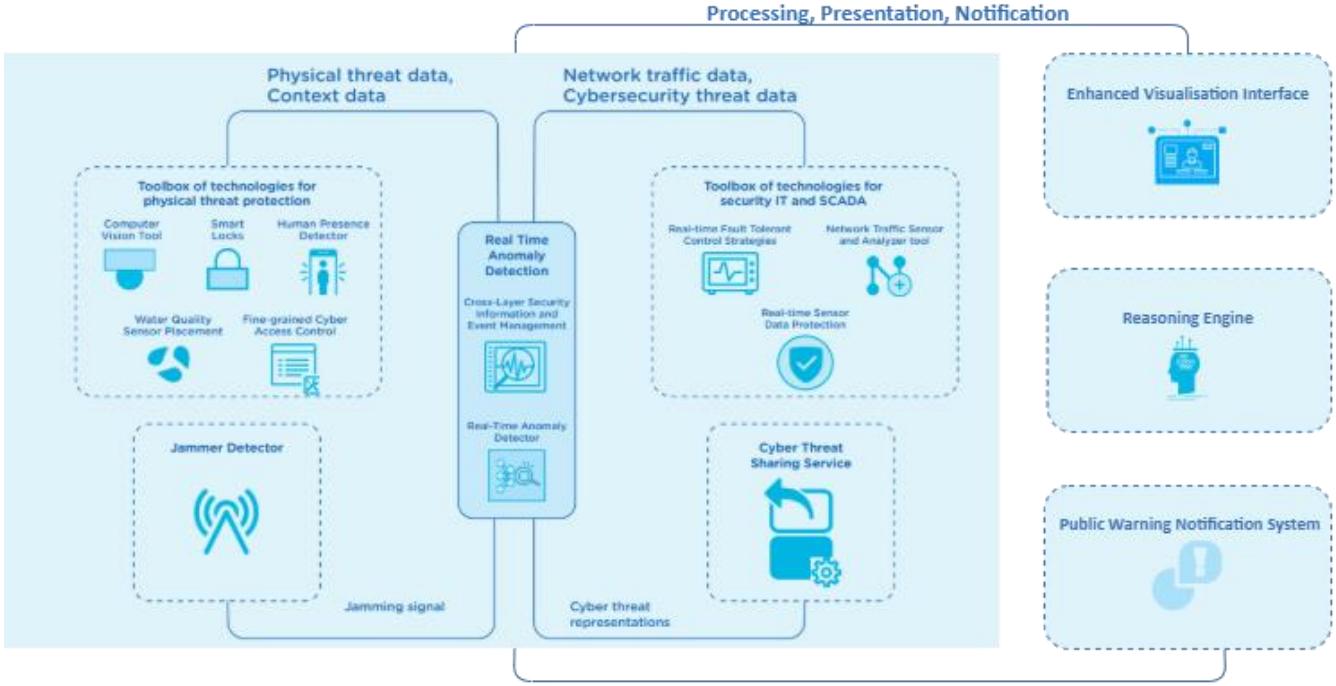
The STOP-IT Platform

Introduce and evaluate a novel integrated approach for the security of water critical infrastructures that combines **cyber** and **physical** protection modules in an overarching solution.



ROADMAP

Towards the integrated STOP-IT Platform




Design

ARCHITECTURE

Design the security framework.

Develop

MODULES

Development of solutions that cover presentation, notification and processing needs

Integrate

PLATFORM

Combine modules into an integrated whole

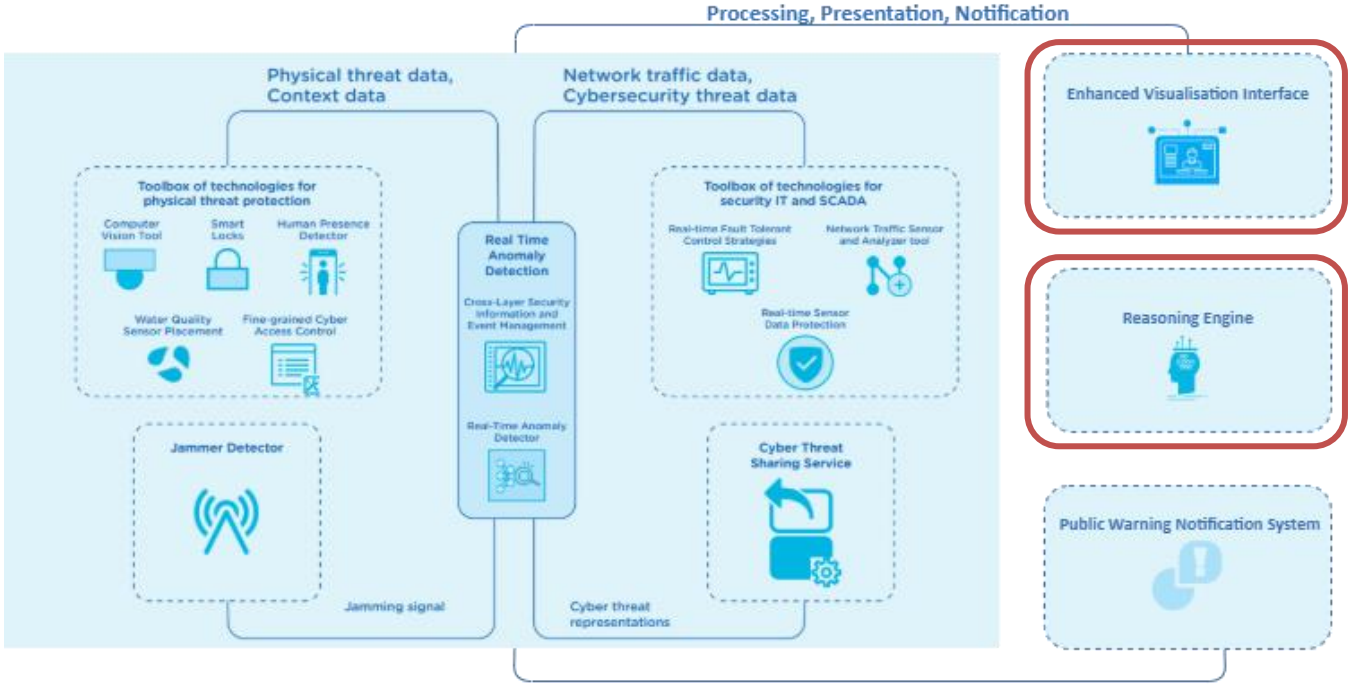
Validate

PROTOTYPE

Definition of the evaluation plan and validation in a simulated operational scenario

The STOP-IT Platform

Introduce and evaluate a novel integrated approach for the security of water critical infrastructures that combines **cyber** and **physical** protection modules in an overarching solution.



