H2020 STOP-IT PROJECT

Enhancing the security of water critical infrastructure at strategic, tactical and operational level with solutions for preventing, detecting, responding to, and recovering from cyber and physical threats.

www.stop-it-project.eu

Physical and Cyber security integration and modelling at strategic and tactical levels

KWR
National Technical
University of Athens

SPEAKER:

CHRISTOS MAKROPOULOS, PROFESSOR

OUR WORLD IS GOING DIGITAL – FAST!

We are in the middle of a **transformation** from "*physical infrastructure*" to "*physical with some sensors*" to "*cyber-physical infrastructure*"
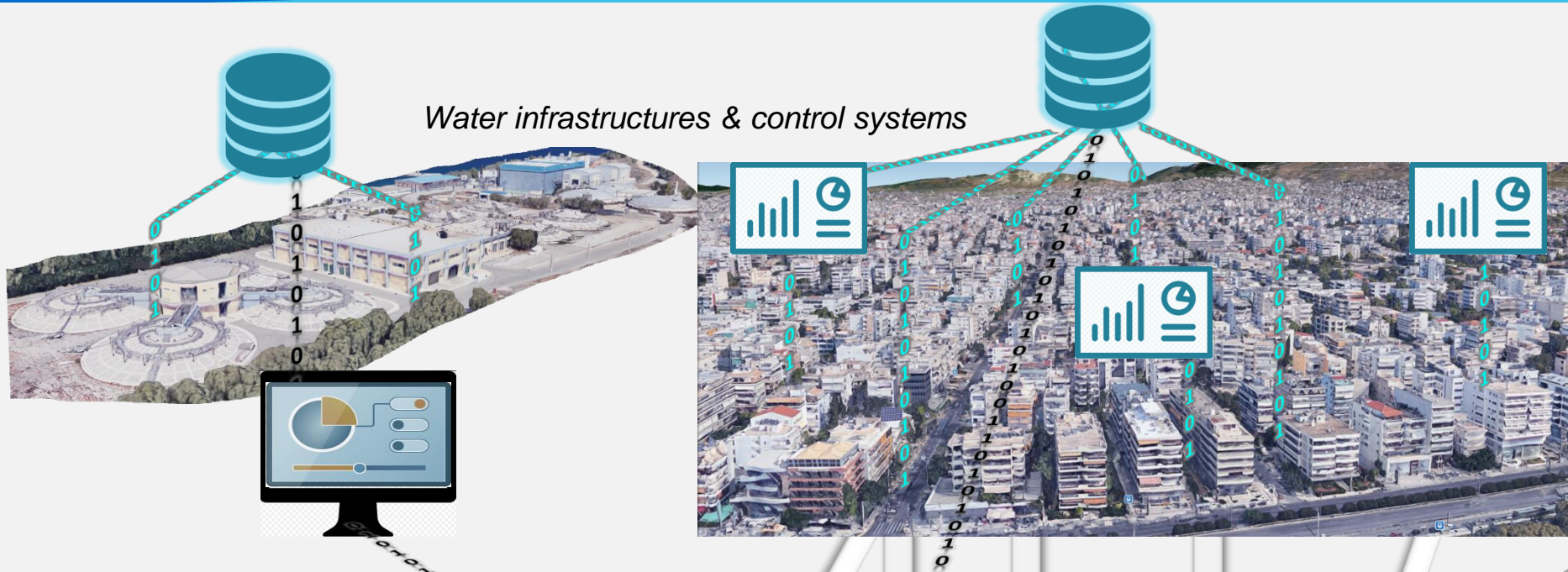
Analog   `Digital`

- **Advantages are numerous**: automation, adaptability, efficiency, functionality, reliability, safety, and usability of large systems
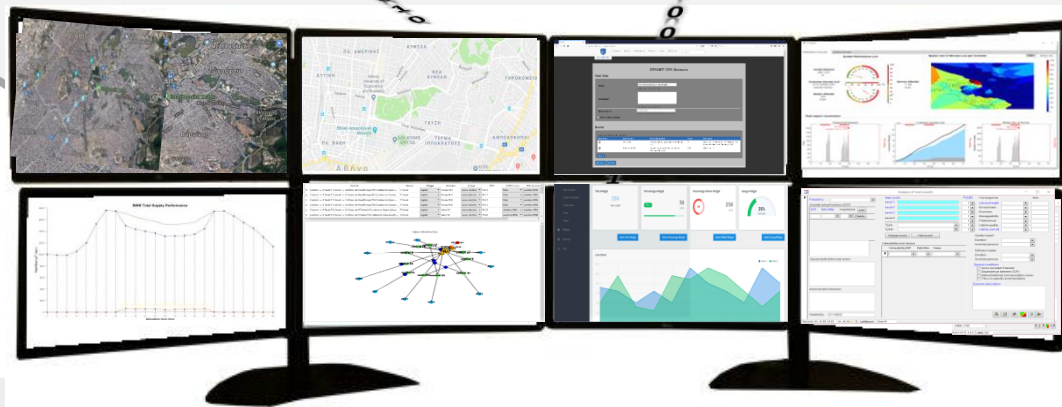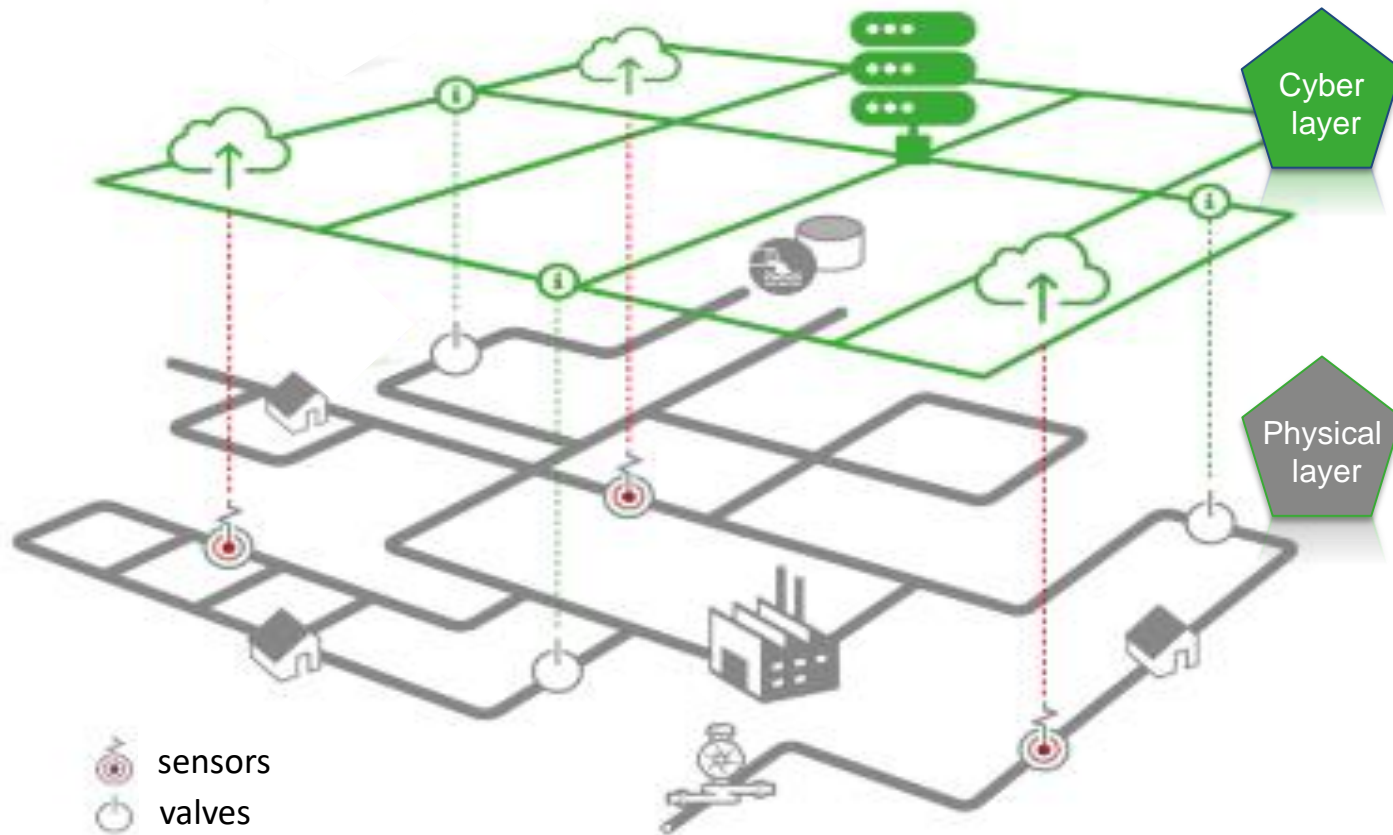- **But there is a catch**: Exposure to an expanded attack surface…

STOP-IT

Water infrastructures & control systems

Water infrastructures
As cyber-physical infrastructures

SCADA room

STOP-IT

Cyber layer

Physical layer

sensors
valves

We argue that since the **cyber** and **physical** systems interact continuously, and **cascading effects** between them are not ease to track (or back-track to improve designs or identify sources of attacks) we need to combine cyber and hydraulic engineering knowledge to develop **cyber-physical security concepts and tools**.

