


Article

Protection of Water Distribution Networks against Cyber and Physical Threats: The STOP-IT Approach Demonstrated in a Case Study

Camillo Bosco ^{1,*}, Gema Sakti Raspati ¹, Kebebe Tefera ², Harald Rishovd ² and Rita Ugarelli ¹¹ SINTEF Community, Group Water and Environment, S.P. Andersens vei 3, 7465 Trondheim, Norway² Agency for Water and Wastewater Services, Herslebs Gate 5, 0561 Oslo, Norway

* Correspondence: camillo.bosco@sintef.no

Abstract: Water critical infrastructures are undergoing a process of digital transformation that entails an increasing integration between the physical and cyber layers of the system. This integration brings efficiency and monitoring advantages, but it also exposes water systems to a new threat surface that includes cyberattacks. Formed in 2017, STOP-IT is Europe's first project dedicated to developing cyber-physical security solutions tailored to the water sector. During the 4 years of collaboration, the STOP-IT team has codeveloped an extensive list of technologies that integrates cyber and physical layers of infrastructure, allowing water utilities to prevent, detect, assess, and treat risks, as well as simulate scenarios of attacks and explore how to react to increase preparedness. This article first introduces the overall aim and main outcomes of the STOP-IT project and then focuses on the risk management integrated framework composed of modeling solutions developed to help water utilities identify vulnerabilities and protect critical parts of their systems. The solutions are presented along with the results from the demonstration activities performed by a selected water utility concerning three risk scenarios that were assessed through the mentioned integrated framework.

Keywords: critical infrastructure protection; cyber-physical systems; cyber-physical attacks; digitalization; risk management; water systems and services



Citation: Bosco, C.; Raspati, G.S.; Tefera, K.; Rishovd, H.; Ugarelli, R. Protection of Water Distribution Networks against Cyber and Physical Threats: The STOP-IT Approach Demonstrated in a Case Study. *Water* **2022**, *14*, 3895. <https://doi.org/10.3390/w14233895>

Academic Editors: Rita Salgado Brito and Helena Alegre

Received: 24 October 2022

Accepted: 25 November 2022

Published: 30 November 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Managing urban water systems is challenged by several factors, such as infrastructure deterioration, large water losses, and increasing pressures on water resources with respect to both quantity and quality [1–4]. These factors are exacerbated by global pressures, such as demographic growth, increased water stress, urban development and migration to urban areas, and climate change impacts [5,6]. In addition to this, stringent regulations for quality, security, and the environment are enforced. These change drivers place pressure on the need for a paradigm shift from traditional management of the water sector, grounded in the process of digital transformation [7–11].

However, in the water sector, the process of digitalization is slower compared to other critical infrastructure sectors, and this is also due to a list of security challenges limiting the modernization of the sector [12].

Although safety has been a high priority in the water sector for years and cybersecurity is becoming of greater concern, measures and approaches that consider a global integrated security context, physical and cyber, are still missing, therefore leading to the inability to cope with combined cyber-physical attacks, which are of major concern [13,14].

Furthermore, the water sector lacks collective situational awareness of cyber threats [15]. This is because water utilities and associated information technology (IT) service providers do not systematically share information on experienced cyberattack events that could help to further assess the state of cybersecurity in the water sector and increase preparedness and the ability to protect the service.

Developing proper prevention and response strategies requires not only implementing technical security measures but also establishing a cybersecurity culture through competence building, awareness creation, and communication. There is currently a gap in digital knowledge in general and specifically in cybersecurity in the water sector. The knowledge gaps are both potential sources of risks and barriers to the process of digitalization. With these challenges in mind, STOP-IT (<https://stop-it-project.eu/>, 24 November 2022) has worked in multiple directions to contribute to increasing the protection of water critical infrastructure: on one side, effort has been made to increase awareness and competence among operators, and on the other side, to provide flexible and adaptable modular solutions.

From a technological point of view, the ultimate outcome of STOP-IT is the STOP-IT platform, which integrates 28 solutions that can be applied standalone but also in combination, thanks to the established interoperability between the different components. The platform was validated in an operational environment, and all solutions have been demonstrated in real environments; thus, all solutions have reached at least technology readiness level 7.

The STOP-IT platform is structured into nine technological modules clustering the 28 technological solutions and analysis tools, which can be further distinguished into strategic/tactical tools and operational tools:

- Strategic and tactical tools are analysis tools developed to support risk managers and decision-makers in increasing preparedness against the impact of cyber-physical threats on the service to be provided. They allow to generate customized scenarios of attack, assess their associated risk in terms of service disruption, and compute the effectiveness of risk reduction measures to increase the system's resilience.
- Operational tools support the near real-time or real-time operation of the cyber-physical integrated system by providing an extensive list of technologies to detect anomalies of different nature, such as jamming attacks, IT and physical intrusions, abnormal behaviors, and loss of data availability and integrity.

The paper focuses on the presentation of the strategic tactical tools of STOP-IT through their adoption and demonstration to protect a water distribution system.

The tools and methods presented have been developed in STOP-IT to increase preparedness against cyber-physical threats; however, their application can be extended to any kind of threats affecting operational functions to support water utilities in performing scenario-based risk assessment and provide valuable inputs to strategic asset management plans. The paper is structured in sections. First, the methods are presented, including a description of the selected software tools, the considered risk scenarios, as well as general information on the adopted simulation model. Secondly, results from the different selected tools are presented, with emphasis on the steps to be undertaken by the tools' users. Finally, simulation results are discussed, pointing out how the adopted methods can support water utilities in managing cyber-physical threats, including future perspectives and main conclusions.

2. Materials and Methods

The study made use of the strategic and tactical solution developed within STOP-IT: Risk Analysis and Evaluation Toolkit (RAET) [16]. RAET is a holistic, integrated platform that aims to support water utilities in managing cyber-physical risks for their critical systems and services, reinforcing resilience [17,18] in the water sector. The platform builds on the risk management process described by ISO 31000:2009/2018 [19] (following the steps of risk identification, analysis, evaluation, and treatment) and adapts its steps and methodologies to serve the needs and security scopes of cyber-physical security. RAET integrates the following tools:

- Asset Vulnerability Assessment Tool (AVAT) to show the criticality of each element in the water network, using vulnerability metrics such as the Link Criticality Index, defined as the number of disconnected nodes resulting from an element outage [20]. This tool helps to handle the complexity of water distribution networks, in which it

might be difficult to gain knowledge on the location of certain vulnerable components. AVAT can score the system vulnerability for different configurations of the network, providing a ranking of pipes based on the potential impact on the system that every single pipe would have if its failure occurred.

