



# STOP-IT

## **Deliverable 4.4: Cyber – physical threats stress – testing platform**

SINTEF  
November 2019

[stop-it-project.eu](http://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 author's views and the European Union is not liable for any use that may be made of the information contained therein.



## Development of a stress-testing platform for mitigation options

### D4.4: CYBER – PHYSICAL THREATS STRESS – TESTING PLATFORM

#### SUMMARY

This report describes the details of STOP-IT cyber-physical threats stress-testing approach. The approach can be divided into two distinct but interconnected parts. The first part focuses on the cyber and physical infrastructures and by using models, the system can be stress-tested based on scenarios developed for instance in Risk Identification Database (WP3 of the project). The second part focuses on the provision of a gaming-approach for training the skills available in a water company and documenting the available processes/solutions to deal with stressors and to improve these by identifying the gaps and determine possible solutions. To this end, TORC is adopted as a gaming approach to stress test the organizational resiliency of a water utility in case of cyber and/or physical attacks. The use of these two parts are ensured in WP8 for training and transfer activities to deal with cyber, physical threats and combination of these two in water utilities.

#### DELIVERABLE NUMBER

#### WORK PACKAGE

D4.4

WP4

#### LEAD BENEFICIARY

#### DELIVERABLE AUTHOR(S)

SINTEF AS

Mehdi Ahmadi (SINTEF)  
 Rita Ugarelli (SINTEF)  
 Tor Olav Grøtan (SINTEF)  
 Gema Raspati (SINTEF)  
 Ingrid Selseth (SINTEF)  
 Christos Makropoulos (KWR)  
 Dionysios Nikolopoulos (ICCS)  
 Georgios Moraitis (ICCS)  
 George Karavokiros (ICCS)  
 Dimitrios Bouziotas (KWR)  
 Archontia Lykou (ICCS)  
 Ioannis Tsoukalas (ICCS)

#### QUALITY ASSURANCE

Relly Baron  
Patrick Smeets

Mekorot  
KWR

#### PLANNED DELIVERY DATE

#### ACTUAL DELIVERY DATE

30/11/2019

31/12/2019

#### DISSEMINATION LEVEL

- PU = Public
- PP = Restricted to other programme participants
- RE = Restricted to a group specified by the consortium.  
Please specify: \_\_\_\_\_
- CO = Confidential, only for members of the consortium



## Table of contents

TABLE OF CONTENTS .....	II
LIST OF FIGURES .....	IV
LIST OF TABLES.....	V
LIST OF ACRONYMS AND ABBREVIATIONS.....	VI
EXECUTIVE SUMMARY .....	1
1 INTRODUCTION .....	2
2 CYBER-PHYSICAL THREATS STRESS-TESTING PLATFORM.....	5
2.1 <i>Stress-testing</i> .....	5
2.1.1 System-wide stress testing.....	5
2.2 <i>STOP-IT stress-testing platform models and approach</i> .....	11
2.2.1 STOP-IT stress-testing platform within an integrated framework.....	11
2.2.2 epanet-CPA .....	14
2.2.3 EPANET-MSX .....	19
2.2.4 RISKNOUGHT.....	20
2.3 <i>Stress-testing methodology for Water Distribution Networks</i> .....	23
2.3.1 Methodology for stress-testing in the context of STOP-IT .....	23
2.3.2 Integration with the RAET.....	27
2.4 <i>Stress-testing platform in WP4</i> .....	32
3 TRAINING FOR OPERATIONAL RESILIENCE (TORC) .....	34
3.1 <i>Training for Operational Resilience (TORC)</i> .....	34
3.1.1 Training for Operational Resilience: the TORC original version .....	34
3.1.2 The expected aims for training with TORC .....	35
3.1.3 The TORC references .....	36
3.2 <i>The STOP-IT training for operational resilience</i> .....	38
3.2.1 Purpose of adopting TORC in STOP-IT .....	38
3.2.2 Adaptation of TORC to STOP-IT .....	39
3.2.3 Expected benefit from TORC .....	40
3.3 <i>The STOP-IT TORC gaming approach</i> .....	41
3.3.1 The STOP-IT TORC Game inventory.....	41
3.3.2 The board game pad .....	41
3.3.3 The resource cards.....	42
3.3.4 The Risk Reduction Measures cards .....	43
3.3.5 The value cards .....	46
3.3.6 The players and their roles .....	46
3.4 <i>Playing the STOP-IT TORC game</i> .....	48



3.4.1	How to play the game .....	50
3.4.2	Case: denial of service due to signal jamming .....	54
3.5	<i>Recommendation for the facilitator</i> .....	55
3.5.1	Calibrating the training scenario according to objective .....	55
3.5.2	Description of the role of the facilitator .....	55
3.5.3	Preparatory work of the facilitator .....	57
3.6	<i>TORC use in STOP-IT WP8</i> .....	60
4	REFERENCES .....	61
5	ANNEX A: STP INTERFACE .....	67
5.1	<i>Simulation results</i> .....	67
5.1.1	Retrieve Simulation results .....	67
5.1.2	API response .....	67
5.2	<i>Scenario data for EPANET CPA</i> .....	70
5.2.1	API response .....	70
5.3	<i>Notifications to RAET</i> .....	70
6	ANNEX B: THE TORC INVENTORY .....	72
6.1	<i>TORC GAME BOARD</i> .....	72
6.2	<i>RESOURCE CARDS</i> .....	73
6.3	<i>RISK REDUCTION CARDS</i> .....	80
6.4	<i>VALUE CARD</i> .....	146



## List of Figures

Figure 1: Scenario types for stress-testing UWS grouped by magnitude and rate of change over a design horizon (Makropoulos et al, 2018).....	7
Figure 2: Graphical representations of resilience and robustness as results from stress-testing scenarios (adapted from Makropoulos et al, 2018) .....	7
Figure 3: STOP-IT Risk Assessment and Treatment process (figure reproduced from D4.2).....	12
Figure 4: STOP-IT Risk Assessment and Treatment Framework & its components (figure reproduces from D4.2) .....	13
Figure 5: Process workflow for stress-testing using epanetCPA.....	16
Figure 6: The impact of a cyber-physical attack to nodal pressure and demand in a C-Town node, provided by three of the provided engine options. ....	18
Figure 7: Schematic representation of RISKNOUGHT simulation step (Nikolopoulos et al. n.d.).....	22
Figure 8: Schematic representation of the Stress Testing Platform and its components .....	24
Figure 9: RAET homepage, including the illustration which links to the Stress-Testing Platform (STP).....	28
Figure 10: Stress-test procedures list page .....	30
Figure 11: Selection of the base scenario for the stress-testing procedure .....	30
Figure 12: Specification of control variables parameters .....	31
Figure 13: Stress Test procedure page.....	32
Figure 14: High level scenarios of use of Module I tools .....	33
Figure 15: The STOP-IT TORC board game pad.....	42
Figure 16: Template of the resource cards .....	42
Figure 17: Example of RRM card .....	45
Figure 18: Template of the value cards.....	46
Figure 19: Key features of playing the TORC game.....	49



## List of Tables

Table 1: Symbols and colors used in the RRM cards for quick identification of the type of threat originating a risk event .....	43
Table 2: Symbols used in the RRM cards for quick identification of the type of asset affected by the outcome of the risk event .....	44
Table 3: Symbols used in the RRM cards for quick identification of the event consequence .....	45
Table 4: Playing with STOP-IT TORC .....	53
Table 5: Example of playing with STOP-IT TORC .....	54
Table 6: Returned simulation results structure .....	67
Table 7: Returned scenario data for EPANET CPA .....	70



## List of Acronyms and Abbreviations

API	: Application Programming Interface
AS	: Advanced Search
AVAT	: Asset Vulnerability Assessment Tool
CI	: Critical Infrastructure
CPA	: Cyber-Physical Attack
CPS	: Cyber-Physical System
D	: Deliverable
DB	: Database
DDA	: Demand Driven Analysis
DLL	: Dynamic Linked Library
DoS	: Denial-Of-Service
EPA	: Environmental Protection Agency
FL	: Follower water utilities
FR	: Front Runner water utilities
FT	: Fault Tree
GUI	: Graphical User Interface
HMI	: Human-Machine Interface
ICT	: Information and Communication Technology
IT	: Information Technology
KPI	: Key Performance Indicator
MSX	: Multi Species Extension
NFV	: Network Function Virtualization
NHFR	: Nodal Head-Flow Relationship



OWA	: Open Water Analytics
PDA	: Pressure Driven Analysis
PDD	: Pressure Driven Demand
PLC	: Programmable Logic Controller
RAET	: Risk Analysis and Evaluation Toolkit
REA	: Resilience Engineering Association
RET	: Risk Exploration Tool
RIDB	: Risk Identification Data Base
RRM	: Risk Reduction Measure
RRMD	: Risk Reduction Measure Database
SCADA	: Supervisory Control and Data Acquisition
SDN	: Software-Defined Networks
SP	: Scenario Planner
SQL	: Structured Query Language
STM	: Stress-Testing Management
STP	: Stress-Testing Platform
TCP	: Transmission Control Protocol
TL	: Toolkit Library
TORC	: Training for Operational Resilience
UWS	: Urban Water System
WDN	: Water Distribution Network
WNTR	: Water Network Tool for Resilience
WP	: Work Package





## Executive summary

This report describes the STOP-IT stress-testing approach for water critical infrastructures under physical, cyber threats and/or combination of these two. These infrastructures can be roughly divided into hard and soft levels (hard: physical and cyber infrastructures; soft: human expertise and organizational procedures and settings to encounter risks and stressors). Considering the premises of the STOP-IT project, stress-testing of these two levels provides a test bed for alternative risk treatment options (both for RRM included in the RRMD and the technologies provided in WP5 of the project).

On the hard level, Cyber-physical threats stress-testing platform, deals with stress-testing procedures and their appliance in the context of STOP-IT project using models. A concise literature review sets the scene with related methods seen in urban water systems and the links with system resilience and robustness. As reviewed, stress-tests are commonly performed by decision makers for a variety of reasons in order to quantify performance under uncertainty and extreme conditions deviating from normal operations, as can be the case with cyber-physical attacks. As such events are typical and their statistical characteristic unknown, the rationale for the use of scenarios is elaborated.

Some models that can be used with stress-testing procedures are also presented from the two main categories: a) emulation-based and b) simulation-based approaches to cyber-physical model formulation. As explained, simulation-based approaches bear some significant advantages in the form of easier coupling to physical processes and scenario creation, with the drawback of reduced fidelity in bit-wise cyber process detail. This drawback is not very significant when exploring and speculating cyber-security in stress-testing scenarios, when the result of an event is more important than the exact cause of it. Therefore, in the context of STOP-IT, a simulation based approach is used in the stress-testing methodology developed. The specific models utilized in STOP-IT stress testing platform are reviewed in Section 2.2. The interconnection of the cyber-physical models with other tools in the Risk Analysis and Evaluation Toolkit (RAET), along with the formal stress-testing step by step methodology description, are elaborated in Section 2.3.

On the soft level, STOP-IT provides a gaming-approach for training the skills available in a water company and documenting the available processes/solutions to deal with stressors and to improve these by identifying the gaps and determine possible solutions. To this end, TORC is adopted as a gaming approach to stress test the organizational resiliency of a water utility in case of cyber and/or physical attacks. The scope of the game is about being trained at avoiding mistakes that it is possible to anticipate and prepare for, while also being able to handle unexpected situations, disturbances and disruptions that will inevitably arise. Dealing with the expected and the unexpected requires relatively different organizational abilities. The focus of TORC is how these two abilities can be merged. Therefore, Chapter 3 of this report provides details on how the game is designed, how a gaming session should be conducted and provides detailed information on the relation of the game with other STOP-IT outcomes. The use of TORC is ensured through WP8 in the project.



## 1 Introduction

Both from a public health and an economic perspective, water supply represents a critical infrastructure that must be protected. The current trend of water sector, the digitalization, brings abundant opportunities but also some new challenges and risks for water utilities. The introduction of new digital systems and devices need new types of expertise for their operations and being prepared for any incidents due to these changes. In order to address these issues, the overall strategic objective of the STOP-IT project is to make water systems secure and resilient by improving preparedness, awareness and response level to physical, cyber threats, and their combination.

The STOP-IT project provides several solutions in strategic, tactical and operational level of risk management framework (based on ISO 31000-2009) for the physical and cyber protection of water critical infrastructures. In addition, the project builds on a Front Runner (FR) and Follower (FL) approach. Within this approach, FR water utilities will demonstrate the solutions provided in the project and will be twinned with FL water utilities in order to raise awareness and preparedness, stimulate mutual learning, transfer, and uptake of solutions.

In line with the overall objectives of the project, WP4 of STOP-IT project aims at developing a risk assessment and treatment framework in strategic and tactical levels and provide a toolkit able to analyse and evaluate physical and cyber risks on water critical infrastructures and their combination to support the choice of appropriate risk treatment options (risk-reduction measures) and evaluate their effectiveness.

One of the means of testing and measuring the robustness of a water system is pushing the system beyond its normal operational conditions in order to observe the resulting behavior and determine through formal analysis the stability of the system against stressors. This approach is called stress-testing a system. Stress-testing is pertinent to systems that exhibit inherent uncertainty in their operation, their future state and/or the external pressures that act upon them.

The water systems can be roughly divided into the hard and soft levels (hard: physical and cyber infrastructures; soft: human expertise and organizational procedures and settings to encounter risks and stressors).

**On the hard level**, stress-testing through modelling is broadly used to explore the ability of the water systems to provide water under a certain number of stressor(s) and scenarios and the continuity of the service both considering the amount and the quality of the water provided. The outcome of this step can be used to compare different system's settings in the improvement planning phase to implement/modify risk reduction measures.

STOP-IT stress-testing platform models covering the hardware level is described in Chapter 2 of this report. This builds on the overall WP3-WP4 results in the project. The nature of cyber-physical threats (i.e. uncertainty, non-repeatability, unknown adversaries, high impact etc.) makes the stress-testing methodology essential in understanding cyber-physical



systems' behavior under attack and the resulting consequences. To do so, a complete cyber-physical modelling platform should be constructed. Chapter 2 of this report provides an overview of the available tools to model both cyber and physical worlds together for stress-testing purposes. Afterwards, it describes STOP-IT stress-testing modelling platform mainly based on epanet-CPA by building on several other components provided in the project such as scenario-planner (SP) tool and Risk Analysis and Evaluation Toolkit (RAET). The user can test a single or multiple scenarios defined (or inspired based on Risk Identification Database provided in WP3 of the project). Then, the results of the scenario(s) are translated to KPI defined in D4.2 and can be exported to other STOP-IT tools.

**On the soft level**, STOP-IT provides, within this task and report, a gaming-approach for training the human skills available in a water company and documenting the available processes to deal with stressors and to improve these by identifying the potential gaps and determine contextually possible solutions.

Chapter 3 of this report described "Training for Operational Resilience (TORC)" which is designed to facilitate organizations and teams that seek to reveal, understand, articulate, demonstrate and/or develop their inherent repertoire of resilient performance in face of unexpected deviations, disturbances and shocks as a training-by-gaming approach. The outcomes and experiences are captured in a way that prepares them to be used as raw material of technological, human, organizational and managerial priorities and resources that are needed to transform the experience from the training exercise into effective resilience capabilities under a more formal managerial supervision. The TORC game setup is available for free and comprises a paper-based game board, and generic supporting material regarding intake and preparation for TORC training. This will be used in WP8 for training and transfer purposes within the premises of the project and beyond.

The simplicity of the TORC approach and gaming material per se is somewhat counterweighed by the need to prepare detailed training material for specific training contexts, e.g., specifications of the operational situations subject to potential disturbance, and the specific disturbances that emulates the "surprise" for trainees as system's stressors. The common ground for any application of TORC is the premise that resilient properties may not be "imported" from the outside as a ready-to-go concept but should be nurtured and developed by addressing and naming the existing rudiments of resilience through training on practical situations. By actively using the practitioners' own language, it is also possible to reinforce and build a resilience inventory in terms of skills, competences, resources and collaborative strategies (processes) to combine them.

Building the local resilience inventory is a key aim and outcome of TORC, enabling not only after-action reviews there and then, but also creating the means for interchange and discussion of experience, and projection of situated practices towards other operational contexts in the same organization. By means of this, different parts of the organization can improve their mutual understanding of practices as well as rationales for action, enabling more sophisticated, polycentric training scenarios in which different professions and roles can coordinate in a diverse but altogether resilient manner.



Another key aim of TORC is to distinguish between as well as reconcile operational vs managerial training. That is, understanding the relation between the needed margin for successful operation, and the managerial mandate that sets the limits for the explorative nature of resilience as well as the corresponding accountabilities. This is especially relevant when something goes wrong, despite an attempt of acting resiliently. Also it gives the opportunity to build a suitable training for different segments in the water companies, according to the profession and responsibilities of the trainees.

To this end, TORC is adopted in STOP-IT as a gaming approach to stress test the organizational resilience of a water utility in case of cyber and/or physical attacks. The scope of the game is about being trained at avoiding or preparing for mistakes that it is possible to be anticipated and prepare for, while also being able to handle unexpected situations, disturbances and disruptions that will inevitably arise. Dealing with the expected and the unexpected, however, requires relatively different organizational abilities. The focus of TORC is how these two abilities can be merged. Therefore, Chapter 3 of this report provides extensive details on the way that the game is designed, how a gaming session should be conducted and provides detailed information on the requirements for setting up the inventory for the game. We foresee that the FR and FL will be able to implement this game in their routine training programs as a result of STOP-IT and develop resilience skills of a significant quantity of employees, and therefore, creating a positive change in their resilience.

The STOP-IT project aims at making the water systems secure and resilient by improving preparedness, awareness and response level to physical, cyber threats and their combination. To this purpose, STOP-IT provides modular solutions in WP4, 5 and 6 (technologies, tools and guidelines) embedded into the STOP-IT platform. One of these tools on the strategic and tactical levels is the stress-testing platform by modelling. However, making solutions available is not enough: creating awareness about the benefit of implementing them, assessing the preparedness of an organization in adopting them, defining the way their use is mandated and subjected to governance in the organization, identifying the operational constraints and principles regarding their deployment and uses are equally relevant factors to be covered to improve the resilience of the water sector. The water sector must maintain a resilient operating environment in the face of ever-changing cyber threats while also supporting digital innovations.



## 2 Cyber-physical threats stress-testing platform

### 2.1 Stress-testing

#### 2.1.1 System-wide stress testing

##### 2.1.1.1 Concept & goals of stress-testing

Stress testing can be defined as a systematic procedure formed of deliberate intense testing of a system (Agudelo-Vera et al. 2016), either physically (in small scale) or typically through a simulation model. Intense testing involves pushing the system beyond normal operational conditions, in order to observe the resulting behavior and determine through formal analysis the stability or robustness of a given system against pressures. These are properties sought after by most decision makers (Herman et al. 2015), even at the expense of performance in a system, as safety against failures. As such, stress-testing is pertinent to systems that exhibit inherent uncertainty in their operation, their future state and/or the external pressures that act upon them.

In the context of water distribution systems (WDN) and urban water systems (UWS) in general, stress testing (or similar techniques) is broadly employed for various types of studies with modelling and simulation, for example:

- to explore the ability of a water distribution system to supply water under extreme circumstances (Agudelo-Vera et al. 2016);
- to quantify uncertainty in water delivery due to changing demand patterns and other future pressures (Kang and Lansey 2013);
- to explore the plausibility of the continuity of water supply under failures (e.g. pipe bursts, firefighting) (Vreeburg et al. 2009) and measure resilience metrics (Diao et al. 2016);
- to operationalize resilience in UWSs (Makropoulos et al. 2018) and compare different system designs in the strategic planning phase (Nikolopoulos et al. 2019a).

A stress testing approach can use traditional stochastic techniques giving a probabilistic description of the unknown parameters on the basis of historical data, as is the case with some of the aforementioned examples. Given the probabilistic nature of the stochastic process, the generated input data and parameters can lead to encountering conditions and parameter values outside of the normal range of the system. When a substantial statistical base is available, and reliable probabilistic laws can adequately describe parameters' uncertainty and their possible outcomes (Ruszczyński 1997), this can be a very efficient approach (Pallottino et al. 2005). However, it is well-known that stochastic approaches cannot be used when there is insufficient historical data and statistical information, when probabilistic rules cannot be derived for particular components of the system, or in the case of information not present in the dataset. Predominantly, in low probability (even considered improbable) but high consequence events e.g. "black swan events" (Taleb 2007) and "unknown unknowns" (Pawson et al. 2011), there is no straightforward mathematical way to generate



such data for simulation from what is already known. A common practice is to use a scenario analysis technique as an alternative approach (Dembo 1991; Rockafellar and Wets 1991). Scenario analysis can model real problems, where decisions are based on an uncertain (even unanticipated) future, whose uncertainty is described by means of a set of possible future outcomes, called “scenarios”.

A framework of morphogenesis and creation of such scenarios is presented in Makropoulos et al. (2018) resilience assessment method, where urban water systems were stress-tested under long term uncertainty for scenarios accounting for changing condition throughout the whole design lifespan. The scenarios’ types incorporated different magnitude and rate of change for selected parameters, ranging from mild to extreme future conditions, as can be seen in Figure 1. The results from the stress-testing are used in an operationalized definition of UWS resilience, defined as “the degree to which an urban water system continues to perform under progressively increasing disturbance” and robustness, defined as “as the extent to which a system can keep performing within design specifications under increasing stress”. Therefore, in stress-testing scenarios, robustness is a desired trait of components in a system, that enables a system to withstand pressures without failing in stress-testing. On the other hand, resilience is a system wide property that makes a system “safe to fail” when facing severe uncertainty in a changing environment. For this reason, resilience is currently emerging in the policy discourse on ‘future-proofing’ systems (Rockstrom et al. 2014). A graphical representation of resilience and robustness properties is shown in Figure 2.

An expansion to the resilience assessment method in Nikolopoulos et al. (2019) incorporated “wildcard” modelling into scenarios by introducing explicit low probability but stressful events. These events (“wildcards”) do not represent a continued change of a parameter in the scenario (e.g. population growth with water demand that overburdens the systems limits), but rather a single (no matter its duration) unpredictable, non-repeatable stressful incident, e.g. hacking of critical infrastructure. As shown in Nikolopoulos et al. (2019) attacks on the cyber-physical infrastructure of a UWS or WDN can have serious implications and should be incorporated in stress testing studies.

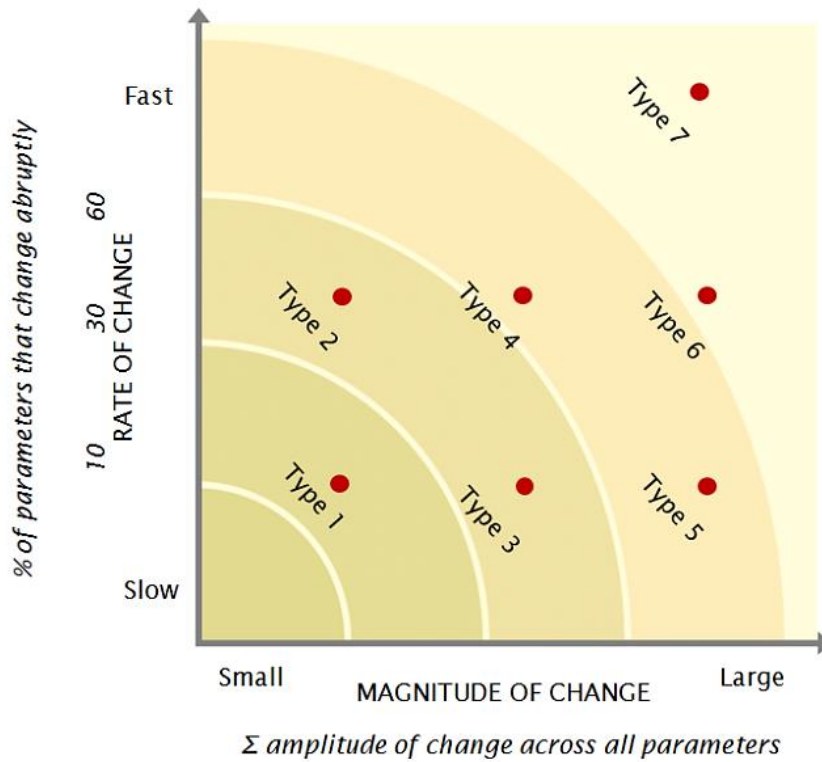


Figure 1: Scenario types for stress-testing UWS grouped by magnitude and rate of change over a design horizon (Makropoulos et al, 2018).

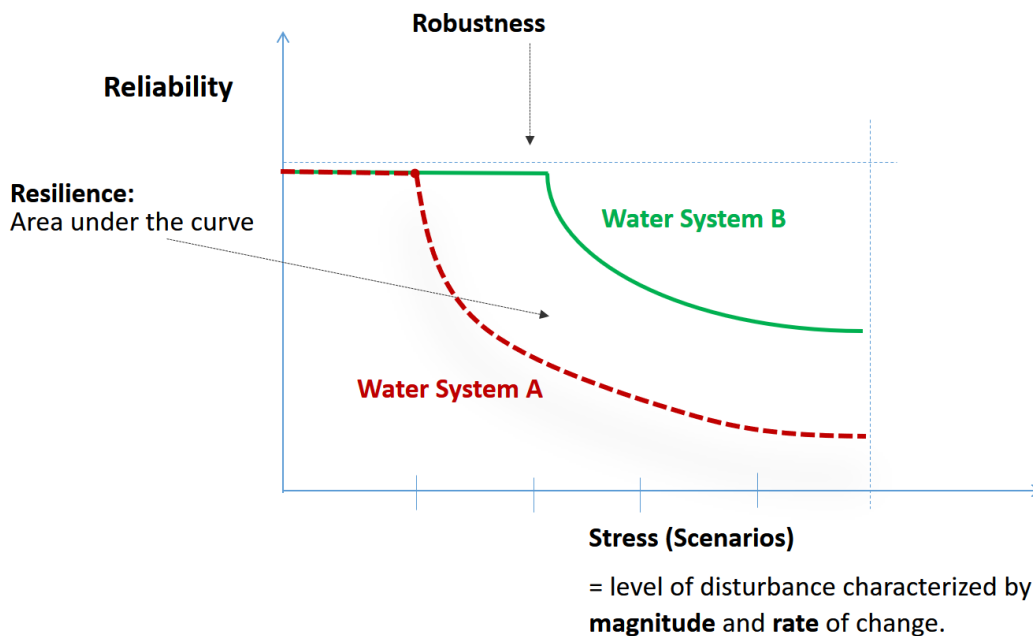


Figure 2: Graphical representations of resilience and robustness as results from stress-testing scenarios (adapted from Makropoulos et al, 2018).



## 2.1.1.2 Stress-testing cyber-physical water systems

A major disadvantage of the networking, communication and remote control schemes within cyber-physical systems (CPS) is the exposure to a much expanded attack surface (Rasekh et al. 2016) compared to non-cyber systems. Cyber-physical systems aside from typical physical attacks (e.g. component destruction, sabotage, etc.) includes cyber-attacks (e.g. Denial of Service (DoS) attacks to disrupt communication between components, Structured Query Language (SQL) injection to destroy databases) or combinations (e.g. in the case of water CPS, manipulation of quality sensor readings and deliberate contamination of water sources) in the form of Cyber-Physical Attacks (CPA) (Taormina et al. 2017). A wide range of adversaries, ranging from hacktivists to terrorists (Nicholson et al. 2012), can exploit this attack surface for various reasons.

