the most significant risks.
- **Decision-Making Support:** Risk assessment provides valuable information for decision-making processes. By understanding the risks associated with different options or courses of action, organizations can make informed decisions and select the most appropriate strategies that align with their risk tolerance and objectives.
- **Compliance and Legal Requirements:** Many industries and sectors are subject to regulatory and legal requirements related to risk assessment and management. Adhering to these requirements not only ensures compliance but also helps organizations demonstrate their commitment to stakeholder safety and due diligence.

To support the overall processes, the PROCRUSTES platform integrates a series of interchangeable tools for the analysis, management, and strategic response to cyber-physical threats against urban water networks. The platform supports users at all stages of the framework, from identifying and assessing potential threats in terms of their likelihood and potential impacts, to assessing the level of risk and exploring possible mitigation measures. The platform also adapts to the objectives and end goals of the processes, offering multiple levels of analysis, that allow (a) the investigation of either single scenarios or multiple scenarios and (b) facilitate both comprehensive, system-wide assessments and threat specific risk assessments. In addition, the platform allows for incorporation of uncertainty within the model chain, and/or optimization approaches, through stochastic demand timeseries and Monte-Carlo type analysis of scenarios. These are achieved through a sequence of interconnected models, integrated in the PROCRUSTES platform. A brief description of the tools is provided below.

2.1.1 CPRISK-ABM

The PROCRUSTES CPRISK-ABM (Koutiva et al., 2021; Moraitis et al., 2023) is a generic agent-based model aiming to simulate the behaviour of potential threat agents against key cyber assets of any utility with specific characteristics, as well as the effects a utility's actions can have on the threat landscape parameters. The model relies on a red team/blue team dynamic interaction and integrates the socio-technical mechanisms that lead to successful or unsuccessful attacks, according to the level of cyber-security of each utility. The cyber-security level of each utility derives from a semi-quantitative questionnaire that also adheres to the practices and provision of the Hellenic Ministry of Digital Governance National Cybersecurity Authority. The CPRISK-ABM simulates (a) the actions of utility personnel distributed in the network, controlling, and reinforcing nodes of the digital infrastructure and (b) attackers who follow independent behavioural rules of conduct to select their targets and execute attacks against them, according to their motivations and capabilities. Through an iterative process, the model simulates the dynamic equilibrium between the two parties and derives the probabilities of vulnerability-induced attacks against assets of the system and their characteristics.

2.1.2 SCENARIO GENERATOR (SG)

The Scenario Generator lays at the core of the PROCRUSTES platform architecture, as it is interconnected with most of the available tools, i.e., CPRISK-ABM, Stochastic Demand Generator, Stress-testing Platform and the Risk Reduction Knowledgebase (Moraitis et al., 2023, 2021). It is an automated scenario planning environment that a) supports and guides users in creating threat scenarios under the status quo or with the addition of measures, b) provides automated generation of multiple scenarios based on the CPRISK-ABM results, c) is responsible for managing the scenarios and their database, c) automatically prepares the input data of each scenario for simulation with downstream models, including the integration of stochastic demand timeseries and the Monte-Carlo type assignment of parameters, and d) provides easy and fast visualization of the results.

2.1.3 STOCHASTIC DEMAND GENERATOR (SDG)

The SDG is an embedded stochastic time series generation model capable of synthesizing realistic surrogate time series of historical demand patterns. This enables the simulation of multiple scenarios for a range of stochastic boundary conditions, and thus integrating uncertainty into the cyber-physical threat analysis chain (Moraitis et al., 2022; Tsoukalas et al., 2020).

2.1.4 RISK REDUCTION KNOWLEDGEBASE (RRKB)

An expandable and interactive knowledgebase that contains best practices and measures to mitigate or avoid cyber-physical risks. The measures can be aimed at either reducing the likelihood of occurrence or reducing the impact that threats can have on the system or acting in combination. The knowledgebase can link measures to specific threats to suggest the most relevant solutions, and is designed to be scalable, enabling the continuous incorporation of the newest best practices and novel technologies that can help address the threats faced by water utilities. Measures of the RRKB can also be assessed in terms of their performance by comparing the results of simulation scenarios with their application measures with the results of simulations with the scenario without them.

2.1.5 STRESS-TESTING PLATFORM

The Stress-Testing Platform is the embedded simulation engine of PROCRUSTES, which explores water distribution networks as cyber-physical systems by simulating the assets' behaviour at the cyber and physical layers and their interactions in a unified process. The simulation renders the sensing, computation and remote action loop based on the system's control logic and automations, that subsequently affect the hydraulic behaviour of the system. Besides individual asset behaviour, the stress-testing platform simulates the cascade both from edge devices upstream to the connected PLCs and SCADA, and from the control devices (i.e., PLC and SCADA) to the downstream connected edge devices. The platform is thus capable of quantifying the "physical" consequences of composite cyber-physical attacks against the various SCADA elements, including sensors, actuators and PLCs, i.e., the targets of the cyber-physical attacks. The behaviour of the cyber-physical system under threat, is mapped into suitable KPIs that capture the severity of the consequences in various dimensions, such as unmet demand, customers insufficiently supplied, population contaminated, earliest detection time, as well as spatial extend of the impacts. According to the end goal of the analysis, users can utilise the STP to explore (a) a specific threat scenario and estimate the potential consequences of a given event, (b) multiple variations of a threat scenario, to investigate the range of consequences and identify critical assets in the system, (c) the risk level of the utility against the surrounding threat landscape, to establish a bird's eye understanding of the current status or (d) the effectiveness of risk reduction measures and how they can alter the risks at hand. The STP allows the user to assess the exposure and resilience of an infrastructure, under normal conditions, under cyber-physical attacks and after incorporating risk reduction measures.

2.1.6 CYBER-PHYSICAL RESILIENCE SENSOR PLACEMENT OPTIMIZATION TOOL (CPR-SPOT)

The cyber-physical resilience sensor placement optimization tool (CPR-SPOT) (Nikolopoulos et al., 2022; Nikolopoulos and Makropoulos, 2023) is a module that strategically places sensors in a water distribution network, aiming at maximizing the resilience of the network against cyber-attacks that target water quality sensors. CPR-SPOT analyses threat events and places a user-customizable number of water quality sensors in a "resilient" way that retains good performance in nominal operation conditions and maximizes the expected performance when a subset of sensors is compromised (reporting fake readings or are offline) under scenarios of cyber-physical attacks in an increasing order of disturbance. CPR-SPOT maximizes the resilience score in two distinct sensor layout problems:

a) The generation of a new sensor layout that maximizes resilience in terms of a reducing the expected impact of cyber-physical attacks. The user specifies the number of sensors, the detection threshold for the contaminant, and the dosage threshold that is dangerous for consumers.

b) The upgrade of a pre-existing sensor layout by placing an extra sensor with the goal to maximize resilience in terms of reducing the expected impact of cyber-physical attacks. The user specifies the existing sensor locations, the number of extra sensors to be placed, the detection threshold for the contaminant, and the dosage threshold that is dangerous for consumers.

2.1.7 THE PROCRUSTES PLATFORM

The PROCRUSTES platform (Moraitis et al., 2021) embodies an advanced simulation and results analysis framework for water distribution networks, leveraging parallelisation techniques at the application/task level. This platform employs Celery, a sophisticated Python-based asynchronous job queue, enabling the efficient distribution of computational workloads across multiple threads or machines. Capitalizing on the capabilities of Celery, the current version of the PROCRUSTES platform can harness the full potential of the running server's 16 CPU cores – or any number *N* of CPU cores in future installations. Consequently, this allows for the execution of up to *N* concurrent tasks, each representing different attack scenarios. This architecture provides a substantial reduction in computational time for processes requiring extensive scenario simulations, such as sensitivity analysis and stress testing. Through this high-level parallelisation, PROCRUSTES provides a robust and scalable solution for simulating and analysing cyber-physical attacks on water distribution networks.

Overall, the platform is designed to support multiple users and different profiles, based on which the access and processing rights are defined by the administrator. In this way, sensitive information related to the operation or security of the infrastructure and unauthorised uses of the platform by staff without the appropriate credentials are secured.

More details on the tools and approaches can also be found in the relevant deliverables of WP2, WP3 and WP4 and on the PROCRUSTES publications, listed below.

- Moraitis, G., Sakki, G. K., Karavokiros, G., Nikolopoulos, D., Tsoukalas, I., Kossieris, P., and Makropoulos, C. (2023). "Exploring the Cyber-Physical Threat Landscape of Water Systems: A Socio-Technical Modelling Approach." Water (Switzerland), 15(9). https://doi.org/10.3390/w15091687
- Nikolopoulos, D., and Makropoulos, C. (2023). "A novel cyber-physical resilience-based strategy for water quality sensor placement in water distribution networks." Urban Water Journal, 20(3), 278–297. https://doi.org/10.1080/1573062X.2023.2174032
- Moraitis, G., Tsoukalas, I., Kossieris, P., Nikolopoulos, D., Karavokiros, G., Kalogeras, D., and Makropoulos, C. (2022). "Assessing Cyber-Physical Threats under Water Demand Uncertainty." EWaS5, MDPI, Basel Switzerland, 18. https://doi.org/10.3390/environsciproc2022021018
- Nikolopoulos, D., Moraitis, G., Karavokiros, G., Bouziotas, D., and Makropoulos, C. (2022). "Stress-Testing Alternative Water Quality Sensor Designs under Cyber-Physical Attack Scenarios." EWaS5, MDPI, Basel Switzerland, 17. https://doi.org/10.3390/environsciproc2022021017
- Koutiva, I., Moraitis, G., and Makropoulos, C. (2021). "An Agent-Based Modelling approach to assess risk in Cyber-Physical Systems (CPS)." Proceedings of the 17th International Conference on Environmental Science and Technology, Athens, Greece. https://doi.org/10.30955/gnc2021.00194
- Moraitis, G., Nikolopoulos, D., Koutiva, I., Tsoukalas, I., Karavokiros, G., and Makropoulos, C. (2021). "The PROCRUSTES testbed: tackling cyber-physical risk for water systems." EGU General Assembly 2021. https://doi.org/10.5194/egusphere-egu21-14903

2.2 Multi-user strategic planning

To support those processes operationally, the platform builds on a collaborative, cross-departmental workflow that allows different types of users to seamlessly pass and retrieve information/data from other colleagues and perform tasks, according to their profile. The PROCRUSTES platform is a "role-based access control" (RBAC) system, i.e., users are assigned roles that define their responsibilities and access privileges.

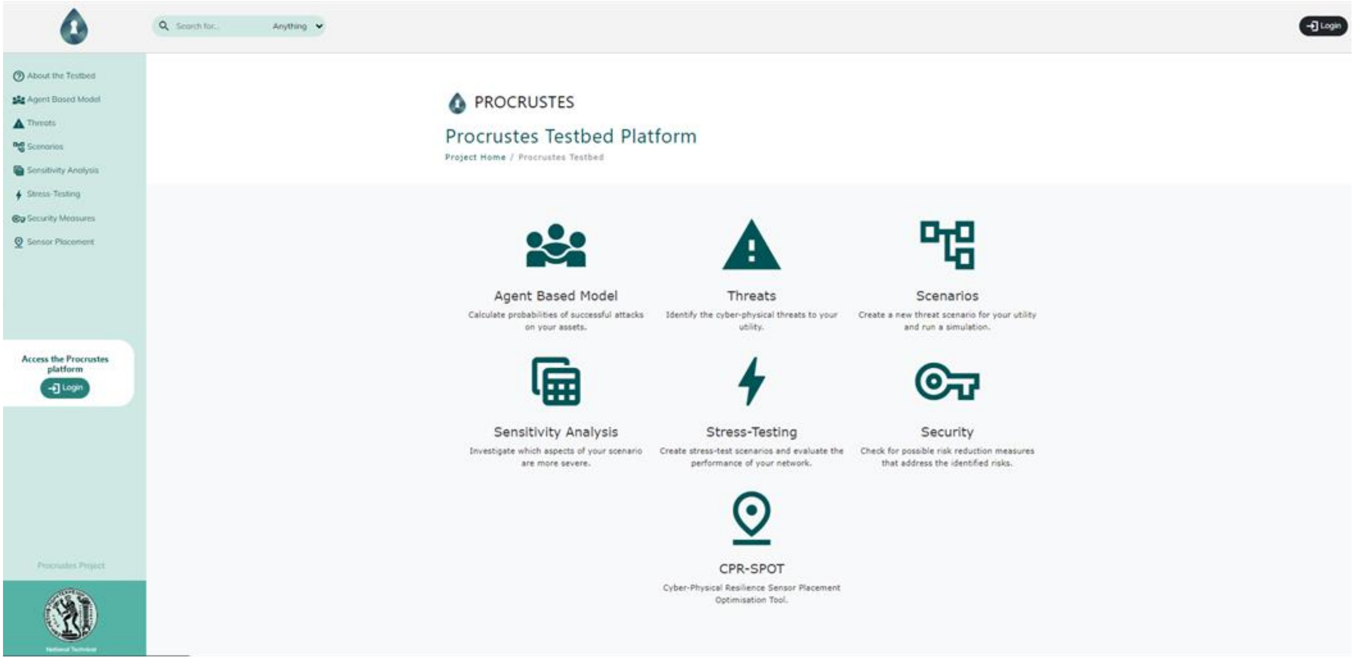
Each role has a predefined set of permissions and access rights associated with it. The platform enforces these access controls by allowing or denying users' actions and data requests based on their assigned roles. This provides a granular and flexible way to manage access based on user profiles and roles and ensures that users only have access to the capabilities and data that are necessary for their tasks or responsibilities while restricting access to sensitive or confidential information. This helps utilities maintain data privacy, security, and maintain proper segregation of duties and tasks in each step of the risk management process. Access to the PROCRUSTES Platform is structured around specific roles, each carrying its own set of permissions and access rights:

- **Utility Staff Member:** Staff members have view-only access to select utility data and procedure results. They are prohibited from executing simulations or other procedures.
- **Utility Data Manager:** Data Managers are granted access to view or modify their utility's data, subject to the Utility Administrator's approval. They typically have view-only access to aggregated utility data and can initiate processes on these data. Permissions can be adapted to conform to a utility's policy.
- **Utility Administrator:** Administrators possess unrestricted access to their utility's data. Unless service restrictions apply, Administrators can freely use the platform's functionalities.
- **System Administrator:** System Administrators have unlimited access to all data and functionalities, taking charge of the utility's management. System Administrators on the PROCRUSTES Platform have the capability to selectively enable an array of services for users within a specific utility, including the following:
    - Calculating the probability of successful attacks on utility assets via CPRISK-ABM
    - Creating and simulating single threat scenarios
    - Conducting a sensitivity analysis
    - Executing a stress-testing procedure
    - Determining the optimal position for quality sensors within the network

3 The PROCRUSTES Platform use case

3.1 Accessing the PROCRUSTES platform and Setting up the utility data

The main page of the platform (Figure 3) provides direct access to all available tools, depending on the rights of each user. Logging in to each user's existing account is done by selecting "Log-in" at the top right. The platform redirects the user to the log-in page, where the unique credentials (username and personal password) are required (Figure 4).



Agent Based Model
Calculate probabilities of successful attacks on your assets.

Threats
Identify the cyber-physical threats to your utility.

Scenarios
Create a new threat scenario for your utility and run a simulation.

Sensitivity Analysis
Investigate which aspects of your scenario are more severe.

Stress-Testing
Create stress-test scenarios and evaluate the performance of your network.

Security
Check for possible risk reduction measures that address the identified risks.

CPR-SPOT
Cyber-Physical Resilience Sensor Placement Optimisation Tool.

Figure 3 PROCRUSTES platform main page prior to log-in

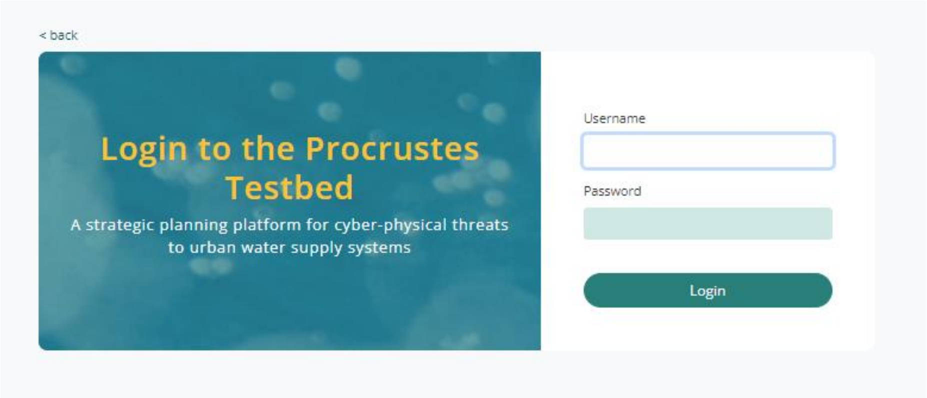
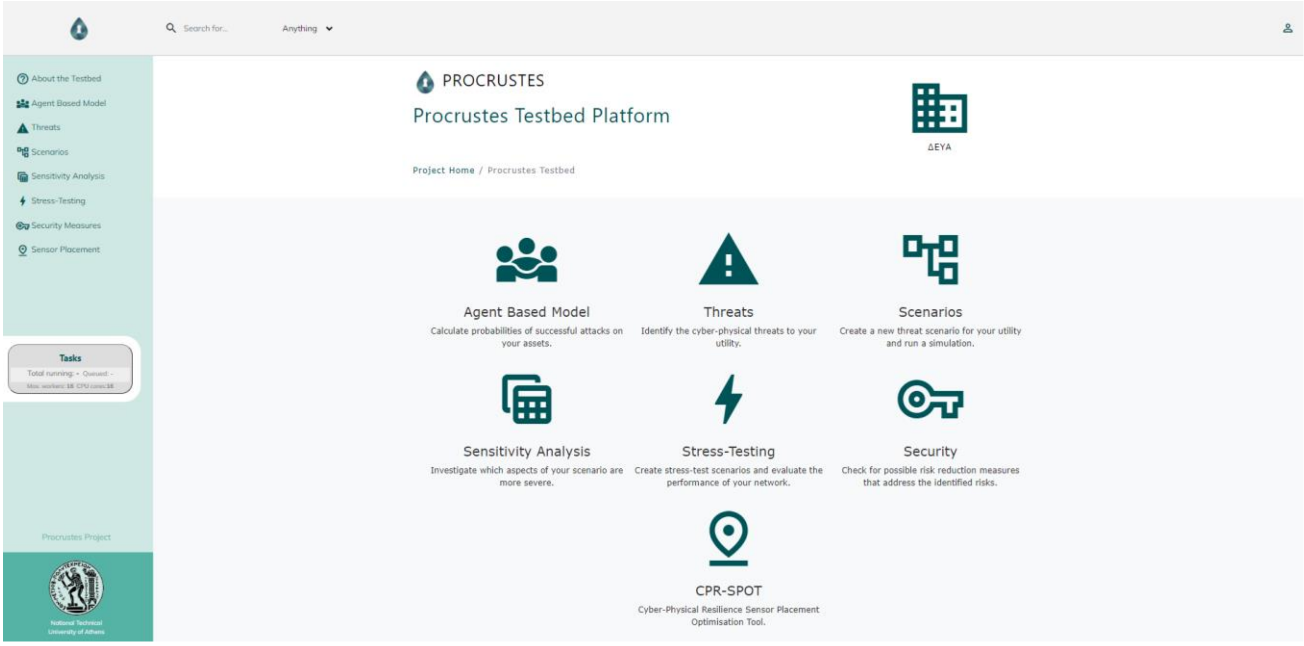

< back
Login to the Procrustes Testbed
A strategic planning platform for cyber-physical threats to urban water supply systems
Username
Password
Login

Figure 4 PROCRUSTES platform log-in page

After logging in to the platform, and according to the user’s access rights defined by the system administrator, the platform adjusts its content and active links (Figure 5). The platform provides access to the integrated tools and processes, through the relevant icons in the main page, or through the tab list on the left side of the screen that remains visible throughout the navigation.



Procrustes Testbed Platform

Agent Based Model

Calculate probabilities of successful attacks on your assets.

Threats

Identify the cyber-physical threats to your utility.

Scenarios

Create a new threat scenario for your utility and run a simulation.

Sensitivity Analysis

Investigate which aspects of your scenario are more severe.

Stress-Testing

Create stress-test scenarios and evaluate the performance of your network.

Security

Check for possible risk reduction measures that address the identified risks.

CPR-SPOT

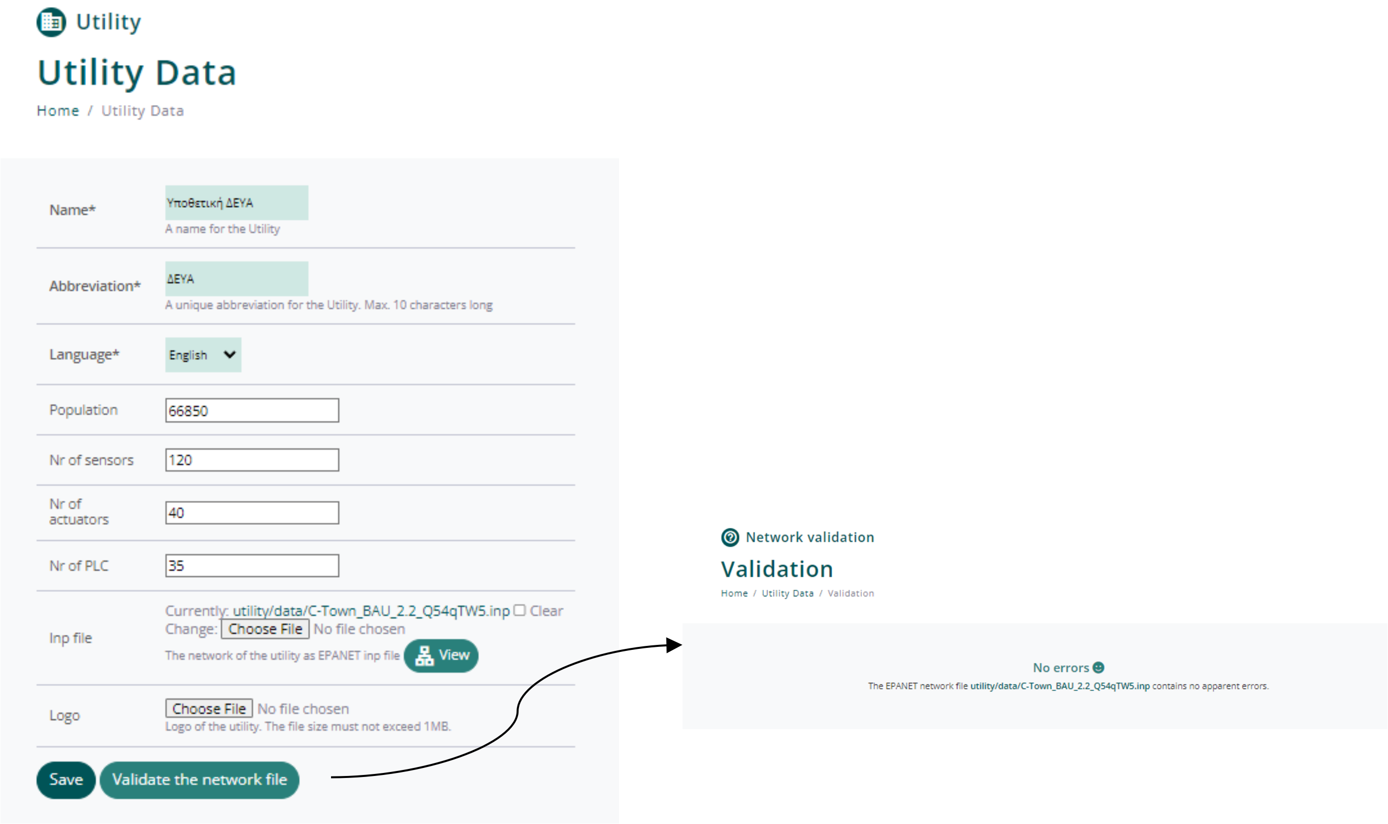
Cyber-Physical Resilience Sensor Placement Optimisation Tool.

Figure 5 PROCRUSTES platform main page after user log-in

In addition to the list of tools and automated process available to the user, the system also allows access to and editing of the Utility Data. When the platform is used for the first time, the set-up of the Utility's data is a mandatory step. This step will typically require a collaboration between modelling experts of the system and the risk assessors, under the supervision/guidance of the system administrator. As seen in Figure 6, the platform has a pre-set form of required data that follow the utility in the downstream processes. After assigning a name and an abbreviation for the Utility profile, the users are asked to provide information regarding the serviced population and the cyber-layer of the utility. To facilitate the supported quantitative analysis processes, users need to provide with a model of the utility's network in an EPANET 2.2. format[1].

For the purposes of the use case, we create a hypothetical water company that serves the water needs of 66,850 customers. Its digital infrastructure includes 120 sensors, 40 remote control devices for valves and pumps (actuators) and 45 PLCs fully connected to the central SCADA. For the quantitative analysis processes, we use the EPANET model of the C-TOWN network, and its operating rules. This model is based on a real medium sized network serving 5 DMAs, each with different demand profiles. The above information constitutes the main characteristics that make up the "profile" of the water company on the platform and are used to automatically adapt the downstream models to utility-specific parameters. Once the fields are filled in, the profile is created or updated by pressing the save button. To ensure the correctness of the model file, the platform also offers the option of verification as to the format and compliance to EPANET standards (see "Validate the network file" button in the UI snapshot of Figure 6). Please note that the model of the network can be of any level of detail, both spatially e.g., skeletonised layout of the system, and temporally, e.g., a model for a typical day or week of the system with an hourly analysis step.

[1] For more information on EPANET and the structure of the model, please see Appendix .



Utility

Utility Data

Home / Utility Data

Name* Υποθετική ΔΕΥΑ
A name for the Utility

Abbreviation* ΔΕΥΑ
A unique abbreviation for the Utility. Max. 10 characters long

Language* English

Population 66850

Nr of sensors 120

Nr of actuators 40

Nr of PLC 35

Inp file Currently: utility/data/C-Town_BAU_2.2_Q54qTW5.inp □ Clear
Change: Choose File No file chosen
The network of the utility as EPANET inp file

Logo Choose File No file chosen
Logo of the utility. The file size must not exceed 1MB.

Network validation

Validation

Home / Utility Data / Validation

No errors

The EPANET network file utility/data/C-Town_BAU_2.2_Q54qTW5.inp contains no apparent errors.