STOP-IT

Modular components of
the STOP-IT risk management platform
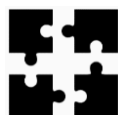
Operational

Strategic & Tactical

Solutions that support:

- **Strategic/tactical planning and post action assessment**
- **Operational decision making**

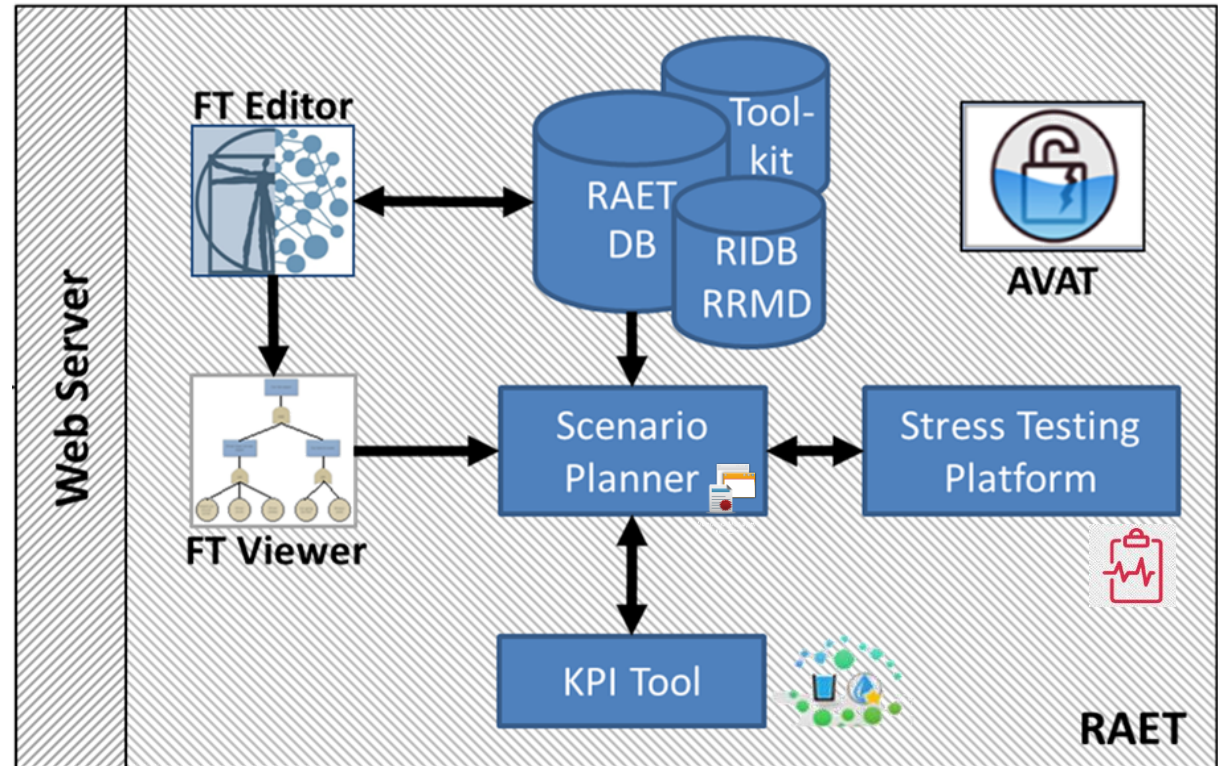towards cyber-physical security of water infrastructures

Scalable　　**Adaptable**　　**Flexible**

STOP-IT modules:

- ❑ **Module1: Risk Assessment & Treatment Framework**

- ❑ Module 2: Secure wireless sensor communications module

- ❑ Module 3: Toolbox of technologies for securing IT and SCADA

- ❑ Module 4:Toolbox of technologies for protecting against physical threats in CI

- ❑ Module 5: Cyber Threat Incident Service

- ❑ Module 6: Real-Time anomaly detection system

- ❑ Module 7: Public Warning System-Secure Information Exchange Technologies

- ❑ Module 8:Reasoning Engine

- ❑ Module 9: Enhanced Visualisation Interface for the water utilities

STOP-IT

Risk Identification

Asset Vulnerability Assessment

Analysis

Risk Evaluation

Treatment Analysis

Treatment Evaluation

High level use-cases of Module I components:

1. **Assess vulnerability (AVAT)**
2. **Navigate through potential risks & design/configure** multiple **risks scenarios**
3. **Simulate physical** system interacting with their **cyber layer**
4. **Visualise system's response and quantify/assess** overall **impacts**
5. **Assess scenarios of measure(s) implementation** to the system
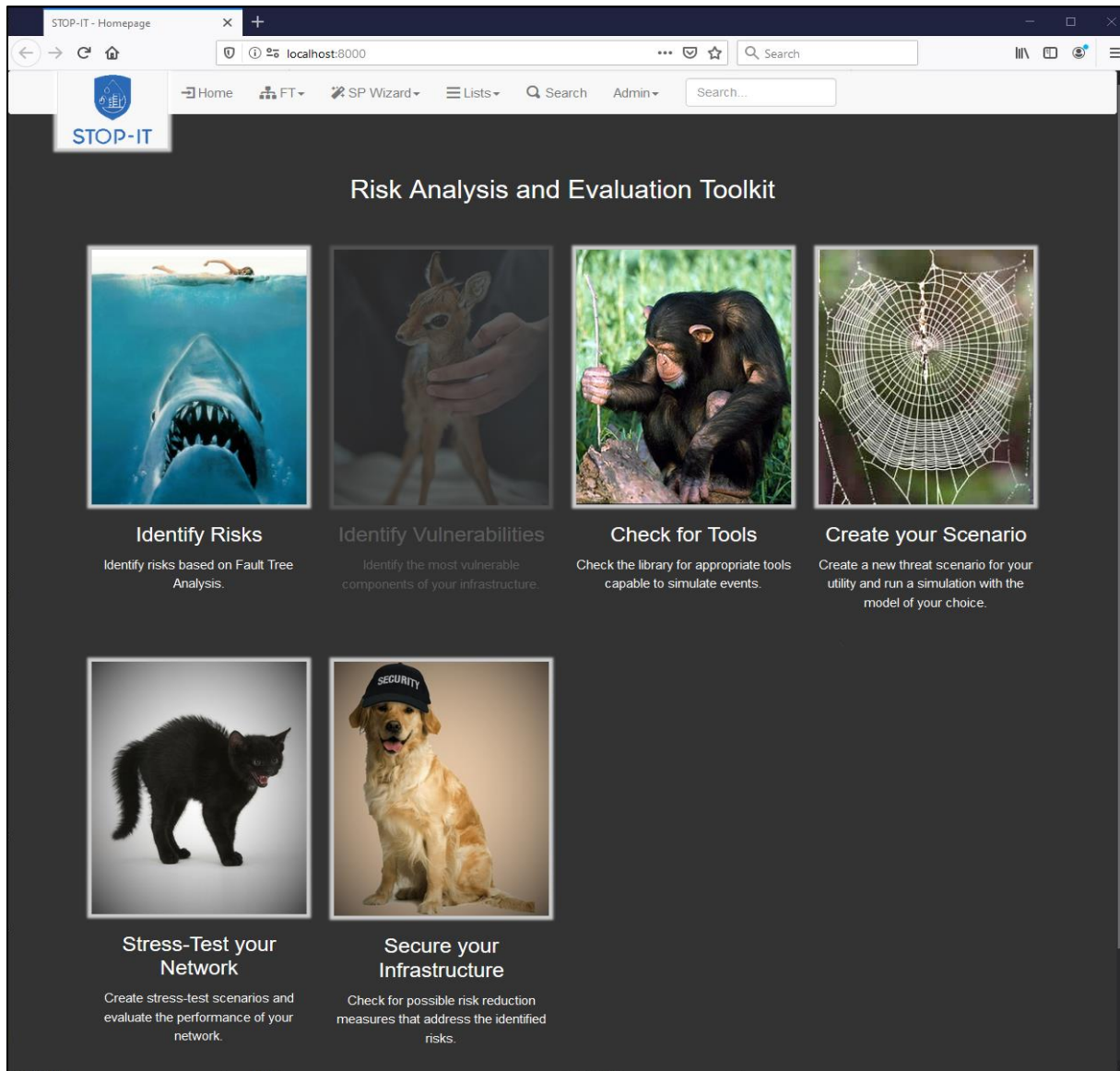
- ❑ **Scenario Planner**
  Identify risks and build a network specific **threat scenario**

