STOP-IT

Secure your water infrastructures against cyber-physical attacks and threats with the STOP-IT platform

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. 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.

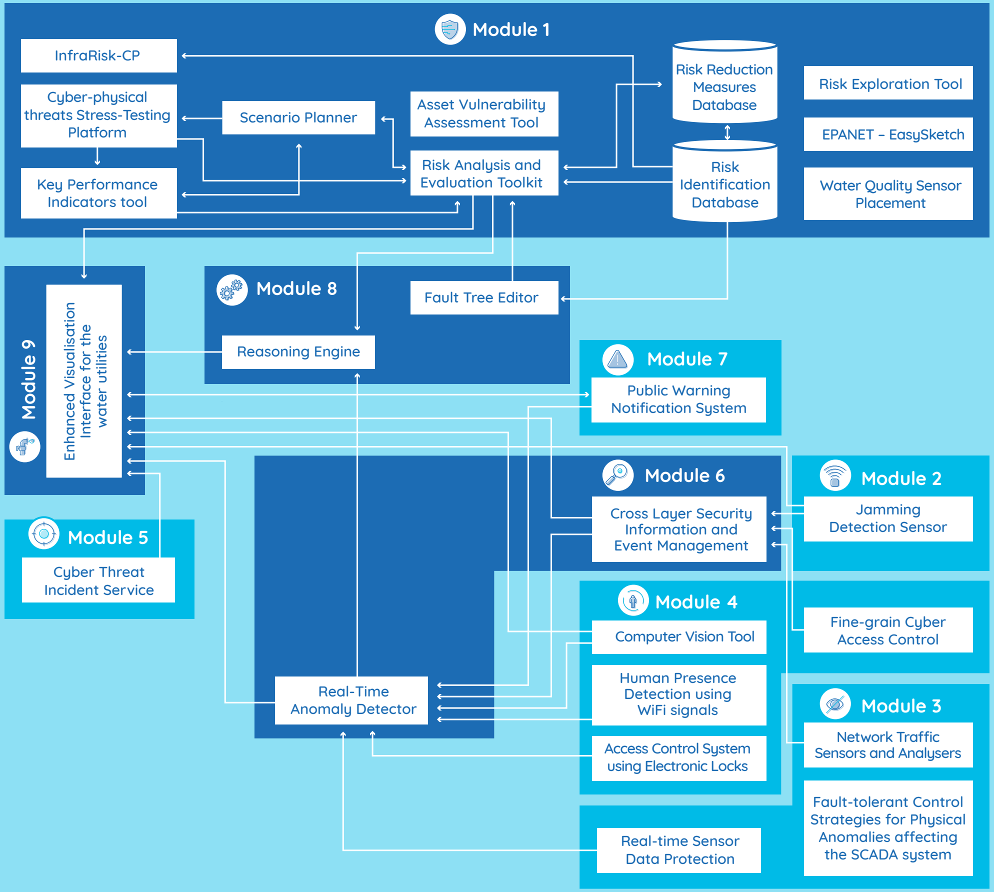
The STOP-IT platform was developed to protect your critical infrastructure against cyber and physical threats and a combination thereof. The core modules (marked in dark blue colour) form the backbone of the platform, the remaining cyber and physical modules offer additional protection or information to critical infrastructure operators.

The main added value of the platform is that all modules are integrated, connected to each other and interoperable, therefore ensuring the protection against combined cyber-physical threats and allowing the analysis of cascading effects of physical and cyber events.

The platform was validated in an operational environment and all solutions were demonstrated in real environments.

STOP-IT platform video

STOP-IT platform



Module 1

InfraRisk-CP

Cyber-physical threats Stress-Testing Platform

Key Performance Indicators tool

Scenario Planner

Asset Vulnerability Assessment Tool

Risk Analysis and Evaluation Toolkit

Risk Reduction Measures Database

Risk Identification Database

Risk Exploration Tool

EPANET – EasySketch

Water Quality Sensor Placement

Module 9

Enhanced Visualisation Interface for the water utilities

Module 8

Fault Tree Editor

Reasoning Engine

Module 7

Public Warning Notification System

Module 5

Cyber Threat Incident Service

Module 6

Cross Layer Security Information and Event Management

Module 2

Jamming Detection Sensor

Module 4

Computer Vision Tool

Human Presence Detection using WiFi signals

Access Control System using Electronic Locks

Real-Time Anomaly Detector

Fine-grain Cyber Access Control

Module 3

Network Traffic Sensors and Analysers

Fault-tolerant Control Strategies for Physical Anomalies affecting the SCADA system