The main target of attacks usually is the Supervisory Control And Data Acquisition system (SCADA), which forms the main part of the cyber infrastructure of the CPS. Some older SCADA systems were connected to local intranets isolated from public networks (Fovino et al. 2010) and this led the industry to adopt a sense of false sandbox-security. Most of them still rely on common, but now obsolete, communication protocols like Modbus and DNP3, which were not designed with cyber-security in mind. In contrast, modern SCADA and upgrades of older systems are connected to the main corporate/business network for the infrastructure operator to take advantage of ICT technologies and increased connectivity. Nevertheless, later operational encasement increases vulnerability, now more than in the past, taking into account the difficulties of securing hard real-time systems with many remote field devices with low capability hardware.

The very nature of cyber-physical threats (i.e. uncertainty, non-repeatability, unknown adversaries, high impact etc.) makes the stress-testing methodology essential in understanding CPS behavior under attack and the resulting consequences. To do so, a complete cyber-physical modelling platform should be constructed.

In order to achieve this particular aim, real SCADA testbeds have been used in the past for stress-testing research (Oman and Phillips 2007). A drawback is that these solutions are typically cost prohibitive for actual operational deployment and most importantly proprietary to a single existing system. Therefore it is non-scalable to other utilities (Nikolopoulos et al. 2018). In lieu of this, other CPS modelling tools have emerged in practice and in literature including emulators, virtual machines, software-defined networks (SDNs) and network function virtualization (NFV) (Piedrahita et al. 2017).

MiniCPS (Antonioli and Tippenhauer 2015) is an extension of Mininet (Lantz et al. 2010), a light network virtualization tool, allowing the communication between emulated programmable logic controllers (PLCs). An extension of MiniCPS is shown to implement the field network (connections between PLCs, sensors and actuators) and interact with physical processes in a water treatment process (Piedrahita et al. 2017). Other models employ the CORE emulator (Ahrenholz et al. 2008), like SCADAvt (Almalawi et al. 2013). It expands the emulator through plugin systems that emulate the Modbus/TCP slave master protocols and simulators of field devices. SCADAvt is coupled through server simulation with the well-





known pressurized pipe network EPANET modelling tool and manipulated with a Transmission Control Protocol (TCP)-based protocol to open or close pumps in the system. Other similar tools used for security research of CPS are EPIC (Siaterlis et al. 2013) which is based on Emulab (White et al. 2004) and can be coupled with physical process simulation tools. There also exist discrete event simulators like OMNET++ (Varga and Hornig 2008) and NS-3 (NS-3 Consortium 2019), which can also be used for the same purpose after customization. Such tools provide high fidelity in the actual modelling of the cyber-element of any CPS (especially when using emulators), as it is explicitly emulated through the emulation or simulation of real virtual components, networks, software and protocols (Siaterlis et al. 2013). However, the emulation/virtualization or simulation type of approaches to water cyber-physical modelling and stress-testing have some trade-offs:

- It is essential to utilize an Information Technology (IT)/Information Communication technology (ICT) expert in order to model a virtualization of the cyber layer of respective water CPS, as is a very demanding and specialized task.
- Performing a multitude of cyber-physical attacks for stress-testing is not intuitive as doing so results essentially in a form of penetration-testing to uncover unpatched processes, security issues, backdoors, bugs, glitches etc.
- These solutions tend to be proprietary and tailored made for a specific CPS. Also, in large scale systems, as is the case of most real water CPS, they tend to be cost intensive, at least in terms of development time.
- It is argued that while emulators and virtualization techniques are precise, experiment and measurements repeatability is not ensured (Fovino et al. 2010), in contrast to cyber layer simulation approaches (Queiroz et al. 2009), which usually trade-off fidelity with strong repeatability for security experiments (Siaterlis et al. 2013). Thus, the choice of tool type may affect stress-testing results reproducibility.
- Extensive work may be needed to couple these tools with a physical process simulator and as many of these tools employ real-time emulation or discrete event simulation, the physical process simulator should be compatible.

Another emergent approach to CPS modelling is purely simulation-based for both the cyber infrastructure and physical processes. A drawback is that information flow in the cyber layer is represented with lower fidelity, because the method does not try to represent the actual real bit-wise interaction of components, but rather focuses on the simulated outcome of a cyber-operation or the state of a cyber-component. This simulation approach despite the lower fidelity in the cyber-layer has the following two substantial advantages:

- Straight-forward modeling of various types of cyber-physical attacks, as the attack is modelled as a definitive stress-testing scenario event, not a series of very detailed steps involving discovering possibly unknown vulnerabilities in a CPS with specific components.
- Easier coupling to models of the physical processes, as the cyber layer model could issue control statements and receive feedback from operation without the use of complex “middleware” (software to interconnect the discrete event



emulation/virtualization processes with translated inputs/outputs of the physical model). The coupling can be implemented with direct use of software wrappers for the physical model, or through calling dynamic link libraries.

Influential work in this field is introduced by Taormina et al. (2017), with the conceptualization of models for cyber-physical attacks in water distribution systems, methodologies based on deep-learning for detection of such attacks (Taormina and Galelli 2018) and the release of epanetCPA, an EPANET-based MATLAB modelling toolbox (Taormina et al. 2019). A simulation-based stress-testing platform for cyber-physical water distribution networks can be found on Nikolopoulos et al (2019).



## 2.2 STOP-IT stress-testing platform models and approach

### 2.2.1 STOP-IT stress-testing platform within an integrated framework

The STOP-IT project works towards the development, demonstration, evaluation and preparation of scalable, adaptable and flexible solutions to support strategic/tactical planning, real-time/operational decision making and post-action assessment for the key parts of the water infrastructure. WP4 specifically, has developed a strategic and tactical risk assessment framework and the associated toolkit able to analyse and evaluate physical and cyber risks on water Critical Infrastructures (CIs) and their combination, as well as to support the choice of appropriate risk treatment options and evaluate their effectiveness.

Under Task 4.2, as reported in D4.2 (Makropoulos et al. 2019), an ISO compatible framework has been developed which orchestrates WP4 outcomes in order to support users in the processes of risk identification, analysis, evaluation and treatment (Figure 3). The framework is designed to serve multiple levels of analysis. Those are:

- the generic assessment (1<sup>st</sup> level of analysis) which requires very little specific data and it is based on the experts' judgment and knowledge of infrastructure,
- the single scenario assessment (2<sup>nd</sup> level of analysis) which involves detailed risk analysis, assessment and treatment options through simulations of single scenarios (cyber, physical or combined) and requires specific utility's network information
- the multiple scenario assessment (3<sup>rd</sup> level of analysis) which assists in a more holistic view by moving from a single threat to a set of events/threats for a specific network

End users can implement all three levels sequentially but can also omit or combine processes according to their needs and data availability. Further, the STOP-IT methodology is not limited to utilities which are aligned to the aforementioned ISO framework. On the contrary, it is adoptable to any utilities' needs and processes.



Figure 3: STOP-IT Risk Assessment and Treatment process (figure reproduced from D4.2)

The STOP-IT methodological approach, which supports strategic/tactical planning and post action assessment, is deployed through several tools. Those tools form the Module I of STOP-IT and can be accessed through the Risk Analysis and Evaluation Toolkit (RAET) interface presented in Figure 4. RAET has been developed under T4.2 and documented in D4.2 (Makropoulos et al. 2019). It consists of or is connected with the following components:

- the **Risk Identification DataBase (RIDB)** of risk events which may lead to water quality or quantity issues (developed under Task 3.2 and documented in D3.2, enhanced and transformed into FTs structure in T4.2 and described in D4.2)
- the **Asset Vulnerability Assessment Tool (AVAT)** (developed under Task 4.1 and documented in the EU restricted D4.1) for the identification of the most vulnerable components of an infrastructure
- the **InfraRisk-CP** (developed under T4.2 and documented in D4.2) to support mostly the generic risk assessment
- the **Fault Tree Editor (FT Editor)** for creating, editing and modifying fault trees (developed under D6.3, utilized under T4.2 and described in D4.2)
- the **Scenario Planner (SP)** (developed under T4.2 and documented in D4.2) which a) supports through a wizard the creation of scenarios, b) is responsible for the scenario management c) prepares input data for simulation with selected mathematical models according to the scenario and d) shows simulation results. The SP also includes the **FT Viewer** which enables FT analysis and supports the



identification and selection of risks for further use in the Scenario Planner, the **Toolkit Library (TL)** providing access to information about tools, mathematical models and methodologies related CP risk analysis and evaluation in the water infrastructure and the **Advanced Search (AS)** functionality, for querying within the RRMD, the RIDB and the related data, based on user defined criteria

- the **Stress-Testing Platform (STP)** that can simulate both physical and cyber scenarios for stress-testing and benchmarking purposes (developed under T4.4 and described in the current document)
- the **Key Performance Indicators tool (KPIs tool)** (developed under T4.2 and documented in D4.2) for detailed assessment of results and the impact of cyber-physical events to the water network
- the **Risk Reduction Measure Database (RRMD)** supporting the identification of suitable actions to avoid or mitigate the occurrence of risk events to water CIs (developed under T4.3 and documented in D4.3 (Mälzer et al. 2019))

There are different levels of integration of the aforementioned components. Some of them are essential, core parts of RAET, developed in a single web application (FT Viewer, SP, TL, AS, STP). Others are autonomous Windows applications which are loosely coupled with RAET (FT Editor, AVAT, KPI Tool) or are 3rd party software which have been adjusted to the needs of this project and are invoked by RAET (epanetCPA, EPANET-MSX). Both databases, RIDB and RRMD have been integrated in the RAET database.

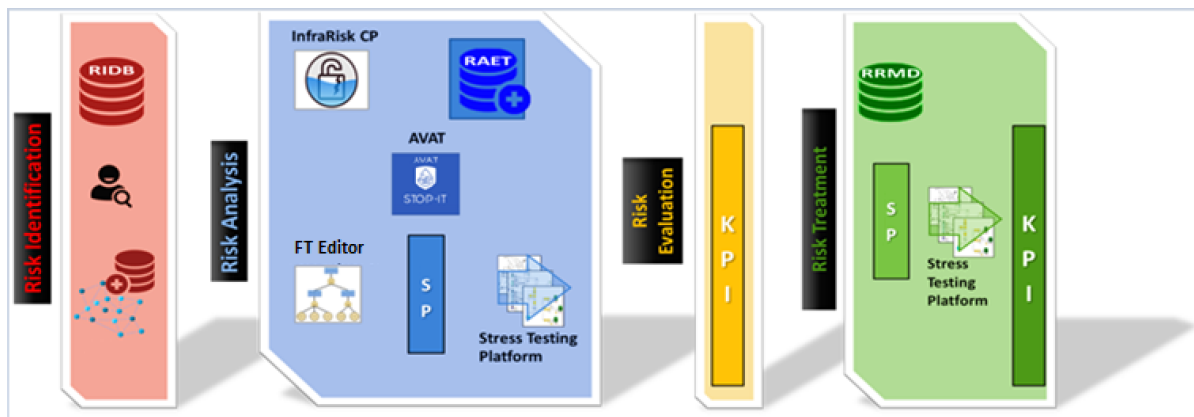


Figure 4: STOP-IT Risk Assessment and Treatment Framework & its components (figure reproduces from D4.2)

In the current deliverable, the Stress-Testing Platform component (STP) of RAET is documented, as developed under T4.4. From the STP, the user has access to a number of available modelling tools that can be used to simulate system's behaviour under various threat scenarios, integrated with other STOP-IT components (e.g. the Scenario Planner). The STP models (e.g. the epanetCPA, the EPANET – MSX, the RISKNOUGHT described in the following sections) are able to simulate the cyber layer information flow and control logic, as well as the physical layer's processes. It is noted that, unless otherwise stated, in this



document epanetCPA refers to the STOP-IT enhanced standalone tool, originating from the free licensed toolbox developed by Taormina et al. (2018).

## 2.2.2 epanet-CPA

### 2.2.2.1 Overview, cyber-physical coupling

In recent years the EPANET model (Rossman 2000), designed and distributed from the Environmental Protection Agency (EPA), has started transforming towards more integrated cyber-physical simulations. Recently, Eliades et al. (2016) released a MATLAB® programming interface for the original EPANET solver, utilized by Taormina et al. (Taormina et al. 2018) to deploy epanetCPA toolbox and link monitoring and control devices interactions to the hydraulic network. In an additional input file, the user defines, in a predefined structure, the cyber network of the system and attacks to be simulated. As epanetCPA does not provide any Graphical User Interface (GUI), such files have to be manually produced and passed to the model through the MATLAB® coding environment. The epanetCPA can simulate:

- deception attacks (manipulation of measurements and control signals)
- denial-of-service (DoS) of communication channels
- eavesdropping and replay attacks
- alteration of control statements
- physical attacks to sensors
- physical attacks to actuators

Those are achieved through 4 attack classes:

- Attack on Sensor
- Attack on Actuator
- Attack on Control

In stress testing conditions, the system operates outside the optimal pressure range. During events like a power outage or a control manipulation of a pumping station, pressure deficiency conditions occur in the system, for which Demand Driven Analysis (like the original EPANET solver approach) poses known limitations (Chmielewski et al. 2016). Unrealistic demand satisfaction and hydraulic performance of the system, in such cases, is the result of the false assumption that supply is unaffected by the pressure deficiency condition. In order to simulate pressure deficiency more realistically, the Pressure Driven Demand approach is proposed (Todini 2003). This approach links nodal outflow to pressure through Nodal Head-Flow Relationship (NHFR) formulas (e.g. Fujiwara and Li 1998; Germanopoulos 1985; Wagner et al. 1988) to fully meet demand at optimal pressure conditions and gradually reduce demand satisfaction as pressure drops.



Over a decade of the last release from EPA, an open-source community (Open Water Analytics - OWA) has been formed (Salomons et al. 2018) with the aim of advancing core EPANET functionalities further and has succeeded in producing two new EPANET versions (2.1. and 2.2) that solve a number of modelling inconsistencies and add pressure-driven demand (PDD) capabilities as part of the core functionality (Davis and Janke 2018). PDD functionality has been also addressed with the development of custom extension solvers, such as EPANETpdd (Morley and Tricarico 2008). The STOP-IT Stress-Testing-Platform in turn, utilized the available functionalities and solved simulation inconsistencies by integrating a new .dll (dynamic-link library). Run with the newest EPANET 2.2+ solver expansion, offers a dynamic engine to explore CP attacks that lead to pressure deficiency and low flow cases. The STOP-IT STP is designed to deal with real water system conditions, where multiple supply zones with different operational pressure ranges exist within the distribution network. Having the advantage of testing the new developments on real networks, in collaboration with the FRs, additional capabilities were added to resolve this issue. This new version, combines the features of EPANET 2.2 (the newest engine version available in [OWA](#)) with features of the EPANETpdd engine, thus allowing for an assignment of PDD variables per node, which makes it a more adjustable and realistic approach.

Real water network topologies contain thousands of nodes and assets. Even skeletonized network models, with known limitations and shortcomings (Davis and Janke 2018), are computationally expensive, while fine time resolution adds more load to the simulation. In order to produce a tool applicable to the demanding operational environment of water companies, the STOP-IT STP version of the tool was further improved by optimizing part of the existing code in terms of computational time. Thus, making the STOP-IT version more realistic (PDD capabilities), more detailed (variables defined at node level) and faster (optimized functions).

Parallel to the STOP-IT enhancements, a PDD version of epanetCPA was also developed by Taormina et al. (2019). This new PDD version of the tool was also adjusted to the STOP-IT needs and is part of the STP, providing additional solver choices. The workflow for the use of any of the engines can be seen below Figure 5.

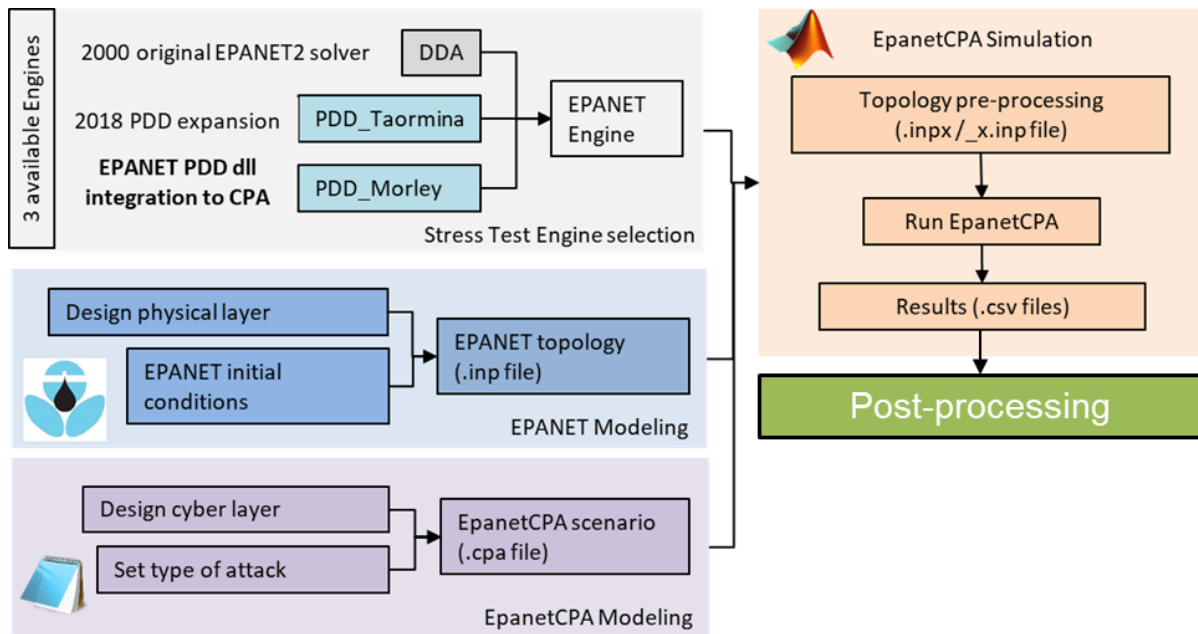


Figure 5: Process workflow for stress-testing using epanetCPA

In order to model cyber-attacks with a physical expansion, an additional input file is required (.cpa expansion as introduced by Taormina et al. (2018)) that contains cyber network connectivity information. This information is found in the first section of the file, linking between “cybernodes” of the network, i.e. between PLCs, sensors and actuators. To indicate sensors and actuators that are located on the physical network, within the cpa file, those cybernodes are identified using the same asset IDs as the one found in the physical network topology file (.inp). The .cpa file also contains “attack” information and control changes to be implemented in the system. Such information is found in the second section of the file, under the title [CYBERATTACKS]. Within this section, and for each event separately the type of attack, the target and attack arguments such as starting or end time are declared. Under the [CYBEROPTIONS] section, the user can define the PDD approach and variables that best fits the simulated network.

An example of a .cpa file created for the C-Town network can be seen next.

```

[CYBERNODES]
; Name Sensors Actuators
PLC1      PU1, PU2, PU3
PLC2 T1
PLC3 T2   PU4, PU5, PU6, PU7, V2
PLC4 T3
PLC5      PU8, PU9, PU10, PU11
PLC6 T4
PLC7 T5
PLC8 T6
  
```





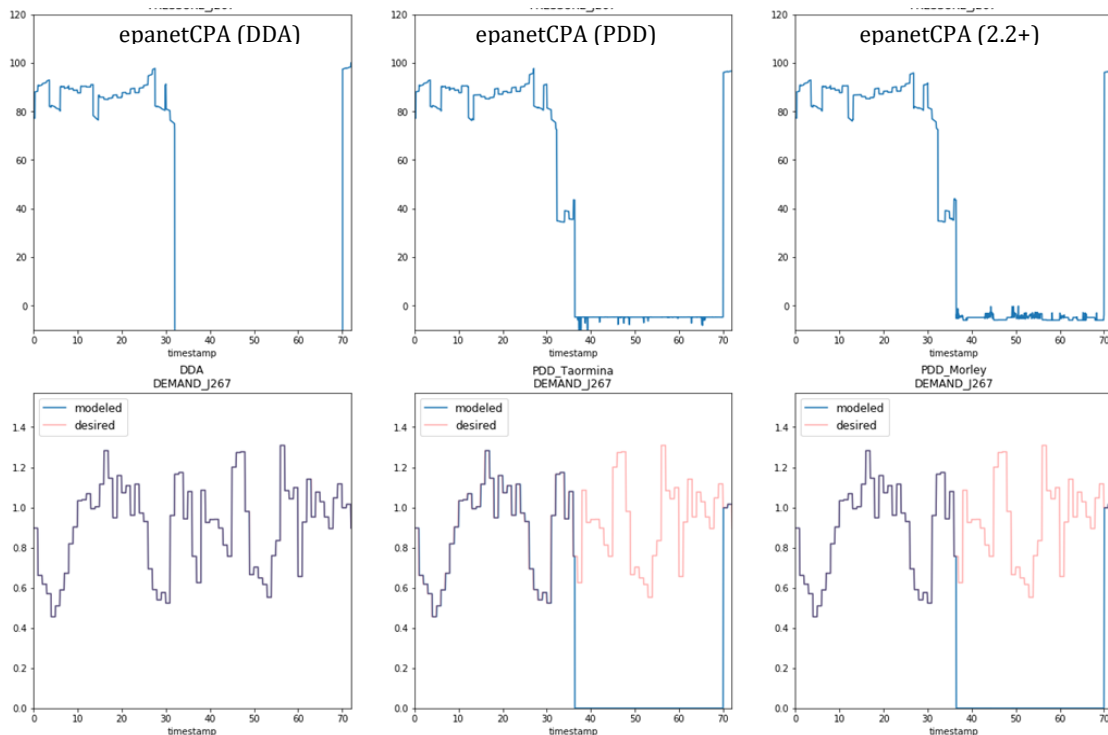
```
PLC9 T7
; SCADA

[CYBERATTACKS]
; Type Target Init_cond      End_cond      Arguments
; Attack on communication link between T2 water level sensor and PLC3. A constant
;(HIGH) value of 5.6 meters ; is injected, leading PLC3 to close valve V2. Tank T2
empties ;and network is disconnected.
Communication      PHY-T2-PLC3TIME==10    TIME==20    constant, 5.6

[CYBEROPTIONS]
verbosity          1
what_to_store      everything
pda_options        0.5    3    50    Wagner
```

### 2.2.2.2 PDA vs DDA engines

As mentioned in the previous paragraph, analysis performed with demand driven equations have some limitations. To provide a comparison of the available engines in the STP, a cyber-attack scenario was examined in the demo network of CTown (Ostfeld et al. 2012), deploying all 3 available engines (Figure 6). The attack chosen was a tank sensor signal manipulation, leading PLC and the operators to believe that a tank was full while in reality was emptied, creating pressure deficiency in the system. Seen in the figures below, the DDA approach of fully meeting the demand at 0-pressure conditions is unrealistic, proving the necessity of PDD in cyber-physical attacks stress testing.



**Figure 6: The impact of a cyber-physical attack to nodal pressure and demand in a C-Town node, provided by three of the provided engine options.**

Comparing the available PDD engines, both agree on the timeframes of pressure deficiency and inability to cover demand and thus model the impacts of the attack to the WDN. The PDD found in Taormina et al. (2019), can be considered a safe estimator that finds the timeframe of the impact to the attack and model the impact to the system on the safe side, but may hide partially met demand. On the other hand, the STP development, that deploys the new PDD capabilities, is able to simulate pressure instabilities  $\Delta p$  during the attack and can be thus used for finer studies (e.g. partially met demand, water hammer estimation).

### 2.2.2.3 Compilation

Original epanetCPA is neither a standalone executable, nor does it provide a GUI for users to select and set parameters. The .cpa files that contain the cyber network connectivity and the attack parameters files have to be manually produced and passed to the model through the MATLAB® coding environment. In order for the STOP-IT version to be seamlessly connected with the RAET workflow (described in section 2.3), additional effort was taken to properly adjust the code. The RAET integration was achieved in three steps. The first step was the development of a unique wizard to translate scenario data and parameters selected through the Scenario Planner to the appropriate file format (.inp and .cpa). This allows the data flow from the RAET Fault Trees to the hydraulic solver, through the SP GUI while at the same time leverage the adjustable framework of RAET. This process is designed so that users can define the desired scenario parameters without having to manually create the file or get familiar with the predefined .cpa file structure and requirements.



The second step towards the seamless integration was to create a unique communication path between models and the back-end database, based on RAET's API. This step disengages the user from the need to "import" and "run" the files previously created for the scenario, allowing for the deployment of the engines without the need to interact or even be familiar with the MATLAB® coding environment. Additionally, the uniquely defined two-way API communication allows the direct update of the RAET DB with the scenario simulation results and a set of selected KPIs, produced by the STP. Additional metadata and simulation information are also reported and registered to ensure the integrity of the DB. More details on the API data flow can be found in Section 2.3.

The third and last step was the compilation of the STOP-IT version of epanetCPA. The compiled standalone STOP-IT version available, requires less computational time, while, unlike the original epanetCPA, it doesn't require MATLAB® license to run. The compiled version of the simulation engine also ensures that no changes and code alterations are applied, adding to the assurance of simulations' integrity.

### 2.2.3 EPANET-MSX

#### 2.2.3.1 Overview, coupling with the stress-testing platform

EPANET-MSX (Multi Species Extension) (Shang et al. 2008) is an extension to EPANET, aimed at better fidelity in the water quality simulation. EPANET-MSX allows users to analyze multiple interacting species seamlessly in a combined water quality and hydraulics simulation. Different sets of reactions, analytical chemistry equations and species kinetics can be defined from the user both for bulk flow in the network and on the pipe walls. This greatly enhances EPANET's capability to track chemicals' fate in the network through diffusion mechanisms and chemical/biological reactions. With EPANET-MSX coupled to the stress-testing platform users are able to model complex physical contamination events as scenarios either deliberate or accidental and of chemical or biological type.

#### 2.2.3.2 Data inputs and parameters

EPANET-MSX accesses the base .inp file describing the hydraulic network topology with the respective simulation parameters. Another file (.msx) must be supplied or defined by the user that states the species as variables and the quality parameters. By using the species as variables, users are able to construct complex analytical chemical equations, by supplying named constants, terms and rates. Among parameters that can be programmed in the .msx are the source(s) of the contamination, the start/end times, patterns, concentrations, initial quality conditions and numerical solvers to be utilized.

#### 2.2.3.3 Usage of the EPANET-MSX .dll in the stress-testing procedure

The stress-testing platform incorporates a software wrapper that utilizes the official dynamic linked library of the EPANET-MSX and exposes all available actions. Through the wrapper, users are able to customize any stress-testing scenario in WDNs by introducing water quality related events, with the functionality to define new .msx files from scratch and binding them to the base .inp file of the network. Also, the STP includes templates of contamination events



that pass predefined arguments of equation, terms, constants, rates and species to EPANET-MSX in order to create an empty scenario, while users specify only concentration values and points of entry to populate the scenario.

