WP8: 1st training session on WP4 tools – Profile 2

Introduction to WP4 Tools & Demonstration

November 29th, 2019

Dr. Christos Makropoulos (KWR)
George Karavokiros (ICCS)
Georgios Moraitis (ICCS)
Dionysios Nikolopoulos (ICCS)
Archontia Lykou (ICCS)

STOP-IT

www.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.

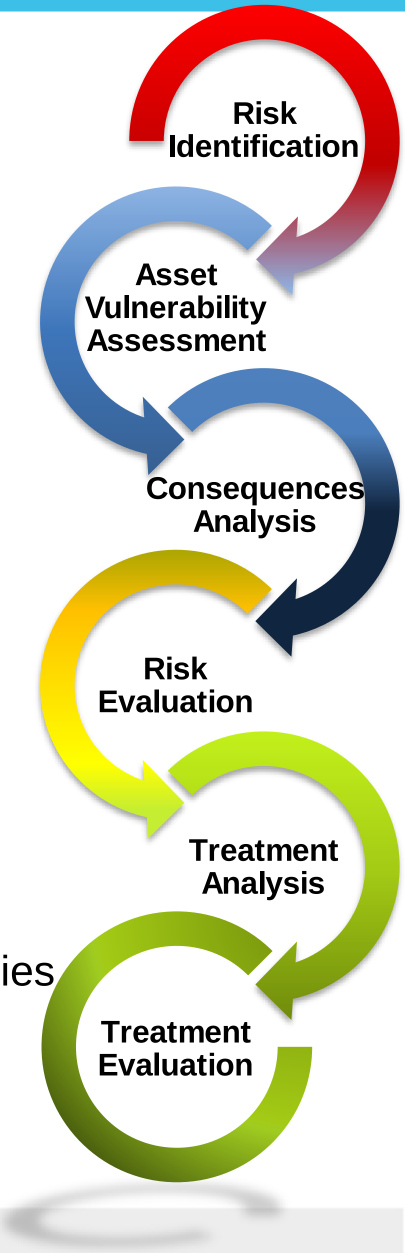
STOP-IT: Tools and technologies

Solutions that support:

1. **Strategic/tactical** planning and post action assessment
2. **Operational** decision making

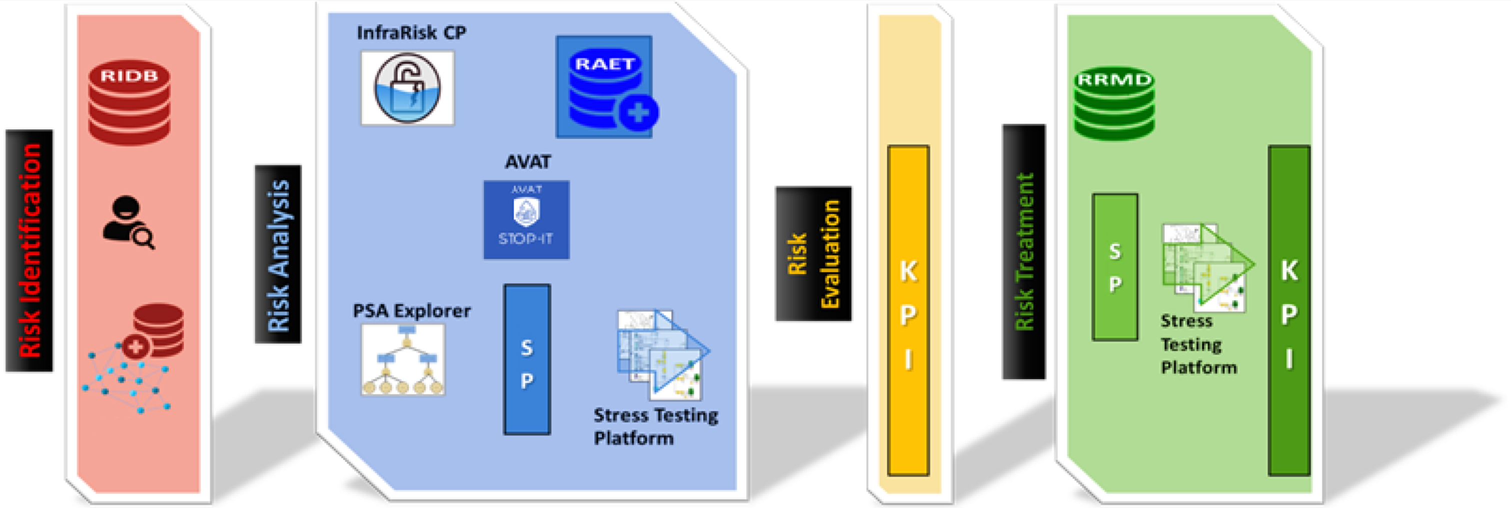
STOP-IT modules:

- **Module 1: Risk Assessment and Treatment Framework (*ISO 31000 compatible*)**
- Module 2: Secure wireless sensor communications module
- Module 3: Toolbox of technologies for securing IT and SCADA
- Module 4:Technologies 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

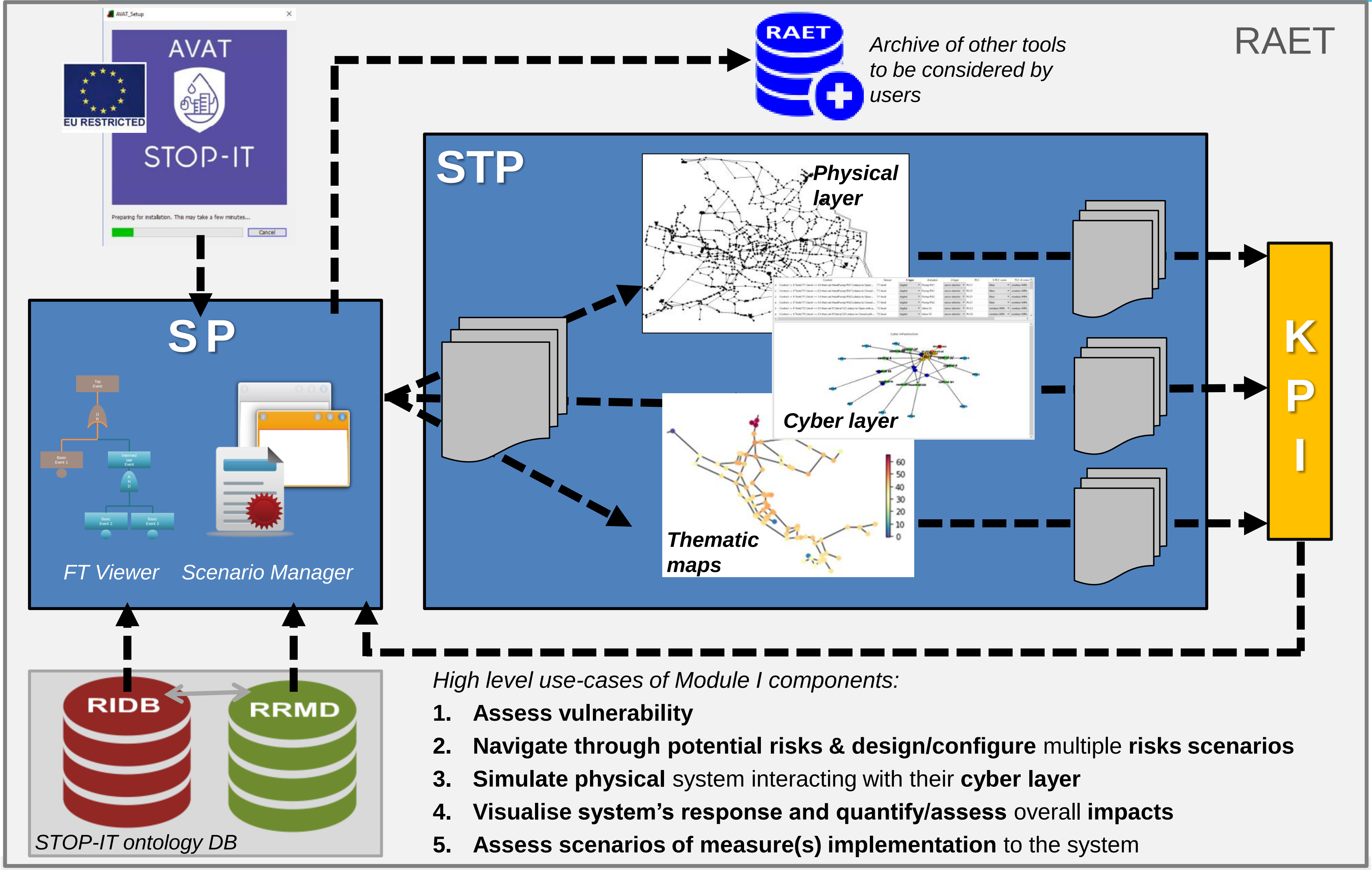
STOP-IT Risk Assessment and Treatment Framework & its components available to users



- ❑ Components of the Framework available to users (**standalone** and **in combination**):
  - **R**isk **I**dentification **D**ata**B**ase i.e. a repository of cyber-physical events/threat (T3.2)
  - **Infrarisk-CP** for generic risk assessment of cyber-physical events (T4.2)
  - **A**sset **V**ulnerability **A**ssessment **T**ool for assets' and systems vulnerabilities (T4.1)
  - **F**aults **T**ree Editor for Fault Trees development (T6.3)
  - **S**cenario **P**lanner for enhanced navigation on potential threats, cascading effects and pathways of systems failure examined in attack-threat scenarios (T4.2)
  - **Cyber-physical Stress Testing Platform** for monitoring systems behaviour (both physical infrastructure & cyber components) under different scenarios (T4.4)
  - **Metrics and K**ey **P**erformance **I**ndicators tool assessing performance of WDS and impacts (T4.2)
  - **R**isk **R**eduction **M**easure **D**atabase for identification of appropriate risk reduction measures (T4.3)
  - **R**isk **A**nalysis & **E**valuation **T**oolkit with state-of-art models and tools for risk analysis & evaluation (T4.2)

STOP-IT

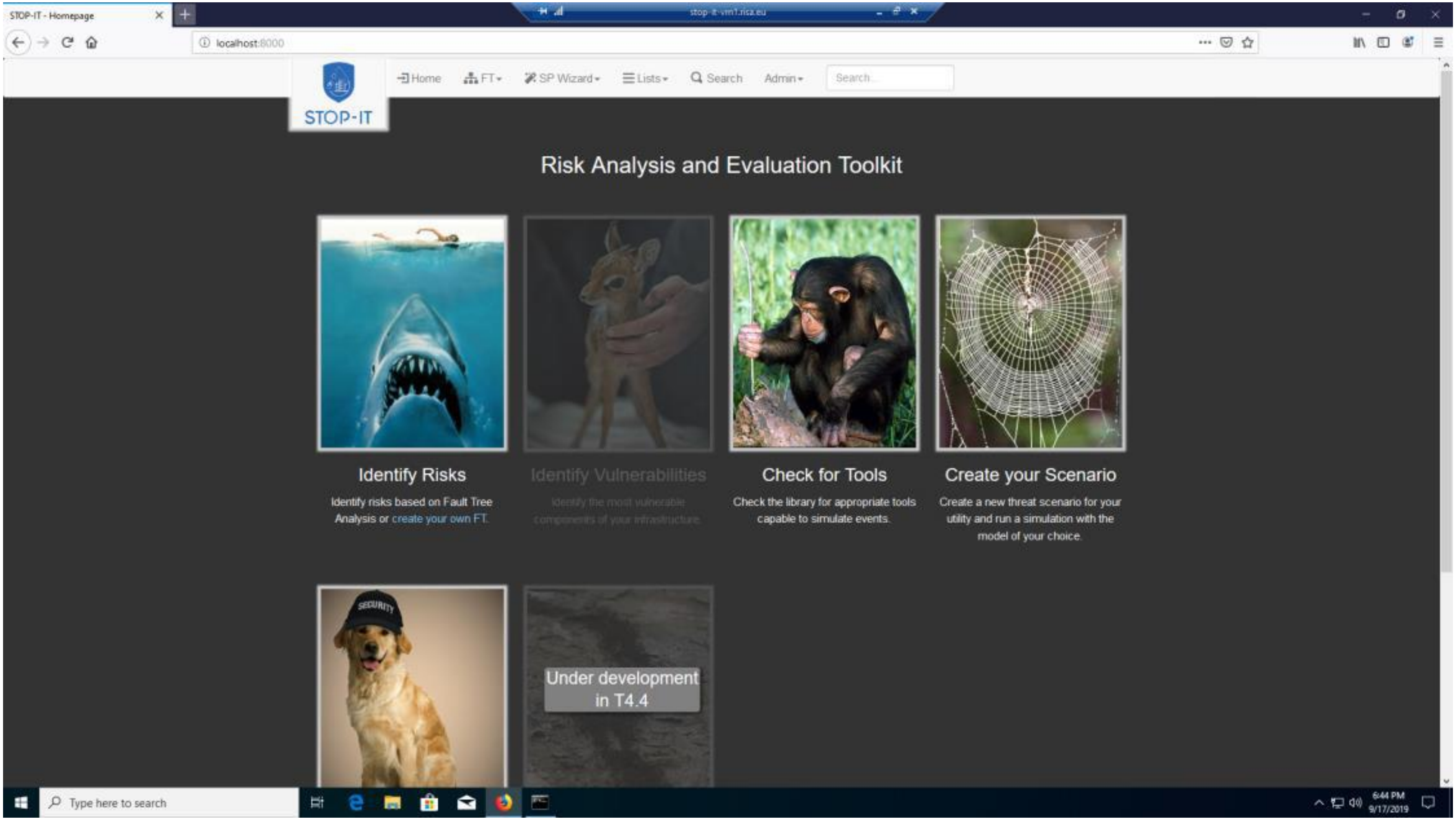
Module 1: A Risk Assessment and Treatment Framework



High level use-cases of Module I components:

1. **Assess vulnerability**
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

Risk Analysis and Evaluation Toolkit (RAET)



Risk Analysis and Evaluation Toolkit

Identify Risks
Identify risks based on Fault Tree Analysis or create your own FT.

