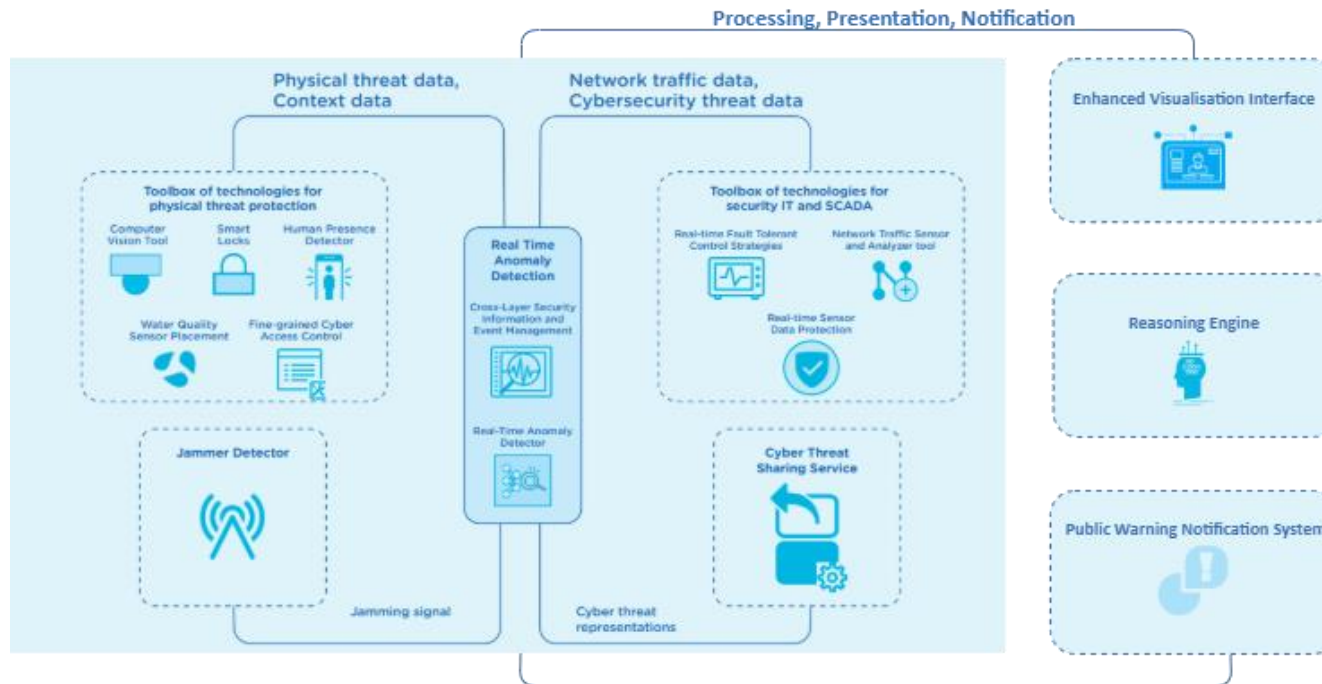




# The STOP-IT Platform

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**

**Develop**

**Integrate**

**Validate**

### ARCHITECTURE

Design the security framework.

### MODULES

Development of solutions that cover presentation, notification and processing needs