Figure 6 Utility data set-up page (left) and Utility's EPANET network file validation report (right)

After setting up the required utility data, the users can also visually inspect the selected network model and the layout, by clicking the "view" button in the utility data set-up page. The page offers a quick view over the layout, and the assets of the network, i.e., reservoirs, tanks, pumps, valves and consumption nodes. Figure 7 presents the layout of the C-town network used for the use case.

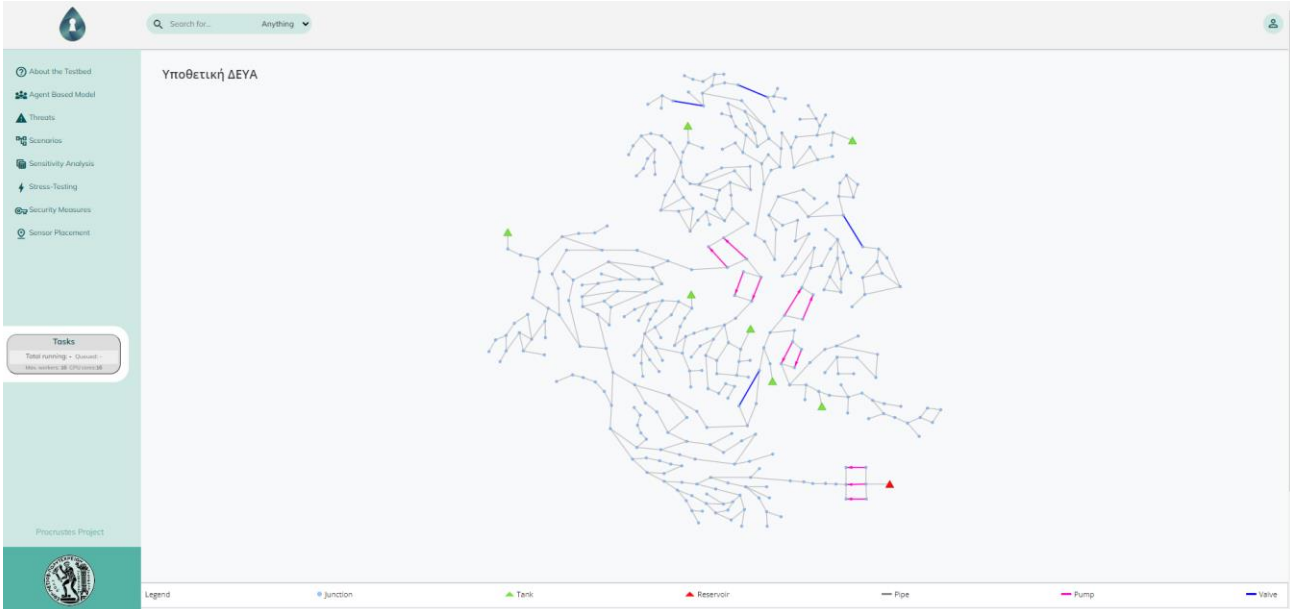
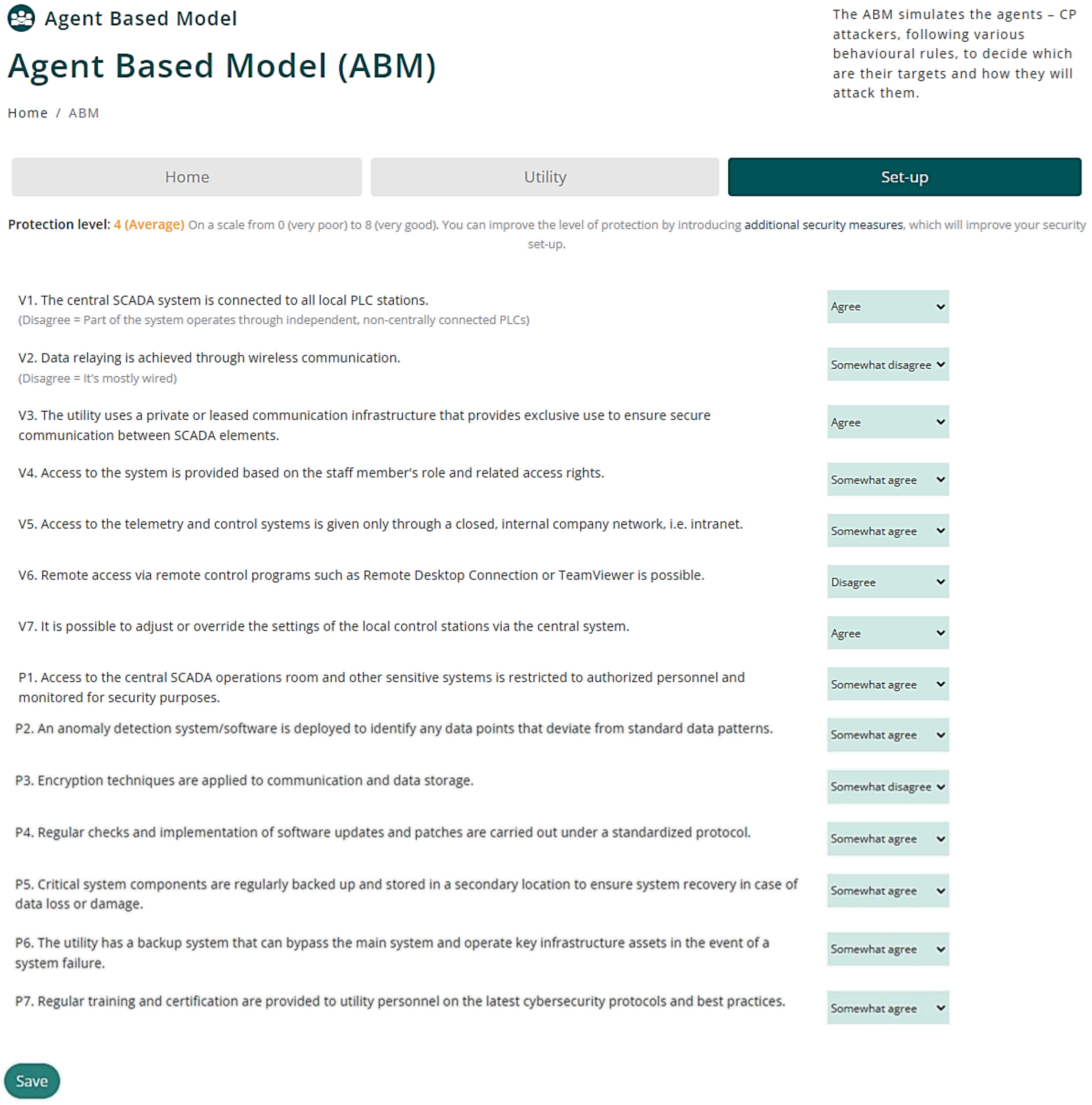


Figure 7 Network visualisation page

After completing the inserting the basic information of the utility, and the model of reference, the user can also use the embedded self-assessment questionnaire that helps capture the level of protection against cyber-physical threats. The user fills in the questionnaire Figure 8 which includes information on the practices and protection measures in place and is used by the platform to customize the models to the specific conditions of the utility.



Agent Based Model (ABM)

The ABM simulates the agents – CP attackers, following various behavioural rules, to decide which are their targets and how they will attack them.

Protection level: 4 (Average) On a scale from 0 (very poor) to 8 (very good). You can improve the level of protection by introducing additional security measures, which will improve your security set-up.

V1. The central SCADA system is connected to all local PLC stations. (Disagree = Part of the system operates through independent, non-centrally connected PLCs)	Agree
V2. Data relaying is achieved through wireless communication. (Disagree = It's mostly wired)	Somewhat disagree
V3. The utility uses a private or leased communication infrastructure that provides exclusive use to ensure secure communication between SCADA elements.	Agree
V4. Access to the system is provided based on the staff member's role and related access rights.	Somewhat agree
V5. Access to the telemetry and control systems is given only through a closed, internal company network, i.e. intranet.	Somewhat agree
V6. Remote access via remote control programs such as Remote Desktop Connection or TeamViewer is possible.	Disagree
V7. It is possible to adjust or override the settings of the local control stations via the central system.	Agree
P1. Access to the central SCADA operations room and other sensitive systems is restricted to authorized personnel and monitored for security purposes.	Somewhat agree
P2. An anomaly detection system/software is deployed to identify any data points that deviate from standard data patterns.	Somewhat agree
P3. Encryption techniques are applied to communication and data storage.	Somewhat disagree
P4. Regular checks and implementation of software updates and patches are carried out under a standardized protocol.	Somewhat agree
P5. Critical system components are regularly backed up and stored in a secondary location to ensure system recovery in case of data loss or damage.	Somewhat agree
P6. The utility has a backup system that can bypass the main system and operate key infrastructure assets in the event of a system failure.	Somewhat agree
P7. Regular training and certification are provided to utility personnel on the latest cybersecurity protocols and best practices.	Somewhat agree

Figure 8 Utility cyber-security questionnaire

The level of protection is obtained by evaluating the answers given to each of the questions, with the range varying between the qualitative scales from 0 - 8, with 8 being the highest possible. Once all questions have been completed, the user confirms the answers and proceeds to save. The user may return at any point and adjust the answers to better fit the current state, processes and measures applied by the utility. For the needs of this use case, we assumed that the semi-hypothetical utility selected implements cyber-security protocols and best practices at a moderate level. More specifically, the utility has a fully connected SCADA system that transmits signals mainly wirelessly through privately owned infrastructure. The access to critical systems is provided to authorised personnel, mainly through the internal company network (intranet), while the use of remote access and control software, e.g., Remote Desktop Connection, TeamViewer etc., is prohibited. The utility updates the system and carries out backups at a moderately regular basis, and applies encryption and anomaly detection techniques, but only to a portion of its systems. Lastly, the utility has recently begun to hold annual training for personnel on the topic of cyber-security, necessitated by rising trends in the sector's threat. Those practices are reflected through the questionnaire seen in Figure 8, and which shows that the practices applied correspond to the protection level scale 4 (medium level).

3.2 Risk assessment and treatment

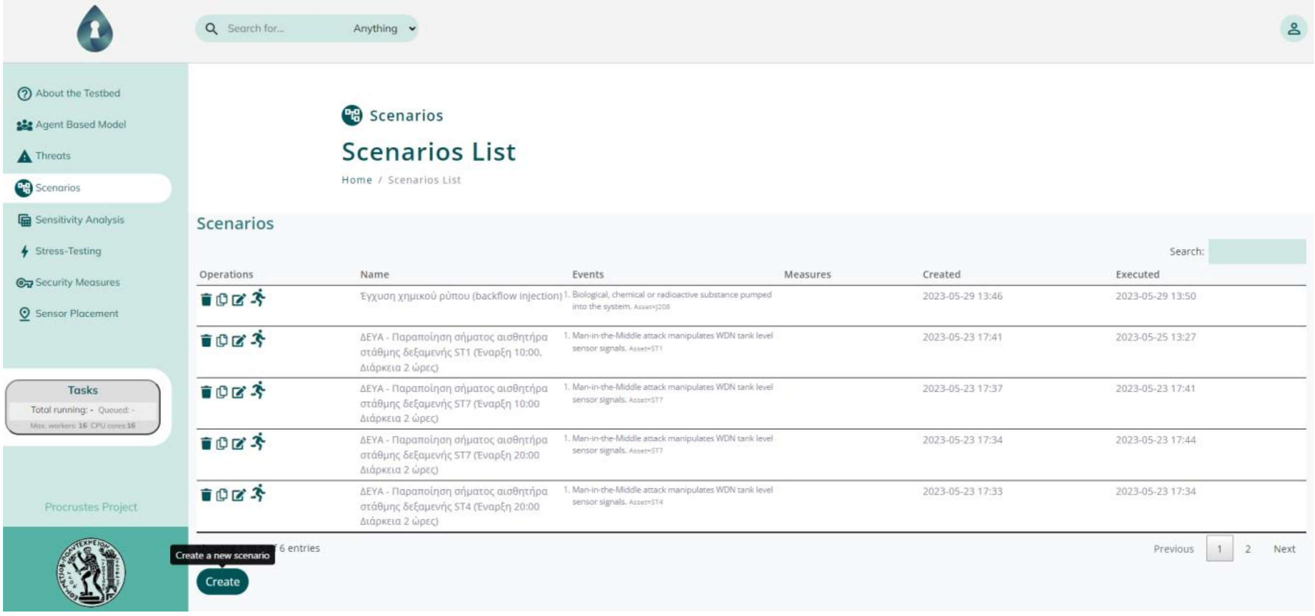
After setting all the necessary data input, the platform is ready to be utilised for all the steps of the risk assessment and treatment. Those processes are typically carried out by dedicated personnel (risk assessors), with the collaboration of modellers that assist in the proper formulation or re-design of the reference model and decision-makers that guide the objectives and desired risk information outcomes based on the regulatory/legal provisions and the strategic goals of the utility. The PROCRUSTES platform allows for a series of actions according to a particular "goal". The following sections display the set of possible sequences of interactions between the user and the system (each component) related to:

1. Single scenario analysis that allows the **exploration of event-specific consequences**, focused e.g., on the most probable type of asset from the previous step or based on an insight provided by the Cybersecurity Authority or other official government bodies.
2. Sensitivity analysis to explore variations of a risk and help **identify critical assets** of the system and/or time of attack.
3. ABM analysis to **assess the likelihood of attack**, at system level and per asset/attacker type.
4. Stress-testing analysis to **define the risk level of the utility**, and its exposure to the entire cyber-physical threat landscape as characterised by the CPRISK-ABM analysis, incl. assessment of risk level per asset type.
5. Selection and evaluation of potential treatment measures to assess their efficiency, to provide **evidence-based prioritisation of actions** and help guide the decision-making process.
6. Design of a new quality sensor layout or upgrade of a pre-existing with the goal of **maximizing the resilience** in terms of a reducing the expected impact of cyber-physical attacks.

3.2.1 EXPLORING AND ASSESSING A SINGLE THREAT SCENARIO

One of the fundamental risk analysis processes is the analysis and evaluation of single threat scenarios. In risk assessment, a single scenario analysis is a method used to evaluate the potential impact of a given risk event or a combination of events, under specific user-defined characteristics.

This process is available through the PROCRUSTES platform and can be accessed through the “Scenarios” button on the main screen (see Figure 5).



Scenarios

Scenarios List

Home / Scenarios List

Scenarios

Search:

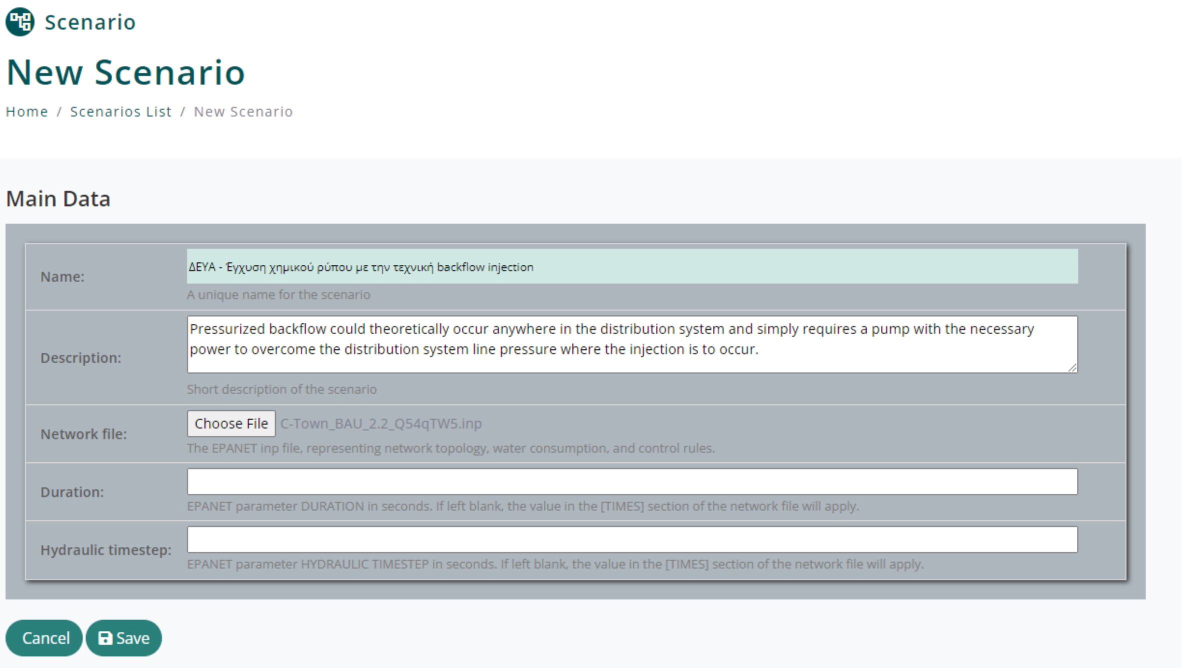
Operations	Name	Events	Measures	Created	Executed
🗑 ⧉ ✎ 🏃	Έγχυση χημικού ρύπου (backflow injection)	1. Biological, chemical or radioactive substance pumped into the system. Asset=J208		2023-05-29 13:46	2023-05-29 13:50
🗑 ⧉ ✎ 🏃	ΔΕΥΑ - Παραποίηση σήματος αισθητήρα στάθμης δεξαμενής ST1 (Έναρξη 10:00, Διάρκεια 2 ώρες)	1. Man-in-the-Middle attack manipulates WDN tank level sensor signals. Asset=ST1		2023-05-23 17:41	2023-05-25 13:27
🗑 ⧉ ✎ 🏃	ΔΕΥΑ - Παραποίηση σήματος αισθητήρα στάθμης δεξαμενής ST7 (Έναρξη 10:00 Διάρκεια 2 ώρες)	1. Man-in-the-Middle attack manipulates WDN tank level sensor signals. Asset=ST7		2023-05-23 17:37	2023-05-23 17:41
🗑 ⧉ ✎ 🏃	ΔΕΥΑ - Παραποίηση σήματος αισθητήρα στάθμης δεξαμενής ST7 (Έναρξη 20:00 Διάρκεια 2 ώρες)	1. Man-in-the-Middle attack manipulates WDN tank level sensor signals. Asset=ST7		2023-05-23 17:34	2023-05-23 17:44
🗑 ⧉ ✎ 🏃	ΔΕΥΑ - Παραποίηση σήματος αισθητήρα στάθμης δεξαμενής ST4 (Έναρξη 20:00 Διάρκεια 2 ώρες)	1. Man-in-the-Middle attack manipulates WDN tank level sensor signals. Asset=ST4		2023-05-23 17:33	2023-05-23 17:34

f 6 entries

Previous 1 2 Next

Figure 9 Scenario List page for the monitoring, management, and creation of single threat scenarios

In the landing screen, seen in Figure 9, the user can start the process of creating a new scenario by pressing the “Create” button on the bottom left side. The user is guided to the Scenario Generator interface for the creation of a new scenario, seen in Figure 10. In the New Scenario form, the user defines the name of the new scenario, and an optional description. Then, the user selects the network model to be used as reference and is given the right to modify the characteristics of the simulation if needed. In particular, the user can modify the duration of the simulation (e.g., 1 day, 1 week, etc.) as well as the step of the analysis (e.g., hourly) and save changes. Then, by selecting “add event”, the user can identify and select the cyber-physical threat for investigation from the drop-down list (see Figure 11) and specify the asset targeted. This is done by selecting the asset code that matched the ID of the asset in the reference model.



Name: ΔΕΥΑ - Έγχυση χημικού ρύπου με την τεχνική backflow injection
A unique name for the scenario

Description: Pressurized backflow could theoretically occur anywhere in the distribution system and simply requires a pump with the necessary power to overcome the distribution system line pressure where the injection is to occur.
Short description of the scenario

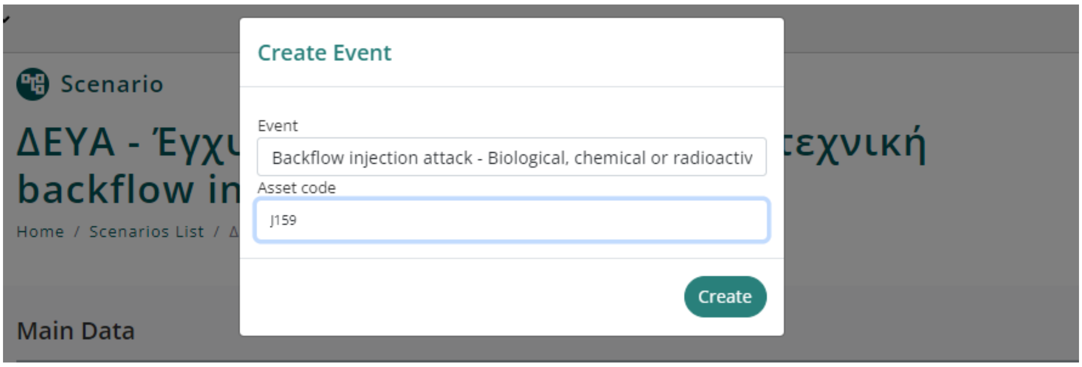
Network file: Choose File C-Town_BAU_2.2_Q54qTW5.inp
The EPANET inp file, representing network topology, water consumption, and control rules.

Duration:
EPANET parameter DURATION in seconds. If left blank, the value in the [TIMES] section of the network file will apply.

Hydraulic timestep:
EPANET parameter HYDRAULIC TIMESTEP in seconds. If left blank, the value in the [TIMES] section of the network file will apply.

Figure 10 Scenario Generator interface for the creation of single scenario

For the needs of this section's analysis, we use the network of the semi-hypothetical water company previously defined, with a duration of 24 hours (1 typical day of operation) and an hourly analysis step. As a reference threat, we identify a contamination attack against the system. More specifically we will explore a backflow injection attack, i.e., inserting a contaminant by overcoming the system's pressure, occurring at node "J159". This is a node located in the main distribution line of the system, near the only water source.

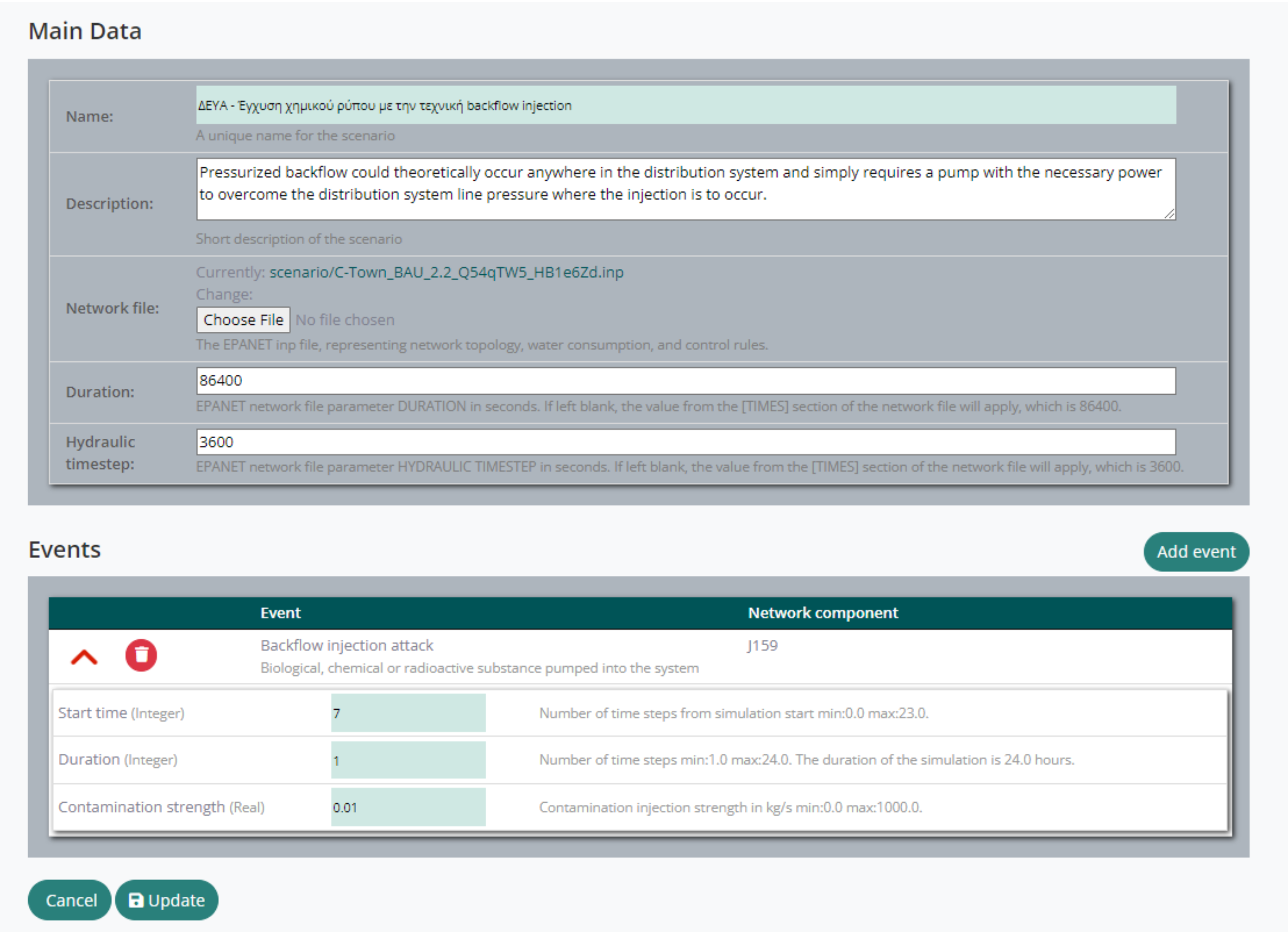


Event: Backflow injection attack - Biological, chemical or radioactiv

Asset code: J159

Figure 11 Scenario Generator interface for the selection of identified threats (drop-down menu) and asset targeted for a single scenario

After selecting the identified threat for analysis, the user needs to further define the event-like characteristics, including the start time and the duration. This is done through the event parameterisation interface seen in Figure 12, that adjusts its content according to the threat in hand. For this analysis, we define the backflow injection threat as an event that starts at 7:00 am and has an injection rate of 0.01 kg/s that lasts for 1 hour.



