STOP-IT tools validated

STOP-IT

STOP-IT solutions implemented at City of Oslo, Agency for Water and Wastewater Services (VAV) in Norway

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 740610.

stop-it-project.eu

Challenges

The level of service in water supply systems is guaranteed by the optimal operations of pumps and valves, and by the continuous monitoring of pressure values and frequency of pipe breaks. Pressure drops in the distribution network can be detrimental to users' water demand satisfaction. The ongoing digitalization in the water sector brings opportunities to increase the efficiency of processes, but also new challenges related to potential cyber-attacks on the water systems. Therefore, we are interested in a set of tools which can provide a system of defense against cyber and physical threats on our water supply system.

Our goal is to provide clean water for the benefit of people and the environment in Oslo. We have a long history of innovation for resilience and security purposes, thus it is natural for us to participate in European innovation projects like STOP-IT.

Approach

A comprehensive approach has been adopted by implementing several tools, developed within the STOP-IT project, in order to increase our cyber as well as physical security, on all levels from strategical and tactical planning to operations. The solutions included in Module I of the STOP-IT platform were adopted to improve the resilience of the physical infrastructure by enhancing the capability of our water supply system in providing water to customers under attack. At the operational level, VAV has selected several solutions to increase the security of the cyber infrastructure, with the aim of detecting a) unauthorised data traffic in process network, b) humans or obstacles in a selected area with debris-catching grids in rivers, c) unauthorised personnel entering facilities inside the waterworks, and d) real-time anomalies in the process network.

Employees in VAV are trained to guarantee the physical security of our assets

Successful application of STOP-IT tools at VAV

Risk Analysis and Evaluation Toolkit (RAET)

This toolkit links all the steps of risk management (identification, analysis, evaluation, and treatment of the risk) in a platform with a seamless workflow. Our scenarios of interest were related to the manipulation of the tank level sensors and the failure of a critical pipe (identified through AVAT, a STOP-IT tool nested in the RAET). We tried to assess the time to repair a structure before falling into a failure status of unmet demands, and to identify the critical areas through calculations of the relevant key performance indicators.

Network Traffic Sensors and Analysers (NTSA)

This tool was adopted to model the regular behaviour associated to the data traffic in our water critical infrastructure. Hence, the model could be used to detect abnormal network traffic behaviour in real time. Specifically, anomalies were recognised when an unauthorised individual accessed the process network, introducing a false packet containing a setpoint change to a PLC.

Cyber Threat Sharing Service (CTSS)

This tool collects and shares information about known threats and incidents that could affect critical infrastructures. The information is structured using standards to facilitate the exchange of the security threats identified, establishing a global exchange to prevent, reduce, mitigate and recover from existing threats. In collaboration with KraftCERT (the CERT for the Norwegian power industry), the process of collecting and sharing cyber threats was started, identifying the criteria on how to share the events both at a national and international level.

Computer Vision Tool (CVT)

By using recorded images, a classifier of normal actions and behaviours caught on security cameras can be generated. VAV applied this tool for the cameras used for surveillance of debris-catching grids in rivers, where excess debris can create blockages and flood areas downstream. We also saw this as an opportunity to detect humans, e.g. playing children, falling into the river. The tool automatically raises the alarm to operating personnel in case of an in irregular situation, dramatically reducing the necessity to drive around manually checking the river grids.

Real-Time Anomaly Detector (RTAD)

This tool is based on the use of a Big Data platform and machine learning algorithms, which provide an additional layer of security by detecting complex and combined potential threats and attacks. Based on alarms and historical event logs in our SCADA system (i.e., signals of overflows, and physical access control messages), the tool was used to distinguish real anomalies in our process network from false positives.

Cross Layer Security Information and Event Management (XL-SIEM)

This tool indicates the risk level of multiple cyber-security events coming from different sources, generating correlated alarms and detailed information about the event (description, IP source and destination, port source and destination protocols). Its application was successfully tested, using live data and the detection of real events in the process network logs as input to XL-SIEM.