- ❑ **Stress Test Platform**
  Simulate the scenario

- ❑ **KPI tool**
  Evaluate the scenario consequences

- ❑ **Scenario Planner**
  Explore appropriate **treatment** options

A **user-friendly graphical environment** for the investigation of threat and cascading effect scenarios
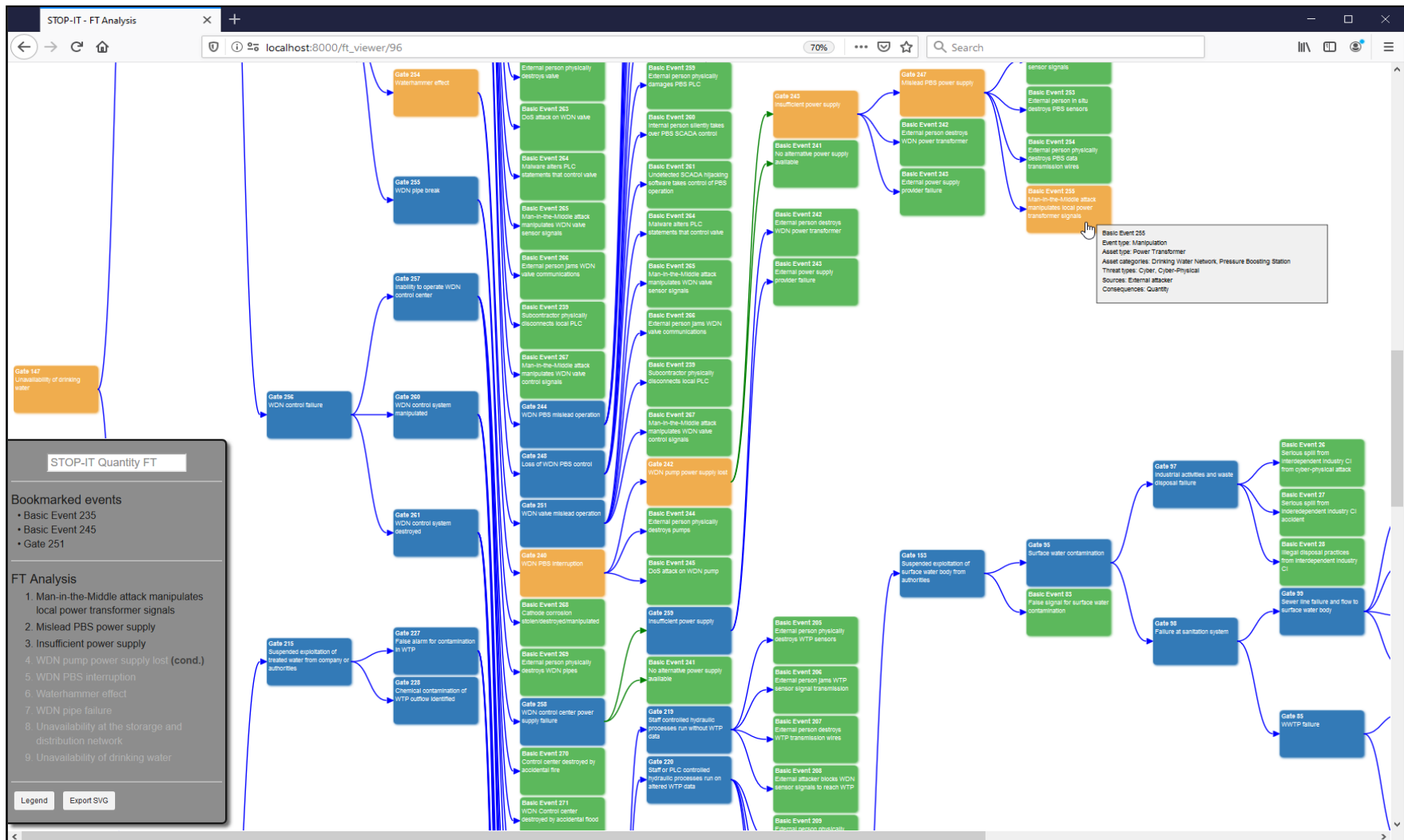

GUI of FT Viewer of SP
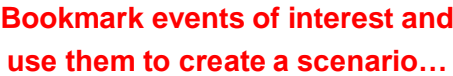
Users may utilise any Quantity or Quality FT:

- **Interact with STOP-IT generic predefined FTs** for an all hazard approach (cyber-physical attacks, natural disasters, human error, etc.). *OR*
- **Customise existing FTs or create new** FTs by using the PSA Explorer and then
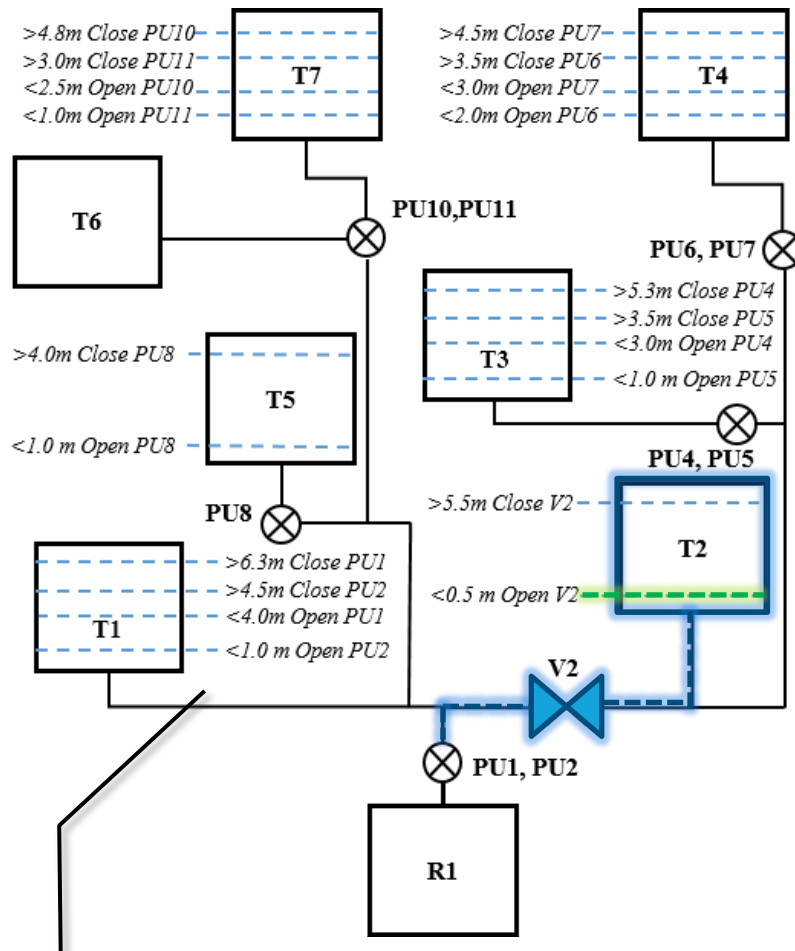 **Load the user- developed** FTs (based on an open PSA format)