## 2.2.4 RISKNOUGHT

### 2.2.4.1 Overview

RISKNOUGHT (Nikolopoulos et al. 2019b) is a recently developed (Nikolopoulos et al, 2019), stand-alone stress-testing and modelling platform for water cyber-physical distribution networks. It is based on a simulation approach, able to represent information flow, control logic and interconnections of the cyber layer with the physical processes in a higher fidelity, realistic and extensible way, aiding in risk management practices. As RISKNOUGHT is Python-based, it employs the Water Network Tool for Resilience (WNTR) Python package (Klise et al. 2017, 2018), which includes both bindings to EPANET routines, as well as a complete port of EPANET routines to Python, called WNTR simulator in order to facilitate pressure-driven demand (PDD) hydraulic equations (Wagner et al. 1988) as opposed to demand-driven (DD) equations that basic EPANET uses. The usage of WNTR within RISKNOUGHT also allows handling of input/output files, enriched interaction with network elements (add/remove/modify properties) and permits simulation of physical damage due to disasters, i.e. pipe leaks, tank leaks etc. RISKNOUGHT further enhances WNTR capabilities with geospatial I/O using geopandas (Jordahl et al. 2019), shapely (Gillies and others 2007) and gdal (GDAL/OGR contributors 2019) packages allowing the import of pressure zones as shapefiles with nominal and minimum pressure levels as attributes for the nodes of the zone for PDD purposes.

### 2.2.4.2 Cyber-physical modelling

The cyber layer of RISKNOUGHT is built based on a network of interconnected cyber components. The whole cyber infrastructure is represented as a directed graph, with nodes acting as the components (sensors, actuators, PLCs etc.) and connections (wireless transmission, fiber, etc.) between components as edges. Components are built as classes that include the following common types of cyber components:

- **Sensor:** acquire data from the physical layer.
- **Actuator:** perform an action on the physical layer.
- **Logic:** virtual components (software bits), that implement control logic via using input data from sensors to decide physical procedures as outputs through actuators. Logic components are assembled into PLC units.
- **PLC:** oversees and interconnects Logic components.
- **Central SCADA:** oversees and interconnects all connected PLCs and also acts as the Human-Machine-Interface (HMI) interface. Gathers all I/O data.



- **Historian:** records all operations and I/O data (essentially the SCADA database).

Cyber and physical layers are coupled through a unified simulation process, with feedback loops between each discrete cyber and physical layers simulation step. In a single timestep, the physical layer feeds input data (e.g. node pressure, tank level, pipe velocities etc.) from the hydraulic simulation to the cyber layer, which ultimately passes decisions to the physical layer, affecting the hydraulic state for the next step of the hydraulic simulation (e.g. valve state, pump state etc.), as shown in Figure 7.

### 2.2.4.3 Cyber-physical attack scenarios for stress-testing

In order to model Cyber-Physical attacks as scenarios, RISKNOUGHT employs a special class, each instance of which holds the information that define a single generic attack event i.e. start time, end time, event type, target, special characteristics of the attack (if any, from a predefined dictionary), special values to be used in the attack generation (if any). More than one instances can be executed in the same cyber-physical simulation, making the cyber-attack scenario as complex as the modeller needs. The events can be overlapping or not, or have the same or different targets without restrictions. In order to execute the cyber-physical simulation under attack, there are class methods that alter the behaviour of the cyber-layer. Without going into coding detail, these include the methods to perform cyber-attacks on Sensors, Actuators, Logic Parts, PLCs, central SCADA and Historian units as can be summarized by target in the following list:

- **Sensor:** DoS on the connection with PLC, data manipulation types: assign specific value or timeseries to output data, don't let the sensor update output data, replace output data values from a sinewave function, add random noise to output data.
- **Actuator:** DoS on the connection with PLC, action manipulation by: do not send ACK and do not perform action, send ACK and perform random action, send ACK and do not perform action, do not send ACK and perform action
- **Logic part:** modify the Logic part by: change threshold, change action output, delete Logic part, suspend Logic part from execution
- **PLC:** DoS on the connection with central SCADA, allow exploitation of Logic parts
- **central SCADA:** DoS on all connections
- **Historian:** delete data, replace data by: specific timeseries, random values

Finally, some physical attacks are reproducible in RISKNOUGHT, such as contamination events (leveraging EPANET's quality solver), pipe bursts, destruction of cyber components etc.

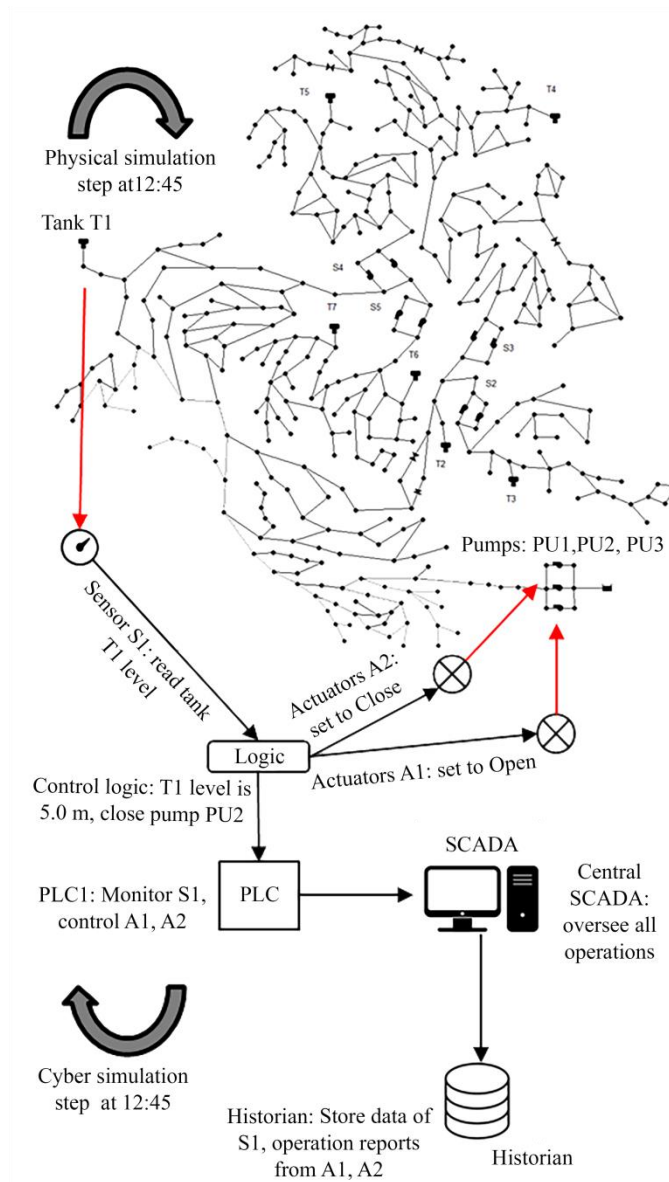


Figure 7: Schematic representation of RISKNOUGHT simulation step (Nikolopoulos et al. n.d.)



## 2.3 Stress-testing methodology for Water Distribution Networks

### 2.3.1 Methodology for stress-testing in the context of STOP-IT

As briefly mentioned in Section 2.1.1 of the current report, the STP is one of the integral parts of the STOP-IT risk assessment and treatment framework and its associated toolkit (i.e. RAET) documented in detail in D4.2. The STP and its models (described in Sections 2.2.2, 2.2.3, and 2.2.4 of this document), provide a test bed for alternative cyber-physical risks and risk treatment options. Even though the STP can be considered as a standalone tool, it has been intergrated with other components of RAET, such as the Scenario Planner (SP) i.e the wizard which assists users in creating and configuring their sceanarios and seamlessly import them to the STP for simumlation, or the KPI tool which enables users to perform in depth analysis of results of scenarios produced through the STP. In the following paragraphs, the developments of the STP per se are being described and the way the STP “communicates” with the other components of RAET.

#### 2.3.1.1 Architectural design of the Stress Testing Platform

The following Figure 8 shows the main components of the Stress-Testing Platform and the dataflow between them, as well as how the STP is integrated with other omponents of RAET describes in D4.2 and briefly mentioned in Section 2.1.1 of the current report.

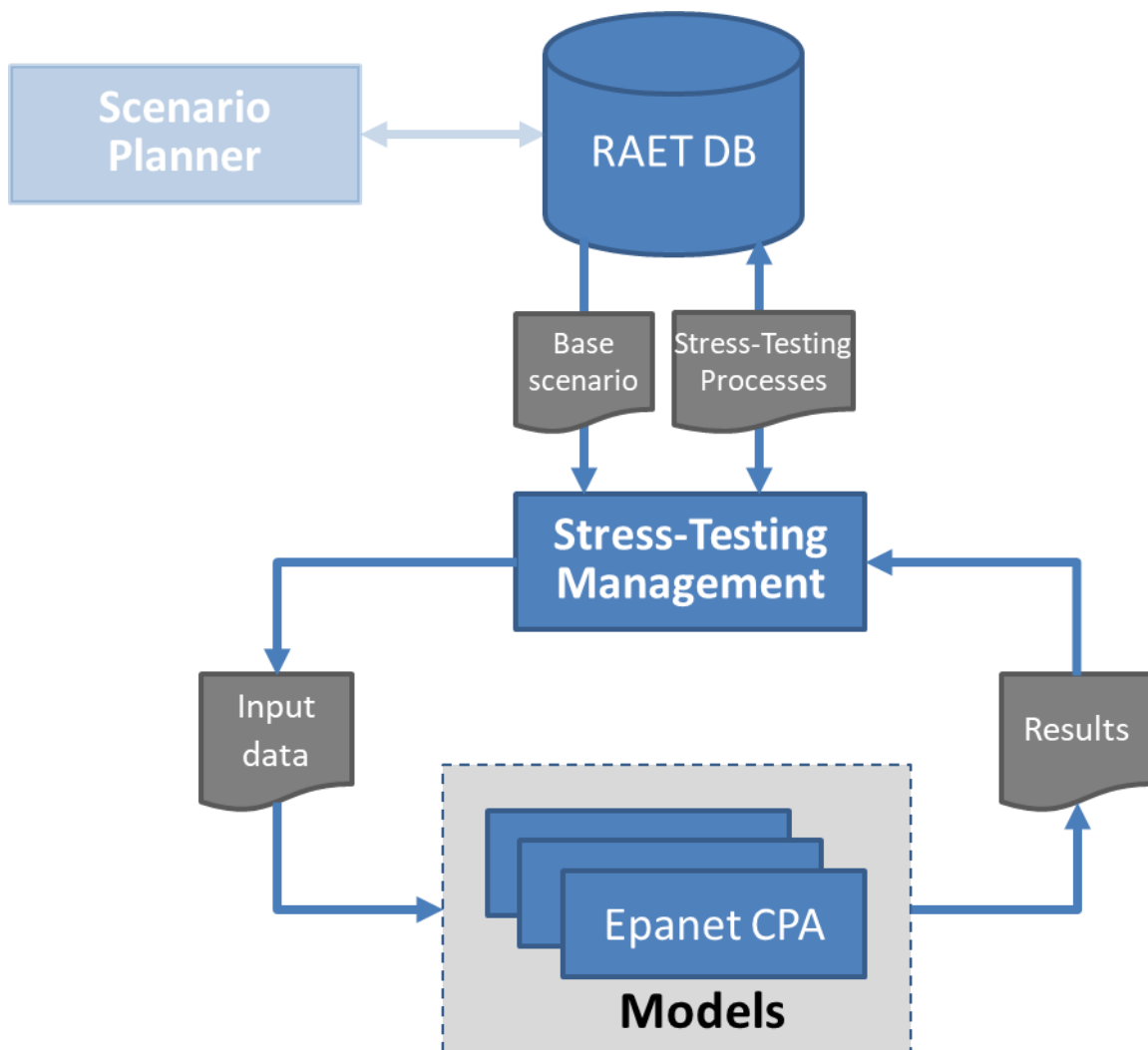


Figure 8: Schematic representation of the Stress Testing Platform and its components

The Stress Testing Platform consists of the following main components:

**Stress-Testing Management (STM).** This component is responsible for the management of the stress testing procedures. It supports the creation of such procedures in the following ways:

- By selecting the **base scenario**. Variations of the base scenario, defined by the control variables, will be executed and evaluated by the stress testing platform. The base scenario must have been developed by the **Scenario Planner** and stored in the RAET database. The Scenario Planner is part of the RAET, developed in Task 4.2 and has been discussed in detail in Deliverable D4.2.
- By defining the value range of the **control variables**, a set of which is used in each simulation run. Each new set with values constitutes a stress-testing scenario.
- By specifying other **procedure parameters**, and most notably the methodology for the selection of the values of the control variables and/or the number of simulations.





The scenario sets derived from the base scenario are differentiated in the control variables with two discrete methods:

- Random selection of procedure parameters: The control variable values are randomly sampled from user defined bounds for each variable.
- Systematic combination of parameters: The control variable values are incrementally sampled from user defined bounds for each variable.

The STM initiates a series of simulation runs by creating the necessary input data files according to the requirements of the selected model. For epanetCPA the interface that has been designed between the STP and the model is documented in Annex A. After the termination of the simulation, the STM component loads and evaluates the simulation results and stores them in the RAET DB for future use. Annex A also documents the developed API for the transfer of the simulation results together with an example.

It is important to note that at this stage of the project, the STM does not select the control variable values for the next run based on past simulation results. It rather executes and evaluates a predefined series of simulations, derived either from random or systematic sample of parameters.

**Models** (i.e. epanetCPA, EPANET-MSX, RISKNOUGHT) can be defined and installed in RAET and used by the Stress-Testing Platform for the simulation of water infrastructures as demonstrated with epanetCPA.

The **RAET DB** is the database used by the Risk Analysis and Evaluation Toolkit (RAET), developed in Task 4.2. The Stress Testing Platform uses RAET DB for the following purposes:

- a) To select the base scenario for the stress testing procedure. The base scenario consists of a CP infrastructure, events that may jeopardize the security of the infrastructure, the affected assets and other simulation parameters depending on the event types.
- b) To select the model for the simulation of the infrastructure. For this purpose relevant models have to be declared in RAET and must be capable to simulate events, as defined in the chosen scenario.
- c) To store the stress testing procedure parameters. These can be retrieved in a later stage in order to perform further tests.
- d) To store simulation results for future analysis

### 2.3.1.2 Scenario Control variables

Typically every aspect of a specific threat scenario built within the SP can be used as a control variable, including:

- Temporal characteristics e.g. the start time of the attack, the end time of the attack etc.



- Specific characteristics of an attack e.g. if bogus data are fed to a controller, specify values, concentration values for chemical contamination events etc.
- Various special conditions, e.g. enable/disable any risk reduction measures, vary the residual chlorine in the WDN, change initial conditions of the hydraulic simulation etc.

### 2.3.1.3 Stress-Test scenario set exploration procedure

The scenario sets derived from the base scenario are differentiated in the control variables with two discrete methods:

- Random selection of procedure parameters: The control variable values are randomly sampled from user defined bounds for each variable.
- Systematic combination of parameters: The control variable values are incrementally sampled from user defined bounds for each variable.

### 2.3.1.4 Performance indicators

Stress-testing models produce simulation results files that contain detailed data on the system behavior. The data are at the finest spatial and temporal scale, as the models register information for every node and link of the system in each timestep. For the stress-testing procedure to be of value, a direct and easy to understand meaning of the simulation results was defined based on the indicators created within the project and presented in D4.2. Seamlessly integrated within the stress-testing simulation procedure, a post-processing algorithm is embedded to the declared models. The algorithm, communicating with RAET's back-end database, accesses and retrieves the required data files to perform a failure analysis. The files requested are those containing the business-as-usual performance data to be used as reference. Detailed explanations on the indicators framework can be found in the relevant deliverable. The selected indicators to be used in the post-processing algorithm are:

1. Unmet Demand
2. Nodes Insufficiently Supplied
3. Customers Affected
4. Customer Minutes Lost
5. Service Hours lost

The above selection can provide a quick answer on how much supply was lost, at what spatial extent, affecting how many people and for how long. The post-processing algorithm produces 3 types of data for each of the above indicators: the *absolute value*, the *percentage* and the *timeseries*. The *absolute value* declares the magnitude of failure as the total performance lost under the stress-test scenario. The *percentage* provides a direct comparison with the optimal performance under no stress. The *timeseries* form reveals how failure propagates in



the system through time. Using those metrics, or combination of them, the users can later rank and prioritize the stress-test scenarios run.

The RAET architecture requests a specific file format to be followed for the data flow between components. For the post-process algorithm of the STP models, it is a file in JSON format. The produced JSON file contains 2 objects, the KPI and the Metadata. In the KPI object, for each metric, the fields "Title", "Overall", "OverallPercent", "Timeseries" and "Units" are contained. Metadata contain information for the stress-test scenario, simulation, parameters and results in addition to secondary integrity check information like timestamps, tools used, user ID and computer name etc. An example of such JSON file can be seen in Annex A.

## 2.3.2 Integration with the RAET

### 2.3.2.1 Interface with the Scenario Planner

The Stress-Testing Platform (STP) fits seamlessly into the concept of the Risk Analysis and Evaluation Toolkit (RAET) and has interfaces with its other components, such as the Scenario Planner (SP) (further information can be found in D4.2). While with the SP privileged users can create, manage and execute simulations of single scenarios, with the STP they can evaluate variations of the initial (base) attack scenario by starting and controlling a series of simulations in one process.

From the user perspective, the entry point for the STP is clicking on the related illustration on the homepage of RAET (see Figure 9: RAET homepage, including the illustration which links to the Stress-Testing Platform (STP)). Another way to navigate to the Stress-Test page is through the main menu by selecting `Lists/ST procedures`.

Ideally, the user has previously identified risks and vulnerabilities of his infrastructure by using e.g. the available FTs or the AVAT tool, has explored possible measures addressing risks with the Risk Exploration Tool (RET, see D4.5 (Cochero et al. 2019)), has selected the appropriate tool for simulation and has created an initial attack scenario that will be used as basis for the stress-testing procedure.

More specifically, in the Scenario Planner (SP) the user specifies scenarios to be simulated with a selected tool (model). The scenario data comprises the following:

- **Tools** capable to simulate CP processes.
- A **utility network**, its characteristics and initial conditions given by the tool specific files.
- A series of **events** that pose the risk according to the scenario. Events are further specified by their parameters and triggered on specific **assets**.
- Possibly risk reduction **measures** which are applied in this scenario in order to assess their performance against the given events/threats. The selected measures are documented in the tool specific files.

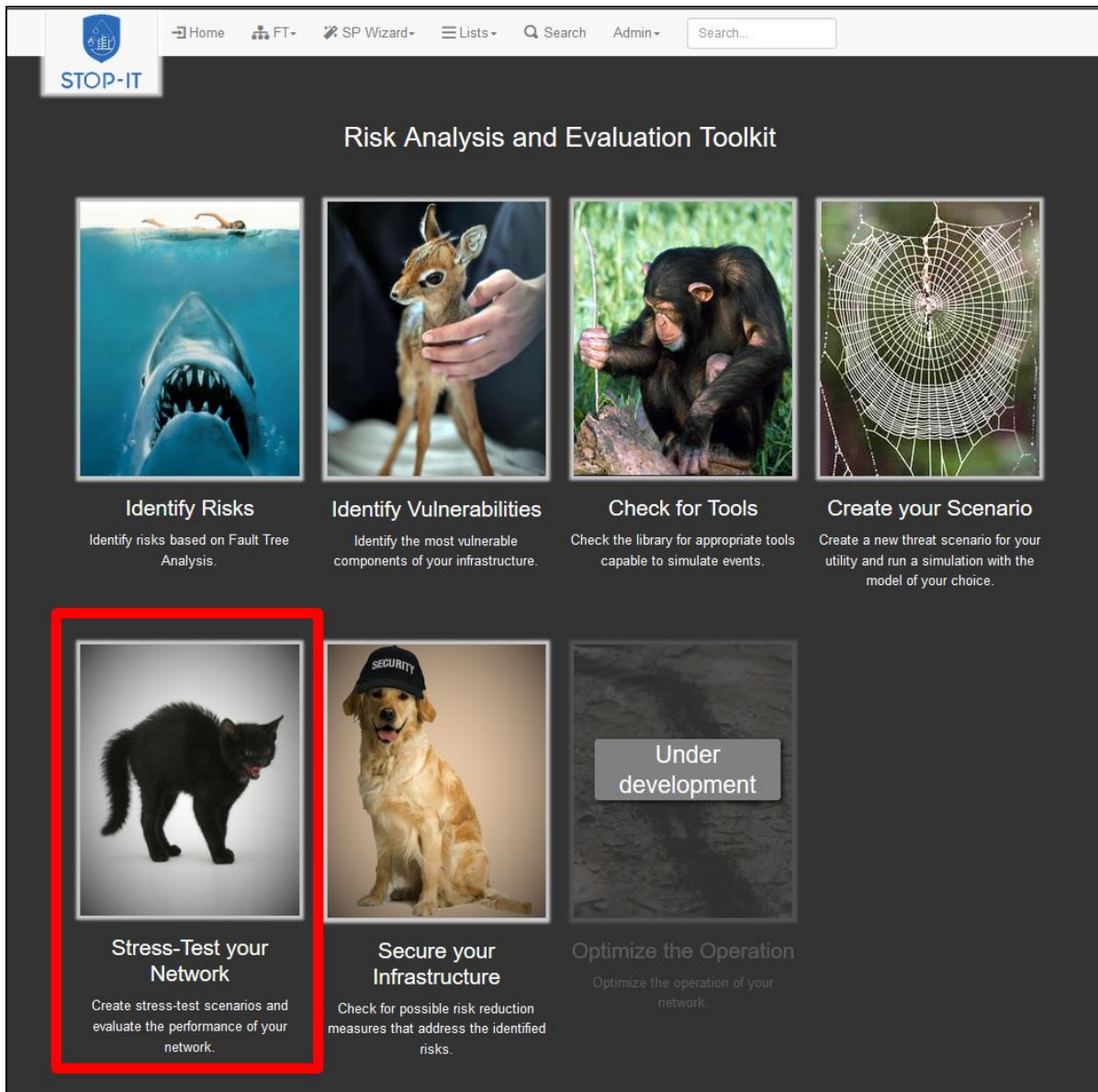


Figure 9: RAET homepage, including the illustration which links to the Stress-Testing Platform (STP)

As described in Section 2.2.1 in the current report, users may access all the tools of Module I of STOP-IT, apart from the Stress-Testing Platform, through the interface of RAET (Figure 9) and implement the single or/and multiple risk assessment briefly described in the following Sections (2.3.2.2 and 2.3.2.3). Specifically,

- the “Identify Risks” icon launches the FT Viewer developed and reported under D4.2 (content of the RIDB, which has been reported in D3.2, has been incorporated to the STOP-IT FTs),
- the “Identify Vulnerabilities” icon launches the AVAT tool developed in T4.1 and reported in D4.1



- the “Check for Tools” icon gives users access to the tool’s library which is an integral part of RAET developed in T4.2
- the “Create your Scenario” icon launches the Scenario Planner described in detail in D4.2.
- the “Stress-Test your network” icon initiates the Stress-Testing Platform developed under T4.4 and reported in the current report
- the “Secure your Infrastructure” icon which enables the users to be navigated through the Risk Reduction Measure Databased of T4.3. An additional possibility for exploring the relations between risks and risk reduction measures is provided through the Risk Exploration Tool based on the elaborated STOP-IT ontology (see D4.5).

The STP, as part of RAET, is available through the RAET demo server by following the link: <http://raet.itia.civil.ntua.gr:8001/>. To access the STP functionality and certain integrated tools of RAET, login to the system is required. Credentials for accessing it can be obtained from Dr. Christos Makropoulos ([Christos.Makropoulos@kwrwater.nl](mailto:Christos.Makropoulos@kwrwater.nl) or [cmakro@chi.civil.ntua.gr](mailto:cmakro@chi.civil.ntua.gr)).

### 2.3.2.2 Single scenario assessment

The single scenario assessment corresponds to the 2<sup>nd</sup> level of analysis as described in Deliverable 4.2 (see Section 2.4.2). This process is invoked from the RAET homepage (Figure 9: RAET homepage, including the illustration which links to the Stress-Testing Platform (STP)) and concludes with the evaluation of a single scenario. Several scenarios can be created by the user and their results can be compared using elements such as table and spider chart.

### 2.3.2.3 Multiple scenario assessment

The multiple scenario assessment implements the 3<sup>rd</sup> level of analysis, as described in deliverable D4.2. Having analysed the overall procedure of exploring, simulating and evaluating a risk in a single scenario step, in the multiple scenario assessment the user is able to create, configure and run through the Stress-Testing Platform (STP) stress-test procedures, each of which consists of a series of simulations.

The main control page of the STP is shown in Figure 10. From this page, the user can review the results of stress-test procedures executed in the past or create new ones by clicking on the *New* button.

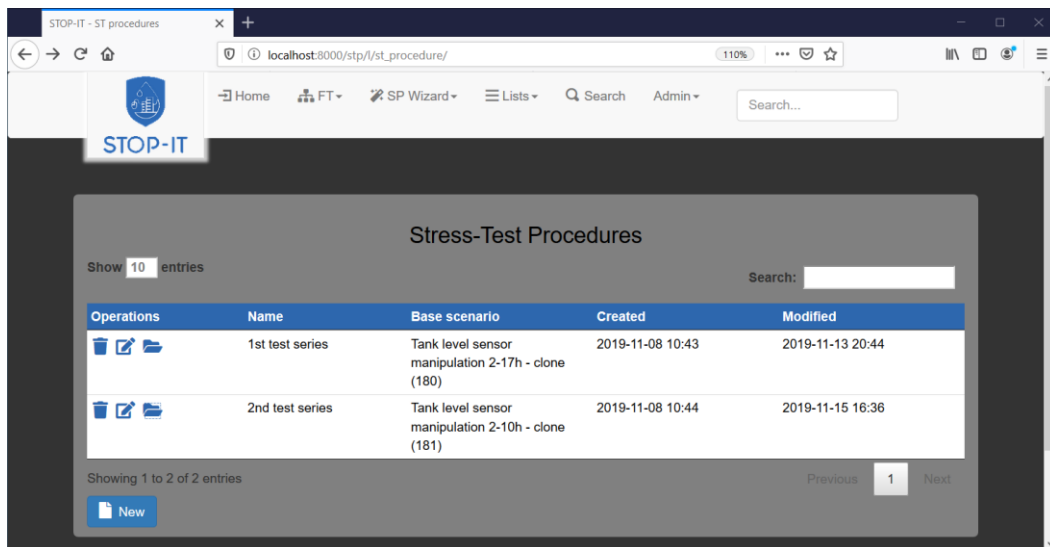


Figure 10: Stress-test procedures list page

The Stress-Testing Platform has full access to the scenarios defined by the SP and stored in the RAET DB. When creating a new procedure, the user can select a scenario to be used as the base scenario in the stress-testing procedure Figure 11

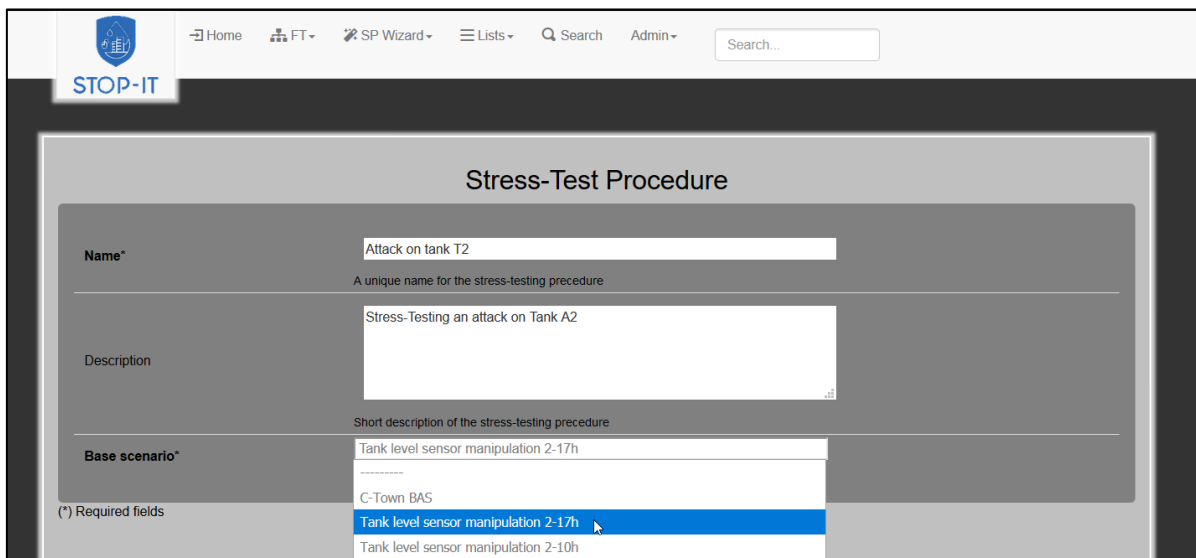


Figure 11: Selection of the base scenario for the stress-testing procedure

Furthermore, the user has to specify ranges of values for the control variables to be used in the simulation series. The number and type of the control variables vary depending on the event specified with the base scenario. All variables take numerical values Figure 12.