What is the Reasoning engine?

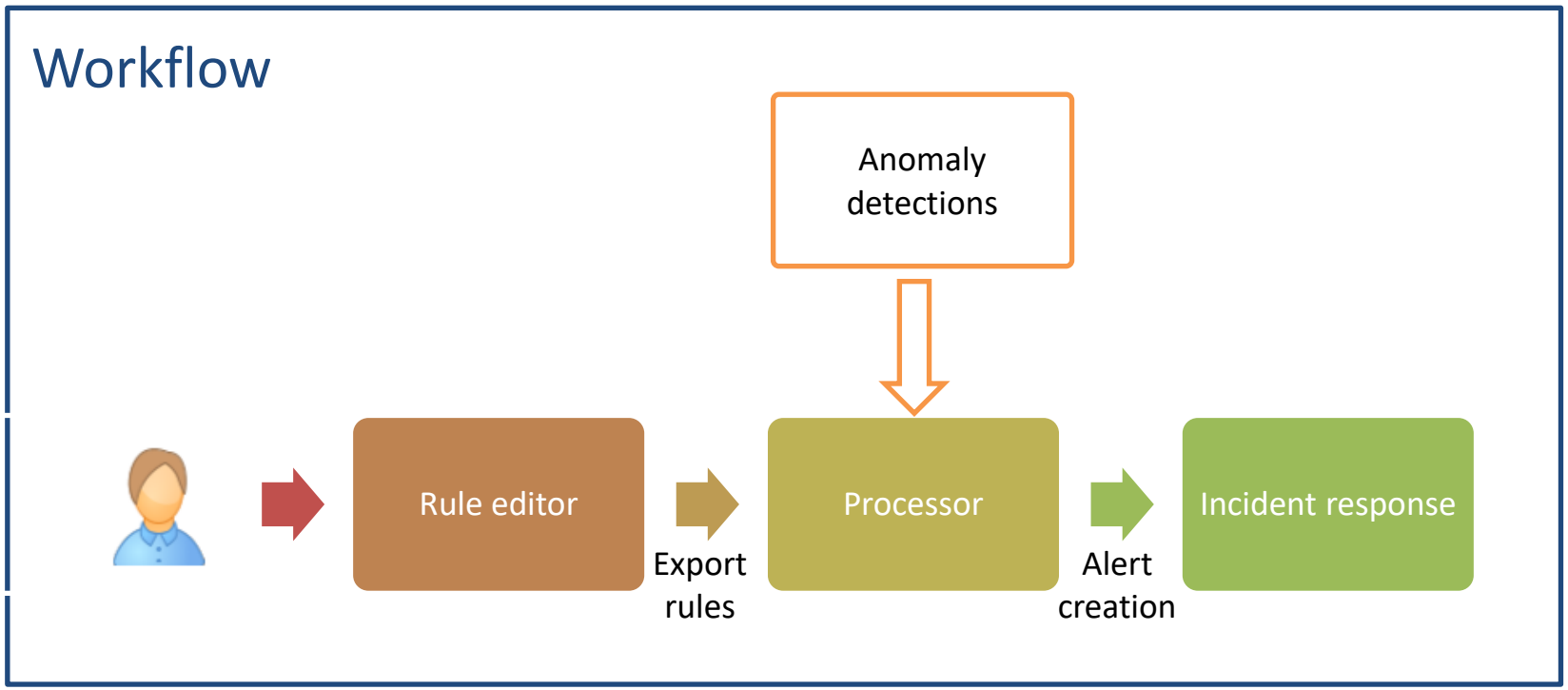
A tool for real-time custom **alert generation** enhanced with **mitigation actions proposition**.

How does it work?

The tool allows the configuration of rules for processing detections (**referring to cyber and physical level**) and, using Complex Event Processing (CEP), it generates important alerts and enriches them with mitigation actions to be taken and extra information that facilitate the operators.

Information is provided instantly for display to the Enhanced Visualization Interface.