Use a FT architecture to visualise the **event cascade** from a basic event (e.g. an attack) to the undesired end event (e.g. water supply disruption)
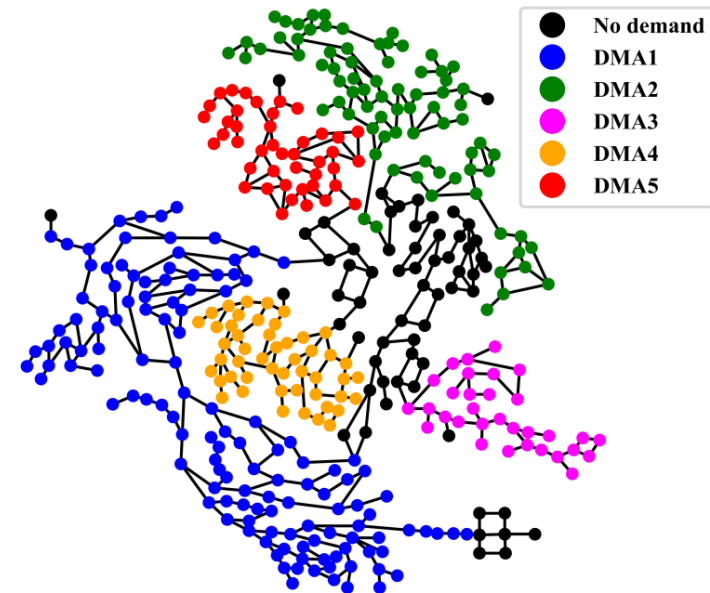
For example, a scenario where a **tank level sensor is manipulated**, misleading the monitoring and control system to believe **the tank has enough water** …

Simplified schematic representation of WDN Cyber-physical control logic

$>4.8m$ Close PU10
$>3.0m$ Close PU11
$<2.5m$ Open PU10
$<1.0m$ Open PU11

T7

$>4.5m$ Close PU7
$>3.5m$ Close PU6
$<3.0m$ Open PU7
$<2.0m$ Open PU6

T4

T6

PU10, PU11

PU6, PU7

$>5.3m$ Close PU4
$>3.5m$ Close PU5
$<3.0m$ Open PU4
$<1.0 m$ Open PU5

T3

$>4.0m$ Close PU8

T5

$<1.0 m$ Open PU8

PU4, PU5

$>5.5m$ Close V2

T2

PU8

$>6.3m$ Close PU1
$>4.5m$ Close PU2
$<4.0m$ Open PU1
$<1.0 m$ Open PU2

$<0.5 m$ Open V2

T1

V2

PU1, PU2

R1

C-town DMAs

●	No demand
●	DMA1
●	DMA2
●	DMA3
●	DMA4
●	DMA5

Sensor data that lead to actuator response through PLC or SCADA control

GUI of SP: Building an EPANET-CPA scenario

Creating a scenario

Defining an event/threat

Defining the asset(s) affected

Defining the simulation parameters

STOP-IT

Stress-Test Procedures

Show 10 entries

Operations	Name	Base scenario	Created
🗑 ✏ 📁	ST procedure 2	Tank level sensor manipulation 2-10h	2020-04-06
🗑 ✏ 📁	ST Procedure 3	Tank level sensor manipulation 2-20h	2020-04-06
🗑 ✏ 📁	Pollution and sensor manipulation	Pollution and sensor manipulation	2020-05-05

Showing 1 to 3 of 3 entries

New

Creating a ST procedure

Name	New ST procedure
Description	
Base scenario	Tank level sensor manipulation 2-10h
Tool	Epanet CPA
Created	2020-05-31 08:35
Modified	2020-05-31 21:15
Completed runs	5 out of 16
Estimated remaining time	6' 8"
Status	**Running** ↻

Control Variables
1. External person in situ manipulates WDN tank level sensor (Basic Event 235), Asset: T2, Values: 8-16, Method: Incremental
2. External person in situ manipulates WDN tank level sensor (Basic Event 235), Asset: T2, Values: 5.7-5.7, Method: Random selection
3. External person in situ manipulates WDN tank level sensor (Basic Event 235), Asset: T2, Values: 2-8, Method: Random selection

KPI1: Customer minutes lost [Customer Minutes]
KPI2: Customers experiencing insufficient service [Customers]
KPI3: Nodes insufficiently supplied [Nodes]
KPI4: System service hours lost [Hours]
KPI5: Unmet demand [liters]

⚔ Interrupt 🏃 Run ✖ Clear

Copy   CSV

Nr	Executed	Control variables	Time [s]	KPI1	KPI2	KPI3	KPI4	KPI5
5	2020-05-31 21:18	Duration 10, Value 5.70, Start time 2	29.60	4326947.42	44674.20	174.00	4.00	603318.96
4	2020-05-31 21:17	Duration 8, Value 5.70, Start time 6	30.57	0.00	26719.98	118.00	0.00	2981.16
3	2020-05-31 21:17	Duration 8, Value 5.70, Start time 3	29.68	0.00	27060.31	119.00	0.00	1042.92
2	2020-05-31 21:16	Duration 8, Value 5.70, Start time 2	30.55	1875542.69	39869.37	173.00	2.00	261876.60
1	2020-05-31 21:16	Duration 8, Value 5.70, Start time 2	46.80	1875542.69	39869.37	173.00	2.00	261876.60

Create a series of scenario variants

Stress-Test Procedure

Name*	New ST procedure

A unique name for the stress-testing precedure

Description	

Short description of the stress-testing precedure

Base scenario*	Tank level sensor manipulation 2-10h

Select the base scenario for stress-testing. Excluded are scenarios having no parameters to calibrate (u

(*) Required fields

Specifying ST procedure attributes

Control variables

Name	Minimum	Maximum	Method	Nr. of values	Event
Duration	0	16	Incremental	4	*Event*: Basic Event 235 *Asset*: T2 (Sensor)
Value	5.5	5.9	Random selection	4	*Event*: Basic Event 235 *Asset*: T2 (Sensor)
Start time	2	6	Random selection	2	*Event*: Basic Event 235 *Asset*: T2 (Sensor)

Specifying the values for the control variables

Cancel   💾 Save

✓ **Scenario Planner**
Identify risks and build a network specific **threat scenario**
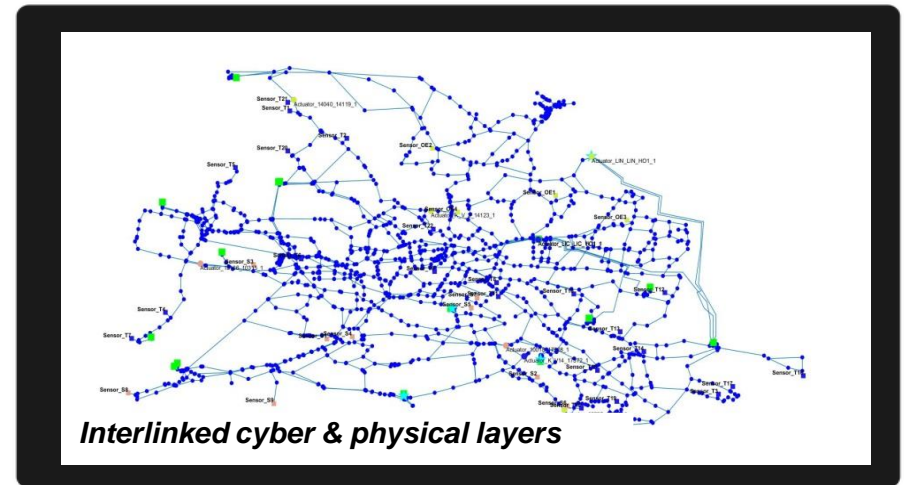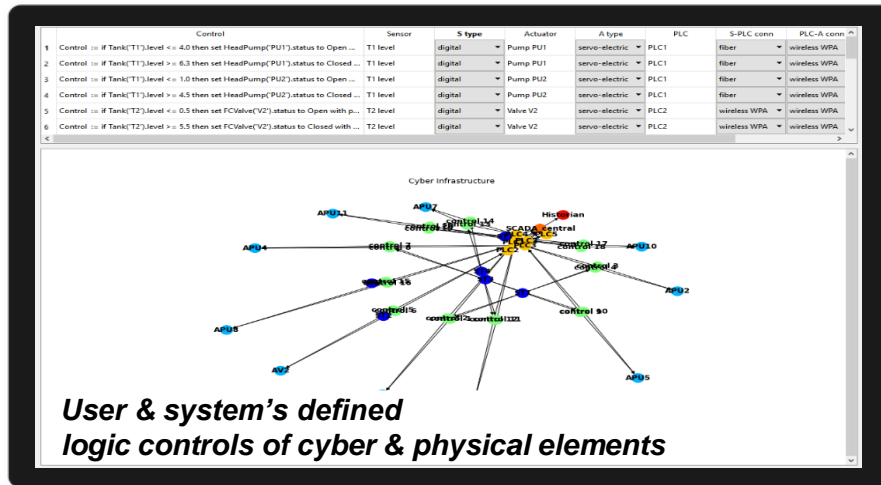
❑ **Stress Test Platform**
Simulate the scenario