Identify Vulnerabilities
Identify the most vulnerable components of your infrastructure

Check for Tools
Check the library for appropriate tools capable to simulate events.

Create your Scenario
Create a new threat scenario for your utility and run a simulation with the model of your choice.

Under development in T4.4

All the modelling tools developed and collected are/will be **available through the RAET** assisting users in stages of risk identification, analysis, evaluation and eventually treatment.

STOP-IT

Risk identification: From RIDB to FTs

A generates a B C of D affecting E, which might lead to a F issue

A	B	C	D	E	F	General	Example
Type of source e.g. External attacker	Type of threat e.g. cyber	Type of event e.g. manipulation	Specific asset e.g. PLC	Type of asset e.g. Drinking Water Network	Consequence e.g. Quantity Issue	Description A to F	Description Details

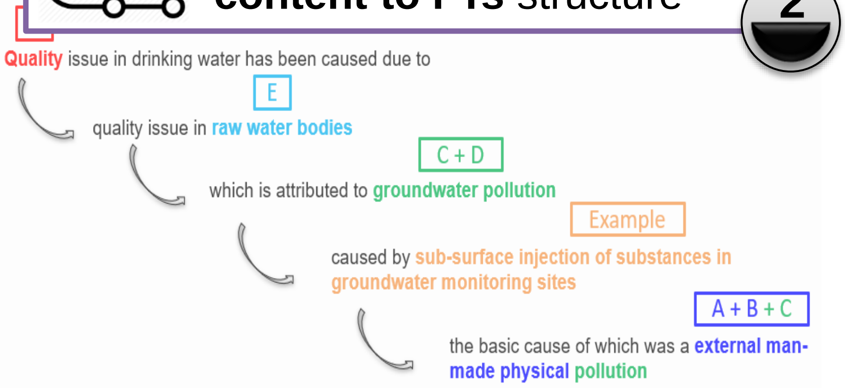
RIDB

Utilised structure & content of the **RIDB**
(being in MS Excel format)

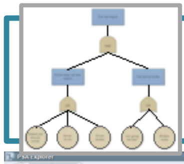
1

Developed **a step-by-step process** converting the **RIDB content to FTs** structure

2

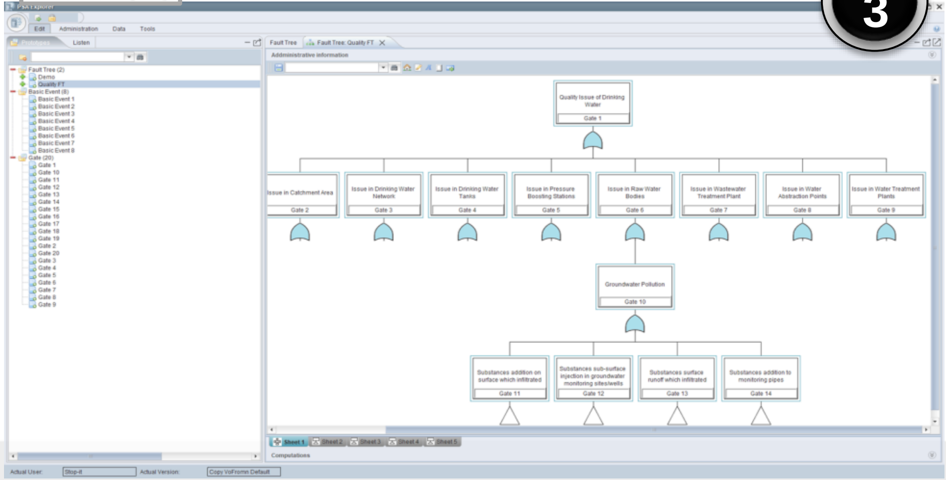


F
Quality issue in drinking water has been caused due to
E
quality issue in raw water bodies
C + D
which is attributed to groundwater pollution
Example
caused by sub-surface injection of substances in groundwater monitoring sites
A + B + C
the basic cause of which was a external man-made physical pollution



Used the **FT Editor** of RISA and **developed** the **STOP-IT FTs**

3



Edit
Administration
Data
Tools
Listen
Fault Tree (2)
Demo
Quality FT
Basic Event (8)
Basic Event 1
Basic Event 2
Basic Event 3
Basic Event 4
Basic Event 5
Basic Event 6
Basic Event 7
Basic Event 8
Gate (20)
Fault Tree
Fault Tree: Quality FT
Addministrative information
Quality Issue of Drinking Water
Gate 1
Issue in Catchment Area
Gate 2
Issue in Drinking Water Network
Gate 3
Issue in Drinking Water Tanks
Gate 4
Issue in Pressure Boosting Stations
Gate 5
Issue in Raw Water Bodies
Gate 6
Issue in Wastewater Treatment Plant
Gate 7
Issue in Water Abstraction Points
Gate 8
Issue in Water Treatment Plants
Gate 9
Groundwater Pollution
Gate 10
Substances addition on surface which infiltrated
Gate 11
Substances sub-surface injection in groundwater monitoring sites/wells
Gate 12
Substances surface runoff which infiltrated
Gate 13
Substances addition to monitoring pipes
Gate 14
Sheet 1
Sheet 2
Sheet 3
Sheet 4
Sheet 5
Computations
Actual User:
Stop-it
Actual Version:
Copy VoFromn Default

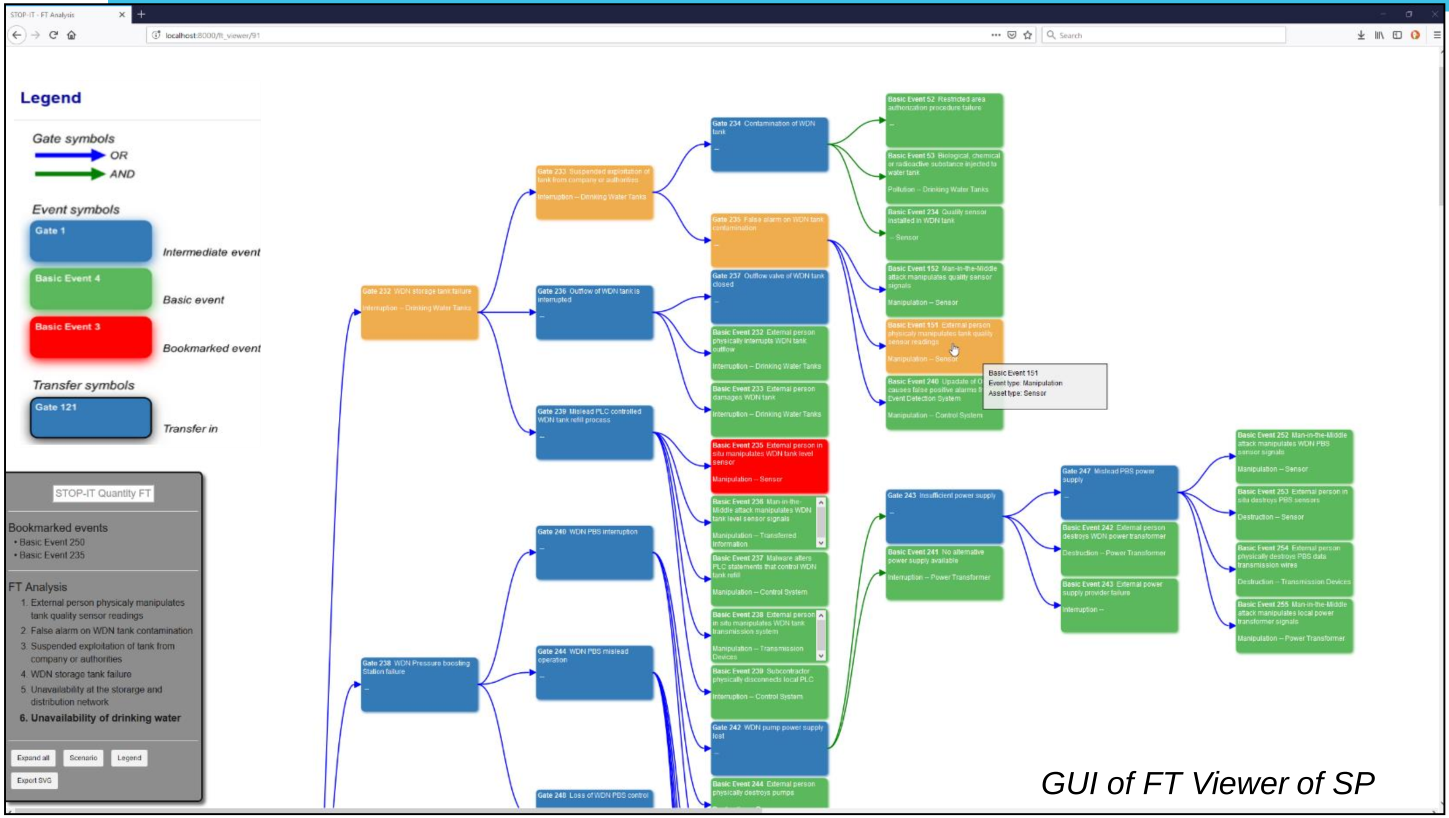
FTs DB

of both **cyber-physical events**

4

Built **FTs using** enriched RIDB **interlinked events** (Top to Basic Event) with causal **relationships**, **pathways of failure**, etc. to be used in next steps of risk analysis

Scenario Planner: Identifying Risks through FTs


STOP-IT - FT Analysis
localhost:8000/ft_viewer/91
Search
Legend
Gate symbols
OR
AND
Event symbols
Gate 1
Intermediate event
Basic Event 4
Basic event
Basic Event 3
Bookmarked event
Transfer symbols
Gate 121
Transfer in
Gate 232 WDN storage tank failure
Interruption -- Drinking Water Tanks
Gate 233 Suspended exploitation of tank from company or authorities
Interruption -- Drinking Water Tanks
Gate 236 Outflow of WDN tank is interrupted
--
Gate 239 Mislead PLC controlled WDN tank refill process
--
Gate 240 WDN PBS interruption
--
Gate 238 WDN Pressure boosting Station failure
--
Gate 244 WDN PBS mislead operation
--
Gate 248 Loss of WDN PBS control
Gate 234 Contamination of WDN tank
--
Gate 235 False alarm on WDN tank contamination
--
Gate 237 Outflow valve of WDN tank closed
--
Basic Event 232 External person physically interrupts WDN tank outflow
Interruption -- Drinking Water Tanks
Basic Event 233 External person damages WDN tank
Interruption -- Drinking Water Tanks
Basic Event 235 External person in situ manipulates WDN tank level sensor
Manipulation -- Sensor
Basic Event 236 Man-in-the-Middle attack manipulates WDN tank level sensor signals
Manipulation -- Transferred Information
Basic Event 237 Malware alters PLC statements that control WDN tank refill
Manipulation -- Control System
Basic Event 238 External person in situ manipulates WDN tank transmission system
Manipulation -- Transmission Devices
Basic Event 239 Subcontractor physically disconnects local PLC
Interruption -- Control System
Gate 242 WDN pump power supply lost
--
Basic Event 244 External person physically destroys pumps
Basic Event 52 Restricted area authorization procedure failure
--
Basic Event 53 Biological, chemical or radioactive substance injected to water tank
Pollution -- Drinking Water Tanks
Basic Event 234 Quality sensor installed in WDN tank
-- Sensor
Basic Event 152 Man-in-the-Middle attack manipulates quality sensor signals
Manipulation -- Sensor
Basic Event 151 External person physicaly manipulates tank quality sensor readings
Manipulation -- Sensor
Basic Event 240 Upadate of O causes false positive alarms fr Event Detection System
Manipulation -- Control System
Basic Event 151
Event type: Manipulation
Asset type: Sensor
Gate 243 Insufficient power supply
--
Basic Event 241 No alternative power supply available
Interruption -- Power Transformer
Gate 247 Mislead PBS power supply
--
Basic Event 242 External person destroys WDN power transformer
Destruction -- Power Transformer
Basic Event 243 External power supply provider failure
Interruption --
Basic Event 252 Man-in-the-Middle attack manipulates WDN PBS sensor signals
Manipulation -- Sensor
Basic Event 253 External person in situ destroys PBS sensors
Destruction -- Sensor
Basic Event 254 External person physically destroys PBS data transmission wires
Destruction -- Transmission Devices
Basic Event 255 Man-in-the-Middle attack manipulates local power transformer signals
Manipulation -- Power Transformer
Expand all
Scenario
Legend
Export SVG