Reasoning engine: workflow



STEP 1
Configurable expert rules

STEP2
Real-time/batch processing

STEP3
Enrichment

Reasoning engine: alert generation

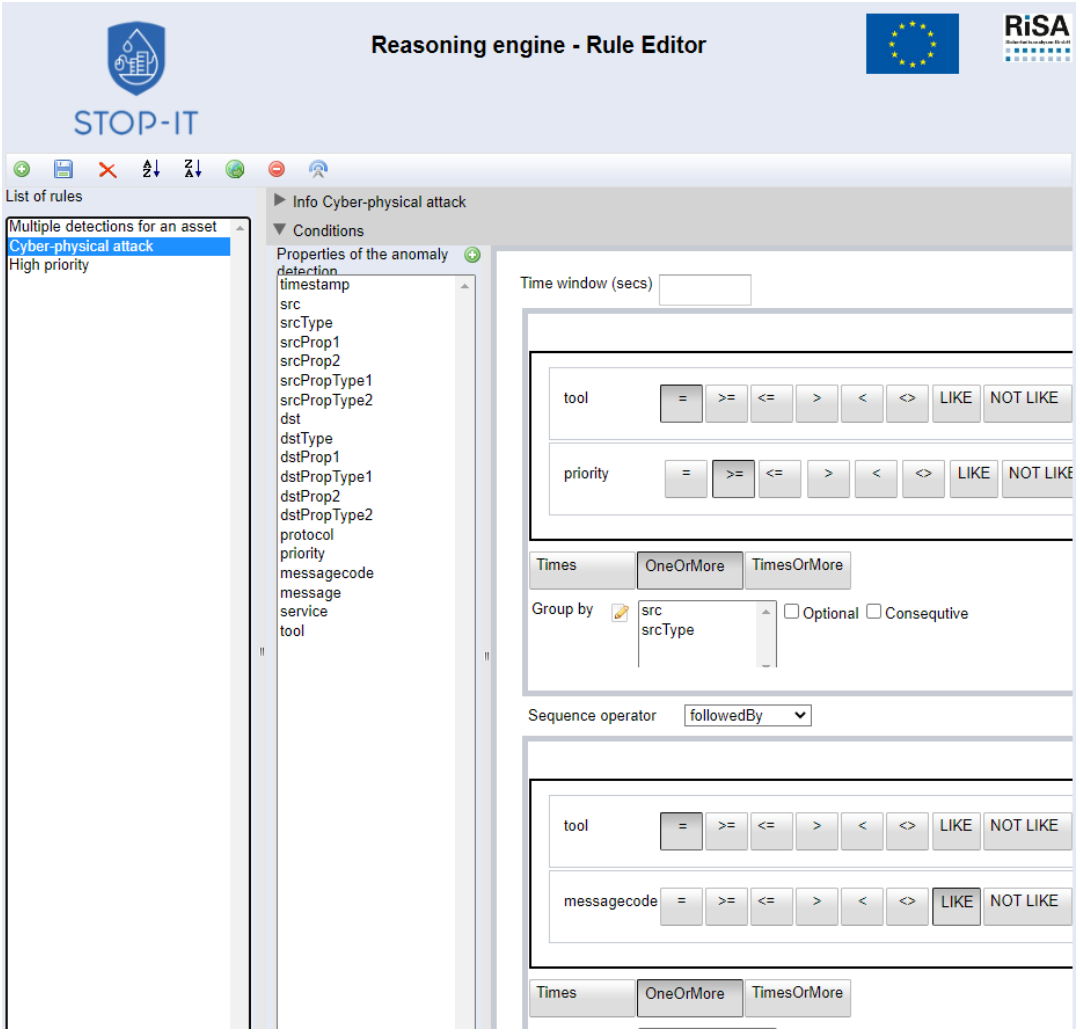
Rule editor: Configuration of a processing rules

Rule definition includes general information,

the patterns that trigger an alarm generation

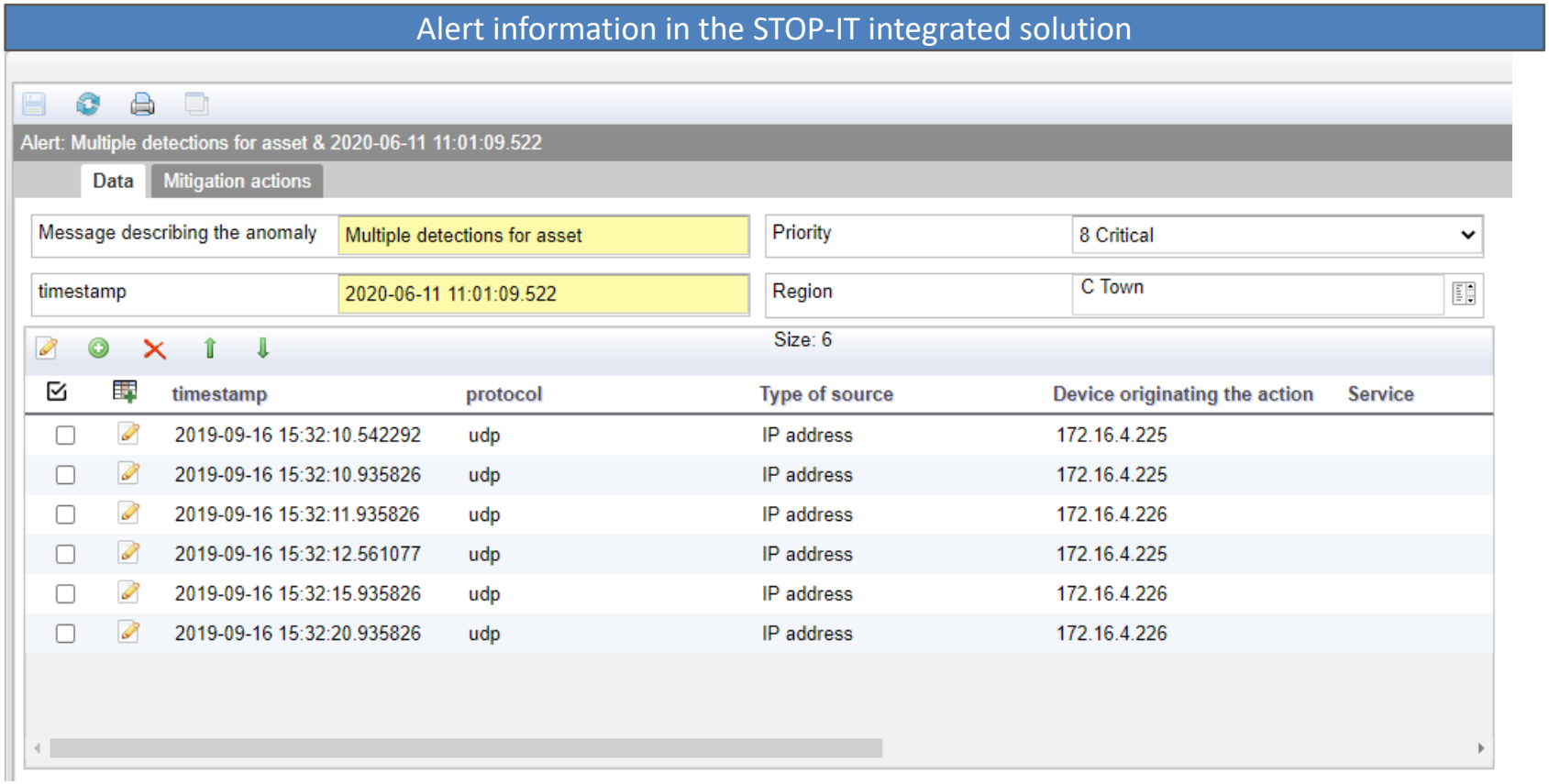
- Individual patterns
  - Simple conditions on the properties
  - Combining conditions with logical constrains
  - Looping conditions
  - Iterative conditions
  - Time constrains
- Combining patterns
  - Individual patterns
  - Contiguity conditions

…and the alert to be generated



Reasoning engine: alert generation

Alert information in the STOP-IT integrated solution



Example alert generated when there are multiple detections (defining a lower and upper limit) for an asset (without specifying any specific asset) within a time window.

