STOP-IT

stop-it-project.eu

rita.ugarelli@sintef.no
(Project Coordinator)

Are your water infrastructures secure against physical and cyber attacks?

The **STOP-IT software platform** allows you to **identify** cyber-physical risks, **simulate** scenarios, **evaluate** consequences, **explore** best treatment options and **select** from a range of state-of-art **solutions** at strategic, tactical and operational scale.

The platform is:

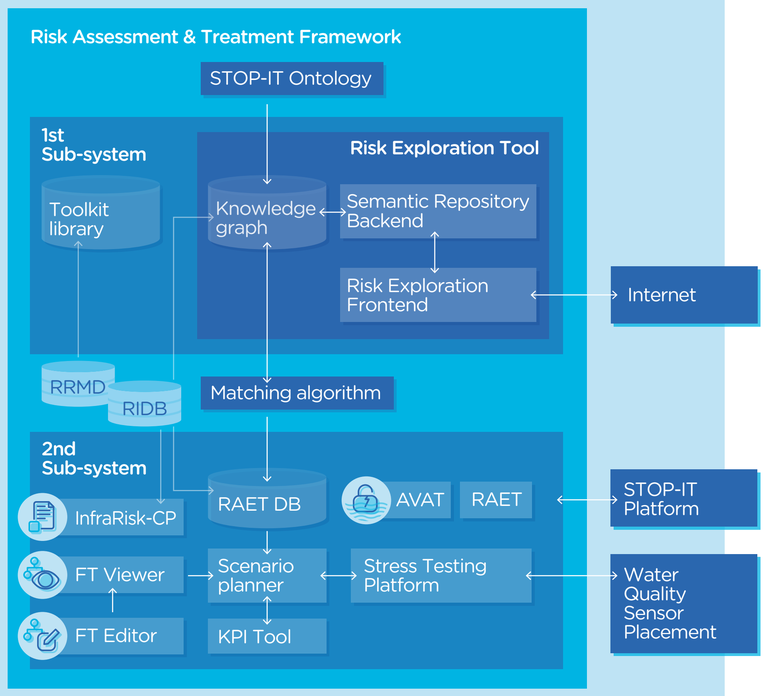
Scalable: Usable by small and large water utilities

Adaptable: Different modules for different needs

Flexible: Usable by experts but also non-technical staff

Assess risks and their impact on your network – solutions at strategic and tactical level

The **Risk Analysis and Evaluation Toolkit (RAET)** helps water utilities to identify the most vulnerable elements in their system, create and simulate scenarios to 'play out' cyber-physical attacks, visualize the system's response and identify countermeasures that could protect their water infrastructure (see Figure).



The solutions at operational level

STOP-IT toolboxes cover a large spectrum of technologies to ensure protection against physical and cyber threats

Toolbox of technologies for physical threat protection

A **Human Presence Detector (HPD)** detects human presence in a room/area, using WiFi commercial devices and channel state information (CSI).

Computer Vision Tools (CVT) detect suspicious behavior, using computer vision algorithms in real-time.

An **Access Control System based on the use of Electronic Locks (Smart Locks)** and a mobile App, directly connected to the SCADA systems.

A **Fine-grain Cyber Access Control (FCAC)** that employs user specified policies to determine who can access which resources and for what purpose.

Toolbox of technologies for securing IT and SCADA

Network Traffic Sensors and Analysers (NTSA) to monitor network traffic and logs to accurately detect anomalies that might represent attacks to an infrastructure.

A **Real-time Sensor Data Protection (RSDP)** tool based on blockchain technology to provide a record of the generated data and a mechanism to verify its integrity.

Fault-Tolerant Control Strategies (FTCS) for physical anomalies affecting the SCADA system, focused on the recovery phase once the failure is isolated.

Solutions for real-time decision support

Reasoning Engine that generates alerts and proposes countermeasure actions to mitigate the negative effects based on utility-defined rules.

Public Warning System to detect incidents and inform users and citizens by sending information and instructions to follow.

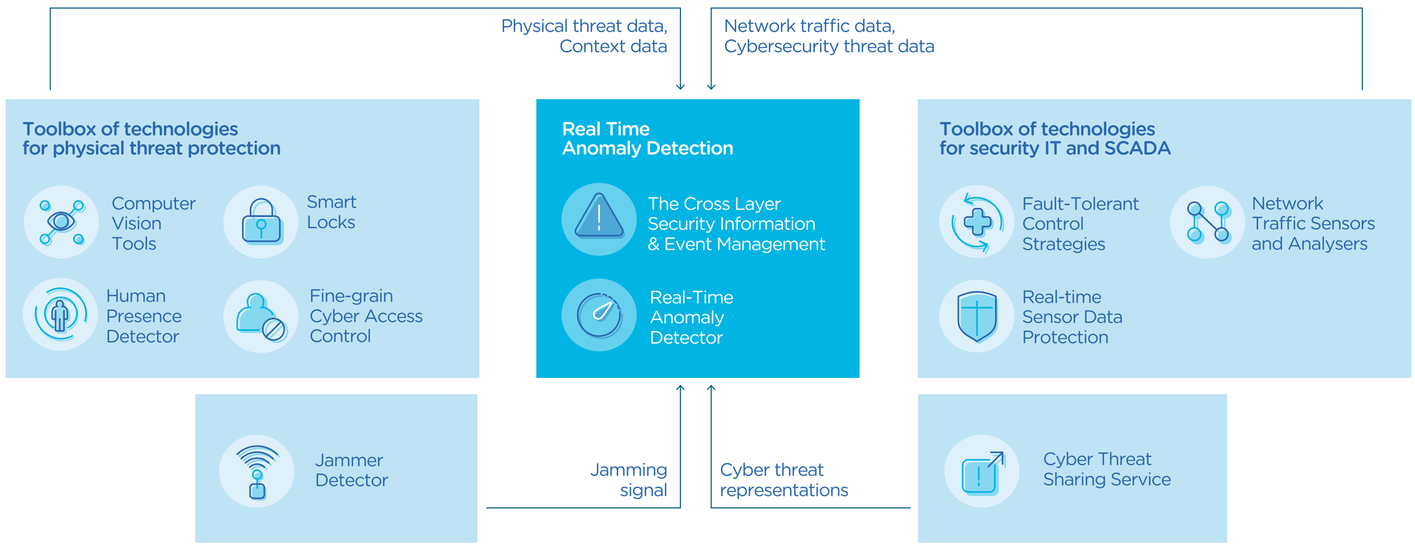
Enhanced Visualization Interface to share operational infomation for the understanding of the current situation in a water utility.

The **Cross Layer Security Information and Event Management (XL-SIEM)** detects incidents, correlates events received from different monitoring probes and generates the corresponding alerts when incidents are detected.

The **Real-Time Anomaly Detector (RTAD)** detects potential threats by injecting data logs from physical and cyber network environments into a security big data platform.

The **Jamming detection sensor (JDet)** detects anomalies on the physical layer and informs when there is an attack going on.

The **Cyber Threat Sharing Service (CTSS)** allows to collect and share existing threats from relevant internal and external sources, using standard protocols like STIX/TAXII v2.



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 740610. The publication reflects only the authors' views and the European Union is not liable for any use that may be made of the information contained therein.