STOP-IT

Deliverable 4.2: Risk Analysis and Evaluation Toolkit

KWR

May, 2019

www.stop-it-project.eu

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 740610.

D4.2: RISK ANALYSIS EVALUATION TOOLKIT

SUMMARY

Deliverable 4.2 – Risk analysis and evaluation toolkit - aims at presenting the work fulfilled, under Task 4.2 and in WP4 as a whole, towards the development of the toolkit which is consisted of state of art models and tools for the analyis and evaluation of risks (from physical, cyber and combined events) to the water systems (with focus on the vulnerable assets identified). Considering the close connection and interoperability of all components foreseen under the Risk Assessement and Treatment Framework, this document aims at providing the readers with a vivid and complete picture of all autonomous, yet interoperable, tools towards the tactical and strategic risk assessment and intervention planning. The first part of this report provides a common ground in the field of cyber-physical systems and their secutiry through a thorough literature review on relavent terms, legal frameworks, standards and state-of-the-art methodologies and tools for risk identification/analysis/management/treatment, whereas the second part documents the STOP-IT products and the overall established methdology. After ensuring compatibility with ISO 31000, inter-related components of STOP-IT are described, the methodological approach and different levels of analysis are explained which are concluded with the user's perspective descriptions and scenarios of use. Further, a more detailed description is provided for the developemnt of the InfraRisk-CP, the Risk Analysis and Evaluation Toolkit (RAET) and the Key Performance Indicators (KPIs) which are some of the key elements of the framework explicitely described under T4.2.

DELIVERABLE NUMBER	WORK PACKAGE
D4.2	WP4
LEAD BENEFICIARY	**DELIVERABLE AUTHOR(S)**
KWR	Christos Makropoulos (KWR) George Moraitis (ICCS) Dionisis Nikolopoulos (ICCS) George Karavokiros (ICCS) Archontia Lykou (ICCS) Ioannis Tsoukalas (ICCS) Mark Morley (KWR) Mario Castro Gama (KWR) Eivind Okstad (SINTEF) Jørn Vatn (SINTEF)
QUALITY ASSURANCE	
Reviewer 1: Dimitrios Bouziotas Reviewer 2: Jordi Meseguer	KWR CETAQUA
PLANNED DELIVERY DATE	**ACTUAL DELIVERY DATE**
31/05/2019	05/06/2019

DISSEMINATION LEVEL	X 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

List of Figures

List of Tables

List of Acronyms and Abbreviations

CA: Consortium Agreement

CIP: Critical Infrastructure Protection

CIs: Critical Infrastructures

CO: Confidential

CPS: Cyber-Physical Systems

DoW: Description of Work, referring to the Annex I of the Grant Agreement

EC: European Commission

ETA: Event Tree Analysis

FRs: Front Runners

FTA: Fault Tree Analysis

GA: Grant Agreement

IPR: Intellectual Property Rights

MOB: Multiple Occurring Branches

MOE: Multiple Occurring Events

OSP: Operator Security Plan

PDA: Pressure-Driven-Analysis

PDD: Pressure-Driven-Demand

PLC: Programmable Logic Controller

PPR: Project Progress Reports

PSA: Probabilistic Safety Assessment

PSB: Project Steering Board

PU: Public

QA: Quality Assurance

RAET: Risk Analysis and Evaluation Toolkit

RBD: Reliability Block Diagrams

SAB: Security Advisory Board

SCADA: Supervisory Control And Data Acquisition

SP: Scenario Planner

STC: Scientific and Technical Committee

STP: Stress Testing Platform

TL: Toolkit Library

VI: Vulnerability Index

WDN: Water Distribution Networks

WP: Work Package

WSC: Water Supply Company

Executive summary

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 key parts of the water infrastructure. One of the modular components of the STOP-IT risk management platform is the **Risk Assessment and Treatment Framework** of **WP4 (Module I)**. The aforementioned integral component of the project platform is deployed through several autonomous, yet interoperable, tools aimed towards the tactical and strategic risk assessment and intervention planning. Those tools are:

- the Risk Identification Database (**RIDB**) of Task 3.2,
- a step-by-step guide for vulnerability assessment implemented through the Asset Vulnerability Assessment Tool (**AVAT**) (T4.1),
- the Risk Analysis and Evaluation Toolkit (**RAET**) including state-of-the-art models and tools, for the analysis and evaluation of risk (from physical, cyber and combined events perspective) to the water systems (T4.2) including, among others, the **Infrarisk-CP** tool, the **Scenario Planner** (**SP**) and the Probabilistic Safety Assessment tool, i.e. Fault Tree Editor (**FT Editor**),
- the Risk Reduction Measure Database (**RRMD**) (T4.3) recommending actions to avoid or mitigate the occurrence and consequences of risk events for water CIs,
- the Stress-Testing Platform (**STP**) to conduct cyber-physical simulation (T4.4)
- Key Performance Indicators (**KPIs**) tool (T4.2) used within the STP to evaluate the effectiveness of risk reduction measures.

The current document (Deliverable 4.2 “Risk Analysis and Evaluation Toolkit”) is the outcome of a conscious effort to commit all autonomous, yet interoperable tools of RAET developed under the Risk Assessment and Treatment Framework to paper. The deliverable was developed by KWR, ICCS and SINTEF partners within Task 4.2 “Development of Risk Analysis and Evaluation Toolkit” of WP4, led by the KWR partner.

The primary objective of this document is to give end-users a clear and concise picture of the overall framework and its different components which are essential for cyber-physical risk management. The respective Parts A to E of the document have been drafted to assist users’ understanding in terms of the RAET tools’ actual interoperability and combined use. Detailed descriptions of some tools are provided in other STOP-IT deliverables and thus references are given to those documents when necessary. An indicative example is the Risk Identification Database (RIDB), a component developed under WP3 and documented in Deliverable 3.2, which is a perquisite for the threat/events identification implemented within RAET.

To support the aforementioned goal i.e. providing thorough information on the STOP-IT framework, this document has been divided into five parts. The first part (Part A) consists of a comprehensive literature review, in order to create a solid base on cyber-physical risk terminology but also to form a record of state-of-the-art methodologies, tools and approaches

in the field of the cyber-physical security. Specifically, Part A begins with a brief introduction on cyber-physical systems and attacks and provides examples supporting the fact that the different processes governing modern water systems should be considered as a combined cyber-physical system (CPS). The next sections familiarize readers with legal frameworks of critical infrastructures and ISO standards. Considering that the STOP-IT methodology is aligned to ISO 31000, emphasis has been given to the aforementioned standard. The paragraphs that follow enable users to have an overview of different methodologies and tools used for risk management and get acquainted with concepts such as cyber-physical layers modelling, stress-testing testbeds and the corresponding Key Performance Indicators.

The second part of this report (Part B) has been developed in order to guide the users through core STOP-IT methodologies and developments. In the first section, an introduction to the STOP-IT Risk Assessment and Treatment Framework is being made and information is provided on STOP-IT's compatibility with the ISO 31000:2009. The latter is considered a key element for the acceptance and interoperability of the STOP-IT framework with existing risk management procedures in the water sector. Nevertheless, the described framework and delivered tools can be deployed by utilities not aligned with aforementioned standard. The second section of Part B introduces the users to all autonomous components which are the integral parts of the Risk Assessment and Treatment Framework (Module I). The part that follows documents the STOP-IT methodological approach and describes the three levels of analysis suggested to cover different user's needs and data availability cases.

The final part of the report (Parts C to E) focuses on specific components of the methodological framework and includes examples of using the tools mentioned previously, along with a description of the workflow from the end-user's perspective which assists them in having a better overview of the methodology and the tools. Part C deals with InfraRisk-CP methodology and configuration. A detailed overview of the RAET (system architecture, user's guide) is given in Part D. The specifics of the STOP-IT Key performance Indicators Framework and the respective tool are detailed in Part E.

Additional information is provided in the ANNEX part which includes a glossary of cyber-physical systems and their risk management (ANNEX A), more detailed descriptions on SCADA systems and attack taxonomy (ANNEX B), as well as a full description of Key Performance Indicators (ANNEX C) created for the purposes of our methodological framework. Moreover, supplementary material for InfraRisk-CP is provided (ANNEX D), as well as a mention of the architectural specifics of RAET (ANNEX E).

The RAET (and the publicly available components) are available through the RAET demo server by following the link: http://raet.itia.civil.ntua.gr:8001/. To access certain tools and functionality of RAET, login to the system is required (Part D, section 4.1). Credentials for accessing it can be obtained from Dr. Christos Makropoulos (Christos.Makropoulos@kwrwater.nl or cmakro@chi.civil.ntua.gr).

1.1 Cyber-physical systems and attacks

Almost every major sector of an organized society, such as electricity, water, waste, gas, railway and traffic control, relies on Critical Infrastructure (CI), which essentially is comprised of a Cyber Infrastructure (computers, embedded systems, networks and software) on one side and the physical system on the other side. The common term for these combinatory systems is “cyber-physical systems” (CPS). CPS use a number of field devices to collect information (sensor network) to monitor current conditions and help manage performance. Control logic devices (PLCs, RTUs) can support this process automatically with inherent “rules” based on information provided by the sensors. A number of field devices remotely controlled (actuators) receive the control orders and physically act on the system. These systems are governed usually by SCADA (Supervisory Control And Data Acquisition) systems. SCADA is a “control system architecture that uses computers, networked data communications and graphical user interfaces for high-level process supervisory management, but uses other peripheral devices such as programmable logic controller (PLC) and discrete PID controllers to interface with the process plant or machinery" (Wikipedia n.d.). A SCADA system allows an operator to monitor the functions and gather measurements from a remote location via sensors, make set point changes on distant process controllers via field devices and monitor alarms. In other words, CPS are physical systems controlled by interconnected computational elements. A complete SCADA architecture example is visualised in Figure 1.