The selected method corresponds to the ones defined in the methodology (Section 2.3.1.3). In case of a systematic combination of parameters (*Incremental method*), the user specifies the number of values to be set, equally distant between the minimum and the maximum



value. Another option is to let the system select the value randomly from the given value range.

Name	Minimum	Maximum	Method	Nr. of values	Event
Start time	2	3	Random selection	1	Event: Basic Event 235 Asset: T2 (Sensor)
Duration	8	10	Incremental	3	Event: Basic Event 235 Asset: T2 (Sensor)
Value	5.7	7.7	Random selection	2	Event: Basic Event 235 Asset: T2 (Sensor)
Start time	3	11	Incremental	3	Event: Gate 232 Asset: T3 (Drinking Water Tanks)

Figure 12: Specification of control variables parameters

From the Stress-test procedures list page, by clicking on the folder icon , the user navigates to the page of the selected stress-testing procedure (Figure 13). The user is able to review the characteristics of the procedure and the simulation results executed so far, resulting from variations of the base scenario as specified by the user by the control variable parameters.

The table with the results includes the KPIs defined in D4.2 and produced by a single scenario simulation. Each row includes the control variable values of the respective simulation and the table can be **ordered** (ranked) by any column by clicking on the column title. Clicking on the title a second time, the table will be ordered in the opposite direction.

If the procedure has not been completed yet, it can be restarted by clicking on the runner button. It will continue the process from where it has been stopped. Clicking on the same button a second time, it will stop again after the termination of the current simulation.



**Stress-Test Procedure**

Name: 1st test series  
Description:  
Base scenario: Tank level sensor manipulation 2-17h - clone (180)  
Created: 2019-11-08 10:43  
Modified: 2019-11-13 20:44

Show 10 entries

#	Control variables	KPI 1	KPI 2	KPI 3	KPI 4	KPI 5
1	Event 1: Start time = 2.23, Duration = 8, Value = 5.9 Event 2: Start time = 3	2 041 030	184	51 691	14 666 168	11.0
2	Event 1: Start time = 5.37, Duration = 8, Value = 6.3 Event 2: Start time = 5.66	2 013 493	158	42 912	9 863 278	8.2
3	Event 1: Start time = 4.92, Duration = 8, Value = 7.1 Event 2: Start time = 8.33	1 885 311	132	40 691	8 566 168	7.2.0

Showing 1 to 3 of 3 entries

Previous 1 Next

Cancel Run

Figure 13: Stress Test procedure page.

## 2.4 Stress-testing platform in WP4

As briefly described in Section 2.2.1 of the current report, the STP is an integral part of an ISO compatible framework developed under WP4 which aims at assisting the users in assessing and treating the risk at strategic and tactical level. Under this framework, the different WP4 tools, which form the Module I of STOP-IT, have been orchestrated to support the workflow presented in Figure 14.

Users may start by estimating the assets vulnerability of their network by using the AVAT tool in order to identify potential “weaknesses” that may rise due to cyber-physical threats. At a next step, users could be navigated through the potential risks through the FT Viewer module of the Scenario Planner and then design/configure risk scenarios of interest through the scenario manager module. The SP is interconnected with the content of the RIDB and the RRMD, information which is needed while building a scenario that is of interest. After creating the scenario(s), the users can simulate seamlessly the cyber-physical events that have been defined in their scenario through the use of the STP. When the simulation has been completed, users can visualise and assess system’s response through the KPI tool which





enables them to understand the actual impact of the event/simulated scenario to their system. The above steps can be repeated as many times as the users want. Additionally, the STP functionality can also support the simulation of a set of scenarios, as described in earlier paragraphs of the current report. Apart from examining multiple scenarios, users may alter the network's topology in order to include risk reduction measures before creating and running additional simulations in order to assess the results after a new measure has been incorporated to their network.

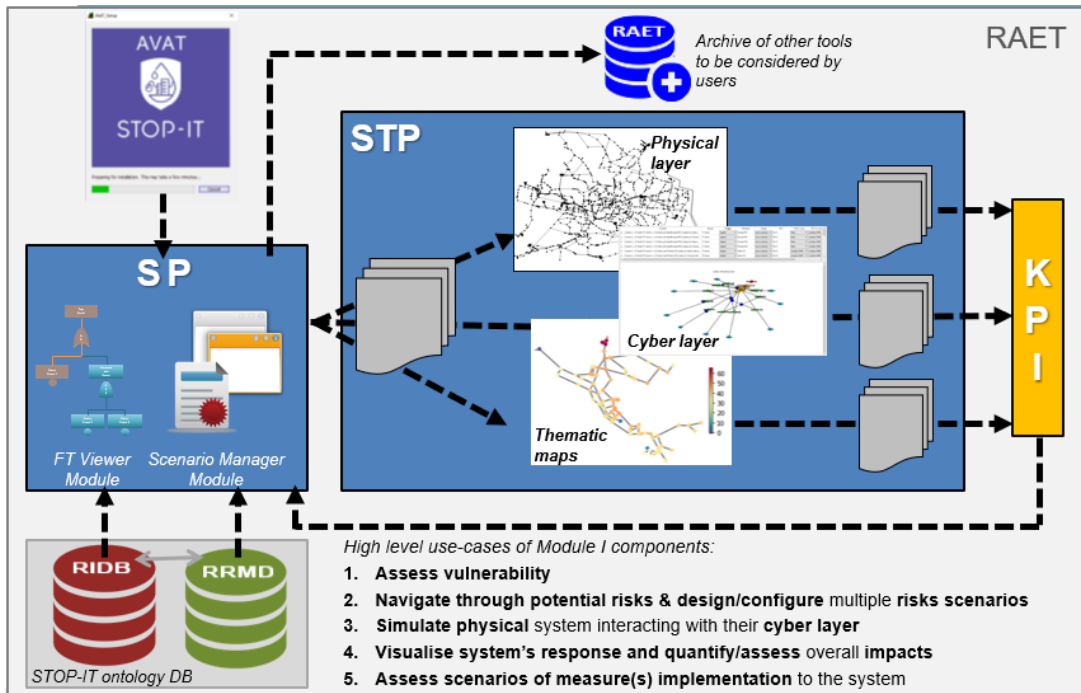


Figure 14: High level scenarios of use of Module I tools

The Stress-Testing Platform with its models, is an essential part of the toolkit of risk analysis, evaluation and treatment, at strategic and tactical level of planning, since it provides the means for simulating cyber-physical events and serves as a test bed for alternative risk events and treatment options.



## 3 Training for Operational Resilience (TORC)

### 3.1 Training for Operational Resilience (TORC)

#### 3.1.1 Training for Operational Resilience: the TORC original version

Training for Operational Resilience (TORC) is a training-by-gaming approach based on a board-game setup. The TORC approach was developed between 2014 and 2016 under the Saf era (ERA-NET) project, coordinated by SINTEF.

TORC is designed to facilitate organizations and teams that seek to reveal, understand, articulate, demonstrate and/or develop their inherent repertoire of resilient performance in face of unexpected deviations, disturbances and shocks. The training outcomes and experiences are captured in a way that prepares them to be used as raw material of technological, human, organizational and managerial priorities and resources that are needed to transform the experience from the training exercise into effective resilience capabilities under a more formal managerial supervision. This approach enables water utilities to develop their human skills while enjoying the benefits of a gaming approach and utilizing competitiveness between the trainees. The foresaid will contribute to the significance of the training.

The TORC game setup is available for free and comprises a paper-based game board, and generic supporting material regarding intake and preparation for TORC training. The joint results and resources from the Saf era project are available at <https://www.sintef.no/en/projects/torc-training-for-operational-resilience-capabilit/>

A TORC game session is suitable for training groups of 5 to 6 people. A substantial improvement can be achieved for autonomous training of a single trainee group with a common challenge and joint field of practice. However, individual training groups and results can be combined interactively across organizational levels and domains and dispersed in time to facilitate a broader strategic objective of resilience training and development beyond the confines of the individual training group. Moreover, TORC training groups may be composed homogeneously or heterogeneously depending on the overall (resilience) objective and needs of the trainees' organization or training sponsor.

The simplicity of the TORC approach and gaming material per se is somewhat counterweighed by the need to prepare detailed training material for specific training contexts, e.g., specifications of the operational situations subject to potential disturbance, and the specific disturbances that emulates the "surprise" for trainees. The development and coordination of an overall strategic objective for several individual training activities may also seem overwhelming at first glance. However, if an incremental rather than a "grand design" approach is chosen, the efforts as well as the rewards may instead develop more organically over time.

Hence, a substantial benefit may also be derived from such a process of preparation, e.g., a clearer understanding of operational vulnerabilities as well as of mitigation options that may



constitute the grounds for effective policies, strategies and objectives for resilience development, training objectives included.

It is therefore highly beneficial that the trainee organization invests in internal competence building to establish an internal coaching capacity for TORC training. The resources from the SaferEra project (link above) are primed to facilitate a "train-the trainer" process, supervised by an external (R&D partner), e.g. from the TORC Consortium.

### 3.1.2 The expected aims for training with TORC

The basic aim of the original TORC is to address, nurture and develop skills, competencies, resources and collaborative strategies and practices that allows the trainees to cope *resiliently* with surprise and disturbance that brings them at or beyond their limits of preparation.

The adverb *resiliently* is used deliberately to signify that although TORC is duly founded on applicable theories of resilience as a concept, emphasis is put on the premise that resilience is a matter of action and practice, not of possession of something, nor of application or embracement of specific terms.

Although resilience is often mentioned as a desired property of an organization, being resilient is never the main purpose of any organization. Resilience has to unfold in the context of some other objective or guiding principle. The questions "resilient to what and why" are too easily forgotten. TORC aims to raise awareness of these premises for engaging in resilience development. Moreover, as safety-critical organizations was the original target for TORC, it is crucial to recognize that the main expectation and imperative from the environment – whether originating from laws and regulations or sheer cultural bias - is to operate safely and intensively according to rules and procedures. In other words, resilience, as an ultimately adaptive practice of addressing unique events in novel and emergent ways, has to unfold in the context of its sheer opposite: the expectation of being safe through reacting to recurrent events by stereotypical and replicable means.

The more narrow and pragmatic aim of TORC is thus to assist those organizations that recognize that they need to train on acting resiliently in the context of a compliance regime, and need to be able to operate safely and sustainably under circumstances and conditions that exceed those of which the compliance regime has expected them to operate under. In short, they need to train on *resilience in the context of compliance*. As a matter of fact, quite many organizations recognize just that, and thereby also recognize that it is actually possible to make some real progress on resilience.

Although originally designed for safety-critical environments, the resilience principles embedded in TORC are also relevant for organizations seeking innovation of operation rather than safety improvement, as a response to emerging new conditions. Even more relevant for STOP-IT, TORC is also very well suited for cyber security objectives, in which the premise of "being prepared to be surprised" rather than "preparing for not being surprised", is much easier to recognize and to accept than in the safety domain.



The common ground for any application of TORC is the premise that resilient properties can not be "imported" from the outside as a ready-to-go concept but should be nurtured and developed by addressing and naming the existing rudiments of resilience through training on practical situations routinely over time. By actively using the practitioners' own language, it is also possible to reinforce and build a resilience inventory in terms of skills, competences, resources and collaborative strategies to combine them.

Building the local resilience inventory is a key aim of TORC, enabling not only after-action reviews there and then, but also creating the means for interchange and discussion of experience, and projection of situated practices towards other operational contexts in the same organization. By means of this, different parts of the organization can improve their mutual understanding of practices as well as rationales for action, enabling more sophisticated, polycentric training scenarios in which different professions and roles can coordinate in a diverse but altogether resilient manner.

TORC also encourages a process of making a distinction between situated practices that work in specific contexts only, and generic practices that may be comparable with, influence or inspire similar practices in other contexts. Through the accumulation of a generic inventory, the organization will increase its chances of not only being able to compare and learn from other, similar organizations, but also to create the conditions for a reflexive space to address the historicity of its own unique resilience, asking questions like "what is our adaptive history?", "how did that influence our precarious present?", "what is our resilient future?" "how do I update the historical version of TORC for new threats".

Another key aim of TORC is to distinguish between as well as reconcile operational vs managerial training. That is, understanding the relation between the needed margin for successful operation, and the managerial mandate that sets the limits for the explorative nature of resilience as well as the corresponding accountabilities and responsibilities of each sector. This is especially relevant when something goes wrong, despite an attempt of acting resiliently. TORC training aims to counteract the misconception that resilience is associated with success only. The TORC premise of "acting resiliently" implies an invitation of doing things differently but carries no guarantee of success. If mandates and accountabilities are unclear, the subsequent consequences may turn into blaming the wrong factor and fault reasoning of the event. That being said, the simple distinction between "operational" and "managerial" may also be delusional and not sufficiently aligned with the broader idea of polycentric governance, which may imply the coordinated action of a broader set of organizational functions, roles and responsibilities. The operational vs. managerial distinction may therefore be seen as an instantiation of a more generic concept of communicative pragmatics that reflects differences in accountability and motivation for organizational action.

### 3.1.3 The TORC references

During the Safëra project, ca 1000 employees from Dutch companies Strukton Rail, Infrasppeed and NAM were doing some form of TORC training as part of the development and piloting process. The project, the deliverables and the experiences are described in TORC



Safëra project website (SINTEF, 2019)

Prior to, during and after the project period, TORC has received positive (scientific) attention at Resilience Engineering Association (REA) Symposia.

At the 5th REA Symposium in Soesterberg, Netherlands, 2014, the safety theoretical foundation for TORC ("compliance vs resilience") was presented at a special session (Grøtan 2014). At the 6th REA Symposium in Lisbon, Portugal in 2015, the elaborated "resilience in the context of compliance" concept was presented by Tor Olav Grøtan, and the Managing Director of Strukton Rail declared their intention, together with other Dutch industrial partners, to use TORC for advancing practical resilience in the industrial context. At the 7th REA Symposium in Liege; Belgium, TORC was the subject of a Special Industry Debriefing Session, organized by John Van Schie, NAM (Netherlands), one of the industry participants in the Safëra project. At the 8th REA Symposium in Karlstad, Sweden, Eder Henriqson from Brazil reported recent TORC experience with aviation pilots and a project that explored the methodological procedures in three phases of the game: preparation (i.e. objectives, game definitions and context), application (i.e. training process and training format) and analyses (i.e. discussion about relevance and training method).

At the *Tools for Resilient Infrastructure Workshop* (REA 2017) in London, February 2019, organized by *The Resilience Shift* (supported by Lloyds Registry Foundation and Arup) and the Schumacher Institute, TORC was presented (Grøtan 2018) and received very well, not at least due to its pragmatic and practicable definition of resilience.

In the H2020 DARWIN project (Herrera et al. 2019), a set of different D-TORC modes were elaborated for further application; emulation mode, reconstruction mode & simulation mode. In September 2019, as part of a webinar series organized as a collaboration between REA and the H2020 Darwin project, TORC is the subject of a designated webinar (Grøtan 2019)

In the Resilience Engineering and Safety Management for Complex Socio-Technical Systems (STERNA) project (see <https://www.ntnu.edu/iot/sterna>), a collaboration between cooperation between four Brazilian universities, NTNU, SINTEF and industrial partners, TORC has been lectured as a separate subject on resilience training through webinars. This webinar has also been the template for the designated TORC webinar published by REA.



## 3.2 The STOP-IT training for operational resilience

### 3.2.1 Purpose of adopting TORC in STOP-IT

Water is a critical sector, and any disruptions in availability or integrity can have disastrous effects on local health and economies. Beside the needed protection of water critical infrastructure against physical threats, for which water utilities are more prepared, there is a need to understand the potential vulnerabilities brought by cyber threats and the physical-cyber threats combination. The cyberspace is developing rapidly, and the challenges are transboundary. To protect against water service disruptions, cyber security must be part of the water utilities' strategy. Unfortunately, cybersecurity experts in the water sector are in short supply and often insufficient for the needs of the operations.

The STOP-IT project aims at making the water systems secure and resilient by improving preparedness, awareness and response level to physical, cyber threats and their combination. To this purpose, STOP-IT provides modular solutions (technologies, tools and guidelines) embedded into the STOP-IT platform. However, making solutions available is not enough: creating awareness about the benefit of implementing them, assessing the preparedness of an organization in adopting them, defining the way their use is (managerially) mandated and subjected to governance in the organization, identifying the operational constraints and principles regarding their deployment and use are equally relevant factors to be covered to improve the resilience of the water sector. The water sector must maintain a resilient operating environment in the face of ever-changing cyberthreats while also supporting digital innovations.

TORC is adopted in STOP-IT as a gaming approach to stress test the organizational resilience of a water utility in case of cyber and/or physical attacks. The point of departure for TORC in STOP-IT is that the notion of resilience comprises both the technical system per se and the socio-technical fit between the system and its use.

The scope of the game is about being trained at avoiding mistakes that it is possible to anticipate and prepare for, while also being able to handle unexpected situations, disturbances and disruptions that will inevitably arise. Dealing with the expected and the unexpected, however, require relatively different organizational abilities. The focus of TORC is how these two abilities can be merged and maintained in the organizational culture.

Through the STOP-IT TORC sessions, the players can:

- Explore and decide on strategies to work with unexpected situations related to scenarios of cyber-physical attack;
- Explore and decide on resources to be deployed to support and back up adaptive action;
- Experience how different teams and the company network are of great value to support protection activities, therefore creating awareness and engaging towards a common goal all the decision levels – strategic, tactical and operational in an aligned decision process;



- Reflect on applied capabilities and review on experience build up as well as positive and negative outcomes.

It is recommended to engage skilled support from researchers or consultants in order to gain maximum benefit from TORC training. With proper strategizing in advance, TORC can be part of a strategic foundation for developing organizational resilience.

### 3.2.2 Adaptation of TORC to STOP-IT

The STOP-IT TORC builds on the original version (SINTEF 2019, Grøtan 2017), but it is adapted to the scope of STOP-IT and its solutions.

The game inventory includes a game board pad, resources cards, risk reduction measure cards and value cards (see Section 3.3.1).

The players include the facilitator and 5-6 trainees with different roles (see Section 3.3.6).

To begin, the game board is placed on the table. The facilitator will then present a scenario reflecting the local conditions of the water utility where the training takes place; the facilitator will challenge the players with a sudden 'disturbance' or referred to as a 'stressor' in TORC terminology. Such a stressor can be, for instance, a cyber-attack for which the potential impacts on the service reliability have to be assessed, the eventual risk reduction measures to treat the risks needs to be selected, and the feasibility of adopting them must be analysed. The reflection during the game on the impact of the proposed stressor and the identification of feasible risk reduction measures is facilitated by covering the steps depicted in the board, as well as the reflection after the game.

In depth details about how to play the game are given in Section 3.4, but the brief information provided here is required to describe how the outcomes from STOP-IT are made available to support the game.

There are three card types, as previously mentioned. The trainees will have to use them to their best effect to cover the different steps of the game.

#### **The resource cards (based on WP4 Module I):**

These cards provide support to the trainee to assess the potential impact of a stressor to the system reliability. Each resource card reflects one of the STOP-IT modelling solutions included in the Module I of the STOP-IT platform. During the game the trainee can go through the resource cards included in the inventory, and, based on the described "ability", propose the use of one of them to assess the stressor impact. The use of the card is limited to the suggestion of adopting a given modelling solution, not real time running of the specific solution is planned during the game. The trainees can also suggest additional resource cards, by creating new ones during the training session, based on other possible resources available in house. The new cards created will then be saved in the TORC inventory for future training sessions.



### **The RRM cards (based on the WP4 RRMD and WP5 solutions):**

The RRM cards consist of the solutions that the trainees can suggest treating the risk. The RRM cards included in the STOP-IT TORC inventory are created from the STOP-IT RRMD in Deliverable D4.3 (Mälzer et. al. 2019) and the solutions developed at operational level (WP5) as general RRMs. During the game the trainees can place on the board selected RRMs and start the assessment of their potential effectiveness and feasible adoption in the actual context. The trainees can also suggest additional RRM cards, by creating new ones during the training session, based on other possible solutions available in house. The new cards created will then be saved in the TORC inventory for future training sessions. The new measures can also be added to the STOP-IT RRMD by using the dedicated entry mask form (see STOP-IT deliverable D4.3, Mälzer et. al. 2019).

### **The value cards:**

The value cards consist a pre-defined template to be used at the end of the game session to let the training group assess its own resilience performance level relating to the whole training session. The value cards are not directly linked to any STOP-IT solutions, being an empty template, but the information they will include at the end of the game session will be of valuable support to facilitate the adoption of the selected solutions (including those of STOP-IT), as the for training, human resources and / or investments.

### **The roles of the trainees during the game reflect the water utilities profiles targeted by WP8:**

The adaptation of the original TORC to the STOP-IT version also relates to the possible roles of the players. Before starting the game, the facilitator appoints the trainees for a specific role, which may or may not be the trainee's role in real life within the organization. The roles reflect those defined in D8.1 (Ahmadi et al. 2018) as selected water utilities profiles for targeting training sessions: the decision maker, the risk assessment officer and the staff responsible for operational activities (see also Section 3.3.6 in this report).

### **3.2.3 Expected benefit from TORC**

Upon completion of a TORC training program, an organization can expect to have gained:

- a unique opportunity to gain insight into hidden, tacit but necessary practices in its own organization; in an advanced training framework that utilize gaming approach advantages, which is not common at the moment in water utilities.
- experience with a conceptual framework and a methodology that gives management the ability to formulate (and take responsibility for) actions enabling sustained harmonization between how work ideally should be done ("work as imagined") and how the work is implemented in practice ("work as done"); this also includes;
  - Identification of possible shortages in organizational resources
  - Identification of potential communication flaws





- Identification of the presence and lack of tools and control options of persons at the job to cope with unexpected situations
- Identification of specific training needs;
- a sustained and productive dialogue between personnel with different perceptions and perspectives on safety and security; and
- a flexible "gaming" platform for further development of safety and security, with many opportunities.
- The ability of the trainees to play a different role than the one that they fulfill in real life can contribute to a better understanding of the point of view of others in the organization and will increase the communication and collaboration in the water utilities.
- Experiencing a stressor and dealing with it in the context of a game can prepare the trainees for the stress they will experience during an actual situation and give them confidence to handle such a situation.

### 3.3 The STOP-IT TORC gaming approach

#### 3.3.1 The STOP-IT TORC Game inventory

The TORC game inventory, adapted for the use in STOP-IT, includes:

1. The board game pad
2. The resource cards
3. The Risk Reduction Measures (RRM) cards
4. The value cards

#### 3.3.2 The board game pad

The TORC board game pad is illustrated in Figure 15. The game pad provides a simple way to structure the exploration or to encounter a scenario that potentially increases the risk of undesired event. Through various types of predefined cards, the game provides guidance on how the scenario may develop and which resources and strategies that can be taken into use to cope with the challenges that arise. However, the predefined cards are not necessarily a constraint as new disturbances, skills, competencies, resources and strategies can be developed *en route* (and "cardified" if wanted) depending on the choice made by the game facilitator.

The inner circles of the game pad labelled as Detect, Prevent and Mitigate correspond to identification of the overall type of strategy followed by the players during the game and it is part of the final assessment of the game session.

The board game pad of the STOP-IT TORC inventory is included in the Annex B (section 6.1).

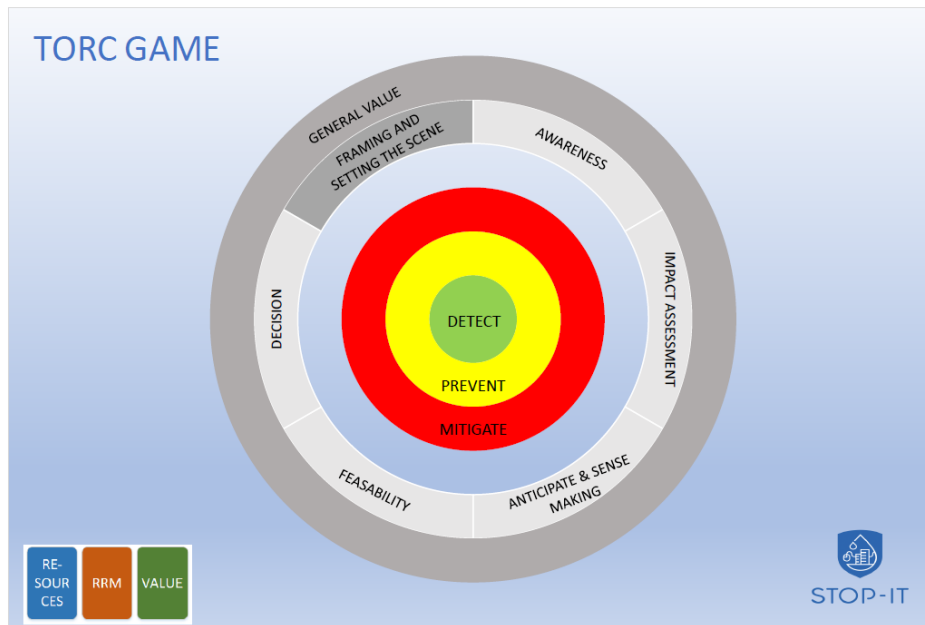


Figure 15: The STOP-IT TORC board game pad

### 3.3.3 The resource cards

The resource cards are played by the trainees during the board step of "impact assessment". At this step the trainees will point out the solutions or modules from STOP-IT that can help assess the impact of the stressor by selecting resource cards available as part of the game inventory. The template of the resource cards is depicted in Figure 16.



#### Description of the card:

**Name:** name of a STOP-IT modelling solution.

**Corresponding module in STOP-IT:** module number in the STOP-IT platform

**Description:** brief description of the modeling solution and purpose of use.

**Type of results:** brief description of the expected results to allow the trainees on the ability of the card (the solution) to provide the kind of assessment needed for the scenario under assessment.

Figure 16: Template of the resource cards

The resource cards are built on selected the STOP-IT solutions; however the trainees can also develop their own resource cards to reflect competencies, resources and strategies available in house. The new cards developed during the game should be saved for future training session as part of the game inventory.



The cards made available as part of the STOP-IT TORC inventory are included in the Annex B (section 6.2).

### 3.3.4 The Risk Reduction Measures cards

The RRM cards must be selected from the list of options included in the inventory as solutions to be considered at the step of "Anticipating the alternatives and sense-making".