### PLATFORM

Combine modules into an integrated whole

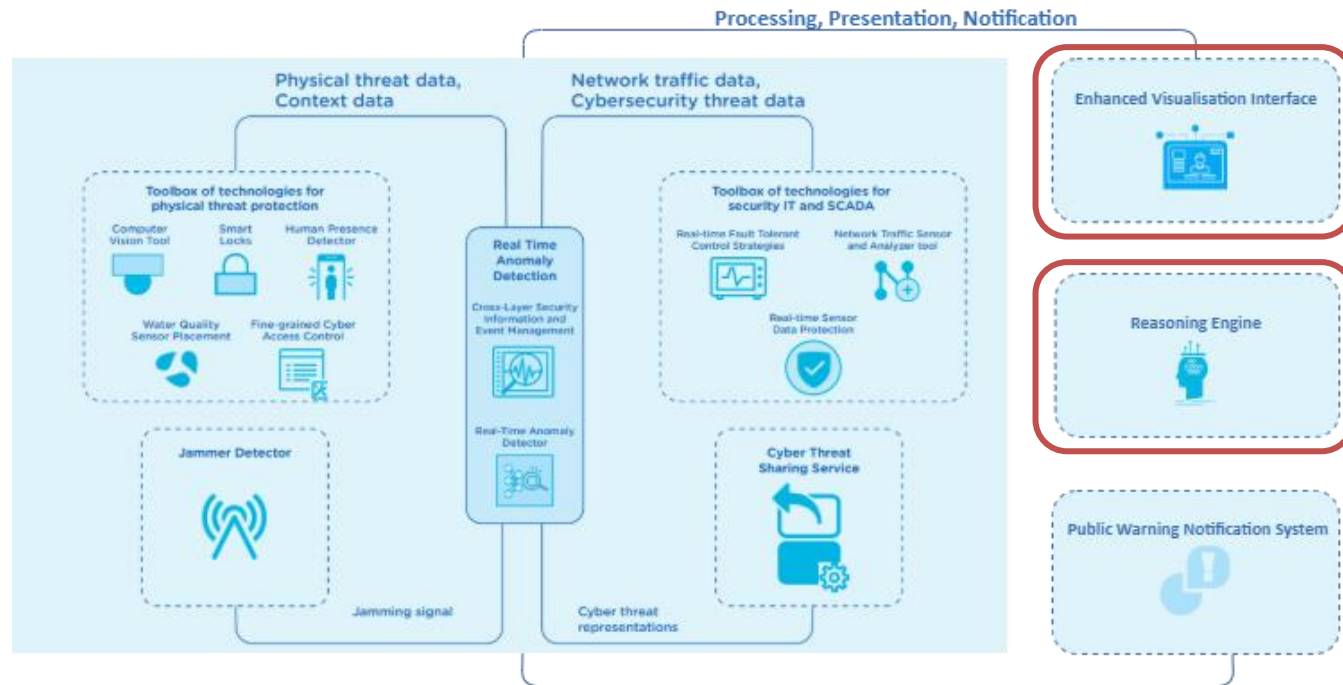
### PROTOTYPE

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.