STOP-IT Quantity FT

Bookmarked events
- Basic Event 250
- Basic Event 235

FT Analysis
1. External person physicaly manipulates tank quality sensor readings
2. False alarm on WDN tank contamination
3. Suspended exploitation of tank from company or authorities
4. WDN storage tank failure
5. Unavailability at the storarge and distribution network
6. **Unavailability of drinking water**

GUI of FT Viewer of SP

STOP-IT FTs:

- Quality issues
- Quantity issues

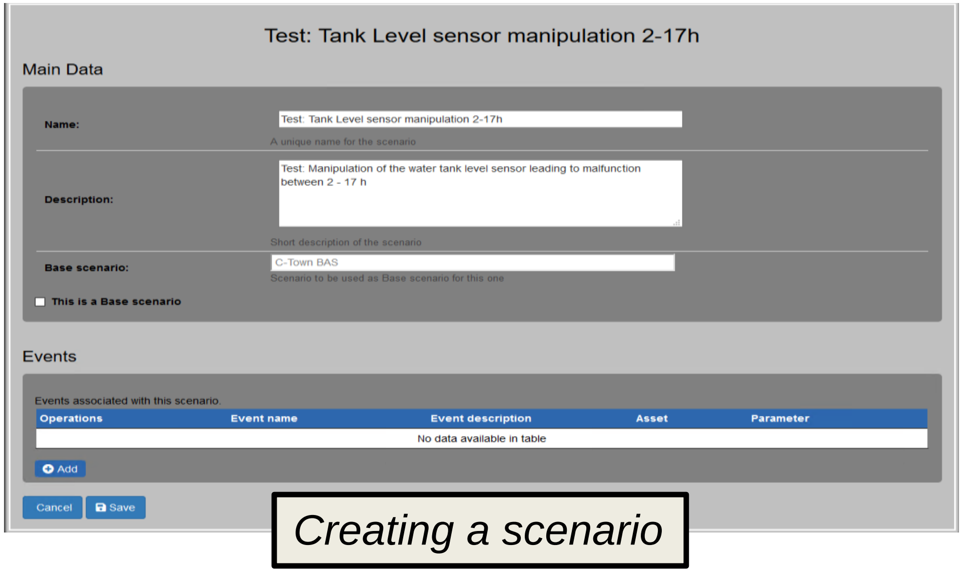
❑ A **user-friendly graphical environment** for the investigation of threat and cascading effect scenarios

❑ 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 FT Editor and then **Load the user-developed** FTs to the FT Viewer of SP (through an open PSA format)

Scenario Planner: Building a scenario

GUI of SP: Building an EPANET-CPA scenario



Test: Tank Level sensor manipulation 2-17h

Main Data

Name: Test: Tank Level sensor manipulation 2-17h
A unique name for the scenario

Description: Test: Manipulation of the water tank level sensor leading to malfunction between 2 - 17 h
Short description of the scenario

Base scenario: C-Town BAS
Scenario to be used as Base scenario for this one

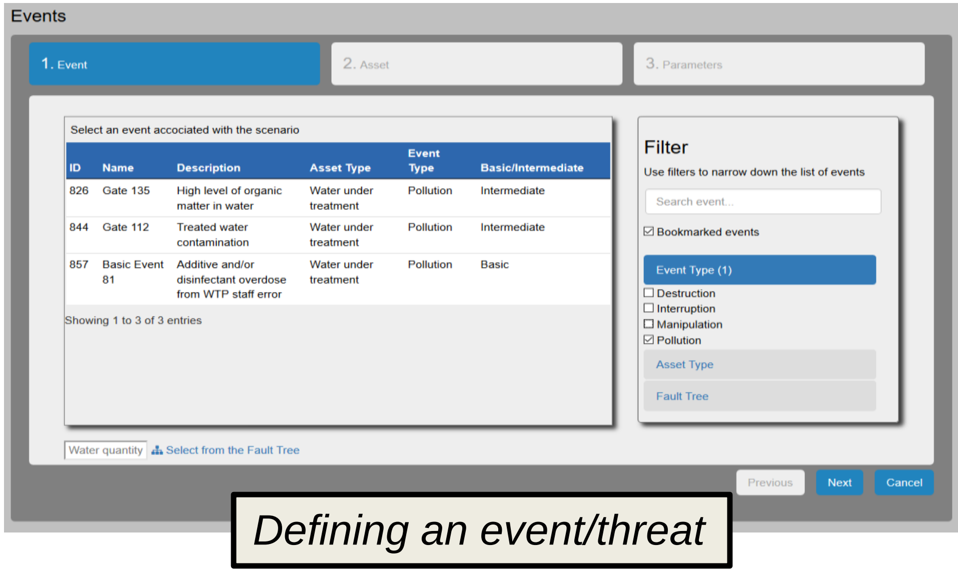
□ **This is a Base scenario**

Events

Events associated with this scenario.

Operations	Event name	Event description	Asset	Parameter
No data available in table				

Creating a scenario



Events

Select an event accociated with the scenario

ID	Name	Description	Asset Type	Event Type	Basic/Intermediate
826	Gate 135	High level of organic matter in water	Water under treatment	Pollution	Intermediate
844	Gate 112	Treated water contamination	Water under treatment	Pollution	Intermediate
857	Basic Event 81	Additive and/or disinfectant overdose from WTP staff error	Water under treatment	Pollution	Basic

Showing 1 to 3 of 3 entries

Filter

Use filters to narrow down the list of events

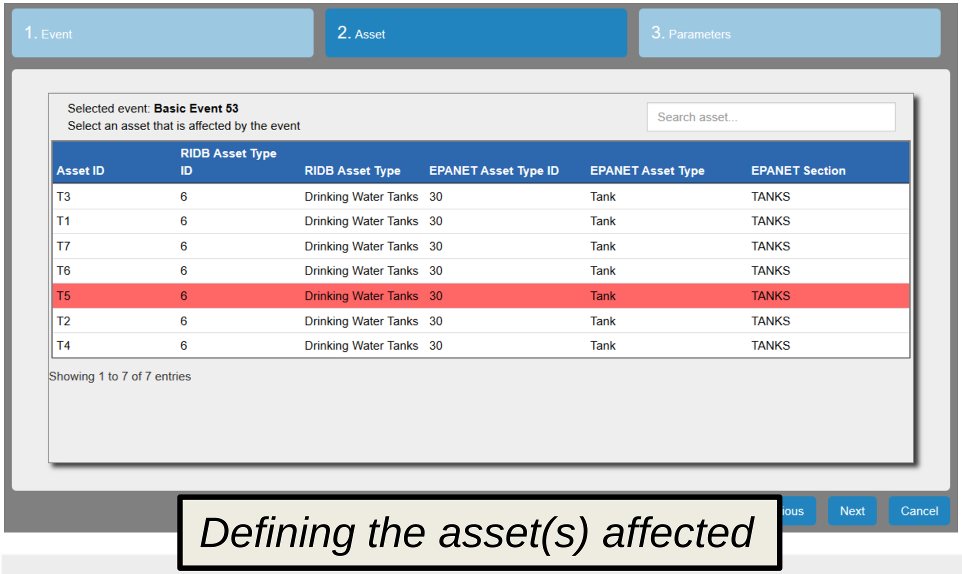
Search event...

☑ Bookmarked events

Event Type (1)

□ Destruction
□ Interruption
□ Manipulation
☑ Pollution

Defining an event/threat



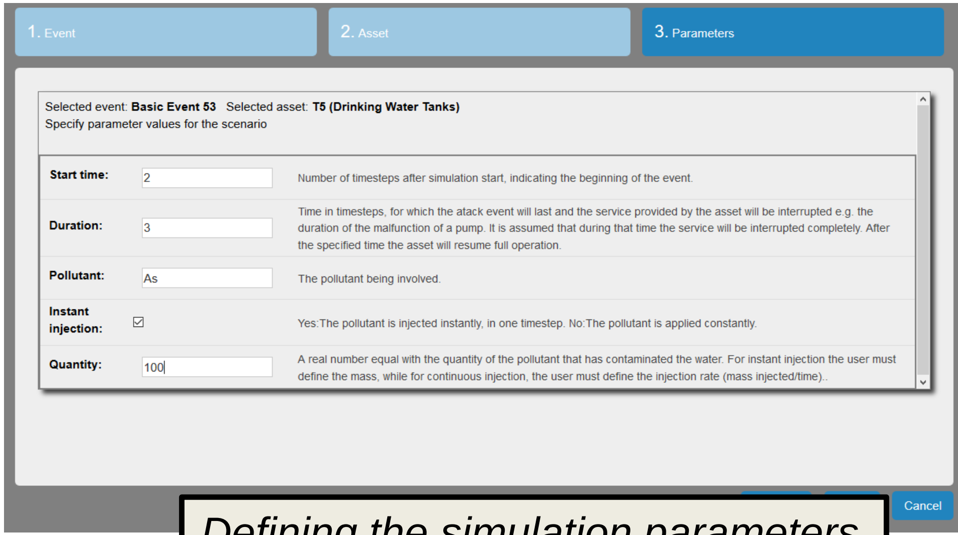
Selected event: **Basic Event 53**
Select an asset that is affected by the event

Search asset...

Asset ID	RIDB Asset Type ID	RIDB Asset Type	EPANET Asset Type ID	EPANET Asset Type	EPANET Section
T3	6	Drinking Water Tanks	30	Tank	TANKS
T1	6	Drinking Water Tanks	30	Tank	TANKS
T7	6	Drinking Water Tanks	30	Tank	TANKS
T6	6	Drinking Water Tanks	30	Tank	TANKS
T5	6	Drinking Water Tanks	30	Tank	TANKS
T2	6	Drinking Water Tanks	30	Tank	TANKS
T4	6	Drinking Water Tanks	30	Tank	TANKS

Showing 1 to 7 of 7 entries

Defining the asset(s) affected



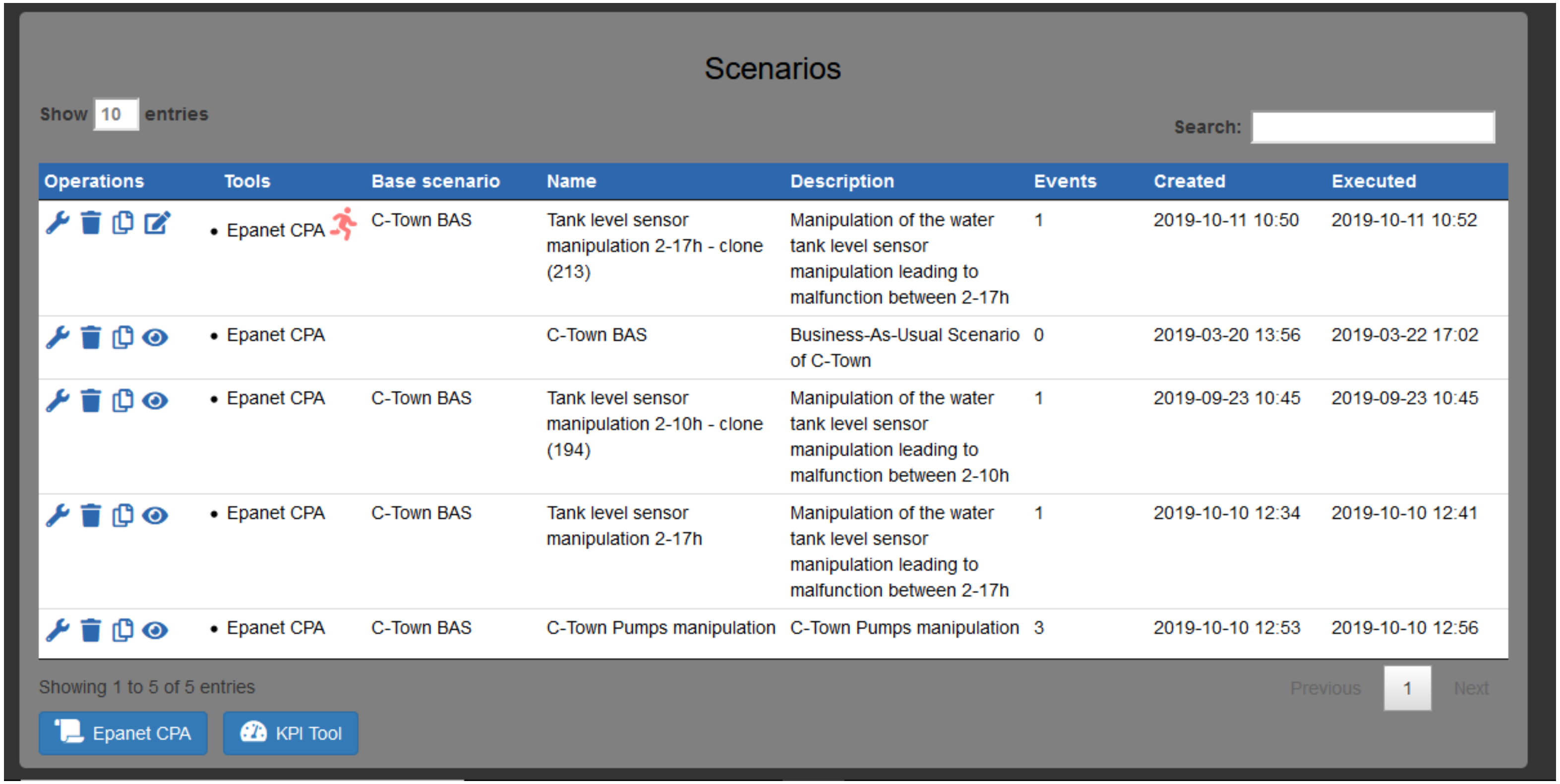
Selected event: **Basic Event 53** Selected asset: **T5 (Drinking Water Tanks)**
Specify parameter values for the scenario