The selection of the RRM cards is facilitate based on different colors and symbols used in each card to reflect three of the criteria used in the STOP-IT RRMD (Deliverable D4.3, Mälzer et al. 2019):

- The *type of threat* that originates a risk event to be treated by a given RRM. The type of threat addressed by a card can be easily identified by the color and symbol indicated in the right-upper side of the card:

Cyber threat: <b>blue</b>	
Physical threat: <b>orange</b>	
Cyber-Physical threat: <b>green</b>	

Table 1: Symbols and colors used in the RRM cards for quick identification of the type of threat originating a risk event

- The *type of asset*, which defines which type of asset is affected by the outcomes of the risk event for which the risk shall be reduced. Depending on the type of asset a specific symbol is indicated in the card:

Catchment Area	
----------------	--



Drinking Water Network	
Drinking Water Tanks	
Pressure Boosting Station	
Raw Water Bodies	
Raw Water Pipeline	
Water Abstraction Points	
Water Treatment Plants	

Table 2: Symbols used in the RRM cards for quick identification of the type of asset affected by the outcome of the risk event

- The *event consequence* defines which consequence dimensions are affected if the given risk event occurs. Depending on the event consequence a specific symbol is indicated in the card:

Quantity	
----------	--



Quality	
Financial	
Reputation	

**Table 3: Symbols used in the RRM cards for quick identification of the event consequence**  
 Additionally, each card will include information related to the specific RRM described:

**Measure ID:** ID used in the STOP-IT RRM. This information is provided in case the trainees plan to extract further information from the STOP-IT RRMD.

**Name:** name of the measure as provided in the RRMD

**Scope of use:** description of the measure and aim of use as provided in the RRMD

**Comments:** additional comments provided for the specific measure, if available, in the RRMD.

Figure 17 depicts an example of RRM card.

2

Risk Reduction Measure

Type of threat  
Cyber-Physical

Measure ID

Name

Scope of use

Comments

Type of asset				Event consequences	
Catchment Area	Drinking Water Network	Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
Raw Water Bodies	Raw Water Pipeline	Water Abstraction Points	Water Treatment Plants	Financial	Reputation

**Figure 17: Example of RRM card**



The cards made available as part of the STOP-IT TORC inventory are included in the Annex B (section 6.3).

### 3.3.5 The value cards

The value cards are created at the end of the game session during the "general value" step.

An empty template is provided in the game inventory for this card and it must be filled in based on the training sessions outcomes (the template is available in the Annex B (section 6.4)).

This card recaps the main findings from the game session. The card should include the description of the scenario played, the actions agreed, and recommendations emerged during the discussion which are of value for the specific utility's decision-makers or could even be shared with other water utilities (e.g. as result of training sessions organized in the context of the STOP-IT Project CoPs). It contains the adaptive action path that the players have adopted during the game regarding the different choices that they made. It also describes the resources (card) used, skills and competences deemed necessary, and plans for coordinated actions.

With this card, the training group assesses its own resilience performance level relating to the whole training session.

The image shows a template for a 'VALUE' card. It is a rounded rectangle with a green border. At the top left, there is a green hexagon containing the number '3', followed by the word 'VALUE' in green. Below this, there are five labeled sections: 'Scenario', 'Facilitator name and organisation', 'Actions agreed', 'Notes', and 'General recommendations'. Each section is followed by a horizontal line indicating where to write.

#### Description of the card:

**Scenario:** describe the scenario and stressor(s) used during the training session.

**Facilitator name and organization:** name of the facilitator and of the trained organization.

**Actions agreed:** brief description of the agreed actions, including the resources used.

**Notes:** it includes additional notes or comments to better clarify the agreed actions.

**General recommendations:** it described the skills, investments and competences deemed necessary, and plans for coordinated actions.

Figure 18: Template of the value cards

### 3.3.6 The players and their roles

To play the STOP-IT TORC game one facilitator and 5-6 trainees are required. In the context of STOP-IT, the trainees will cover the roles of one of the water utilities professional profiles defined in STOP-IT Deliverable D8.1 (Ahmadi et al. 2018), i.e. decision maker, risk



assessment officer or part of the staff responsible for operational activities. It is one of the facilitator tasks to define the trainees' roles when launching the game. The role of each trainee should be assigned depending on the type of training session, i.e. heterogeneous vs. homogeneous. In a heterogeneous training session, the roles may correspond to the roles of the trainees in the real life or may be assigned differently depending on the goal of the stress testing exercise.

The role of the facilitator is crucial for the success of the game session, therefore, recommendations for the facilitator are provided in a fully dedicated section of this report (Section 3.5).

Regarding the roles of the trainees, the definitions of the competences and responsibilities of the three possible profiles, as described in STOP-IT Deliverable D 8.1 (Ahmadi et.al. 2018), are as follows:

**Decision-maker:** The decision-maker or utility manager profile consists of high-level decision makers in the utility. The profile consists of the board members of the utility and relevant top-level managers of the private contractors if identified necessary by the utility's board. The people categorized as decision-makers may have various backgrounds and expertise in different domains but in their capacity as decision makers, no assumption as to their expertise can be made. Since this group possesses the right of decision-making in utilities, the intention is to expose them to a more general overview of the cyber-physical security challenge. Moreover, creating awareness at this level creates a top-down competence building effort aiming at improving the general preparedness of utilities against cyber-physical threats. This will also provide them with information regarding how STOP-IT will enhance risk management in general in utilities.

**Risk assessment officers:** Water utilities have wide and varied responsibilities requiring them to manage a complex set of risks at strategic, tactical and operational levels. However, although risk management process can vary from one utility to another, focal points for risk management (e.g. risk managers, group risk managers, chief risk officers, performance and quality managers including the personnel responsible for modelling activities) play a central role in the process. For the sake of simplicity, we will use the term "risk management officer" throughout this report to describe any individual or group of people having responsibility of risk management at some level in the utility. This group includes also individuals working with the main risk officer of a utility to assess and manage risks within the organization, including water system modellers.

**Staff responsible for real time operations:** This profile focuses on operation and maintenance managers of water production plants or wastewater treatment plants and any staff responsible for real time operations (such as SCADA room operators, maintenance teams) and supporting functions. They have various different backgrounds and can decide about daily real time operations.



## 3.4 Playing the STOP-IT TORC game

The key features of a STOP-IT TORC game are illustrated in Figure 19. Upon launching the game, activities within "Framing and setting the scene" step take place. The facilitator assigns a role to each participant which may or may not be his/her actual daily role or affiliation. The facilitator introduces a predefined scenario which will be played out in the training session.

As the first disturbance (stressor) is introduced by the facilitator, the group embarks on process denoted as "reflection in action" comprising a set of cognitive aspects: awareness building, impact assessment, sense-making, feasibility assessment, and decision making. This step is arguably the most important step in the game starting from building a common understanding how a detrimental scenario may develop, realizing the impact in the context of the service provided by their organization, assessing the possible risk reduction measures and their effectiveness to overcome the challenges, anticipating the requirements for implementing the solution, and taking the decision on which alternative(s) to implement. An additional orchestrated scenario can thus be played out by introducing new stressor(s).

The game facilitator decides time constraints and circulation of roles within the trainee group. When the game is concluded, the facilitator and the players summarize the findings of the game in the process of "reflection after the game". The outcome of this process is in the form of a value card that can help a real-life decision-making if the organization encounters a scenario as played out in the game. Finally, from the assessment of the general value created by the game, the facilitator and the players can drive conclusions of the resulting strategies applied during the game and assess if the decisions made are aimed towards detection, prevention or mitigation actions ("evaluation of the game result").



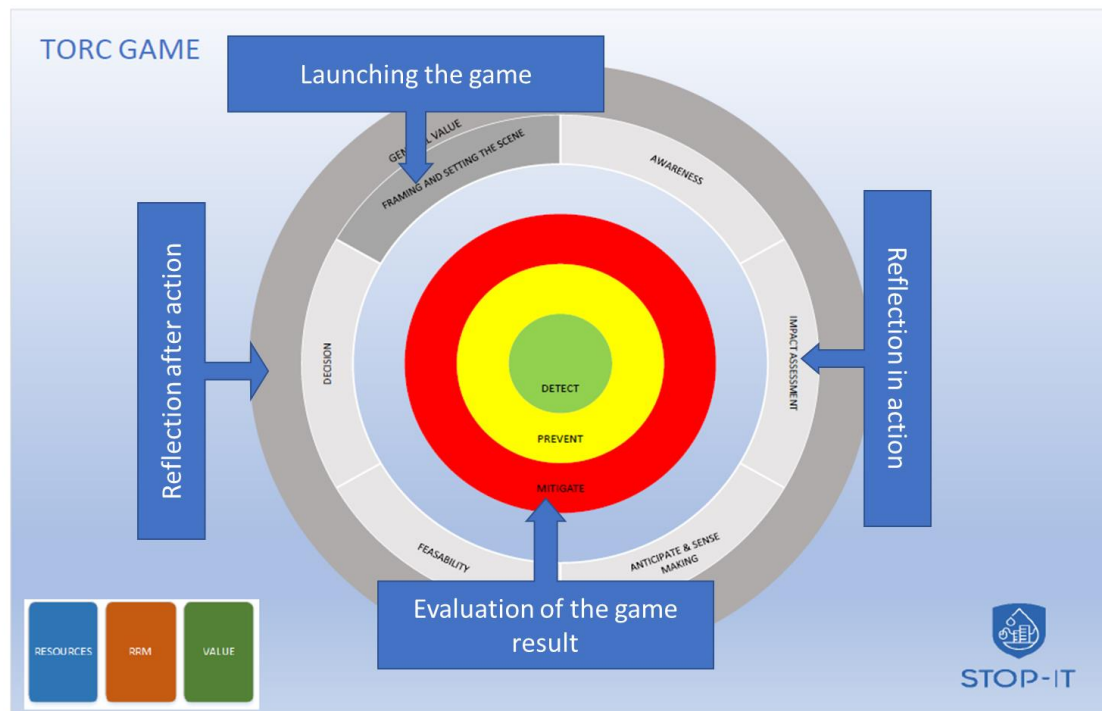


Figure 19: Key features of playing the TORC game

The objectives of each step can be briefly described as follows:

#### Launching the game:

- 1- Framing and setting the scene: the objective of this step is to provide a customized scenario to players with defined roles including local conditions and the stressors.

#### Reflection in action process:

- 2- Awareness: This step assesses, as holistically as possible, what might happen, how the scenario and the disturbance might develop into undesired event.
- 3- Impact assessment of the scenario: the assessment of scenario's impact on the service or the infrastructure by the players contextually using possible relevant STOP-IT modules (described in the resource cards).
- 4- Anticipating the alternatives and sense-making: this step provides a set of possible risk reduction measures (described in the RRM cards) to detect/prevent the stressor and/or to mitigate the consequences of the scenario by evaluating their effectiveness.
- 5- Feasibility: this step studies the technical and organizational feasibility requirements to implement the possible alternatives.
- 6- Decision: within this step, one or a set of alternatives are chosen to be implemented.

#### Reflection after action process:

- 7- Registering the result and value creation: this step summarizes the findings of running the scenario on the value card that can be used as a real-life decision-making



feedback and can feed the inventory of STOP-IT TORC.

### **Evaluation of the game result:**

When the game is concluded, the facilitator and the players can derive conclusions of the resulting strategies applied during the game and assess if the decisions aimed towards detection, prevention or mitigation actions.

#### **3.4.1 How to play the game**

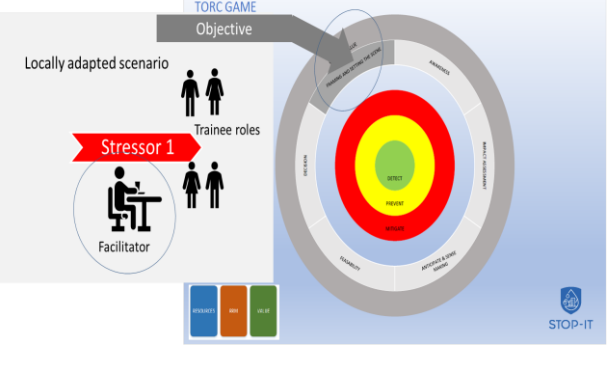
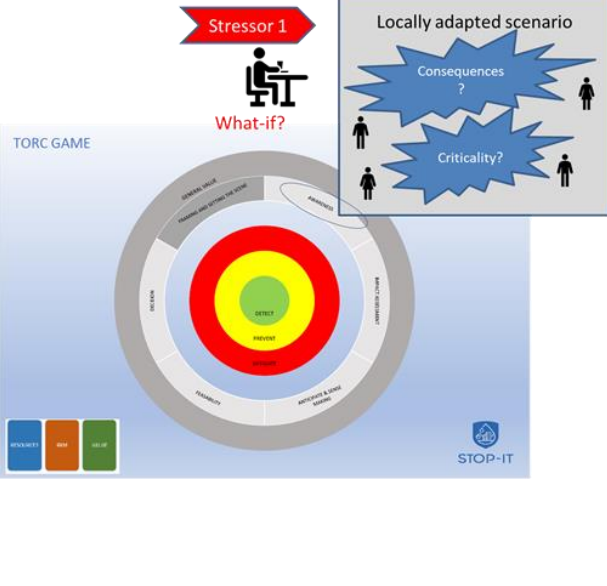
The typical single TORC training session unfolds as follows:

- A training situation is defined as a scenario being on the edge of normalcy. That is, it is conceivable to introduce a disturbance (stressor) that renders the normal preparations and ways of working insufficient to deal with the possible unwanted consequences.
- The training group is composed in a manner to ensure that each of the members are able to recognize the essence of the scenario, identify possible unwanted consequences, and be associated with some level of practice that can influence the situation (after a disturbance is launched).
- A disturbance (stressor) is launched by the facilitator. The group is given a time limit to go through all steps of the game board. One individual trainee is assigned to be the head of the trainee group (the decision maker).
- The game starts at the "awareness" field. Here, the group is expected to identify additional information to understand as much as possible of the disturbance and identify ways of gathering such information.
- The next step is "impact assessment". Here, the group is expected to elaborate and describe the potential (undesired) impact of the disturbance, how it may evolve and identify resource cards that could be used to better assess the impacts.
- The next step is "anticipate and sense making". Here, the group is expected to elaborate and describe various potential alternatives for mitigating the disturbance. The group selects general RRM cards, elaborate on how the general cards should be adapted to the local use and/ or create additional new RRM cards. The group also assess the effectiveness of the proposed RRM.
- The next step is "feasibility". Here, the group assesses the technical and organizational feasibility requirements to implement the possible alternatives.
- The next step is to "decide". Here, the group is expected to select one of the alternative actions. If the group does not agree, the head of the group must decide.
- If a cascading training is wanted, the facilitator issues a new disturbance, the role of head of the training group is shifted, and the whole process is repeated. The new disturbance might be predefined, determined by the facilitator due to the actual circumstance, or derived from the actions of the trainees themselves (e.g., activating an issue that the trainees has identified through the preceding "feasibility" step.

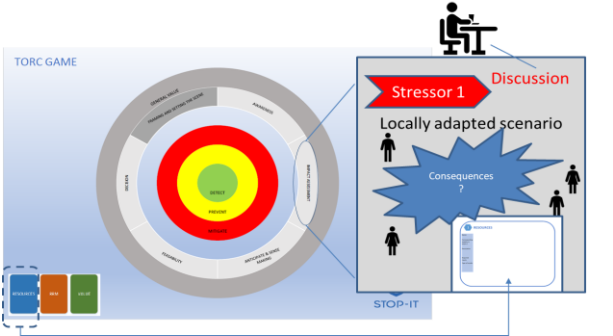
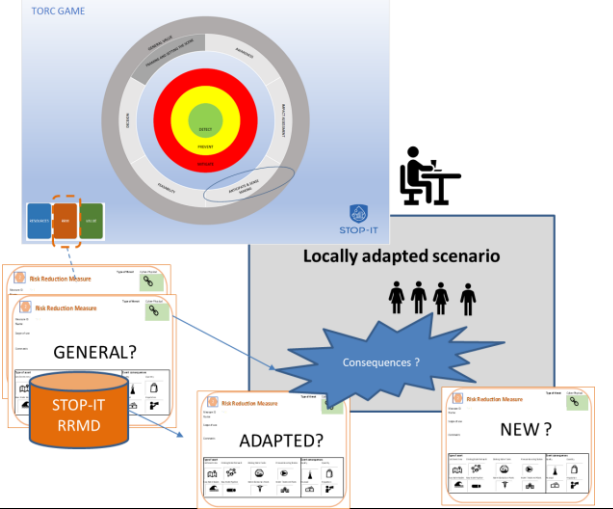
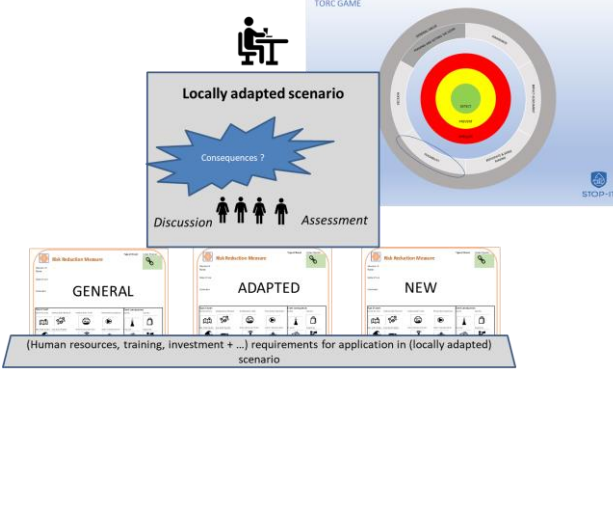


For each of the steps, resources used, skills and competences deemed necessary, and plans for coordinated actions taken must be described on "value cards" and put on the game log contributing to the inventory.

When the training session ends, an evaluation of the game results is conducted by reconstructing the training activity and reflecting on the value cards, including the resilience performance assessment. Table 4 describes the specific actions corresponding to each step of the game and the role of different players.

Game phase and activity	Illustration
<p><b>1) Framing and setting the scene</b></p> <ul style="list-style-type: none"><li>• The facilitator prepares prior to the game a customized setting (stressor-scenario) adapted to the context of the concerned utility playing the game.</li><li>• The facilitator points out the roles of each player, then, he introduces the infrastructure's context.</li><li>• The facilitator then introduces a predefined stressor to the system as a part of the predefined scenario.</li></ul>	
<p><b>2) Awareness</b></p> <ul style="list-style-type: none"><li>• The trainees discuss the actual criticality of the stressor and what are the possible scenario's consequences contextually.</li><li>• The facilitator will lead the discussion and make it as interactive as possible by providing what-if types of discussions.</li><li>• The facilitator must be able to help the trainees to realize the criticality of the stressor and that it poses detrimental consequences. The process should be able to develop a sense of self-realization of the importance of the matter in their own organization context.</li></ul>	



Game phase and activity	Illustration
<p><b>3) Impact assessment of the scenario</b></p> <ul style="list-style-type: none"><li>• The trainees will point out the solutions or modules from STOP-IT that can help to assess the impact of the scenario if any possible by selecting a resource card.</li><li>• The facilitator can then moderate the discussion about their choices</li></ul>	
<p><b>4) Anticipating the alternatives and sense-making</b></p> <ul style="list-style-type: none"><li>• The trainees can select RRM cards in order to detect, prevent and/or mitigate the consequences of the scenario studied.</li><li>• They can adapt RRMs that are already available in the list of RRM cards or they can suggest new types of RRM used in their specific utility's configuration. If new RRM are proposed by the trainees, a card should be made based on the provided template (Section 6.3).</li></ul>	
<p><b>5) Feasibility</b></p> <ul style="list-style-type: none"><li>• Players discuss and assess the requirements (human resources, training, financial resources etc.) to implement the RRMs selected and the needs within the specific utility and/or the boundary conditions described by the facilitator.</li><li>• The aim of this step is to assess the actual feasibility to implement the selected RRM(s), the expected time at which the RRMs are expected to be effective and define the requirements to facilitate their adoption.</li></ul>	



Game phase and activity	Illustration
<p><b>6) Decision-making</b></p> <ul style="list-style-type: none"> <li>Based on the outcomes of the discussion in the previous steps, the most effective solution(s) are chosen by the relevant players with the decision-making roles.</li> <li>The selection is complemented with the list of requirements to be followed up in order to make the adoption of the solutions feasible.</li> <li>This can be the end of the game or the facilitator introduces a new stressor within the system at the current state of the game.</li> </ul>	<p><b>TORC GAME</b></p>
<p><b>Continuation (new round) (optional step)</b></p> <ul style="list-style-type: none"> <li>Before moving to the "value creation" step, the facilitator can decide to run multiple sessions of the game (steps 2-6) by adding additional stressors to the scenario resulting from the decision step of the previous game session. In this case the trainee will start the game over again from step 2.</li> </ul>	
<p><b>7) Value-creation</b></p> <ul style="list-style-type: none"> <li>The facilitator summarizes with the help of the trainees the findings of the game on a final card which is called "value card".</li> <li>The card may include the recommendations for utility's decision-makers or for being shared with other water utilities. It contains the adaptive action path that the players have adopted during the game regarding the different choices that they made. The template of value card is provided in Annex B (section 6.4).</li> </ul>	<p><b>3 VALUE</b></p>

Table 4: Playing with STOP-IT TORC



### 3.4.2 Case: denial of service due to signal jamming

In this paragraph, we develop an example for a playing session. The scenario focuses on the denial of service due to signal jamming. We explore the crucial role of the facilitator on conducting the session and how she/he walks the player through different steps of the game.

<b>Game phase</b>	<b>Activity</b>
<b>1) Framing and setting the scene</b>	After a preliminary talk with the utility's risk assessment officer, the facilitator selects a specific part of the infrastructure (geographically or based on the problematic sectors identified by the risk assessment officers). Then, at the beginning of the game, he/she distributes randomly the role of decision-maker, risk assessment officer or staff in charge of operational activities (3.3.6; Ahmadi et.al 2018) to the players. As this utility uses a certain type of telecommunication technology to send and receive data between the control room, cloud, sensors and actuators, a possible stressor is jamming that can cause the assets not to send or receive data to/from the control room. The facilitator describes to the players the sector that the stressor may happen. For example, reservoirs' levels are critical, and the control room wants to activate the pumping stations. However, due to jamming, the command signal is not received by the pumping stations.
<b>2) Awareness</b>	Players discuss about the possible effects of jamming on the infrastructures and its impacts on the service provided. In our example above, the reservoirs will stay below critical level and empty if no action is taken leading to certain number of customers without water supply for a period of time.
<b>3) Impact assessment of the scenario</b>	The players select the resource card "Stress-testing platform – module 1" in order to assess the number of the customers and the period of time without water supply based on the KPI (D4.2, Makropoulos et al. 2019).
<b>4) Anticipating the alternatives and sense-making</b>	The players select RRM cards, distinguishing between solutions to prevent the event from happening (e.g. jamming detector) and/or to mitigate the effects (e.g. increasing the redundancy of the physical and / or IT system). Building on our example, the players might sort out possible RRM cards such as the jamming detector, cable connection, manual operation of the pumps, etc.
<b>5) Feasibility</b>	For each of the RRM cards proposed, the players discuss and assess the resources needed and the requirements to implement each option. In our example, they should evaluate, for instance, the need of additional manpower for the manual operation of the pumps, or the investments for cable connection, or the price for buying and implementing a jamming detector.
<b>6) Decision-making</b>	The players with decision making role, after considering the information discussed at the feasibility stage, choose the best option of RRM to be implemented.
<b>7) Value-creation</b>	The facilitator describes the decisions made by the players and summarizes the main solutions adopted, delivering in the form of a final card, the recommendations to be followed up by the organization.

Table 5: Example of playing with STOP-IT TORC



## 3.5 Recommendation for the facilitator

### 3.5.1 Calibrating the training scenario according to objective

The degree of adaption and creativity required from the trainees, that is, the degree to which they are expected to be able to choose between, adopt/extend and even create new Risk Mitigation Measures (RMM), is closely related to the objective of training.

One example is the objective of just familiarizing the trainees with the STOP-IT approach, inventory and tools. For this purpose, the facilitator must ensure that the scale of the stressor merely requires a quite straightforward selection of RRM(s), and only minor additional requirements that are as intuitive as possible, and that can be performed in a manner that the trainees are familiar with. This allows the familiarization of the trainees to the outcomes of STOP-IT project.

At the other end of the scale, the objective is to deliberately stress-test the trainees at the edge of their experience and preparation, and force them to stretch their conceptions and practices beyond their normal repertoire, manifested as a need to revise and to create new RRM(s), and specify extensive additional requirements to the core content of the actual RRM(s).

The training objective must anyhow be grounded in the need of the organization (familiarization or "brute" stress-testing, or something in between), and reflected in calibrated balance between the scenario, the stressor and the trainees' experience and competence.

Any objective in between is possible. The main recommendation here is that the facilitator should have a clear thought on what to achieve, for whom.

### 3.5.2 Description of the role of the facilitator

#### 3.5.2.1 The overall role of the facilitator

The overall role of the STOP-IT TORC facilitator is to link the strategic objective for stress-testing of the host organization to the capacities of STOP-IT TORC.

Hence, the overall role is also related to different phases:

- Mediating and organizing the general organizational intake process of STOP-IT TORC as part of the organizational repertoire of an asset owner
- Preparing singular training sessions
- Supervising singular training sessions
- Evaluation of the game result: Capturing, describing and organizing the take-aways from singular training sessions
- Ensuring the continuity and coherence of repeated/successive training sessions



### 3.5.2.2 The role related to each step of the game

In framing and setting the scene, the facilitator is responsible for

- selecting a training scenario
- adapting the scenario to the local context
- connecting the adapted scenario to the actual use of the STOP-IT modeling solutions (the resource cards)
- define the training objective
- define the stressor(s) (and their sequencing)
- identify the criticality issues
- define the trainee's roles
- ensure the availability of resource cards
- ensure the availability of relevant RRM cards
- prepare (print out) the value cards for use to capture results
- explain the basic playing rules for the trainees
- "kick-off" the game by introducing the (first) stressor

In the Awareness phase, the facilitator is responsible for:

- through what-if questions, guide the trainees in assessing criticalities and potential consequences

In impact assessment of the scenario, the facilitator is responsible for:

- guiding the trainees in assessing the consequences, (optionally) by using resources cards

In Anticipating the alternatives and sense-making, the facilitator is responsible for:

- guiding the trainees in selecting RRMs, adapting existing RRMs if necessary, or defining new RRMs, and making sense of their potential effects

In the Feasibility phase, the facilitator is responsible for:

- supervising, and if necessary, supporting the trainees in identifying additional requirements for making the various RRM options feasible for the (locally adapted) scenario

In the Decision-making phase, the facilitator is responsible for:

- ensuring that the trainee appointed as decision maker actually makes a decision, and "QA" that decision to avoid that it is made on obviously "false" premises

In the Value creation phase, the facilitator is responsible for facilitating the trainee group to

- recollect the training session in the form of a value card, herein





- assess the character of the overall training session,
- add the value card to the Inventory, with a special attention to the "additional requirements"
- if feasible, make an addition to the RRMD, according to the procedure defined in STOP-IT Deliverable D4.3 (Mälzer et al. 2019).

### 3.5.3 Preparatory work of the facilitator

#### 3.5.3.1 Preparing the organization: the intake process

The point of departure for the preparation process is that the STOP-IT TORC trainee organization is accustomed to the STOP-IT STP for which the STOP-IT TORC is an integral part.