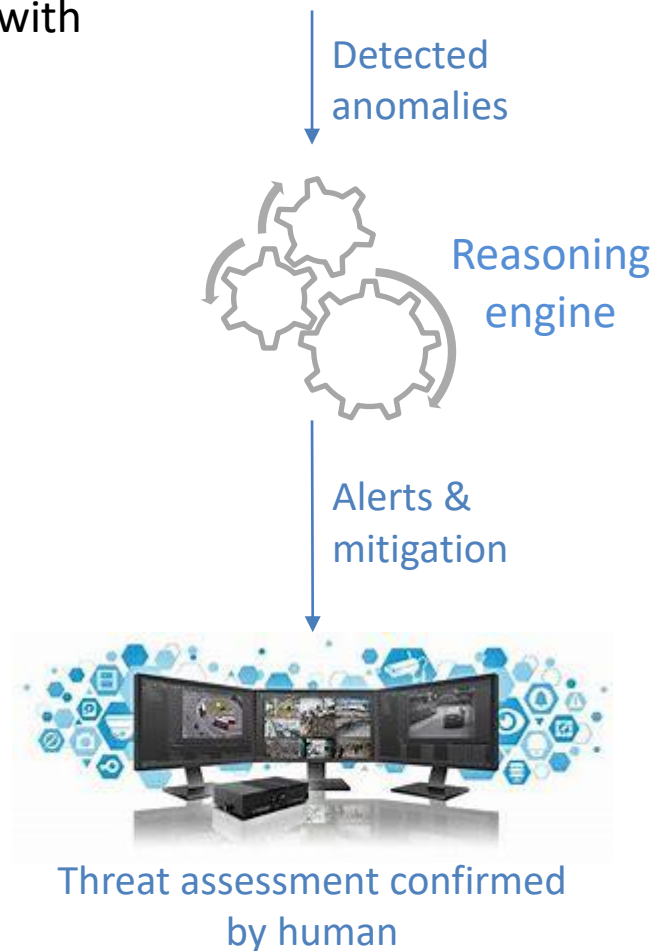


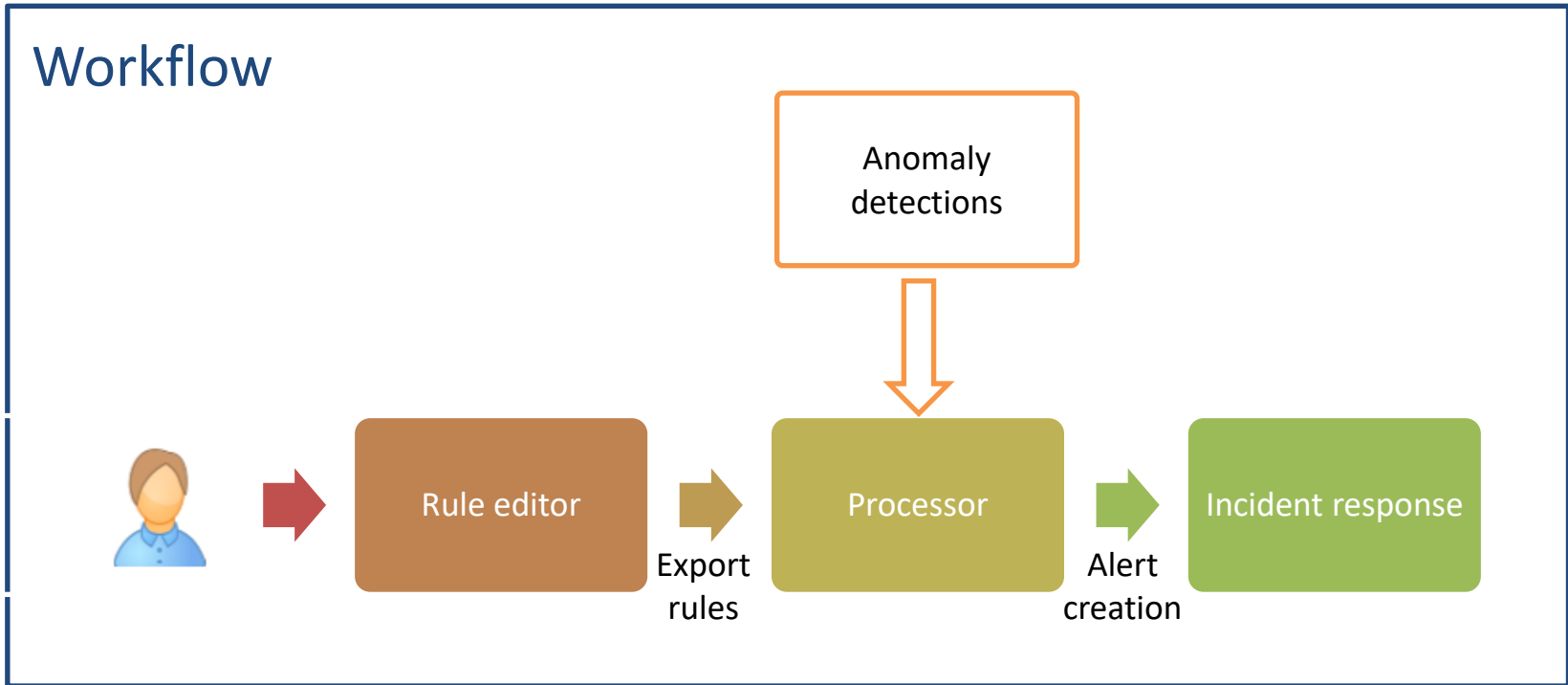
A tool for real-time custom **alert generation** enhanced with **mitigation actions proposition**.