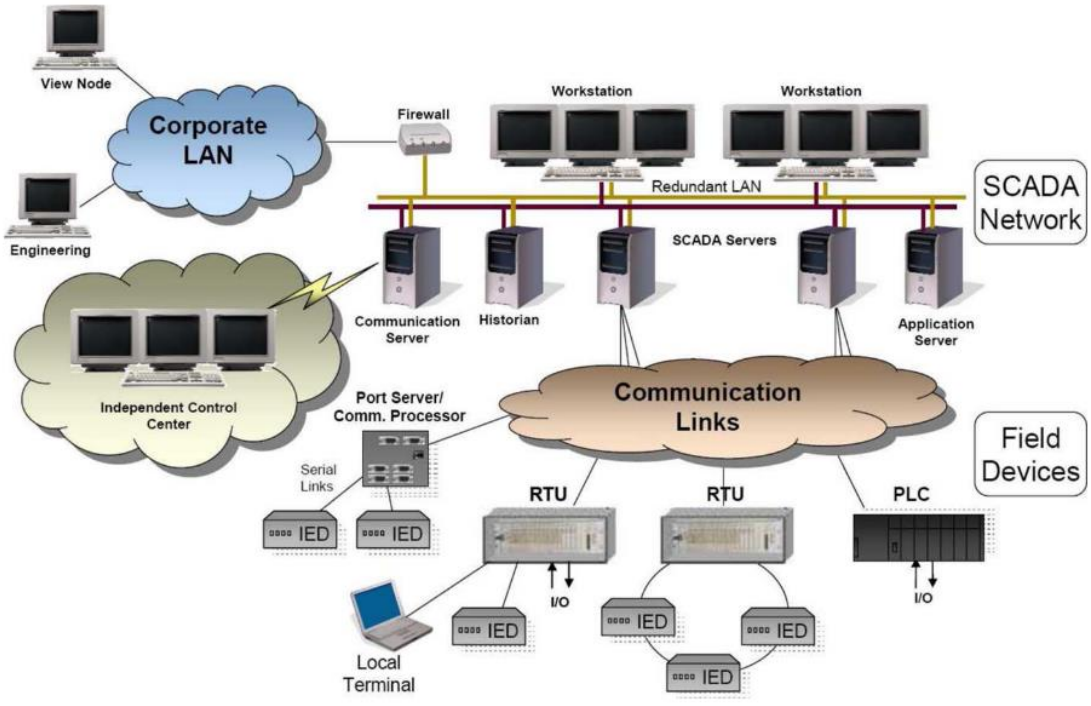


Figure 1: SCADA architecture (Queiroz et al., 2011)

The very nature of the new CP architecture is what makes them susceptible to “cyber and Cyber-Physical Attacks (CPA), which are defined as cyber-threats devised to target an attached physical system” (Taormina et al., 2018).

Probably one of the most intriguing examples of a cyber-physical attack is the Stuxnet virus that targeted the Iranian nuclear CI SCADA. Stuxnet was designed to silently hijack the SCADA, by repeating a 21 seconds long recorded signal of a sensor to the SCADA screens (termed HMI, Human Machine Interface) and then causing overpressure of the centrifuges with dire consequences for the physical process. The virus was designed to cause fatigue to the asset and not catastrophic destruction (Langner, 2013) and was successful in impeding in Iran’s nuclear programme. More than 50 variants of Stuxnet are discovered in similar recent cyber-attacks (Zhu et al., 2011).

An example of catastrophic cyber-attack on water CPS is the incident of the sewage treatment system in Maroochy Shire, Queensland, where 800 000 litters of raw sewage were released to spill out into local parks and rivers, causing death of marine life, stench, and discoloration of water after a man, who was turned down from hire by the Maroochy Counsil but has worked on the SCADA installation with another company, hacked the SCADA system via remote radio controls from stolen equipment to avenge the water company (Queiroz et al., 2011).

Recently, various other incidents of cyber-physical attacks have threatened real-world water CPS, and the cyber-security sector has acknowledged them among the most targeted critical infrastructure (ICS-CERT 2016).

A risk management framework able to simulate the physical systems as a complete cyber-physical infrastructure, and investigate physical attack scenarios, cyber-attack scenarios and their combination is considered of primary importance in order to efficiently protect them under the threats posed due to the ever-changing landscape of the digital world and the rising concerns about security.

1.2 Legal framework on CIP

One of the most important modern global challenges is the so-called Critical Infrastructure Protection (CIP), especially since the terrorist attack of the twin towers of the World Trade Centre on 9/11/2001. The potential threats posed against CIs of all sectors are ever-changing and evolving, taking advantage of the complex interconnection both within and between the systems.

According to Council Directive 2008/114/EC, Critical Infrastructure is *“an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions”*.

According to Homeland Security Presidential Directive 7 (HSPD7), the US maintain the definition given in Critical Infrastructures Protection Act of 2001, that CIs are defined as *"systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters"*.

In both EU and US CIP (Critical Infrastructure Protection) Frameworks, the element of interdependencies of networked CIs is highlighted and incorporated in the risk assessment methodologies proposed. According to Rinaldi et al. (2001), Gillette et al. (2002) and others, there are 4 types of interdependencies:

1. *Physical*: The material output of one infrastructure is used in the operation of another infrastructure
2. *Cyber*: Infrastructure dependency on information transmitted through the information and communication infrastructure
3. *Geographic*: More than two infrastructures are co-located and affected simultaneously by a local effect
4. *Logical*: A dependency not categorized as physical, cyber or geographic (e.g. economic dependency)

Interdependencies play a crucial role in holistic risk identification, analysis and treatment processes, as potential cascading effects due to hyper-connectivity of infrastructures, if not recognized can lead to lack of effective treatment and severe consequences. To demonstrate the importance of interdependencies of CIs, the first step for the development of the CIP programme at the EU level, is the identification of such connectivity in both European and national level.

Although it only refers to the energy (electricity, oil, gas) and transport sectors, EU Commission, in 2006, following EC request for an overall strategy for protection of CIs against terrorist attacks, communicated the principles and processes of a programme for Critical Infrastructure Protection (EPCIP) (COM(2006) 786) and published the Council Directive 2008/114/EC. It has also defined the European Critical Infrastructures (ECIs), as those which, if disrupted, would affect 2 or more Member States. A few years earlier, EU founded the European Network and Information Security Agency (ENISA) with Regulation EC460/2004, aiming to assist EU Member States against cyber threats. In addition, the Critical Infrastructure Warning Information Network (CIWIN) was created, as proposed in COM (2008) 676, providing the means to communicate the best practices among Member States and CIs. Within the EPCIP, no specific methodologies are defined/proposed, except that the risk analysis must consider the threat scenario approach (CD 2008/114/EC, article 2(c)). All Member States are obligated to report on their national CIs and communicate vulnerabilities, based on the Operator Security Plans (OSP), which is an equivalent term to Risk Management Plan of ISO 31000:2009. According to Bouchon et al. (2008), for the OSP 9 key aspects should be considered. Summing them up, the scenarios must be aimed to **loss of service**, based on feasible potential threats that can have **cascading effects** as a result.

The **multiple durations** and **escalations** of events must be evaluated and **existing control** and **availability of alternatives** also taken into account. An **ex-ante analysis** in an **all hazards approach** should be adopted, to describe and give additional information on risks for the evaluation. One of the most intriguing aspects, to be taken into account, for the scenarios is the potential misuse or **"weaponization" of the system** under consideration.

1.3 ISO 31000 and other standards

IMPORTANT NOTE: In this document, the ISO 31000:2009 is used. There has been a recent release of a newer version (ISO 31000:2018). If necessary and applicable, updates will be made in future.

In order to ensure survivability and prosperity of any CI, a Risk Management plan is of paramount importance. As part of it, Risk assessment is the overall process of risk identification, risk analysis and risk evaluation (ISO 73:2009) prior to risk treatment. It is in fact an integral part of any emergency management plan, aiming to provide information in 4 key components of survivability:

a. Preparedness
b. Mitigation
c. Response
d. Recovery

Standards work as a solid, common ground between experts to communicate best practices and processes. Since most are a result of extensive discussions between topic experts, manufacturers, academics and others, standards contain essential information and knowledge. International Organization for Standardization (ISO) has published a series of standards that aim to assist organizations in better managing assets and decision making for experts. The umbrella for the Risk management of assets and support of risk managers is ISO 31000. Its scope is not to create a single, unique management across organizations, but rather to harmonize and set a common background for organizations to build on. ISO 31000:2009 provides the framework under which, an organization can construct an end-to-end Risk Management Plan, which, in ISO principals, is tailored to the organization's needs and profile but takes into account uncertainty, the nature of the organization and how it can be addressed. The structure of the Risk management process under this standard's framework can be visualized in the following figure.

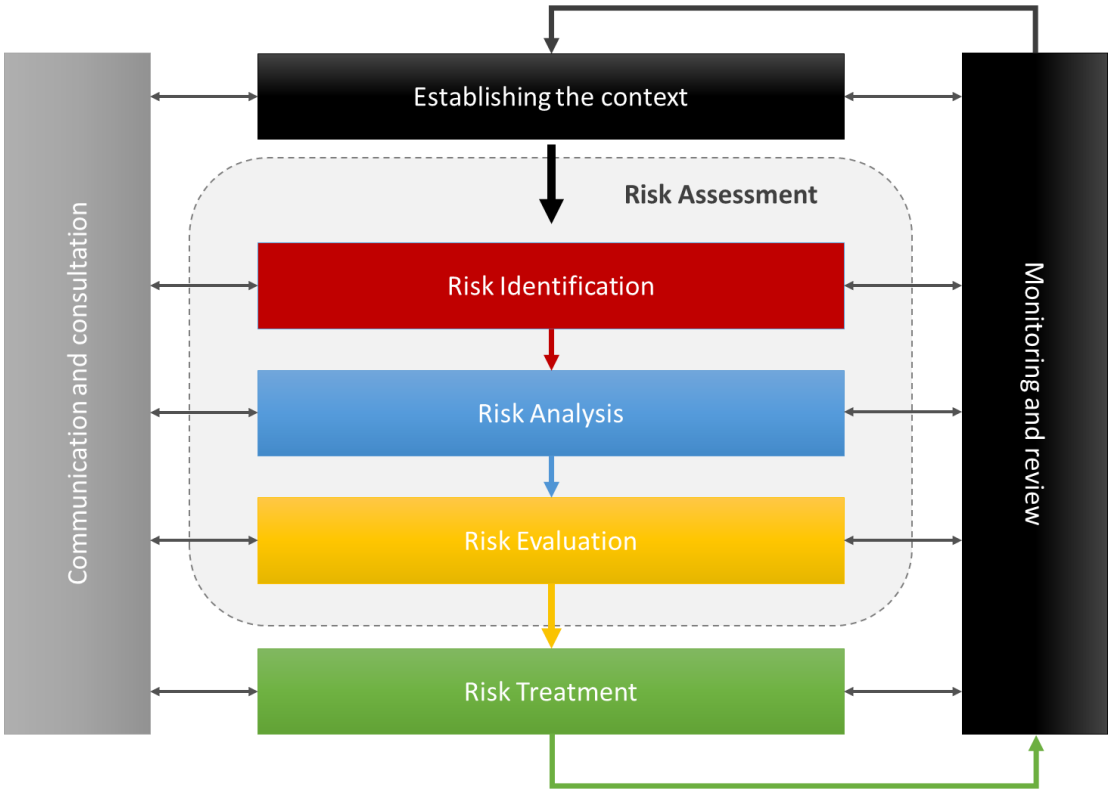


Figure 2: ISO 31000 Risk management process

The first step in constructing an ISO based Risk management plan is the establishment of the internal and external context. External context defines the social, cultural, political, financial, economic, legal and regulatory environment under which the organization is due to operate. In this context, relationships and trends must also be defined in regards to that environment and the organizations objectives. With the term internal context, ISO defines the company's policies, objectives, capabilities, adopted standards etc. in addition to its role and accountabilities. Based on both these contexts, the Risk Criteria are defined for each company. They are terms of reference against which significance of risk is evaluated. In other words, they are the risk acceptance-or-rejection threshold values for each company. Risk criteria levels must also be in line with appropriate levels of analysis e.g. qualitative analysis should be performed and assessed based on qualitative or semi-quantitative levels of Risk Criteria. This step is crucial in understanding the capabilities, expectations and limitations under which the risk management team has to plan, report and act.