- Scenario Planner (SP) to assist the user in creating the scenarios of attack, in launching single simulations, and in visualizing the results. The user can create scenarios by utilizing the Risk Identification Database (RIDB) (in which potential generic risk events can be selected) and the designed STOP-IT fault trees (FTs) (to navigate along potential paths of the identified risk through the so-called gate events) [16]. The simulations are enabled by the selection of specific tools that consider the water distribution system as a cyber-physical integrated model and provide quality and quantity impacts on the considered system due to physical cyber threats. Detailed results can be visualized within the integrated KPI tool (key performance indicator tool).
- Risk Reduction Measures Database (RRMD) [21] with advanced capabilities to facilitate the identification and selection of appropriate risk reduction measures (RRMs). The RRMD has a direct connection to the RIDB through semantic mapping between each other. It is implemented within the STOP-IT risk management process to help the selection and effectiveness assessment of RRMs in increasing the system's performance under a given scenario of attack.
- Stress Testing Platform (STP) [22] to handle multiple simulations that couple the cyber layer (consisting of the interconnections amongst the IT devices) with the hydraulic model of the considered network. STP allows to simultaneously explore the impact of a certain type of scenario under multiple input configurations.

The combination of the mentioned tools in a unique software environment effectively supports the user in performing a structured proper risk management procedure against cyber-physical threats. The logical interconnections amongst the different tools within RAET are illustrated in Figure 1.

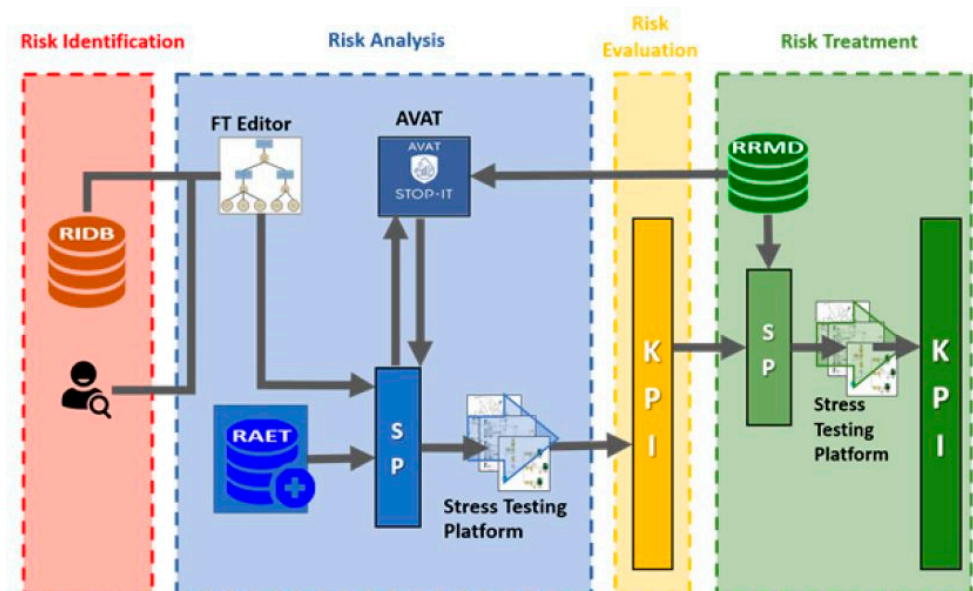


Figure 1. Logical interconnections amongst the different tools within RAET [16].

Since risk scenarios of pressure deficiency conditions were considered for the case study, RISKNOUGHT [23] was adopted in both applications of SP and STP as a tool to integrate, at each simulation step, the solution of a pressure-driven hydraulic model based on EPANET [24] with the information flow of the cyber layer, e.g., from sensors to SCADA (supervisory control and data acquisition) and PLCs (programmable logic controllers) to actuators along the physical system. The platform allows to analyze, for example, the effects of introducing malware to the supervisory system and tracing these effects on the water

distribution network through Key Performance Indicators. RAET was deployed by a water utility partner of the project with the aim of exploring the conditions of a water distribution network that can generate unsupplied demands for customers and for firefighting.

Based on the particular interest of the involved water utility toward certain cyber and physical threats, the following risk events were selected within the detailed scenario-based risk assessment:

- *Manipulation of the tanks' level sensors due to either cyber or physical attacks.* The operations of pumps and valves of the system are often controlled by the level of the tanks. If the sensor's readings fail to provide the correct tank levels, the connected pump and/or valve could fail in allowing the supply of the water demand in the case of normal operations and/or firefighting.
- *Critical pipe failure as a result of an intentional physical attack.* The event takes into account the failure of one critical pipe of the system undetected by the operator. The related consequences might propagate toward the served area in terms of potential pressure deficiencies, which can lead to unsupplied demands, especially when coupled with the manipulation of a tank level sensor.

Based on the two mentioned risk events, the considered three risk scenarios built with the Scenario Planner (RIDB and FT) are described in Table 1.

Table 1. Summary of risk scenarios (RSs) selected by the water utility for the RAET demonstration.

Name	Description
RS 1	Cyber-physical caused manipulation of control system affecting water tanks
RS 2	Combination of RS 1 and physical caused destruction of water tank or pipeline
RS 3	Manipulation of level sensor in water tank used for firefighting

The three risk scenarios shown in Table 1 are *what-if* scenarios, usually adopted for a planning phase, and their customization for the specific water system and the following impact assessment can be performed through RAET.

The risk scenarios (RSs) described above have been used by a water utility to test RAET and were performed by adopting an available hydraulic model related to a selected part of the water distribution system serving 92,877 inhabitants for a total pipe length of 251 km. EPANET 2.2 was the adopted computational engine for the simulation of the hydraulic model with 5482 pipes and 5223 nodes. A water treatment plant (WTP) is connected to three tanks used to distribute drinking water to the supplied areas, connected to each other based on their elevation and actual use. A schematic representation of the connections between the WTP, tanks, and supplied areas is depicted in Figure 2.