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.





*STEP 1*  
Configurable  
expert rules



*STEP 2*  
Real-time/batch  
processing



*STEP 3*  
Enrichment



## 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

The screenshot displays the 'Reasoning engine - Rule Editor' interface. At the top, there are logos for STOP-IT, the European Union, and RiSA. The main window is titled 'Info Cyber-physical attack'. On the left, a 'List of rules' pane shows 'Multiple detections for an asset', 'Cyber-physical attack' (highlighted), and 'High priority'. The central pane, 'Properties of the anomaly', lists various attributes: detection, timestamp, src, srcType, srcProp1, srcProp2, srcPropType1, srcPropType2, dst, dstType, dstProp1, dstPropType1, dstProp2, dstPropType2, protocol, priority, messagecode, message, service, and tool. The right-hand side contains several configuration sections: a 'Time window (secs)' input field; a 'tool' configuration with comparison operators (=, >=, <=, >, <, <>) and 'LIKE', 'NOT LIKE' options; a 'priority' configuration with similar operators and options; a 'Times' section with 'OneOrMore' and 'TimesOrMore' buttons; a 'Group by' section with a dropdown menu showing 'src' and 'srcType', and checkboxes for 'Optional' and 'Consecutive'; a 'Sequence operator' dropdown set to 'followedBy'; and a final configuration section for 'tool' and 'messagecode' with comparison operators and 'LIKE', 'NOT LIKE' options.



Alert information in the STOP-IT integrated solution

Alert: Multiple detections for asset & 2020-06-11 11:01:09.522

**Data** Mitigation actions

Message describing the anomaly: Multiple detections for asset

Priority: 8 Critical

timestamp: 2020-06-11 11:01:09.522

Region: C Town

Size: 6

<input type="checkbox"/>		timestamp	protocol	Type of source	Device originating the action	Service
<input type="checkbox"/>		2019-09-16 15:32:10.542292	udp	IP address	172.16.4.225	
<input type="checkbox"/>		2019-09-16 15:32:10.935826	udp	IP address	172.16.4.225	
<input type="checkbox"/>		2019-09-16 15:32:11.935826	udp	IP address	172.16.4.226	
<input type="checkbox"/>		2019-09-16 15:32:12.561077	udp	IP address	172.16.4.225	
<input type="checkbox"/>		2019-09-16 15:32:15.935826	udp	IP address	172.16.4.226	
<input type="checkbox"/>		2019-09-16 15:32:20.935826	udp	IP address	172.16.4.226	

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.



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.

## Mitigation action proposition

The screenshot displays a web interface for alert management. At the top, an alert is shown: "Alert: Multiple detections for asset & 2020-06-11 11:01:09.522". Below this, there are two main panels. The left panel, titled "Mitigation actions according to the detected anomalies", shows a table with the following data:

MITRE code	Tactic
T1565	Impact
T1119	Collection

The right panel, titled "Mitigation actions according to the detected anomalies: 2", shows a detailed view for a specific tactic. It includes the following information:

- MITRE code: T1565
- Tactic: Impact
- Technique: Data Manipulation
- Description of event that requires action: Unauthorized PLC data modification
- Mitigation: Establish network access control policies, to prevent unregistered devices from communicating with trusted systems. Ensure PLCs are only provisioned to communicate over authorized interfaces

At the bottom of the interface, there is a table for "Specific mitigation actions per asset":