The follow-up process of planning, reporting and acting is termed Risk Assessment.

As seen in Figure 2, the three key steps identified in ISO 31000:2009 for the Risk Assessment process in an organization are the following:

1. Risk Identification
2. Risk Analysis
3. Risk Evaluation

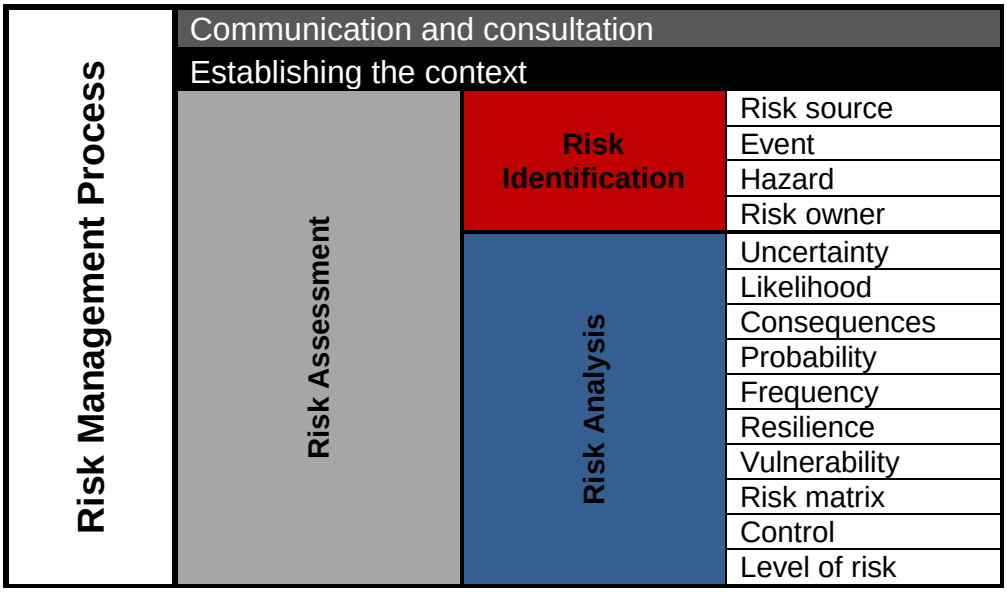
The first step of Risk Assessment is Risk Identification. This step aims at creating a knowledge base of the company's risks, based on events that can have an effect on the achievement of goals (in our case it can be e.g. deliver sufficient and good quality water to customers). This base must include possible causes and scenarios on how consequences occur (ISO 31000:2009). The comprehensive identification of the risks and possible cascading or cumulative effects is of paramount importance, as an undetected risk is an untreated one.

Following the Risk Identification step, a Risk Analysis should be performed in order to understand the nature of risks (consequences, likelihood, level of risk and other attributes), considering their sources and interdependences. Appropriate degree of detail is considered under the variables of risk, purpose and the data available.

The above step must provide all the necessary input for Risk Evaluation, with appropriate risk criteria to evaluate the risk analysed and help decision on whether risks must be treated. Decision should also be made based on policies and regulations.

After Risk Evaluation step, the Risk Assessment process is completed and Risk Treatment is the step that follows. All identified, analysed, quantified and evaluated as to-be-treated risks are inserted in a circular process. A risk treatment measure is assessed and residual risk levels are estimated. If the residual risk is tolerable, then the measure is accepted and ready to modify the controls of the system. If not, a new risk treatment must be generated and effectiveness is reassessed, until risk attitude criteria/limits are met.

In order to facilitate the entire process, ISO has published ISO Guide 73 (2009), the Risk Management vocabulary, creating a common and consistent understanding of the terms used. This also acts a solid ground for communication between experts and deals with misconceptions in risk management frameworks and plans. The basic relationship between terms and Risk Assessment and Treatment steps can be seen next in Figure 3.



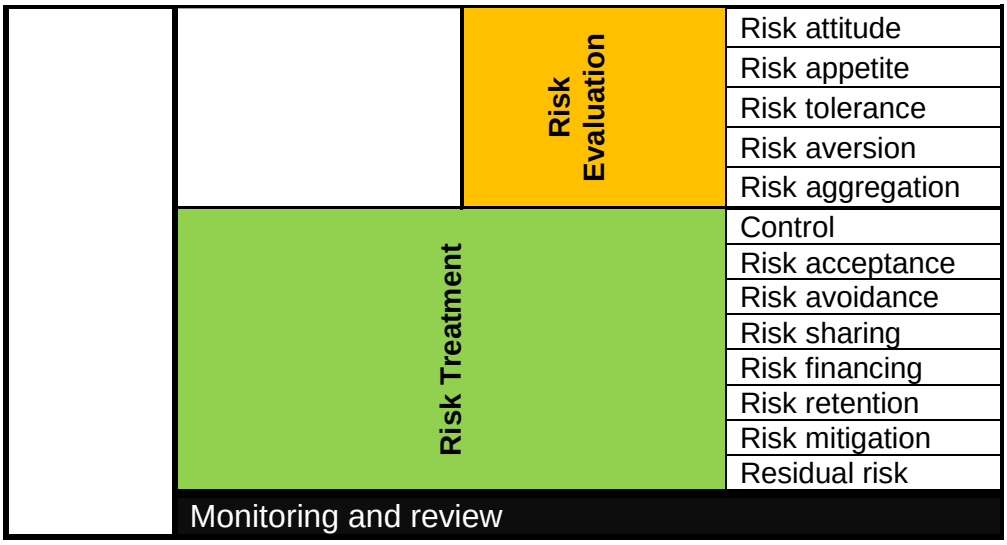


Figure 3: Relationship between key terms used and Risk Management processes (ISO Guide 73, 2009)

Following the creation of a common risk language, ISO took the next step of creating a techniques pool, where risk management teams can refer. This part of the ISO risk management family is ISO/IEC 31010:2009, containing Risk assessment techniques. The potential techniques listed in this ISO document refer to each (or multiple) step of the process and its suitability/applicability to each. In addition, this ISO proposes a set of attributes to assist risk teams decide on the selection of the appropriate tool.

In regards to specifically addressing risk in the water sector, AWWA (American Water Works Association) has published several relevant Standards. Under the legislative umbrella of Homeland Security Presidential Directives (HSPD) that cover the topics of Domestic Incidents, Response Plans, Critical Infrastructure Identification, Prioritization and Protection, National Preparedness and more (HSPD-5, HSPD-7, HSPD-8, HSPD-9), Standards set the minimum requirements for a protective security program in Water and Wastewater utilities (ANSI/AWWA G430-09), requiring up-to-date assessments of risks and vulnerabilities, access control and intrusion detection etc., in water sector CIs. A coordinated effort by AWWA to create a clear frame, under which WSC will perform their Risk Assessment and Treatment plans, is clearly shown by publishing AWWA J100-10 Standard (AWWA, 2010) on risk and resilience management of water and wastewater systems. It is a clear, step-by-step guide to an all-hazards plan that includes methodologies and proposed approaches for all the topics, from risk identification to risk treatment. The J100-10 Standard adopts the RAMCAP Process, visualized in Figure 4. It is noted, that each step of the process is colour coded so as to assist readers in recognising similarities and differences among the Legal frameworks.

Figure 4: RAMCAP Risk and Resilience Management process, colour indicator in matching ISO steps colours

The key aspect of the Standard, in regard to *"malevolent threats"* (i.e. Deliberate Attacks) in the Water Distribution Networks (WDN) CI, is the estimation of likelihood based on a set of attributes concerning adversary's objectives and capabilities, intensions and attractiveness of facility and region. Likelihood can be estimated via 3 approaches, summarized below:

1. *Best estimate*: likelihood is based on informed experience of the organization
2. *Conditional Assignment*: likelihood is considered to be the binary set of probabilities 0 and 1
3. *Proxy Measure*: likelihood is estimated through proxy measures based on attractiveness, vulnerability and other attributes of the facility, area and/or governmental facilities in the area.

Another important aspect, relevant to risk evaluation, is the use of, in addition to risk, resilience-based approaches rather than a simple uncertainty-based approach, giving an enhanced view of the system under various threats, also providing the means to compare options and set the acceptable level of risk between multiple and of-different-nature scenarios.

In regards to the cyber element of the CIs, no specific reference is made within the above Standards. ISO has published a series of standards that refer to the information security risk management. The ISO 27005:2011 Standard, includes security techniques, based on the

terms and processes of ISO 31000 family. It has a clear and well-structured flow between the "tasks" the risk management team has to follow, including examples of typical threats, assets etc. One of the most interesting examples provided within it, is the characterization of two types of assets, delineated between primary and supporting. The supporting assets are the assets the primary rely on and can be distinguished in a first level of detail as follows:

- Primary assets
  - Business process & activities
  - Information
- Supporting assets
  - Hardware
  - Software
  - Network
  - Personnel
  - Site
  - Organization's structure

In that manner, the team can identify and register the company's assets in a structured and well-organized way.

Similar to the ISO 27005:2011 Standard, National Institute of Standards and Technology (NIST) has published a guide for conducting risk assessments for information security (NIST, 2012). The overall proposed process and flow is found to be similar to the ISO 31000:2009, including terminology, with the main difference being the addition of supplemental guidance for each step. This publication includes an extended glossary on the topic as well.

Another standard, relevant to modelling the cyber layer of organizations is the ITU-T X.200 (International Telecommunication Union, 1994), identical to ISO 7498-1:1994. The scope of this standard is to create a common ground for the interconnection of "open" systems and information sharing between them. It also provides a chapter regarding the management of such systems, while previously has defined its architecture and structure. ISO proposed the Open System Interconnection (OSI) model, dividing the system to 7 layers and assigning protocols to each. It is not an actual operating model but a conceptual framework to break down the complex interconnection and communication within the (ideal) network. The OSI model layers' visualization can be seen next in Figure 5.