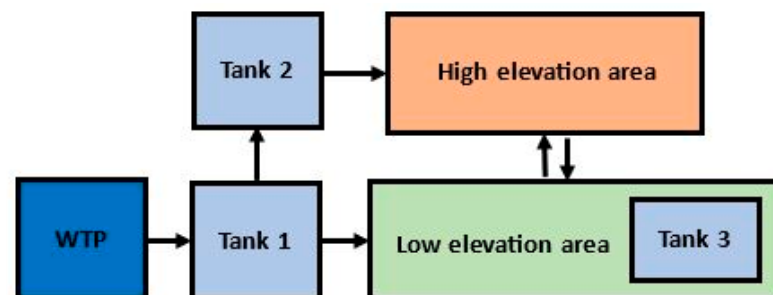


Figure 2. Schematic representation of the connections between main components in the considered system.

The assessment of the risk scenarios was possible through the application of the different modules nested in RAET, which links interdisciplinary approaches into a seamless workflow in order to synthesize actionable intelligence and support informed decision-making in an interactive mode.

3. Results

Starting from the fault trees, which propose a list of risk events with assigned IDs, the event gate 235, “external person in situ manipulates WDN tank level sensor” [16], was selected. To simulate a scenario of attack, firstly, it was necessary to create a baseline scenario, called *business as usual* (BaU) scenario, in which no attacks are considered. For quantity simulations, such as the ones chosen by the water utility to estimate unsupplied demand under the considered attack, RISKNOUGHT requires only an EPANET file as input, so an extended period simulation (EPS) of the BaU scenario was successfully run through the Scenario Planner. Then, the scenario of attack was created by combining the BaU scenario with the event gate 235, selected from the user interface. For the considered gate event, one of the three tanks of the network had to be selected, namely:

- tank 1: the main tank of the network, directly connected upstream to the water source and downstream to all the distribution network and to tank 2;
- tank 2: the tank that supports the supply of tank 1 for more peripheral and elevated areas;
- tank 3: the tank used mainly as storage for firefighting in a zone with high demand.

Since the objective of the assessment of RS 1 was to identify areas with unsupplied demands in case of level readings manipulation, tank 2 was selected to discover the extension of the zones strictly dependent on it. After the selection of the tank, three parameters had to be defined, namely the duration of the attack, the start time of the attack, and the manipulated value of the sensor readings. For the demonstration, the duration of the attack was set to 5 h, the start time to 5 a.m., and the manipulated value to 10 m (i.e., the maximum level of tank 2, which leads the pump connecting tank 1 to tank 2 to remain inactive). The selection of the risk event from the Scenario Planner is shown in Figure 3, while different types of impacts of sensor manipulation are depicted in Figure 4.

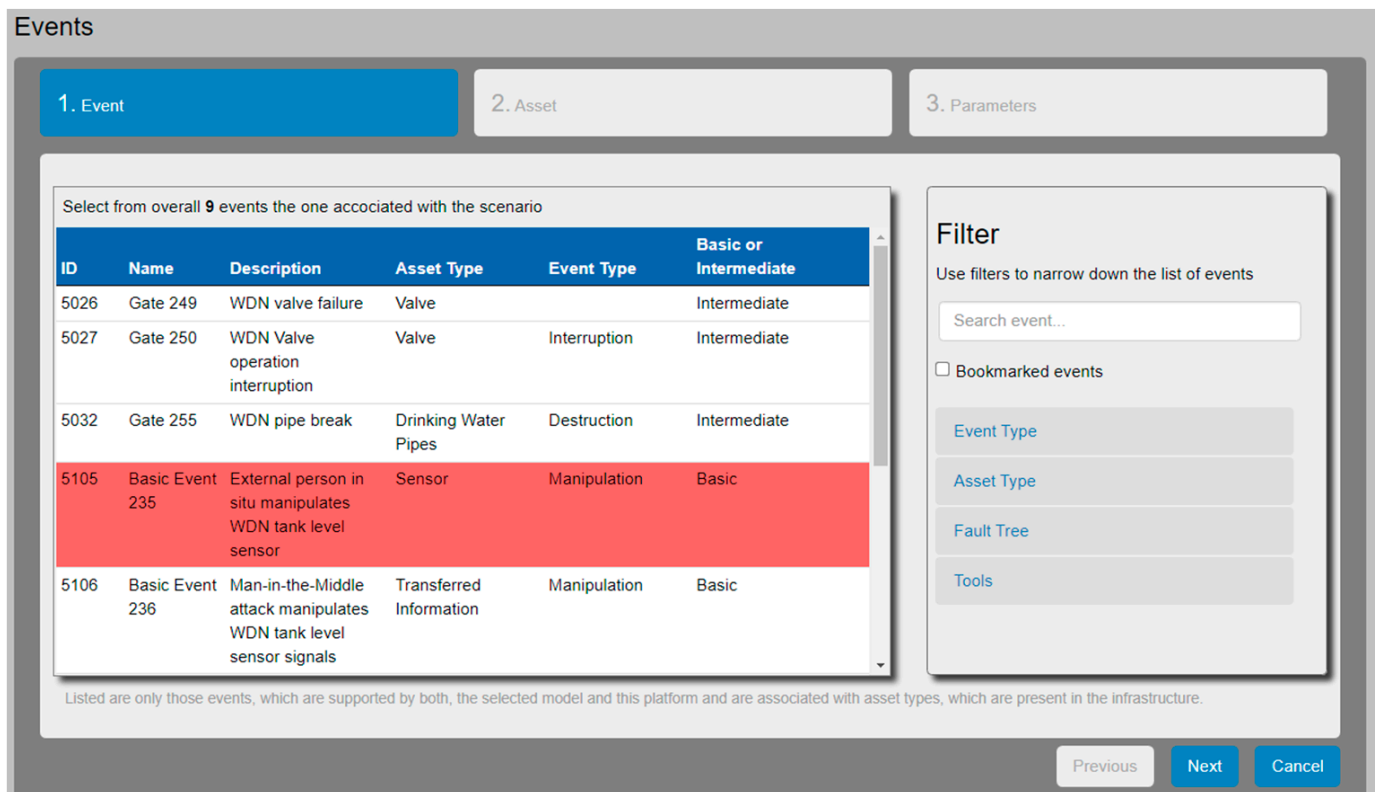


Figure 3. Selection of the risk event of RS 1 proposed by the fault tree within the Scenario Planner.