Main Data

Name:	ΔΕΥΑ - Έγχυση χημικού ρύπου με την τεχνική backflow injection A unique name for the scenario
Description:	Pressurized backflow could theoretically occur anywhere in the distribution system and simply requires a pump with the necessary power to overcome the distribution system line pressure where the injection is to occur. Short description of the scenario
Network file:	Currently: scenario/C-Town_BAU_2.2_Q54qTW5_HB1e6Zd.inp Change: Choose File No file chosen The EPANET inp file, representing network topology, water consumption, and control rules.
Duration:	86400 EPANET network file parameter DURATION in seconds. If left blank, the value from the [TIMES] section of the network file will apply, which is 86400.
Hydraulic timestep:	3600 EPANET network file parameter HYDRAULIC TIMESTEP in seconds. If left blank, the value from the [TIMES] section of the network file will apply, which is 3600.

Events

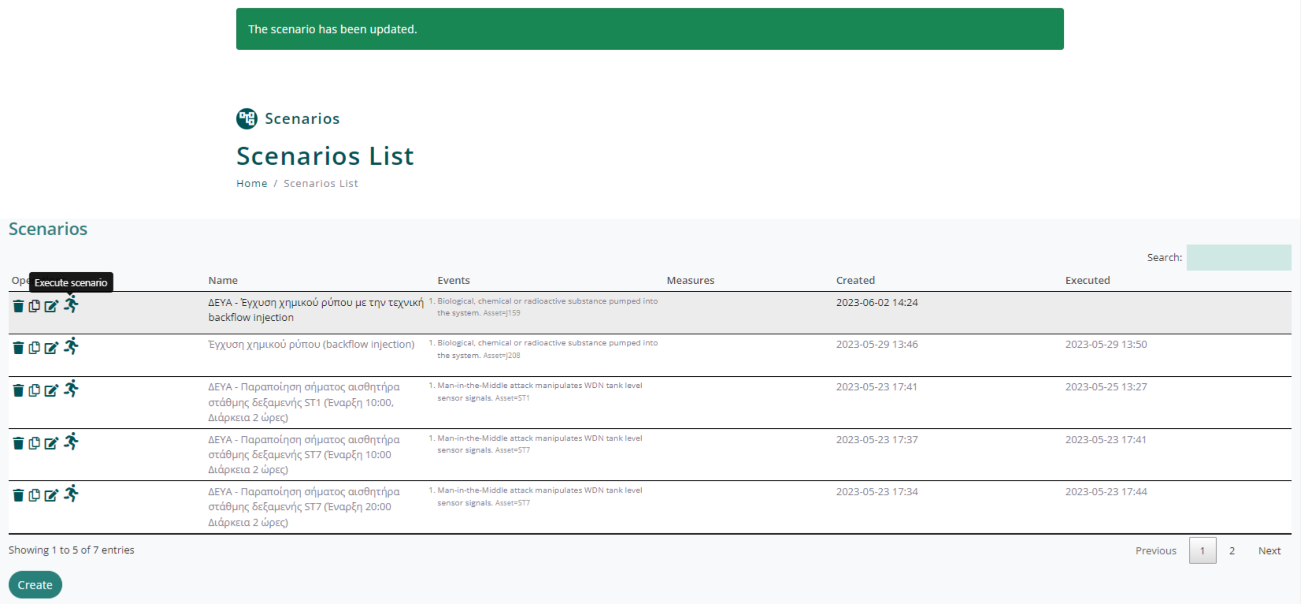
	Event	Network component
	Backflow injection attack Biological, chemical or radioactive substance pumped into the system	J159

Start time (Integer)	7	Number of time steps from simulation start min:0.0 max:23.0.
Duration (Integer)	1	Number of time steps min:1.0 max:24.0. The duration of the simulation is 24.0 hours.
Contamination strength (Real)	0.01	Contamination injection strength in kg/s min:0.0 max:1000.0.

Figure 12 Scenario Generator interface for the parameterisation of the identified quality related threat

If the user wishes to investigate the performance of the system under multiple threats, the system allows additional events to be added, following the same steps as before, i.e., starting with the “add event” button. Upon completion of the configuration, the user selects to save the new scenario and the system automatically transfers users to the Scenarios List page[2] and displays a message for the successful creation/update of the scenario. From there, the user can choose to simulate the newly created scenario by clicking on the "execute scenario" button located to the left of the scenario (see Figure 13) and view the results of the individual simulation via the relevant KPIs (see Figure 14).

[2] It is possible to modify/correct the parameters of the scenario by selecting "edit" from the action list to the left of the scenario. The user goes back to the scenario template, and after making the desired changes, re-saves the scenario.



The scenario has been updated.

Scenarios

Scenarios List

Home / Scenarios List

Scenarios

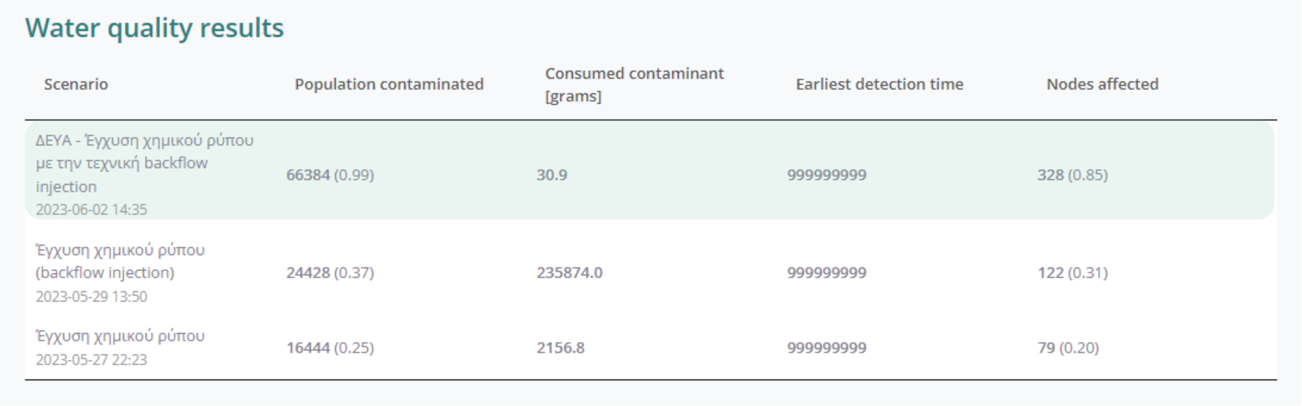
Search:

Ope	Name	Events	Measures	Created	Executed
Execute scenario	ΔΕΥΑ - Έγχυση χημικού ρύπου με την τεχνική backflow injection	1. Biological, chemical or radioactive substance pumped into the system. Asset=J159		2023-06-02 14:24	
	Έγχυση χημικού ρύπου (backflow injection)	1. Biological, chemical or radioactive substance pumped into the system. Asset=J208		2023-05-29 13:46	2023-05-29 13:50
	ΔΕΥΑ - Παραποίηση σήματος αισθητήρα στάθμης δεξαμενής ST1 (Έναρξη 10:00, Διάρκεια 2 ώρες)	1. Man-in-the-Middle attack manipulates WDN tank level sensor signals. Asset=ST1		2023-05-23 17:41	2023-05-25 13:27
	ΔΕΥΑ - Παραποίηση σήματος αισθητήρα στάθμης δεξαμενής ST7 (Έναρξη 10:00 Διάρκεια 2 ώρες)	1. Man-in-the-Middle attack manipulates WDN tank level sensor signals. Asset=ST7		2023-05-23 17:37	2023-05-23 17:41
	ΔΕΥΑ - Παραποίηση σήματος αισθητήρα στάθμης δεξαμενής ST7 (Έναρξη 20:00 Διάρκεια 2 ώρες)	1. Man-in-the-Middle attack manipulates WDN tank level sensor signals. Asset=ST7		2023-05-23 17:34	2023-05-23 17:44

Showing 1 to 5 of 7 entries

Figure 13 Scenario List page with highlighted "run" button for the single scenario created

The platform maps the performance of the system with relevant key performance indicators (KPIs), such as (a) the volume and percentage of unmet demand, (b) the number and percentage of consumers potentially affected, and (c) the number of nodes experiencing a problem, to aggregate the magnitude and expand of the threat's impact, in terms of water supply quantity. For threats that affect the quality of the distributed water, the assessment is made using quality-relevant indicators such as (a) population contaminated, (b) mass of consumed contaminant [grams], (c) earliest detection time, (d) nodes affected, as seen in Figure 14. In addition, the summary presentation of the results for the individual scenarios investigated allows for the comparative assessment between individual scenarios.



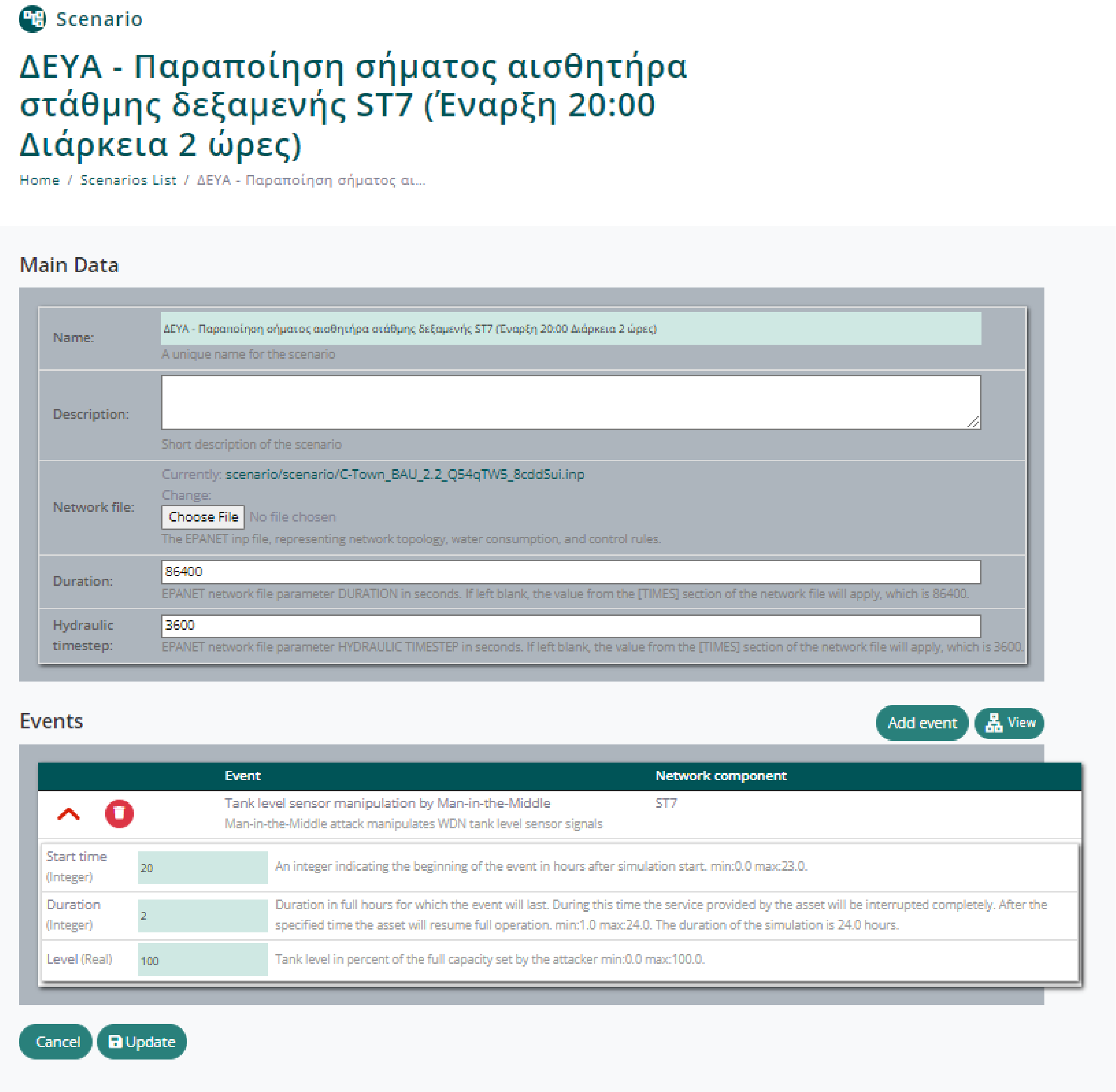
Water quality results

Scenario	Population contaminated	Consumed contaminant [grams]	Earliest detection time	Nodes affected
ΔΕΥΑ - Έγχυση χημικού ρύπου με την τεχνική backflow injection 2023-06-02 14:35	66384 (0.99)	30.9	999999999	328 (0.85)
Έγχυση χημικού ρύπου (backflow injection) 2023-05-29 13:50	24428 (0.37)	235874.0	999999999	122 (0.31)
Έγχυση χημικού ρύπου 2023-05-27 22:23	16444 (0.25)	2156.8	999999999	79 (0.20)

Figure 14 Portion of the Scenario List page with the results table for the simulated quality-related single scenarios (use case scenario highlighted)

Following the same steps as before, the user may also choose to investigate the effects of a cyber-attack against the sensing and monitoring system, such as a Man-in-the-Middle attack against a tank level sensor. This event would falsify the signal received by the tank level sensor and mislead the monitoring and control devices to believe that the tank is full, or above refill level.

As seen in Figure 15 below, the event parameterisation wizard of the Scenario Generator automatically adjusts its contents to the specific threat, and in addition to the start-time and duration of the event, requests as input the “falsified” signal received by PLCs and the SCADA as a result of the attack. In this example, we explore the effects of a Man-in-the-Middle attack against the level sensor of tank “ST7” that starts at 20:00, lasts 2 hours and leads the system to believe that the tank is full (100%).



ΔΕΥΑ - Παραποίηση σήματος αισθητήρα στάθμης δεξαμενής ST7 (Έναρξη 20:00 Διάρκεια 2 ώρες)

Main Data

Name:	ΔΕΥΑ - Παραποίηση σήματος αισθητήρα στάθμης δεξαμενής ST7 (Έναρξη 20:00 Διάρκεια 2 ώρες) A unique name for the scenario
Description:	Short description of the scenario
Network file:	Currently: scenario/scenario/C-Town_BAU_2.2_Q54qTW5_8cdd5ui.inp Change: Choose File No file chosen The EPANET inp file, representing network topology, water consumption, and control rules.
Duration:	86400 EPANET network file parameter DURATION in seconds. If left blank, the value from the [TIMES] section of the network file will apply, which is 86400.
Hydraulic timestep:	3600 EPANET network file parameter HYDRAULIC TIMESTEP in seconds. If left blank, the value from the [TIMES] section of the network file will apply, which is 3600.

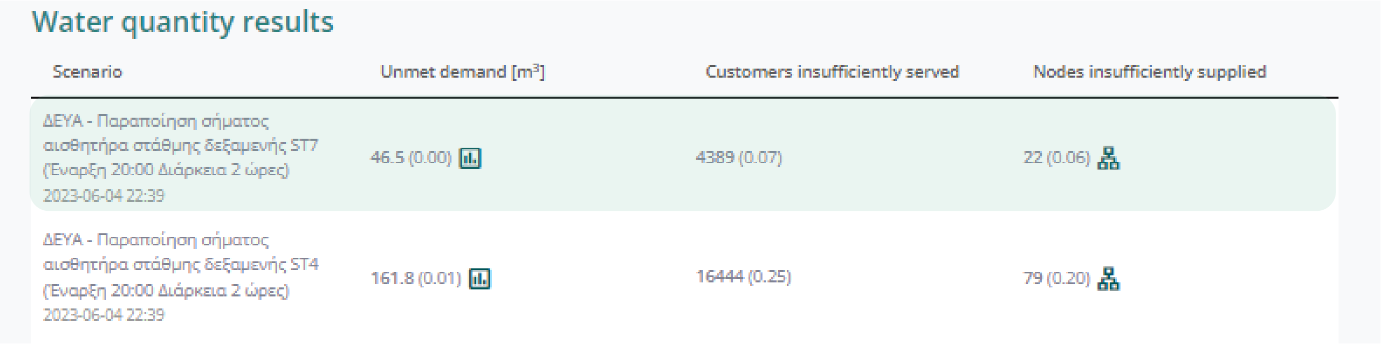
Events

Event	Network component
Tank level sensor manipulation by Man-in-the-Middle Man-in-the-Middle attack manipulates WDN tank level sensor signals	ST7

Start time (Integer)	20	An integer indicating the beginning of the event in hours after simulation start. min:0.0 max:23.0.
Duration (Integer)	2	Duration in full hours for which the event will last. During this time the service provided by the asset will be interrupted completely. After the specified time the asset will resume full operation. min:1.0 max:24.0. The duration of the simulation is 24.0 hours.
Level (Real)	100	Tank level in percent of the full capacity set by the attacker min:0.0 max:100.0.

Figure 15 Scenario Generator interface for the parameterisation of the identified quantity related threat

After simulating the scenario, the results are added to the relevant table, along with other similar scenarios (see Figure 16).



Water quantity results

Scenario	Unmet demand [m³]	Customers insufficiently served	Nodes insufficiently supplied
ΔΕΥΑ - Παραποίηση σήματος αισθητήρα στάθμης δεξαμενής ST7 (Έναρξη 20:00 Διάρκεια 2 ώρες) 2023-06-04 22:39	46.5 (0.00)	4389 (0.07)	22 (0.06)
ΔΕΥΑ - Παραποίηση σήματος αισθητήρα στάθμης δεξαμενής ST4 (Έναρξη 20:00 Διάρκεια 2 ώρες) 2023-06-04 22:39	161.8 (0.01)	16444 (0.25)	79 (0.20)

Figure 16 Portion of the Scenario List page with the results table for the simulated quantity-related single scenarios (use case scenario highlighted)

Besides the aggregated KPI results of the scenario, the platform also allows users to visually interpret the single scenario results. By selecting the “chart” button under the “unmet demand” metric, the system displays the timeseries chart of the system demand and supply, allowing the user to identify the magnitude, duration and start time of the impacts in the supply (see Figure 17).

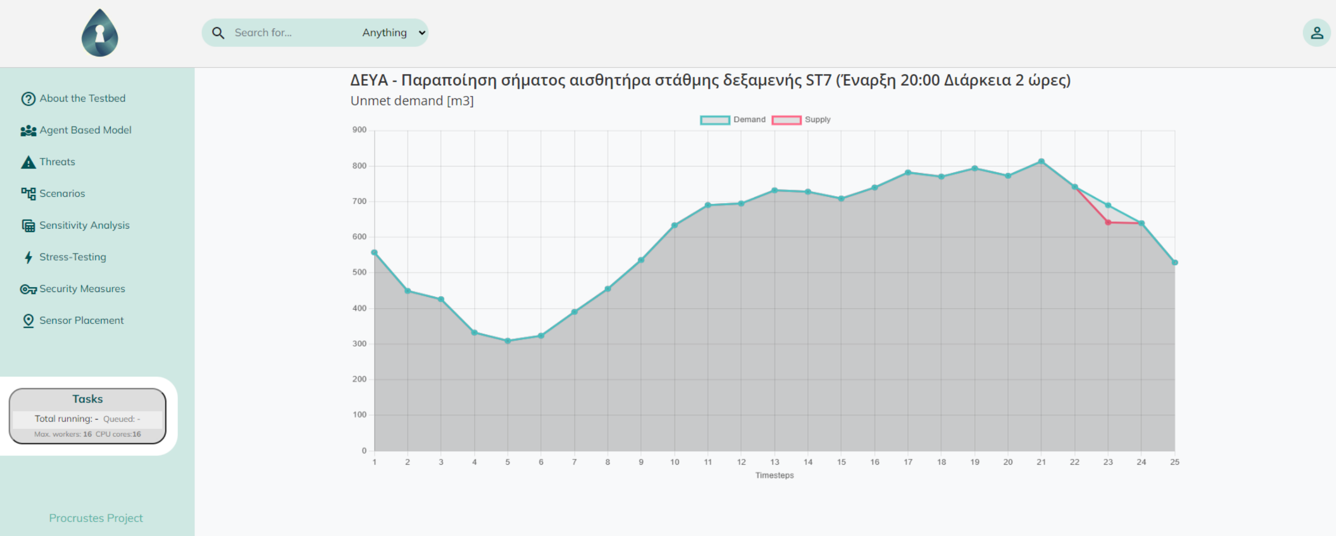
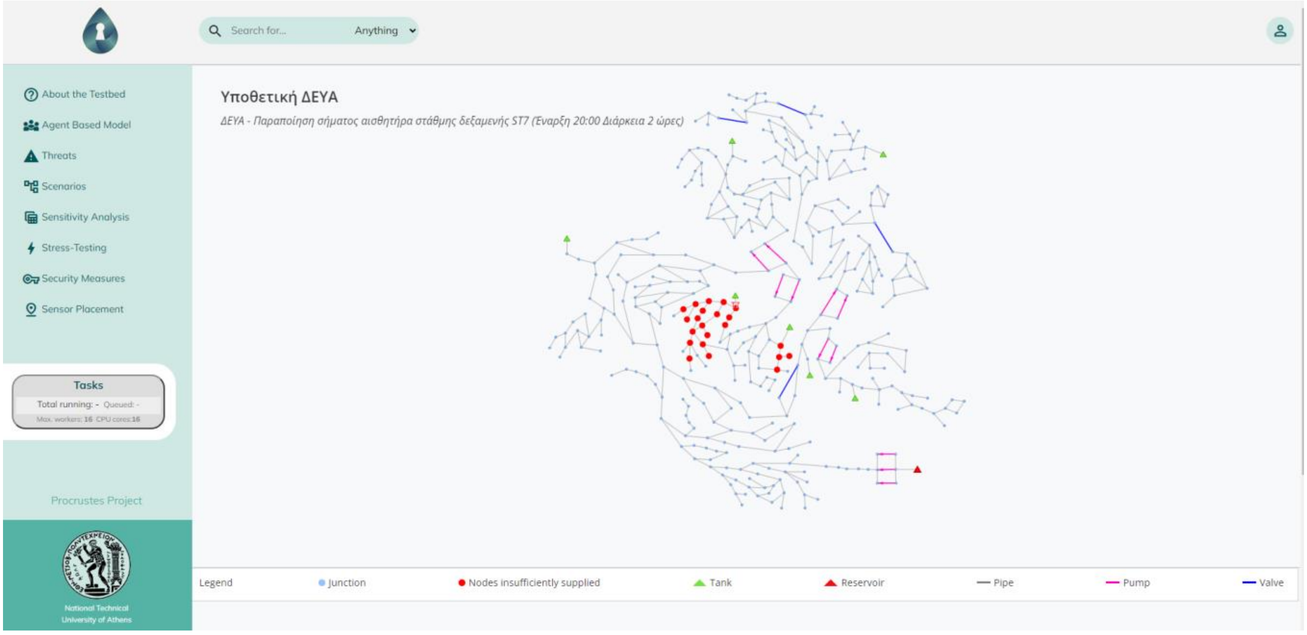


Figure 17 Timeseries chart demonstrating the expected demand and the actual supply of the system under attack

In addition to that, the platform may also display the spatial distribution of the impacts, by pressing the “network” button, under the “nodes insufficiently supplied” metric. The platform visually interprets the consequences in the services and its spatial extent in the network, highlighting the affected nodes of the network, as seen in Figure 18. This feature allows for the evaluation of the impacts in terms of the area affected, and thus, the examination of potential effects against critical nodes of the system such as hospitals, schools, government, or military buildings etc. Such information can be extracted and inserted to relevant reports or risk assessment documentations.


Υποθετική ΔΕΥΑ

ΔΕΥΑ - Παραποίηση σήματος αισθητήρα στάθμης δεξαμενής ST7 (Έναρξη 20:00 Διάρκεια 2 ώρες)

Tasks

Total running: - Queued: -

Max. workers: 16 CPU cores:16

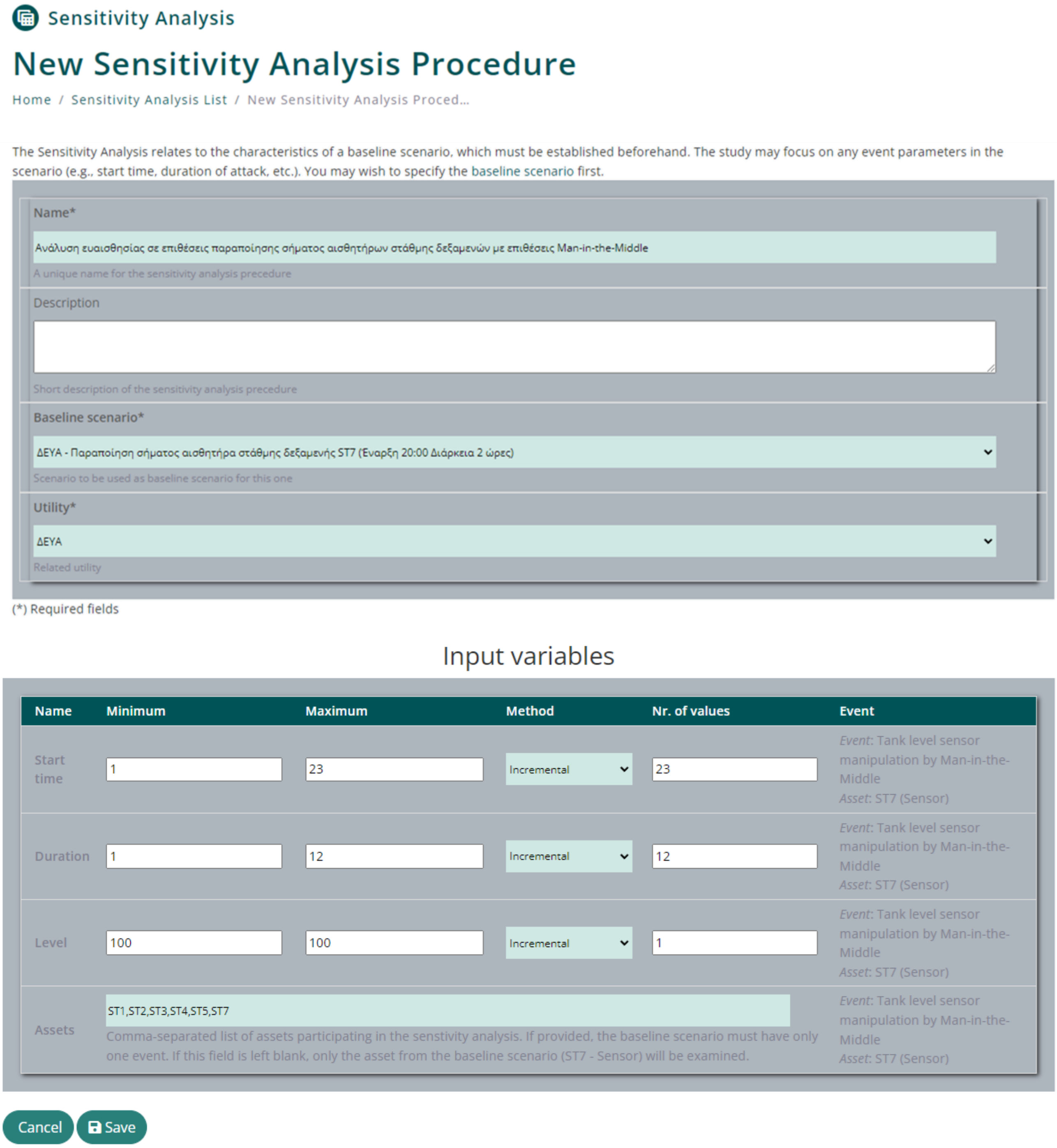
Figure 18 Spatial interpretation of the impacts of the investigated scenario, with nodes being affected highlighted with red

Individual scenarios, however, cannot provide sufficient information to identify and evaluate the critical nodes of a system against a cyber-physical threat. The platform enables the investigation of the importance/criticality of both individual system components and the characteristics of a threat through sensitivity analysis.