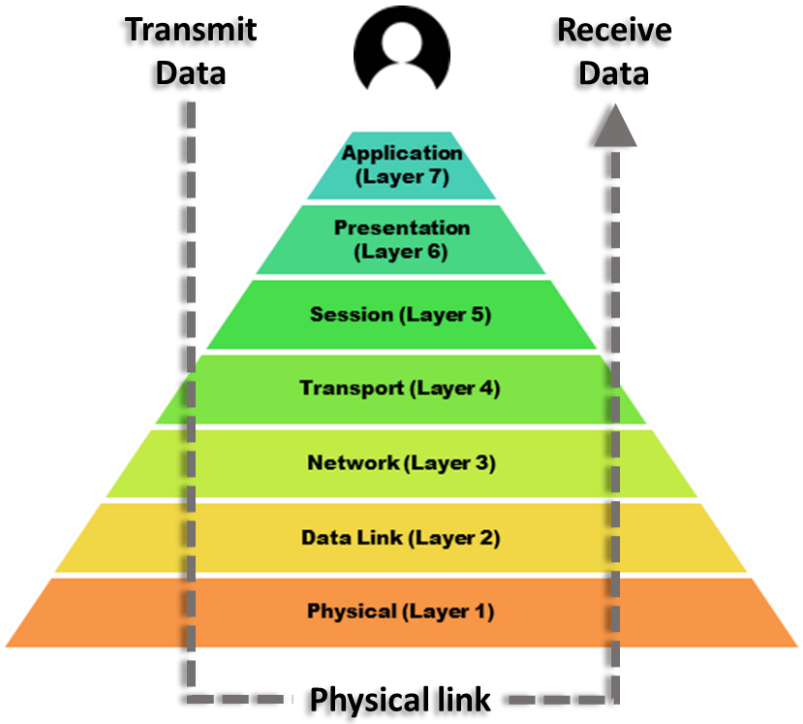


Figure 5: OSI architecture of 7 layers visualization

A short description of the layers is being provided below:

Application layer 7: Supports the end-user processes. It includes sending messages and receiving, through this application-specific layer.

Presentation layer 6: Transform the data between application and network formats, acting as a “translation layer” that also includes encryption processes.

Session layer 5: Manages connections between applications. It establishes and terminates connections/sessions, and manages traffic of data transferring.

Transport layer 4: Transport-service for transparent, error free, reliable and effective transfer of data. The protocols, error detection and recovery of this layers are end-to-end.

Network layer 3: Establishes, maintains and terminates network-connections. This layer includes error notification, reset and receipt of confirmation between the units of the network.

Data Link layer 2: In this layer, functions that detect and possibly correct errors from the Physical layer can be applied. It contains functions such as error detection, control of data-circuit interconnection and data management (sync, sequence control).

Physical layer 1: It is the physical communication path of the OSI model, among physical-entities for the transmission of bits. It includes all physical connections, data units, connection endpoints etc.

1.4 Methodologies and tools for risk management

1.4.1 Overview

A well-aimed Risk Assessment and Treatment procedure is the key to a healthy and safe organization. When that organization happens to be a Water Supply Company (WSC), keeping its Critical Infrastructure (CI) running optimally also means that it preserves a healthy and safe society. It is important to emphasize that water distribution networks (WDN) include an additional cyber layer, interconnected to the physical, adding to the complexity of the system and making it a Cyber-Physical System (CPS). Bearing in mind the importance and the undeniable uniqueness of such infrastructures, the main focus of the literature review that follows is on the best practices applied in CIs.

In the following sections, a number of methodologies and tools related to risk management are reviewed, summarized in Table 1: We first review a number of methodologies that refer to all ISO steps, acting as frameworks and setting the background for the approaches to be followed, with four of them referring explicitly to the water sector CIs. Then a set of Risk Identification methodologies is presented, since little information was found on the general methodologies regarding this crucial step. Getting more practical and following the ISO process flow, the next step after the Risk Identification is to review a number of tools (empirical or model-based) that refer to vulnerability assessment, consequences analysis and treatment analysis such as sensor placement optimisation.

Table 1: Overview of methodologies and tools for risk management

Name	Approach	Purpose	Water sector CI	Focus
Risk management				
COUNTERACT	Methodology	All ISO steps		Mainly deliberate attacks
EURACOM	Methodology	All ISO steps		All-Hazards
BIRR	Methodology	Risk Identification, Vulnerability Assessment, Consequences Analysis	✓	All-Hazards

CIPPS	Dynamic model, Probabilistic optimization	All ISO steps	✓	All-Hazards
SANDIA Methodology	System Dynamic, Empirical	All ISO steps	✓	Deliberate Attacks
RAMCAP-plus	System Dynamic, Empirical	All ISO steps	✓	All-Hazards
HAZOP	Methodology / Empirical	Risk Identification	✓	All-Hazards
SWIFT	Methodology / Empirical	Risk Identification and Risk Analysis	✓	All-Hazards
PHA	Methodology / Empirical	Risk Identification	✓	All-Hazards
Fault Tree Analysis	Methodology	Risk Identification and Risk Analysis	✓	All-Hazards
INFRARISK	Empirical	Risk Identification and Risk Analysis	✓	All-Hazards
FAIT	Empirical, GIS	Risk Identification, Consequences analysis		-
VAMPG	Empirical	Risk Identification, Vulnerability Assessment		Deliberate Attacks
NSRAM	Empirical, Probabilistic, Dynamic FTs, Dynamic System	All ISO steps	✓	All-hazards (including cyber and physical)
WISE	System Dynamic, GIS	All ISO steps	✓	All-Hazards
TEVA	Empirical, Probabilistic, Optimization	Risk Identification, Vulnerability Assessment, Consequences analysis	✓	Water Contamination (deliberate or accidental)

1.4.2 COUNTERACT

Cluster of User Networks in Transport and Energy relating to Anti-terrorist Activities (COUNTERACT) is a risk assessment methodology focused on transport CIs, aiming to create a structured way to face potential deliberate attacks. As seen in the project's deliverable, proposing the generic guidelines, (COUNTERACT, 2009), the types of threat considered are mainly high impact physical attacks, i.e. terrorist attacks, including bombs, hijacking and bio-chemical agents.

As a first step in the overall method, COUNTERACT proposes brainstorming and a systematic visualisation structure of the public transport system under examination, through construction of operational diagrams. One of the key components of the well-aimed methodology proposed is the consideration of attributes of the system that "may increase "attractiveness" of parts of the system as target for attacks" (COUNTERACT, 2009). Such attributes could be the number of passengers, geographical distinct features that could facilitate attacks, symbolic importance or special dates etc.

After the identification of the assets and their characteristics, including aspects that may increase "attractiveness", possible terrorist threats and scenarios are constructed. In order to assess the risks, COUNTERACT, "for practical reasons", proposes a qualitative approach of scoring matrices. The probability of occurrence is defined by the organization, based on 5 qualitative classes (1-5 score), beginning from "Very Unlikely" up to "Very High". Those classes translate to a range of "an execution of the threat is extremely unlikely, and the threat has never been executed in other PT operations" up to "The threat can be executed at any time and/or has been executed within the organization repeatedly". Same approach is proposed for the consequences of threats, with 4 qualitative classes, ranging from "uncritical" to "disastrous". It is important to note that in the definition of the classes of the impact matrix, COUNTERACT considers 2 perspectives of impacts. One is in regards to "persons" impact (passengers/human lives) and the second is regards to the organization ("PT operator") and its services. The final Risk-Categories matrix pairs the results of the two classes to rank the Risk, as seen in Figure 6. Risk level/category, in COUNTERACT methodology, directly assesses the need for risk treatment, and its "priority".

Probability of Occurrence	Risk Categories			
Very high (5)	Tolerable (5)	Precarious (10)	Intolerable (15)	Intolerable (20)
High (4)	Tolerable (4)	Precarious (8)	Precarious (12)	Intolerable (16)
Possible (3)	Negligible (3)	Tolerable (6)	Precarious (9)	Precarious (12)
Low (2)	Negligible (2)	Tolerable (4)	Tolerable (6)	Precarious (8)
Very unlikely (1)	Negligible (1)	Negligible (2)	Negligible (3)	Tolerable (4)
	Uncritical (1)	Marginal(2)	Critical (3)	Disastrous (4)
	Impact / Severity			

Risk-Category	Score	Action Required
Intolerable	15-20	Must be avoided or Impact must be mitigated as far as possible
Precarious	8-12	Shall only be accepted if the efforts for prevention and/or mitigation of impact is unreasonable high
Tolerable	4-6	Shall be accepted, but threat needs to be assessed regularly
Negligible	1-3	Shall be accepted

Figure 6: (a) Risk categories matrix of COUNTERACT with categories being colour highlighted, (b) Actions required based on risk-category (COUNTERACT, 2009)

The evaluation of potential measures against assessed risks is done by considering:

1. Cost of implementation
2. Effectiveness of measure (reduction of risk score)
3. Time of implementation
4. Potential additional benefits in safety
5. Insurance impact

COUNTERACT includes all steps of ISO 31000 regarding assessment and treatment of risk, with a semi-quantitative way (scoring matrices), based on informed decision making of policy makers in the organization, focused mainly on direct attacks against a specific sector. It is one of the first attempts to propose a structured way of assessing risks in EU's public transport critical infrastructures, after the 2004 terrorist attacks in Madrid.

1.4.3 EURACOM

European Risk Assessment and Contingency Planning Methodologies for Interconnected Energy Networks (EURACOM) project was focused on creating a holistic all hazards risk assessment methodological framework for policy makers of the energy sector CI. More specifically, EURACOM project investigates electricity, gas and oil energy sectors separately in regards to 4 steps of commodity flows: production, transmission, distribution and consumption. As found in EURACOM (2011), the 7 steps of the risk assessment methodology proposed are:

1. Set up holistic team with a holistic view
2. Define the holistic scope
3. Define risk assessment scales
4. Understand the assets
5. Understand the threat context
6. Review security/Identify vulnerabilities
7. Evaluate and rank risks

These steps are considered a wide framework suitable for higher level risk assessment such as the entire CI sector or nation, and not at an asset level. When it comes to the nature of threats to be analysed using this framework, EURACOM also proposes the analysis of cyber threats to the information and communication technology-based controls used in the CI, aiming to disrupt energy systems.