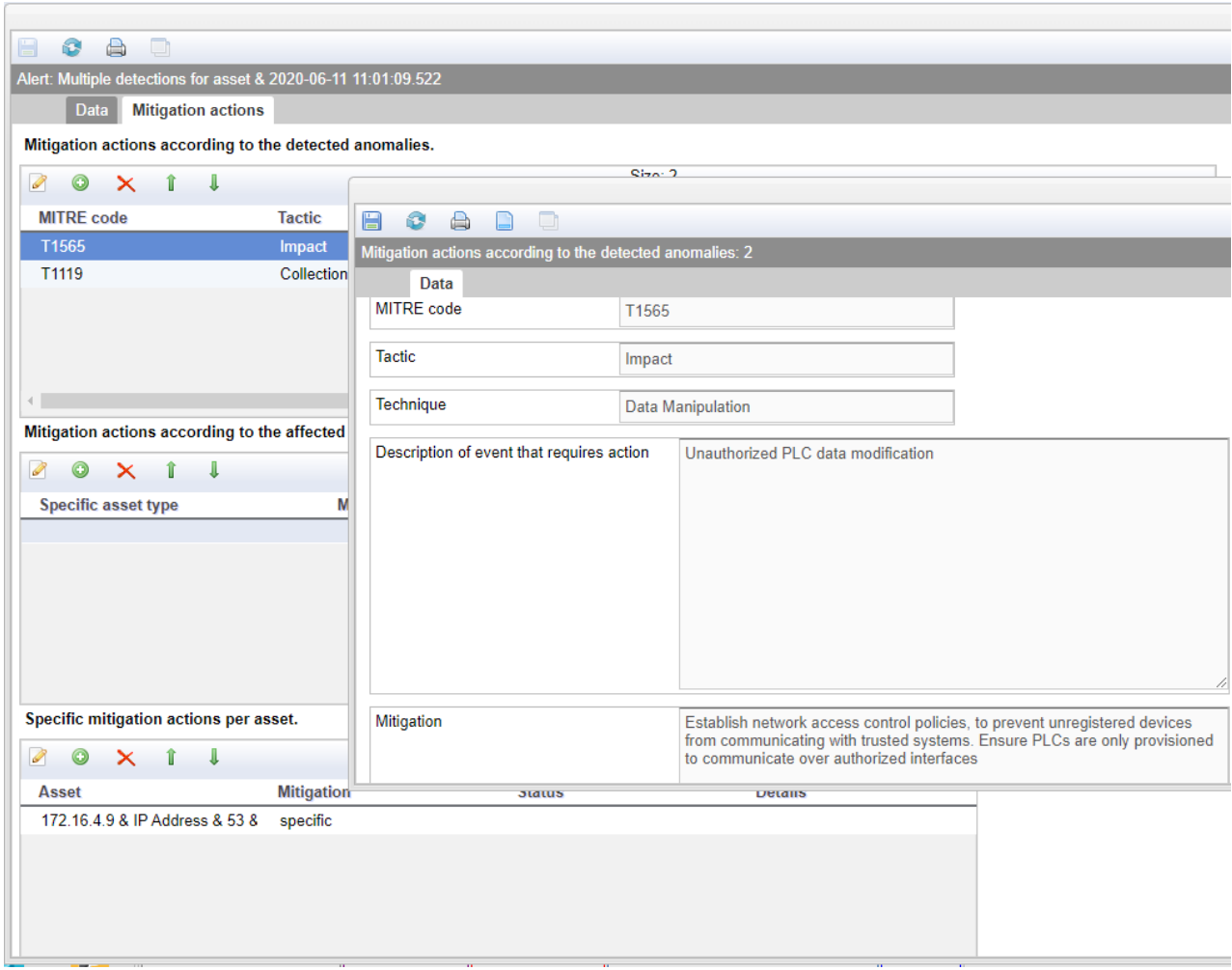
Reasoning engine: mitigation action proposition

Mitigation action proposition

MITRE ATT&CK tactic and technique available to the advice on how to mitigate the technique for the received events. The information is combined to speed investigations and response.