3.2.2 PERFORM SENSITIVITY ANALYSIS AND IDENTIFY CRITICAL ASSETS

In this section, we present the steps for the sensitivity analysis of cyber-physical threats that helps utilities identify critical nodes in the network as well as critical characteristics of a cyber-physical attack. For the sensitivity analysis, the user should first have created a single scenario to be investigated. If one does not already exist, they can choose from the main menu to go to the Scenarios list, where they are given the option to create a new scenario as described in the previous section. Once the scenario that will be used as a reference has been created, the user chooses to go to the Sensitivity Analysis function, either from the main page of the platform or from the list of functions located on the left side of the screen, where it is then possible to create a new process.

The user is then guided to the Sensitivity Analysis form (see Figure 19), where a name and an appropriate description of the process should be provided. Then, the user selects the scenario that will act as a reference scenario. The platform automatically receives the information about the embedded threats in the reference scenario and displays the "input variables" form, with the relevant parameters. The form includes all threats (single or multiple) embedded in the reference scenario. From there, the user can select (a) the range of values of each parameter, setting the maximum and minimum, (b) the sample size, and (c) how to sample within the given range, for each parameter (see Figure 19). Sampling can be done either in a random manner (selecting "Random selection" from the list of options) or incrementally with a fixed step (selecting "Incremental" from the list of options). Finally, it is also possible to generate a list of alternative possible targets where the threat may manifest itself.



Sensitivity Analysis

New Sensitivity Analysis Procedure

Home / Sensitivity Analysis List / New Sensitivity Analysis Proced...

The Sensitivity Analysis relates to the characteristics of a baseline scenario, which must be established beforehand. The study may focus on any event parameters in the scenario (e.g., start time, duration of attack, etc.). You may wish to specify the baseline scenario first.

Name*

Ανάλυση ευαισθησίας σε επιθέσεις παραποίησης σήματος αισθητήρων στάθμης δεξαμενών με επιθέσεις Man-in-the-Middle

A unique name for the sensitivity analysis precedure

Description

Short description of the sensitivity analysis precedure

Baseline scenario*

ΔΕΥΑ - Παραποίηση σήματος αισθητήρα στάθμης δεξαμενής ST7 (Εναρξη 20:00 Διάρκεια 2 ώρες)

Scenario to be used as baseline scenario for this one

Utility*

ΔΕΥΑ

Related utility

(*) Required fields

Input variables

Name	Minimum	Maximum	Method	Nr. of values	Event
Start time	1	23	Incremental	23	*Event*: Tank level sensor manipulation by Man-in-the-Middle *Asset*: ST7 (Sensor)
Duration	1	12	Incremental	12	*Event*: Tank level sensor manipulation by Man-in-the-Middle *Asset*: ST7 (Sensor)
Level	100	100	Incremental	1	*Event*: Tank level sensor manipulation by Man-in-the-Middle *Asset*: ST7 (Sensor)
Assets	ST1,ST2,ST3,ST4,ST5,ST7 Comma-separated list of assets participating in the senstivity analysis. If provided, the baseline scenario must have only one event. If this field is left blank, only the asset from the baseline scenario (ST7 - Sensor) will be examined.				*Event*: Tank level sensor manipulation by Man-in-the-Middle *Asset*: ST7 (Sensor)

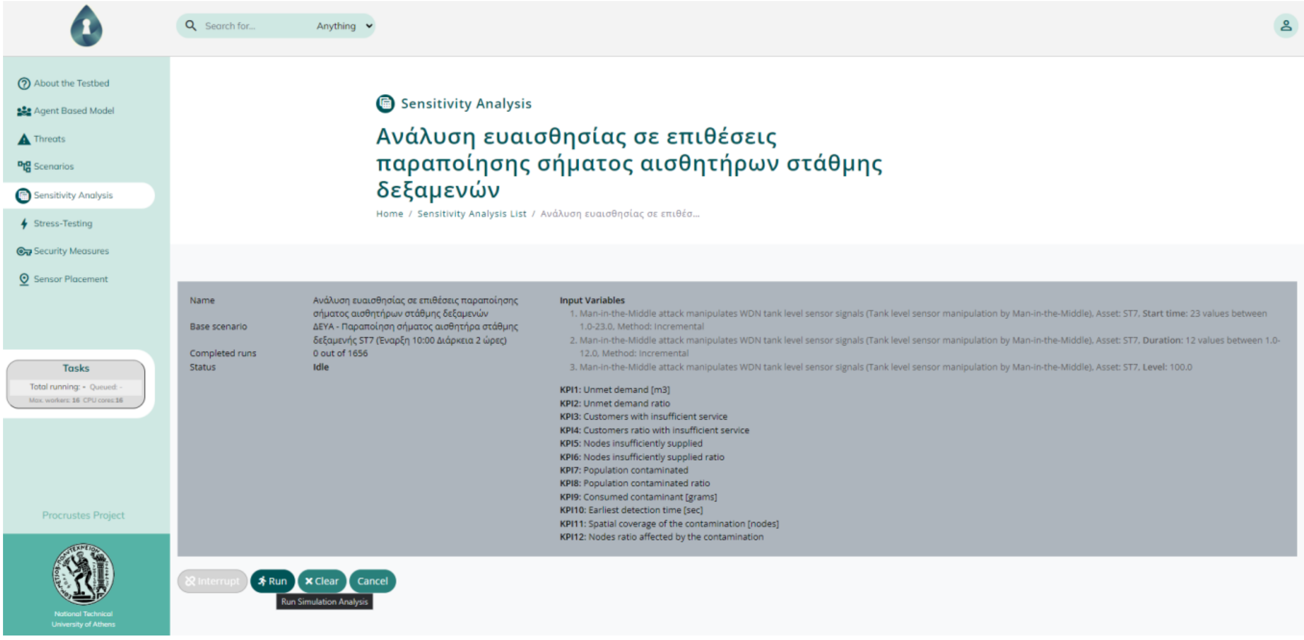
Figure 19 Sensitivity Analysis form to create and parameterise the process based on a reference scenario

For the use case of this section, we choose to investigate the tank level sensor signal tampering scenario created in the previous section. To generate the sensitivity analysis of attacks against tank level sensors of the semi-hypothetical system, we selected:

- Investigation of every hour of the day as a possible attack start-time
  (23 serial parameter values in the range 1:00-23:00)
- Investigation of attacks with a duration of 1 up to 12 hours, with a fixed step of 1 hour
  (12 serial parameter values in the range 1-12)
- As the value of the spoofed/falsified signal the indication 100% (tank full)
  (1 constant parameter value)
- Investigation of the attack event in each of the 6 water tanks equipped with a level sensor and connected to PLC and SCADA.
  (7 asset IDs as parameter values)

The above configuration generates 1656 combinations, each of which is a scenario to be investigated in the process.

After finalising the configuration of the sensitivity analysis, and selecting save, the system automatically generates the scenarios corresponding to the selected parameter combinations. Then, by selecting the sensitivity analysis folder, the user chooses to start the simulation of the scenarios by pressing the "run" button (see Figure 20).



Sensitivity Analysis

Ανάλυση ευαισθησίας σε επιθέσεις παραποίησης σήματος αισθητήρων στάθμης δεξαμενών

Home / Sensitivity Analysis List / Ανάλυση ευαισθησίας σε επιθέσ...

Name: Ανάλυση ευαισθησίας σε επιθέσεις παραποίησης σήματος αισθητήρων στάθμης δεξαμενών
Base scenario: ΔΕΥΑ - Παραποίηση σήματος αισθητήρα στάθμης δεξαμενής ST7 (Έναρξη 10:00 Διάρκεια 2 ώρες)
Completed runs: 0 out of 1656
Status: **Idle**

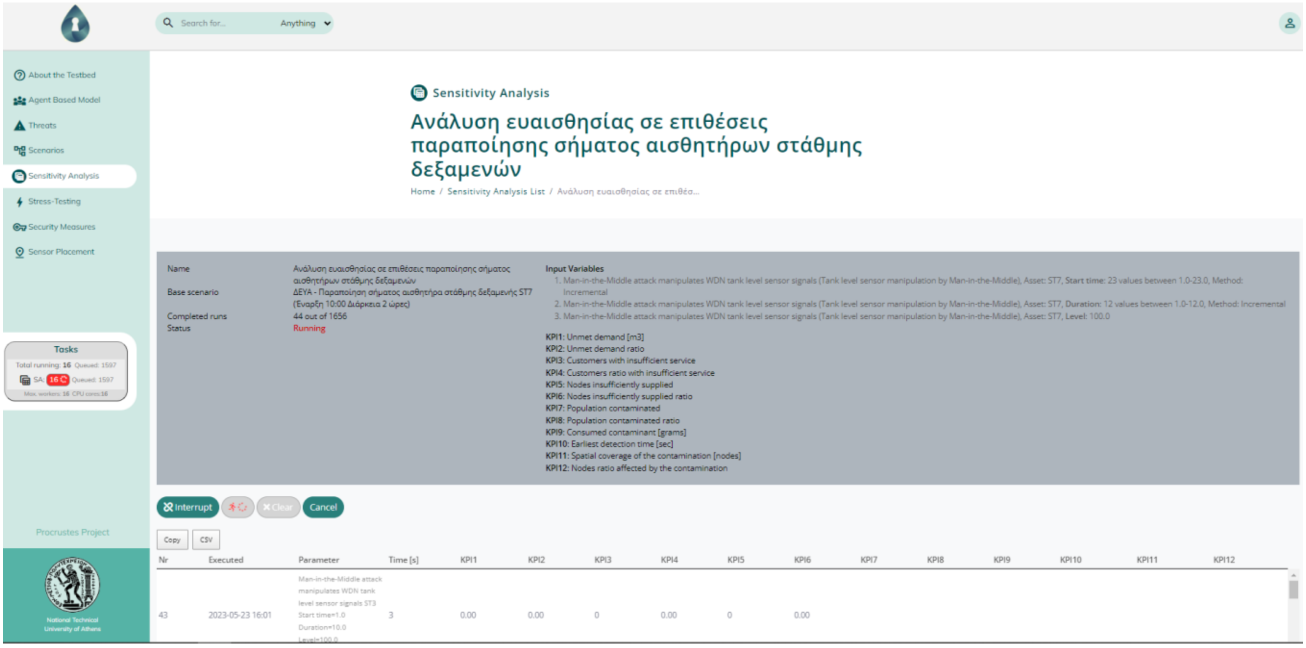
Input Variables

1. Man-in-the-Middle attack manipulates WDN tank level sensor signals (Tank level sensor manipulation by Man-in-the-Middle), Asset: ST7, **Start time**: 23 values between 1.0-23.0, Method: Incremental
2. Man-in-the-Middle attack manipulates WDN tank level sensor signals (Tank level sensor manipulation by Man-in-the-Middle), Asset: ST7, **Duration**: 12 values between 1.0-12.0, Method: Incremental
3. Man-in-the-Middle attack manipulates WDN tank level sensor signals (Tank level sensor manipulation by Man-in-the-Middle), Asset: ST7, **Level**: 100.0

KPI1: Unmet demand [m3]
KPI2: Unmet demand ratio
KPI3: Customers with insufficient service
KPI4: Customers ratio with insufficient service
KPI5: Nodes insufficiently supplied
KPI6: Nodes insufficiently supplied ratio
KPI7: Population contaminated
KPI8: Population contaminated ratio
KPI9: Consumed contaminant [grams]
KPI10: Earliest detection time [sec]
KPI11: Spatial coverage of the contamination [nodes]
KPI12: Nodes ratio affected by the contamination

Figure 20 Start simulation of sensitivity analysis scenarios

The platform provides continuous updates on the progress of the analysis, the number of simulations running in parallel, and the number and results of completed simulations (see Figure 21). Upon completion of the simulation cycle, the system changes the status from "running" to "completed", indicating to the user that the sensitivity analysis has been completed.



Sensitivity Analysis

Ανάλυση ευαισθησίας σε επιθέσεις παραποίησης σήματος αισθητήρων στάθμης δεξαμενών

Home / Sensitivity Analysis List / Ανάλυση ευαισθησίας σε επιθέσ...

Name	Ανάλυση ευαισθησίας σε επιθέσεις παραποίησης σήματος αισθητήρων στάθμης δεξαμενών
Base scenario	ΔΕΥΑ - Παραποίηση σήματος αισθητήρα στάθμης δεξαμενής ST7 (Εναρξη 10:00 Διάρκεια 2 ώρες)
Completed runs	44 out of 1656
Status	Running

Input Variables

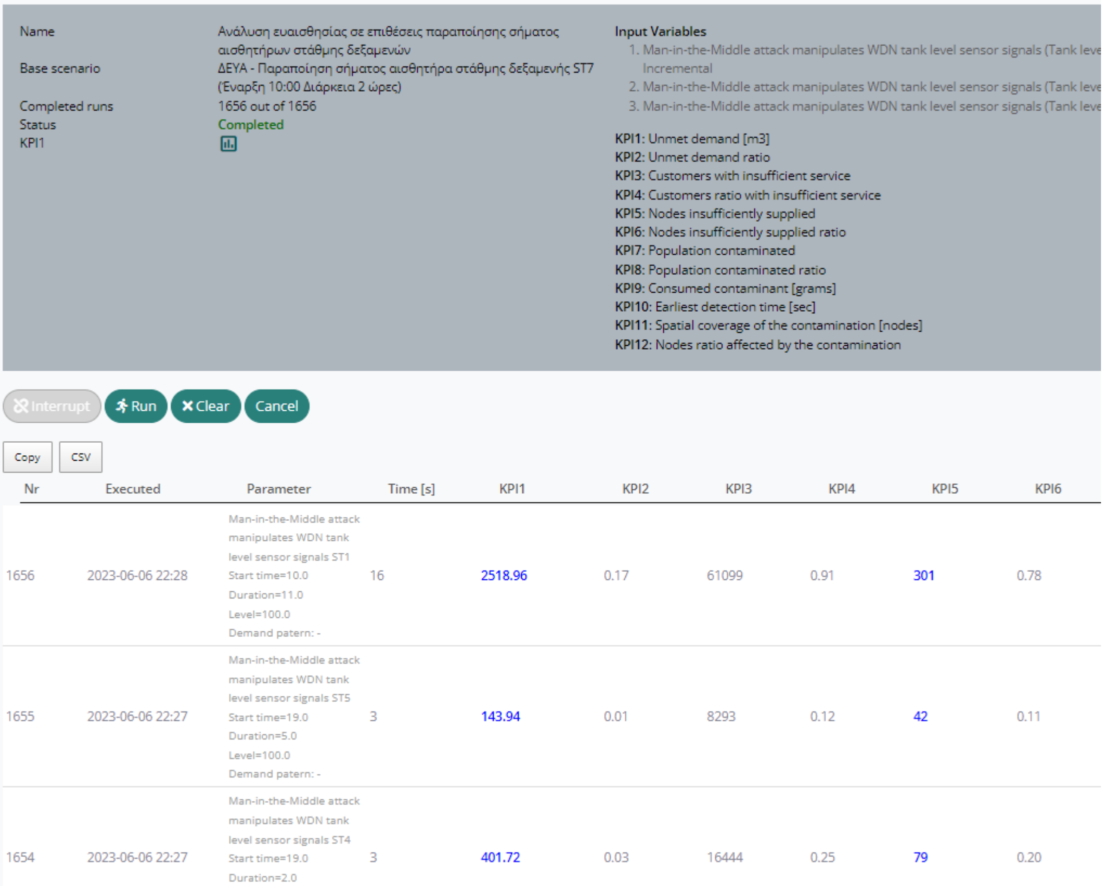
1. Man-in-the-Middle attack manipulates WDN tank level sensor signals (Tank level sensor manipulation by Man-in-the-Middle), Asset: ST7, **Start time:** 23 values between 1.0-23.0, Method: Incremental
2. Man-in-the-Middle attack manipulates WDN tank level sensor signals (Tank level sensor manipulation by Man-in-the-Middle), Asset: ST7, **Duration:** 12 values between 1.0-12.0, Method: Incremental
3. Man-in-the-Middle attack manipulates WDN tank level sensor signals (Tank level sensor manipulation by Man-in-the-Middle), Asset: ST7, **Level:** 100.0

KPI1: Unmet demand [m3]
KPI2: Unmet demand ratio
KPI3: Customers with insufficient service
KPI4: Customers ratio with insufficient service
KPI5: Nodes insufficiently supplied
KPI6: Nodes insufficiently supplied ratio
KPI7: Population contaminated
KPI8: Population contaminated ratio
KPI9: Consumed contaminant [grams]
KPI10: Earliest detection time [sec]
KPI11: Spatial coverage of the contamination [nodes]
KPI12: Nodes ratio affected by the contamination

Nr	Executed	Parameter	Time [s]	KPI1	KPI2	KPI3	KPI4	KPI5	KPI6	KPI7	KPI8	KPI9	KPI10	KPI11	KPI12
43	2023-05-23 16:01	Man-in-the-Middle attack manipulates WDN tank level sensor signals ST3 Start time=1.0 Duration=10.0 Level=100.0	3	0.00	0.00	0	0.00	0	0.00						

Figure 21 Progress of parallel sensitivity analysis simulations

The Sensitivity Analysis interface provides an overview of each scenario's results using the key performance measures mentioned in the analysis of the single scenario. From there, the user can sort the scenarios based on a specific indicator or export the table for further analysis.



Name	Ανάλυση ευαισθησίας σε επιθέσεις παραποίησης σήματος αισθητήρων στάθμης δεξαμενών
Base scenario	ΔΕΥΑ - Παραποίηση σήματος αισθητήρα στάθμης δεξαμενής ST7 (Εναρξη 10:00 Διάρκεια 2 ώρες)
Completed runs	1656 out of 1656
Status	Completed
KPI1	

Input Variables

1. Man-in-the-Middle attack manipulates WDN tank level sensor signals (Tank leve Incremental
2. Man-in-the-Middle attack manipulates WDN tank level sensor signals (Tank leve
3. Man-in-the-Middle attack manipulates WDN tank level sensor signals (Tank leve

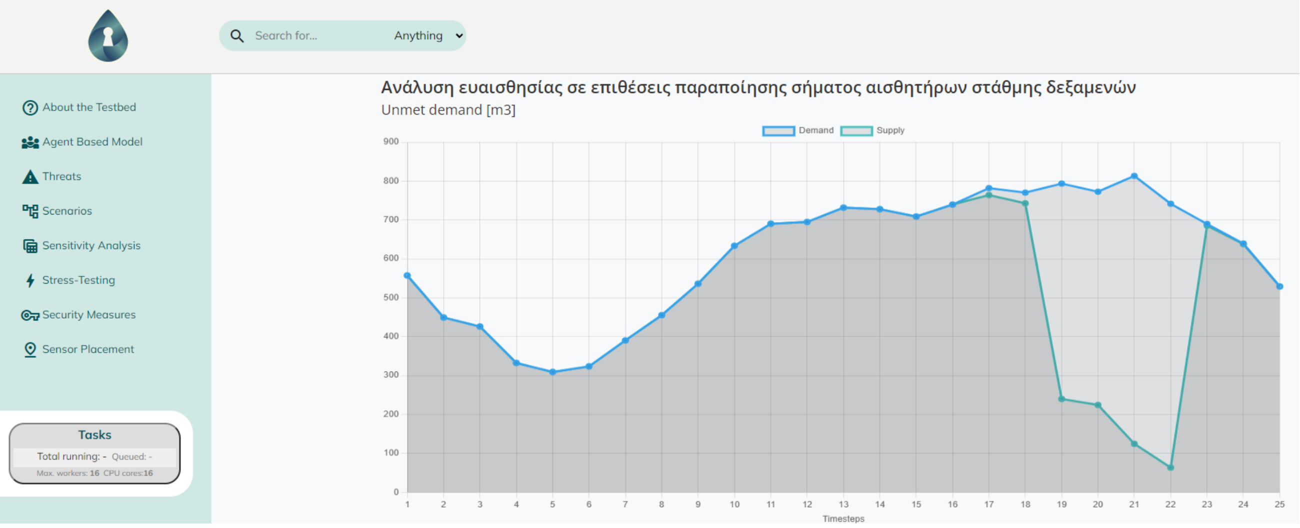
KPI1: Unmet demand [m3]
KPI2: Unmet demand ratio
KPI3: Customers with insufficient service
KPI4: Customers ratio with insufficient service
KPI5: Nodes insufficiently supplied
KPI6: Nodes insufficiently supplied ratio
KPI7: Population contaminated
KPI8: Population contaminated ratio
KPI9: Consumed contaminant [grams]
KPI10: Earliest detection time [sec]
KPI11: Spatial coverage of the contamination [nodes]
KPI12: Nodes ratio affected by the contamination

Nr	Executed	Parameter	Time [s]	KPI1	KPI2	KPI3	KPI4	KPI5	KPI6
1656	2023-06-06 22:28	Man-in-the-Middle attack manipulates WDN tank level sensor signals ST1 Start time=10.0 Duration=11.0 Level=100.0 Demand patern: -	16	2518.96	0.17	61099	0.91	301	0.78
1655	2023-06-06 22:27	Man-in-the-Middle attack manipulates WDN tank level sensor signals ST5 Start time=19.0 Duration=5.0 Level=100.0 Demand patern: -	3	143.94	0.01	8293	0.12	42	0.11
1654	2023-06-06 22:27	Man-in-the-Middle attack manipulates WDN tank level sensor signals ST4 Start time=19.0 Duration=2.0	3	401.72	0.03	16444	0.25	79	0.20

Figure 22 Sensitivity analysis results and visualisation options highlighted

In the example of this use case and by sorting the scenarios based on the unmet demand indicator (KPI1), we identify that the 25 most critical tank level signal manipulation scenarios are for tank ST1, with values ranging from 3262.53 m^3 (21% of daily demand) to 2305.56 m^3 (15% of daily demand).

In addition to ranking the scenarios, the user can visually explore the impacts of each individual scenario, by selecting the relevant KPI in the Sensitivity Analysis page, as seen in Figure 22. For example, by ranking the scenarios according to the total unmet demand metric and selecting the scenario with the highest impact, the platform will display a timeseries chart of the performance of the system, indicated by the expected demand and the actual supply at system level, as in Figure 23.



Ανάλυση ευαισθησίας σε επιθέσεις παραποίησης σήματος αισθητήρων στάθμης δεξαμενών

Unmet demand [m3]

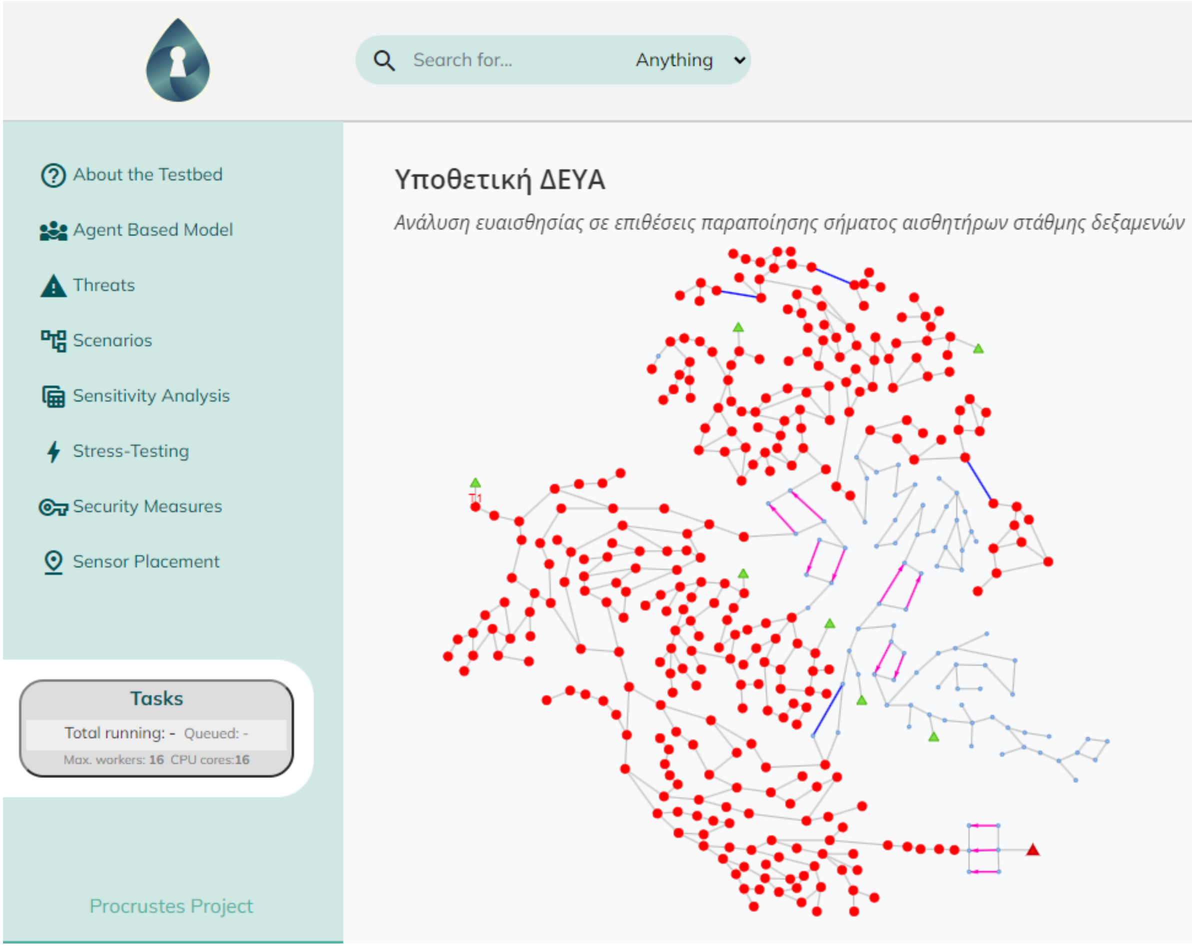
Tasks

Total running: - Queued: -

Max. workers: 16 CPU cores:16

Figure 23 Timeseries chart demonstrating the expected demand and the actual supply of the system under the most critical tank manipulation attack identified from the sensitivity analysis

This allows the quick inspection of the magnitude, the time of occurrence and the duration of the impacts under the given scenario, at system level. The user may also wish to view the spatial extent of the most critical scenario impacts, in terms of the nodes affected in the system. By selecting the relevant KPI (KPI5), the platform will display the network and highlight the affected nodes under the selected scenario, as in Figure 24. This allows for the evaluation of the impacts of the selected scenario in terms of the area affected, and thus, the examination of potential impacts against critical nodes of the system such as hospitals, schools, government, or military buildings etc.