Real-time Sensor Data Protection

Modular components of the integrated STOP-IT platform

Module 1
Strategic and tactical decision making tools

Module 2
Tool to detect and inform about wireless jamming attacks

Module 3
Tools to monitor and protect SCADA and IT systems

Module 4
Tools for protection against physical threats

Module 5
Tool storing and sharing information about cyber threats and attacks across critical infrastructure

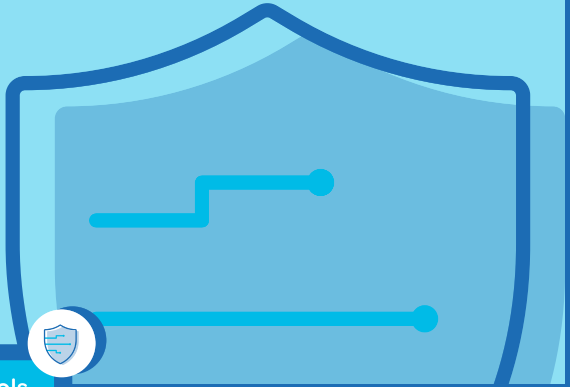
Module 6
Tools to detect cyber-physical anomalies

Module 7
Tool for alerting users/citizens about a critical situation

Module 8
Tools for risk exposure assessment, alert generation and countermeasure proposition

Module 9
Tool that visualises information in the STOP-IT platform from all modules

STOP-IT platform



Module 1

Strategic and tactical decision making tools

Risk Analysis and Evaluation Toolkit (RAET)

A platform for identifying, analysing and evaluating cyber-physical risks and assorted mitigation actions by providing access to specific tools and models. The RAET links interdisciplinary approaches into a seamless workflow to synthesize actionable intelligence and support informed decision making in an interactive mode.

Risk Identification Database (RIDB)

A comprehensive, adaptable database of risk events for the entire water critical infrastructure system. It is used as a base for strategic, tactical and operational level of planning and is linked to the Risk Reduction Measures Database (RRMD).

InfraRisk (CP)

A standalone desktop application to assist in identification and prioritization of cyber-physical threats against water systems as part of a generic risk assessment.

Asset Vulnerability Assessment Tool (AVAT)

This tool is acting as a procedural "step-by-step" guide for the assessment of vulnerability of water distribution system assets, taking into consideration the specific characteristics of the assets and the importance of the components for water supply and their "attractiveness" to be attacked.

Scenario Planner (SP)

The scenario planner is an intuitive scenario planning environment to specify multiple-threat scenarios by guiding through available fault trees and mitigation options. It generates model-specific data according to the formulated scenario and passes it to the embedded cyber-physical solvers.

Cyber-physical threats Stress-Testing Platform (STP)

An EPANET-based platform which provides a simulation environment for both, physical and cyber sub-systems, to assess the behaviour of the cyber physical water system by deliberately stressing it under different attack scenarios. The STP can simulate multiple variations of a given scenario in a single batch procedure, similar to a sensitivity analysis.

Key Performance Indicators tool (KPI Tool)

A standalone application designed to assist water utilities to gauge and evaluate potential cyber-physical attacks to their network and account for critical community systems and services (e.g. hospitals, schools, military facilities etc.).

Risk Reduction Measures Database (RRMD)

An expandable database linked with RAET functionalities that facilitates the identification, selection and prioritization of appropriate risk reduction measures as actions, activities or processes that can be applied to reduce the occurrence and minimize consequences of events. It is linked to the Risk Identification Database (RIDB).

Water Quality Sensor Placement Tool (WQSP)

The multi-objective optimization tool provides a model for the conjunctive placement of hydraulic and water quality sensors in water distribution systems.

Risk Exploration Tool (RET)

A risk exploration tool that helps to link risk with mitigation actions.