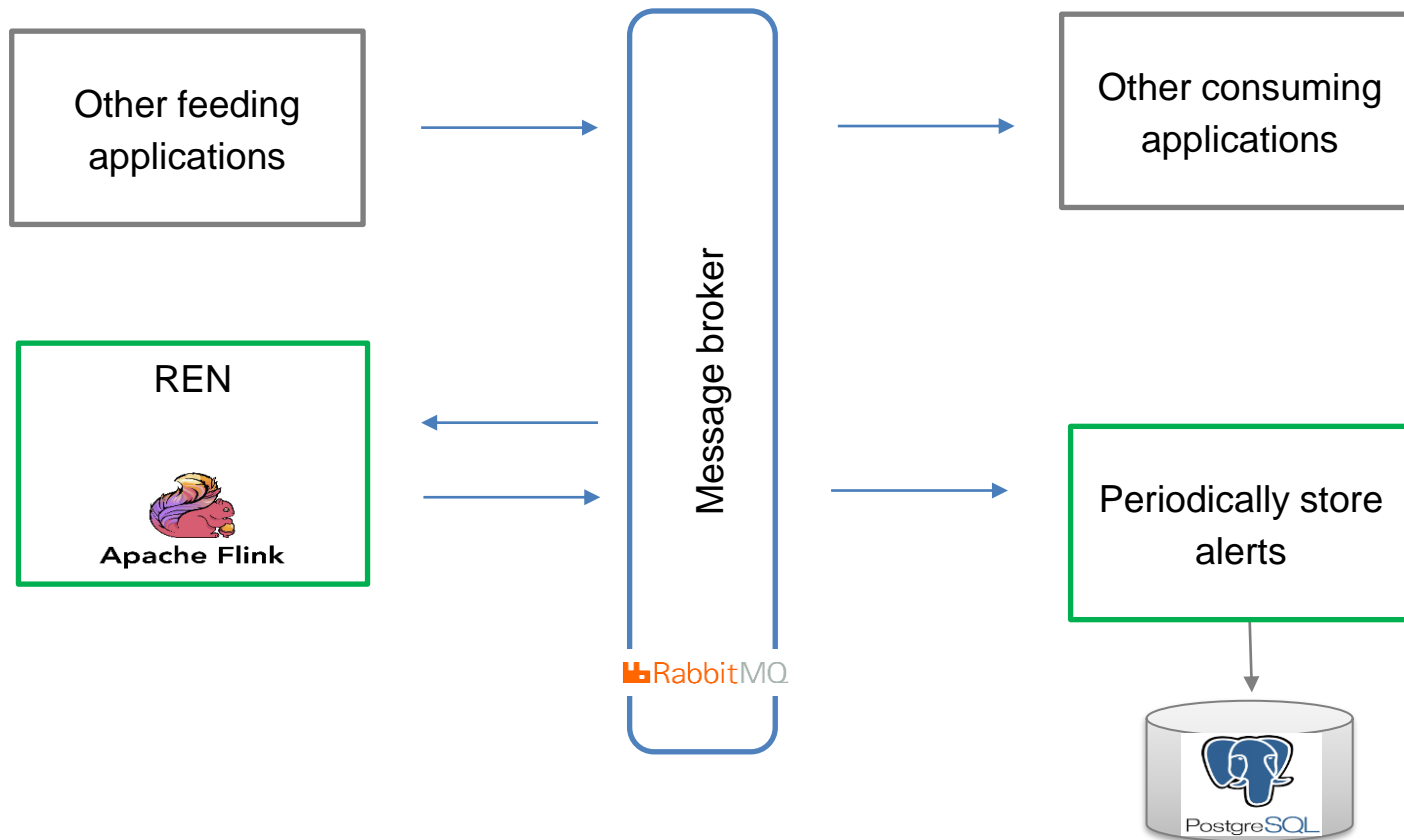
Asset	Mitigation
172.16.4.9 & IP Address & 53 &	specific

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





## Architecture





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

How?