Υποθετική ΔΕΥΑ

Ανάλυση ευαισθησίας σε επιθέσεις παραποίησης σήματος αισθητήρων στάθμης δεξαμενών

Total running: - Queued: -

Max. workers: 16 CPU cores:16

Figure 24 Visualisation of the spatial extent of impacts in the provided services under the most critical tank manipulation attack identified from the sensitivity analysis (affected nodes highlighted with red)

To provide a better understanding of the overall performance of the system under the given type of threat or threats examined in the sensitivity analysis, the user may also select to see the spectrum of the system's performance under the entire set of sensitivity analysis scenarios. This can be done by selecting the "chart" button, located below the status of the sensitivity analysis process, at the top banner (grey) of the screen (see Figure 22). The system will post-process the results of the entire scenario set for the given metric, export the statistical characteristics, and display the "aggregated" results in a single chart, as in Figure 25.

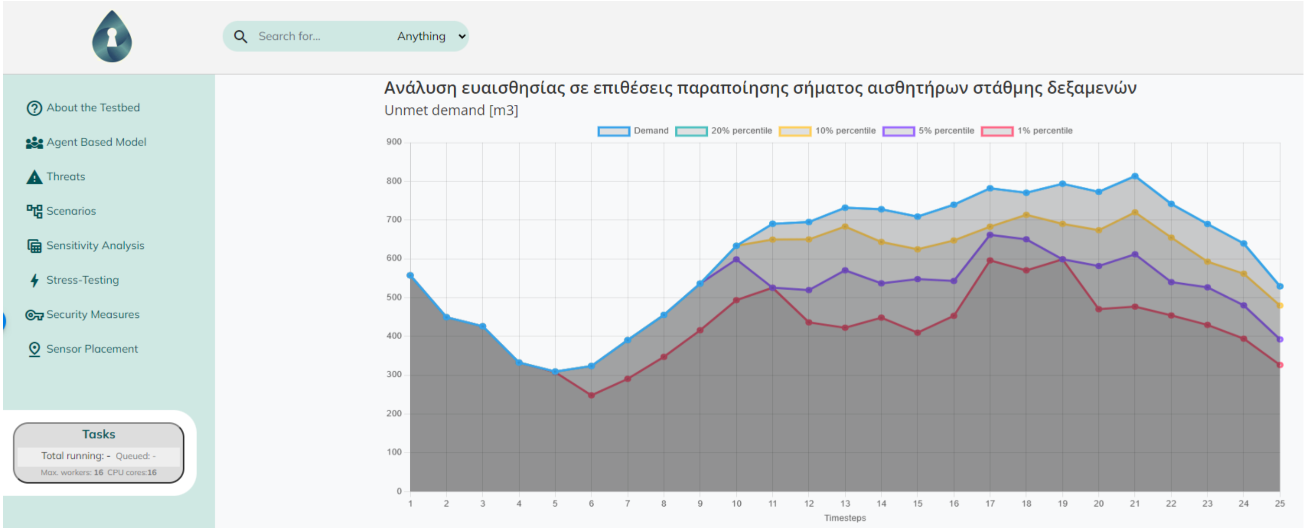
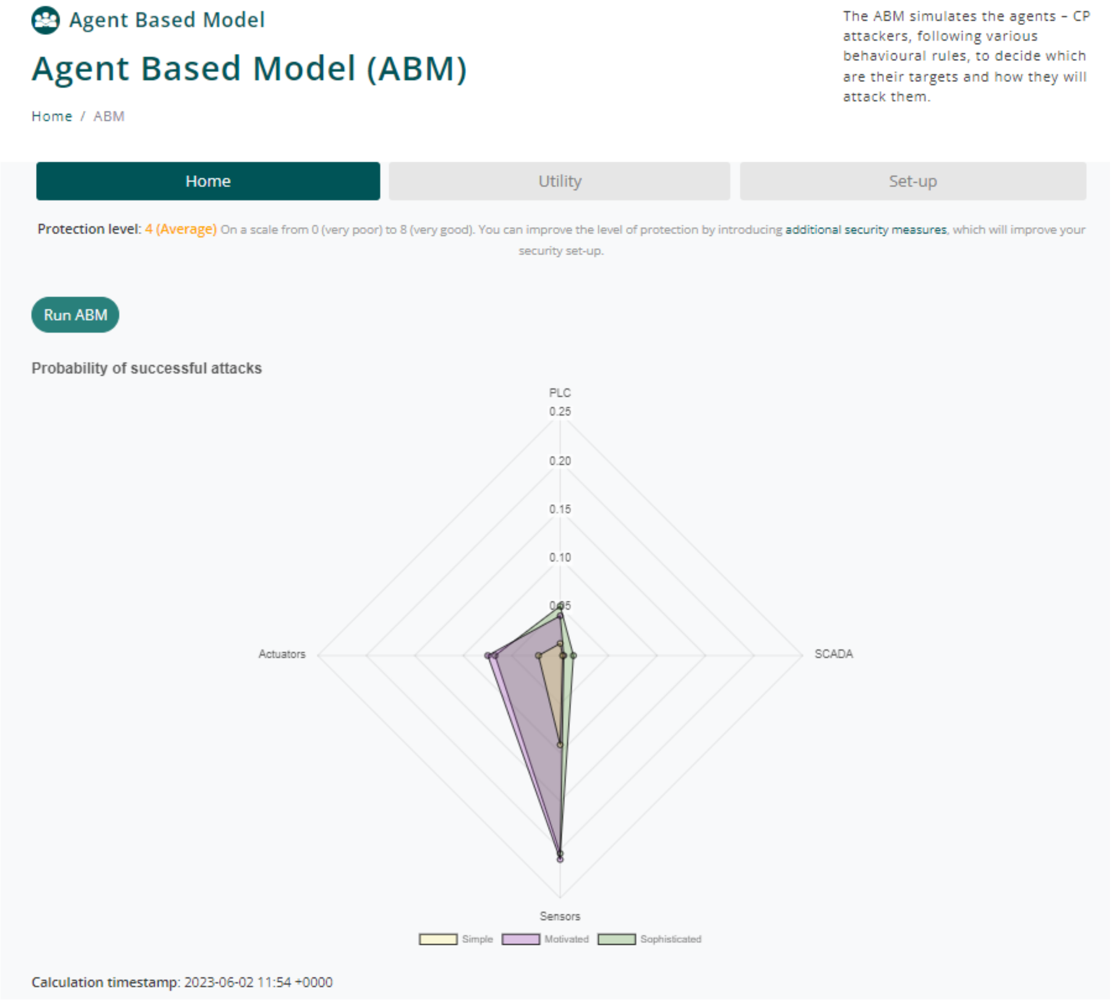


Figure 25 Sensitivity analysis aggregated timeseries chart demonstrating the expected demand and the average supply performance of the system under the 1% most critical scenarios, 5% most critical scenarios, 10% most critical scenarios and 20% most critical scenarios identified by the process

3.2.3 ASSESS THE LIKELIHOOD OF POTENTIAL CYBER-PHYSICAL THREATS

One of the fundamental steps in the risk assessment process is the identification and characterisation of potential cyber-physical threats and their likelihood of occurrence. This helps develop a better understanding of the utility's exposure to the threat landscape and the risks at hand. This step can be streamlined by the CPRISK-ABM (Koutiva et al., 2021; Moraitis et al., 2023) that can be accessed by the user through the "Agent Based Model" button (see Figure 5). With the necessary data provided in the previous step and after having configured the protection level though the questionnaire, the user can proceed to the analysis of the threat landscape and assess the likelihood of related cyber-physical attacks by clicking the "run" button. The model automatically calibrates its internal parameters to adjust to the utility specific characteristics and perform the assessment for both the network as a whole and for each element of the digital infrastructure, from sensors to SCADA. The platform provides a quick visualisation of the results in a spider diagram, seen in Figure 26.



Agent Based Model

Agent Based Model (ABM)

Home / ABM

The ABM simulates the agents – CP attackers, following various behavioural rules, to decide which are their targets and how they will attack them.

Protection level: 4 (Average) On a scale from 0 (very poor) to 8 (very good). You can improve the level of protection by introducing additional security measures, which will improve your security set-up.

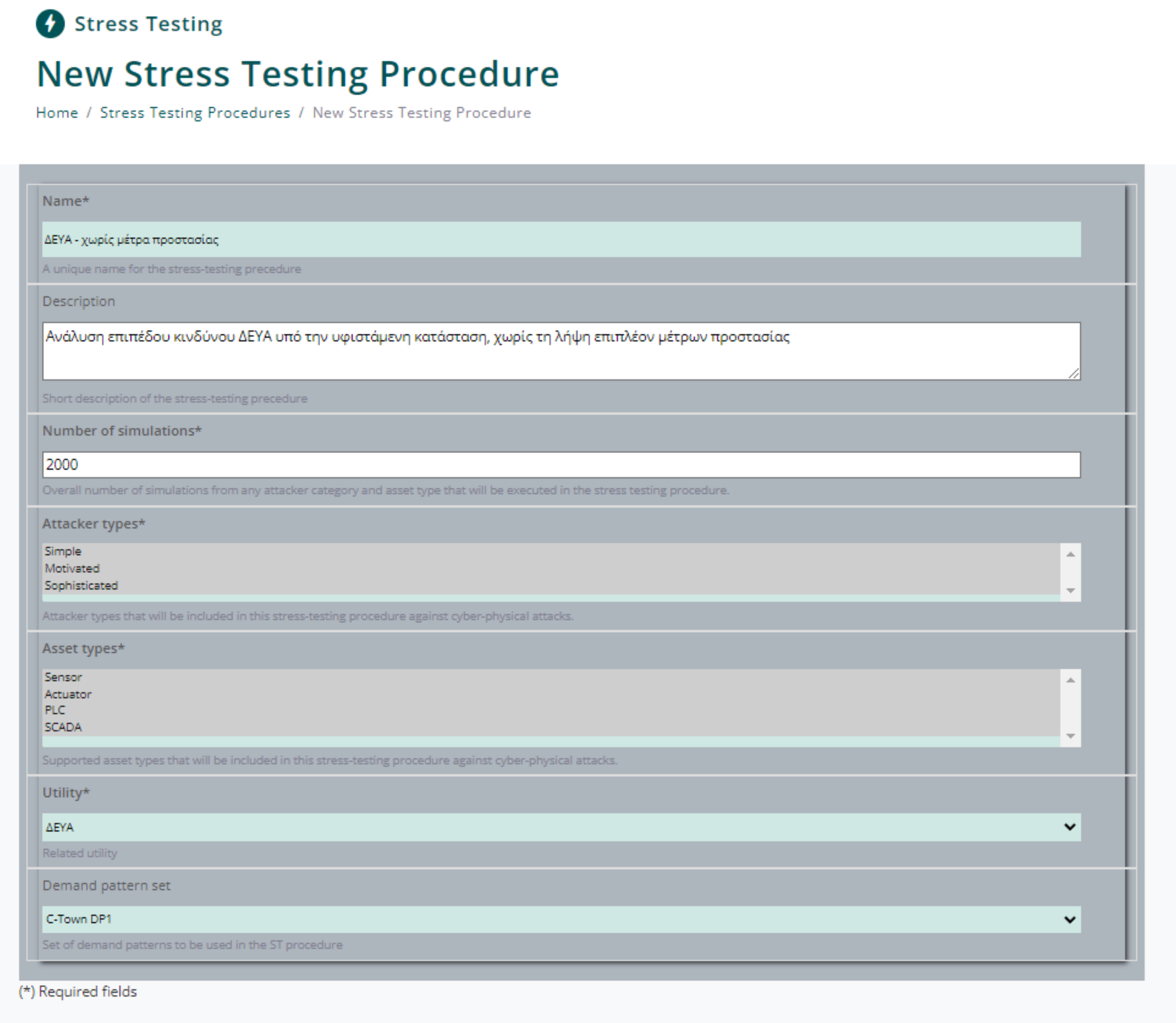
Calculation timestamp: 2023-06-02 11:54 +0000

Figure 26 CPRISK-ABM home page and visualisation of the analysis results per asset type

The ABM results for the semi-hypothetical utility of the case study, under the given cyber-security level, demonstrate a higher probability of successful attacks against the sensors of the system by all types of attackers. This adversarial preference can be attributed both to the behavioural choices of the attackers, and to the inbuild characteristics and vulnerabilities of such edge devices, in comparison for example with the more protected SCADA system. Those results however must not be misinterpreted as an indication that the SCADA system or the PLCs are sufficiently protected or attack-proof. They rather display the probability distribution of the threat landscape across the different assets of the system and the attackers' profile that would be associated with those attacks, under the existing practices and cyber-security protocols of the utility.

3.2.4 STRESS-TESTING AGAINST THE CURRENT CYBER-PHYSICAL THREAT LANDSCAPE

Having assessed the probabilities and characteristics of the cyber-physical threat landscape, the user can proceed with their analysis in the form of scenarios. After selecting from the menu (see Figure 5) to go to the Stress-testing Platform, the user selects to create a new stress test procedure. The user is then guided to the Stress-testing Procedure form (see Figure 27) where the user is asked to provide a name, while in addition an optional appropriate description can also be given. The user then selects the total number of scenarios to be automatically generated by the system, as well as whether these will concern the overall threat landscape resulting from ABM or part of it, e.g., with a focus only on specific types of devices or types of attacks. In the creation form, the platform automatically assigns the model defined within the utility's profile, yet it allows the user to choose a different model if needed. Finally, the system offers the option to stress-test the system using stochastic demand time series, created through the Stochastic Demand Generator, in order to account for the inherent uncertainties driven by demand variability (Moraitis et al., 2022; Tsoukalas et al., 2020, 2018). This allows to account for inherent, demand-driven uncertainties of the system's state under which a cyber-physical attack may occur.



Stress Testing

New Stress Testing Procedure

Home / Stress Testing Procedures / New Stress Testing Procedure

Name*

ΔΕΥΑ - χωρίς μέτρα προστασίας

A unique name for the stress-testing precedure

Description

Ανάλυση επιπέδου κινδύνου ΔΕΥΑ υπό την υφιστάμενη κατάσταση, χωρίς τη λήψη επιπλέον μέτρων προστασίας

Short description of the stress-testing precedure

Number of simulations*

2000

Overall number of simulations from any attacker category and asset type that will be executed in the stress testing procedure.

Attacker types*

Simple
Motivated
Sophisticated

Attacker types that will be included in this stress-testing procedure against cyber-physical attacks.

Asset types*

Sensor
Actuator
PLC
SCADA

Supported asset types that will be included in this stress-testing procedure against cyber-physical attacks.

Utility*

ΔΕΥΑ

Related utility

Demand pattern set

C-Town DP1

Set of demand patterns to be used in the ST procedure

(*) Required fields

Figure 27 Stress-testing Procedure form to create and parameterise the automated creation of scenarios based on the assessed cyber-physical threat landscape

For the purposes of this use case, a series of scenarios was created that represents the entire threat landscape of the hypothetical company, according to the applicable level of protection, for all types of devices and attacks, using the generated stochastic demand time series. The analysis was performed for a set of 2000 scenarios, which is considered a satisfactory sample of possible combinations. Nevertheless, the user may also choose smaller or larger sets of scenarios. After completing the creation and parameterisation of the stress-testing procedure, and initiating the analysis process, the system automatically composes the new scenarios, following the probability distributions derived from the CPRISK-ABM and randomly assigns to each of them a set of stochastic demand time series. Upon completion of the analysis, the user can explore the risk level both at system level and per asset type, through the relevant risk matrices, as seen in Figure 28.

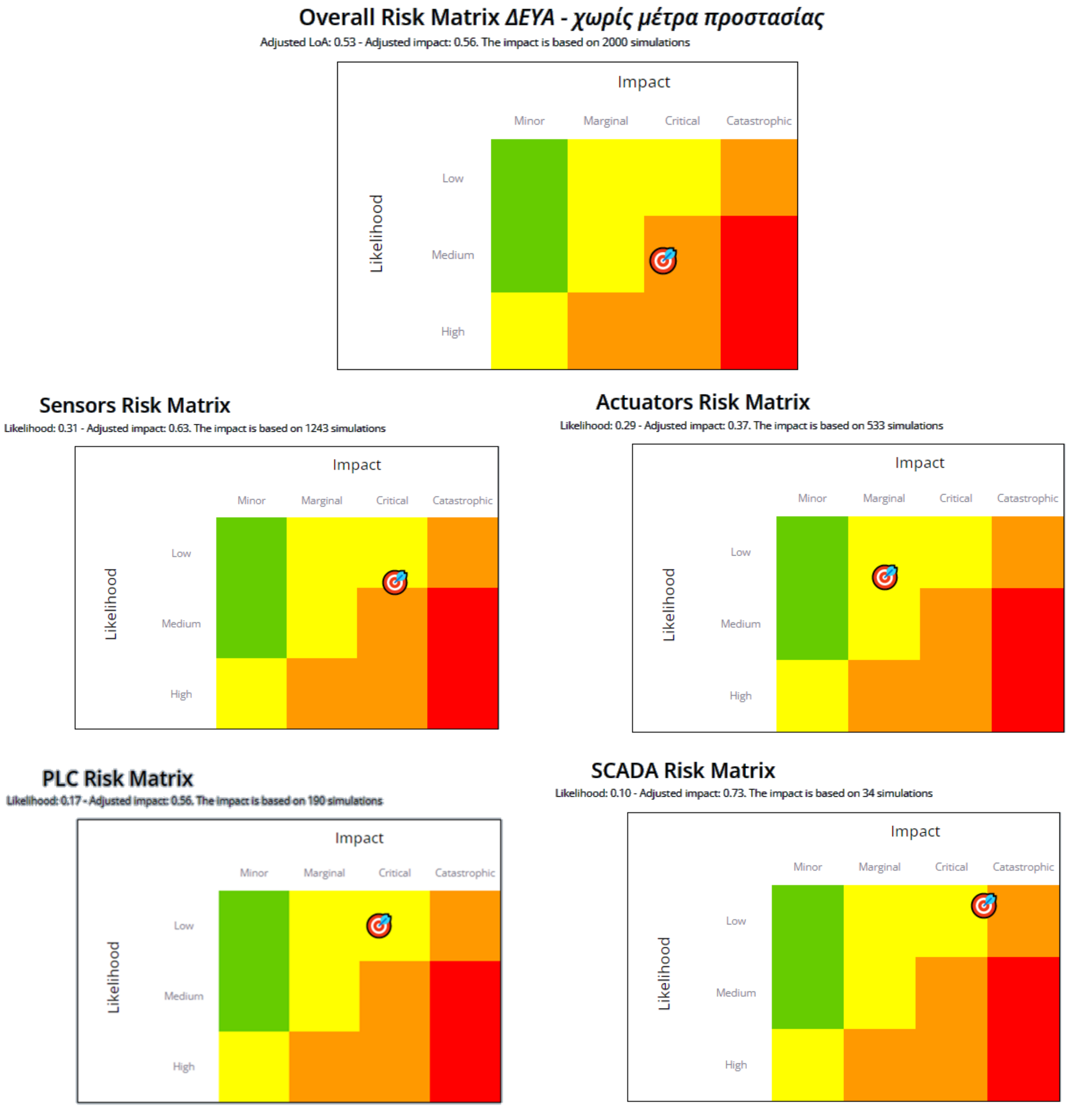
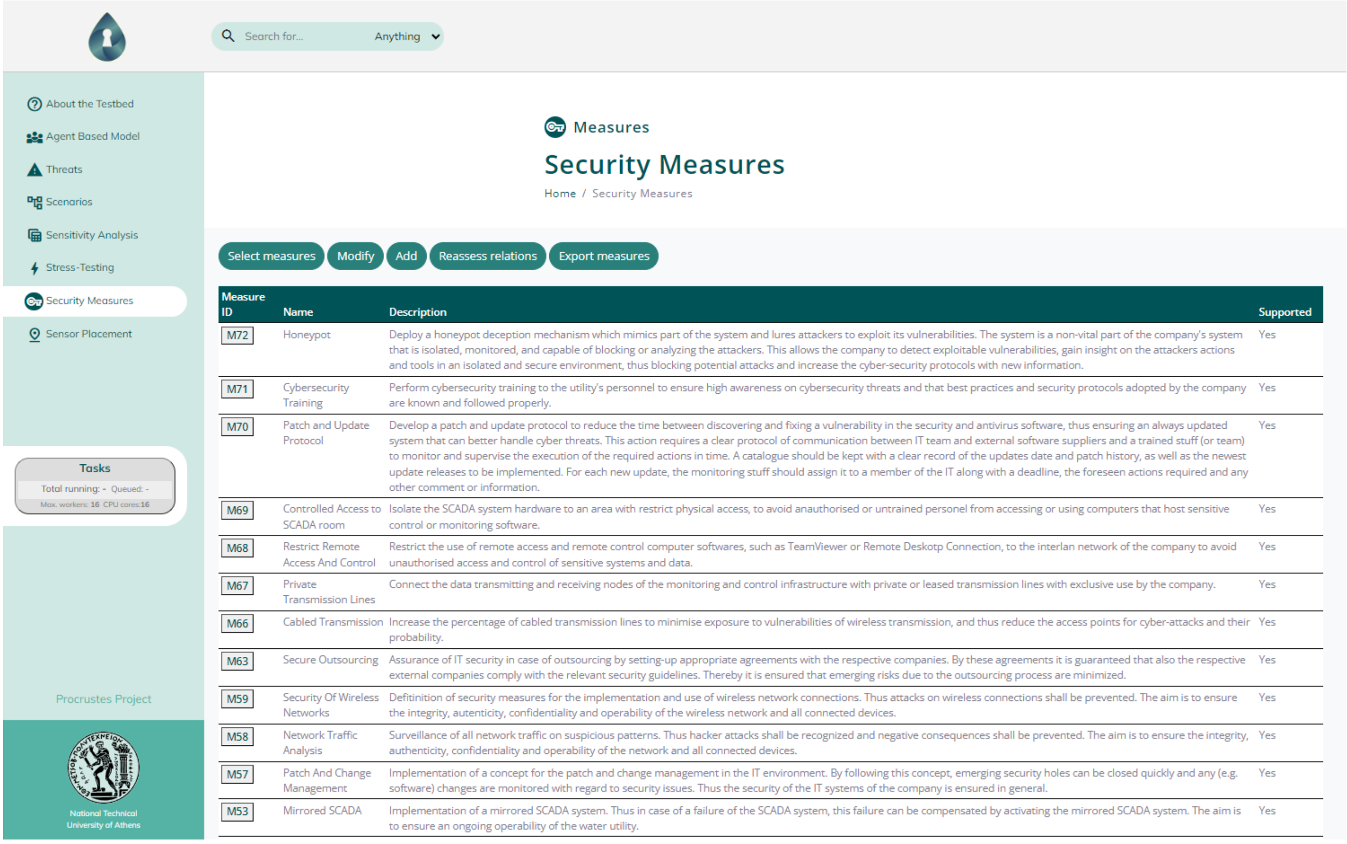


Figure 28 PROCRUSTES risk matrices in respect to the total system and the risk level per asset type

It is worth noting that the classes on both the axis of probability (vertical) and that of impact (horizontal) can be adjusted by the platform operator, to represent the company's risk criteria and tolerance. The simulation of the 2000 scenarios lasted approximately 1 hour, since the system's parallel computing significantly accelerates time-consuming processes.