EPANET – EasySketch (EES)

The access to most of the tools of Module 1 is only possible for water companies that already have a hydraulic model of the pipeline network and can create an EPANET input file, which is the basis for the calculations to be done e.g. in the RAET. The EPANET – EasySketch (EES) tool is used to generate an EPANET input file, starting from a simplified sketch of the system without the use of EPANET software.

Module 2

Tool to detect and inform about wireless jamming attacks

Jamming Detection Sensor (Jdet) Detects physical disturbances of wireless communications and therefore ensures that wireless communications are not compromised by Denial of Service (DoS).

Module 3

Tools to monitor and protect SCADA and IT systems

Network Traffic Sensors and Analysers (NTSA) Incorporates five categories of sensors able to identify different malicious patterns, such as TTL-based attacks, brute force attacks, DNS answer attacks, time-based attacks, and domain-based attacks.

Real-time Sensor Data Protection (RSDP) This service guarantees the integrity of data. Customers can detect data modifications (or corruption) once data has been gathered (or generated) by sensors and stored.

Fault-tolerant Control Strategies for Physical Anomalies affecting the SCADA system (FTCS) Simulation environment to support operators to optimize the selection of potential interventions that could be deployed.

Module 4

Tools for protection against physical threats

Computer Vision Tool (CVT) Computer vision and machine learning tool for automated surveying of water utilities' critical infrastructure.

Access Control System using Electronic Locks (Smart-Locks) Provides users with the ability to arm and disarm the security systems on the sites on demand. Allows to centralise access requests, automating the process of granting access to specific areas within the same site, as well as to give access for a limited time.

Human Presence Detection using WiFi signals (HPD) The tool processes and analyses the changes on the WiFi spectrum to detect the movement of intruders in an area with WiFi coverage.

Fine-grain Cyber Access Control (FCAC) Evaluates authorization request for users of the STOP-IT platform and provides rules to be implemented by physical security devices.

Module 5

Tool storing and sharing information about cyber threats and attacks across critical infrastructure

Cyber Threat Incident Service (CTSS) Real-time information about threats and incidents that are affecting critical infrastructures, thus improving their security by creating sharing-communication of the threats and incidents.

Module 6

Tools to detect cyber-physical anomalies

Real-Time Anomaly Detector (RTAD) Real time anomaly detection in cyber-physical infrastructures using machine learning and signature-based detection of abnormal behaviours within the network.

Cross Layer Security Information and Event Management (XL-SIEM) This tool receives events coming from different sources to generate correlated alarms that indicate the risk level and detailed information about the event.

Module 7

Tool for alerting users/citizens about a critical situation

Public Warning Notification System (PWNS) Designed to notify the surrounding population of a risk event in order to protect peoples' lives and decrease the impact of the event.

Module 8

Tools for risk exposure assessment, alert generation and countermeasure proposition

Reasoning Engine (REN) This tool provides real-time custom alerting and mitigation action proposition for cyber, physical events and their combinations.

Fault Tree Editor (FTE) This tool is a fault tree editor customized to the needs of water utilities and an analysis toolbox for tactical and strategic decisions and planning.

Module 9

Tool that visualises information in the STOP-IT platform from all modules

Enhanced Visualisation Interface for the water utilities (EVI) This tool is the user interface of the STOP-IT platform, which displays the current state of the critical infrastructure.

Learn more about the STOP-IT project and our research results

Visit the STOP-IT website and find out more about the STOP-IT platform and our strategic, tactical, operational and real-time solutions and tools:
stop-it-project.eu

Project Partners

SINTEF

IWW
IWW Water Centre

CETAQUA
Water Technology Centre

KWR

Aigües de Barcelona

emasagra

World Sensing

Berliner Wasserbetriebe

mnemonic
– securing your business

Aplicatzia

hessenwasser

eurecat

Water Europe
Technology & Innovation

MEKOROT

TECHNION
Israel Institute of Technology

RiSA
Sicherheitsanalysen GmbH

BERGEN KOMMUNE

De Watergroep

PNO
Connecting Ambitions

ΕΠΙΣΕΥ
ICCS

Atos

oylo
Trust Engineering

Oslo