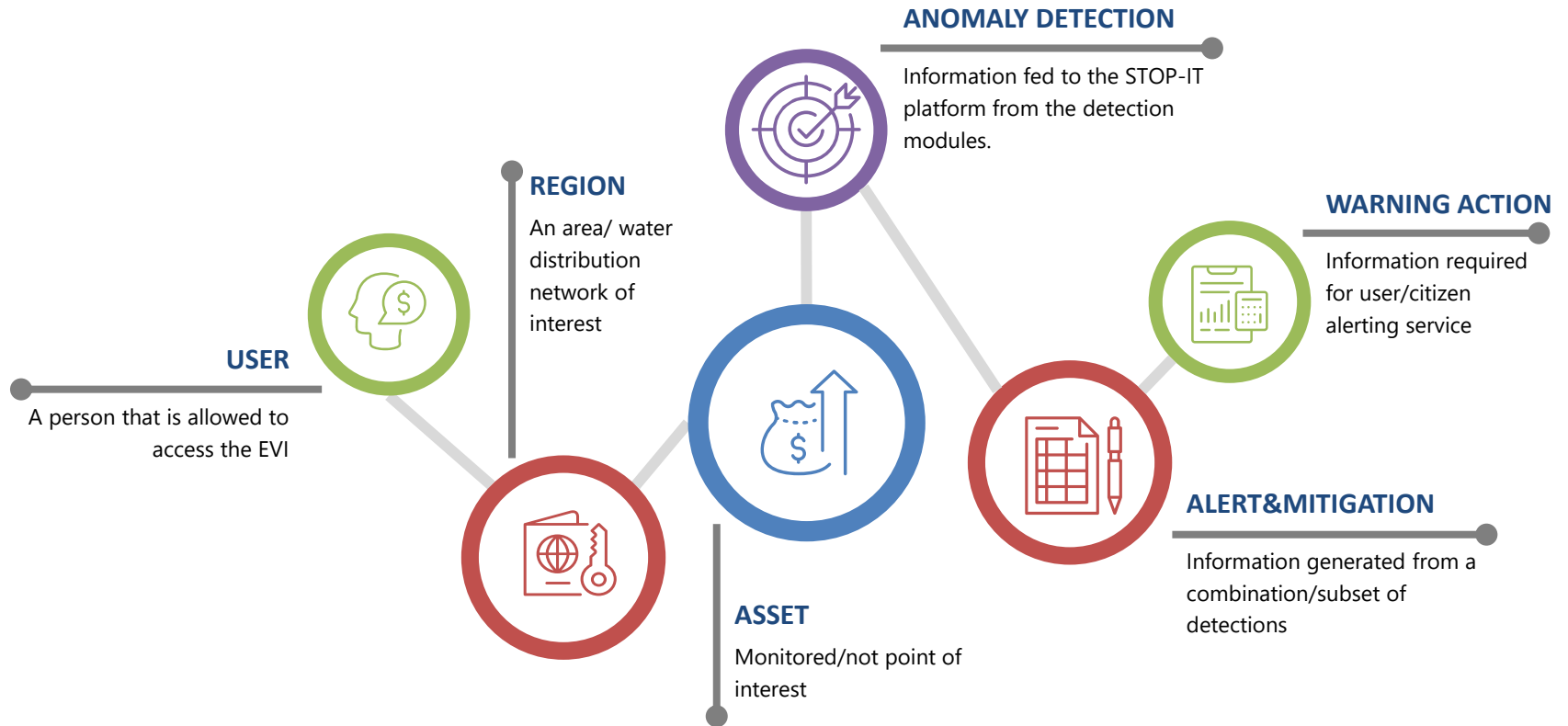
Through a user **customized** web tool that unites a variety of information and applications essential for understanding the CI situation. Information are displayed with multiple perspectives in operational and strategic level. Data sources can vary and indicatively include real-time detections and alerts,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





- ❖ 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

STOP-IT

Improve situational awareness at strategic, tactical and operational level

RiSA

Regions

Name

- Barcelona
- Berlin
- C Town
- Oslo
- Tel Aviv

Select view

Map Alerts Fault trees History data Notifications

STOP-IT toolbox

Cyber Threat Sharing Service Jammer detector Reasoning Engine Risk Assessment & Treatment Framework XL-SIEM