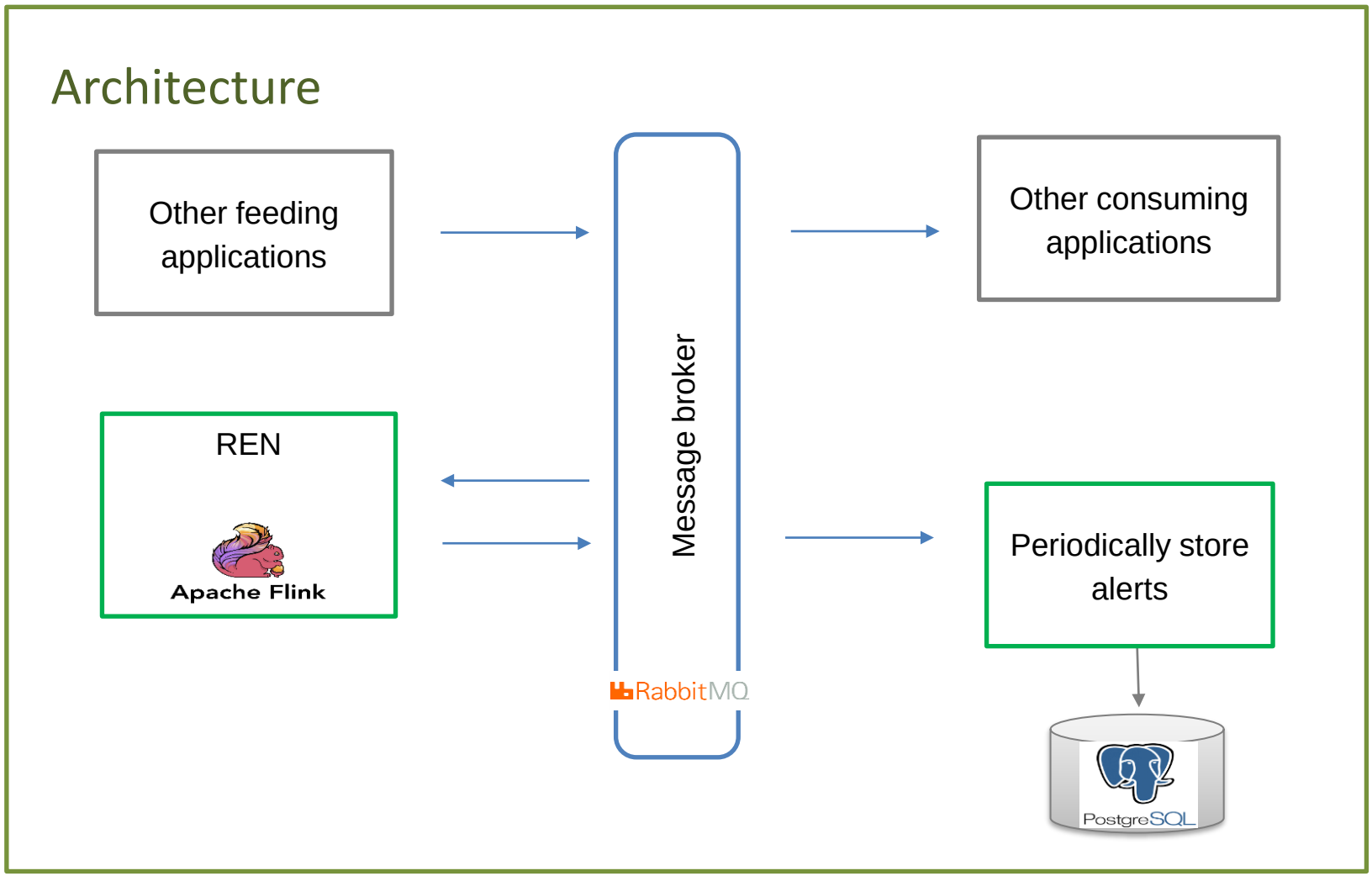
Mitigation actions are also proposed based on the type of affected assets and their specific properties.

To facilitate operators we can use code names for assets and alerts.



Standardized operational data exchange in compliance with the MITRE ATT&CK framework.

Reasoning engine: architecture



What is the Enhanced Visualisation Interface?

The solution offers a common operation picture to provide a shared understanding of the current situation in a water utility.

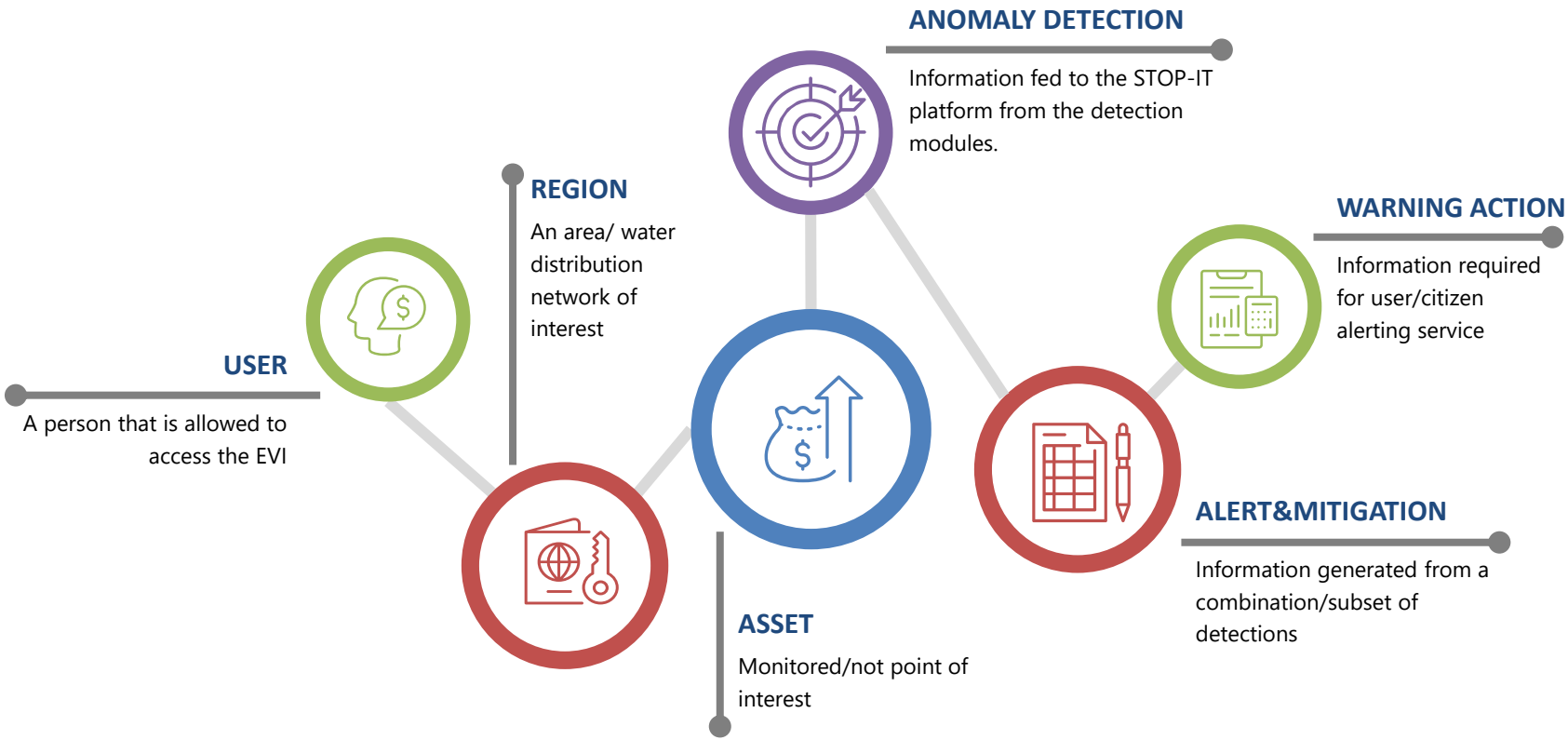
How?