❑ **KPI tool**
Evaluate the scenario consequences

❑ **RRMD-RIDB**
Explore appropriate **treatment** options

User & system's defined logic controls of cyber & physical elements

Interlinked cyber & physical layers

The core Stress Testing Platform is an **EPANET based model**

Users:

❑ Have access to a **number of available simulation tools** (for cyber & physical and desired levels of analysis)

❑ **Visualise the cyber network** on top of the **physical topology** of a real network and define its control logic

❑ **Link** and **simulate the combined cyber and physical system** (explicitly modelling interactions)
   e.g. simulate combined system (a) under normal conditions, (b) after incorporating a risk reduction measures, (c) under cyber-physical attacks *(denial-of-service, physical substance insertion into a node & sensor reading alterations)*

❑ **Choose** between Pressure-Driven-Analysis (**PDA**) & Demand-Driven-Analysis (**DDA**) for water **quantity** and **quality** issues

❑ **Assess system response** under the examined scenarios through **thematic maps** and **figures**

❑ **Compare impacts** from different scenarios by selecting specific **performance metric** and **KPIs**

Ratio of demand covered at time 00:00:00
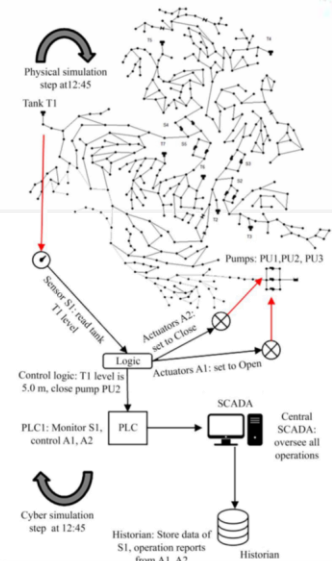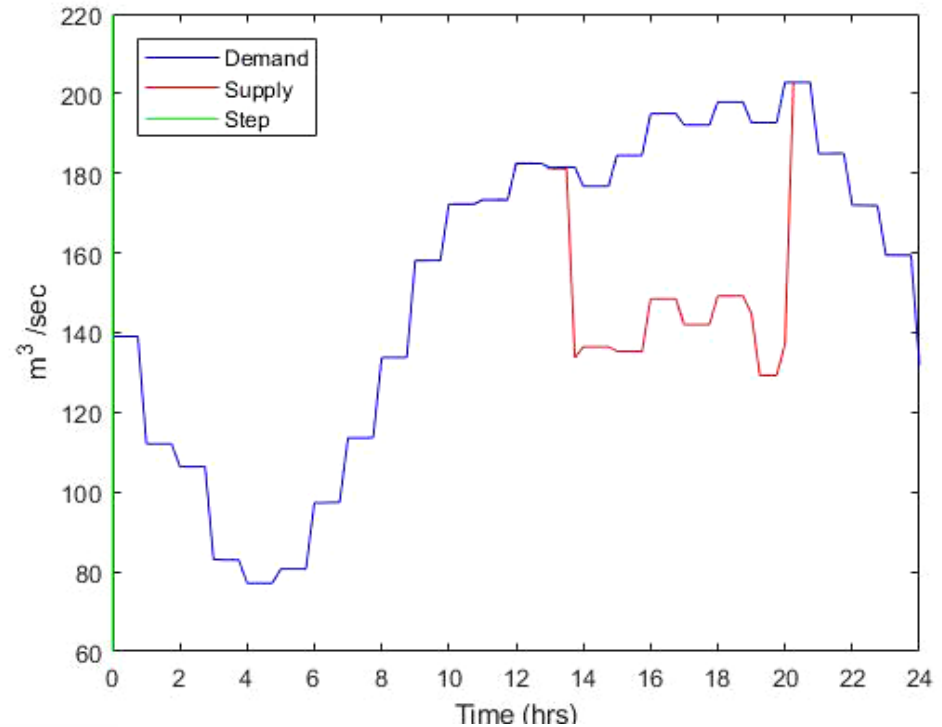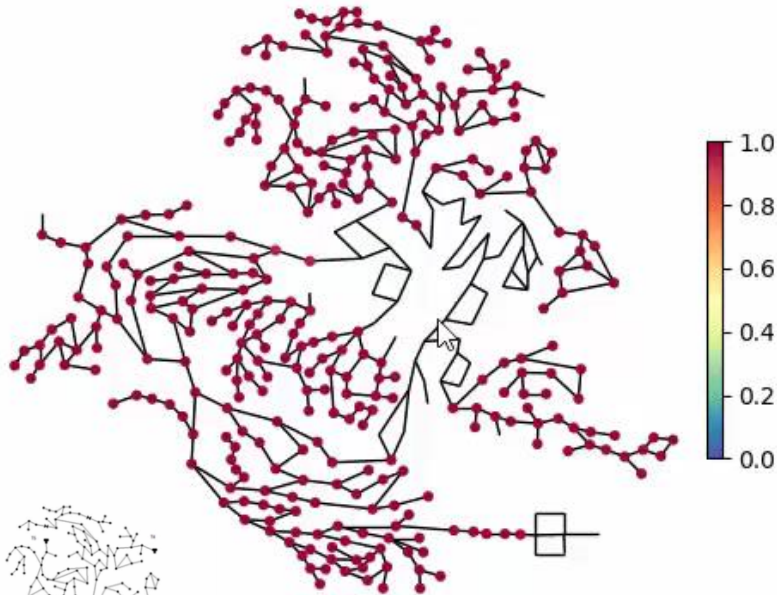
- **RISKNOUGHT** simulates the **flow of information within the cyber layer** (SCADA) and the **interconnection** with physical processes (hydraulic model)
- **Control logic** of the WDN is explicitly formulated
- **Hydraulics** are solved interactively with EPANET (using **PDA equations**)

New water quality simulation capabilities:

❑ Sensors can measure quality concentration indexes from coupled EPANET quality simulation

❑ Augments EPANET **control logic** by incorporating complex rules regarding quality monitoring:

- Isolation of DMAs and PMAs
- Main supply cut-off, cut-off supply from specific tanks
- Activation of flushing units for contaminant removal