Start time:	2	Number of timesteps after simulation start, indicating the beginning of the event.
Duration:	3	Time in timesteps, for which the atack event will last and the service provided by the asset will be interrupted e.g. the duration of the malfunction of a pump. It is assumed that during that time the service will be interrupted completely. After the specified time the asset will resume full operation.
Pollutant:	As	The pollutant being involved.
Instant injection:	☑	Yes:The pollutant is injected instantly, in one timestep. No:The pollutant is applied constantly.
Quantity:	100	A real number equal with the quantity of the pollutant that has contaminated the water. For instant injection the user must define the mass, while for continuous injection, the user must define the injection rate (mass injected/time)..

Defining the simulation parameters

STOP-IT

Scenario Planner Tool: Scenario(s) management



Scenarios

Show 10 entries

Search:

Operations	Tools	Base scenario	Name	Description	Events	Created	Executed
	• Epanet CPA	C-Town BAS	Tank level sensor manipulation 2-17h - clone (213)	Manipulation of the water tank level sensor manipulation leading to malfunction between 2-17h	1	2019-10-11 10:50	2019-10-11 10:52
	• Epanet CPA		C-Town BAS	Business-As-Usual Scenario of C-Town	0	2019-03-20 13:56	2019-03-22 17:02
	• Epanet CPA	C-Town BAS	Tank level sensor manipulation 2-10h - clone (194)	Manipulation of the water tank level sensor manipulation leading to malfunction between 2-10h	1	2019-09-23 10:45	2019-09-23 10:45
	• Epanet CPA	C-Town BAS	Tank level sensor manipulation 2-17h	Manipulation of the water tank level sensor manipulation leading to malfunction between 2-17h	1	2019-10-10 12:34	2019-10-10 12:41
	• Epanet CPA	C-Town BAS	C-Town Pumps manipulation	C-Town Pumps manipulation	3	2019-10-10 12:53	2019-10-10 12:56

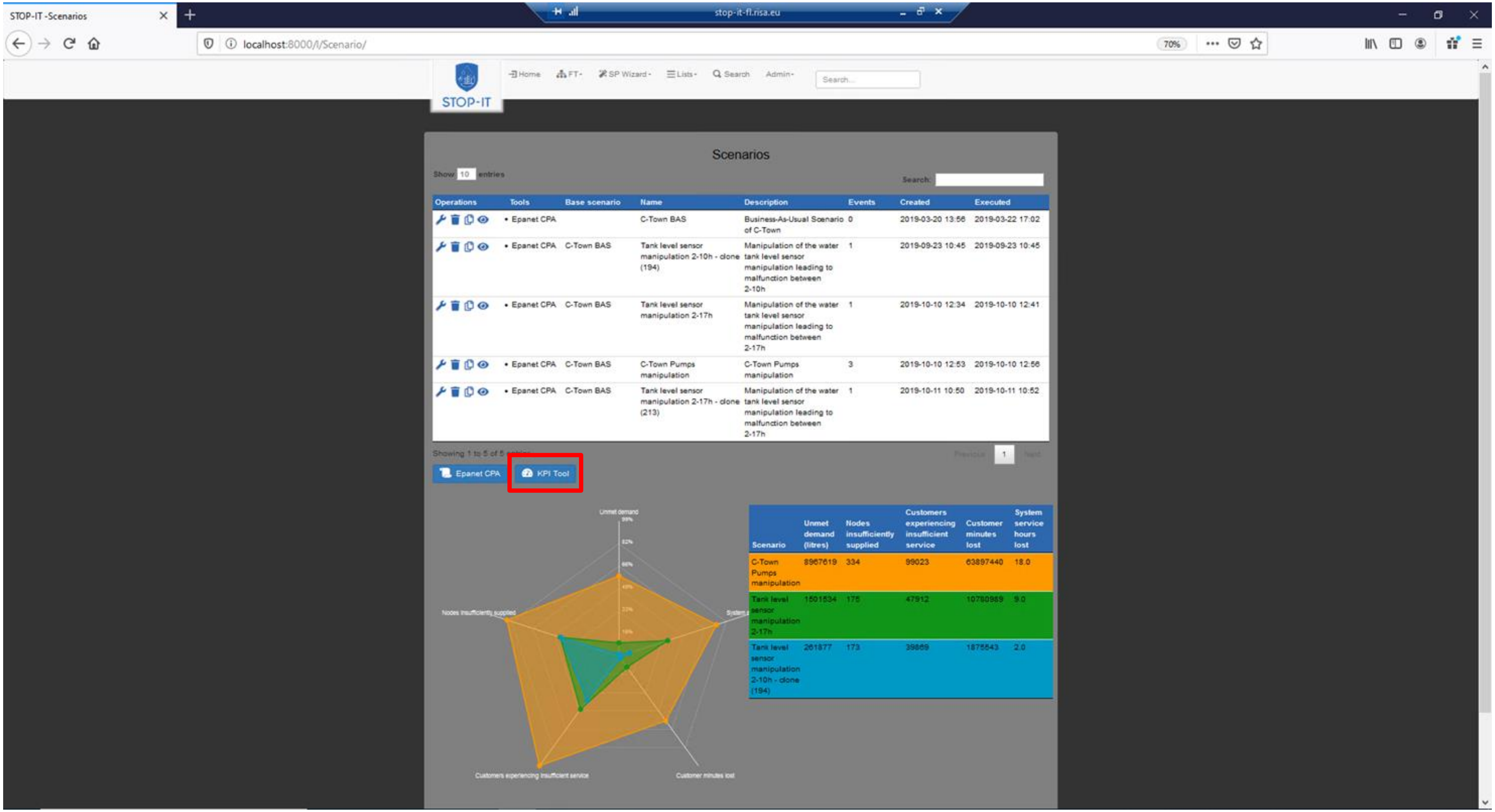
Showing 1 to 5 of 5 entries

GUI of SP: Scenario manager & primary metadata

Users can:

- ❑ Export scenarios for evaluation:
  - Either (**manually** – through a human readable scenario report) setup scenarios **in own (non-STOP-IT) simulation platforms**
  - Or (**automatically** – through the *wizard*) setup scenarios for **the STOP-IT** cyber-physical stress-testing platform
- ❑ Manage their scenarios (store locally, archive, edit, delete, clone, retrieve, organise results etc.)
- ❑ **Launch the KPI tool** to further examine scenario(s) impact through STOP-IT KPIs

Scenario Planner: Visualising high level results of scenario(s)



Scenarios

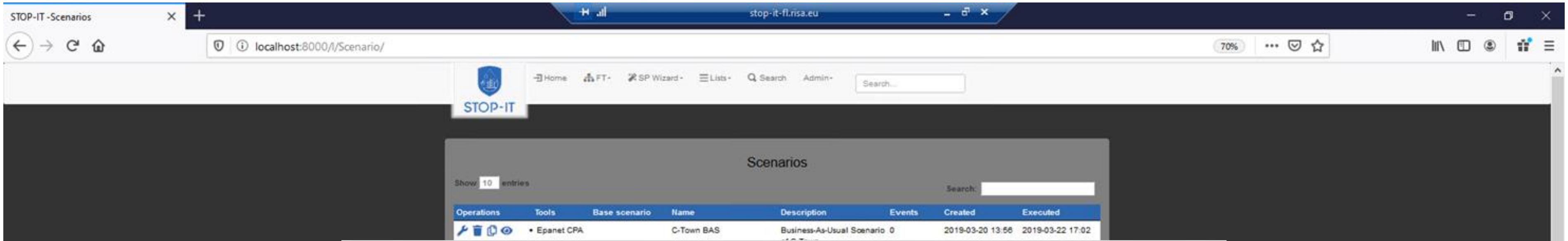
Operations	Tools	Base scenario	Name	Description	Events	Created	Executed
	• Epanet CPA		C-Town BAS	Business-As-Usual Scenario of C-Town	0	2019-03-20 13:56	2019-03-22 17:02
	• Epanet CPA	C-Town BAS	Tank level sensor manipulation 2-10h - clone (194)	Manipulation of the water tank level sensor manipulation leading to malfunction between 2-10h	1	2019-09-23 10:45	2019-09-23 10:45
	• Epanet CPA	C-Town BAS	Tank level sensor manipulation 2-17h	Manipulation of the water tank level sensor manipulation leading to malfunction between 2-17h	1	2019-10-10 12:34	2019-10-10 12:41
	• Epanet CPA	C-Town BAS	C-Town Pumps manipulation	C-Town Pumps manipulation	3	2019-10-10 12:53	2019-10-10 12:56
	• Epanet CPA	C-Town BAS	Tank level sensor manipulation 2-17h - clone (213)	Manipulation of the water tank level sensor manipulation leading to malfunction between 2-17h	1	2019-10-11 10:50	2019-10-11 10:52

Scenario	Unmet demand (litres)	Nodes insufficiently supplied	Customers experiencing insufficient service	Customer minutes lost	System service hours lost
C-Town Pumps manipulation	8967619	334	99023	63897440	18.0
Tank level sensor manipulation 2-17h	1501534	175	47912	10780989	9.0
Tank level sensor manipulation 2-10h - clone (194)	261877	173	39869	1875543	2.0

GUI of SP: Visualising key results of simulated scenario(s)

STOP-IT

KPI tool: Assessment and detailed visualisation of results



Scenarios

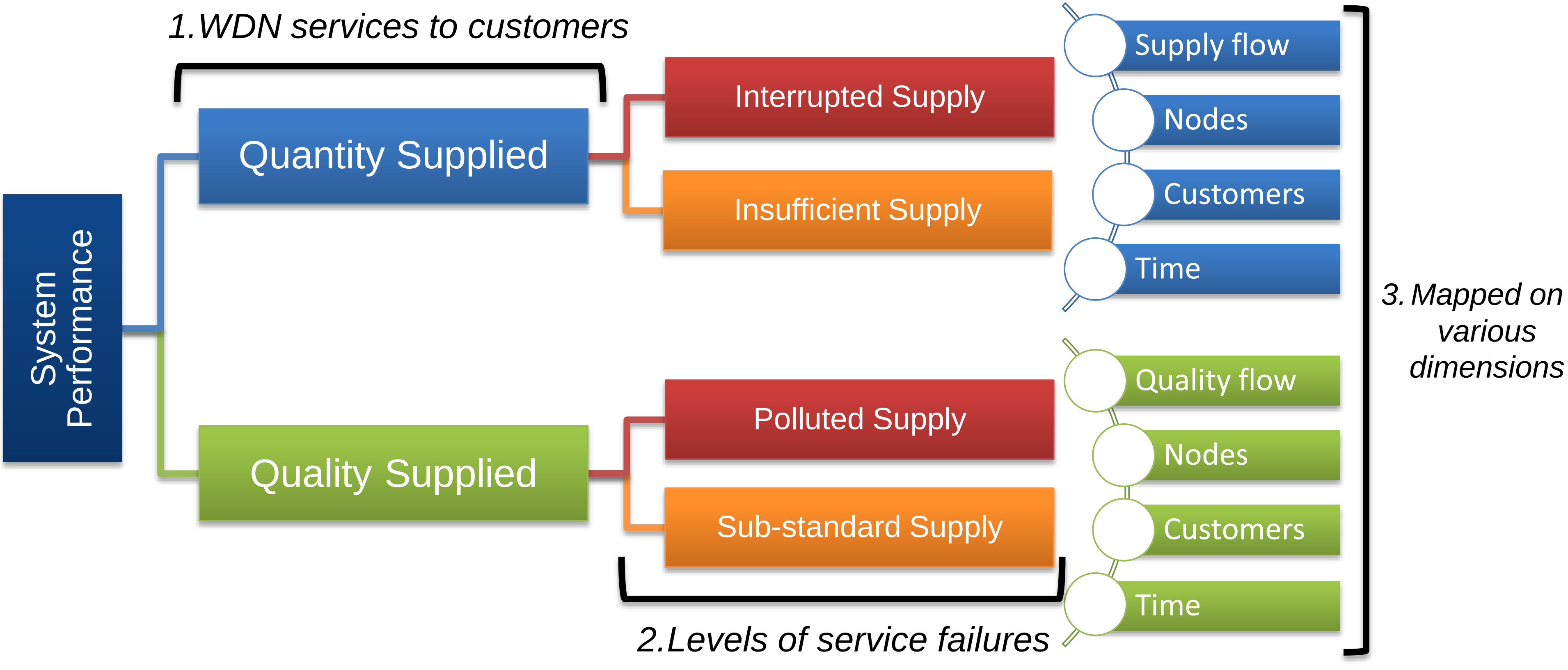
Show 10 entries

Search:

Operations	Tools	Base scenario	Name	Description	Events	Created	Executed
	• Epanet CPA		C-Town BAS	Business-As-Usual Scenario	0	2019-03-20 13:56	2019-03-22 17:02

STOP-IT KPI Tool: Framework behind the tool (1/2)

WDN optimal performance is to provide sufficient quantity and quality water, covering customer's needs (and expectations) in the entire network 24hrs a day, 7 days a week!

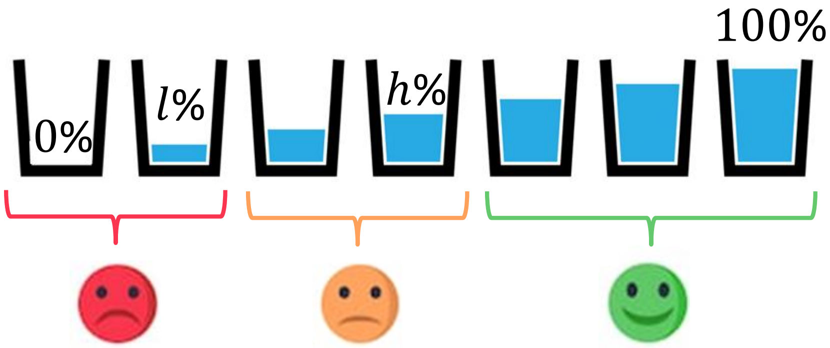


1.Complete service failure

2.Partial service failure

STOP-IT KPI Tool: Framework behind the tool (2/2)

Quantity Supplied



Critical Moderate

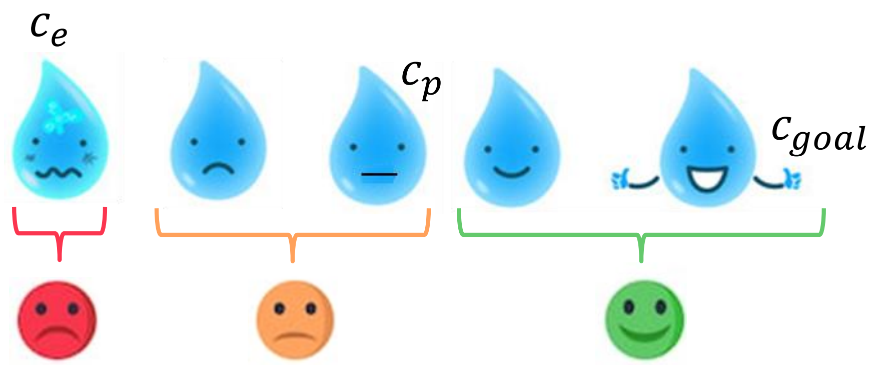
Interrupted Supply

$Supply < l * Demand$, where l is the service level below which customers don't open the tap

Insufficient Supply

$Supply < h * Demand$, where h is the threshold below which customers are not fully satisfied (i.e. reputational damage)

Quality Supplied



Critical Moderate

Polluted Supply

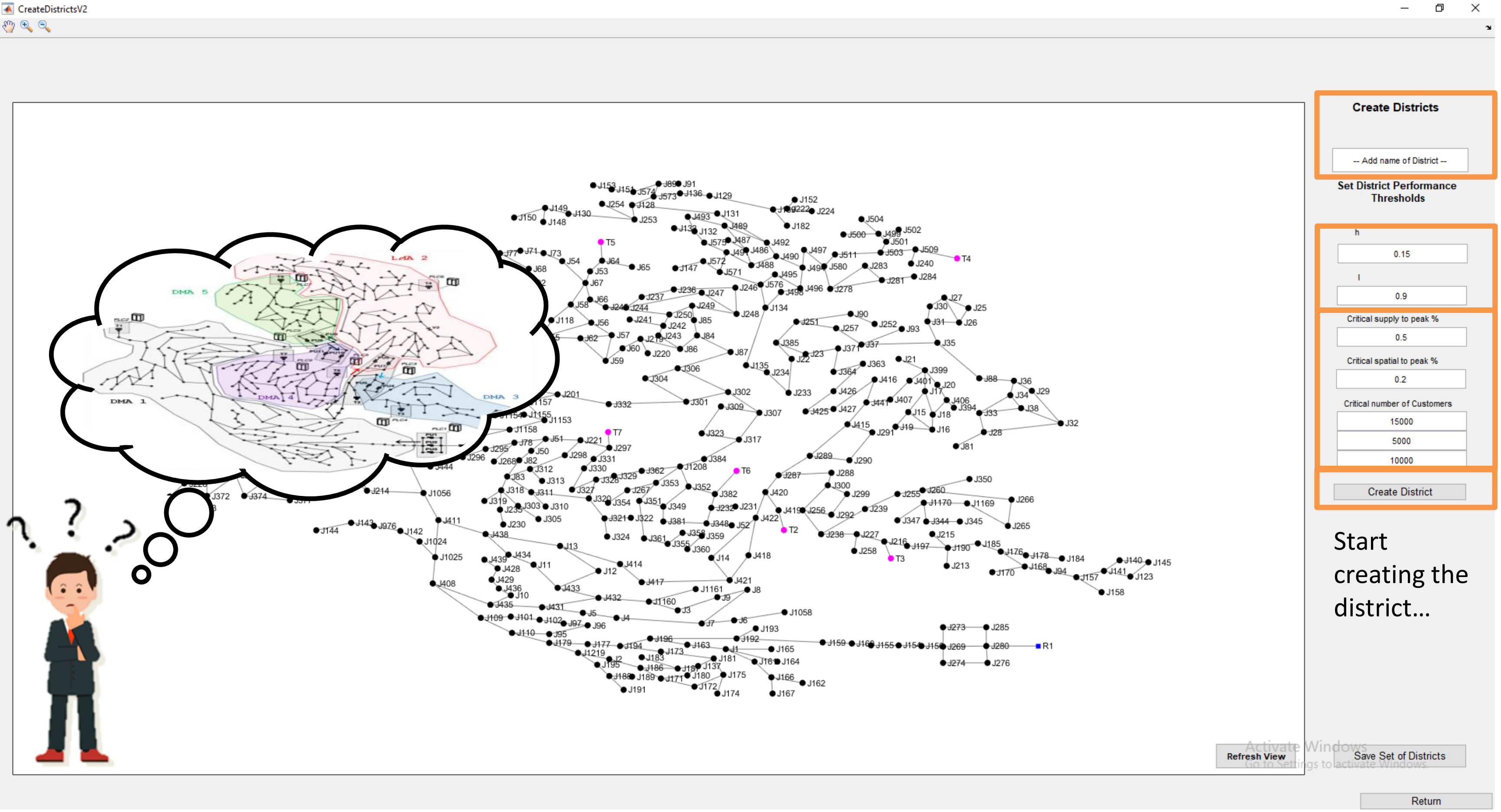
$c \geq c_e$, where $c_e$is the threshold concentration deemed critical for humans health, including lethality e.g. LC_{50}

Sub-standard Supply

$c_e > c > c_p$, where c_p is the permissible concentration threshold, based on legislation, regulations or standards. No major health related impacts causing discomfort but is not life threatening

Similar to an amber and red alert for the system!!!

STOP-IT KPI tool: Defining service levels and thresholds for critical customers



Create Districts

-- Add name of District --

Set District Performance Thresholds

h: 0.15

l: 0.9

Critical supply to peak %: 0.5

Critical spatial to peak %: 0.2

Critical number of Customers: 15000, 5000, 10000

District ID

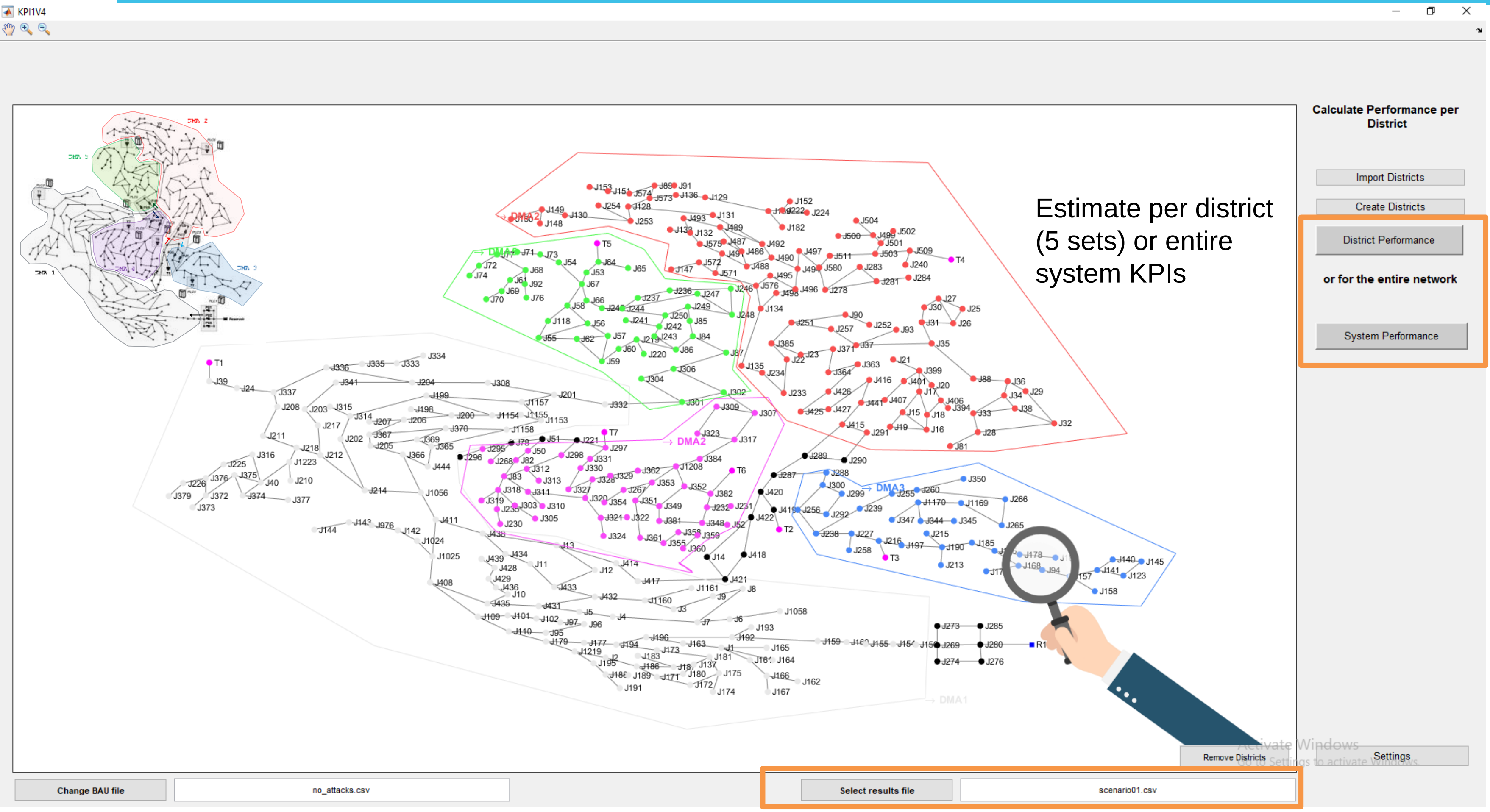
Set service levels

Set critical state levels

Start creating the district…

Through the GUI users can set the **service levels,** but also set different thresholds for **critical customers**.