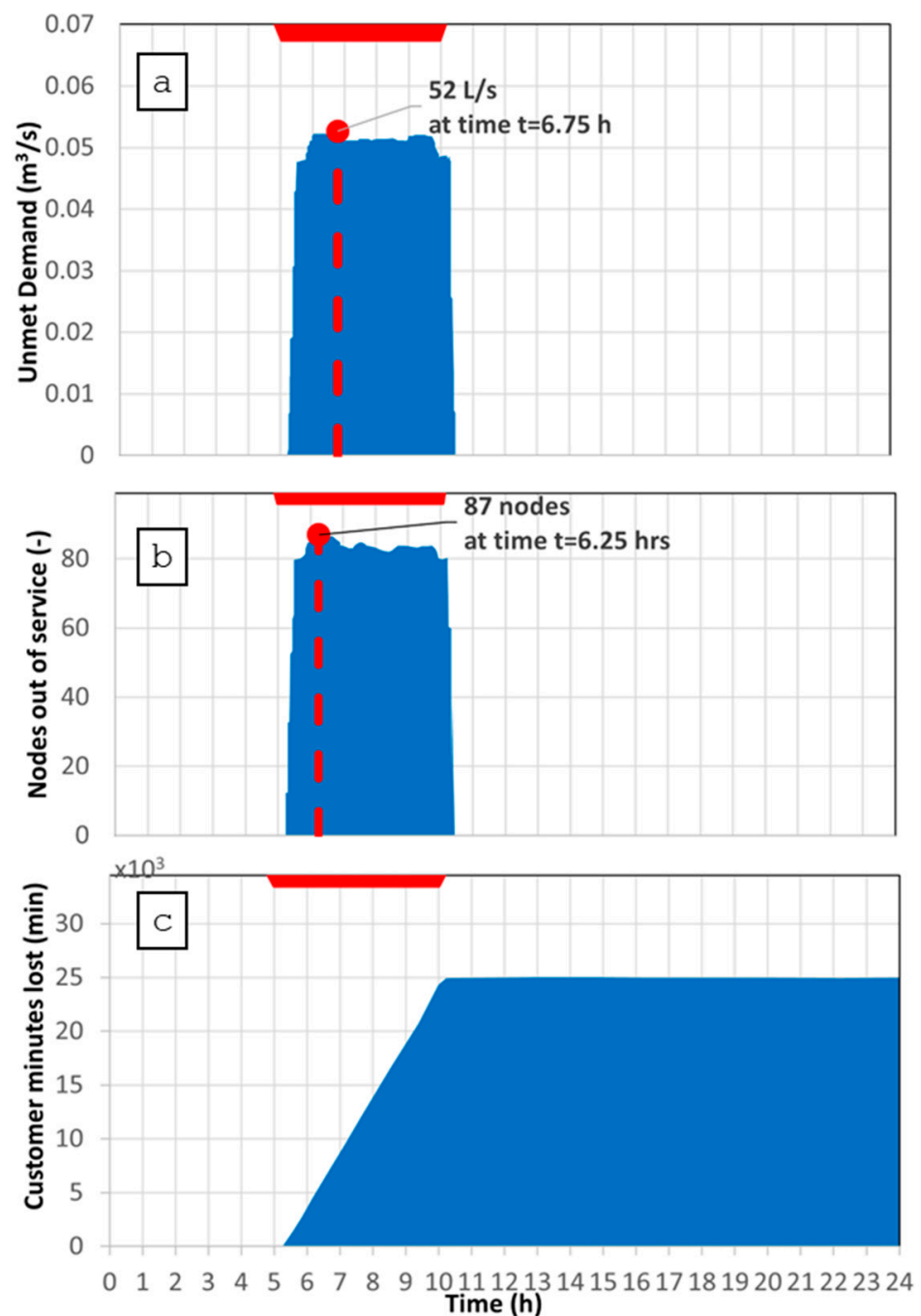


Figure 4. Unmet demand (m³/s) (a), nodes out of service [–] (b), and customer minutes lost (as indicated, values on y-axis are scaled by 10³) (min) (c), derived from the KPI tool for RS 1.

The consequences shown in Figure 4 were assessed by using the KPI tool, in which the impact was assessed in terms of unmet demand (a), nodes out of service (b), and customer minutes lost (c). RS 1 was adopted to also test the STP of RAET by varying one of the three parameters of the selected event. Specifically, the start time was gradually increased from 5 a.m. to 3 p.m., while the duration of the attack and the manipulated value of the tank level were always kept to 5 h and 10 m, respectively. The STP gives additional insights into the simulation because it allows to simultaneously explore the effects on the system of different input values, such as the attack start time of the considered risk event. In Figure 5, the user interface of STP is reported, in which results are listed as values of different KPIs, namely *customer minutes lost* as KPI 1, *nodes out of service* as KPI 2, and *unmet demand* as KPI 3.

Nr	Executed	Control variables	Time [s]	KPI1	KPI2	KPI3
18	2021-06-14 14:34	Duration 5, Level 10.00, Start time 15	126.34	37987.00	393.00	414.77
17	2021-06-14 14:32	Duration 5, Level 10.00, Start time 13	122.82	30410.00	295.00	276.87
16	2021-06-14 14:30	Duration 5, Level 10.00, Start time 11	146.06	37714.00	371.00	395.73
15	2021-06-14 14:28	Duration 5, Level 10.00, Start time 10	136.14	39312.00	401.00	525.57
14	2021-06-14 14:26	Duration 5, Level 10.00, Start time 8	135.07	40382.00	427.00	799.45
13	2021-06-14 14:23	Duration 5, Level 10.00, Start time 6	147.20	40684.00	438.00	925.43

Figure 5. Overview of results in the STP related to RS 1 when changing the attack start time.

Finally, the RRMD was explored to identify measures that could mitigate the risk associated with the specified event of an attack. The risk reduction measures related to the protection of the site of tank 2 would decrease the probability of an external attacker gaining entry into the asset's area; thus, the following measures of the RRMD were suggested within the RAET in connection to the selected risk event:

- M01: fences and walls;
- M02: motion detectors;
- M03: camera surveillance;
- M04: patrols;
- M07: binary contacts;
- M08: secure doors and windows;
- M09: entrance access control;
- M10: secure locks.

RS 2 consisted of the combination of RS 1 and the failure of a critical pipe identified by the Asset Vulnerability Assessment to Risk Events tool (AVAT).

The demonstration of AVAT consisted of preparing and running two input files, namely an EPANET INP file and an Excel file, in which specific probabilities of pipe failures can eventually be inserted. The simulation duration setting was changed from 24 h to zero because AVAT works with only one simulation snapshot. Figure 6 illustrates the successfully loaded network for the AVAT simulation.