❑ Can model purely physical attacks (contaminant injection), cyber-attacks (false-positive contamination event by sensor manipulation) or combined cyber-physical attacks (contaminant injection and sensor manipulation)
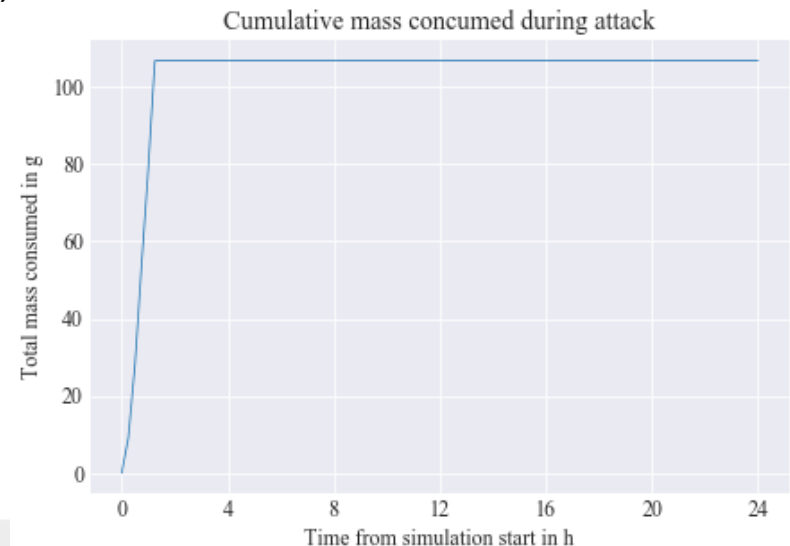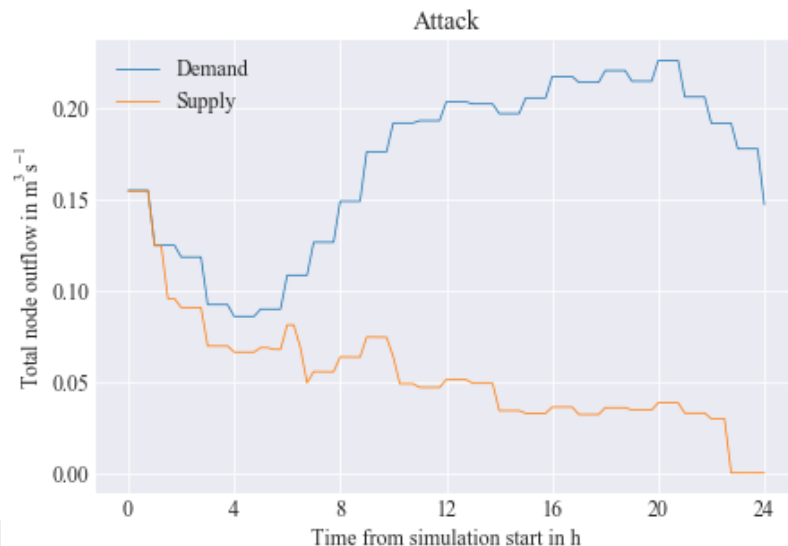
✓ **Scenario Planner**
Identify risks and build a network specific **threat scenario**
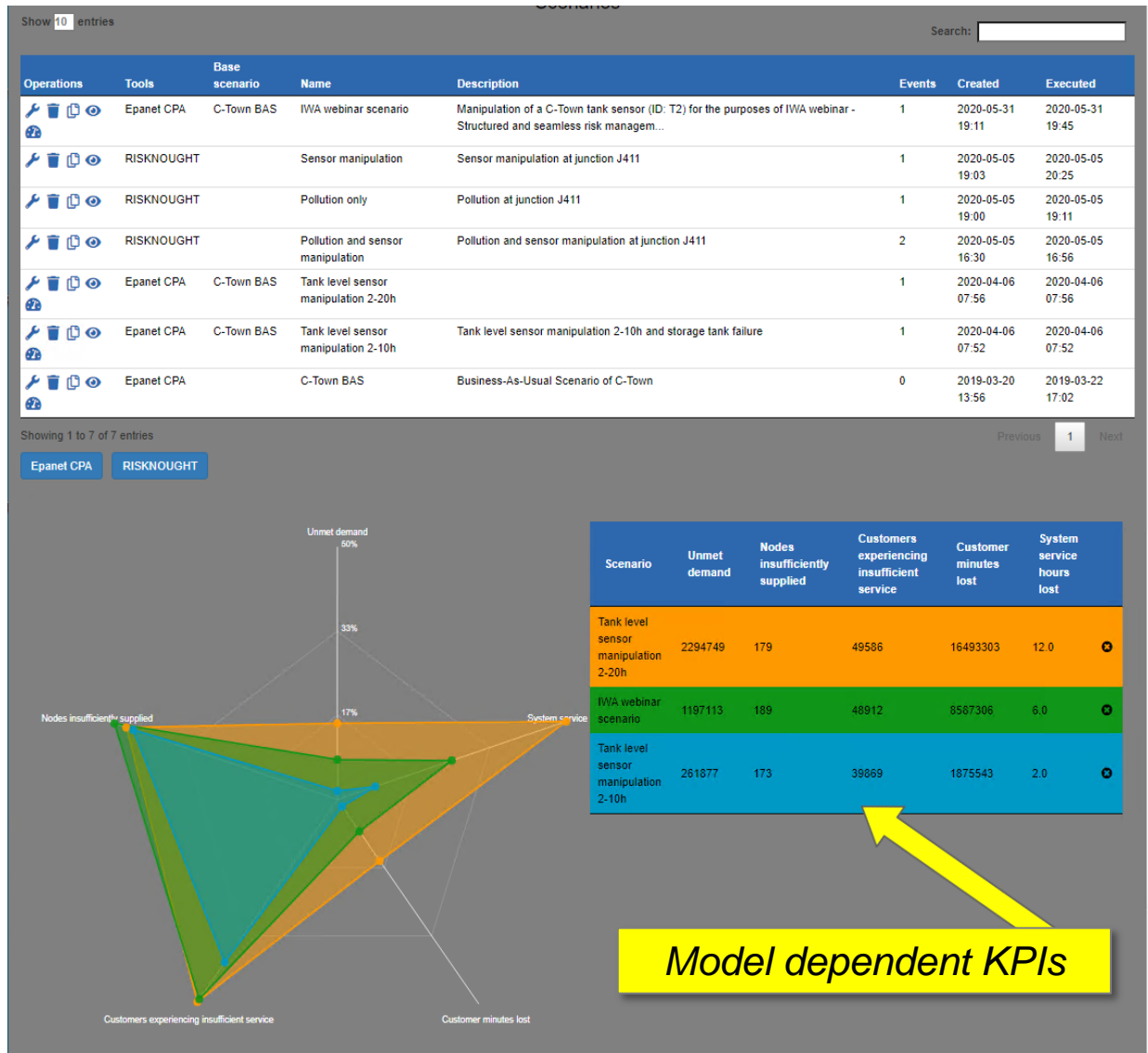
✓ **Stress Test Platform**
Simulate the scenario

❑ **KPI tool**
Evaluate the scenario consequences

❑ **Scenario Planner**
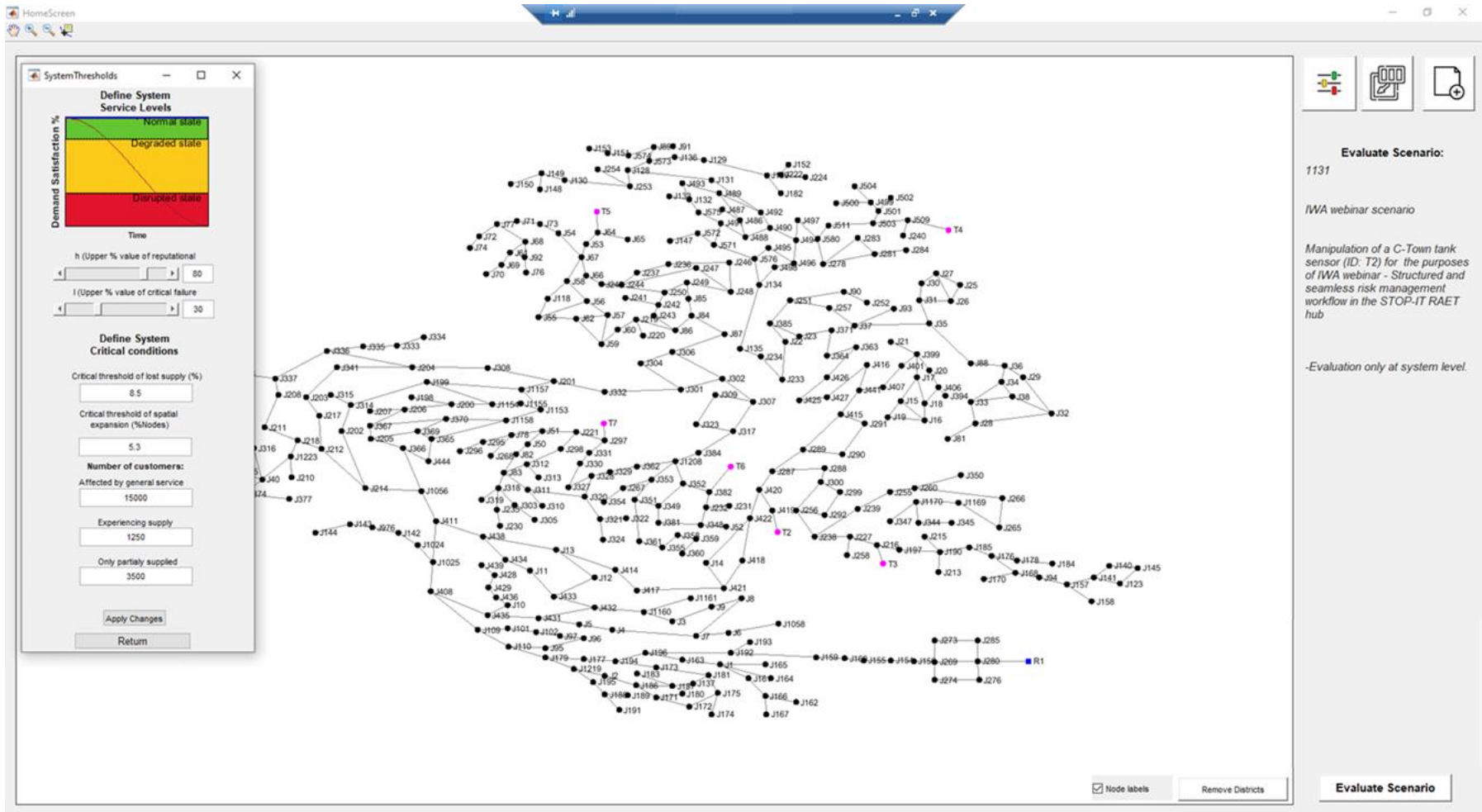Explore appropriate **treatment** options

Users can:

❑ can set the **service levels** for **different districts** & different thresholds for **critical customers**

❑ Visualise results and STOP-IT KPIs **for any grouping they choose** (DMAs etc.)