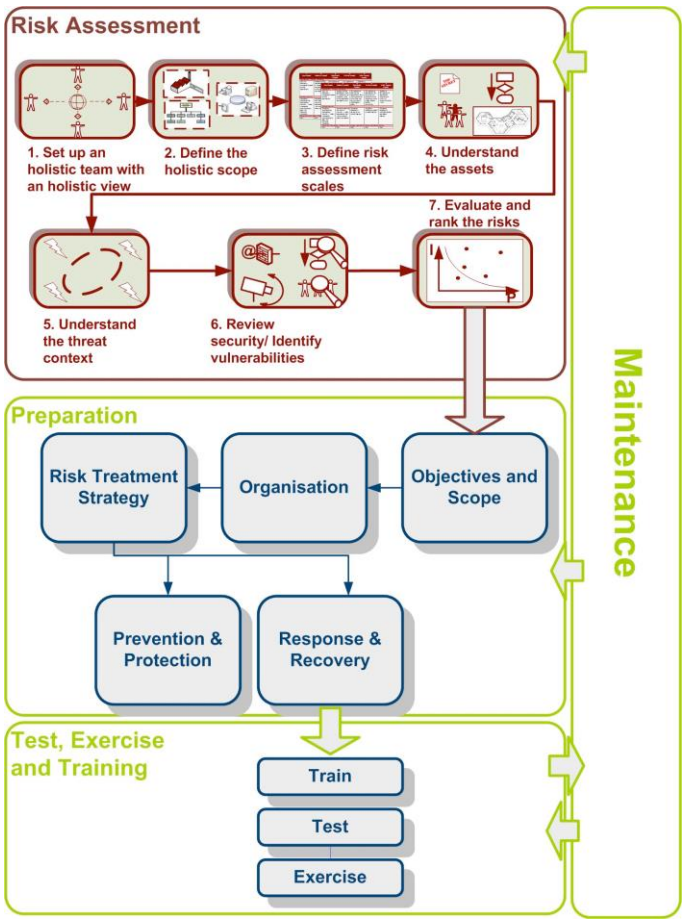


Figure 7: EURACOM Methodology for Risk Assessment and Contingency Planning (EURACOM, 2011)

In this framework, no resilience indicator is proposed (Giannopoulos et al., 2012). The framework includes all steps of Risk Assessment and Treatment in a general context.

1.4.4 BIRR

As part of the Enhanced Critical Infrastructure Protection (ECIP), Argonne National Laboratory developed Better Infrastructure Risk and Resilience (BIRR). It is a broad methodology facing risk and resilience in both natural and man-made hazards in many CI sectors (energy, transportation, water treatment etc.). Based on data collected from expert opinion, BIRR has developed a methodology that gives priority to measures mainly against deliberate attacks.

A database containing "what-if' scenarios is given in order to assess security of assets against identified threats. The methodology contains more than 1500 variables, covering major security components, aiming to assist policy makers identify and report critical vulnerabilities in multiple sector CIs.

Figure 8: BIRR user interface (Giannopoulos et al., 2012)

The process is based on 3 indexes. Based on the collected data from multiple sectors, Argonne has created the novel approach of Vulnerability Index (VI). VI was developed as an indicator for comparing vulnerabilities between different sectors and CIs under the same scenarios. Vulnerability Index is based on the Protective Measures Index (PMI), designed to increase as more measures are added. By including a Resilience Index (RI) (Giannopoulos et al., 2012), this methodology addresses resilience issues of CIs and provides the means to compare results and behaviours between different CI sectors.

1.4.5 CIPPS

Critical Infrastructure Protection Decision Support System (CIPDSS) is a pure risk assessment tool with a complete methodology that can be applied in all sectors concerning CIs (Giannopoulos et al., 2012; Stergiopoulos et al., 2016; Yusta et al., 2011). As it can be used in multiple sectors, it also takes into account their interdependencies and allows comparison of effectiveness of controls to reduce probability of risk scenarios using common metrics (fatalities, nonfatal injuries, economic losses, public confidence etc.). It is designed as a dynamic model, with continuous time-step simulation, and is used as a probabilistic optimization system based on informed decisions, taking into account the risk attitude of policy makers (Samsa et al., 2008).

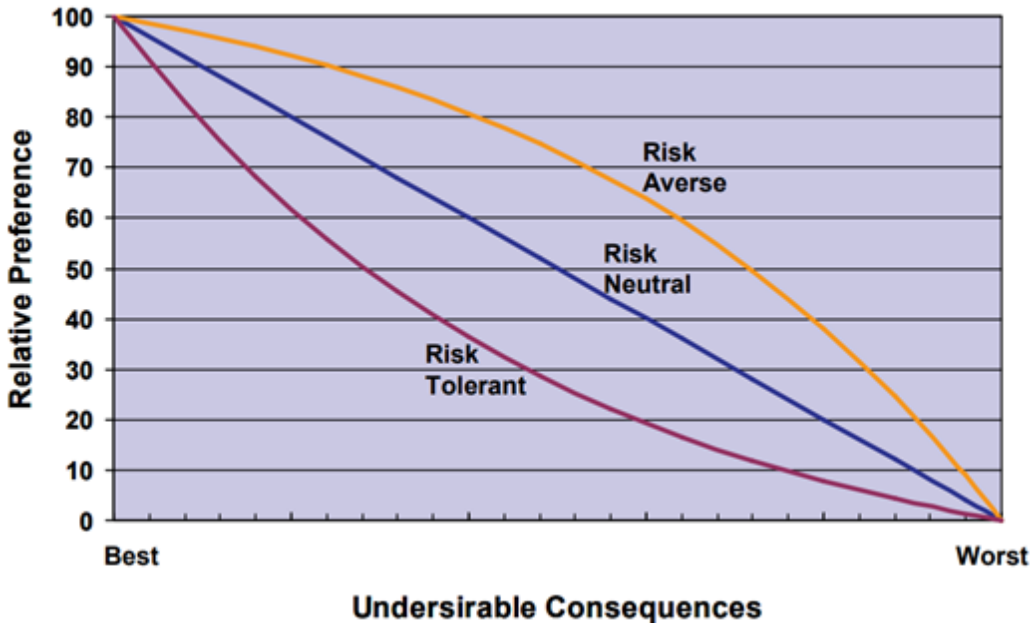


Figure 9: Decision maker's attitude to risk (Samsa et al., 2008)

One form of final output can be a set of scores for different counter-measures evaluation (satisfaction/regret curves), based on indexes based on "satisfaction" and "regret", summing up to an index of "Expected overall payoff" score. This provides the means to compare different measures under a specific risk attitude. It should be noted that CIPDSS does not report any resilience index or goal in its methodology.

1.4.6 SANDIA Methodology

Under the umbrella of National Infrastructure Protection Plan criteria, Sandia National Laboratory has developed an automated risk assessment tool for physical CIs (RAM tool).

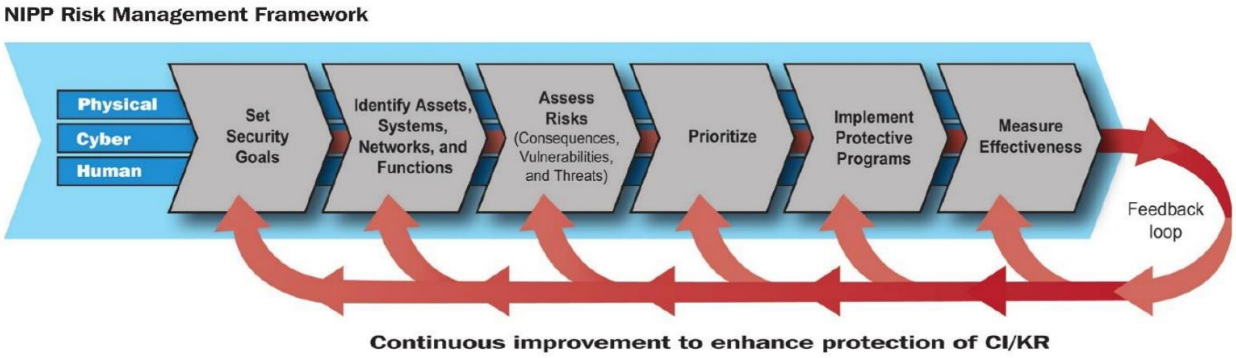


Figure 10: NIPP Framework schematic flow of processes

The scope of the analysis performed within this approach is clearly towards increasing resilience of, multiple sectors, CIs against deliberate attacks. The steps of the methodology are:

1. Threat definition and identification of undesired events and critical assets
2. Worst-case paths are analysed
3. Measurement of current security system effectiveness
4. Identification of vulnerabilities
5. Risk estimation
6. Recommendations for system upgrades, aiming at risk reduction from deliberate attacks

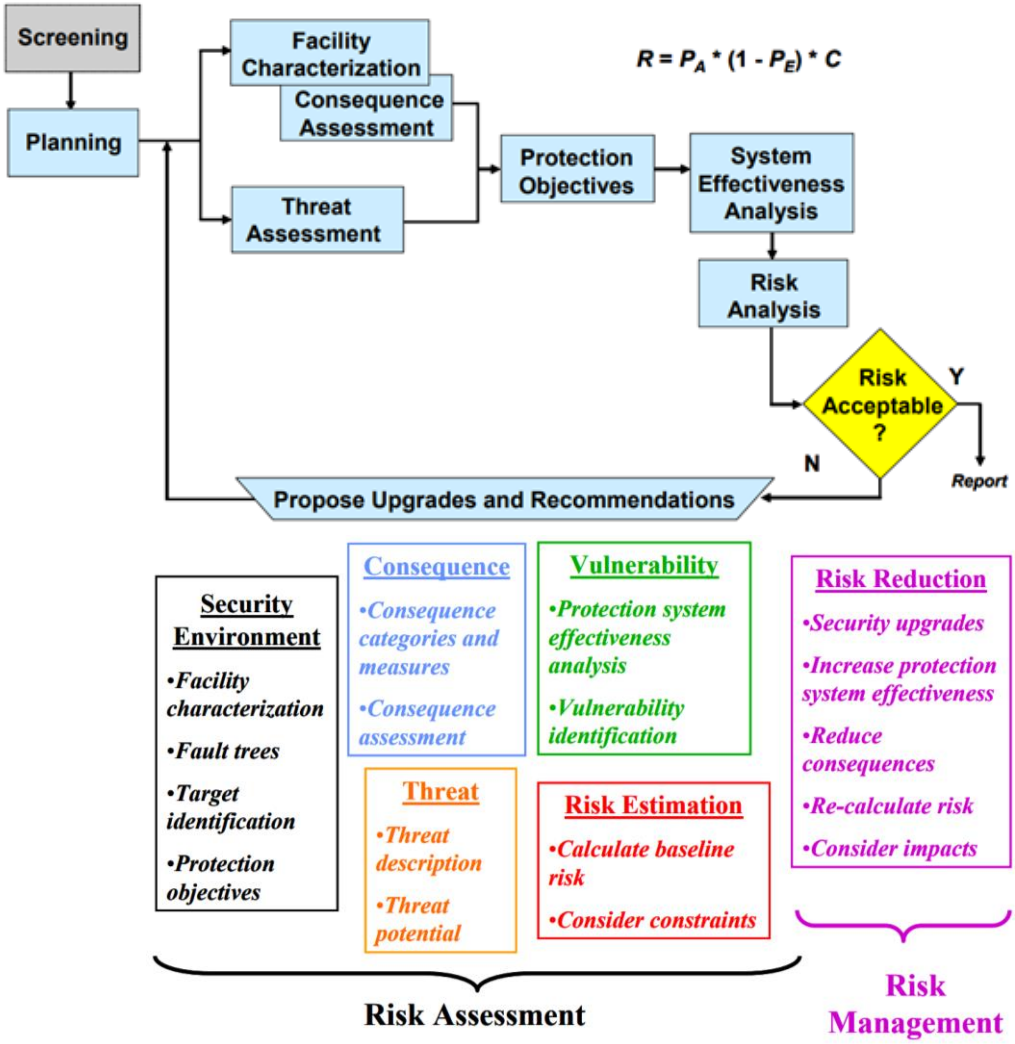


Figure 11: (a) Risk Assessment Methodology Process Flow Diagram (b) Major Modules in Risk Assessment & Treatment (Jaeger et al., 2008)

Risk is described as a function of "threat", "consequence" and "vulnerability", using the following equation:

$$R = P_A * (1 - P_E) * C$$

where:

R is the risk associated with the attack
P_A is the likelihood of the attack
P_E is the likelihood of successful measure against the attack (control effectiveness)
and C is the consequence

$1\text{-}P_E$ represents the probability that the attack is successful (vulnerability) (Jaeger et al., 2008). Since the focus of the methodology is on man-made threats, the estimation of a successful deliberate attack is a key indicator/parameter of the scenarios under investigation.