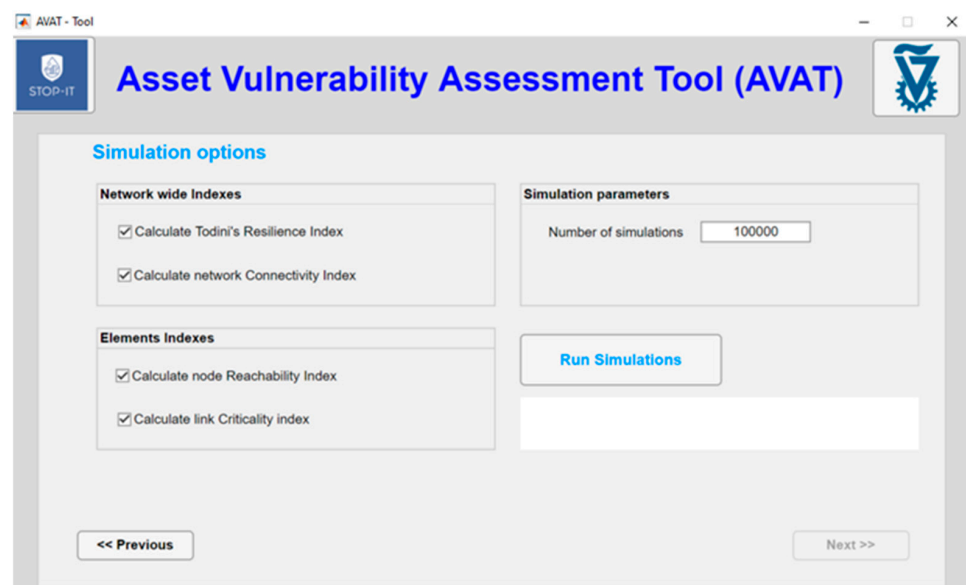


Figure 6. Simulation options window in AVAT.

The simulation of AVAT was used to identify the most critical pipes of the network, which resulted in the main pipe receiving water directly from tank 1, as expected, and another pipe in the distribution network whose criticality was previously less evident. This pipe in the distribution network was selected in the Scenario Planner, then its failure was added to the attack of RS 1. In fact, after the identification of the critical pipe, the same steps of risk scenario 1 were taken in RAET within the Scenario Planner, with the difference of also inserting a major leak on the identified critical pipe for the duration of the simulation in addition to the previous event of manipulation of the tank level sensor. Hence, event gate 255, “WDN pipe break” [16], was selected. The only parameter in RAET that describes event gate 255 is the emitter coefficient [24], set to a value of 5, distributed among the two end nodes of the considered pipe, leading to a major leak on the selected pipe. The results of water shortage in RS 1 and RS 2 are compared in Figure 7. Based on the obtained results, the same relevant RRM identified for RS 1 applies to RS 2.

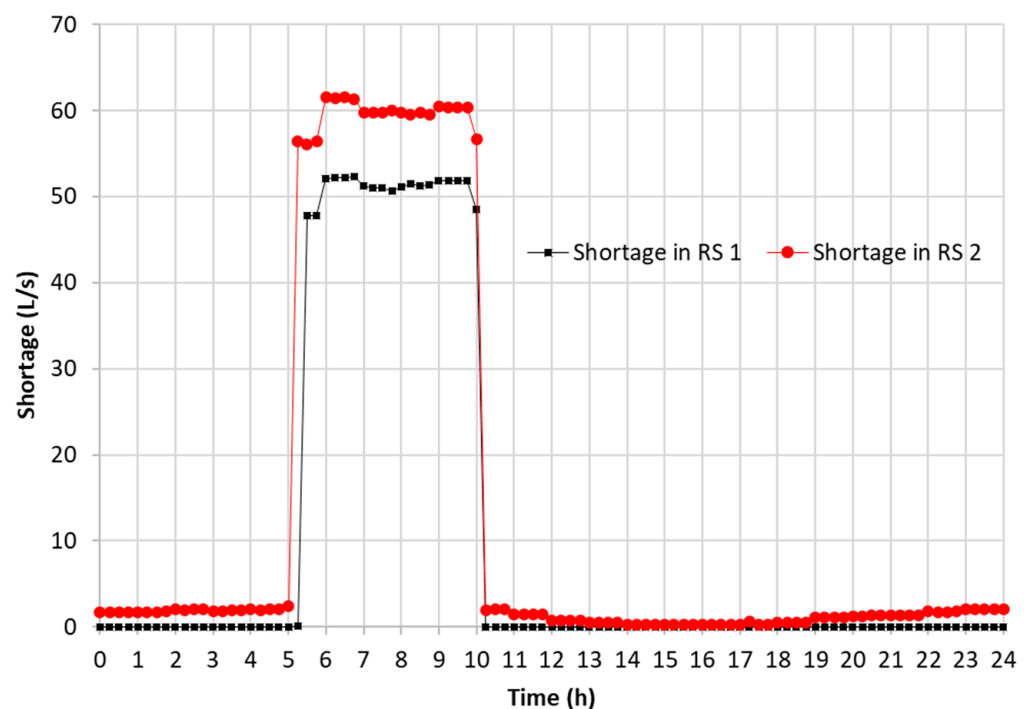


Figure 7. Comparison of unmet demand results for RS 1 (black line) and RS 2 (red line).

RS 3 is conceptually similar to RS 1, but from the fault trees instead of event gate 235, event gate 236, “Man in the middle attack manipulates WDN tank level sensor signals” [16], was selected. In the Scenario Planner, RISKNOUGHT was chosen, and a baseline scenario with an operational condition of firefighting was considered. Specifically, a demand of 50 L/s was inserted in the hydraulic model for a relevant zone of the city from 11 a.m. to 6 p.m. Since tank 3 works mainly as a storage for firefighting in the analyzed zone, it was selected to identify the maximum time to repair before falling into the failure status of unmet demand. Similar to the previous case, three parameters had to be defined, namely the duration of the attack, the start time of the attack, and the manipulated value of the sensor readings. The duration of the cyberattack was set to 10 h, the start time to 10 a.m., and the manipulated value to 6.5 m (i.e., the maximum level of tank 3, which leads the valve providing the supply to remain closed).