STOP-IT
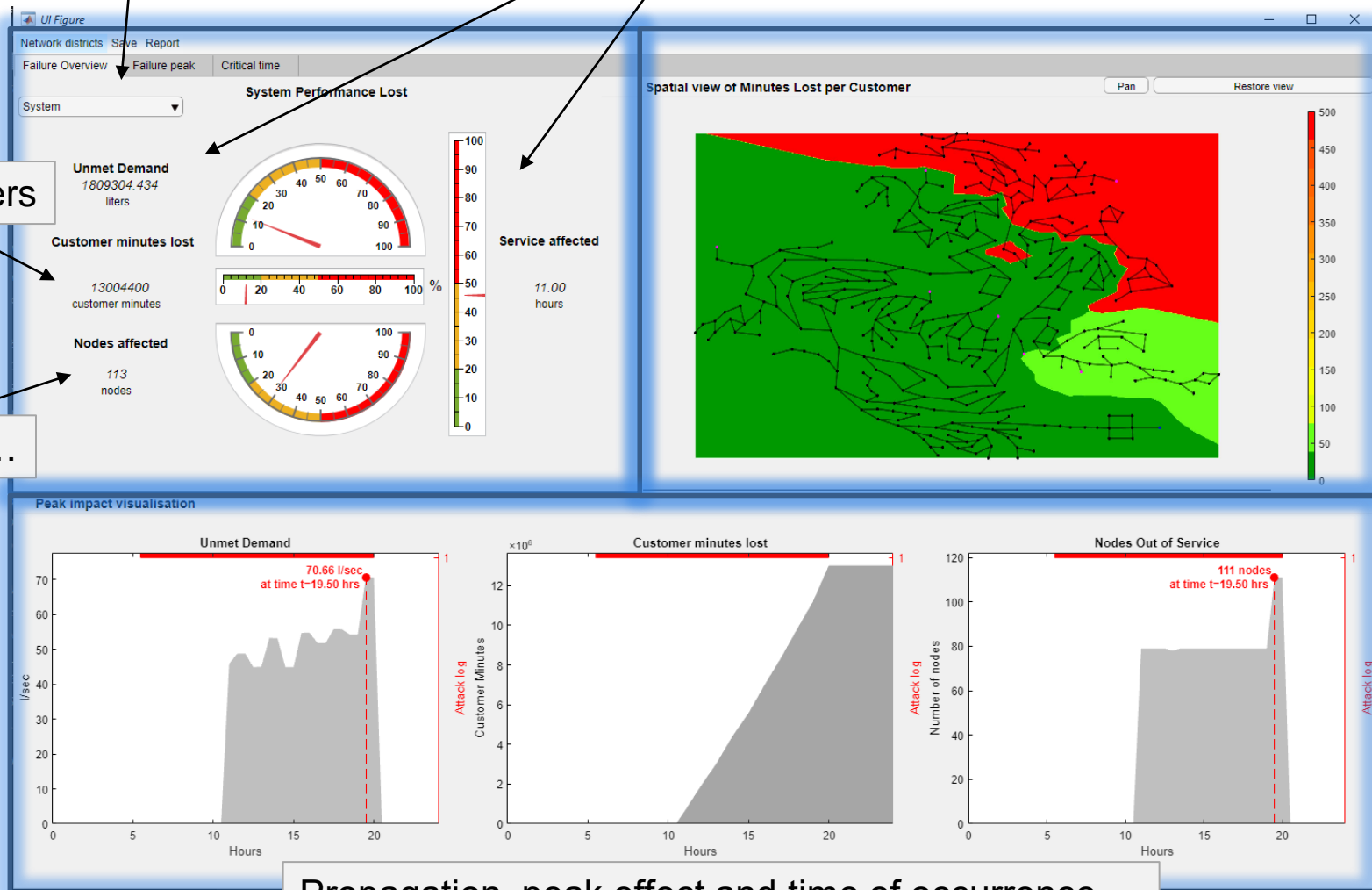

For the system.. Or each district

Supply…

Time

Customers

Nodes…

Propagation, peak effect and time of occurrence…

Generate Risk Analysis Report
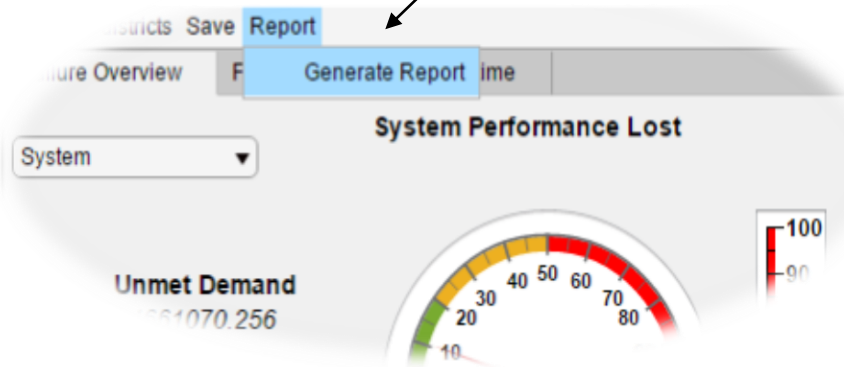
Fully automated report generation with a push of a button…

- Report *System* and *DMA* level Information in rich text
- Support Risk communication
  & Management documentation
- Metadata included for integrity and quality check
- Content can be **tailored** to utility's preferences

✓ **Scenario Planner**
Identify risks and build a network specific **threat scenario**

✓ **Stress Test Platform**
Simulate the scenario

✓ **KPI tool**
Evaluate the scenario consequences

❑ **Scenario Planner**
Explore appropriate **treatment** options

GUI of SP: navigating through the measures available in the RRMD

GUI of SP supporting multiple filtering capabilities

Incorporating measure(s) into scenarios and assessing their impact to system's performance