Through a user **customized** web tool that unites a variety of information and applications essential for understanding the CI situation. Information are displayed with multiple perspectives in operational and strategic level. Data sources can vary and indicatively include real-time detections and alerts, GIS mapping data, incident information and mitigation actions.

The module is **scalable** from small businesses to large ones and it can be **expanded** to consume information from other external modules and sources.

Basic concepts

THAT DRIVE THE MODULE AND ITS FEATURES



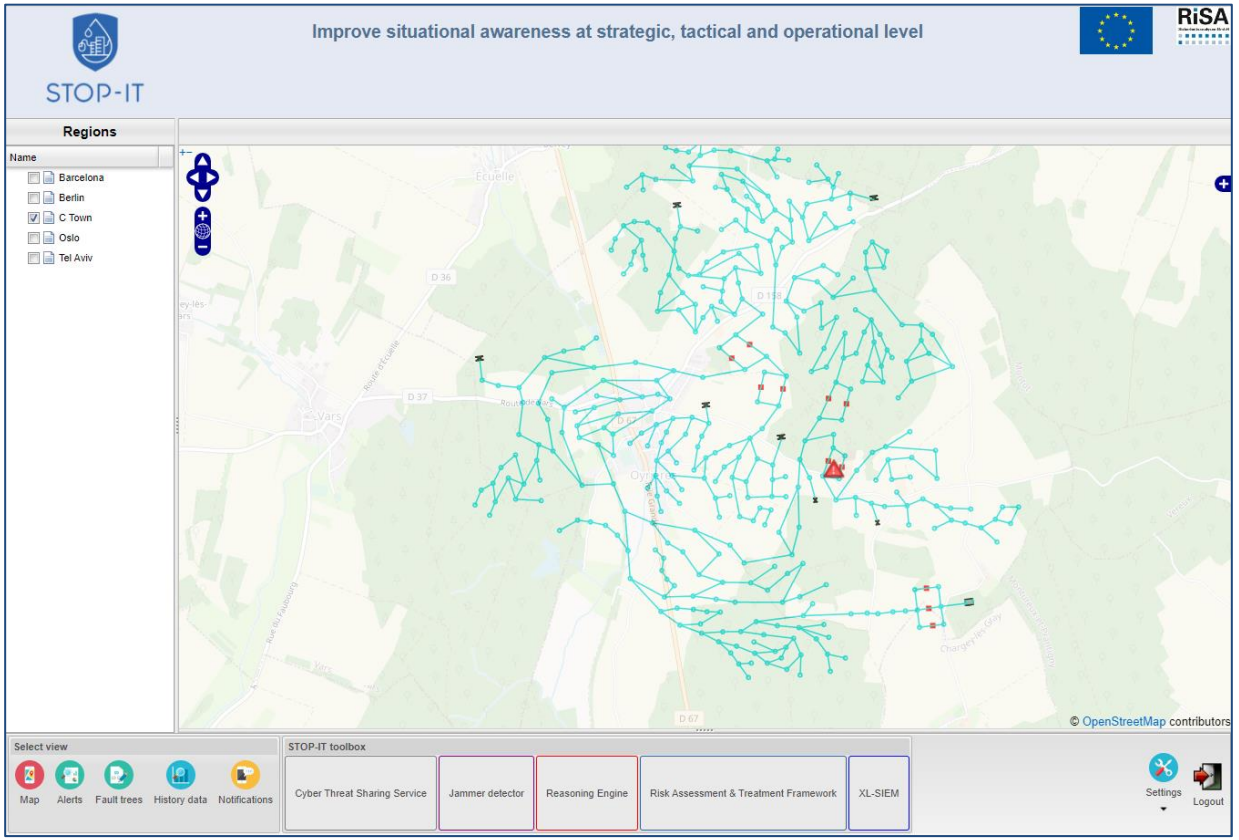
Enhanced visualization interface

- Information organized in multiple views
- Control publishing of data and configuration of displays
- Toolbox of the STOP-IT tools