Settings Logout



### Alert view

Improve situational awareness at strategic, tactical and operational level

STOP-IT

Select region of interest: C Town  All

**Alert**

- Assets involved in alerts
  - Specific asset
    - Additives
  - Control center
    - Asset
  - Control system
    - Asset
    - PLC 1
    - Dosing system

**Indicators**

- Total events: 12 (Last update on Aug 1, 2019, 8:42:50 PM)
- Total alerts: 3 (Last update on Aug 1, 2019, 8:42:50 PM)

**Timeline**

Filter by Event Name:  Hide Unused Lanes

Aug 1, 2019 - Aug 1, 2019

Regions	:30	20:31	20:32	20:33	20:34	20:35	20:36	20
C Town				Multiple Unauthor Read Request				
Town I					Multiple Unauthorized Read Request to a PLC 2019-08-01 20:33:00			
Town II								
Town III								

**Detection log**

Priority	Message	Timestamp
9 Critical	Unauthorized Access Detected	2019-05-11 11:03:40
0 Diagnostic	HPD Working, No presence det...	2019-05-23 17:43:43
0 Diagnostic	HPD Working, No presence det...	2019-05-23 17:43:54
0 Diagnostic	HPD Working, No presence det...	2019-05-23 17:44:26
0 Diagnostic	HPD Working, No presence det...	2019-05-23 17:44:40
7 High	'Exfiltration Over Alternative Pr...	2019-05-24 17:01:25
0 Diagnostic	HPD Working, No presence det...	2019-05-26 14:52:17
0 Diagnostic	HPD Working, No presence det...	2019-05-26 14:52:22
0 Diagnostic	HPD Working, No presence det...	2019-05-26 14:52:27
0 Diagnostic	HPD Working, No presence det...	2019-06-15 17:45:10
0 Diagnostic	HPD Working, No presence det...	2019-06-20 17:44:59
0 Diagnostic	HPD Working, No presence det...	2019-06-23 17:43:19

Select view: Map Alerts Fault trees History data Notifications

Settings Logout

Region selector

List of affected assets

Counters for anomaly detections and alerts

Anomaly detection log with live feeds to the system

Timeline for alerts



## Fault tree view

Improve situational awareness at strategic, tactical and operational level

STOP-IT

Gates: [dropdown] Basic Events: External person breaks

Faulttree

Sheet 1 Sheet 4 Sheet 3 Sheet 2

1 Quality FT  
2 Quality issues  
3 RWB Quality FT  
4 RWB Quantity FT  
5 STOP-IT Quality FT  
6 STOP-IT Quantity FT  
7 WTP Quality FT  
8 WTP Quantity FT  
9 WWTP Quality FT

WWTP site flooded (Gate 87)

Inappropriate hydraulic operation of WWTP by intruder (Gate 88)

Heavy rain (Basic Event 14)

Insufficiency / failure of WWTP flood measures (Basic Event 17)

External person breaks in WWTP and takes over SCADA (Basic Event 18)

Internal person intrudes WWTP control room and takes over SCADA (Basic Event 19)

SCADA hijacking software takes control of WWTP operation (Basic Event 20)

Select view: Map Alerts Fault trees History data Notifications

Settings Logout

## Historical data view

Improve situational awareness at strategic, tactical and operational level

STOP-IT

Alerts by Region

Region	Year 2019	Year 2020	Year 2021
Water supply 1	133	973	
Water supply 2	156	914	
Water supply 3		947	4 054
Waste water treatment 1	408	732	
Waste water treatment 2	34		