Figure 8 shows the selection of the risk event from the Scenario Planner, and Figure 9 shows the results obtained in terms of water production and shortage during firefighting whether or not RS 3 was simulated.

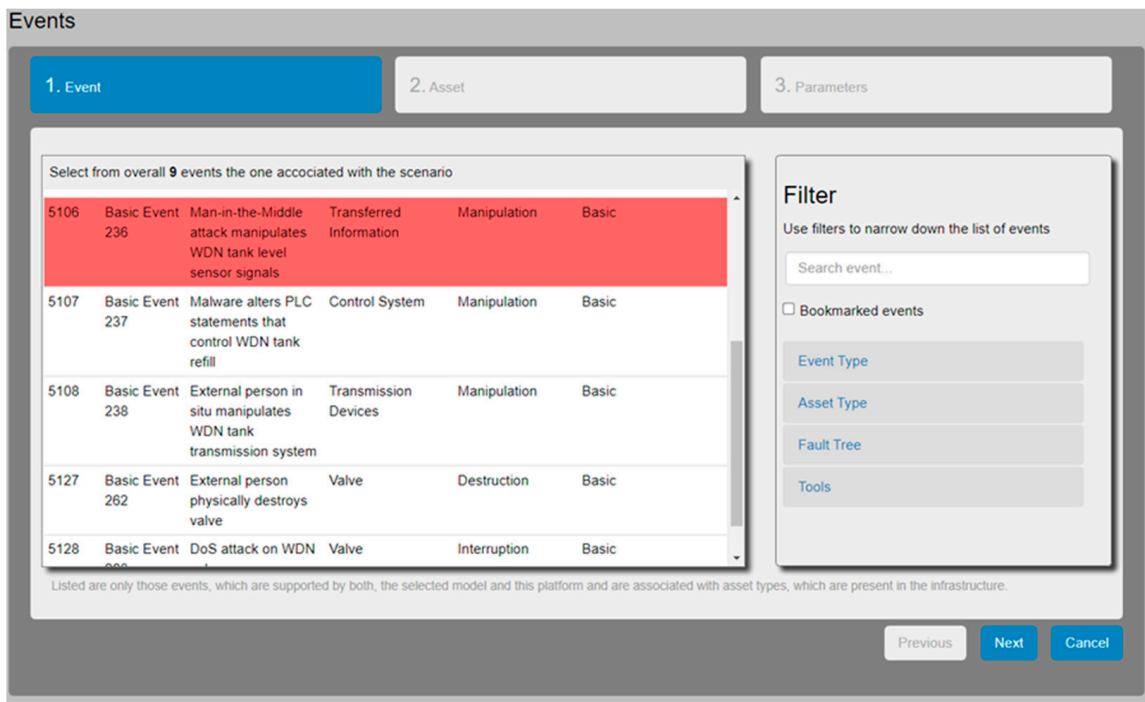


Figure 8. Selection of the risk event of RS 3 proposed by the fault tree within the Scenario Planner.

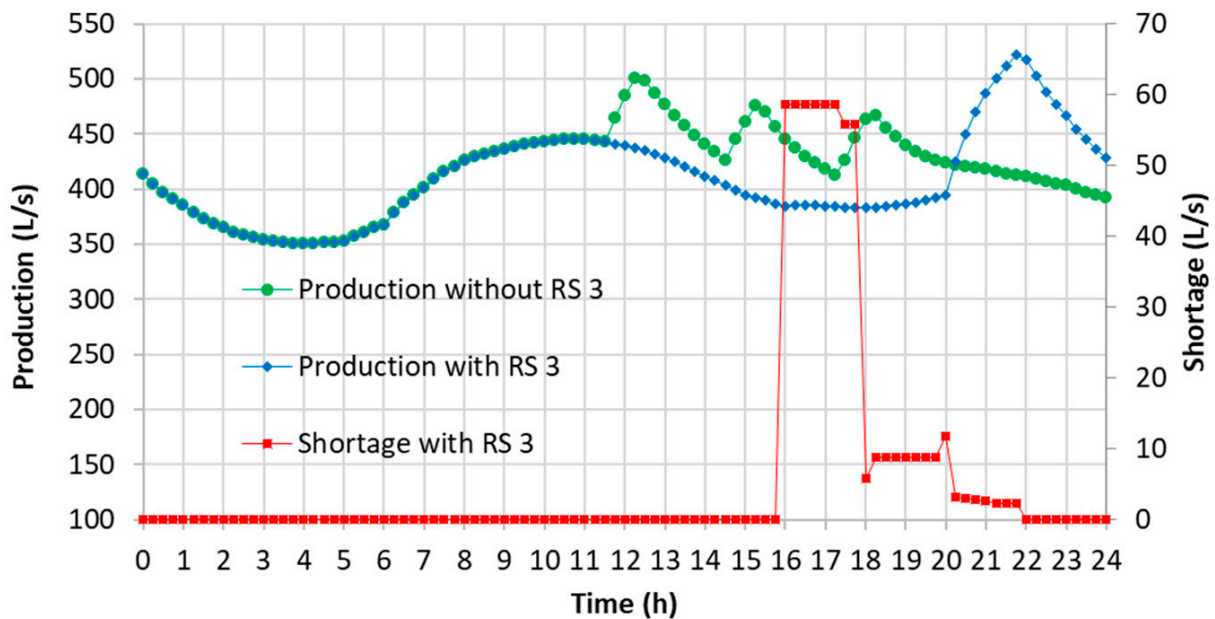


Figure 9. Water production and generated water shortage in the system under RS 3 in comparison with water production in the system under baseline scenario conditions without RS 3.

From Figure 9, it is possible to understand that the stored volume of tank 3 was not enough to supply the firefighting water of the selected scenario, clearly shown by the red line, which indicates a major water shortage. Thus, in order to guarantee water supply for the considered amount of time, additional storage for firefighting purposes might be selected as a risk reduction measure, corresponding to *additional storage capacity* (M33) in the RRMD, as shown in Figure 10.