Map view

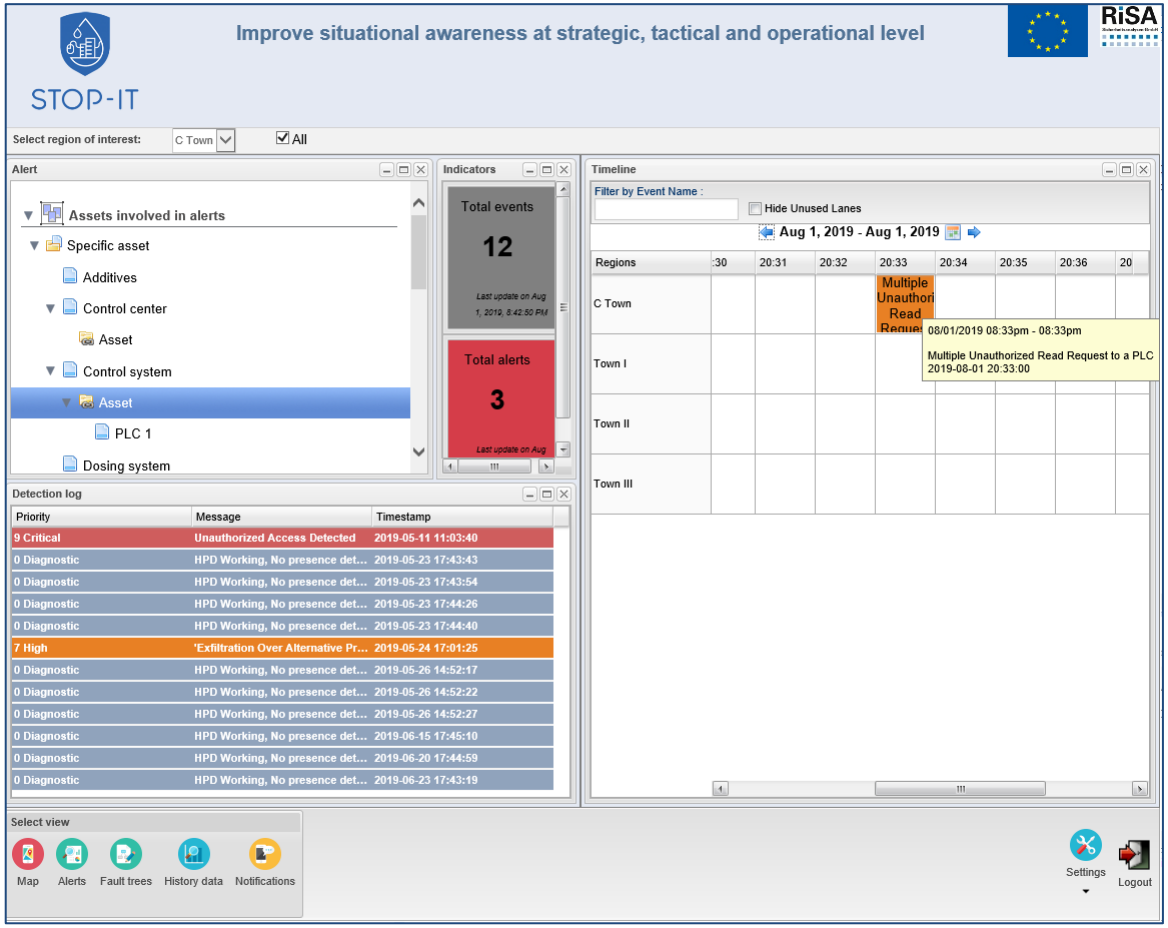
Geographical distribution of alerts in relevance with the WDN

Organized per regions



Enhanced visualization interface

Alert view



Region selector

List of affected assets

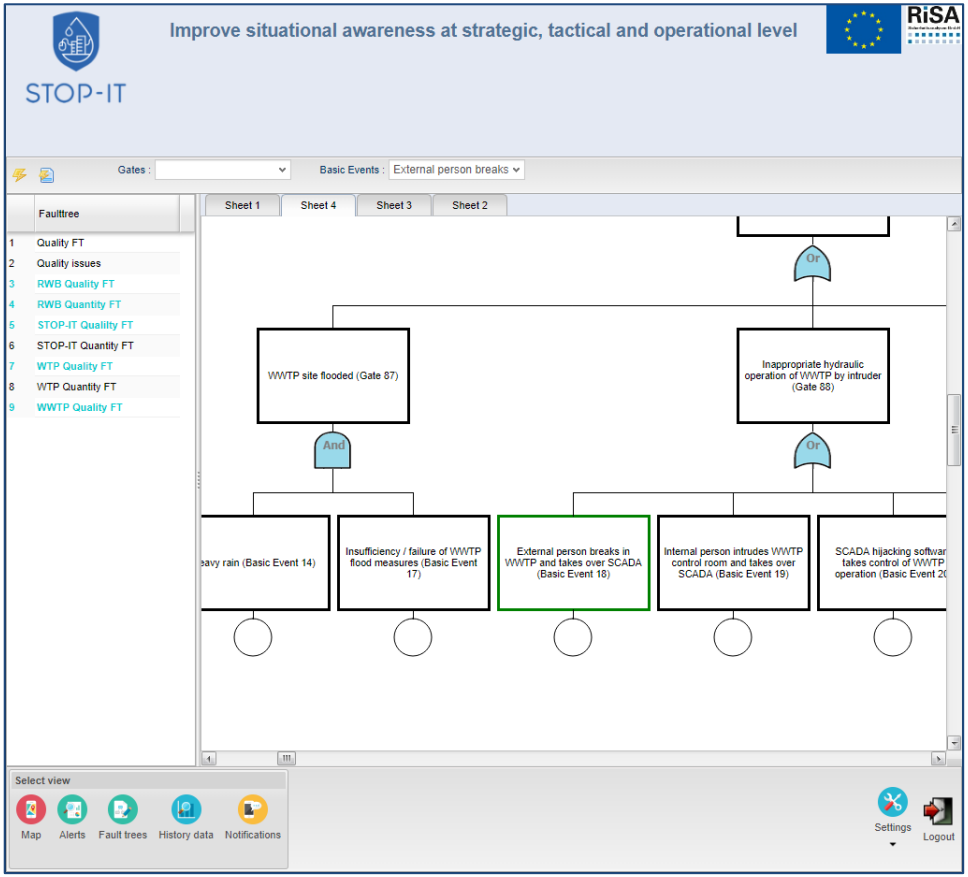
Counters for anomaly detections and alerts