Risk is categorized, similarly to COUNTERACT, in a risk table based on vulnerability and consequences.

One of the key components of the methodology proposed by Sandia is the use of generic Fault Trees (FT), for which further information can be found in paragraph 1.4.11, based on the recognized undesired events. When the methodology is used for sector-specific analysis, those trees can be further customized to include lower-level details, as well as critical assets with site-specific attributes. Such approach gives the basis for an analysis with any desired resolution, based on recognized events and threats.

Using qualitative approach, consequences of all undesired states (top events of FTs) are presented through appropriate measures, based on expert opinion to determine the score and capturing all aspects of the nature of consequences. Such measures, as proposed (Jaeger et al., 2008), can be:

- Loss of life
- Serious injury
- Loss of critical mission/operations
- Duration of loss
- Economic loss (to the facility, to the community)
- Psychological impact
- National security impact
- Other, as specified by the facility

Similar to other approaches, deliberate attack threat potential is estimated through several parameters, including “interest in site”,” current surveillance” and “historic interest”, creating a specific profile for each threat scenario, according to the criteria of AWWA J100-10 (AWWA, 2010).

1.4.7 RAMCAP-plus

In 2009, American Society of Mechanical Engineers (ASME) developed and proposed Risk Analysis and Management for Critical Asset Protection (RAMCAP) methodology. It is an all-hazard approach (terrorism, naturally occurring events and interruptions), aiming to identify and prioritize protection of national CIs, in all sectors, by addressing protection and resilience against the identified threats. The entire process of assessment and treatment is focused on the most critical assets of the infrastructure.

The methodology proposed is implemented through a seven steps approach, visualized in Figure 4. Those steps are:

1. Asset Characterization: Identification of critical, to the functionality of the CI, facilities and assets
2. Threat Characterization: Asset specific identification of potential threats
3. Consequence Analysis: Estimation of the outcomes for all the above recognized threats

4. Vulnerability Analysis: Probability of threat considering the effectiveness level of existing measures of the system
5. Threat Assessment: Likelihood of the threat's actual realization
6. Risk and Resilience Assessment: Estimation of Risk and Resilience metrics
7. Risk and Resilience Management: Evaluation of measures based on risk-reduction and resilience values and implementation of satisfactory

Those steps serve as data-gathering and filtering processes, providing the necessary information for the overall assessment and treatment of the threats in the system, similar to the ISO 31000:2009 framework.

After recognizing the most critical assets (physical and/or cyber system elements, knowledge bases, suppliers etc.), the organisation must define threat scenarios, assisted by a list of generic reference threats, and apply a scoring system e.g. 1 to 5 or very low to very high for the consequence estimation. The assessment team is advised to aim at the highest possible consequence of each threat while expending the minimum resources of the attacker. An interesting approach in the consequence metrics is the use of the common "economic impact" indicator dually, besides the usual "fatalities", "injuries" etc. The economic impact of the organization (risk owner) is the standard approach to consequences, but RAMCAP-plus proposes also the use of "economic impact of the served community", demonstrating the severity of the lost functionality of the CI. Regarding the Vulnerability Analysis step, 4 methods are proposed within the methodology, similar to the AWWA approach, while 8 classes of vulnerability exist.

1. Direct expert elicitation: An evaluation team with adequate knowledge of the infrastructure make informed decisions on assessing the likelihood of the threats
2. Vulnerability Logic Diagrams (VLDs): Describes the flow of events and effects from the initial successful realization of a threat up to the final event associated with a specific likelihood estimate, considering obstacles and existing measures
3. Event trees (Fault Trees): The evaluation team estimates the likelihood of each "branch" of threats in a Fault Tree, based on the probability rules of the gates connecting the cascading events. "The sum of the probabilities of all branches on which the attack succeeds is the vulnerability estimate"(ASME-ITI, 2009)
4. Hybrid combinations of these

Terrorist attack threat likelihood is assessed through attributes such as "objectives", "capabilities", "facility attractiveness" and "asset vulnerability". ASME recognizes the lack of satisfactory method for terrorism risk estimation at asset level (ASME-ITI, 2009).

Table 2: RAMCAP-plus Vulnerability Scale table (ASME-ITI, 2009).

Bin		Decimal Description	Percentage Range (%)	Successes per Attempts
5	A	0.90 – 1.00	90 – 100	$9/10 \leq L \leq 1$
	B	0.75 – 0.89	75 – 89	$3/4 \leq L < 9/10$
	C	0.50 – 0.74	50 – 74	$1/2 \leq L < ¾$
4		0.25 – 0.49	25 – 49	$1/4 \leq L < ½$
3		0.125 – 0.249	12.5 – 24.9	$1/8 \leq L < 1/4$
2		0.0625 – 0.124	6.25 – 12.4	$1/16 \leq L < 1/8$
1		0.0312 – 0.0624	3.12 – 6.24	$1/32 \leq L < 1/16$
0		< 0.0311	<3.11	$L < 1/32$

Under the same legislative umbrella, RAMCAP-plus uses the same approach on risk calculation to Sandia Risk Assessment Methodology. Risk is the product of consequences, vulnerability and threat likelihood, while Resilience is calculated for both the risk owner and the community, as a product of economic impact, vulnerability and threat.

1.4.8 HAZOP

Hazard and Operability (HAZOP) is an examination study of existing processes, procedures and objectives of a system (ISO/IEC 31010:2009). It is used to identify potential threats from human, environment, equipment or organization actions by a qualitative approach of asking questions regarding the way objectives can be achieved, revealing potential risk sources to be registered. It can be applied by a team for simple or complex processes in many applications such as mechanical systems or organizations. The steps of a HAZOP study include the definition of the scope, the creation of a set of guidewords and assemble a team with appropriate technical expertise to detect and evaluate deviation from the normal status. The study results in a set of possible causes that lead to the identified deviation by the team. The main advantage of this method is its applicability to a large variety of systems and operations.

1.4.9 SWIFT

Structured What-if technique (SWIFT) was developed as an alternative of HAZOP, initially aimed to petrochemical infrastructures. The steps of this method include a questions and answers (Q&A) process on known risks, incidents, controls and constraints coupled with a "what-if" discussion on those topics. This creates a set of "scenarios" of potential events and causes for the team. Using a set of words or phrases of what-if type, stimulates the risk identification team to further investigate the system, processes and objectives to reveal potential threats. It is widely used to examine the alterations of potential risks and consequences by making changes in the existing system (ISO/IEC 31010:2009). The main advantage, similar to HAZOP, is its fast applicability to a variety of systems and organizations with the creation of a clear, simple, picture of the potential threats. As all "expert judgment" based identification techniques, SWIFT studies are difficult to identify complex and interrelated threats.

1.4.10 PHA

Preliminary Hazard Analysis aims to identify threats, risk sources and events that can have potential consequences to the infrastructure examined in a simple process. It is usually used as a generic first step in the Risk Assessment step to give an overview of the system and the potential consequences or prioritizing threats and risks for the analysis step (ISO/IEC 31010:2009). It also includes the qualitative analysis of consequences and the threat probabilities, creating a first set of information of the identified risks. This method is valuable in low or generic data conditions, usually in the early stages of a process, taking into account the equipment used, the operating environment and the interfaces of the system.

1.4.11 Fault Tree Analysis

Fault Trees are a logical structure of relationships/dependencies between events (Nai Fovino et al., 2009). The top event, also known as the undesired state of the system, shows the last "event" that can be derived if a sequence of lower-level events (contributors) are activated (through a Boolean logic approach). Top event is the starting point of the FT construction, moving downwards and analysing the potential causes of that event, tracing it back to the events that trigger it. The events between the undesired state and the event that triggers it are called intermediate. The intermediate events are connected through gates (logical gates of AND, OR, Exclusive OR etc.) between themselves and the lowest level events, called basic events. Basic events demonstrate the potential threats recognized, that trigger the failure path of the system.

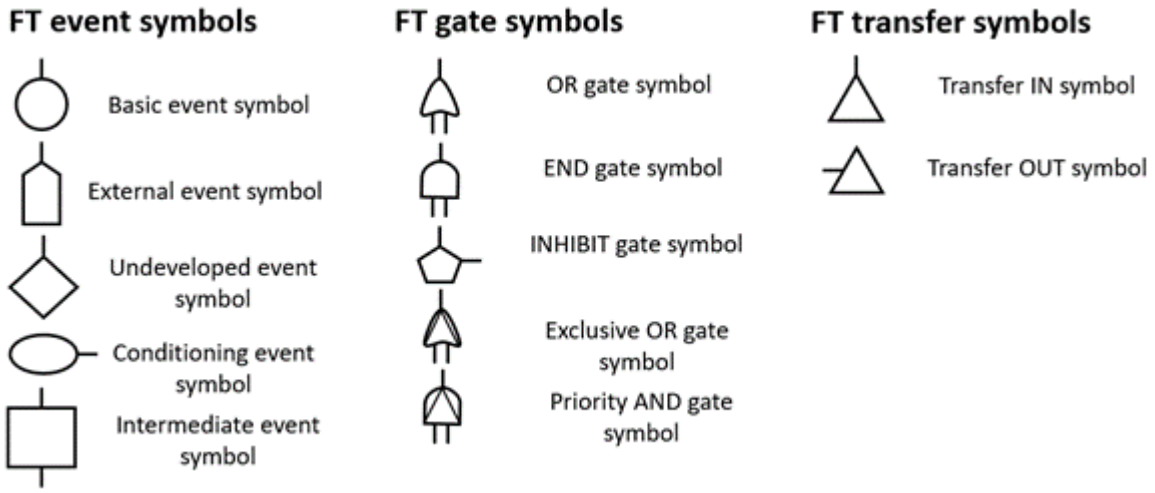


Figure 12: Commonly used symbols in the visualization of Fault Trees

Fault Trees can have multiple level of detail, as one FT can be used as an input (transferred) to a second one. This is a result of the complexity of the system analysed using the FTs, as this indicates a failure of a sub-system that leads to the failure of the system. Exploring the vocabulary of FTs, it is interesting to note the term Primary Fault. Primary Fault is a component failure that cannot be further defined at a lower level. Including Primary Faults in a Fault Tree of a CI is almost impossible and that level of detail can almost certainly be more

confusing than helpful. A Secondary Fault is a fault that can be further explained but is not defined in details, as there is no such need for the process.