Alerts per type

Inner circle: 2019, outer circle: 2020

Discovery

Data Hiding

Exfiltration

Human presence detect

Alerts per priority

Inner circle: 2019, outer circle: 2020

Low

Medium

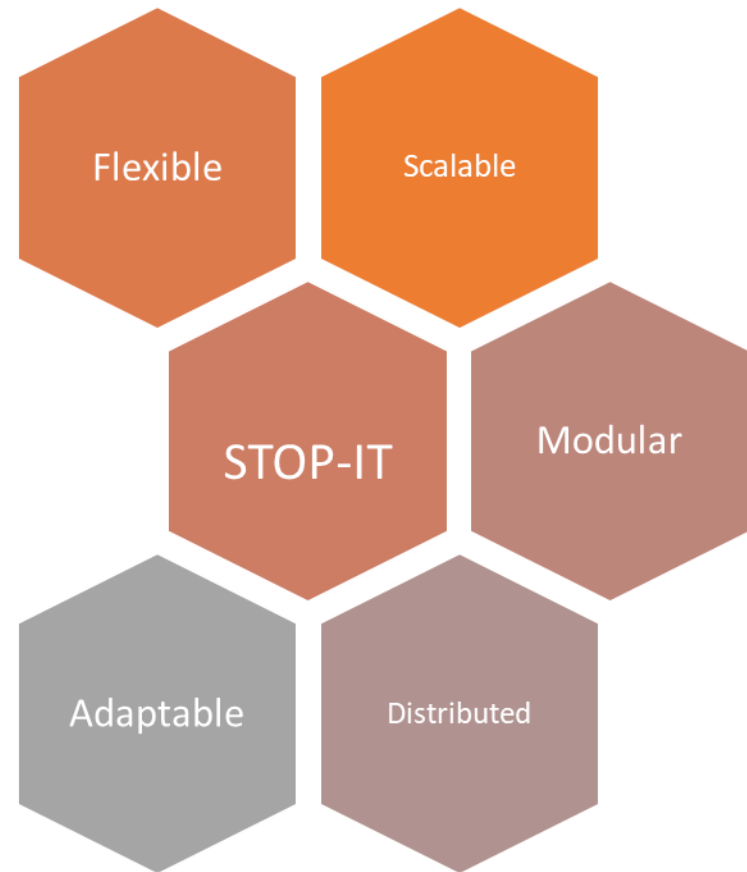
Critical

Select view: Map Alerts Business rules History data Notifications

Settings Logout

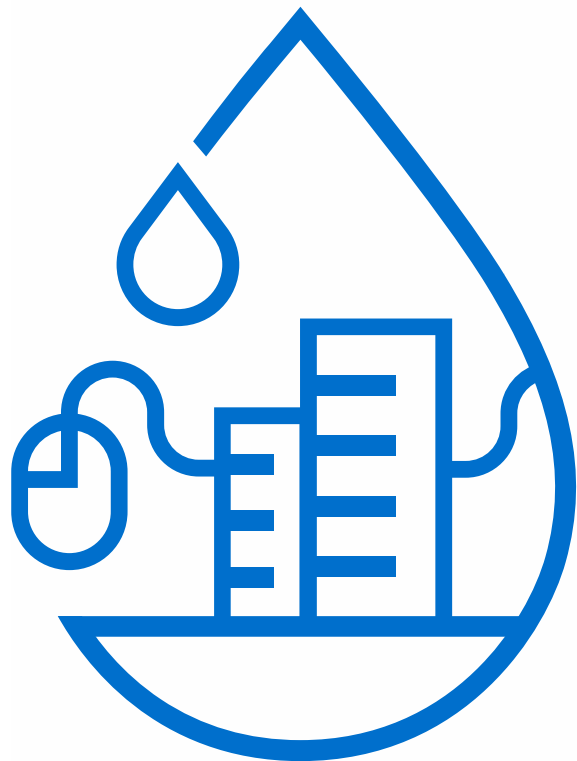


- **Oslo VAV** has selected and will soon start the demonstration of the tools.
- The solutions have a wide application range in **critical infrastructures**.
  - They are also currently deployed and demonstrated in the food processing plants of ELSAP S.A. under the CLARION project for operational monitoring





STOP-IT



STOP-IT

**THANK YOU FOR YOUR  
ATTENTION**

[stop-it-project.eu](http://stop-it-project.eu)

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