The objective for the preparation process is therefore to explain and anchor the rationale for and expected benefit from using STOP-IT TORC as an add-on activity to the STOP-IT STP, and to ensure that the organization and the trainees are sufficiently primed and prepared for engaging in STOP-IT TORC training with realistic expectations, and able to utilize the outcomes in an effective and efficient manner.

Before STOP-IT TORC training is commenced, it is therefore recommended that an intake process is implemented that anchors the approach in the receiving trainees' organization, aligns the objectives with those of using the STOP-IT STP, and provides the facilitator with the necessary authority and legitimacy to work effectively and efficiently.

The intake process should draw on the generic recommendations from the TORC project, but also explicitly address the specific aim of supplementing the STOP-IT STP with STOP-IT TORC features.

For the intake process, some of the recommendations from Grøtan et. al. (2016) can be translated specifically into the STOP-IT context.

- The intake process should be organized as a project with a STOP-IT STP/TORC competent project manager (who could be the "facilitator-to-become")
- The intake process should identify a "master" scenario that clearly demonstrates the key issues of presumed STOP-IT TORC, and that can be a joint reference and a talking point for a variety of communicative actions in the organizations
- The intake process should legitimate resilient performance by identifying and highlighting a typical case of adaptation in a situation where normal procedures (e.g., "RRMs") are underspecified or do not work
- If necessary, explorative interviews and workshops are conducted to identify master scenarios and case of adaptation
- A "master plan" of training scenarios, trainee groups and sequencing should be worked out
- An intake process project plan can be developed on the basis of Grøtan et al. (2016), Section 2.4, but must be adapted to the STOP-IT concept.



The intake process should also ensure that:

- The facilitator should be skilled in the overall STOP-IT approach, familiar with the main properties of the asset, and familiar with all RMMs relevant for use in actual training
- The facilitator should not be a "lone wolf" or stranger to the operational and managerial environment in which STOP-IT STP is utilized.
- A broader, selected support group of people (focus group) should be appointed to support the facilitators work also after the intake process, design the training groups and help to disseminate and assimilate the experiences gained over time. The group should reflect all STOP-IT user roles according to WP8, D8.1 (Ahmadi et al. 2018).
- Through the support group, the facilitator should also be familiarized with the typical working contexts of the trainees.

A key element is to explain and communicate the concept of stress-testing outcome for the users, specifically as the generic abilities to *detect*, *avoid* or *mitigate* risks by means of RMMs. All these abilities may carry some aspect of resilient performance. Hence, an initial *level of ambition* for using STOP-IT TORC as a complement to STOP-IT STP should also be established at the *strategic* level of the trainee organization, along with a clear understanding of how the ambition level relates to the underlying *resilience* concept.

Here, a "lower" ambition level is to use STOP-IT TORC as a tool to familiarize trainees with the basics of STOP-IT STP (Chapter 2) and be able to utilize existing RMMs in a straightforward manner. The "higher" ambition level is to use STOP-IT TORC as a stress-testing device that challenges the limits of "any" RRM available.

The (resilience) ambition level will have direct implications and be instrumental for how the training scenarios are designed. At a "low" level, the stressors are only minor and within the trainees' horizon of understanding and experience. At a "high" level, the trainees will be exposed to highly unusual and even disturbing scenarios.

It is implicit that it makes little sense to start a STOP-IT TORC training program at a "high" level, unless there is a strategic objective to "shake" the trainees. The default option should be to "familiarize" in order to facilitate a coherent use of STOP-IT STP and STOP-IT TORC, in a sustainable manner.

A STOP-IT TORC training program must hence be established according to the overall ambition aligned with the overall objective for using STOP-IT STP and be regularly modified to reflect training experiences and overall objectives.

By establishing a scale of resilient performance as a yardstick underlying the ambition level for STOP-IT training, the trainees' organization also establishes a measure for resilience that can support other activities, e.g., for capturing, describing and organizing the take-aways from singular training sessions (Section 3.5.3.3), and for maintaining a training program



(Section 3.5.3.4) that is aligned with a *strategic resilience objective* for the organization (if applicable). In this manner, STOP-IT STP may have implications beyond its primary scope.

### 3.5.3.2 Preparing a training session

Before a training session, the facilitator should

- a) Know in detail the actual scenario, how it would play out, its delimitations as well as criticalities.
- b) If not done before, make a table-top exercise with the focus group (see Section 3.5.3.1), in which:
  - The comprehensibility and relevance of the stressor(s) for the asset and the trainees are verified.
  - The comprehensibility and severity of the stressor related to the training scenario is consistent with the STOP-IT TORC training program and aligned with the ambition level. If applicable, align the training scenario with the strategic resilience objective.
- c) Develop a set of expectations for the outcome of the training as a reference, for the purpose of (post-training) evaluating the actual outcome, identifying take-aways and considering impact on the overall training program. Such expectations shall be anchored with the focus group.
- d) When done repeatedly, the latter actions may also be a learning loop for the focus group.

### 3.5.3.3 Capturing, describing and organizing the take-aways from singular training sessions

After the training, the facilitator should

- a) Organize and document all relevant cards developed and maintained as a result of the training session
- b) Provide a "facilitator's report" that includes learning points beyond the predefined action points in the training session, including an assessment of how the trainees performed as a group
- c) Evaluate the experiences vs. the expectations, including
  - The correspondence with the presumed overall response of the training group (detect, avoid or mitigate)
  - The correspondence with the presumed ambition level (resilience performance level)
- d) Forward all relevant learning points to the focus group for comments, including suggestions for improvements

### 3.5.3.4 Maintaining a training program

The facilitator should regularly invoke the focus group for a joint effort of ensuring the continuity and coherence of repeated/successive training sessions. As part of this effort:



- a) Experiences with a number of past training sessions should be evaluated according to all relevant objectives (e.g. alignment with STOP-IT STP, ambition levels), and corrective measures identified if necessary.
- b) If necessary, the whole training program including ambition levels, training programs and trainee groups, should be evaluated and revised through workshops periodically. A number of representatives of the trainees should take part in the workshop, to make their perspective heard, and contribute to practicable and effective steps for dissemination and assimilation of experiences, competences, resources and skills created through STOP-IT TORC training.

### 3.6 TORC use in STOP-IT WP8

The use of TORC in STOP-IT training and transfer work package (WP8) is foreseen through D8.1 (Ahmadi et al., 2018). It will be delivered through tabletop exercises foreseen for profile 2 originally but certainly can be played by profile 1 and 3.

The following paragraphs, taken from D8.1, confirms the role that TORC will play in the training and transfer activities in STOP-IT through WP8:

*A tabletop exercise is a discussion-based activity facilitated by a group of persons (facilitator) according to a scripted scenario in a similar-to-real environment. It should be designed to promote discussion as participants (referred to as trainees) examine and resolve problems based on existing modalities within utilities. One of the most important outcomes of this exercise will be the identification of modalities and processes that need to be improved or redefined within utilities.*

*In order to design a highly interactive tabletop exercise, the facilitator should guide the discussion according to the initial design of the exercise to achieve the predefined goals. The facilitator role is to create a framework that promotes discussion within the whole group (not focusing on few people during the meeting), capture innovative ideas, identify shortcomings, create teamwork, and educate attendees by providing feedback on the exercise.*

*The tabletop exercise should have the following structure:*

- *Roundtable of the attendees*
- *Agenda of the day*
- *Introduction to the exercise by the facilitator*
- *Overall goals of the exercise*
- *Exercise overview: current situation*
- *Event (scenario) introduction*
- *Discussion on the event unfolding*
- *Event development in different phases according to the scenario*
- *Discussion on the event developing*
- *Assessment of the discussions and feedback*

For more information, we refer to Section 5.2.3 of D8.1 (Ahmadi et al., 2018).



## 4 References

- Agudelo-Vera, C., Blokker, M., Vreeburg, J., Vogelaar, H., Hillegers, S., and Van der Hoek, J. P. (2016). "Testing the robustness of two water distribution system layouts under changing drinking water demand." *Journal of Water Resources Planning and Management*, 142(8), 05016003.
- Ahmadi, M., Makropoulos, C., Lykou, D.A., and Zimmermann, L. (2018). "Course design for multiple end-users." Deliverable of STOP-IT Project D8.1.
- Ahrenholz, J., Danilov, C., Henderson, T. R., and Kim, J. H. (2008). "CORE: A real-time network emulator." *Proceedings - IEEE Military Communications Conference MILCOM*.
- Almalawi, A., Tari, Z., Khalil, I., and Fahad, A. (2013). "SCADA-VT-A framework for SCADA security testbed based on virtualization technology." *Proceedings - Conference on Local Computer Networks, LCN*, 639–646.
- Antonioli, D., and Tippenhauer, N. O. (2015). "MiniCPS." *Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or Privacy - CPS-SPC '15*, ACM Press, New York, New York, USA, 91–100.
- Chmielewski, H., Guidotti, R., McAllister, T., and Gardoni, P. (2016). "Response of Water Systems under Extreme Events: A Comprehensive Approach to Modeling Water System Resilience." *World Environmental and Water Resources Congress 2016*, American Society of Civil Engineers: Reston, VA, USA, 2016, West Palm Beach, FL, USA, 658–667.
- Corchero, A. Makropoulos, C., Karavokiros, G. (2019). "Risk Assessment and Treatment Framework." Deliverable STOP-IT Project D4.5.
- Davis, M. J., and Janke, R. (2018). "The effect of a loss of model structural detail due to network skeletonization on contamination warning system design: case studies." *Drinking water engineering and science*, 1–25.
- Dembo, R. S. (1991). "Scenario optimization." *Annals of Operations Research*, 30(1), 63–80.
- Diao, K., Sweetapple, C., Farmani, R., Fu, G., Ward, S., and Butler, D. (2016). "Global resilience analysis of water distribution systems." *Water Research*, 106, 383–393.
- Eliades, D. G., Kyriakou, M., Vrachimis, S. G., and Polycarpou, M. M. (2016). "EPANET-MATLAB Toolkit: An Open-Source Software for Interfacing EPANET with MATLAB." *Computing and Control for the Water Industry CCWI 2016*, 1–8.
- Fovino, I. N., Masera, M., Guidi, L., and Carpi, G. (2010). "An experimental platform for assessing SCADA vulnerabilities and countermeasures in power plants." *3rd International Conference on Human System Interaction, HSI'2010 - Conference Proceedings, IEEE*, 679–686.
- Fujiwara, O., and Li, J. (1998). "Reliability analysis of water distribution networks in consideration of equity, redistribution, and pressure- dependent demand." *WATER*



RESOURCES RESEARCH, 34(7), 1843–1850.

GDAL/OGR contributors. (2019). "{GDAL/OGR} Geospatial Data Abstraction software Library."

Germanopoulos, G. (1985). "A technical note on the inclusion of pressure dependent demand and leakage terms in water supply network models." *Civil Engineering Systems*, 2(3), 171–179.

Gillies, S., and others. (2007). "Shapely: manipulation and analysis of geometric objects."

Grøtan, T.O. (2014). "Compliance versus resilience." Resilience Engineering Association (REA). Retrieved from <https://www.youtube.com/watch?v=UMA1gCM9jXs>.

Grøtan, T.O.(2017). "Training for Operational Resilience Capabilities (TORC): Summary of concept and experiences." SINTEF Report A28099. <https://www.sintef.no/globalassets/sintef-teknologi-og-samfunn/rapporter-sintef-ts/a28099-torc-d4-1-report-a28099-v1-march17.pdf>.

Grøtan, T.O. (2018). "TORC; Training (by gaming) for Operational Resilience Capabilities." Resilience Shift Workshop. Retrieved from <https://www.slideshare.net/resilienceshift/torc-presented-at-the-resilience-shift-tools-workshop>.

Grøtan, T.O. (2019). "Training for Operational Resilience Capabilities (TORC) – A Pragmatic View of the Past, Present, and Future of the TORC Approach." New Resilience Engineering Webinar Series. Retrieved from [https://drive.google.com/file/d/1LDR57\\_Ztqj3dtwCSFGilfDe05K458w8q/view](https://drive.google.com/file/d/1LDR57_Ztqj3dtwCSFGilfDe05K458w8q/view).

Grøtan, T.O., v.d. Vorm, J., Zuiderwijk, D., v.d. Beek, D., Wærø, I., Macchi, L., Evjemo, T.E., and Veldhuis, G. (2016). "Guidelines for the preparatory work needed to implement a TORC training program." <https://www.sintef.no/globalassets/sintef-teknologi-og-samfunn/rapporter-sintef-ts/sintef-a27931-v1.pdf>.

Herman, J. D., Reed, P. M., Zeff, H. B., and Characklis, G. W. (2015). "How Should Robustness Be Defined for Water Systems Planning under Change?" *Journal of Water Resources Planning and Management*, 141(10), 04015012.

Herrera, I., Branlat, M., Grøtan, T.O., Save, L., Ruscio, D., Woltjer, R., Hermelin, J., Trnka, J., Feuerle, T., Förster, P., Cohen, O., Cafiero, L., Cedrini, V., Mancini, M., Ferrara, G., Mandarino, G., Rosi, L., Johnson, C.O., Morin, E., Shawn, E., Kieran, J., Costello, M. (2019). "Resilience Management Guidelines for Critical Infrastructures, Practical Solutions Addressing Expected and Unexpected Events." Concluding Paper of DARWIN Project (H2020/2014-2020).

Jordahl, K., Bossche, J. Van den, Wasserman, J., McBride, J., Gerard, J., Tratner, J., Perry, M., and Farmer, C. (2019). "geopandas/geopandas: v0.5.0."

Kang, D., and Lansey, K. (2013). "Scenario-based robust optimization of regional water and wastewater infrastructure." *Journal of Water Resources Planning and Management*, 139(3),



325–338.

Klise, K. A., Bynum, M., Moriarty, D., and Murray, R. (2017). "A software framework for assessing the resilience of drinking water systems to disasters with an example earthquake case study." *Environmental Modelling & Software*, 95, 420–431.

Klise, K. A., Murray, R., and Haxton, T. (2018). "An overview of the Water Network Tool for Resilience (WNTR)." 1st International WDSA/CCWI Joint Conference, Kingston, Ontario, Canada, 8.

Lantz, B., Heller, B., and McKeown, N. (2010). "A network in a laptop." *Proceedings of the Ninth ACM SIGCOMM Workshop on Hot Topics in Networks - Hotnets '10*, ACM Press, New York, New York, USA, 1–6.

Makropoulos, C., Nikolopoulos, D., Palmen, L., Kools, S., Segrave, A., Vries, D., Koop, S., van Alphen, H. J., Vonk, E., van Thienen, P., Rozos, E., and Medema, G. (2018). "A resilience assessment method for urban water systems." *Urban Water Journal*, Taylor & Francis, 15(4), 316–328.

Makropoulos, C., Moraitis, G., Nikolopoulos, D., Karavokiros, G., Lykou, A., Tsoukalas, I., Morley, M., Gama, M.C., Okstad, E., and Vatn, J. (2019). "Risk Analysis and Evaluation Toolkit." Deliverable of STOP-IT Project D4.2.

Medema, G., and Makropoulos, C. (2019a). "Tackling the 'New Normal': A Resilience Assessment Method Applied to Real-World Urban Water Systems." *Water*, 11(2), 330.

Morley, M. S., and Tricarico, C. (2008). "Pressure-Driven Demand Extension for EPANET (EPANETpdd)." Technical Report No. 2008/02, Centre for Water Systems, University of Exeter.

Mälzer, H-J., Vollmer, F., and Corchero, A. (2019). "Risk Reduction Measures Database (RRMD)." Deliverable of STOP-IT Project D4.3 – Supporting Document.

Nicholson, A., Webber, S., Dyer, S., Patel, T., and Janicke, H. (2012). "SCADA security in the light of cyber-warfare." *Computers and Security*, Elsevier Ltd, 31(4), 418–436.

Nikolopoulos, D., Makropoulos, C., Kalogeras, D., Monokrousou, K., and Tsoukalas, I. (2018). "Developing a Stress-Testing Platform for Cyber-Physical Water Infrastructure." 2018 International Workshop on Cyber-physical Systems for Smart Water Networks (CySWater), IEEE, 9–11.

Nikolopoulos, D., Moraitis, G., Bouziotas, D., Lykou, A., Karavokiros, G., and Makropoulos, C. (n.d.). "Cyber-Physical Stress-Testing Platform for Water Distribution Networks." *Journal of Environmental Engineering: Special Collection on "Physical and Cyber Safety in Critical Water Infrastructure"* (under review).

Nikolopoulos, D., Moraitis, G., Bouziotas, D., Lykou, A., Karavokiros, G., and Makropoulos, C. (2019b). "RISKNOUGHT: A Cyber-Physical Stress-Testing Platform for Water Distribution Networks." 11th World Congress on Water Resources and Environment (EWRA 2019)



“Managing Water Resources for a Sustainable Future,” Madrid, Spain.

Nikolopoulos, D., van Alphen, H.-J., Vries, D., Palmen, L., Koop, S., van Thienen, P.,

NS-3 Consortium. (2019). “NS-3 network simulator.” NSAM, <<https://www.nsnam.org/>> (Aug. 5, 2019).

Oman, P., and Phillips, M. (2007). “Intrusion detection and event monitoring in SCADA networks.” IFIP International Federation for Information Processing, 253, 161–173.

Ostfeld, A., Salomons, E., Ormsbee, L., Uber, J. G., Bros, C. M., Kalungi, P., Burd, R., Zazula-Coetzee, B., Belrain, T., Kang, D., Lansey, K., Shen, H., McBean, E., Yi Wu, Z., Walski, T., Alvisi, S., Franchini, M., Johnson, J. P., Ghimire, S. R., Barkdoll, B. D., Koppel, T., Vassiljev, A., Kim, J. H., Chung, G., Yoo, D. G., Diao, K., Zhou, Y., Li, J., Liu, Z., Chang, K., Gao, J., Qu, S., Yuan, Y., Prasad, T. D., Laucelli, D., Vamvakeridou Lyroudia, L. S., Kapelan, Z., Savic, D., Berardi, L., Barbaro, G., Giustolisi, O., Asadzadeh, M., Tolson, B. A., and McKillop, R. (2012). “Battle of the Water Calibration Networks.” *Journal of Water Resources Planning and Management*, 138(5), 523–532.

Pallottino, S., Sechi, G. M., and Zuddas, P. (2005). “A DSS for water resources management under uncertainty by scenario analysis.” *Environmental Modelling and Software*, 20(8), 1031–1042.

Pawson, R., Wong, G., and Owen, L. (2011). “Known knowns, known unknowns, unknown unknowns: The predicament of evidence-based policy.” *American Journal of Evaluation*, 32(4), 518–546.

Piedrahita, A. F. M., Gaur, V., Giraldo, J., Cardenas, A. A., and Rueda, S. J. (2017). “Leveraging Software-Defined Networking for Incident Response in Industrial Control Systems.” *IEEE Software*, 35(1), 44–50.

Queiroz, C., Mahmood, A., Hu, J., Tari, Z., and Yu, X. (2009). “Building a SCADA security testbed.” *NSS 2009 - Network and System Security, IEEE*, 357–364.

Rasekh, A., Hassanzadeh, A., Mulchandani, S., Modi, S., and Banks, M. K. (2016). “Smart Water Networks and Cyber Security.” *Journal of Water Resources Planning and Management*, 142(7), 01816004.

Resilience Engineering Association – REA (2017). “Provisional Program 7<sup>th</sup> REA Symposium 26<sup>th</sup>-29<sup>th</sup> June 2017.” Retrieved from <http://www.rea-symposium.org/wp-content/uploads/2017/06/REASYM-2017-Provisional-Program-v22061407.pdf>.

Rockafellar, R. T., and Wets, R. J.-B. (1991). “Scenarios and Policy Aggregation in Optimization Under Uncertainty.” *Mathematics of Operations Research*, 16(1), 119–147.

Rockstrom, J., Falkenmark, M., Folke, C., Lannerstad, M., Barron, J., Enfors, E., Gordon, L., Heinke, J., Hoff, H., and Pahl-Wostl, C. (2014). *Water Resilience for Human Prosperity*. Cambridge University Press, Cambridge.

Rossman, L. a. (2000). “EPANET Programmer’s Toolkit.” 1–74.





- Ruszczynski, A. (1997). "Decomposition methods in stochastic programming." *Mathematical Programming, Series B*, 79(1–3), 333–353.
- Salomons, E., Hatchett, S., and Eliades, D. G. (2018). "The epanet open source initiative." *M*(June 2000), 0–7.
- Shang, F., Uber, J. A., and Rossman, L. (2008). *EPANET Multi-Species Extension User's Manual*. United States Environmental Protection Agency, Cincinnati, Ohio.
- Siaterlis, C., Genge, B., and Hohenadel, M. (2013). "EPIC: A testbed for scientifically rigorous cyber-physical security experimentation." *IEEE Transactions on Emerging Topics in Computing*, 1(2), 319–330.
- SINTEF (2019). "TORC Saf€ra project website." <https://www.sintef.no/en/projects/torc-training-for-operational-resilience-capabilit/>.
- Taleb, N. N. (2007). *The Black Swan: The Impact of the Highly Improbable*. Random House, New York.
- Taormina, R., and Galelli, S. (2018). "Deep-Learning Approach to the Detection and Localization of Cyber-Physical Attacks on Water Distribution Systems." *Journal of Water Resources Planning and Management*, 144(10), 04018065.
- Taormina, R., Galelli, S., Douglas, H. C., Tippenhauer, N. O., Salomons, E., and Ostfeld, A. (2018). "Modeling Cyber-Physical Attacks on Water Networks with epanetCPA Overview of epanetCPA toolbox."
- Taormina, R., Galelli, S., Douglas, H. C., Tippenhauer, N. O., Salomons, E., and Ostfeld, A. (2019). "A toolbox for assessing the impacts of cyber-physical attacks on water distribution systems." *Environmental Modelling and Software*, Elsevier, 112(May 2018), 46–51.
- Taormina, R., Galelli, S., Tippenhauer, N. O., Salomons, E., and Ostfeld, A. (2017). "Characterizing Cyber-Physical Attacks on Water Distribution Systems." *Journal of Water Resources Planning and Management*, 143(5), 04017009.
- Todini, E. (2003). "A more realistic approach to the 'extended period simulation' of water distribution networks." *Advances in Water Supply Management*, Taylor & Francis.
- Varga, A., and Hornig, R. (2008). "AN OVERVIEW OF THE OMNeT++ SIMULATION ENVIRONMENT." *Proceedings of the First International ICST Conference on Simulation Tools and Techniques for Communications Networks and Systems*, ICST.
- Vreeburg, J. H. G., Blokker, E. J. M., Horst, P., and Van Dijk, J. C. (2009). "Velocity-based self-cleaning residential drinking water distribution systems." *Water Science and Technology: Water Supply*, 9(6), 635–641.
- Wagner, J. M., Shamir, U., and Marks, D. H. (1988). "Water Distribution Reliability: Simulation Methods." *Journal of Water Resources Planning and Management*, 114(3), 276–294.
- White, B., Lepreau, J., Stoller, L., Ricci, R., Guruprasad, S., Newbold, M., Hibler, M., Barb,



C., and Joglekar, A. (2004). "An integrated experimental environment for distributed systems and networks." *ACM SIGOPS Operating Systems Review*, 36(SI), 255.



## 5 ANNEX A: STP Interface

### 5.1 Simulation results

#### 5.1.1 Retrieve Simulation results

Simulation results for a specific scenario can be retrieved using the following GET request:

```
http://<RAET domain>/api/simulation?id=scenario_id
```

where `scenario_id` is the ID of the related scenario. The scenario must have been executed so that simulation results have been produced.

#### 5.1.2 API response

The response from a request for simulation results is normally a JSON object. In case of an error (e.g. invalid filter syntax or value) or if the scenario hasn't been executed yet, the response will be simple text explaining the issue. Table 5 describes the returned simulation results structure.

Table 6: Returned simulation results structure

Element	Description
KPI	Array of KPI resulted from the scenario simulation. Each array item consists of the following parameters:
Title	The title of the KPI
Overall	The overall value of the KPI as a real number
OverallPercent	Percentage value of the KPI, if applicable, otherwise <i>null</i>
Timeseries	The timeseries of the KPI as an array of (x,y) tuples, from which the overall value is calculated.
Unit	The unit of measurement for the parameter
Metadata	Array of metadata related with the simulation
ScenarioID	The ID of the scenario
Timestamp	The timestamp of the simulation in ISO 8601 format
InputFiles	An array of input file data, consisting of title, path and possibly notes for each one of the files.
OutputFiles	An array of output file data, consisting of title, path and possibly notes for each one of the files.
Parameters	An array of parameters used in the simulation, consisting of title, value and possibly notes for each one of the parameters.
User	Data related with the user executing the simulation
Computer	Data related with the machine in which the simulation took place
Tools	Array of tools that have been used for the simulation. Each item consists of strings representing tool name, version and notes.
ComputationTime	Elapsed time for the simulation and the unit of measurement.

The following is a sample of a simulation result in JSON format. It is a result from the aforementioned GET request from which the timeseries and the parameter arrays has been



deleted and replaced by dots. Paths and computer name are partially hashed in this document.

```
{
  "KPI":[
    {
      "Title":"Unmet demand",
      "Overall":2257.2000000000007,
      "OverallPercent":0.00014808472250540841,
      "Timeseries":[
        . . . . .
      ],
      "Units":"liters"
    },
    {
      "Title":"Nodes insufficiently supplied",
      "Overall":118,
      "OverallPercent":0.30412371134020616,
      "Timeseries":[
        . . . . .
      ],
      "Units":"Nodes"
    },
    {
      "Title":"Customers experiencing insufficient service",
      "Overall":27027.648,
      "OverallPercent":0.26979672961377466,
      "Timeseries":[
        . . . . .
      ],
      "Units":"Customers"
    },
    {
      "Title":"Customer minutes lost",
      "Overall":0,
      "OverallPercent":0,
      "Timeseries":[
        . . . . .
      ],
      "Units":"Hours with nodes off-service"
    },
    {
      "Title":"System service hours lost",
      "Overall":0,
      "OverallPercent":0,
      "Timeseries":[
        . . . . .
      ]
    }
  ],
  "Metadata":{
    "ScenarioID":125,
    "Timestamp":"20190620T114059",
    "InputFiles":[
      {
        "Title":"EPANET .inp file used",
        "Path":"#####\STOPIT\T4.2\FT_viewer\Stopit_SP\site_media\tool_1\s
cenarios\125\scen.inp",
        "Notes": "none"
      },
      {

```



```
    "Title": "Cybernetwork .cpa file used",
    "Path": "###\\STOPIT\\T4.2\\FT_viewer\\Stopit_SP\\site_media\\tool_1\\scenarios\\125\\scen.cpa",
    "Notes": "none"
  }
],
"OutputFiles": [
  {
    "Title": "Main scenario results file",
    "Path": "###\\STOPIT\\T4.2\\FT_viewer\\Stopit_SP\\site_media\\tool_1\\scenarios\\125\\scen_results.csv",
    "Notes": "none"
  },
  {
    "Title": "Original, no attack, base scenario used to export consequences",
    "Path": "###\\STOPIT\\T4.2\\FT_viewer\\Stopit_SP\\site_media\\tool_1\\scenarios\\23\\scen_reults.csv",
    "Notes": "none"
  }
],
"Parameters": [
  {
    "Title": "alterMethod",
    "Value": "constant",
    "Notes": "none"
  },
  . . . . .
],
"User": {
  "Title": "Calculated by",
  "Value": "quartz"
},
"Computer": {
  "Title": "Computer",
  "Value": "DESKTOP-###"
},
"Tools": [
  {
    "Name": "Epanet CPA",
    "Version": "none",
    "Notes": "none"
  },
  {
    "Name": "Matlab",
    "Version": "9.3.0.713579 (R2017b)",
    "Notes": "none"
  }
],
"ComputationTime": {
  "Units": "seconds",
  "Value": 44.540226215756761
}
}
}
```



## 5.2 Scenario data for EPANET CPA

This service returns scenario data which are useful for the simulation of the scenario with the EPANET CPA tool. It contains mainly information related with absolute paths of the scenario files. The request may have one of the following forms:

- 1) `http://<RAET domain>/api/EpanetCPA_scenario_data`  
or
- 2) `http://<RAET domain>/api/EpanetCPA_scenario_data?id=ID`

While in the 1<sup>st</sup> case RAET returns the data of the scenario which has been executed most recently and is still running, with the 2<sup>nd</sup> form Epanet CPA can retrieve the same data of the scenario with the given ID.