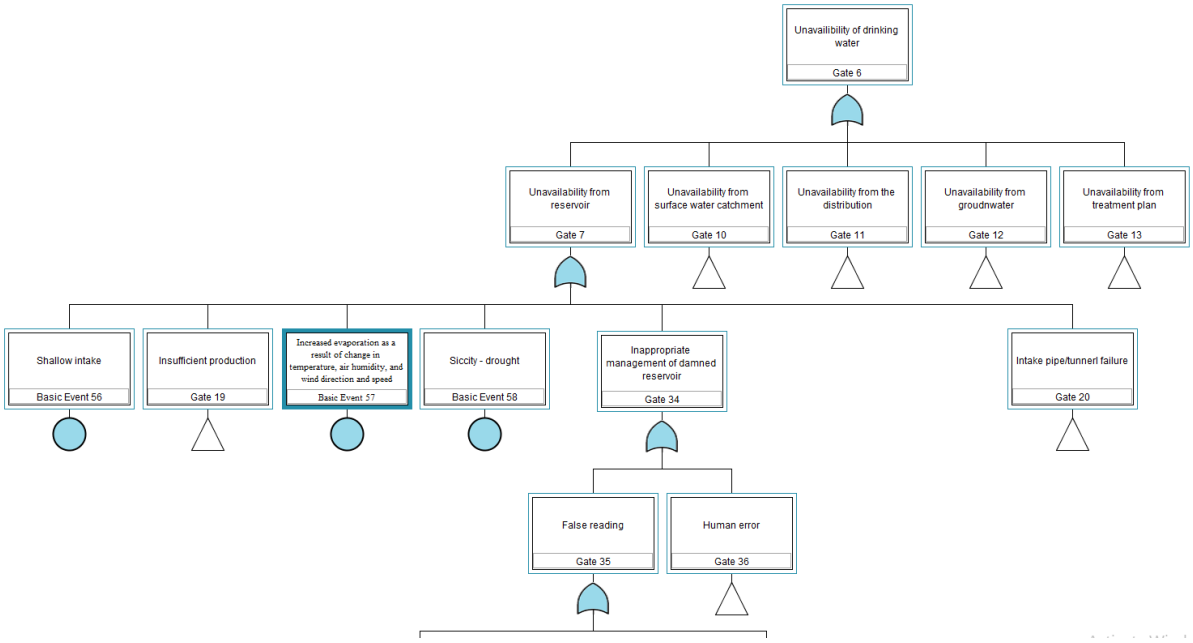


Figure 13: Part of the "unavailability of drinking water" FT created in PREPARED project, with a basic event highlighted

FTs take into account the probability of events and pass it through Boolean logic using the following formulas based on the gate:

- An AND gate:

$$P(A \text{ and } B) = P(A \cap B) = P(A)\,P(B)$$

- An OR gate:

$$P(A \text{ or } B) = P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

Fault Trees can be used in two ways. The first, and most obvious one, is the qualitative analysis in the risk identification process. This method allows the visualisation of interconnecting, usually cascading, events following an event. The visual structure of the events links the failure to its cause or causes. In addition, one event can be the cause of more than one failure, triggering a cascading event in a different subsystem. The second process that the FTA method is able to provide, is the quantitative analysis of the top event's probability of occurrence, provided that the basic events' probabilities are given. Boolean logic and the interconnected events give the FTA method its ability to further assist in the risk assessment process, as those top event probabilities "can be used to calculate risk in financial or other terms" (Ralston et al., 2007)

1.4.12 INFRARISK

The InfraRisk tool, a DECRIS project outcome (Utne et al.,2008), supports two levels of analysis. The first level the tool corresponds to a Preliminary Hazard Analysis (PHA). Risk is directly assessed by specifying frequencies and consequences. A predefined list of main events related to critical infrastructure is used as the seed. For each main event it is possible to link Societal Critical Functions (SCFs) that are relevant. These SCFs can be seen as generic components or functions in the critical infrastructure. The probabilities and the consequences of an event are influenced (at varying degrees) by one or more vulnerability factors defined by the user.

It is possible to perform a more explicit linking between the SCFs and the main event in the comprehensive analysis. Typically, such relations are established by Fault Tree Analysis (FTA), Reliability Block Diagrams (RBDs) and Event Tree Analysis (ETA). Some functionalities to support such analyses are available as separate sub-modules in the InfraRisk tool.

The InfraRisk tool supports risk analysis where the focal point is the so-called main events. Main events are describing the nature of the risk by structuring “What can go wrong?” in a hierarchical structure of events. The main events can be:

- Natural catastrophe (N)
- Technical event (T)
- Dysfunctional human behaviour (D)
- (Malicious) acts against nation, inhabitants, or interest (M)

Note that component failures are not a starting point of the analysis. Component failures are addressed by listing one or more SCFs related to a main event. The term “function” is used rather than “component” to emphasize that there are functions to be carried out, for example “pumping water”, “store water”, “control water flow” and so on. In most cases there are components installed to carry out these functions, i.e., pumps, water tanks and valves respectively. Note that there is a many-to-many relation between the main events and the SCFs. For one main event like Failure to deliver (critical infrastructure) (D) - Lack of water (1) - Waterworks and purification (2), there are seven associated SCFs: Coagulation, Filtration, Chlorination, UV, CO2, pH adjustment and Pumps.

1.4.13 FAIT

Fast Analysis Infrastructure tool (FAIT) was designed to define the significance and the interdependencies of CIs. The FAIT is based on expert opinion and knowledge, through a rule-based language that expresses the multiple infrastructures and their connection. The key element in dealing with interdependencies is the use of spatial data to determine the geographical interdependencies of infrastructures. It supports visualisation using Google Earth and interactive mapping tools (Kelic et al., 2008). It contains a large spatial database of CIs and their assets, enabling the site-specific assessment of threats to interconnected elements of the system. It also provides the ability to assess the economic impact of a

disruption in systems production continuity, taking into account the time to recover and the duration of the event (Giannopoulos et al., 2012).

1.4.14 VAMPG

Adding an interesting twist to the vulnerability assessment, under the scope of efficient military missions, RAND Arroyo Center created the Vulnerability Assessment Methodology Pocket Guide (VAMPG). What is commonly seen as a vulnerability assessment, is on the other side of the coin when it comes to prepare an attack, although VAMPG methodology can be performed under both aims, attack and/or protection.

When the behaviour of approach is supportive or non-hostile (protection), the methodology aims at identifying the most critical assets of one's system and/or friendly system, similarly to approaching the interdependencies of CIs. "The vulnerability assessment identifies physical characteristics or procedures that render critical assets, areas, infrastructures, or special events vulnerable to known or potential threats and hazards" (Schnaubelt et al., 2014). In order to assist the decision making of the vulnerability assessment, Department of Defence (DoD) has created some tools.

The first tool is the MSHARPP, which assesses personnel, facility or asset vulnerability through 7 characteristics/variables of the system, with a scoring system of 1 to 5 (lower to higher vulnerability or likelihood) for each.

1. Mission
2. Symbolism
3. History
4. Accessibility
5. Recognizability
6. Population
7. Proximity

The final value of vulnerability is the total of the scores for each variable applicable to the threat examined.

The second approach is the CARVER scoring system, developed by the U.S. Special Forces. CARVER stands for Criticality, Accessibility, Recuperability, Vulnerability, Effect and Recognizability which are the 6 criteria examined under the viewpoint of the attacker to assess the vulnerability of an asset, infrastructure or action of the system. The scoring can range to the needs of each study (1-5, 1-10 etc.), as long as the qualitative aspect remains the same, i.e. higher value signifies higher vulnerability.

Table 3: Example of MSHARPP vulnerability score matrix (Schnaubelt et al., 2014)

Target	M	S	H	A	R	P	P	Total	Threat Weapon
Headquarters building	5	4	5	1	3	4	1	23	4,000-pound, vehicle-borne improvised explosive device
Troop barracks	2	4	5	4	4	4	2	25	220-pound, vehicle-borne improvised explosive device
Communications center	5	4	2	3	5	3	1	23	4,000-pound, vehicle-borne improvised explosive device
Emergency operations center	3	3	2	4	4	4	2	22	50-pound satchel charge
Fuel storage facility	4	3	1	5	5	1	3	22	Small-arms ammunition and mortars
Airfield	5	5	3	2	5	5	4	29	Mortars and rocket-propelled grenades
Ammunition supply point	5	5	1	1	5	3	1	21	Small-arms ammunition and mortars
Water purification facility	5	2	3	5	5	0	4	24	Chemical, biological, and radiological contamination

Table 4: Example of CARVER vulnerability scoring with a range of 1 to 10 for each criterion (Schnaubelt et al., 2014)

Invulnerable to all but the most extreme targeting measures.	1
Effect (on the population)	
Overwhelming positive effects, but no significant negative effects.	10
Moderately positive effects and a few significant negative effects.	8
No significant effects and remains neutral.	6
Moderate negative effects and few significant positive effects.	4
Overwhelming negative effects and no significant positive effects.	1
Recognizability	
Clearly recognizable under all conditions and from a distance and requires little or no personnel training for recognition.	10
Easily recognizable at small-arms range and requires little personnel training for recognition.	8
Difficult to recognize at night during inclement weather or might be confused with other targets or target components. Some personnel training required for recognition.	6
Difficult to recognize at night or in inclement weather (even in small-arms range). The target can easily be confused with other targets or components and requires extensive personnel training for recognition.	4
The target cannot be recognized under any conditions, except by experts.	1

Criteria	Relative Value Rating
Criticality	
Immediate output halt or 100 percent curtailment. Target cannot function without asset.	10
Halt less than 1 day or 75 percent curtailment in output, production, or service.	8
Halt less than 1 week or 50 percent curtailment in output, production, or service.	6
Halt in more than 1 week and less than 25 percent curtailment in output, production, or service	4
No significant effect.	1
Accessibility	
Standoff weapons can be deployed.	10
Inside perimeter fence, but outdoors.	8
Inside a building, but on a ground floor.	6
Inside a building, but on the second floor or in basement. Climbing or lowering is required.	4
Not accessible or only accessible with extreme difficulty.	1
Recuperability	
Replacement, repair, or substitution requires 1 month or more.	10
Replacement, repair, or substitution requires 1 week to 1 month.	8
Replacement, repair, or substitution requires 72 hours to 1 week.	6
Replacement, repair, or substitution requires 24 to 72 hours.	4
Same-day replacement, repair, or substitution.	1
Vulnerability	
Vulnerable to long-range target designation, small arms, or charges (weighing 5 pounds or less).	10
Vulnerable to light antiarmor weapons fire or charges (weighing 5 to 10 pounds).	8
Vulnerable to medium antiarmor weapons fire, bulk charges (weighing 10 to 30 pounds), or carefully placed smaller charges.	6
Vulnerable to heavy antiarmor weapons fire, bulk charges (weighing 30 to 50 pounds), or special weapons.	4

1.4.15 NSRAM

Network Security Risk Assessment Modelling (NSRAM) is a two level approach toolset developed by the James Madison University CIPP team (Baker et al., 2003). CI failure modes due to unintentional or intentional threats (accidents, aging or deliberate attacks and sabotages) are addressed at both cyber and physical level. In order to grasp the potential propagation effects of a seemingly isolated and/or not major threat, both approaches of NSRAM focus on the networked architecture of flows (energy, water, transactions or commodities flow networks).