3.2.5 SELECTION AND EVALUATION OF POTENTIAL TREATMENT MEASURES

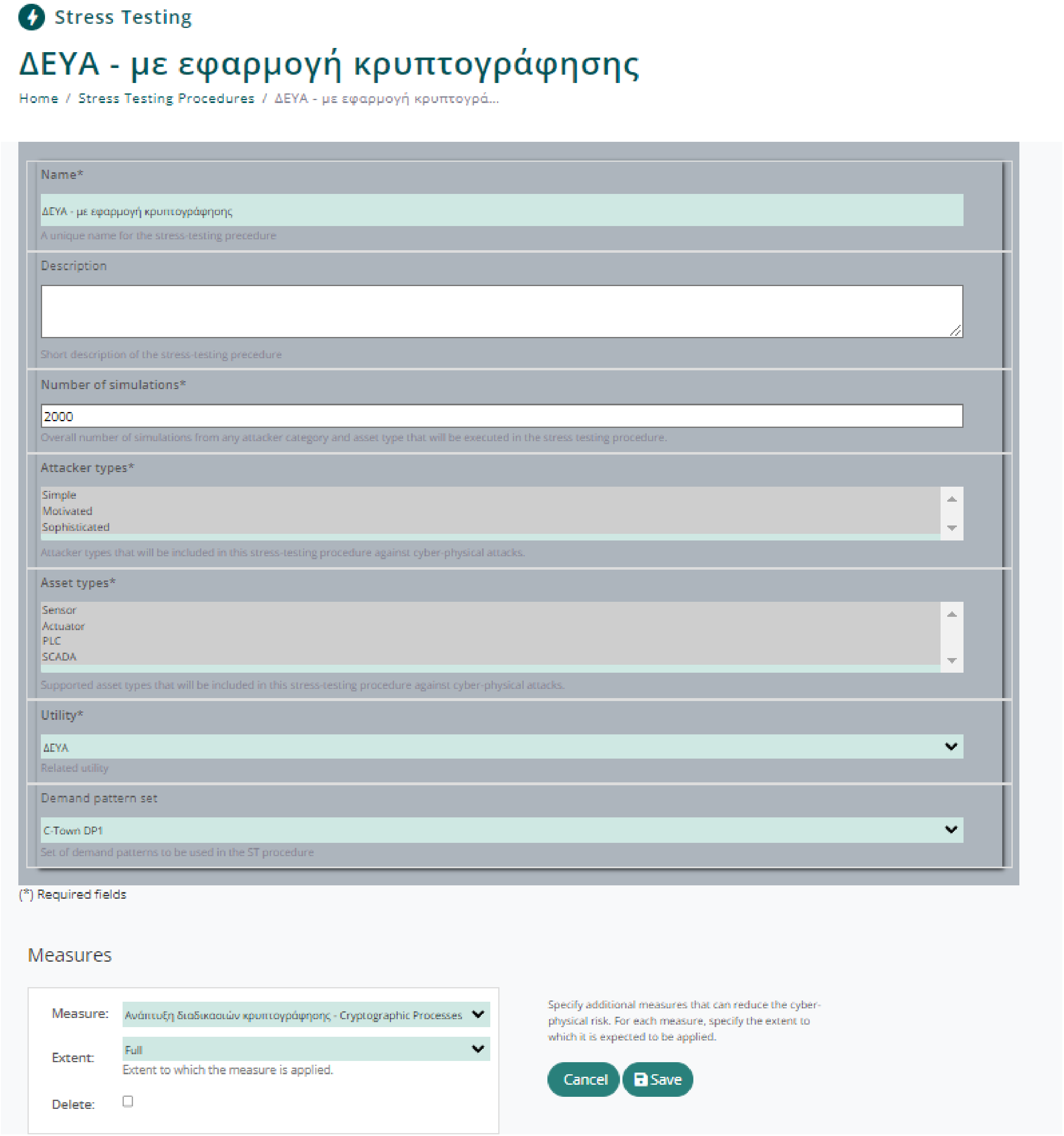
In addition to analysing the risk level under the existing protection level, the platform offers the ability to select, analyse and evaluate the performance of various protection and mitigation measures. Those measures can aim either at reducing the likelihood of occurrence or the impact those threats can have on the system or can act in combination. Those measures can be explored through the Risk Reduction Knowledge Base (RRKB), seen in Figure 29. The RRKB is designed to be scalable and enables the continuous integration of the latest best practices and innovative technologies that can help address the threats faced by the water utilities. The performance of some selected measures can be assessed by comparing the results of simulated scenarios with improved measures with the results of simulations without them.



Measure ID	Name	Description	Supported
M72	Honeypot	Deploy a honeypot deception mechanism which mimics part of the system and lures attackers to exploit its vulnerabilities. The system is a non-vital part of the company's system that is isolated, monitored, and capable of blocking or analyzing the attackers. This allows the company to detect exploitable vulnerabilities, gain insight on the attackers actions and tools in an isolated and secure environment, thus blocking potential attacks and increase the cyber-security protocols with new information.	Yes
M71	Cybersecurity Training	Perform cybersecurity training to the utility's personnel to ensure high awareness on cybersecurity threats and that best practices and security protocols adopted by the company are known and followed properly.	Yes
M70	Patch and Update Protocol	Develop a patch and update protocol to reduce the time between discovering and fixing a vulnerability in the security and antivirus software, thus ensuring an always updated system that can better handle cyber threats. This action requires a clear protocol of communication between IT team and external software suppliers and a trained stuff (or team) to monitor and supervise the execution of the required actions in time. A catalogue should be kept with a clear record of the updates date and patch history, as well as the newest update releases to be implemented. For each new update, the monitoring stuff should assign it to a member of the IT along with a deadline, the foreseen actions required and any other comment or information.	Yes
M69	Controlled Access to SCADA room	Isolate the SCADA system hardware to an area with restrict physical access, to avoid anauthorised or untrained personel from accessing or using computers that host sensitive control or monitoring software.	Yes
M68	Restrict Remote Access And Control	Restrict the use of remote access and remote control computer softwares, such as TeamViewer or Remote Deskotp Connection, to the interlan network of the company to avoid unauthorised access and control of sensitive systems and data.	Yes
M67	Private Transmission Lines	Connect the data transmitting and receiving nodes of the monitoring and control infrastructure with private or leased transmission lines with exclusive use by the company.	Yes
M66	Cabled Transmission	Increase the percentage of cabled transmission lines to minimise exposure to vulnerabilities of wireless transmission, and thus reduce the access points for cyber-attacks and their probability.	Yes
M63	Secure Outsourcing	Assurance of IT security in case of outsourcing by setting-up appropriate agreements with the respective companies. By these agreements it is guaranteed that also the respective external companies comply with the relevant security guidelines. Thereby it is ensured that emerging risks due to the outsourcing process are minimized.	Yes
M59	Security Of Wireless Networks	Defitinition of security measures for the implementation and use of wireless network connections. Thus attacks on wireless connections shall be prevented. The aim is to ensure the integrity, autenticity, confidentiality and operability of the wireless network and all connected devices.	Yes
M58	Network Traffic Analysis	Surveillance of all network traffic on suspicious patterns. Thus hacker attacks shall be recognized and negative consequences shall be prevented. The aim is to ensure the integrity, authenticity, confidentiality and operability of the network and all connected devices.	Yes
M57	Patch And Change Management	Implementation of a concept for the patch and change management in the IT environment. By following this concept, emerging security holes can be closed quickly and any (e.g. software) changes are monitored with regard to security issues. Thus the security of the IT systems of the company is ensured in general.	Yes
M53	Mirrored SCADA	Implementation of a mirrored SCADA system. Thus in case of a failure of the SCADA system, this failure can be compensated by activating the mirrored SCADA system. The aim is to ensure an ongoing operability of the water utility.	Yes

Figure 29 RRKB interface with a portion of the registered risk reduction measures for exploration

To investigate the effects and efficiency of one or multiple protection measures on the utility's risk level, the platform allows for their automatic integration during the design of stress testing scenarios. Following the same steps to create a new stress-testing procedure, the user provides the name and description of the analysis, the desired number of scenarios as well as the investigation of all possible attacks and asset types or for a part of them. At the end, the selects from a dropdown list the desired risk reduction measure for examination as well as the degree of its implementation (full, partial or limited application), as shown in Figure 30.



Stress Testing

ΔΕΥΑ - με εφαρμογή κρυπτογράφησης

Home / Stress Testing Procedures / ΔΕΥΑ - με εφαρμογή κρυπτογρά...

Name*

ΔΕΥΑ - με εφαρμογή κρυπτογράφησης

A unique name for the stress-testing precedure

Description

Short description of the stress-testing precedure

Number of simulations*

2000

Overall number of simulations from any attacker category and asset type that will be executed in the stress testing procedure.

Attacker types*

Simple
Motivated
Sophisticated

Attacker types that will be included in this stress-testing procedure against cyber-physical attacks.

Asset types*

Sensor
Actuator
PLC
SCADA

Supported asset types that will be included in this stress-testing procedure against cyber-physical attacks.

Utility*

ΔΕΥΑ

Related utility

Demand pattern set

C-Town DP1

Set of demand patterns to be used in the ST procedure

(*) Required fields

Measures

Measure: Ανάπτυξη διαδικασιών κρυπτογράφησης - Cryptographic Processes

Extent: Full

Extent to which the measure is applied.

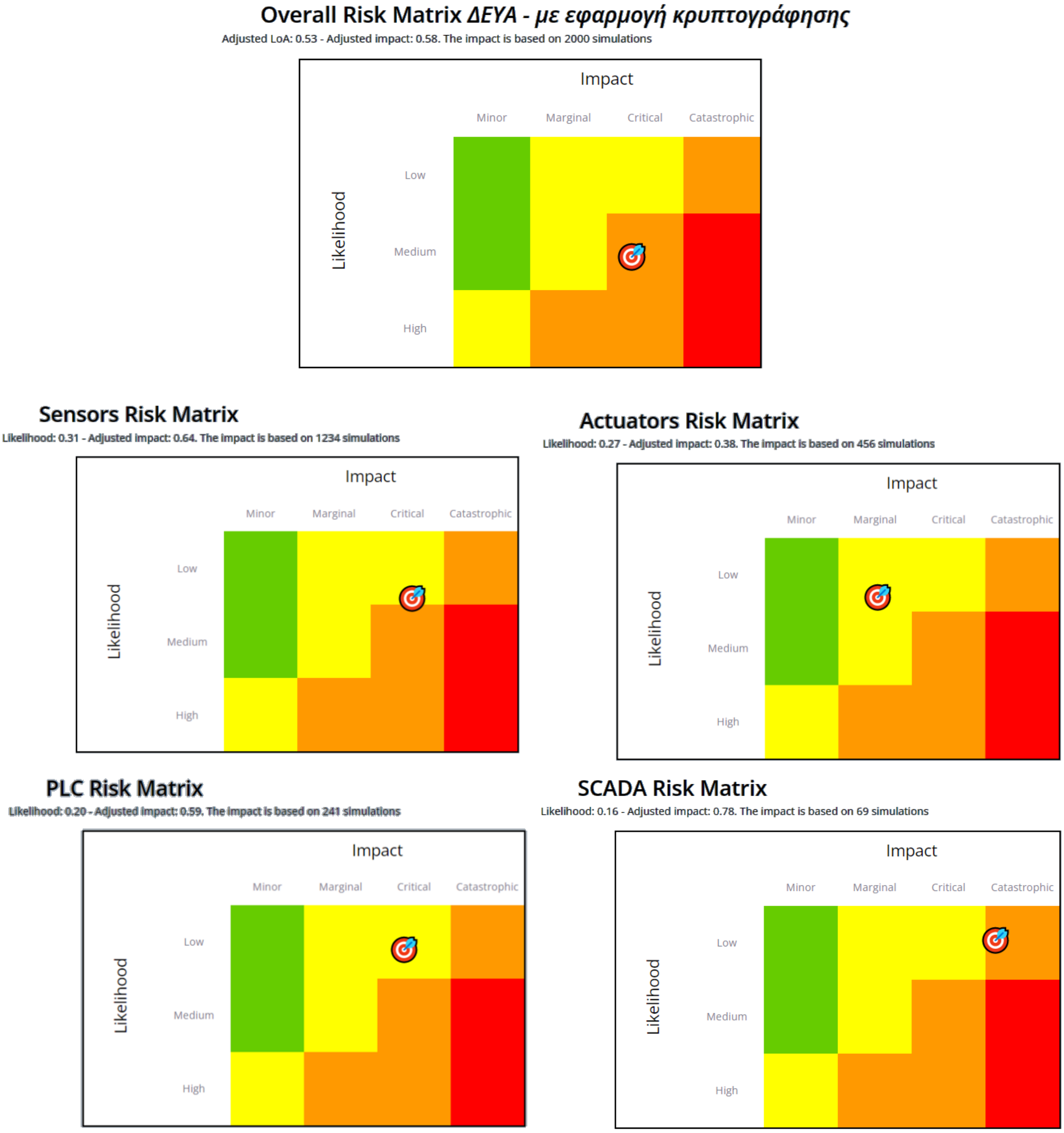
Delete: □

Specify additional measures that can reduce the cyber-physical risk. For each measure, specify the extent to which it is expected to be applied.

Figure 30 Stress-testing Procedure form to create and parameterise the automated creation of scenarios based on the assessed cyber-physical threat landscape with the addition of risk reduction measures

Having identified and selected the desired measure(s) for evaluation, the user can proceed to save the new stress-testing procedure and initiate the simulation as before. The system automatically integrates the user-selected measures into the processes, redefining the company's level of protection – from which the new distribution of attacks for analysis is derived.

For the purposes of this use case, we explore the full implementation of cryptographic processes, as a measure selected by the supporting Greek utilities in the relevant technical meeting under MS4.1. The results of the measures implementation in respect to the modification of risk at system and asset level can be seen in Figure 31.



Overall Risk Matrix ΔΕΥΑ - με εφαρμογή κρυπτογράφησης

Adjusted LoA: 0.53 - Adjusted impact: 0.58. The impact is based on 2000 simulations

Sensors Risk Matrix

Likelihood: 0.31 - Adjusted impact: 0.64. The impact is based on 1234 simulations

Actuators Risk Matrix

Likelihood: 0.27 - Adjusted impact: 0.38. The impact is based on 456 simulations

PLC Risk Matrix

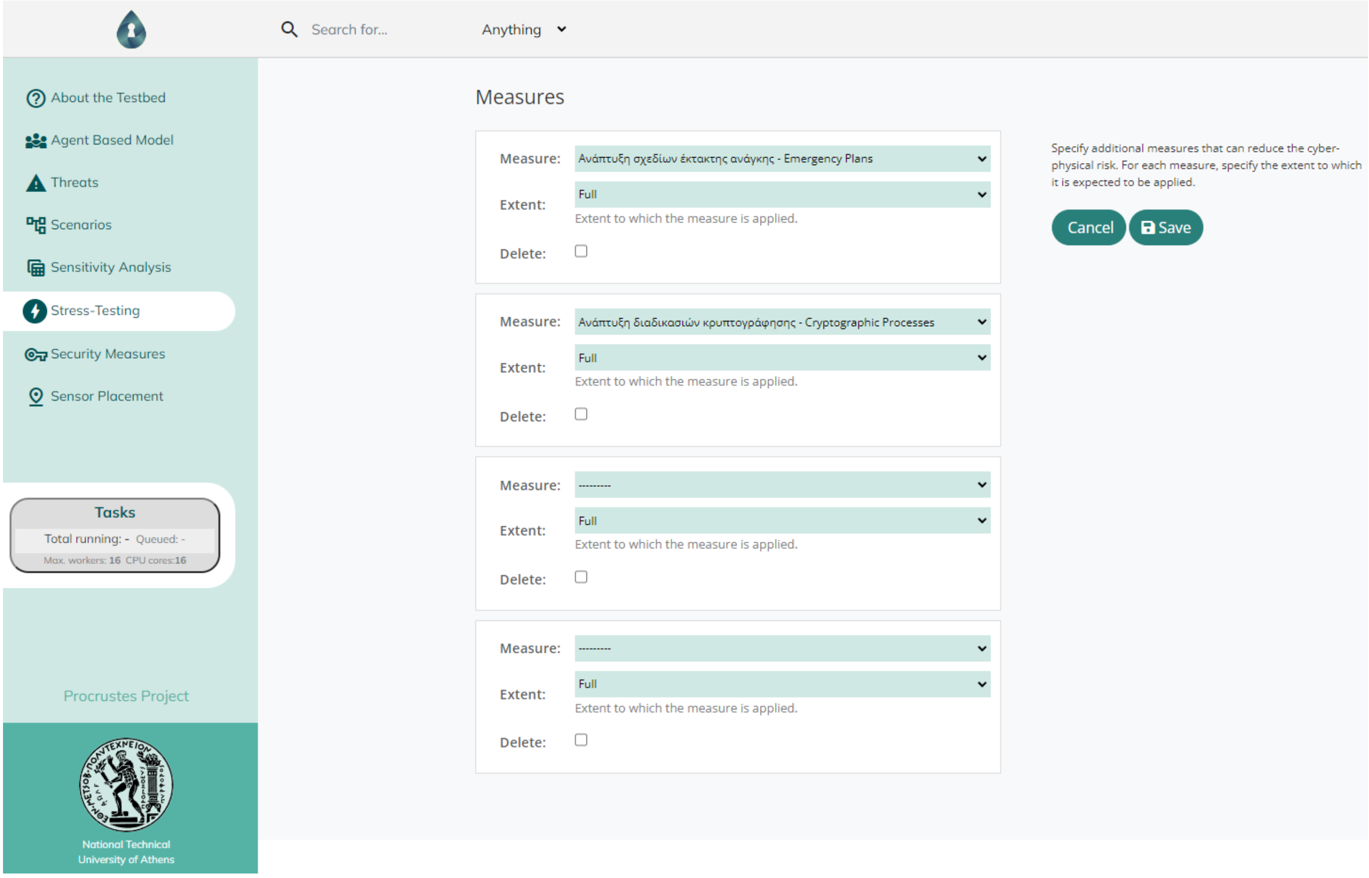
Likelihood: 0.20 - Adjusted impact: 0.59. The impact is based on 241 simulations

SCADA Risk Matrix

Likelihood: 0.16 - Adjusted impact: 0.78. The impact is based on 69 simulations

Figure 31 PROCRUSTES risk matrices in respect to the total system and the risk level per asset type with the full implementation of cryptographic processes

The user may also select to explore the combinatory effects of more than one measures, to analyse and evaluate the potentials of a multistep strategic plan to modify cyber-physical risks and ensure more secure and resilient services. After following the steps of creating a new stress-testing procedure, as described, the user can select to select and import additional measures, and independently select their degrees of implementation (full, partial, or limited application). After filling in the available forms, the platform will automatically generate new forms for additional measures. An example of multiple measures selection in the stress-testing procedure, can be seen in Figure 32.



Total running: - Queued: -
Max. workers: 16 CPU cores:16

Measures

Measure: Ανάπτυξη σχεδίων έκτακτης ανάγκης - Emergency Plans
Extent: Full
Extent to which the measure is applied.
Delete: □

Measure: Ανάπτυξη διαδικασιών κρυπτογράφησης - Cryptographic Processes
Extent: Full
Extent to which the measure is applied.
Delete: □

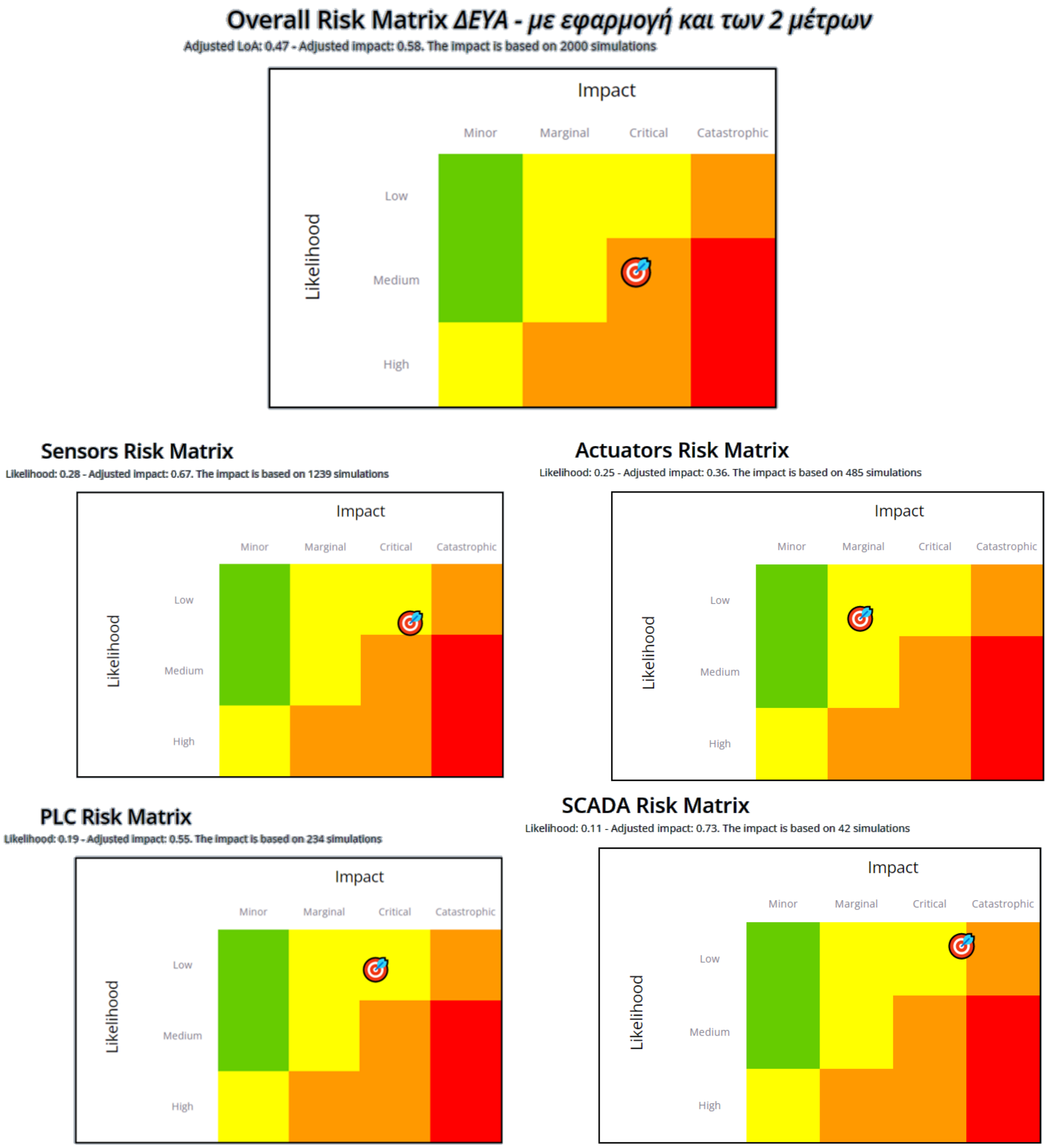
Measure: ---------
Extent: Full
Extent to which the measure is applied.
Delete: □

Measure: ---------
Extent: Full
Extent to which the measure is applied.
Delete: □

Specify additional measures that can reduce the cyber-physical risk. For each measure, specify the extent to which it is expected to be applied.

Figure 32 Measure selection forms for the selection of one or multiple mitigation measures from the RRKB to be integrated and analysed under a stress-testing procedure – example with the selection of 2 measures, (a) Emergency Plans and (b) Cryptographic Processes, with full implementation

For the needs of this case study, we select the addition of the second risk reduction measure, as ranked in the MS4.1 by the supporting water utilities. To maintain comparability among the stress-testing outcomes, the new procedure also accounts for the entire threat landscape against all types of assets, under a set of 2000 scenarios with stochastic demand timeseries. The combinatory effects of the 2 selected measures implementation in respect to the modification of risk at system and asset level can be seen in Figure 33.



Overall Risk Matrix ΔΕΥΑ - με εφαρμογή και των 2 μέτρων

Adjusted LoA: 0.47 - Adjusted impact: 0.58. The impact is based on 2000 simulations

Sensors Risk Matrix

Likelihood: 0.28 - Adjusted impact: 0.67. The impact is based on 1239 simulations

Actuators Risk Matrix

Likelihood: 0.25 - Adjusted impact: 0.36. The impact is based on 485 simulations

PLC Risk Matrix

Likelihood: 0.19 - Adjusted impact: 0.55. The impact is based on 234 simulations

SCADA Risk Matrix

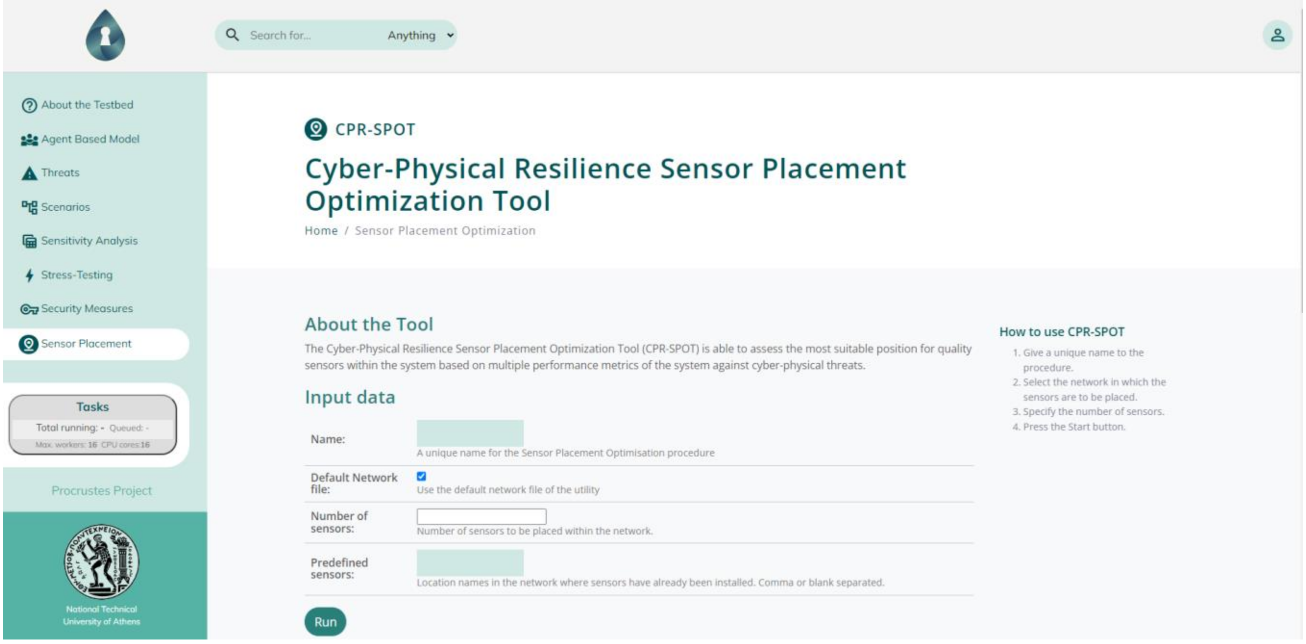
Likelihood: 0.11 - Adjusted impact: 0.73. The impact is based on 42 simulations

Figure 33 PROCRUSTES risk matrices in respect to the total system and the risk level per asset type with the combinatory effects of (a) cryptographic processes and (b) emergency plans

To provide a better understanding of the performance of the system under a given type of threat or threats examined in the stress-testing procedure, the user may also select to see the spectrum of the system's performance under any given scenario. This can be done by selecting the relevant KPI metric next to the scenario, from the scenario list, as seen in the sensitivity analysis section. As before, the stress-testing outputs are exportable for further post-processing and/or reporting.

3.2.6 OPTIMAL SENSOR PLACEMENT

In addition to the enhancement of the physical and cybersecurity practices and the adoption of new technologies to help prevent, mitigate, or respond to cyber-physical incidents, the utilities may also seek to design new quality sensor layout or upgrade of a pre-existing with the goal of maximizing the resilience in terms of a reducing the expected impact of cyber-physical attacks. The Cyber-Physical Resilience Sensor Placement Optimization Tool (CPR-SPOT) (Nikolopoulos et al., 2022; Nikolopoulos and Makropoulos, 2023) is able to assess the most suitable position for quality sensors within the system based on multiple performance metrics of the system against cyber-physical threats. The user can access the tool through the "CPR-SPOT" button on the main screen (see Figure 5), or select "Sensor Placement" from the tools' banner located on the left side of the screen. Then, the user will be guided to a new interface, as seen in Figure 34 below.