### 5.2.1 API response

The response to a request, as far as it is valid, comprises the following data:

Table 7: Returned scenario data for EPANET CPA

Element	Description
ScenarioPath	The absolute path of the scenario files folder
inpFileName	The name of the network file created for the scenario, followed by the INP File Extension
cpaFileName	The name of the cyberphysical file created for the scenario, followed by the CPA File Extension
BAUfile	The absolute path of the reference, no-attack, simulation results file

The following is a sample of a request response in JSON format.

```
{
  cpaFileName: "scen.cpa"
  inpFileName: "scen.inp"
  BAUfile:
"C:\\prg\\STOPIIT\\raet\\site_media\\tool_1\\scenarios\\23\\scen_reults.csv"
  ScenarioPath: "C:\\prg\\STOPIIT\\raet\\site_media\\tool_1\\scenarios\\86"
}
```

## 5.3 Notifications to RAET

A simulation tool may notify to RAET the end of a simulation with the following POST request:

```
http://<RAET domain>/api/simulation_response/<ID>/<code>
```

where ID is an integer value that equals with the unique identification number of the scenario and the code corresponds to the response of the simulation. The code may have the following value



Code	Description
200	OK (Standard response for successful requests)
500	Unsuccessful simulation

The POST request has the following parameter:

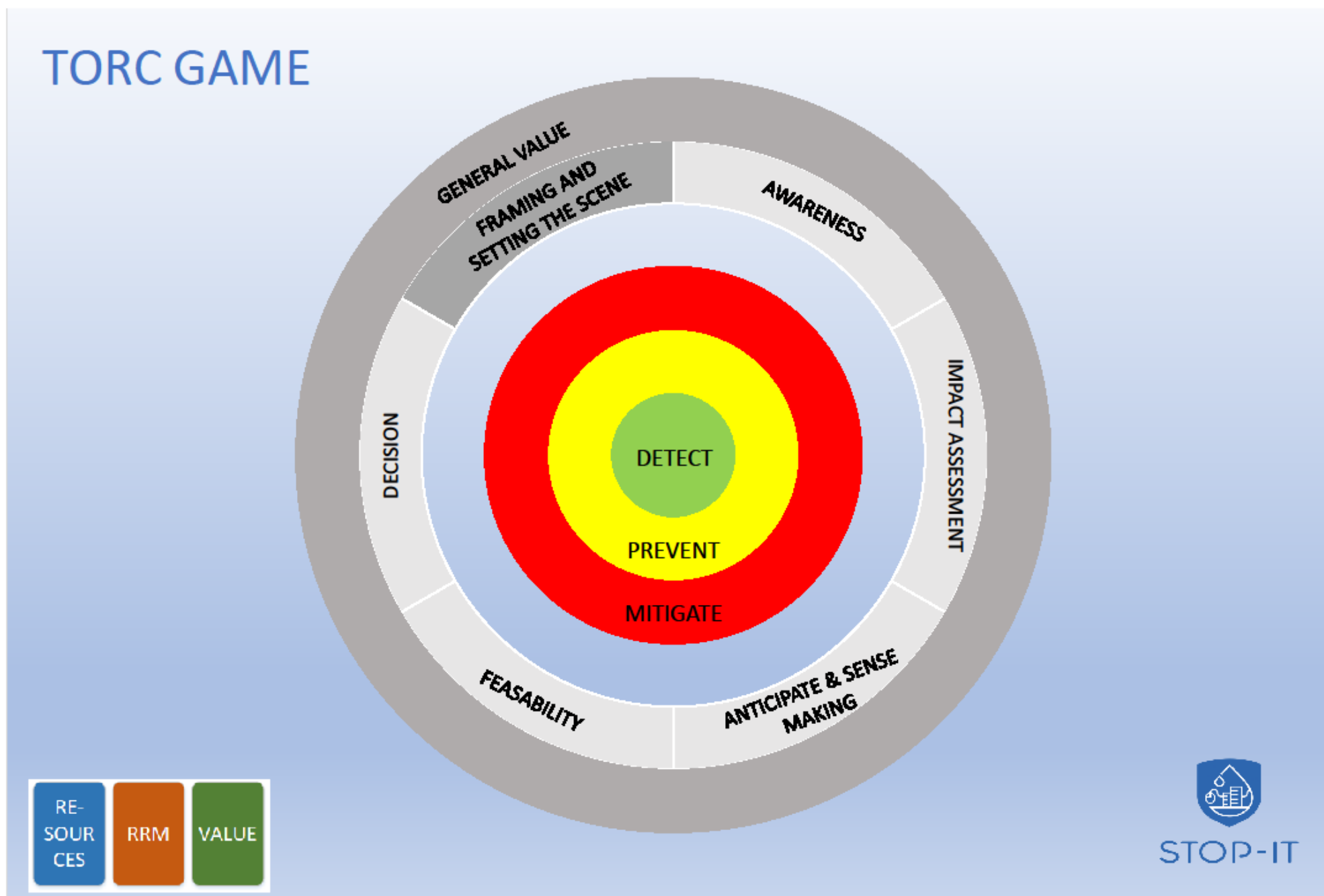
Parameter	Description
hash	A hash code that combines the ID of the scenario and a passphrase that is known to RAET and the simulation tool. It is used to validate the request of the remote system.

Upon receiving the request, RAET validates the request and sets the status of the scenario from “running” to “executed”. It then returns an HTTP 200 status code with no content. In case of an error, the following error messages may be returned:

Error code	Message
404	There is no scenario with ID: <ID>
403	Scenario with ID: <ID> is already in status “executed”
403	Permission denied for this operation

6 ANNEX B: The TORC inventory

6.1 TORC GAME BOARD







## 6.2 RESOURCE CARDS

1

### RESOURCES

Name	Asset Vulnerability Assessment Tool (AVAT)		
Corresponding module in STOP-IT	Module I	Reference	D4.1
Description	AVAT is a tool (available as desktop or online application) 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, the importance of the components for water supply and their "attractiveness" to be attacked. AVAT calculates system wide and element-specific indexes requiring limited data from users and provides fast initial assessment of vulnerable areas in the network and the criticality of assets.		
Required Inputs	A steady state hydraulic simulation EPANET (.inp file) and A data MS-Excel file, with a specific structure, containing default values of analysis, specific elements		
Type of results	Todini's Resilience Index Connectivity Index Node Reachability Index Link Criticality Index		



## 1

## RESOURCES

Name	Cyber Physical threats Stress Testing Platform (CPSTP)		
Corresponding module in STOP-IT	Module I	Reference	D4.4
Description	Cyber-physical threats Stress-Testing Platform (STP) is an EPANET based platform which provides a simulation environment for both physical and cyber sub-systems. The aim is to assess the behaviour of the cyber physical water system by deliberately stressing it under different attack scenarios, which can be developed through the Scenario Planner tool. STP will assess the system's response to a given attack and also allow the user to then simulate selected RRM (from RRMD) and assess their performance against attack scenarios using a set of KPIs.		
Required Inputs	Selected Tool, such as a Water Network Model based on EPANET Selected scenario from Scenario Planner		
Type of results	Stress-testing models produce simulation results files that contain detailed data on the system behaviour. The data are at the finest spatial and temporal scale, as the models register information for every node and link of the system in each timestep. The results include: Key Performance Indexes (KPI): KPIs aid the assessment of affected populations in terms of various matrices, such as loss of supplied water (customer minutes lost) or supply of sub-standard/polluted water and related health risks; disruption of service to critical customers (hospitals, schools, government, first responders); system survival time after an incident based on dynamic parameters such as water demand and incident response times, demonstrating the system's integrity.  Points/results of interest on the Water Network based on the analysis executed		



## 1

## RESOURCES

Name	Jammer Detector (JDet)		
Corresponding module in STOP-IT	Module II	Reference	D5.1
Description	JDet analyses the wireless spectrum range of several technologies (from WiFi to cellular) to detect different type of radio security threats, such as denial of service. It also allows to locate the identified threats geographically. In the TORC game it can be both proposed as a resource for detection to verify if Jamming is occurring and as a RRM for prevention		
Required inputs	Standalone module		
Type of results	Alert describing detected jamming models		



## 1

## RESOURCES

Name	Network Traffic Sensors and Analysers (NTSA)		
Corresponding module in STOP-IT	Module III	Reference	D5.4
Description	<p>NTSA analyses the Netflow traffic data generated by routing and switching devices to detect anomalous behaviour in the traffic. By analysing the network traffic, it is possible to identify the normal behaviour of the system e.g., by defining the number of packets transferred during a given period of time, the volume of packets sent and received, the IP sources/destinations used in the communications, the port sources/destinations required for communications, the protocols used, etc., therefore, everything that falls outside this will be considered as suspicious, and the tool will alert the systems accordingly.</p> <p>The tool addresses network anomalies e.g., high volume of traffic during a given period of time; communications coming from unknown or malicious IP sources; communications going to unknown or malicious IP destinations; suspicious ports/protocols connections; and other actions that could lead to attacks such as brute force, DoS, and botnets.</p> <p>In the TORC game it can be both proposed as a <u>resource</u> for detection to verify if anomalies are occurring and as a <u>RRM</u> for prevention</p>		
Required inputs	Netflow dataset about the network traffic to be used to train the model that will make predictions about the normal/abnormal behaviour of the system/network		
Type of results	The tool provides data and images of the region considered to capture the normal/legitimate traffic points as well as the points that fall out of the region (which are considered to be anomalous)		



## 1

## RESOURCES

Name	Real-time sensor data protection (RSDP)		
Corresponding module in STOP-IT	Module III	Reference	D5.4
Description	RSDP applies blockchain schemes to protect the integrity of all the data generated during a critical infrastructure operation (logs, sensor data, etc.), both against intentional attacks or malfunction. In the TORC game it can be both proposed as a resource for detection to verify if anomalies/malfunctions are occurring and as a RRM for prevention		
Required Inputs	Sensor data to be stored in the Cloud or in an alternative storage system and the identification of the device which generated that data.		
Type of results	A record of the generated data and the result of the data integrity test.		



## 1

## RESOURCES

Name	Optimization Tool for Sensor Placement and Management		
Corresponding module in STOP-IT	Module IV	Reference	D5.5
Description	<p>The tool allows to detect events of drinking water contamination and the source of intrusion based on flow and quality data from sensors. It is based on a optimization methodology for water quantity (hydraulic) and water quality sensor placement, a method for event detection of water quality intrusions, and a scheme for contamination source identification.</p> <p>The type of threat addressed is a contamination intrusion into a water distribution system. This intrusion can be a result of a terrorism action of deliberately injecting contaminants into the system or an occasional intrusion such as a pollutant entering a well.</p> <p>In the TORC game it can be both proposed as a <u>resource</u> for detection of the eventual source of contamination and as a <u>RRM</u> for prevention (by implementing the resulting optimal sensors placement strategy)</p>		
Required Inputs	Water distribution system modelled in EPANET Water quantity and water quality data collected by sensors according to specific requirements		
Type of results	Optimal placement of hydraulic and water quality sensors in water distribution systems Events detection utilizing water quantity and water quality data collected by the sensors Event detection module for estimating the most probable source intrusion locations, based on the water distribution system layout and information received from the water quantity and water quality sensors		



Empty template of Resource card made available to create new ones during the training session.

## 1 RESOURCES

Name
Corresponding module in STOP-IT
Description
Required inputs
Type of results



## 6.3 RISK REDUCTION CARDS

2

### Risk Reduction Measure

Type of threat: Physical



Measure ID: M01  
Name: FencesAndWalls

Scope of use: 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.

Type of asset			Event consequences			
Catchment Area		Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity	
Raw Water Bodies		Water Abstraction Points	Water Treatment Plants	Financial	Reputation	





2

## Risk Reduction Measure

Type of threat: Physical



Measure ID: M02  
Name: MotionDetectors

Scope of use: Implementation of motion detectors. Thus the intrusion of unauthorized personnel to sensitive sites is automatically detected. The aim is to be able to react quickly to occurring intrusions.

Comments: Different reactions are possible if a motion detector is triggered by an intruder. A silent alarm could be sent to the staff (thus the probability that the intruder is caught by the police could be increased) or a loud alarm sound could be started (this could lead to a flight of the intruder before he/she causes any more serious consequences).  
Example of solution provided by STOP-IT: Human Presence Detection using WiFi signals (HPD) (Module IV)

Type of asset				Event consequences	
		Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
			Water Treatment Plants	Financial	Reputation



2

## Risk Reduction Measure

Type of threat: Physical



Measure ID: M03  
Name: CameraSurveillance

Scope of use: Surveillance of sensitive sites, buildings or assets with camera systems. Thus intruders are detected by the staff that is surveilling the monitors. The aim is to be able to react quickly to occurring intrusions or intrusion attempts and to be able to identify the attacker after an occurring attack.

Comments: Example of solution provided by STOP-IT:  
Computer Vision Tools (CVT) (Module IV)

Type of asset		Event consequences	
		Drinking Water Tanks 	Pressure Boosting Station 
		Water Abstraction Points 	Water Treatment Plants 
		Quality 	Quantity 
		Financial 	Reputation 



2

## Risk Reduction Measure

Type of threat: Physical



Measure ID

M04

Name

Patrols

Scope of use

Organization of regular or irregular patrols at sensitive sites, buildings and assets. Thus intruders shall be noticed and the investigated sites, buildings and assets are checked for any obvious damages or similar. The aim is to prevent malicious attacks and to ensure the functionality of the water supply system.

Comments

A positive side-effect of patrols might be the deterrent effect on potential attackers decreasing the likelihood of malicious attacks.

Type of asset				Event consequences	
Catchment Area		Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
Raw Water Bodies	Raw Water Pipeline	Water Abstraction Points	Water Treatment Plants	Financial	Reputation



2

## Risk Reduction Measure

Type of threat: Physical



Measure ID: M05  
Name: FloodProtection

Scope of use: Implementation of flood protection measures. By the building of dams or object protection measures against floods the intrusion of flood water to sensitive sites shall be prevented. The aim is to prevent any assets or buildings from being damaged by flood water and to ensure an ongoing high water quality.

Comments: 0

Type of asset				Event consequences	
Catchment Area			Pressure Boosting Station	Quality	Quantity
	<input type="checkbox"/>	<input type="checkbox"/>			
Raw Water Bodies		Water Abstraction Points	Water Treatment Plants	Financial	
	<input type="checkbox"/>				<input type="checkbox"/>



2

## Risk Reduction Measure

Type of threat: Physical



Measure ID: M06  
Name: BarredWindows

Scope of use: Protection of windows with bars. Thus intruders cannot enter a building by destroying a window. The aim is to ensure that only authorized personnel can enter sensitive objects or sites.

Comments: It might be sufficient to implement bars at windows below the second floor as the height of all other windows could be a sufficient physical barrier.

Type of asset			Pressure Boosting Station	Event consequences	
				Quality	Quantity
			Water Treatment Plants	Financial	Reputation



2

## Risk Reduction Measure

Type of threat: Physical



Measure ID: M07  
Name: BinaryContacts

Scope of use: Implementation of binary contacts as alarm system at doors, windows or storage tanks. Thus the intrusion of unauthorized personnel to sensitive site is automatically detected. The aim is to be able to react quickly to occurring intrusions.

Comments: Different reactions are possible if a binary contact is triggered by an intruder. A silent alarm could be sent to the staff (thus the probability that the intruder is caught by the police could be increased) or a loud alarm sound could be started (this could lead to a flight of the intruder before he/she causes any more serious consequences).

Type of asset				Event consequences	
		Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
			Water Treatment Plants	Financial	



2

## Risk Reduction Measure

Type of threat: Physical



Measure ID: M08  
Name: SecureDoorsAndWindows

Scope of use: Construction of doors and windows with a sufficient resistance class. Thus the time and effort that an attacker needs to overcome the respective barrier is increased. The aim is to gain more time to detect an attack and to react on the attack, furthermore the attractiveness for an attack is reduced.

Comments: An appropriate resistance class for doors and windows of specific buildings depends on the security zone that the building is assigned to.

Type of asset				Event consequences	
		Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
			Water Treatment Plants	Financial	Reputation



2

## Risk Reduction Measure

Type of threat: Physical



Measure ID: M09  
Name: EntranceAccessControl

Scope of use: Implementation of an access control system for entrances to sensitive sites. Thus it shall be avoided that unauthorized people get access to the sensitive sites. The aim is to protect the infrastructures of the water utility from damages.

Comments: The physical access control can be implemented in different forms. The most common way of access control is the distribution of keys or access cards for sensitive sites only to authorized personnel. Another way of access control would be the implementation of regularly changing codes that are necessary to open doors. Also the access permission via biometric data like fingerprints is possible. In case of biometric entrance systems special attention has to be paid to data protection issues. Access control can also be realized by personnel that is positioned at entrances to check access permissions manually. The principle of minimum access permissions should be applied, that means that as few access authorizations as possible should be distributed. Example of solution made available by STOP-IT: The Fine-grained Cyber Access Control tool (FCAC) (Module IV)

Type of asset				Event consequences	
		Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
			Water Treatment Plants	Financial	Reputation





2

## Risk Reduction Measure

Type of threat: Physical



Measure ID: M10  
Name: SecureLocks

Scope of use: Installation of secure locks. Thus the picking of locks is substantially complicated. The aim is to prevent that attackers can easily enter sensitive sites by picking locks.

Comments: Example of solution provided by STOP-IT: Smart-Locks - access control systems based on intelligent electronic locks, and dedicated applications to service employees and to central management system.

(Module IV)

Type of asset		Event consequences	
		Drinking Water Tanks 	Pressure Boosting Station 
		Water Abstraction Points 	Water Treatment Plants 
		Quality 	Quantity 
		Financial 	Reputation 



2

## Risk Reduction Measure

Type of threat: Physical



Measure ID: M11  
Name: DiscreetAppearance

Scope of use: If possible, sensitive sites and buildings should be designed in a discreet appearance. Thus it shall be avoided that the sites or areas raise awareness of potential attackers. The aim is to lower the probability of attacks.

Comments: An example for a discreet design could be pumping stations. The building in which the pumps are located should not directly indicate that this is a pumping station for drinking water so that potential attackers are directly aware of a potential attack point. Also areas on a water utility's properties where for example servers or the control center are located should not be directly recognisable. This would quickly indicate an attractive attack point for a potential intruder.

Type of asset		Event consequences	
		Drinking Water Tanks 	Pressure Boosting Station 
		Water Abstraction Points 	Water Treatment Plants 
		Quality 	Quantity 
		Financial 	



2

## Risk Reduction Measure

Type of threat: Physical



Measure ID: M12  
Name: SupervisionOfExternals

Scope of use: Supervision of any external people entering the water utility or sensitive sites. Any people who enter sites and who are not part of the utility's staff are supervised and not left alone at any time. Thus any data thefts, manipulations or similar shall be prevented.

Comments: 0

Type of asset				Event consequences			
		Drinking Water Tanks 	Pressure Boosting Station 	Quality 	Quantity 		
		Water Abstraction Points 	Water Treatment Plants 	Financial 	Reputation 		



2

## Risk Reduction Measure

Type of threat: Physical



Measure ID M13  
Name SmokeDetectors

Scope of use Installation of smoke detectors. Thus fires are immediately noticed by the present staff. The aim is to protect all employees and infrastructures from serious injuries or damages caused by fire.

Comments 0

Type of asset				Event consequences	
		Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
			Water Treatment Plants	Financial	



2

## Risk Reduction Measure

Type of threat: Physical



Measure ID: M14  
Name: ContainmentStructures

Scope of use: Construction of containment structures at sensitive locations like roads or airports. Thus raw water contaminations due to traffic accidents, leakages or similar are kept away from raw water sources for drinking water production. The aim is to ensure the constant and sufficient availability of raw water of a sufficient quality for drinking water production.

Comments: 0

Type of asset				Event consequences		
Catchment Area		<input type="checkbox"/>	<input type="checkbox"/>	Quality		<input type="checkbox"/>
Raw Water Bodies		<input type="checkbox"/>	<input type="checkbox"/>	Financial		<input type="checkbox"/>



2

## Risk Reduction Measure

Type of threat: Physical



Measure ID: M15  
Name: RawWaterPipelineProtection

Scope of use: Physical protection of raw water transmission pipeline and equipment (pumps, valves,...). The aim is to protect the water transmission pipes against corrosion, intrusion, failure, etc.

Comments: This measure includes for example regular inspections of the raw water pipelines.

Type of asset				Event consequences	
				Quality	Quantity
Raw Water Pipeline		Water Abstraction Points		Financial	Reputation



2

## Risk Reduction Measure

Type of threat: Physical



Measure ID: M16  
Name: SourceWaterQualityControl

Scope of use: Control of raw water quality. The aim is to control the raw water quality in order to select the best treatment process and operation.

Comments: 0

Type of asset				Event consequences		
Catchment Area		<input type="text"/>	<input type="text"/>	Quality		<input type="text"/>
Raw Water Bodies		<input type="text"/>	<input type="text"/>			<input type="text"/>
			Water Treatment Plants			<input type="text"/>



2

## Risk Reduction Measure







Type of threat: Physical



Measure ID: M17  
Name: WatershedProtection

Scope of use: Pollution sources in the watershed may affect raw water quality. The aim is to control the activities within the watershed affecting raw water quality.

Comments: One of the objectives of the Water framework directive is to protect the drinking water sources. Part of this measures could be inspections of the watersheds and regulations of human activities in the watershed (especially regulations of traffic, industry, agriculture, residential areas).

Type of asset			Event consequences				
Catchment Area		<input type="text"/>	<input type="text"/>	Quality		<input type="text"/>	
Raw Water Bodies		<input type="text"/>	Water Abstraction Points		Financial		<input type="text"/>
			Water Treatment Plants				





2

## Risk Reduction Measure

Type of threat: Physical



Measure ID: M18  
Name: InflowAndBackflowPrevention

Scope of use: Implementation of inflow and backflow prevention devices at relevant points of the network (e.g. house connections, fire hydrants). Thus the contamination of the drinking water network via these sources is prevented. The aim is to prevent intentional and unintentional contaminations so that a high water quality is ensured.

Comments: 0

Type of asset				Event consequences	
Drinking Water Network				Quality	
				Financial	Reputation



2

## Risk Reduction Measure

Type of threat: Physical



Measure ID: M19  
Name: FiltersInAerationProcesses

Scope of use: All air for aeration purposes in water treatment plants and water storage tanks should be filtered. Thus it is aimed to prevent contaminations induced by entering air by the provision of physical barriers. The aim is to ensure an ongoing high quality of the supplied water.

Comments: Filters should be installed at every air intake for aeration purposes. Furthermore, no openings for aeration purposes should be built directly over the water surface to prevent that attackers can easily induce dangerous substances or that dangerous substances are induced in a natural way.

Type of asset				Event consequences	
		Drinking Water Tanks 		Quality 	
			Water Treatment Plants 	Financial 	Reputation 



2

## Risk Reduction Measure

Type of threat: Cyber



Measure ID: M20  
Name: PressureAndFlowSensors

Scope of use: Installation of pressure and flow sensors at different positions in the water distribution network. Thus it can be checked if the network is operated in the desired conditions. The aim is to ensure a water supply in sufficient quantity and pressure.

Comments: With this measure failures in the distribution network due to intended attacks like destructions of pumps or pipes might be detected. Furthermore, also failures due to naturally occurring damages like pipe breakages are detected (induced by natural phenomena or by wrong operation/human fault).  
Example of solution provided by STOP-IT: Optimization Tool for Sensor Placement and Management and Real-time sensor data protection (RSDP) (Module III)

Type of asset				Event consequences	
	Drinking Water Network		Drinking Water Tanks		Quantity
	Raw Water Pipeline		Water Abstraction Points		Financial
					Reputation



2

## Risk Reduction Measure

Type of threat: Physical



Measure ID: M21  
Name: OscillationSensors

Scope of use: Installation of oscillation sensors at pumps. Thus any imminent damages of the pump or manipulations of the pump operation or settings are detected by changed oscillation patterns. The aim is to ensure an ongoing proper pump functionality and to detect any manipulations.

Comments: This measure might indicate imminent pump failures due to wear or intended pump manipulations which are not detected in another way because the signal of the pump status to the control center was manipulated to show the desired values.

Type of asset				Event consequences	
			Pressure Boosting Station 		Quantity 
				Financial 	



2

## Risk Reduction Measure

Type of threat: Physical



Measure ID: M22  
Name: ValvePositionSensors

Scope of use: Installation of sensors indicating the position of valves. Thus it can be checked if all valves are in the position that they are obliged to. The aim is to check if the operating parameters are performed as they should or if any malfunctions or manipulations of the valves exist.

Comments: 0

Type of asset				Event consequences	
<input type="checkbox"/>	Drinking Water Network 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Quantity 
<input type="checkbox"/>	Raw Water Pipeline 	<input type="checkbox"/>	Water Treatment Plants 	Financial 	<input type="checkbox"/>



2

## Risk Reduction Measure

Type of threat: Physical



Measure ID: M23  
Name: LevelSensors

Scope of use: Installation of sensors indicating the filling level of storage tanks or additive reservoirs. Thus it can be supervised if any storage tanks or reservoirs are running dry or overflow. The aim is to ensure a desired filling level in all reservoirs and storage tanks.

Comments: 0

Type of asset				Event consequences	
		Drinking Water Tanks 		Quantity 	
			Water Treatment Plants 	Financial 	



## Risk Reduction Measure

Type of threat: Physical



Measure ID: M24  
Name: AutomatedValveControl

Scope of use: Automated control of valves to regulate required pressures and flows. Thus human errors e.g. leading to pressure shocks are avoided. The aim is to ensure ongoing desired conditions in the network and to protect the infrastructure from damages.

Comments: Although the control of valves is automated, the possibility of a manual control should be given at every point of time.

Type of asset				Event consequences	
	Drinking Water Network			Quantity	
	Raw Water Pipeline			Financial	



2

## Risk Reduction Measure

Type of threat: Cyber-Physical



Measure ID: M25  
Name: OperatingParameterSurveillance

Scope of use: Surveillance of operating parameters from the catchment to the final distribution point. Thus any damages, malfunctions or manipulations in the supply chain are directly detected. The aim is to enable fast reactions to damages, malfunctions or manipulations.

Comments: Potential parameters to be supervised are volume flows and pressures of water at different positions in the system, pressure losses (e.g. at filters), membrane permeabilities or volume flows and pressures of air at aerations. The surveillance can be realized manually or automatically by the definition of certain allowed operating ranges.