The screenshot shows a web interface titled "Measures". At the top right, there are buttons for "Advanced Search", "Modify", "Add", and "Reassess relations". Below these is a search bar containing the text "tank". The main content is a table with the following data:

Measure ID	Name	Description	Comments	Terms and Keywords	Risk reduction mechanism
M07	BinaryContacts	Implementation of binary contacts as alarm system at doors, windows or storage tanks. Thus the intrusion of unauthorized personnel to ...	Different reactions are possible if a binary contact is triggered by an intruder. A silent alarm could be sent to ...		Consequences
M19	FiltersInAerationProcesses	All air for aeration purposes in water treatment plants and water storage tanks should be filtered. Thus it is aimed ...	Filters should be installed at every air intake for aeration purposes. Furthermore, no openings for aeration purposes should be built ...		Frequency/Likelihood
M23	LevelSensors	Installation of sensors indicating the filling level of storage tanks or additive reservoirs. Thus it can be supervised if any ...			Frequency/Likelihood
M33	AdditionalStorageCapacity	Construction of additional storage tanks. Thus periods of water scarcity can be bridged easier due to a higher amount of ...			Consequences

At the bottom of the table, it says "Showing 1 to 4 of 4 entries (filtered from 65 total entries)". There are also "Previous" and "Next" navigation buttons.

Figure 10. User interface of the RRMD displaying suggested risk reduction measures.

4. Discussion

Concerning RS 1, in Figure 4a, it is shown that the unsupplied demands start and finish respectively just after 5 a.m. and 10 a.m., with a small delay with respect to the attack. The peak of water shortage is close to 7 a.m., when the majority of customers start their day, then an almost constant water shortage of 50 L/s is observed. In Figure 4b, the number of nodes out of service resembles the unmet demand graph, pointing out that almost all the area remains without service. In fact, the customer minutes lost, represented in Figure 4c, grows linearly with time until the end of the attack. The simulation within the SP of RS 1 produced insightful results concerning the impacts in the case of manipulation of sensor readings of the level in tank 2 in terms of the considered KPIs. Moreover, from the simulations through the STP, it was confirmed that the most critical moment of the day in terms of unmet demand is the early morning.

Concerning RS 2, the water utility was already aware that the main pipeline directly connected to the source was the most critical, but there were uncertainties on the localization of other critical pipes in the distribution network. Thanks to AVAT, it was possible to recognize the importance of the components for the water supply and their corresponding “attractiveness” to be attacked. The damage to the main pipeline directly connected to tank 1 would affect the entire supply; hence, this critical component of the network is undoubtedly important. From the water utility’s perspective, it was more interesting to identify an unknown critical pipe of the distribution network. The resilience of the highly looped network was confirmed by AVAT results. In fact, according to AVAT, the most critical pipe of the distribution system is a peripheral pipe connecting a final branch of the network. As expected, the manipulation of the sensor level in tank 2 had a much more relevant impact on the network in comparison with the considered major leak since the pipe failure introduces only a small additional water shortage with respect to the results obtained with RS 1, as illustrated in Figure 7.

The simulation within the SP of RS 3 produced insightful results concerning the time to repair before having a critical status of the system during firefighting operations in the case of a cyberattack on the sensor reading of tank 3, highlighting that the water shortage begins after 5 h from the start of firefighting. In fact, considering Figure 9, it can be observed that the cyclical process of filling tank 3 started right after 11 a.m., and from 4 p.m. to 6 p.m., the water for firefighting could not be supplied. From 6 p.m., it was assumed that the fire emergency was over, but the cyberattack was ongoing for 2 more hours; thus, there were smaller water shortages due to customers in the area who remained without service until

8 p.m. when the cyberattack finished. After the attack, the connection for the supply to tank 3 was restored; hence, the production process of tank filling started right after 8 p.m.

Overall, the performed simulations supported the water utility in quantifying the loss of service connected to the identified risk scenarios in terms of relevant KPIs. Future applications of the adopted integrated framework might also highlight critical components of water quality aspects. Recognizing the value of the information provided by the simulations within the pilot area, the water utility is now moving toward implementing RAET on a full-scale network and adopting it as a decision support tool not only for risk management strategies but also for assessing the resilience of the system under multiple complex scenarios leading to service disruption.

5. Conclusions

The STOP-IT project, which ended in 2021, aimed at increasing awareness, competence, and preparedness on the topic of cyber-physical protection of water critical infrastructure. The project contributed to training and awareness raising based on the establishment of communities of practice as arenas for knowledge exchange on the topic of cybersecurity, the creation of training material for different user profiles and requirements, and extensive dissemination activities.

On the technological side, the STOP-IT platform provides users with the option to select technologies relevant to their specific challenges while leaving open the possibility to build on the selection by adding additional components to intensify, on need, protection against combined cyber-physical threats and to allow the analysis of cascading effects of physical and cyber events.

The paper focuses on the technological outcomes of the project and, specifically, on the RAET framework designed to support the strategic, tactical decision level of water utilities. By creating potential scenarios of attack and testing the system performance, the user of RAET can investigate opportunities for increasing preparedness by identifying measures to be adopted for risk prevention and risk mitigation, as well as assessing the available time to react in case of an attack before the performance of the system is seriously compromised. The simulations performed, besides the specific application to increase security against cyber-physical attacks, proves the relevance of RAET in supporting water utility decision-makers in performing scenario-based reliability analysis and risk assessment exercises and, overall, in increasing the level of preparedness against complex scenarios combining safety and security aspects. The insights obtained from the demonstration of RAET in the real environment presented here have been highly recognized by the water utility, leading to the adoption of RAET as part of their risk management practice beyond the scope of the STOP-IT project.