Cyber-Physical Resilience Sensor Placement Optimization Tool

Home / Sensor Placement Optimization

About the Tool

The Cyber-Physical Resilience Sensor Placement Optimization Tool (CPR-SPOT) is able to assess the most suitable position for quality sensors within the system based on multiple performance metrics of the system against cyber-physical threats.

Input data

Name: A unique name for the Sensor Placement Optimisation procedure

Default Network file: ☑ Use the default network file of the utility

Number of sensors: Number of sensors to be placed within the network.

Predefined sensors: Location names in the network where sensors have already been installed. Comma or blank separated.

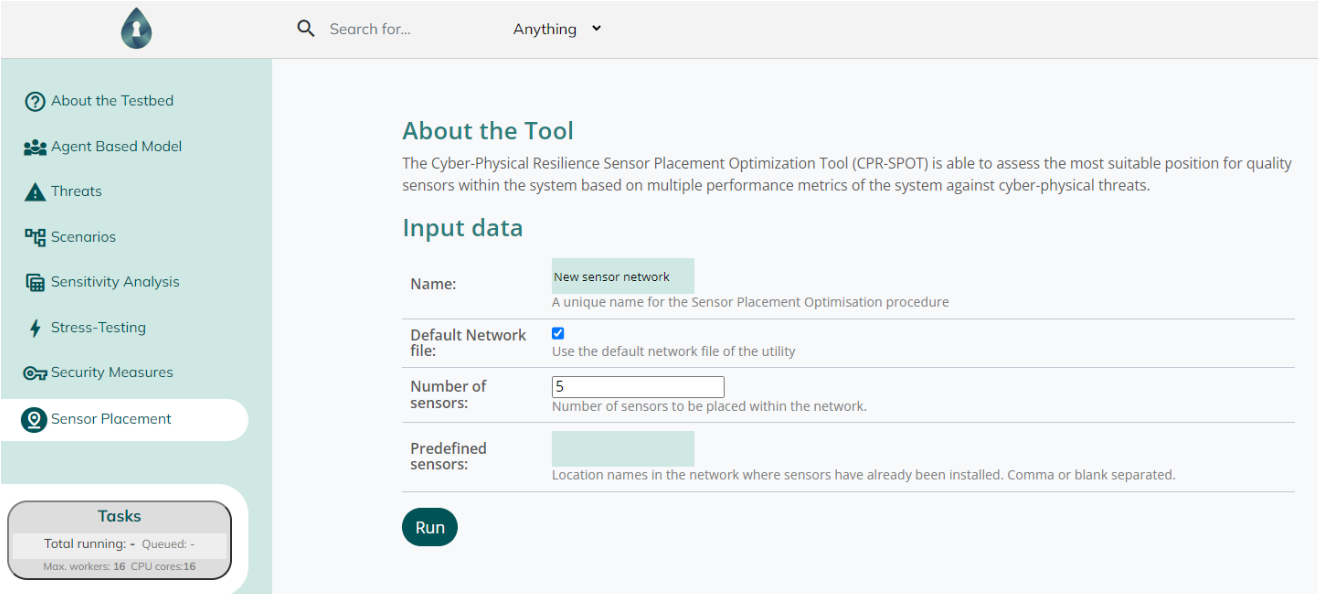
Run

How to use CPR-SPOT

1. Give a unique name to the procedure.
2. Select the network in which the sensors are to be placed.
3. Specify the number of sensors.
4. Press the Start button.

Figure 34 CPR-SPOT tool interface for the creation and parameterisation of the resilient sensor placement optimisation

The tool can be utilised under 2 potential use cases, i.e., to provide a new optimal sensor placement design of water quality sensors, or to provide the optimal sensor placement of new sensors in an existing sensing network. To design from scratch a new optimal sensor design, the user can create a new optimisation scheme using the CPR-SPOT interface and define the number of sensors that the utility plans/wishes to install. For the needs of this use case we assume that the utility does not have an existing quality sensor network and plans to install a network of 5 quality sensors. The user provides a name for the optimisation procedure and selects the number of sensors in the relevant field of the CPR-SPOT form, leaving empty the filed of "predefined sensors", as seen in Figure 35.



About the Tool

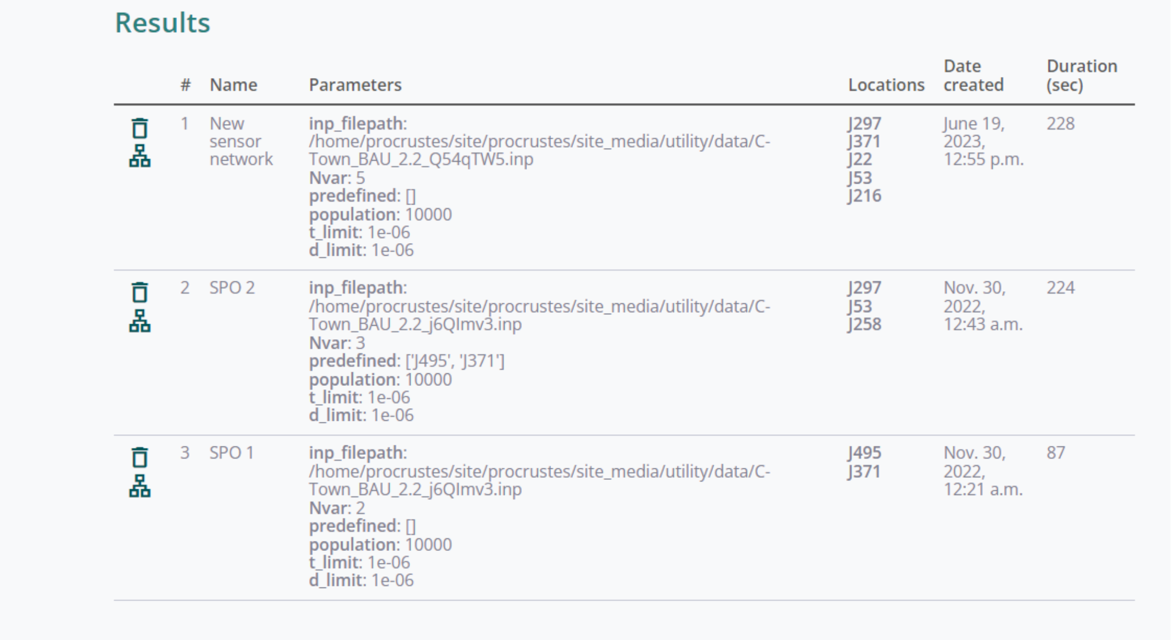
The Cyber-Physical Resilience Sensor Placement Optimization Tool (CPR-SPOT) is able to assess the most suitable position for quality sensors within the system based on multiple performance metrics of the system against cyber-physical threats.

Input data

Name:	New sensor network A unique name for the Sensor Placement Optimisation procedure
Default Network file:	☑ Use the default network file of the utility
Number of sensors:	5 Number of sensors to be placed within the network.
Predefined sensors:	 Location names in the network where sensors have already been installed. Comma or blank separated.

Figure 35 CPR-SPOT tool interface for the creation and parameterisation of a new optimal design with 5 quality sensors

After setting-up the optimisation, the user selects to initiate the procedure by clicking the “Run” button located below the parameters field. Upon completion, the system updates the “Results” field in the interface. From there, the user can quickly see the optimal location of the new sensors in the “Locations” column, representing the ID of the node as found in the network model. By selecting the “Network” button, located on the left of each optimisation result, the user can gain a visual overview of the optimal sensor locations, as seen in Figure 37. The CPR-SPOT optimal positioning can also be used to optimally allocate existing sensors placed in the system, without the need of acquiring new instruments.



Results

#	Name	Parameters	Locations	Date created	Duration (sec)
1	New sensor network	**inp_filepath:** /home/procrustes/site/procrustes/site_media/utility/data/C-Town_BAU_2.2_Q54qTW5.inp **Nvar:** 5 **predefined:** [] **population:** 10000 **t_limit:** 1e-06 **d_limit:** 1e-06	J297 J371 J22 J53 J216	June 19, 2023, 12:55 p.m.	228
2	SPO 2	**inp_filepath:** /home/procrustes/site/procrustes/site_media/utility/data/C-Town_BAU_2.2_j6QImv3.inp **Nvar:** 3 **predefined:** ['J495', 'J371'] **population:** 10000 **t_limit:** 1e-06 **d_limit:** 1e-06	J297 J53 J258	Nov. 30, 2022, 12:43 a.m.	224
3	SPO 1	**inp_filepath:** /home/procrustes/site/procrustes/site_media/utility/data/C-Town_BAU_2.2_j6QImv3.inp **Nvar:** 2 **predefined:** [] **population:** 10000 **t_limit:** 1e-06 **d_limit:** 1e-06	J495 J371	Nov. 30, 2022, 12:21 a.m.	87

Figure 36 CPR-SPOT results interface

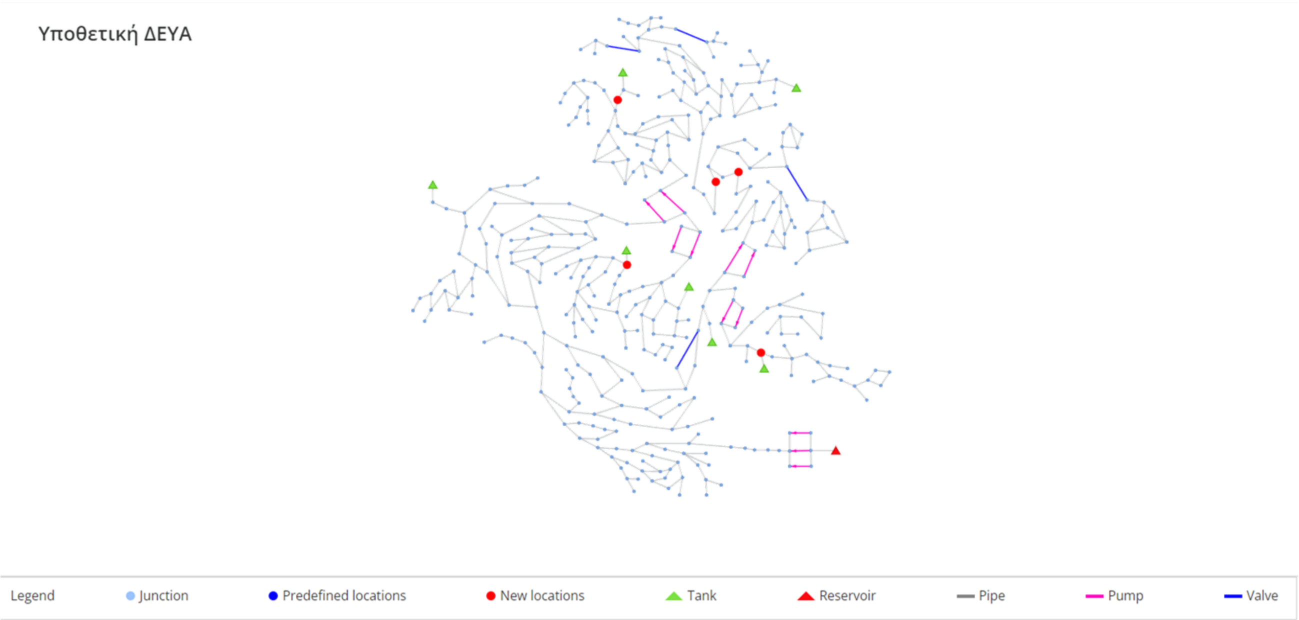
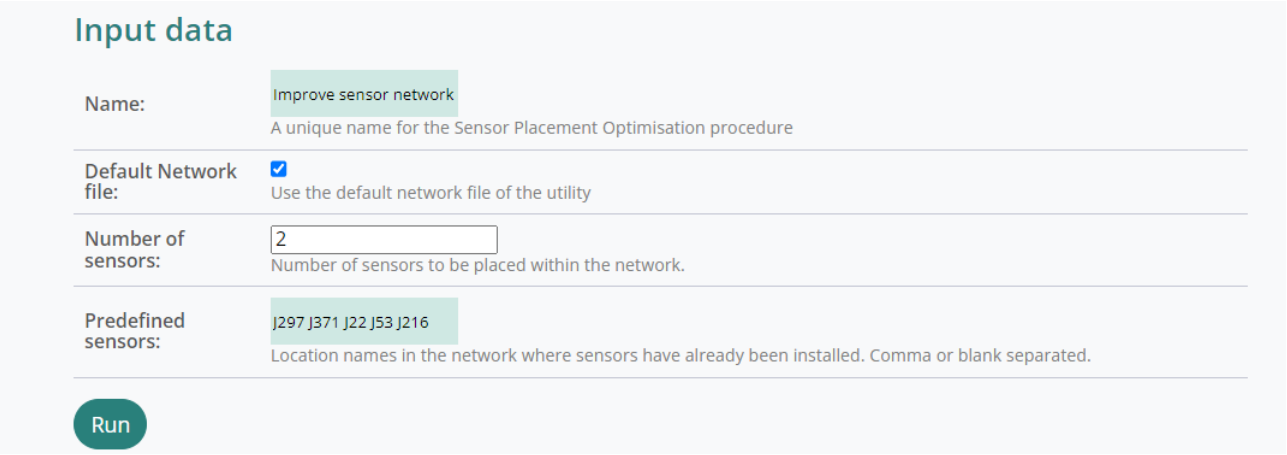


Figure 37 Spatial visualisation of CPR-SPOT identified optimal locations of 5 new quality sensors – marked with red circles

The second use case of the CPR-SPOT tool is for the purposes of improving the resilience of an existing sensor network with the addition of new quality sensors in the network. For this use, the user will follow the steps previously described, providing a new name for the optimisation procedure, the desired/planned number of new sensors to be placed in the network and the position of the existing sensors in the network. Assuming the semi-hypothetical utility of the use case wished to expand the optimal quality sensor network previously identified with 2 extra sensors, the user fills the relevant fields in the CPR-SPOT form, as seen in Figure 38.



Input data

Name:	Improve sensor network A unique name for the Sensor Placement Optimisation procedure
Default Network file:	☑ Use the default network file of the utility
Number of sensors:	2 Number of sensors to be placed within the network.
Predefined sensors:	J297 J371 J22 J53 J216 Location names in the network where sensors have already been installed. Comma or blank separated.

Figure 38 CPR-SPOT tool interface for the creation and parameterisation of an optimal enhancement of existing network with the addition of 2 new sensors

As before, the user can identify the optimal location of the 2 new sensors in the network by browsing the results table and visually overview their position in the system by pressing the “Network” button located on the left side of the scenario. The spatial overview of the enhanced quality sensor network can be seen in Figure 39.

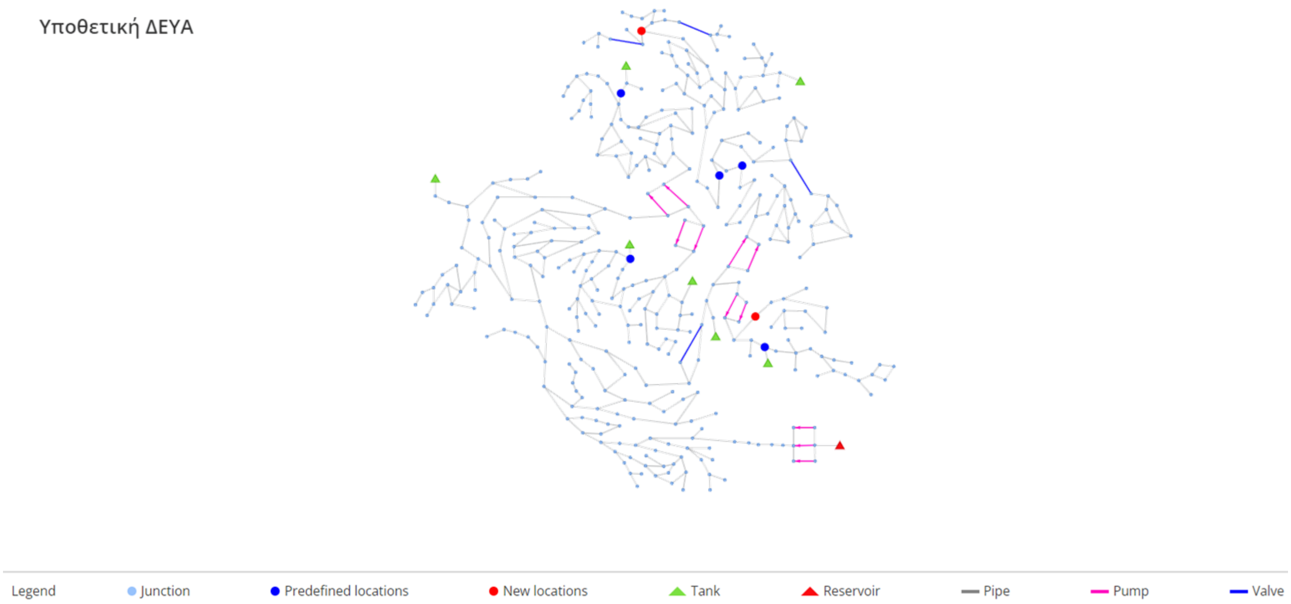


Figure 39 Spatial visualisation of CPR-SPOT identified optimal locations of 2 new quality sensors, marked with red circles, taking into account the existing network, marked with blue circles

4 EU and National Legislation & Standards

In December 2022, the EU published the NIS2 Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148[3]. NIS2 Directive identifies the water sector as essential, in amendment of NIS, and thus applies to public and private water utilities – characterising them as "essential" or "important" entities. The NIS2 updates the legal framework of EU around cybersecurity with the provision of security requirements and incident reporting by the water utilities. More specifically it strictly foresees accountability for top management for non-compliance with cybersecurity risk management measures and calls for risk-based approaches that will allow the identification of appropriate and proportionate cybersecurity measures for each utility.

Adhering to the up to now Directive in force, i.e., NIS, the Ministry of Digital Governance and the National Cybersecurity Authority of the Hellenic Republic, published in December 2020 the National Cybersecurity Strategy 2020-2025[4], a comprehensive document that outlines the strategic objectives and activities to enhance cybersecurity Greece. The strategy aims to address the evolving cyber threats landscape and safeguard critical infrastructure and essential services.

The document begins with a situation analysis, identifying various types of cyber threats, including malicious software, web-based attacks, phishing, and denial of service attacks. It emphasizes the need for a functional cybersecurity governance system to effectively combat these threats. The strategy focuses on five strategic goals: developing a functional cybersecurity governance system, protecting critical infrastructures, optimizing incident management, creating a modern environment for cybersecurity investments, and building capacity in cybersecurity. To achieve these goals, specific objectives and flagship activities are outlined. These include strengthening national, European, and international collaborations, comprehending technological developments and their effects on digital governance, conducting information and network security audits, ensuring compliance with security policies and standards, and protecting personal data. The strategy also highlights the importance of public-private partnerships, research and development, and investments in security measures. It emphasizes the need for contingency planning, incident reporting, and security and privacy protection. Overall, the National Cybersecurity Strategy for 2020-2025 aims to enhance the resilience of critical infrastructure, strengthen cybersecurity capabilities, promote international cooperation, and raise awareness about cybersecurity risks. It

[3] The Member states shall repeal the NIS Directive and put the NIS2 Directive into force by no later than 17th of October 2024.

[4] Accessible through: https://mindigital.gr/wp-content/uploads/2022/11/EL-NATIONAL-CYBER-SECURITY-STRATEGY-2020_2025.pdf

provides a roadmap for the Hellenic Republic to effectively address cyber threats and protect its digital landscape. This strategy is accompanied by key legislative initiatives at national level, that include the laws 4577/2018 (associated to Ministerial Decision 1027/2019 - Official Gazette 3739/B/8-10-2019 and the previous NIS Directive) and 4961/2022 - Official Gazette A 146/27.07.2022 on strengthening digital governance and critical digital infrastructure, which inter alia foresee the incidents' report to the National Cybersecurity Authority of Greece (see Appendix B).

At EU level, another important legislative initiative was the issue of Directive on Critical Entities Resilience (CER Directive (EU) 2022/2557), aiming to reinforce the ability of EU critical entities to prevent, protect against, respond to, and recover from incidents that have the potential to disrupt the provision of essential services. In amendment of the repealed Council Directive 2008/114/EC, the CER Directive explicitly refers to the drinking water sector as "providers of essential services", thus enforcing the implementation to suppliers and distributors of water intended for human consumption as defined in Directive (EU) 2020/2184 (in article 2, point (1)(a)).

In order to be able to ensure their resilience, critical entities should have a comprehensive understanding of all relevant risks to which they are exposed and analyse those risks. To that aim the Directive foresees the obligation of critical water entities to carry out a risk assessment **within nine months** of receiving a notification of their official declaration as critical entities by the Member State and **at least every four years**, on the basis of Member State risk assessments and other relevant sources of information, in order to assess all relevant risks that could disrupt the provision of their essential services ('critical entity risk assessment'). According to the CER Directive, the critical entity risk assessments shall account for all the relevant natural and man-made risks which could lead to an incident, including terrorist offences as provided for in Directive (EU) 2017/541. The latter, specifically designates as such the act of "*interfering with or disrupting the supply of water […]*". In order to determine the significance of the disruption or the potential disruption to the critical entity's operations resulting from an incident, the following parameters shall, in particular, be taken into account (a) the impacts that incidents could have, in terms of degree and duration, on economic and societal activities, the environment and public safety; (b) the number of users affected; and (c) the geographical area affected.

The CER Directive foresees that critical entities shall take **appropriate and proportionate technical, security and organisational measures** to ensure their resilience, based on the relevant information provided by Member States on the Member State risk assessment and on the outcomes of the critical entity risk assessment, including measures necessary to:

(a) **prevent incidents** from occurring, duly considering disaster risk reduction and climate adaptation measures;
(b) **ensure adequate physical protection** of their premises and critical infrastructure, duly considering, for example, fencing, barriers, perimeter monitoring tools and routines, detection equipment and access controls;

(c) **respond to, resist and mitigate the consequences of incidents**, duly considering the implementation of risk and crisis management procedures and protocols and alert routines;

(d) **recover from incidents**, duly considering business continuity measures and the identification of alternative supply chains, in order to resume the provision of the essential service;

(e) **ensure adequate employee security management**, duly considering measures such as setting out categories of personnel who exercise critical functions, establishing access rights to premises, critical infrastructure and sensitive information, setting up procedures for background checks in accordance with Article 14 and designating the categories of persons who are required to undergo such background checks, and laying down appropriate training requirements and qualifications;

(f) **raise awareness** about the measures referred to in points (a) to (e) among relevant personnel, duly **considering training courses, information materials and exercises**.

Although critical entities should take measures on all points specified in this Directive, the details and extent of the measures should reflect the different risks that each entity has identified as part of its risk assessment and the specificities of such entity in an appropriate and proportionate way. In the interest of effectiveness and accountability, critical entities should describe those measures, with a level of detail to sufficiently achieve those aims, having regard to the risks identified, in a resilience plan or in a document or documents that are equivalent to a resilience plan, and apply that plan in practice. Subsequently, the competent authority may declare existing or foreseen resilience-enhancing measures taken by a critical entity that address the technical, security and organisational measures as compliant, in whole or in part, with the obligations under this Directive or, where necessary, issue orders for remedy, refinement or adjustments to meet the criteria.

To promote its convergent implementation, the Directive encourages the use of European and international standards and technical specifications relevant to the security and resilience measures applicable to critical entities. A relevant European Standard for the water sector is the EN 15975-2 Standard Security of drinking water supply – Guidelines for risk and crisis management[5], that covers in detail fundamentals of crisis management, including relevant recommendations for drinking water suppliers, incorporates fundamental elements of the WHO Water Safety Plan approach and supports water suppliers to actively address safety issues in the context of routine water supply management and operations. The EN 15975-2 standard describes the principles of a risk management approach to improve/support the integrity of the drinking water supply system, with the key guidelines being:

1. In preparing to undertake a risk assessment of the drinking water supply system, **the drinking water supplier will need to create a framework and set of rules for the task**. It is important to **clearly define the risk assessment criteria** and to ensure that these are consulted widely upon within the organisation and are endorsed by the responsible managers in the organisation.
2. Risk analysis requires the **interdisciplinary group to work systematically through the list of identified hazards and corresponding hazardous events**. The interdisciplinary group should **estimate the likelihood** of each hazardous event occurring **and the severity of consequences** of the resulting hazard.

[5] CEN members are bound to comply with the CEN/CENELEC internal regulations which stipulate the conditions for giving this European standard the status of a national standard without any alteration.

3. The purpose of risk analysis is to **score each risk** individually **and facilitate efficient comparison** of different types of risk **to support** decision making in the **allocation of scarce resources**.
4. Risk analysis should initially **consider the severity of consequences and the likelihood** that would exist **in the absence of risk control measures** (or following their failure). Risk analysis should subsequently consider severity of consequences and likelihood with current risk control measures in place.
5. To ensure consistency, the drinking water supplier should **develop its own tables, defining appropriate terms and ranges for likelihood and severity of consequences**. These terms and ranges will assist in scoring individual risks and positioning them on the chosen risk assessment matrix.
6. **Caution should be exercised when using a quantitative** or semi-quantitative **approach**. Their apparently precise values **can imply a false sense of accuracy although uncertainty may exist**.
7. The purpose of **risk evaluation is to compare and prioritise risks** regarding their estimated effect **on the drinking water supply system's integrity** and to make decisions about the need for amended or additional risk control measures. […] **the drinking water supplier should** aim to **eliminate or**, where elimination is impracticable, to **lower as far as reasonably practicable the likelihood of hazardous events and/or the hazard's severity of consequences** causing this risk.
8. **Risk control** measures applied **may be preventive or reactive** to mitigate the risks. **Some existing control** measures identified in risk analysis and risk evaluation **may require improvement**. For risks with no current risk control measures in place, they may need to be established.
9. In cases where no risk control measures are reasonably practicable or key control measures fail, **crisis management should exist as a final control measure** to ensure an effective and efficient response and recovery from this situation.
10. Validation is concerned with **actively obtaining evidence that existing or new measures are suitable to control a specific risk and perform effectively under a range of conditions**. Complementary steps may be applied for risk control measure validation purposes, e.g.: evaluation of comparable long-term data sets collected under expected operating conditions; evaluation of critical operating conditions (e.g., **by simulating hazardous event scenarios**).