Type of asset				Event consequences	
	Drinking Water Network	Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
	Raw Water Pipeline	Water Abstraction Points	Water Treatment Plants	Financial	Reputation





2

## Risk Reduction Measure

Type of threat: Cyber



Measure ID

M26

Name

ProcedureForPersonnelChanges

Scope of use

Following of a structured procedure in case of new employees entering the company or employees leaving the company. Thus new employees directly learn about all important information security issues and leaving employees are informed about their duty of confidentiality. By this measure, data losses due to leaving employees and faults due to unawareness of new employees shall be prevented.

Comments

For new employees checklists should be used to ensure that no important issues about information security are forgotten. If possible, the leaving employee should train the new employee. All access rights have to be taken from the leaving employee.

Type of asset				Event consequences	
	Drinking Water Network	Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
	Raw Water Pipeline	Water Abstraction Points	Water Treatment Plants	Financial	Reputation



## Risk Reduction Measure

Type of threat: Cyber-Physical



Measure ID: M27  
Name: Employees Trainings

Scope of use: Regular trainings, seminars, updates and informations on security issues should be implemented for all employees. Thus the staff is always kept up to date about any security relevant developments, behavioural rules and acute risks, both in the cyber and in the physical sector. The aim is to prevent hazards occurring due to unawareness and human faults.

Comments: 0

Type of asset				Event consequences	
Catchment Area	Drinking Water Network	Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
Raw Water Bodies	Raw Water Pipeline	Water Abstraction Points	Water Treatment Plants	Financial	Reputation



## Risk Reduction Measure

Type of threat: Cyber-Physical



Measure ID: M28  
Name: SecurityCheckOfEmployees

Scope of use: Security check of new employees. By checking relevant data of new employees like the completeness of the CV and the criminal record, the confidentiality and reliability of the potential employee is checked. The aim is to employ trustworthy and reliable employees to ensure a safe operation.

Comments: The possibilities for security checks are significantly limited by different laws and regulations in the field of data protection. Therefore it has to be ensured that all information gaining processes are lying in the frame of legally allowed and ethically justifiable investigations.

Type of asset				Event consequences	
Catchment Area	Drinking Water Network	Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
Raw Water Bodies	Raw Water Pipeline	Water Abstraction Points	Water Treatment Plants	Financial	Reputation



2

## Risk Reduction Measure

Type of threat: Cyber-Physical



Measure ID: M29  
Name: EmergencyPlans

Scope of use: Setting up of emergency plans. Thus clear responsibilities, courses of action, procedures and contacts are defined and documented for emergency cases. The aim is to reduce the consequences after serious cyber, physical or cyber-physical incidents.

Comments: A complete crisis plan should exist including responsibilities, pending tasks, important contacts etc. All tasks from the evaluation of the situation over the determination of appropriate reactions to the crisis until the final realization of the actions and their effectiveness check have to be defined. Therefore also an emergency service must exist.

Type of asset				Event consequences	
Catchment Area	Drinking Water Network	Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
Raw Water Bodies	Raw Water Pipeline	Water Abstraction Points	Water Treatment Plants	Financial	Reputation



2

## Risk Reduction Measure

Type of threat: Cyber-Physical



Measure ID: M30  
Name: RedundantAssetsAndInfrastructures

Scope of use: Constructions of redundant infrastructures and assets along the whole water supply chain. Thus the failure of one component can, at least partially, be compensated by the respective redundant asset. The aim is to ensure a constant supply of water with adequate quantity, quality and pressure.

Comments: Redundant infrastructures could exist in the water extraction (wells, river extractions, reservoir extractions, spring water), water treatment infrastructures (filtration, adsorption, aeration, sedimentation, softening), water storage (tanks), water distribution (main pipes, distribution pipes, pressure boosting station) or similar infrastructures. Another kind of redundancy implementation that might make sense is the cooperation with other suppliers e.g. with neighbouring municipalities in supply networks.

Type of asset				Event consequences	
Catchment Area	Drinking Water Network	Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
Raw Water Bodies	Raw Water Pipeline	Water Abstraction Points	Water Treatment Plants	Financial	Reputation



2

## Risk Reduction Measure

Type of threat: Cyber-Physical



Measure ID: M31  
Name: DistributedEnergySupply

Scope of use: Supply of energy from more than one supplier. Thus a potential supply failure of one electrical energy supplier can quickly be replaced by the supply of the redundant supplier. The aim is to prevent downtimes due to a lack of electrical energy.

Comments: 0

Type of asset				Event consequences	
	Drinking Water Network	Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
		Water Abstraction Points	Water Treatment Plants	Financial	Reputation



2

## Risk Reduction Measure

Type of threat: Physical



Measure ID: M32  
Name: EmergencyGenerators

Scope of use: Installation of emergency generators. Thus a complete failure of external energy supply can be compensated by the emergency generators. The aim is to prevent downtimes due to a lack of electrical energy.

Comments: 0

Type of asset				Event consequences	
	Drinking Water Network	Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
		Water Abstraction Points	Water Treatment Plants	Financial	Reputation



2

## Risk Reduction Measure

Type of threat: Physical



Measure ID: M33  
Name: AdditionalStorageCapacity

Scope of use: Construction of additional storage tanks. Thus periods of water scarcity can be bridged easier due to a higher amount of stored water. The aim is to ensure a constant supply with drinking water also in times of reduced raw water availability or attacks on water treatment or supply elements.

Comments: 0

Type of asset				Event consequences	
Catchment Area	Drinking Water Network	Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
Raw Water Bodies	Raw Water Pipeline	Water Abstraction Points	Water Treatment Plants	Financial	Reputation





## Risk Reduction Measure

Type of threat: Physical



Measure ID: M34  
Name: WaterIntakeAdaption

Scope of use: Re-designing of water intakes for periods of raw water scarcities. Thus the usual sources for raw water can also be used in case of low water levels e.g. by the construction of pumps, modified water intakes or additional wells. The aim is to ensure a constant supply with raw water.

Comments: 0

Type of asset			Event consequences	
Catchment Area				Quantity
	<input type="text"/>	<input type="text"/>	<input type="text"/>	
Raw Water Bodies		Water Abstraction Points		Financial
	<input type="text"/>		<input type="text"/>	



## Risk Reduction Measure

Type of threat: Physical



Measure ID: M35  
Name: WaterQualityOnlineSurveillance

Scope of use: Surveillance of the water composition along the supply chain by online sensors. Thus degradations of water quality (from raw water to the point of supply) are early detected. The aim is to enable fast reactions and the potential isolation of affected network parts or infrastructures.

Comments: The quality should be checked with respect to chemical, microbiological and physical parameters. Potential parameters can for example be taken from existing laws or guidelines defining the required drinking water quality, examples are temperatures, pH values, conductivities, oxygen concentrations, turbidities, UV absorption or redox potential.

Type of asset				Event consequences	
Catchment Area	Drinking Water Network	Drinking Water Tanks	.	Quality	.
Raw Water Bodies	.	Water Abstraction Points	Water Treatment Plants	Financial	Reputation



## Risk Reduction Measure

Type of threat: Physical



Measure ID: M36  
Name: WaterTreatmentControl

Scope of use: Implementation of monitoring, treatment and disinfection processes in order to comply with the water quality standards under all circumstances.

Comments: This is a measure for process control & optimization.

Type of asset				Event consequences	
Catchment Area				Quality	Quantity
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
Raw Water Bodies		Water Abstraction Points	Water Treatment Plants	Financial	Reputation
	<input type="checkbox"/>				



2

## Risk Reduction Measure

Type of threat: Cyber-Physical



Measure ID: M37  
Name: WaterQualityOfflineSurveillance

Scope of use: Offline monitoring of water quality parameters in the distribution systems to comply with the water quality standards under all circumstances.

Comments: 0

Type of asset				Event consequences	
	Drinking Water Network	Drinking Water Tanks		Quality	Quantity
<input type="checkbox"/>			<input type="checkbox"/>		
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Financial	Reputation



2

## Risk Reduction Measure

Type of threat: Physical



Measure ID M38  
Name MonitoringAndControlOfDistributionSystem

Scope of use Monitoring and controlling the distribution system for biofilms, deposits and corrosion.

Comments 0

Type of asset				Event consequences	
Drinking Water Network		Drinking Water Tanks		Quality	Quantity
			Water Treatment Plants	Financial	



2

## Risk Reduction Measure

Type of threat: Physical



Measure ID: M39  
Name: WaterNetworkInterventionsForWaterSupplyRecovery

Scope of use: There are many events that potentially may lead to anomalies affecting the physical elements of the water network (i.e. pipe breakdown). When this occurs, a segment of the network containing the faulty element is isolated for its repair. This isolation may affect the supply of certain demand nodes in terms of quantity and pressure. Then, a set of network interventions must be enabled in order to recover the water supply service in the affected area during this emergency period. In general, this interventions aims to enable new water pathways to the affected area and/or adapting PRVs and pumping strategies to recover pressure assuring enough autonomy in the water tanks.

Comments: 0

Type of asset				Event consequences	
	Drinking Water Network	Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
					Reputation 



## Risk Reduction Measure

Type of threat: Physical



Measure ID

M40

Name

AdditivesQualityCheck

Scope of use

Supervision of quality of delivered additives. Thus the use of additives produced with substandard quality or the use of subsequently (intentionally or unintentionally) polluted additives is prevented. The aim is to prevent the pollution of drinking water caused by the use of polluted additives.

Comments

0

Type of asset				Event consequences	
				Quality 	
			Water Treatment Plants 	Financial 	Reputation 



2

## Risk Reduction Measure

Type of threat: Cyber-Physical



Measure ID: M41  
Name: InfrastructureAndAssetInspections

Scope of use: Regular and/or continuous inspections of existing infrastructure and assets by trained and professional personnel. Thus existing or impending damages, failures or manipulations are early detected. The aim is to undo damages, failures or manipulations to prevent more serious consequences on existing infrastructures.

Comments: The inspections shall detect intended manipulations of the assets and infrastructure by attackers as well as existing and imminent damages or failures due to wrong operation or wear.

Type of asset				Event consequences	
	Drinking Water Network	Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
	Raw Water Pipeline	Water Abstraction Points	Water Treatment Plants	Financial	Reputation





2

## Risk Reduction Measure

Type of threat: Cyber-Physical



Measure ID: M42  
Name: InformationSecurityGuidelines

Scope of use: Establishment of a guideline for information security. This guideline contains all relevant aspects about the company's information security aims and underlying processes. Thus the employees are aware of the importance of information security procedures and know how to behave to ensure information security.

Comments: The guideline(s) should contain information about the importance of information security, the security objectives, the most important aspects of the security strategy as well as the organisational structure established for information security. A clear scope must be defined. All employees must be informed about the guideline on information security. The guideline should regularly be updated.

Type of asset				Event consequences	
	Drinking Water Network	Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
	Raw Water Pipeline	Water Abstraction Points	Water Treatment Plants	Financial	Reputation



2

## Risk Reduction Measure

Type of threat: Cyber-Physical



Measure ID: M43  
Name: InformationSecurityManagementSystem

Scope of use: Implementation of an Information Security Management System (ISMS). The ISMS enables the implementation and continuous application of a thought out and effective information security process. The aim is to provide a general concept for a continuously updated information security in a water utility.

Comments: An ISMS should be tailored to the existing management structures of the specific water utility. Due to different conditions existing in each site and utility, there cannot be one ISMS fitting as general system for all utilites. Thus there is a need of customization in each case.

Type of asset				Event consequences	
	Drinking Water Network	Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
	Raw Water Pipeline	Water Abstraction Points	Water Treatment Plants	Financial	Reputation



2

## Risk Reduction Measure

Type of threat: Cyber



Measure ID: M44  
Name: PasswordSecurity

Scope of use: Access to sensitive and critical cyber applications, databases, control tools or similar should be protected by secure passwords. Thus only authorized people get access to the respective cyber space. The aim is to prevent attacker's access by hacking and to ensure the cyber system's integrity.

Comments: For the access to any application, database or similar a different password has to be used. Passwords should not be too short (at least 8 symbols) and contain symbols of different kinds (e.g. capital and small letters, special symbols, numbers). Passwords should be changed regularly.

Type of asset				Event consequences	
	Drinking Water Network	Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
	Raw Water Pipeline	Water Abstraction Points	Water Treatment Plants	Financial	Reputation



2

## Risk Reduction Measure

Type of threat: Cyber



Measure ID

M45

Name

TwoFactorAuthentication

Scope of use

Implementation of two-factor authentication for especially sensitive applications. Thus the possibility of unauthorized access to sensitive applications is significantly reduced. The aim is to ensure a special protection for especially sensitive applications.

Comments

Possible realizations for a two-factor authentication could for example be individual codes that are sent via SMS or TAN generators.

Type of asset				Event consequences	
	Drinking Water Network	Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
	Raw Water Pipeline	Water Abstraction Points	Water Treatment Plants	Financial	Reputation



2

## Risk Reduction Measure

Type of threat: Cyber



Measure ID: M46  
Name: RestrictedAccesToITSystem

Scope of use: The company must to restrict the network control actions and information accessibility to particular actors inside the company using a particular protocol acces (double factor). A security level of accessibility should be defined according to the person or group in charge of specific tasks in the company.

Comments: 0

Type of asset				Event consequences	
	Drinking Water Network	Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
		Water Abstraction Points	Water Treatment Plants	Financial	Reputation



2

## Risk Reduction Measure

Type of threat: Cyber

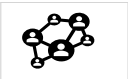








Measure ID M47

Name NonManipulationConnectionTool

Scope of use The company must forbid the network connection to not authorized mobile devices (PC, laptop, etc.).

Comments 0

Type of asset				Event consequences	
<input type="checkbox"/>	Drinking Water Network 	Drinking Water Tanks 	Pressure Boosting Station 	<input type="checkbox"/>	Quantity 
<input type="checkbox"/>	<input type="checkbox"/>	Water Abstraction Points 	Water Treatment Plants 	<input type="checkbox"/>	Reputation 



2

## Risk Reduction Measure

Type of threat: Cyber-Physical



Measure ID: M48  
Name: CryptographicProcesses

Scope of use: Implementation of cryptographic processes. Thus any relevant data is encrypted and therefore unreadable for an attacker. The aim is to ensure that any attacker getting access to sensitive data cannot read the data due to its encryption.

Comments: Additionally to the data encryption, the possibility of encrypting also communication connections should be checked in dependence on the necessary effort for encryption and its practicability. The source and integrity of used cryptographic keys should also be checked. The keys should be changed in a sufficient frequency. Encryptions can be realized for transferred data (wireless connections, wires, mobile storage devices) and for data stored on servers, clients, mobile devices or similar.

Type of asset				Event consequences	
	Drinking Water Network	Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
	Raw Water Pipeline	Water Abstraction Points	Water Treatment Plants	Financial	Reputation



2

## Risk Reduction Measure

Type of threat: Cyber-Physical



Measure ID: M49  
Name: DataBackups

Scope of use: All relevant data should be saved in a data backup regularly. Due to redundant data storages the loss of one data set can be compensated by using the backup data. Thus the ongoing operability of the utility is ensured.

Comments: All relevant factors of influence on the process of data backup generation must be documented, e.g. the amount and time of changed data, availability requirements or similar. If applied, the requirements for online data backups, e.g. in clouds, must be determined (e.g. location of storage, methods of authentication, etc.). The backup data should be encrypted, furthermore the location of the backup data should not be the same as the location of the original data.

Type of asset				Event consequences	
	Drinking Water Network	Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
	Raw Water Pipeline	Water Abstraction Points	Water Treatment Plants	Financial	Reputation





2

## Risk Reduction Measure

Type of threat: Cyber-Physical



Measure ID: M50  
Name: NetworkSeparation

Scope of use: Secure installation and operation of different network security zones. Thus unauthorized entries into sensitive networks can be complicated. The aim is to ensure the integrity, authenticity and confidentiality of all data in the network.

Comments: This measure is dealing with the IT networks. The complete network setup, structure, changes or similar must be documented in detail. The network must be separated into different security zones (e.g. internal network, demilitarized zone [DMZ], external connections [including untrustworthy networks like the internet]). Different security zones should also be physically separated. Firewalls must separate the security zones. Clients and server must be located in different segments of the network. Sensitive information must be transferred by using state-of-the-art secure protocols.

Type of asset				Event consequences	
	Drinking Water Network	Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
	Raw Water Pipeline	Water Abstraction Points	Water Treatment Plants	Financial	Reputation



2

## Risk Reduction Measure

Type of threat: Cyber-Physical



Measure ID: M51  
Name: AppropriateLayingOfWires

Scope of use: Information transmitting wires should be laid in a security conform way. Thus the probability of data thieveries and damages of wires is reduced by preventing unauthorized access to the data transmission wire. The aim is to protect sensitive data.

Comments: It should be made difficult to get access to wires e.g. by underground laying of wires, the protection of wires by mantles or similar.

Type of asset				Event consequences	
	Drinking Water Network	Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
	Raw Water Pipeline	Water Abstraction Points	Water Treatment Plants	Financial	Reputation



2

## Risk Reduction Measure

Type of threat: Cyber-Physical



Measure ID: M52  
Name: ServerRoomSetup

Scope of use: Appropriate setup of server rooms. Thus the lifetime of servers is extended and its ongoing functionality is ensured. The aim is to ensure the continuous operability of all servers under appropriate conditions.

Comments: The server room should be located apart from office rooms and ensure appropriate conditions (temperature, air humidity, constant electrical energy supply, etc.). The room should be secured by doors with an appropriate resistance class and with an appropriate access control system. Furthermore it should be protected against physical hazards like fire, water intrusion etc. A constant supply with electrical energy must be ensured, if necessary an Uninterruptable Power Supply (UPS) must be implemented.

Type of asset				Event consequences	
	Drinking Water Network	Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
	Raw Water Pipeline	Water Abstraction Points	Water Treatment Plants	Financial	Reputation



2

## Risk Reduction Measure

Type of threat: Cyber-Physical



Measure ID: M53  
Name: MirroredSCADA

Scope of use: Implementation of a mirrored SCADA system. Thus in case of a failure of the SCADA system, this failure can be compensated by activating the mirrored SCADA system. The aim is to ensure an ongoing operability of the water utility.

Comments: The mirrored SCADA system should be not be located at the same position as the acutally used SCADA system.

Type of asset				Event consequences	
	Drinking Water Network	Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
	Raw Water Pipeline	Water Abstraction Points	Water Treatment Plants	Financial	Reputation



2

## Risk Reduction Measure

Type of threat: Cyber



Measure ID

M54

Name

DataIntegrityCheck

Scope of use

The integrity of important data should be checked e.g. by blockchain technology. Thus falsified signals are immediately detected. The aim is to ensure that any decision of the utility is based on data with ensured integrity.

Comments

Example of solution provided by STOP-IT:  
Optimization Tool for Sensor Placement and Management and Real-time sensor data protection (RSDP) (Module III)

Type of asset				Event consequences	
	Drinking Water Network	Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
	Raw Water Pipeline	Water Abstraction Points	Water Treatment Plants	Financial	Reputation



2

## Risk Reduction Measure

Type of threat: Cyber-Physical



Measure ID: M55  
Name: MalwareProtectionGuidelines

Scope of use: Implementation of guidelines for a correct behaviour to protect the IT systems from malware. Thus all employees know how to handle hard- and software to ensure a secure IT environment. The aim is to prevent any damages resulting from the malware and to ensure the integrity, authenticity and confidentiality of all data and assets in the IT infrastructure.

Comments: The guidelines should define the handling of potentially harmful soft- and hardware. It should e.g. be defined when and which storage devices may be connected to the IT infrastructure, how annexes of e-mails have to be handled and how executable files have to be treated.

Type of asset				Event consequences	
	Drinking Water Network	Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
	Raw Water Pipeline	Water Abstraction Points	Water Treatment Plants	Financial	Reputation



2

## Risk Reduction Measure

Type of threat: Cyber-Physical



Measure ID: M56  
Name: MalwareProtectionSoftware

Scope of use: Installation of suitable software to protect the IT systems against malware. By this measure malware reaching the IT system shall be blocked, deleted or at least directly noticed. Thus any damages resulting from the malware shall be avoided to ensure the integrity, authenticity and confidentiality of all data and assets in the IT infrastructure.

Comments: Used applications and software for defense against malware should be tailored for the use in enterprises, solutions for home use are not sufficiently safe. Furthermore, the chosen solution should be updated and checked on its effectiveness regularly. The employees should be trained on handling possibly dangerous contents in a sensitive way. Any detections of malware should be reported directly by both, the user detecting the malware and automatically by the system. All relevant data emerging in the IT system should be logged for a fast detection of incidents and for an easier understanding of past attacks.

Type of asset				Event consequences	
	Drinking Water Network	Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
	Raw Water Pipeline	Water Abstraction Points	Water Treatment Plants	Financial	Reputation



2

## Risk Reduction Measure

Type of threat: Cyber



Measure ID

M57

Name

PatchAndChangeManagement

Scope of use

Implementation of a concept for the patch and change management in the IT environment. By following this concept, emerging security holes can be closed quickly and any (e.g. software) changes are monitored with regard to security issues. Thus the security of the IT systems of the company is ensured in general.

Comments

The concept should clearly define all responsibilities and procedures of the patch and changes management process. Furthermore, the handling of auto-updates that might be implemented in the used software should be regulated.

Type of asset				Event consequences	
	Drinking Water Network	Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
	Raw Water Pipeline	Water Abstraction Points	Water Treatment Plants	Financial	Reputation





2

## Risk Reduction Measure

Type of threat: Cyber



Measure ID

M58

Name

NetworkTrafficAnalysis

Scope of use

Surveillance of all network traffic on suspicious patterns. Thus hacker attacks shall be recognized and negative consequences shall be prevented. The aim is to ensure the integrity, authenticity, confidentiality and operability of the network and all connected devices.

Comments

Example of solution from STOP-IT: Network Traffic Sensors and Analysers (NTSA) (Module III)

Type of asset				Event consequences	
	Drinking Water Network	Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
		Water Abstraction Points	Water Treatment Plants	Financial	Reputation



2

## Risk Reduction Measure

Type of threat: Cyber



Measure ID: M59  
Name: SecurityOfWirelessNetworks

Scope of use: Definition of security measures for the implementation and use of wireless network connections. Thus attacks on wireless connections shall be prevented. The aim is to ensure the integrity, authenticity, confidentiality and operability of the wireless network and all connected devices.

Comments: Before the implementation of wireless networks it must be checked if any other wireless networks exist in the same area with similar configurations that could disturb the implemented network. Generally accepted standards for authentication and encryption have to be used. All information transferred via wireless networks has to be encrypted with up-to-date encryption technologies. Access points must be located at positions where no unauthorized personnel can reach them. Access points may not be operated in default configurations. A security barrier should exist between wireless and wired connections. Regular checks for security wholes should be ensured.

Example of solution from STOP-IT: Jammer Detector (JDet) (Module II)

Type of asset				Event consequences	
	Drinking Water Network	Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
	Raw Water Pipeline	Water Abstraction Points	Water Treatment Plants	Financial	Reputation



2

## Risk Reduction Measure

Type of threat: Cyber



Measure ID: M60  
Name: SoftwareManagement

Scope of use: The software management should be organized and carried out by responsible IT experts. Thus only credible software is installed correctly, furthermore an appropriate use of the software is taught to the staff. The aim is to avoid cyber security issues due to the installation of untrustful software, wrong installation of trustful software or inappropriate software uses.

Comments: 0

Type of asset				Event consequences	
	Drinking Water Network	Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
	Raw Water Pipeline	Water Abstraction Points	Water Treatment Plants	Financial	Reputation



2

## Risk Reduction Measure

Type of threat: Cyber



Measure ID: M61  
Name: MobileDeviceUsageRules

Scope of use: Setting up of clear rules for the use of mobile devices. Thus the staff knows how to use mobile devices outside the utility in a secure way. The aim is to ensure data and cyber security also outside of the utility area.

Comments: Examples for rules could be the mandatory use of privacy films for monitors or automatic screen locks after a certain time of inactivity. Losses of IT equipment should be reported as soon as possible to the utility. Portable devices should be encrypted. Connections to the utility's network should only be allowed via Virtual Private Network (VPN) connections.  
A list of mobile devices should exist in the company.

Type of asset				Event consequences	
	Drinking Water Network	Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
	Raw Water Pipeline	Water Abstraction Points	Water Treatment Plants	Financial	Reputation



2

## Risk Reduction Measure

Type of threat: Cyber



Measure ID: M62  
Name: DeletionAndDestructionOfDataCarriers

Scope of use: Ensuring of proper deletion of data and destruction of data carriers. By a proper deletion or destruction, the data shall be irreversibly wiped out. Thus the loss of any sensitive data shall be prevented.

Comments: The data deletion mechanisms should ensure that no data can be restored and that no residual data exist. All employees should be trained how to delete data and destroy data carriers correctly. If data carriers are collected and stored before destruction, the location of collection has to be protected against any possible intruders.

Type of asset				Event consequences	
	Drinking Water Network	Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
	Raw Water Pipeline	Water Abstraction Points	Water Treatment Plants	Financial	Reputation



2

## Risk Reduction Measure

Type of threat: Cyber



Measure ID: M63  
Name: SecureOutsourcing

Scope of use: Assurance of IT security in case of outsourcing by setting-up appropriate agreements with the respective companies. By these agreements it is guaranteed that also the respective external companies comply with the relevant security guidelines. Thereby it is ensured that emerging risks due to the outsourcing process are minimized.

Comments: The agreement should ensure that the commissioned company complies with a sufficiently acknowledged security standard (e.g. the German IT-Grundschutz [IT-Basic Protection]).

Type of asset				Event consequences	
	Drinking Water Network	Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
	Raw Water Pipeline	Water Abstraction Points	Water Treatment Plants	Financial	Reputation



## Risk Reduction Measure

Type of threat: Cyber-Physical



Measure ID: M64  
Name: Documentation

Scope of use: A complete documentation of all relevant assets and processes in the physical and digital infrastructure of the water utility must be ensured. Thus a full overview of the utility and potential risks is available at any point of time. The aim is to be able to recognize any weak points that have to be treated by different risk reduction measures.

Comments: 0

Type of asset				Event consequences	
Catchment Area	Drinking Water Network	Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
Raw Water Bodies	Raw Water Pipeline	Water Abstraction Points	Water Treatment Plants	Financial	Reputation



2

## Risk Reduction Measure

Type of threat: Cyber-Physical



Measure ID: M65  
Name: IdentificationClassificationAndRiskAssessmentTool

Scope of use: The Company must select a particular approach and methodology for risk assessment and analysis that incidents and prioritizes risks based on threats, vulnerabilities and consequences of security.

Comments: Example of solutions from STOP-IT: Cyber Threat Sharing Service (CTsS) (Module V), Real-Time Anomaly Detector (RTAD) and Cross Layer Security Information and Event Management (XL-SIEM) (Module VI), Reasoning Engine (REN) (Module VIII)

Type of asset				Event consequences	
Catchment Area	Drinking Water Network	Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
Raw Water Bodies	Raw Water Pipeline	Water Abstraction Points	Water Treatment Plants	Financial	Reputation





Empty template of Risk Reduction Measure card made available to create new ones during the training session.

2

## Risk Reduction Measure

Asset category:













  

Measure ID

Name

Scope of use

Comments

Type of asset				Event consequences	
Catchment Area	Drinking Water Network	Drinking Water Tanks	Pressure Boosting Station	Quality	Quantity
					
Raw Water Bodies	Raw Water Pipeline	Water Abstraction Points	Water Treatment Plants	Financial	Reputation
					

D4.4 Cyber-physical threats stress-testing platform

[ 145 ]



## 6.4 VALUE CARD

**3** **VALUE**

Scenario

Facilitator name  
and organisation

Actions agreed

Notes

General  
recommendations



STOP-IT



STOP-IT