Author Contributions: Conceptualization, C.B., G.S.R. and R.U.; methodology, C.B., G.S.R. and R.U.; formal analysis, C.B. and G.S.R.; data curation, C.B., G.S.R., K.T. and H.R.; writing—original draft preparation, C.B., G.S.R. and R.U.; writing—review and editing, C.B., G.S.R., R.U., K.T. and H.R.; project administration, R.U.; funding acquisition, R.U. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the European Union’s Horizon 2020 Research and Innovation Programme, grant agreement No. 740610.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: This work was made possible thanks to Technion (IL) and the National Technical University of Athens (NTUA) (GR), which respectively provided valuable technical support for AVAT and RISKNOUGHT, software developed under the H2020 STOP-IT research project.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Liu, G.; Zhang, Y.; Knibbe, W.J.; Feng, C.; Liu, W.; Medema, G.; van der Meer, W. Potential impacts of changing supply-water quality on drinking water distribution: A review. *Water Res.* **2017**, *116*, 135–148. [[CrossRef](#)] [[PubMed](#)]
2. Raspati, G.S.; Bruaset, S.; Bosco, C.; Mushom, L.; Johannessen, B.; Ugarelli, R. A Risk-Based Approach in Rehabilitation of Water Distribution Networks. *Int. J. Environ. Res. Public Health* **2022**, *19*, 1594. [[CrossRef](#)]
3. Caradot, N.; Sonnenberg, H.; Kropp, I.; Ringe, A.; Denhez, S.; Hartmann, A.; Rouault, P. The relevance of sewer deterioration modelling to support asset management strategies. *Urban Water J.* **2017**, *14*, 1007–1015. [[CrossRef](#)]
4. Ferrante, M.; Bosco, C.; Ugarelli, R.; Magenta, L.; Eidsmo, T. Mass, Energy, and Cost Balances in Water Distribution Systems with PATs: The Trondheim Network Case Study. *J. Water Resour. Plan. Manag.* **2020**, *146*, 05020005. [[CrossRef](#)]
5. Elimelech, M. The global challenge for adequate and safe water. *J. Water Supply Res. Technol. AQUA* **2006**, *55*, 3–10. [[CrossRef](#)]
6. Schlosser, C.A.; Strzpek, K.; Gao, X.; Fant, C.; Blanc, É.; Paltsev, S.; Gueneau, A. The future of global water stress: An integrated assessment. *Earth's Future* **2014**, *2*, 341–361. [[CrossRef](#)]
7. Lowe, M.; Qin, R.; Mao, X. A review on machine learning, artificial intelligence, and smart technology in water treatment and monitoring. *Water* **2022**, *14*, 1384. [[CrossRef](#)]
8. Bosco, C.; Pezzinga, G.; Sinagra, M.; Tucciarelli, T. Optimal design of water pipeline and micro-hydro turbine by genetic algorithm. *EPiC Ser. Eng.* **2018**, *3*, 302–309.
9. Romano, M.; Kapelan, Z. Adaptive water demand forecasting for near real-time management of smart water distribution systems. *Environ. Model. Softw.* **2014**, *60*, 265–276. [[CrossRef](#)]
10. Campisano, A.; Creaco, E.; Modica, C. Application of real-time control techniques to reduce water volume discharges from quality-oriented CSO devices. *J. Environ. Eng.* **2016**, *142*, 04015049. [[CrossRef](#)]
11. Bosco, C.; Campisano, A.; Modica, C.; Pezzinga, G. Application of rehabilitation and active pressure control strategies for leakage reduction in a case-study network. *Water* **2020**, *12*, 2215. [[CrossRef](#)]
12. Moy de Vitry, M.; Schneider, M.Y.; Wani, O.F.; Manny, L.; Leitão, J.P.; Eggimann, S. Smart urban water systems: What could possibly go wrong? *Environ. Res. Lett.* **2019**, *14*, 081001. [[CrossRef](#)]
13. Taormina, R.; Galelli, S.; Tippenhauer, N.O.; Salomons, E.; Ostfeld, A. Characterizing cyber-physical attacks on water distribution systems. *J. Water Resour. Plan. Manag.* **2017**, *143*, 04017009. [[CrossRef](#)]
14. Tuptuk, N.; Hazell, P.; Watson, J.; Hailes, S. A systematic review of the state of cyber-security in water systems. *Water* **2021**, *13*, 81. [[CrossRef](#)]
15. Mohebbi, S.; Zhang, Q.; Wells, E.C.; Zhao, T.; Nguyen, H.; Li, M.; Ou, X. Cyber-physical-social interdependencies and organizational resilience: A review of water, transportation, and cyber infrastructure systems and processes. *Sustain. Cities Soc.* **2020**, *62*, 102327. [[CrossRef](#)]
16. Makropoulos, C.; Moraitis, G.; Nikolopoulos, D.; Karavokiros, G.; Lykou, A.; Tsoukalas, I.; Morley, M.; Gama, M.C.; Okstad, E.; Vatn, J. STOP-IT Deliverable 4.2: Risk Analysis and Evaluation Toolkit. 2019. Available online: <https://stop-it-project.eu/download/risk-analysis-and-evaluation-toolkit/> (accessed on 29 November 2022).
17. Makropoulos, C.; Nikolopoulos, D.; Palmen, L.; Kools, S.; Segrave, A.; Vries, D.; Koop, S.; van Alphen, H.J.; Vonk, E.; van Thienen, P. A resilience assessment method for urban water systems. *Urban Water J.* **2018**, *15*, 316–328. [[CrossRef](#)]
18. Nikolopoulos, D.; van Alphen, H.J.; Vries, D.; Palmen, L.; Koop, S.; van Thienen, P.; Medema, G.; Makropoulos, C. Tackling the “new normal”: A resilience assessment method applied to real-world urban water systems. *Water* **2019**, *11*, 330. [[CrossRef](#)]
19. ISO 31 000:2018; Risk Management. Risk Assessment Techniques. International Standards Organization: Geneva, Switzerland, 2018.
20. Ostveld, A.; Salomons, E.; Roth, R.; Zeevi, G.; Weiss, H.; Vatn, J.; Okstad, E. STOP-IT Deliverable D4.1: Asset Vulnerability Assessment to Risk Events. 2018. Available online: <https://stop-it-project.eu/download/asset-vulnerability-assessment-to-risk-events-supporting-document-d4-1/> (accessed on 29 November 2022).
21. Mälzer, H.J.; Vollmer, F.; Corchero, A. STOP-IT Deliverable 4.3: Risk Reduction Measures Database (RRMD) Supporting Document. 2019. Available online: <https://stop-it-project.eu/download/rmd-supporting-document-d4-3/> (accessed on 29 November 2022).
22. Ahmadi, M.; Ugarelli, R.; Grøtan, T.O.; Raspati, G.; Selseth, I.; Makropoulos, C.; Nikolopoulos, D.; Moraitis, G.; Karavokiros, G.; Bouziotas, D.; et al. STOP-IT Deliverable 4.4: Cyber-Physical Threats Stress-Testing Platform. 2019. Available online: <https://stop-it-project.eu/download/cyber-physical-threats-stress-testing-platform-d4-4/> (accessed on 29 November 2022).
23. Nikolopoulos, D.; Moraitis, G.; Bouziotas, D.; Lykou, A.; Karavokiros, G.; Makropoulos, C. Cyber-physical stress-testing platform for water distribution networks. *J. Environ. Eng.* **2020**, *146*, 04020061. [[CrossRef](#)]
24. Rossman, L.A. *EPANET 2: Users Manual*; EPA: Washington, DC, USA, 2000.