One more important remark stemming from the EN 15975-2 Standard is the provision for water utilities to document and archive the outcomes of the analysis so that those conducting the risk management approach have access to suitable guidance and all decisions and assumptions taken in the risk management approach are transparent, traceable and thus revisable. Practicality in the evaluation and review of compliance is also a fundamental aspect of robust risk management approaches.

It should be noted that the EN 15975-2 standard is tightly connected to the recast EU Drinking Water Directive 2020/2184 on the quality of water intended for human consumption, which maintains the reference to that standard as core element of risk-based approaches. Those should be applied by all water suppliers, including small water suppliers, as the evaluation of Directive 98/83/EC showed deficiencies in its implementation. The revised Directive instructs water utilities to also take into account security risks when applying the risk-based approach.

5 Best practices for cybersecurity

This section builds on the existing content of the PROCRUSTES RRKB and the Cybersecurity Handbook[6] developed by The National Cyber Security Authority Of Greece – Ministry Of Digital Governance - Directorate For Cyber Security Strategic Planning - Department For Requirements And Security Architecture. One of the fundamental elements of cybersecurity is the architecture adopted by the water utility in regard to their network and information system, defining its features at both internal and external level.

One such cybersecurity model referenced within the Cybersecurity Handbook is that of Zero, which challenges the "traditional" perimeter-based security model, which assumes that everything within the organization's network can be trusted. Instead, Zero Trust assumes that no user or device should be automatically trusted, regardless of their location or whether they are inside or outside the network perimeter. It emphasizes strict access controls, continuous monitoring, and verification of trustworthiness for every user, device, and transaction.

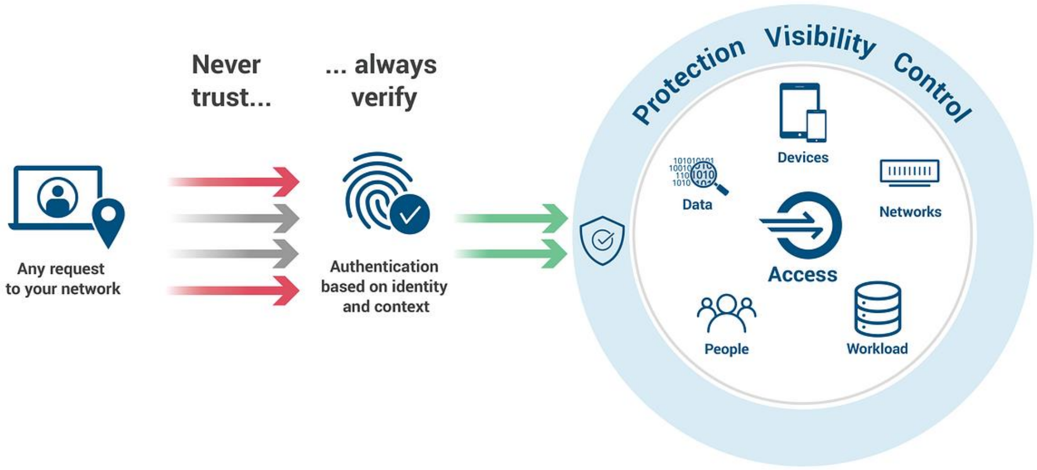


Figure 40 Schematic oF Zero Trust model (source: https://tales-from-a-security-professional.com)

In particular, the fundamental principles of the model are "Never trust, always verify" and "Assume breach". This leads to a set of key principles and components of a Zero Trust architecture, that are:

Identity and Access Management (IAM): Zero Trust relies on strong identity verification and access controls. Users and devices must authenticate and prove their identities before accessing resources. This includes multifactor authentication (MFA), device attestation, and contextual factors like user behavior analysis.

Micro-Segmentation: Zero Trust advocates for segmenting the network into smaller, isolated segments or micro-perimeters. Each segment has its own access controls, and traffic between segments is closely monitored. This helps contain potential breaches and limits lateral movement within the network.

[6] Accessible through: https://mindigital.gr/cybersecurity_handbook.pdf

Network Visibility and Analytics: Zero Trust emphasizes continuous monitoring and analysis of network traffic, user behavior, and security events. Advanced technologies like network traffic analysis (NTA), user and entity behavior analytics (UEBA), and security information and event management (SIEM) systems are used to detect anomalies, identify potential threats, and respond promptly.

Least Privilege: The principle of least privilege is central to Zero Trust. Users and devices are only granted the minimum level of access necessary to perform their tasks. Access privileges are continuously evaluated and adjusted based on contextual information and ongoing risk assessments.

Secure Access Controls: Zero Trust employs fine-grained access controls based on various factors such as user roles, device health, location, and behavior. Dynamic access policies are enforced and can be adjusted based on real-time risk assessments.

Data Encryption: Zero Trust promotes the use of encryption for data protection, both in transit and at rest. Encryption ensures that even if unauthorized access occurs, the data remains unreadable and unusable.

Continuous Authentication and Authorization: Zero Trust requires ongoing authentication and authorization checks throughout a user's session. Continuous monitoring of user behavior, device posture, and other contextual factors helps identify suspicious activities and triggers additional authentication or access revocation when necessary.

Zero Trust for External Networks: Zero Trust extends its principles to external networks and connections, such as remote workers, cloud services, and third-party partnerships. It enforces consistent access controls and security measures regardless of the network or location, treating external connections with the same scrutiny as internal ones.

The Zero Trust architecture promotes a shift from the traditional perimeter-centric approach to a more dynamic, risk-based model. By assuming that no user or device should be trusted by default, it reduces the attack surface, improves security posture, and enhances protection against both internal and external threats.

Another cybersecurity model architecture is that of “defense-in-depth”, which leverages multiple levels of security and measures to protect an organization's assets against cyber threats. The controls can be taxonomised at high level into 3 layers, i.e., physical, technical and administrative, as seen in Figure 41. Physical controls involve measures that are implemented to protect the physical infrastructure and assets of an organization. These controls focus on securing the tangible elements of the system, such as buildings, data centers, sensors, control and data transmission equipment, and physical access points. Examples of physical controls include perimeter fencing, locks, surveillance systems, biometric authentication, access card systems, and security guards. Physical controls aim to prevent unauthorized physical access and protect against theft, vandalism, or tampering with physical assets. On the other side, technical refer to the security measures that are implemented within the information technology (IT) systems and networks. These controls are designed to protect the digital aspects of an organization, including hardware, software, data, and communications and encompass various technologies, configurations, and processes aimed at securing the IT infrastructure. The administrative controls layer, overarches the system cybersecurity through the encompassed policies, procedures, and guidelines that govern the overall security posture of an organization. These controls are focused on the human and administrative aspects of security, including management, awareness, training, and governance. Administrative controls involve defining security policies, conducting risk assessments, implementing security awareness training for employees, enforcing access controls and password policies, performing regular audits and compliance checks, and establishing incident response and business continuity plans. Administrative controls help ensure that security measures are properly implemented, maintained, and adhered to throughout the organization.

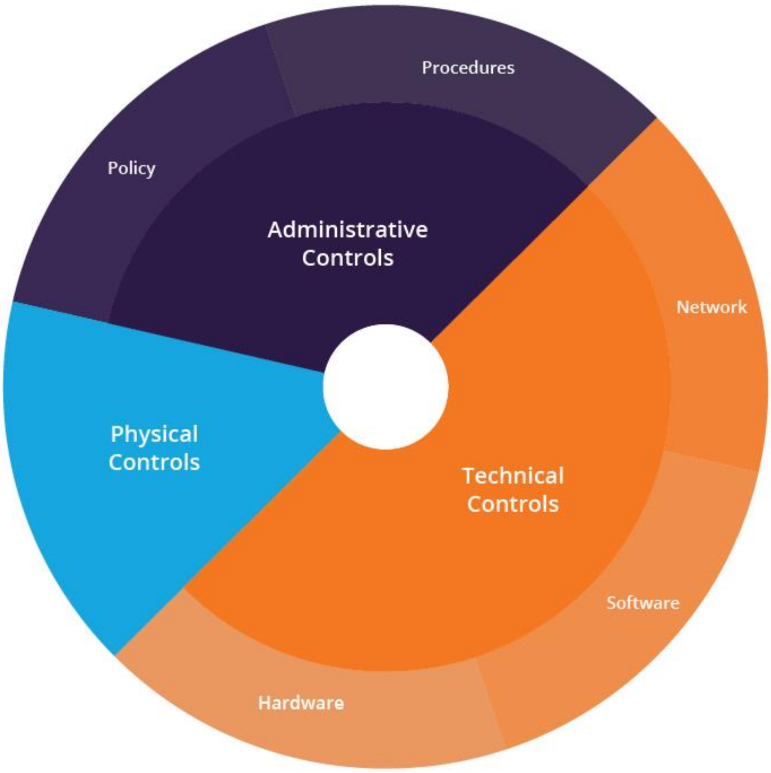


Figure 41 Defense-in-depth schematic (source: https://www.imperva.com/)

By combining physical controls, technical controls (including hardware, software, and network controls), and administrative controls, organizations can establish a comprehensive defense-in-depth strategy that addresses security risks from multiple angles, thereby increasing the overall resilience of their cybersecurity posture. This taxonomy can also be found within RKKB measures (for more information please see D4.2) that provides an ensemble of measures and best practices for cyber-physical water systems, and resemble the set of minimum measures to be applied across Europe’s entities, as instructed by the NIS2 Directive. More specifically it integrates measures and practices to achieve, as per NIS2:

Top management commitment & accountability: This measure emphasizes the importance of senior management's commitment to cybersecurity. It involves establishing a culture of security within the organization, allocating appropriate resources for security initiatives, and ensuring accountability for cyber risks at the highest level.

Network & information security policy: A network and information security policy sets out the organization's guidelines, rules, and procedures for securing its network infrastructure and information assets. It outlines the expectations for security controls, user responsibilities, incident response, and compliance with relevant regulations.

Risk management policy: A risk management policy defines the organization's approach to identifying, assessing, and managing cyber risks. It involves conducting risk assessments, implementing risk mitigation measures, and establishing processes for ongoing risk monitoring and review.

Asset management: Asset management involves identifying and categorizing an organization's information assets, such as hardware, software, and data. It includes processes for asset inventory, classification, ownership, and protection throughout their lifecycle.

Human resources security: Human resources security focuses on ensuring the appropriate level of security awareness and behavior among employees. It includes measures such as background checks, security training and awareness programs, defining user access privileges, and managing employee departures to prevent insider threats.

Basic cyber hygiene practices & Security training: Basic cyber hygiene practices refer to fundamental security measures that individuals and organizations should follow to protect against common cyber threats. This includes practices such as using strong passwords, regularly updating software, implementing malware protection, and conducting security training to educate employees about security best practices.

Supply chain security: Supply chain security addresses the security risks associated with third-party vendors, suppliers, and partners. It involves assessing the security posture of external entities, establishing security requirements in contracts, and implementing controls to ensure the integrity and security of the supply chain.

Access control: Access control measures involve mechanisms and policies that restrict access to information systems, networks, and data. This includes user authentication, authorization, and access privileges management to ensure that only authorized individuals can access specific resources.

Security in network and information systems acquisition, development & maintenance: This measure focuses on integrating security controls and considerations throughout the lifecycle of network and information systems. It involves implementing secure coding practices, conducting security assessments during development, and performing regular maintenance and updates to address vulnerabilities.

Cryptography: Cryptography involves the use of encryption techniques to protect sensitive information. It ensures the confidentiality, integrity, and authenticity of data by encoding it in a secure manner and making it unreadable to unauthorized parties.

Incident handling: Incident handling encompasses the processes and procedures for detecting, responding to, and mitigating security incidents. It includes incident response planning, incident reporting, containment, eradication, and recovery activities to minimize the impact of cyber incidents.

Business continuity & crisis management: Business continuity and crisis management involve preparing for and responding to disruptive events, including cyber attacks. It includes developing continuity plans, backup and recovery strategies, and incident communication plans to ensure the organization can maintain critical operations and recover effectively from incidents.

Environmental and physical security: Environmental and physical security measures focus on protecting the physical infrastructure and facilities of an organization. This includes implementing safeguards such as access controls, surveillance systems, secure storage, and disaster recovery plans to prevent unauthorized physical access, damage, or loss of assets.

Such measures collectively contribute to a comprehensive cybersecurity and resilience strategic planning, addressing various aspects of security to safeguard a utility’s assets, information, and operations against the emerging cyber-physical threat landscape.

REFERENCES

American Water Works Association, 2010. Risk and Resilience Management of Water and Wastewater Systems. AWWA J100-10 (R13), 1st ed. American Water Works Association,US, Denver, United States.

CEN-EN 15975-2, 2013. Security of drinking water supply — Guidelines for risk and crisis management Part 2 : Risk management.

Cimpanu, C., 2020. Two more cyber-attacks hit Israel's water system [WWW Document]. URL https://www.zdnet.com/article/two-more-cyber-attacks-hit-israels-water-system/

Directive (EU) 2022/2557, 2022a. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.

Directive (EU) 2022/2557, 2022b. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.

ENISA, 2019. ENISA threat landscape report 2018 : 15 top cyberthreats and trends. European Union Agency For Network and Information Security, Heraklion, Greece. https://doi.org/10.2824/622757

European Union Agency for Network and Information Security (ENISA), 2022. ENISA Threat Landscape 2022. Athens, Greece. https://doi.org/10.2824/764318

European Union Agency for Network and Information Security (ENISA), 2020. ENISA Threat Landscape: Emerging trends. Maroussi 151 24, Attiki, Greece. https://doi.org/10.2824/552242

ISO, 2018. ISO 31000 Risk management - Principles and guidelines. Int. Organ. Stand. 34.

Johnson, C.S., Badger, M.L., Waltermire, D.A., Snyder, J., Skorupka, C., 2016. Guide to Cyber Threat Information Sharing. Gaithersburg, MD. https://doi.org/10.6028/NIST.SP.800-150

Koutiva, I., Moraitis, G., Makropoulos, C., 2021. An Agent-Based Modelling approach to assess risk in Cyber-Physical Systems (CPS)., in: Proceedings of the 17th International Conference on Environmental Science and Technology. Athens, Greece. https://doi.org/10.30955/gnc2021.00194

Lee, E.A., 2015. The past, present and future of cyber-physical systems: A focus on models. Sensors (Switzerland) 15, 4837–4869. https://doi.org/10.3390/s150304837

Loukas, G., 2015. Front-matter, in: Cyber-Physical Attacks. Elsevier, Oxford, England, pp. i–iii. https://doi.org/10.1016/B978-0-12-801290-1.00008-4

Lu, Y., 2017. Industry 4 . 0 : A survey on technologies , applications and open research issues. J. Ind. Inf. Integr. 6, 1–10. https://doi.org/https://doi.org/10.1016/j.jii.2017.04.005

Makropoulos, C., Savić, D.A., 2019. Urban hydroinformatics: Past, present and future. Water (Switzerland) 11. https://doi.org/https://doi.org/10.3390/w11101959

Moraitis, G., Nikolopoulos, D., Koutiva, I., Tsoukalas, I., Karavokiros, G., Makropoulos, C., 2021. The PROCRUSTES testbed: tackling cyber-physical risk for water systems, in: EGU General Assembly 2021. https://doi.org/https://doi.org/10.5194/egusphere-egu21-14903

Moraitis, G., Sakki, G.K., Karavokiros, G., Nikolopoulos, D., Tsoukalas, I., Kossieris, P., Makropoulos, C., 2023. Exploring the Cyber-Physical Threat Landscape of Water Systems: A Socio-Technical Modelling Approach. Water (Switzerland) 15. https://doi.org/10.3390/w15091687

Moraitis, G., Tsoukalas, I., Kossieris, P., Nikolopoulos, D., Karavokiros, G., Kalogeras, D., Makropoulos, C., 2022. Assessing Cyber-Physical Threats under Water Demand Uncertainty, in: EWaS5. MDPI, Basel Switzerland, p. 18. https://doi.org/https://doi.org/10.3390/environsciproc2022021018

Nikolopoulos, D., Makropoulos, C., 2023. A novel cyber-physical resilience-based strategy for water quality sensor placement in water distribution networks. Urban Water J. 20, 278–297. https://doi.org/10.1080/1573062X.2023.2174032

Nikolopoulos, D., Moraitis, G., Karavokiros, G., Bouziotas, D., Makropoulos, C., 2022. Stress-Testing Alternative Water Quality Sensor Designs under Cyber-Physical Attack Scenarios, in: EWaS5. MDPI, Basel Switzerland, p. 17. https://doi.org/10.3390/environsciproc2022021017

NIS2, 2022. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (E.

Rajkumar, R. (Raj), Lee, I., Sha, L., Stankovic, J., 2017. Cyber-Physical Systems: The Next Computing Revolution. Cybern. Syst. Anal. 53, 821–834. https://doi.org/10.1007/s10559-017-9984-9

Robles, F., Perlroth, N., 2021. ‘Dangerous Stuff’: Hackers Tried to Poison Water Supply of Florida Town [WWW Document]. New York Times. URL https://www.nytimes.com/2021/02/08/us/oldsmar-florida-water-supply-hack.html

Savić, D., 2021. Digital water developments and lessons learned from automation in the car and aircraft industries. Engineering. https://doi.org/https://doi.org/10.1016/j.eng.2021.05.013

Tsoukalas, I., Kossieris, P., Makropoulos, C., 2020. Simulation of Non-Gaussian Correlated Random Variables, Stochastic Processes and Random Fields: Introducing the anySim R-Package for Environmental Applications and Beyond. Water 12, 1645. https://doi.org/10.3390/w12061645

Tsoukalas, I., Makropoulos, C., Koutsoyiannis, D., 2018. Simulation of stochastic processes exhibiting any-range dependence and arbitrary marginal distributions. Water Resour. Res. https://doi.org/10.1029/2017WR022462

Verizon, 2016. Data breach digest. Scenarios from the field.

Water Sector Coordinating Council (WSCC), 2021. Water and Wastewater Systems Cybersecurity 2021 State of the Sector.

APPENDIX A

Quick intro to EPANET 2.2

EPANET is a model/solver engine for extended period simulation of hydraulic and water quality behaviour within pressurized pipe networks. A network consists of pipes, nodes (pipe junctions), pumps, valves and storage tanks or reservoirs. EPANET tracks the flow of water in each pipe, the pressure at each node, the height of water in each tank, and the concentration of a chemical species throughout the network during a simulation period comprised of multiple time steps.

Full-featured and accurate hydraulic modelling is a prerequisite. EPANET contains a state-of-the-art hydraulic analysis engine that includes the following capabilities:

- Places no limit on the size of the network that can be analysed.
- Computes friction headloss using the Hazen-Williams, Darcy-Weisbach, or Chezy-Manning formulas.
- Includes minor head losses for bends, fittings, etc.
- Models constant or variable speed pumps.
- Computes pumping energy and cost.
- Models various types of valves including shutoff, check, pressure regulating, and flow control valves.
- Allows storage tanks to have any shape (i.e., diameter can vary with height).
- Considers multiple demand categories at nodes, each with its own pattern of time variation.
- Models pressure driven flow issuing from emitters (sprinkler heads).
- Models pressure driven demand at nodes.
- Can base system operation on both simple tank level or timer controls and on complex rule-based controls.

The .inp file is a text-based input file used by EPANET to define the characteristics and parameters of a water distribution system model. It serves as the primary means of communicating the network configuration, hydraulic properties, demands, controls, and other relevant information to EPANET. A set of key components and sections typically found in an EPANET .inp file can be seen below:

1. [TITLE]: The first line of the .inp file typically contains a title or description of the model, providing information about the purpose or nature of the simulation.
2. [JUNCTIONS]: This section defines the junctions or nodes in the network. Each junction is specified with a unique ID, along with its coordinates, elevation, and demand information. Additional attributes such as the pattern or category of demand may also be included.
3. [RESERVOIRS]: Reservoirs or water treatment plants are defined in this section. Similar to junctions, each reservoir is assigned a unique ID, and its coordinates, elevation, and other relevant properties are specified.
4. [TANKS]: If the model includes storage tanks, this section provides details about each tank, including its ID, coordinates, initial water level, tank size, and other related attributes.
5. [PIPES]: The pipes section defines the pipes connecting the junctions. Each pipe is identified with a unique ID and is specified with its start and end junction IDs, length, diameter, roughness coefficient, and other properties.

6. [PUMPS]: This section is used to define pumps in the system. Pump objects are specified with their unique ID, start and end junction IDs between which the pump is located, and the pumping curve characteristics.
7. [VALVES]: Valves, such as control valves or check valves, are defined in this section. Each valve is assigned a unique ID, and its type (e.g., PRV), the relevant properties and settings, and the start and end junction IDs between which the valve is located.
8. [DEMANDS]: This section provides information about the demands at each junction. The demand data can be entered directly or referenced from demand patterns defined in a separate section.
9. [PATTERNS]: Demand patterns, which represent the variation of demand over time, are defined in this section. Patterns can be assigned to individual junctions or used in the [DEMANDS] section to specify varying demands.
10. [CONTROLS]: This section provides the system's control rules, such as time-based controls or setpoint-based controls, defined through statements that link sensing and associated automated remote actions.

The above sections provide a general overview of the structure and contents of an EPANET .inp file. Depending on the complexity of the water distribution system and the desired analysis, additional sections and options may be included to further define the model properties, simulations, reporting options, and more. The order of sections is not important. However, whenever a node or link is referred to in a section, e.g., in the system controls, it must have already been defined in the [JUNCTIONS], [RESERVOIRS], [TANKS], [PIPES], [PUMPS], or [VALVES] sections. Therefore, it is recommended that these sections be placed first, right after the [TITLE] section. The .inp file can be edited using a text editor or generated by external tools that integrate with EPANET, facilitating the creation and modification of EPANET models.

APPENDIX B

It should be noted that both NIS2 and the CER Directive also foresee that critical entities notify without undue delay the competent authority of incidents that significantly disrupt or have the potential to significantly disrupt their operations. Notifications shall include any available information necessary to enable the competent authority to understand the nature, cause, and possible consequences of the incident, including so as to determine any cross-border impact of the incident. Such notification shall not make the critical entities subject to increased liability. An example of such a reporting template can be found in this Appendix , and refers to the template of Security Incident Report, as defined by the National Cybersecurity Authority of Greece[7].

[7] Greek water utilities may also directly report to the Hellenic CSIRT (Link: https://csirt.cd.mil.gr/incident-report/).

Security Incident Report, National Cybersecurity Authority of Greece

ΕΘΝΙΚΗ ΑΡΧΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

NATIONAL CYBERSECURITY AUTHORITY of Greece

Αναφορά Συμβάντος Ασφάλειας

Είδος αναφοράς	Επιλέξτε ένα στοιχείο.	Επιλέξτε ένα στοιχείο.
Ημερομηνία	Κάντε κλικ ή πατήστε για να εισαγάγετε ημερομηνία.	

Πληροφορίες Επικοινωνίας			
Στοιχεία Οργανισμού			
Όνομα			
Τηλέφωνο			
Διεύθυνση			
Διεύθυνση E-mail			
Στοιχεία Υπεύθυνου Ασφαλείας Πληροφοριών και Δικτύων		**Στοιχεία Νόμιμου Εκπροσώπου**	
Ονοματεπώνυμο			
Θέση/ Τίτλος			
Τηλέφωνο			
Διεύθυνση E-mail			
Διαθεσιμότητα			
Γενικές Πληροφορίες			
Είδος υπηρεσίας που επηρεάστηκε			
Κατηγορία οργανισμού	☐ **Φ.Ε.Β.Υ.**	☐ **Π.Ψ.Υ.**	☐ **Άλλο**
Τομέας που επηρεάστηκε	Επιλέξτε ένα	Επιλέξτε ένα	*Επεξήγηση*
Υπο-τομέας	Επιλέξτε ένα		
Υπηρεσία που επηρεάστηκε			

Αντίκτυπος Περιστατικού	
Παραβίαση αρχών ασφάλειας πληροφοριών	☐ Εμπιστευτικότητα ☐ Ακεραιότητα ☐ Διαθεσιμότητα
Πλήθος επηρεασμένων χρηστών	
Έκταση διατάραξης της λειτουργίας / Διάρκεια μη διαθεσιμότητας της υπηρεσίας	
Γεωγραφική έκταση	
Πόροι που επηρεάστηκαν	
Εξαρτώμενες οντότητες	
Έκταση επιπτώσεων σε κοινωνικές/ οικονομικές δραστηριότητες	
Εκτιμώμενη Ζημία	
Υλικές ζημιές	
Επιπτώσεις φήμης	
Επιπτώσεις στην Υγεία, τη δημόσια ασφάλεια & προστασία/ πιθανές ανθρώπινες απώλειες	
Απώλεια/ Παραβίαση Δεδομένων	
Τύπος δεδομένων που τέθηκαν σε κίνδυνο	☐ Δημόσια ☐ Προσωπικά ☐ Ευαίσθητα ☐ Απόρρητα ☐ Άγνωστο
Διασυνοριακός αντίκτυπος	
Σύντομη Περιγραφή	Επιλέξτε ένα στοιχείο.

Αναλυτική Περιγραφή Περιστατικού				
Χρόνος συμβάντος	Ημερομηνία	Κάντε κλικ ή	Ώ	--:--:--
Χρόνος εντοπισμού	Ημερομηνία	Κάντε κλικ ή	Ώ	--:--:--
Διάρκεια				
Αναλυτικά αίτια περιστατικού				
Αναλυτικά στοιχεία πόρων που επηρεάστηκαν				

Τρέχουσα Κατάσταση

Μετριασμός επιπτώσεων	
Κατάσταση περιστατικού	Επιλέξτε ένα στοιχείο.
Ενέργειες που έχουν ληφθεί για τον μετριασμό/ περιορισμό του αντικτύπου του περιστατικού	
Επίπεδο μετριασμού επιπτώσεων	
Ενεργοποίηση BCP/ DRPs	☐ **Ναι** ☐ **Όχι**
Κατάσταση σχεδίου	
Προγραμματισμένες ενέργειες	
Χρόνος αποκατάστασης	
Ανάγκη ενίσχυσης από CSIRT	☐ **Ναι** ☐ **Όχι**
Ανάγκη ενίσχυσης από άλλες Αρχές	
Σημειώσεις	
Ενημέρωση Εμπλεκομένων	
Χρήστες που επηρεάστηκαν	
Αρμόδιες (Εθνικές) Αρχές	
Διασυνοριακή ενημέρωση	
Ενημέρωση κοινού	

Η επόμενη μέρα	
Συμπεράσματα	
Κύρια αίτια	
Προκλήσεις	
Προτάσεις	
Μακροπρόθεσμα μέτρα ασφάλειας	