Anomaly detection log with live feeds to the system

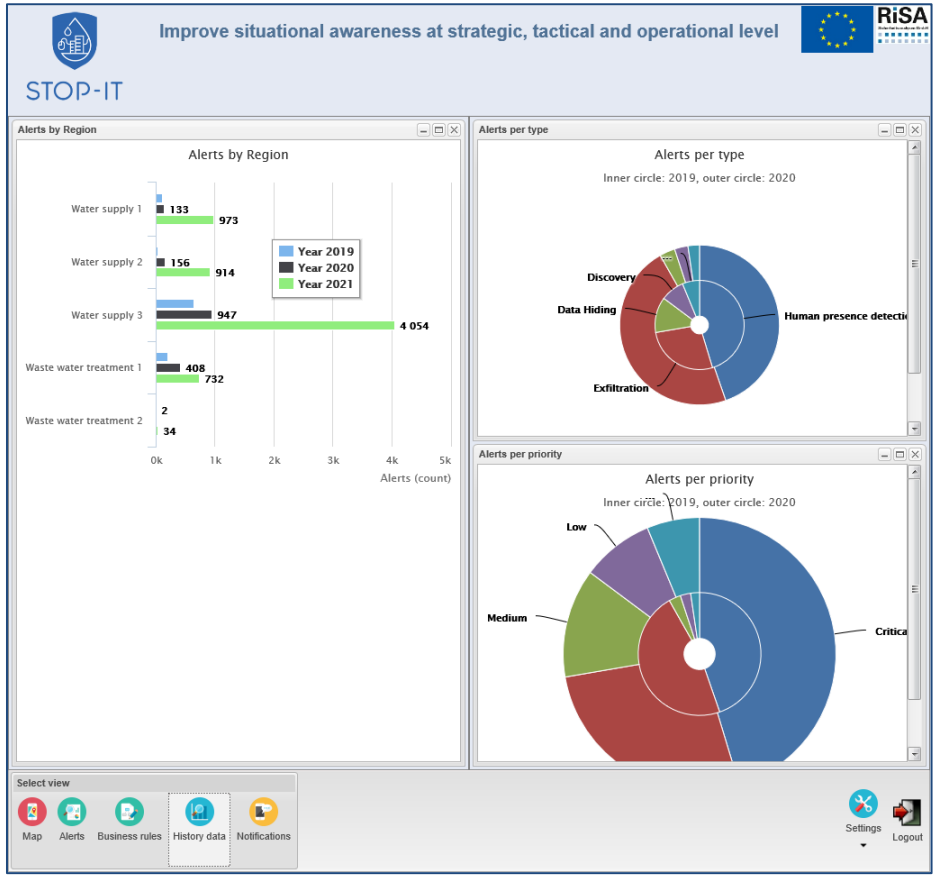
Timeline for alerts

Enhanced visualization interface

Fault tree view

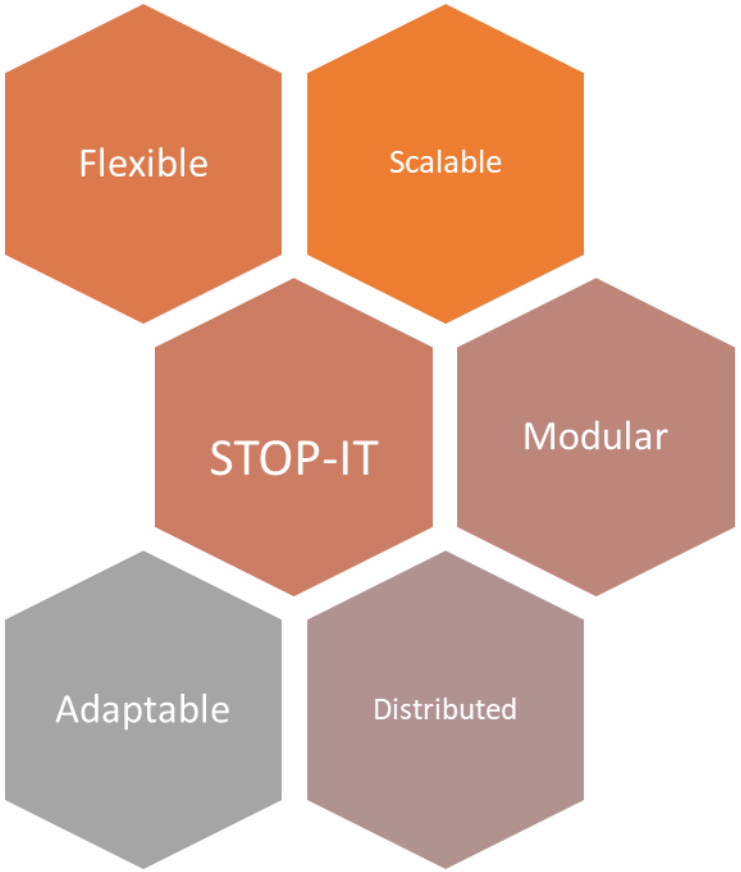


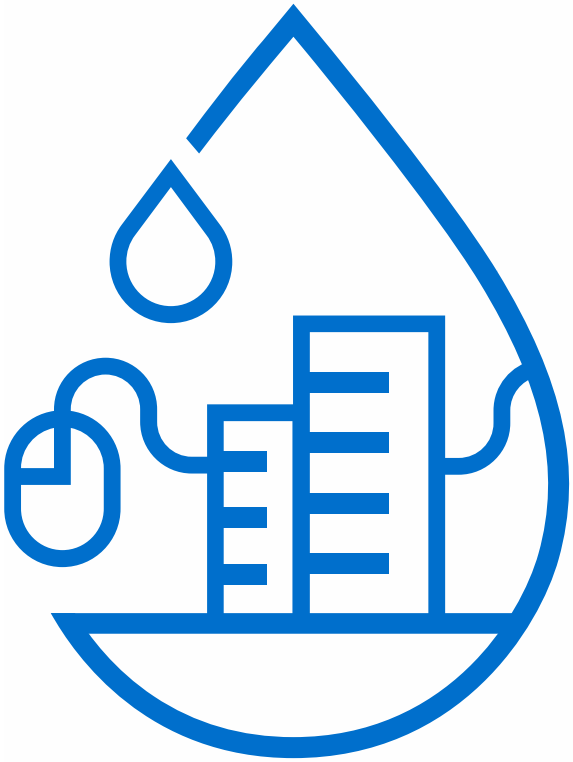
Historical data view



The solutions in deployment

- **Oslo VAV** has selected and will soon start the demonstration of the tools.
- The solutions have a wide application range in **critical infrastructures**.
  - They are also currently deployed and demonstrated in the food processing plants of ELSAP S.A. under the CLARION project for operational monitoring





THANK YOU FOR YOUR ATTENTION

stop-it-project.eu

Theodora Karali
RISA Sicherheitsanalysen GmbH
d.karali@risa.de

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.