STOP-IT KPI tool: Defining districts



Change BAU file: no_attacks.csv

Select results file: scenario01.csv

Estimate per district (5 sets) or entire system KPIs

Load STP results to translate to KPIs

Users can:

- ❑ Set the **service levels** for **different districts**
- ❑ Visualise results and STOP-IT KPIs **for any grouping they choose** (DMAs etc)

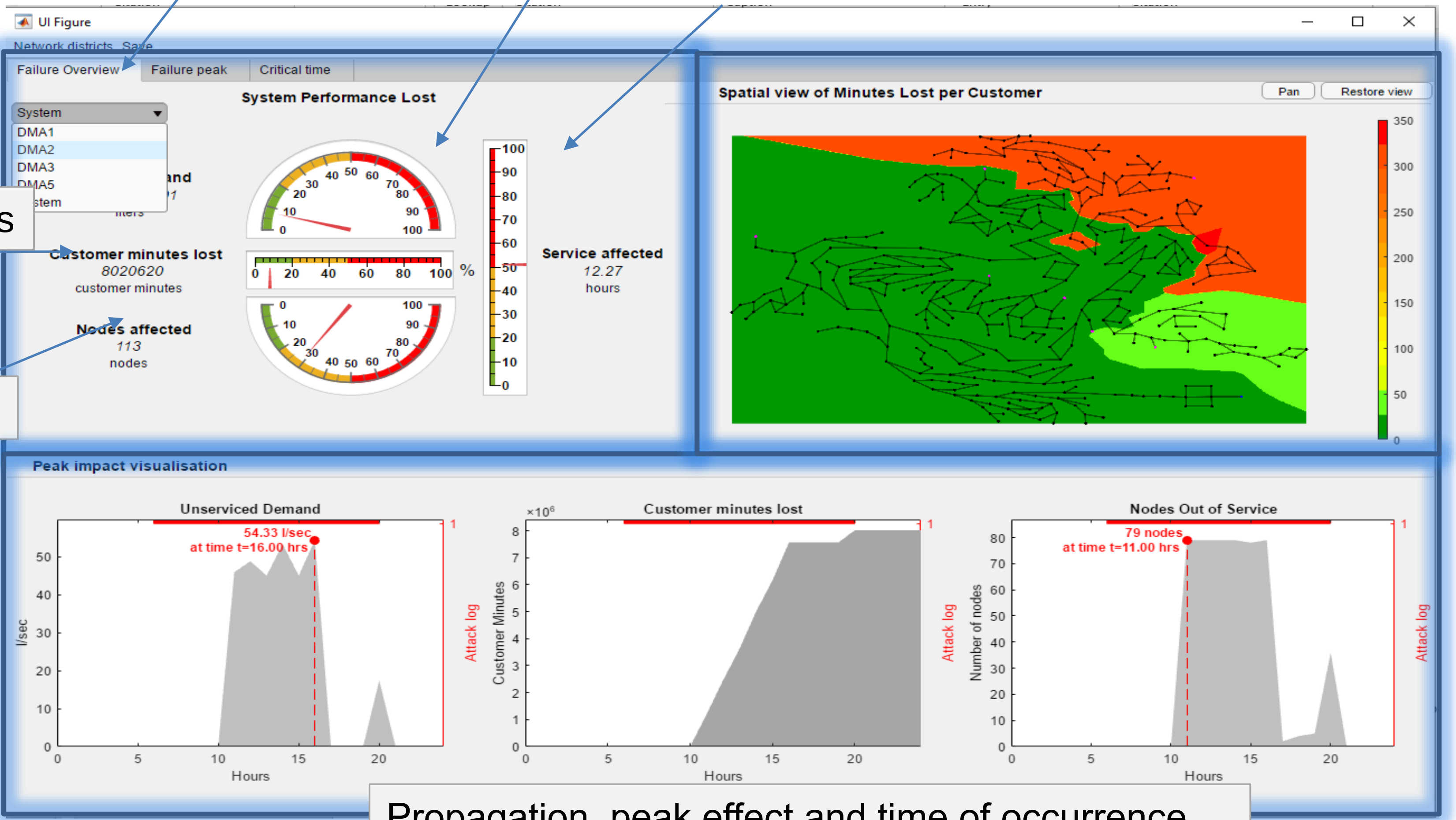
STOP-IT

KPI tool : Assessment of quantity issues results

For the system.. Or each district

Supply…

Time



UI Figure

Network districts Save

Failure Overview | Failure peak | Critical time

System Performance Lost

System
DMA1
DMA2
DMA3
DMA5
System

Customer minutes lost
8020620
customer minutes

Nodes affected
113
nodes

Service affected
12.27
hours

Spatial view of Minutes Lost per Customer

Pan | Restore view

Peak impact visualisation

Unserviced Demand: 54.33 l/sec at time t=16.00 hrs

Customer minutes lost

Nodes Out of Service: 79 nodes at time t=11.00 hrs

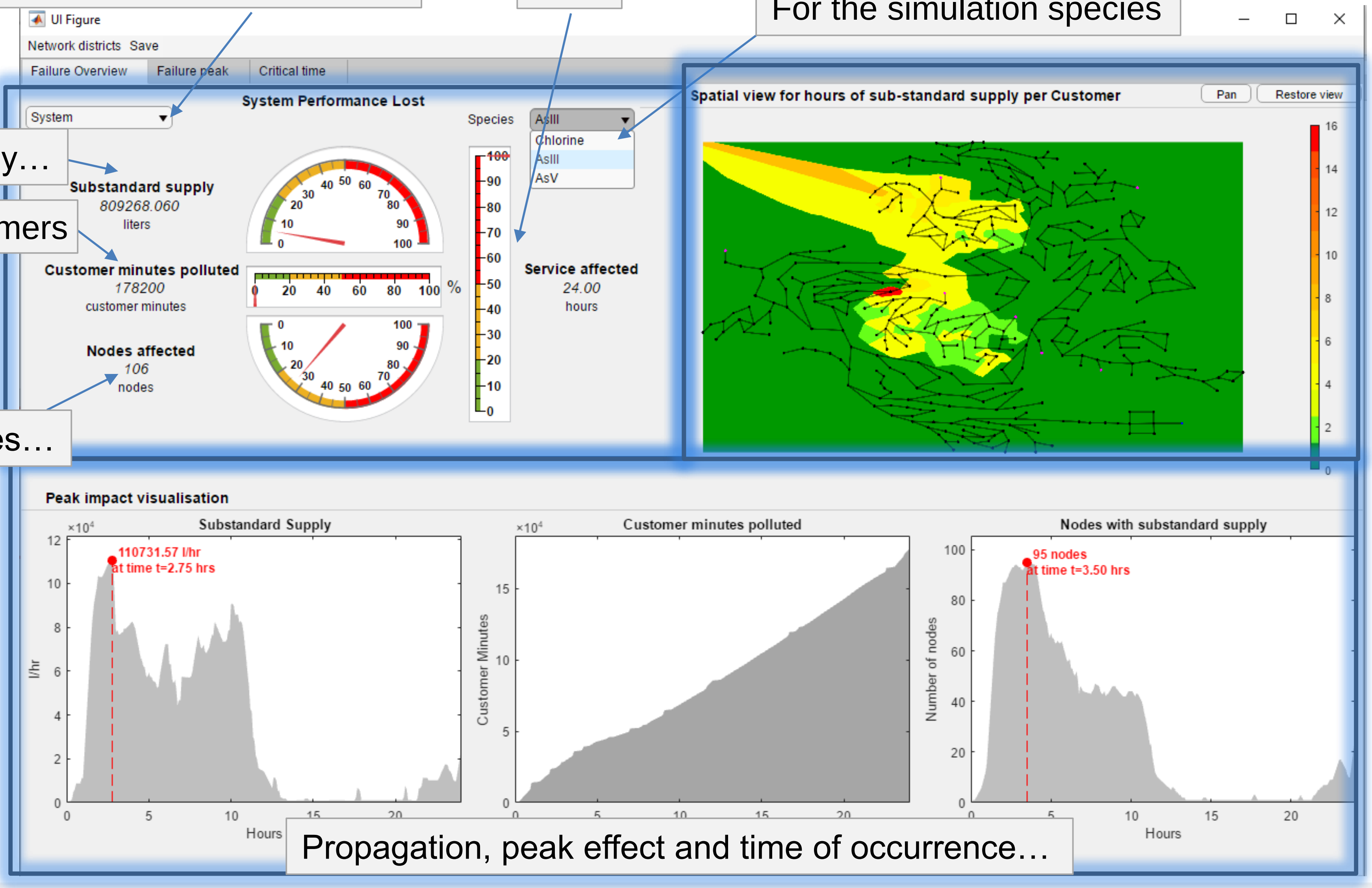
Customers

Nodes…

Propagation, peak effect and time of occurrence…

STOP-IT

KPI tool : Assessment of quality issues results



For the system.. Or each district

Time

For the simulation species

Supply…

Customers

Nodes…

Propagation, peak effect and time of occurrence…

UI Figure

Network districts Save

Failure Overview | Failure peak | Critical time

System Performance Lost

System

Species: AsIII (Chlorine, AsIII, AsV)

Substandard supply
809268.060
liters

Customer minutes polluted
178200
customer minutes

Nodes affected
106
nodes

Service affected
24.00
hours

Spatial view for hours of sub-standard supply per Customer

Peak impact visualisation

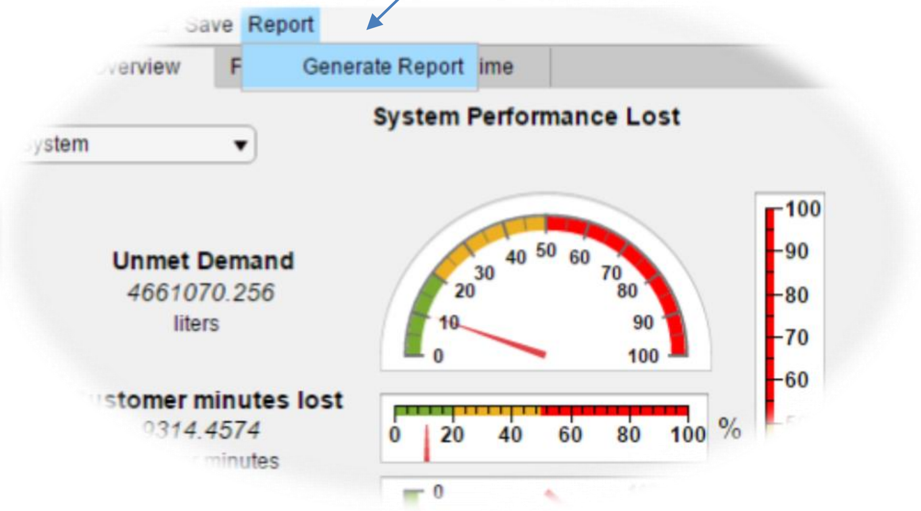
Substandard Supply: 110731.57 l/hr at time t=2.75 hrs