Matching Risks with Potential Risk Reduction Measures

Main event characteristics

Matching attributes, common in RIDB and RRMD

Models & Tools capable to simulate events

Number of potential RRM

List of RRM

ID	Name	Description	Direct Consequence	Node	Fault Tree	Asset Type	Event Type	Asset Category	Threat Categories	Event Source Types	Event Consequences	Related tools	Event supported by RAET	Risk Reduction Measures
5271	Gate 96	Contamination from farming activities	Groundwater contamination	Intermediate	STOP-IT Water Quality FT	Groundwater	Pollution	Catchment Area	Physical	Human fault	Quality	Epanet MSX RISKNOUGHT	RISKNOUGHT	14
5161	Basic Event 27	Serious spill from inderedependent Industry CI accident	Industrial activities and waste disposal failure	Basic	STOP-IT Quantity FT	Surface Water	Pollution	Catchment Area Raw Water Bodies	Physical	Human fault Interdependent CI	Quantity	Epanet MSX RISKNOUGHT	RISKNOUGHT	15
5199	Basic Event 33	Pesticide seepage to groundwater catchment	Contamination from farming activities	Basic	STOP-IT Quantity FT	Groundwater	Pollution	Catchment Area Raw Water Bodies	Physical	Human fault	Quantity	Epanet MSX RISKNOUGHT	RISKNOUGHT	12
5200	Basic Event 34	Nutrient pollution of groundwater catchment	Contamination from farming activities	Basic	STOP-IT Quantity FT	Groundwater	Pollution	Catchment Area Raw Water Bodies	Physical	Human fault Natural phenomena	Quantity	Epanet MSX RISKNOUGHT	RISKNOUGHT	12
5162	Basic Event 28	Illegal disposal practices from interdependent Industry CI	Industrial activities and waste disposal failure	Basic	STOP-IT Quantity FT	Surface Water	Pollution	Catchment Area Raw Water Bodies	Physical	Interdependent CI	Quantity	Epanet MSX RISKNOUGHT	RISKNOUGHT	7
5198	Basic Event 36	Seepage of Interdependent Industry CI waste to groundwater catchment	Groundwater contamination	Basic	STOP-IT Quantity FT	Groundwater	Pollution	Catchment Area Raw Water Bodies	Physical	Interdependent CI	Qua			
5160	Basic Event 26	Serious spill from Interdependent Industry CI from cyber-physical attack	Industrial activities and waste disposal failure	Basic	STOP-IT Quantity FT	Surface Water	Pollution	Catchment Area Raw Water Bodies	Physical Cyber-Physical	Interdependent CI	Qua			
5065	Gate 190	Surface water system mismanagement	Unavailability from reservoir	Intermediate	STOP-IT Quantity FT	Control System	Manipulation	Catchment Area Raw Water Bodies Water Abstraction Points			Qua			
5066	Gate 191	Mislead surface water management system	Surface water system mismanagement	Intermediate	STOP-IT Quantity FT	Control System	Manipulation	Catchment Area Raw Water Bodies Water Abstraction Points		External attacker Internal attacker Human fault	Qua			
5064	Gate 155	Unavailability from reservoir	Unavailability from surface catchment area	Intermediate	STOP-IT Quantity FT	Surface Water	Interruption	Catchment Area Raw Water Bodies Water Abstraction Points			Qua			
5068	Gate 193	Surface water management system functions on altered data	Mislead surface water management system	Intermediate	STOP-IT Quantity FT	Control System	Manipulation	Catchment Area Raw Water Bodies Water	Cyber Cyber-Physical	External attacker Internal attacker	Qua			

| Measure ID	Name	Description	Comments	Terms and Keywords	Risk reduction mechanism
M12	SupervisionOfExternals	Supervision of any external people entering the water utility or sensitive sites. Any people who enter sites and who are …			Frequency/Likelihood
M16	SourceWaterQualityControl	Control of raw water quality. The aim is to control the raw water quality in order to select the best …			Frequency/Likelihood & Consequences
M19	FiltersInAerationProcesses	All air for aeration purposes in water treatment plants and water storage tanks should be filtered. Thus it is aimed …	Filters should be installed at every air intake for aeration purposes. Furthermore, no openings for aeration purposes should be built …		Frequency/Likelihood
M27	EmployeesTrainings	Regular trainings, seminars, updates and informations on security issues should be implemented for all employees. Thus the staff is always …			Frequency/Likelihood & Consequences
M29	EmergencyPlans	Setting up of emergency plans. Thus clear responsabilities, courses of action, procedures and contacts are defined and documented for emergency …	A complete crisis plan should exist including responsibilities, pending tasks, important contacts etc. All tasks from the evaluation of the …		Consequences
M30	RedundantAssetsAndInfrastructures	Constructions of redundant infrastructures and assets along the whole water supply chain. Thus the failure of one component can, at …	Redundant infrastructures could exist in the water extraction (wells, river extractions, reservoir extractions, spring water), water treatment infrastructures (filtration, adsorption, …		Consequences
M33	AdditionalStorageCapacity	Construction of additional storage tanks. Thus periods of water scarcity due to a higher amount of …			Consequences
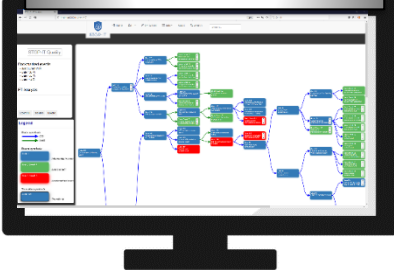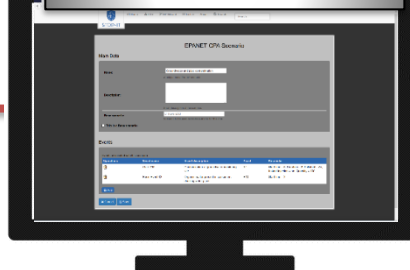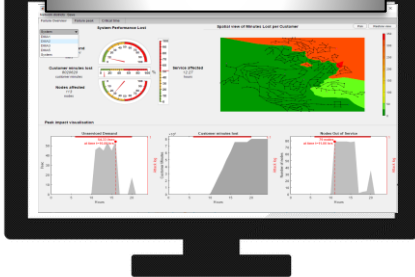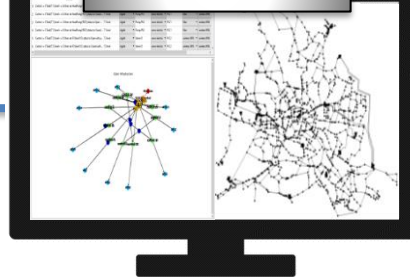
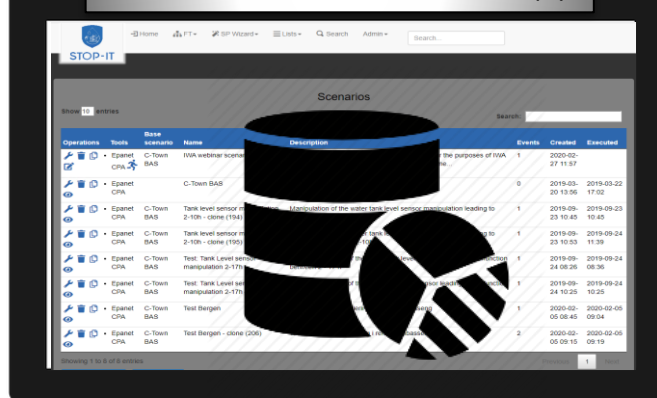✓ **Scenario Planner**
Identify risks and build a network specific **threat scenario**

✓ **Stress Test Platform**
Simulate the scenario

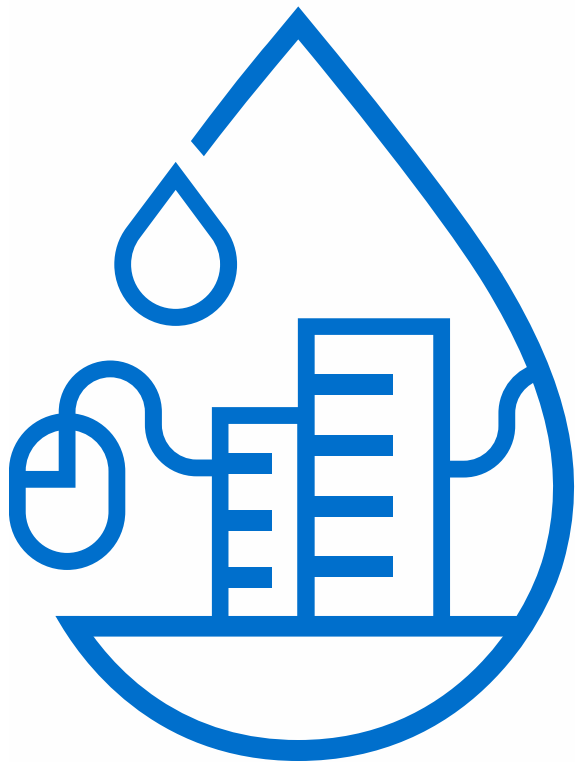✓ **KPI tool**
Evaluate the scenario consequences
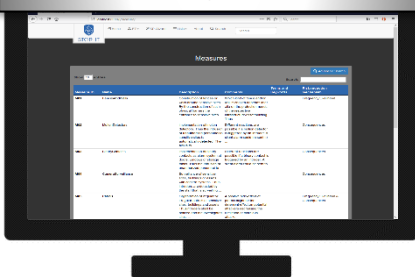
✓ **Scenario Planner**
Explore appropriate **treatment** options

THANK YOU FOR YOUR ATTENTION

stop-it-project.eu

STOP-IT