Successful application of STOP-IT tools at VAV

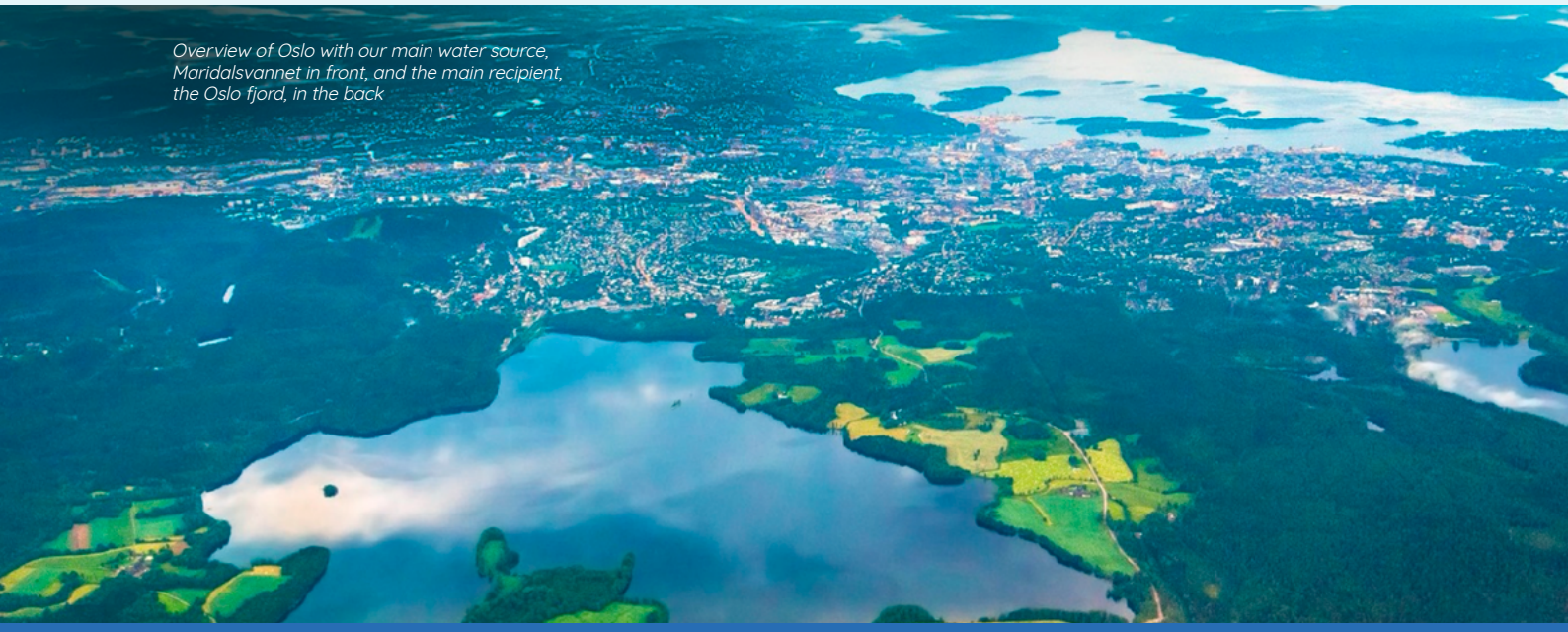
Reasoning Engine (REN) and Enhanced Visualisation Interface (EVI) for water utilities

The Reasoning Engine provides decision support to the system operator based on event sources by filtering, aggregating, correlating and upscaling information with the aim of a proper treatment of the risk. In parallel, the Enhanced Visualization Interface allows to create awareness on the current situation in a water utility by showing multiple views, generated through real-time, historical and GIS mapping data, incident information and shared information. Thanks to EVI, relevant threats were simulated with the aim of detecting them on different dashboards for different types of roles in VAV. Thanks to REN, the threats were recognized as correlated to one distinct event instead of many separate alarms.

The implementation of digital solutions in VAV comes with data protection and cyber-security

Conclusion

By adopting a comprehensive set of tools developed within STOP-IT, our team has benefitted from both, the selected tools by themselves as well as the connection and interaction between them. Thanks to all the partners involved in the project, our organization has successfully demonstrated the selected tools and therefore accomplished our objectives related to a more secure and resilient cyber-physical infrastructure.



Overview of Oslo with our main water source, Maridalsvannet in front, and the main recipient, the Oslo fjord, in the back

About STOP-IT

Water infrastructures are essential for human society, life and health. They can be endangered by physical or cyber threats with severe societal consequences. To protect them, STOP-IT brings together a strong team of 23 partners from across Europe and Israel to develop solutions to the most pressing threats. The team identifies risks and co-develops an all-hazards risk management framework for the physical and cyber protection of critical water infrastructures.

Editor

City of Oslo, Agency for Water and Wastewater Services (VAV)

Contact

harald.rishovd@vav.oslo.kommune.no

More at

https://stop-it-project.eu

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 740610.