Customer minutes polluted

Nodes with substandard supply: 95 nodes at time t=3.50 hrs

KPI tool: Generating Risk Analysis Reports

Generate Risk Analysis Report

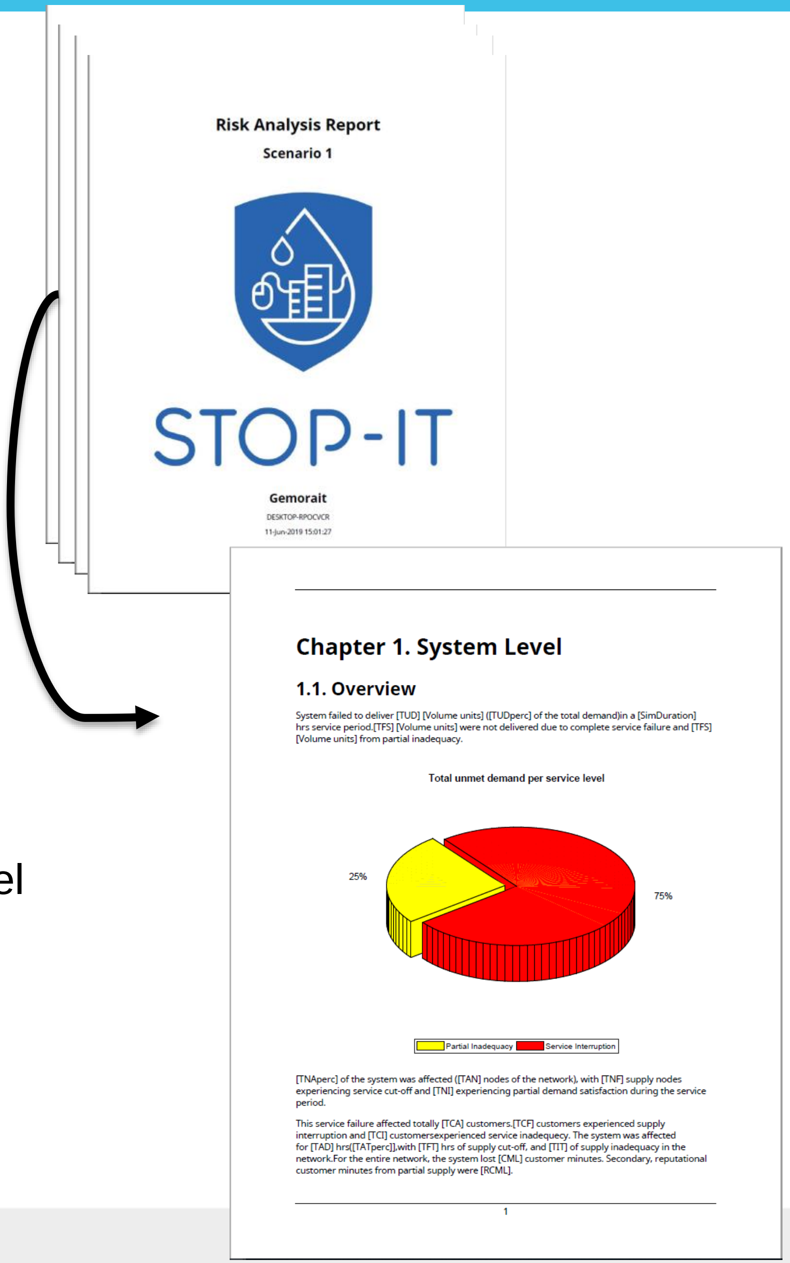


Unmet Demand
4661070.256
liters

stomer minutes lost
9314.4574
minutes

Fully automated report generation with a push of a button…

- Report System and Critical Customer District 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



Risk Analysis Report

Scenario 1

STOP-IT

Gemorait

DESKTOP-RPOCVCR

11-Jun-2019 15:01:27

Chapter 1. System Level

1.1. Overview

System failed to deliver [TUD] [Volume units] ([TUDperc] of the total demand)in a [SimDuration] hrs service period.[TFS] [Volume units] were not delivered due to complete service failure and [TFS] [Volume units] from partial inadequacy.

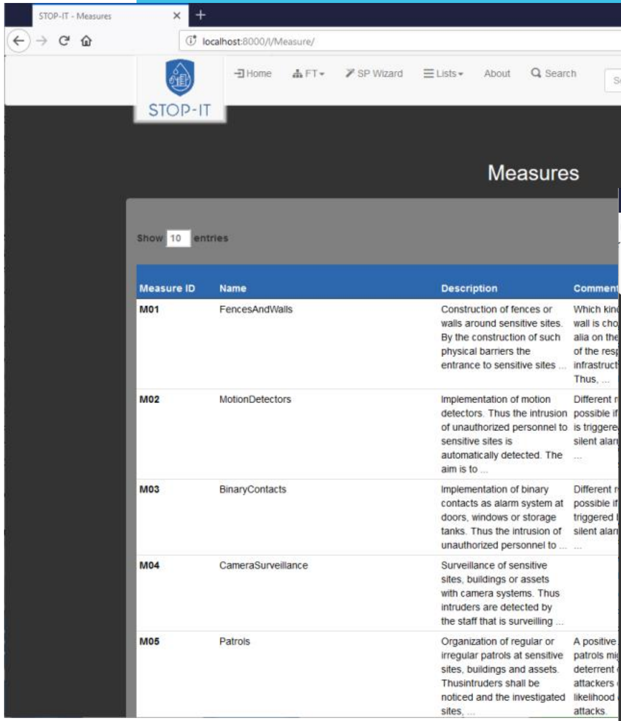
Total unmet demand per service level

[TNAperc] of the system was affected ([TAN] nodes of the network), with [TNF] supply nodes experiencing service cut-off and [TNI] experiencing partial demand satisfaction during the service period.

This service failure affected totally [TCA] customers.[TCF] customers experienced supply interruption and [TCI] customersexperienced service inadequecy. The system was affected for [TAD] hrs([TATperc]],with [TFT] hrs of supply cut-off, and [TIT] of supply inadequacy in the network.For the entire network, the system lost [CML] customer minutes. Secondary, reputational customer minutes from partial supply were [RCML].

1

STOP-IT Scenario Planner: incorporating measures

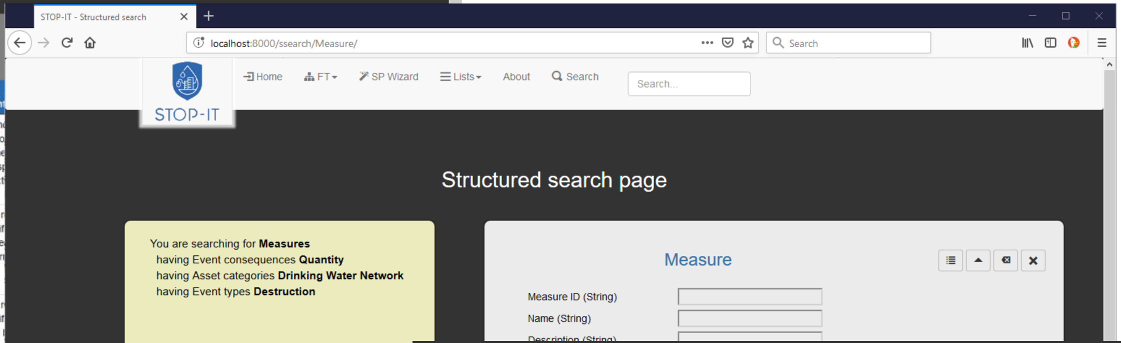


Measures

Show 10 entries

Measure ID	Name	Description	Comment
M01	FencesAndWalls	Construction of fences or walls around sensitive sites. By the construction of such physical barriers the entrance to sensitive sites ...	Which kind wall is cho alia on the of the resp infrastruct Thus, ...
M02	MotionDetectors	Implementation of motion detectors. Thus the intrusion of unauthorized personnel to sensitive sites is automatically detected. The aim is to ...	Different r possible if is triggere silent alar ...
M03	BinaryContacts	Implementation of binary contacts as alarm system at doors, windows or storage tanks. Thus the intrusion of unauthorized personnel to ...	Different r possible if triggered I silent alar ...
M04	CameraSurveillance	Surveillance of sensitive sites, buildings or assets with camera systems. Thus intruders are detected by the staff that is surveilling ...	
M05	Patrols	Organization of regular or irregular patrols at sensitive sites, buildings and assets. Thusintruders shall be noticed and the investigated sites, ...	A positive patrols mi deterrent attackers likelihood attacks. ...

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



Structured search page

You are searching for **Measures**
having Event consequences **Quantity**
having Asset categories **Drinking Water Network**
having Event types **Destruction**

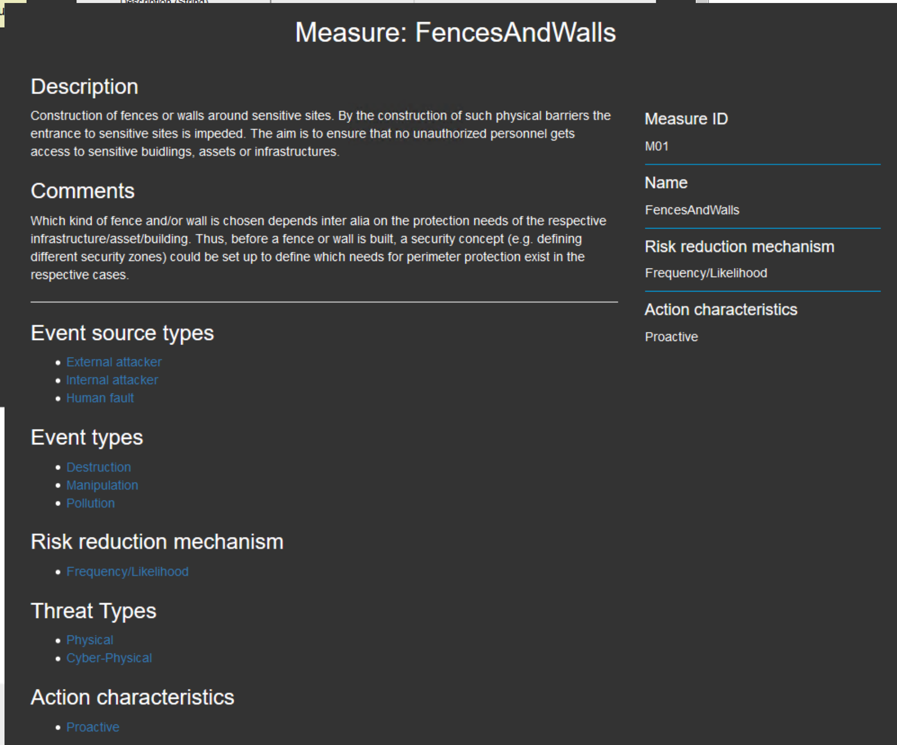
16 items fou

✖ Cancel ☰ Show me

Measure

Measure ID (String)
Name (String)
Description (String)

GUI of SP supporting multiple filtering capabilities



Measure: FencesAndWalls

Description

Construction of fences or walls around sensitive sites. By the construction of such physical barriers the entrance to sensitive sites is impeded. The aim is to ensure that no unauthorized personnel gets access to sensitive buildings, assets or infrastructures.

Comments

Which kind of fence and/or wall is chosen depends inter alia on the protection needs of the respective infrastructure/asset/building. Thus, before a fence or wall is built, a security concept (e.g. defining different security zones) could be set up to define which needs for perimeter protection exist in the respective cases.

Event source types

- External attacker
- Internal attacker
- Human fault

Event types

- Destruction
- Manipulation
- Pollution

Risk reduction mechanism

- Frequency/Likelihood

Threat Types

- Physical
- Cyber-Physical

Action characteristics

- Proactive

Measure ID
M01

Name
FencesAndWalls

Risk reduction mechanism
Frequency/Likelihood

Action characteristics
Proactive

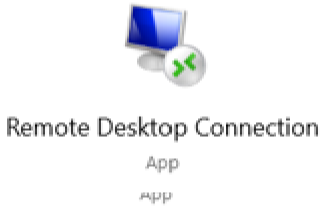
GUI of SP on the detailed page of a measure

STOP-IT

Accessing Module I VM

Tools are accessible through the WP4 VM

Simply…

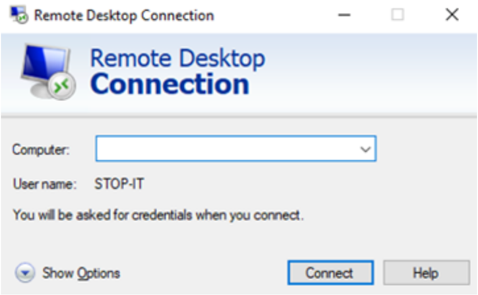


Remote Desktop Connection

App

App

Open Remote Desktop Connection
(Already available in Windows 10)



Remote Desktop Connection

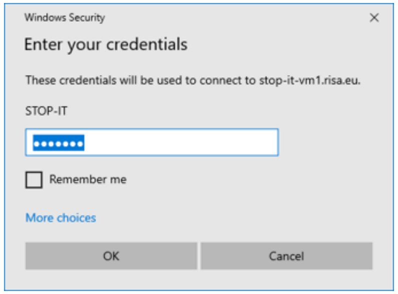
Remote Desktop Connection

Computer:

User name: STOP-IT

You will be asked for credentials when you connect.

State the VM
(defined for FLs)



Windows Security

Enter your credentials

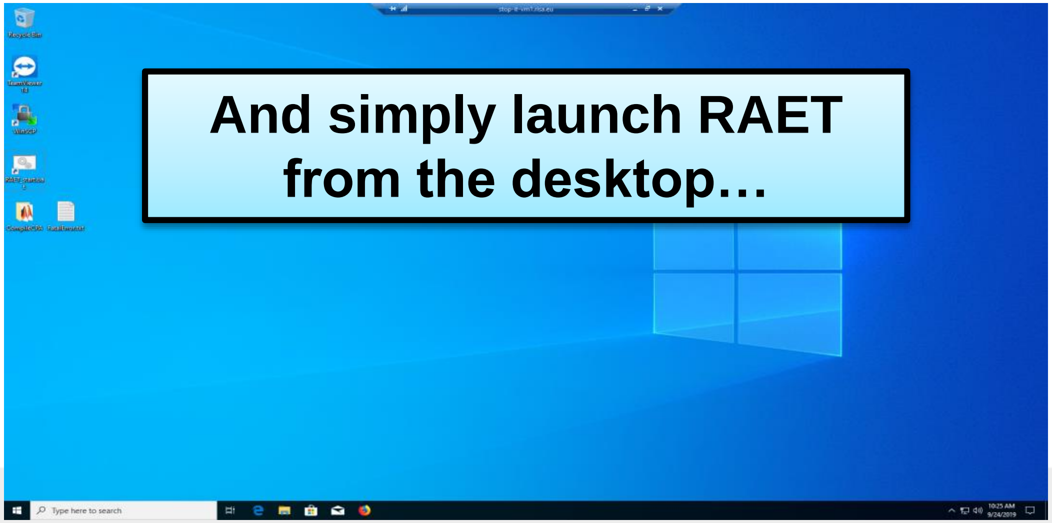
These credentials will be used to connect to stop-it-vm1.risa.eu.

STOP-IT

•••••••

□ Remember me

Enter your credentials
(to be provided for FLs…)



And simply launch RAET from the desktop…

Supportive material

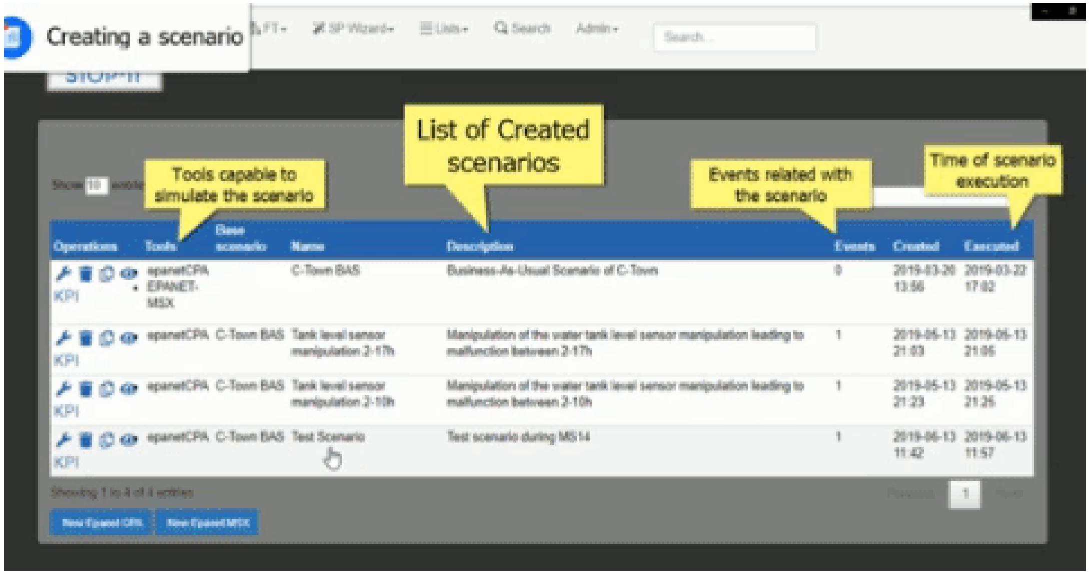
- Overview of RAET
- Scenarios of use
- RAET user's guide
- KPI tool user's guide
- Test data

Supportive material – RAET overview

Overview of RAET

Introducing the building block of Module I

Get familiar with software interfaces & purposes



List of Created scenarios

Tools capable to simulate the scenario

Events related with the scenario

Time of scenario execution

Operations	Tools	Base scenario	Name	Description	Events	Created	Executed
KPI	epanetCPA • EPANET-MSX		C-Town BAS	Business-As-Usual Scenario of C-Town	0	2019-03-20 13:56	2019-03-22 17:02
KPI	epanetCPA	C-Town BAS	Tank level sensor manipulation 2-17h	Manipulation of the water tank level sensor manipulation leading to malfunction between 2-17h	1	2019-05-13 21:03	2019-05-13 21:06
KPI	epanetCPA	C-Town BAS	Tank level sensor manipulation 2-10h	Manipulation of the water tank level sensor manipulation leading to malfunction between 2-10h	1	2019-05-13 21:23	2019-05-13 21:26
KPI	epanetCPA	C-Town BAS	Test Scenario	Test scenario during MS14	1	2019-06-13 11:42	2019-06-13 11:57

Showing 1 to 4 of 4 entries

- •Screen recorded video
- •Quick overview
- •Useful callouts

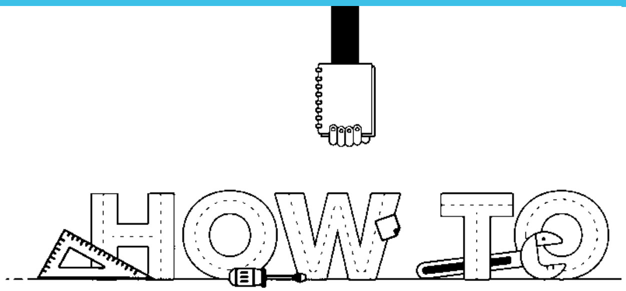
RAET introduction to: Create Simulate Assess cyberphysical scenarios

STOP-IT

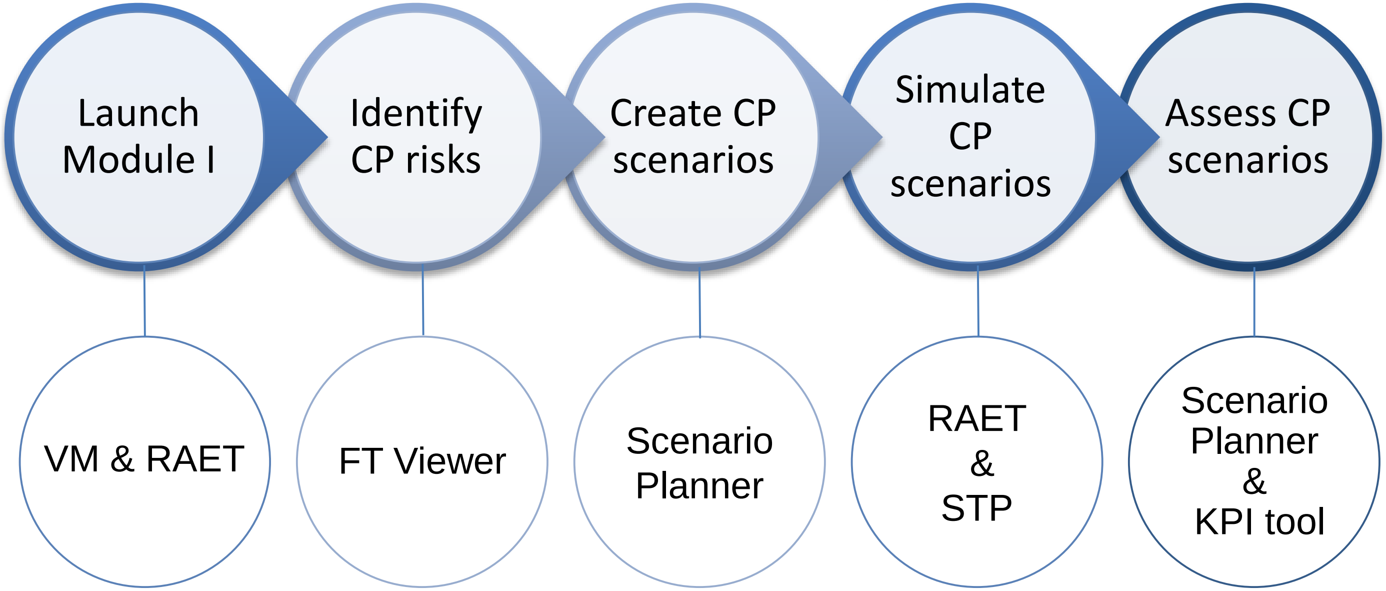
Supportive material – Scenario of Use

Scenarios of use

How to deploy Module I



A step-by-step demonstration guide to:


Launch Module I → Identify CP risks → Create CP scenarios → Simulate CP scenarios → Assess CP scenarios

VM & RAET

FT Viewer

Scenario Planner

RAET & STP

Scenario Planner & KPI tool

+ Risk reduction measures and toolkit library

Explore RAET capabilities

Follow the scenario instructions, discover major functionalities, utilize tools…

STOP-IT

Supportive material – RAET User’s Guide

RAET user’s guide

The RAET full guide

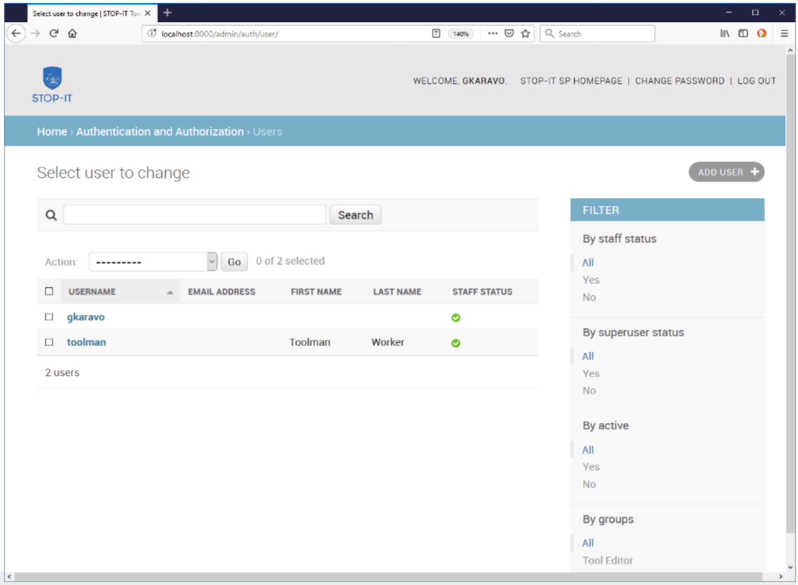
A manual for RAET, focused on its core components

Includes details on:

- ✓ FT Manager
- ✓ FT Viewer
- ✓ Tools Manager
- ✓ RIDB & RRMD searches

Written guide and associated images for different user roles:

- ➢ Simple user
- ➢ Modeler
- ➢ Administrator



Select user to change | STOP-IT Too
localhost:8000/admin/auth/user/
140%
Search

STOP-IT

WELCOME, GKARAVO. STOP-IT SP HOMEPAGE | CHANGE PASSWORD | LOG OUT

Home › Authentication and Authorization › Users

Select user to change

ADD USER +

Search

Action: --------- Go 0 of 2 selected

□	USERNAME	EMAIL ADDRESS	FIRST NAME	LAST NAME	STAFF STATUS
□	gkaravo				✓
□	toolman		Toolman	Worker	✓

2 users

FILTER

By staff status
All
Yes
No

By superuser status
All
Yes
No

By active
All
Yes
No

By groups
All
Tool Editor

STOP-IT

Supportive material – KPI tool User’s Guide

KPI tool user’s guide

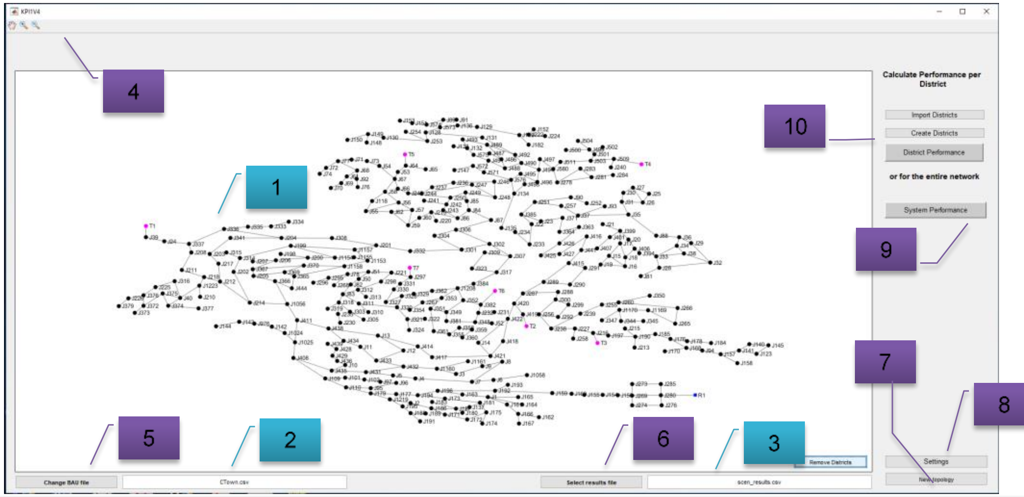
The KPI tool full guide

A manual for KPI tool, in high detail

Details focused on:

- ➢ Loading data
- ➢ Setting parameters
- ➢ Exploring KPIs
- ➢ Generating Risk Report

Written guide and associated images in a step wise approach



Supportive material – Test data

Test data

Ready to test Module I

All required data are included in the starter pack!

A demo cyber-physical network is ready for you in the VM…

STOP-IT

THANK YOU FOR YOUR ATTENTION

www.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.