The first approach of probabilistic risk assessment is the implementation of links between systems, subsystems, assets or networks demonstrating the hierarchy and connectivity, through Fault Trees. Since FTs demonstrate a steady relationship between events at a given time, NSRAM upgrades the analysis. By inserting the time dimension in the FT Analysis, system functionality, response and repair time are taken into account, providing a more dynamic (in comparison to the steady-state initial FTs) approach. Since time is crucial, if a CI's efficiency is reduced, this scenario aspect propagates to the estimated likelihood and seriousness of consequences estimated. Based on those metrics, decision makers can decide on the adaptation of additional measures to reduce risk (probabilities of failure) or accept them, and rely on the emergency response plans (Baker et al., 2003). FTs can be the result of an analysis of System Functional Diagrams, that illustrate the connected elements and the inner-dependencies of the network examined. Under a basic Monte Carlo simulation, probabilities of time *(t)* out-of-service events and the corresponding costs, are used to estimate the Loss Value metric.

$$LossValue = \int_0^t P_o(t) * C(t)dt$$

The second approach of NSRAM is that of network flows simulation. In this approach any CI, network of and interdependencies between flow structured sectors can be simulated. As seen by Baker et al. (2003), information flow as bits through optic fibres or wireless networks, water flows through WDNs, money through the banking network etc. In that context a simulation based on the simple rules of transmitting, storing, transforming, computing and receiving flows through ports can model the complex flow networks of multiple and interconnected CIs. This can be done either in a continuous or discrete step.

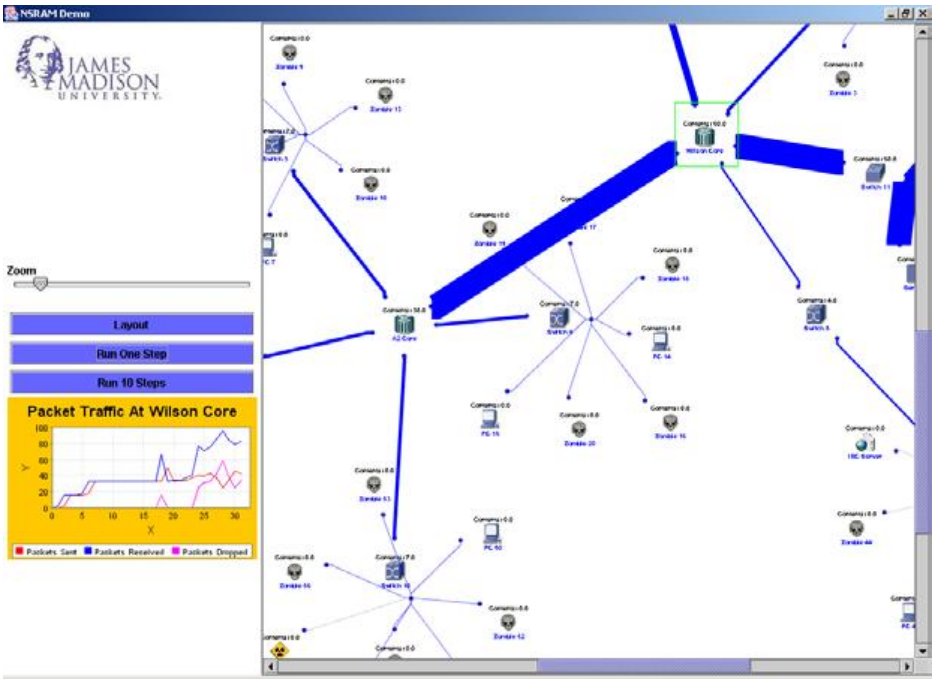


Figure 14: NSRAM tool with highlighted node (Baker et al., 2003)

Overall NSRAM innovation was designing a tool to indicate the system's performance with risk metrics based on the time parameter of the threat and response under the Fault Tree approach, assessing risk and identifying the most critical failure modes.

1.4.16 WISE

The Water Infrastructure Simulation Environment (WISE) project, is an analytical framework, developed by Los Alamos National Laboratory, in order to simulate water infrastructures (water distribution, wastewater network and stormwater systems) in the context of interdependency. The simulation is done in regards to the infrastructure stability after a damage event (McPherson and Burian, 2005). The interdependency of the water sector infrastructures corresponds with the CI sectors of power grid, natural gas and others.

The main advantage of the WISE approach is the initial construction of the water sector's internal interdependency and the unified simulation as a linked infrastructure rather than 3 autonomous systems. This provides a more holistic view of the water cycle within the structures of modern society and the complex man-made environment it grows on.

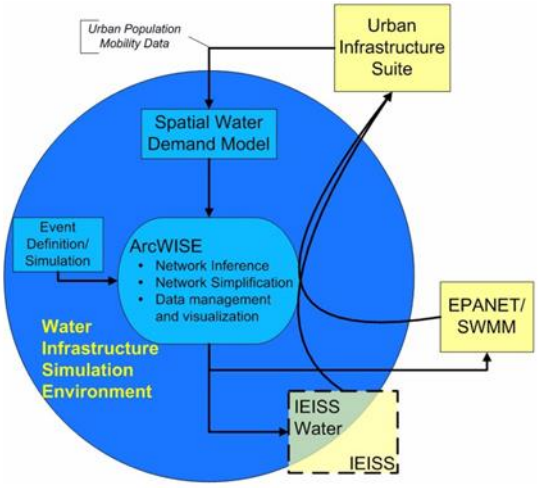


Figure 15: WISE Analytic Framework graphical representation (McPherson and Burian, 2005)

The WISE framework supports both asset and interdependency evaluations of the water system, integrating spatial information with hydraulic and/or interdependency analysis tools. In that direction, ArcWISE tool was developed, which is a GUI based on ArcGIS that enables additional level of analysis and overview of the infrastructure. It can be used to enhance the data for the hydraulic analysis (e.g. attribution of network components, simplification of the network etc.). ArcWISE can also be used to estimate the necessary input data, i.e. water demand and sewage production, based on "customer geolocations, water use coefficients and time patterns, and population mobility" (McPherson and Burian, 2005).

The second tool developed under the same scope is the IEISS Water software, as an extension of the Interdependent Energy Infrastructure Simulation System (IEISS) software. It simulates the physical behaviour (input-output-actions) of a system while including interdependencies at transmission level, in a dynamic, non-linear way, under various scenarios. IEISS is a tool that assists the steps of risk identification, vulnerability assessment and evaluation of controls by modelling critical assets of the network as "a corresponding physical, logical, or functional entity […] with sufficient attribution to represent its real-world counterpart" (McPherson and Burian, 2005). The key attribute of this tool is the ability to screen the study area under 2 classes, the service and the outage areas, giving a visual representation of the geospatial effects of a scenario to the network's services.

1.4.17 TEVA

The Environmental Protection Agency (EPA) has developed the Threat Ensemble Vulnerability Assessment (TEVA) Framework (Murray et al., 2012), taking into great consideration the complexity of the water sector's CIs and the need to take more actions towards the vulnerability of accidental or intentional contamination of potable water. TEVA was developed in order to take into account the non-deterministic dynamic nature of the WDS, accordingly creating a probabilistic environment for its vulnerabilities as well.

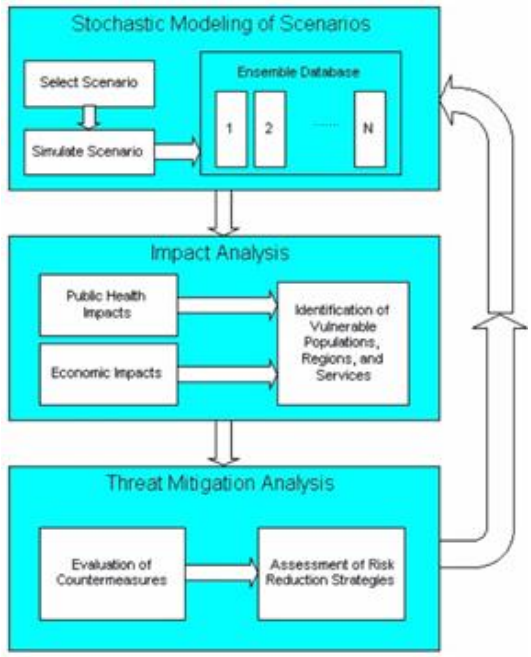


Figure 16: Threat Ensemble Vulnerability Assessment Framework's major components and flow (Murray et al., 2012)

An infinite number of possible scenarios can be created by accounting for the complexity of the network, the vast number of potential points of entry for a contaminant, the various compounds and concentration that can be used, the time and duration of the attack or accident and many more real-world attributes create. In order to assess the vulnerability of the system, TEVA proposes the probabilistic environment of an adequate number of scenarios, stored in the Ensemble Database, as shown in the figure above.

Each scenario of the Ensemble Database is simulated by the system model, in respect to both quantity and quality of supplied water. The results of the above set of simulations provide the input for the Impact Analysis step, where public health and economic impacts for each scenario are assessed. Threat Mitigation step includes the evaluation of existing countermeasures in addition to the typical process of creating a risk reduction plan. The key point of the TEVA framework is the priority it gives to the analysis of distribution network vulnerability with a special focus on contamination events.

As a step towards safer from contamination WDN, EPA developed the TEVA-SPOT (Sensor Placement Optimization Tool). It has been deployed in order to design the optimal sensor's network layer in water utilities via two major processes, the modelling and the decision-making process (Berry et al., 2012). The modelling process is conducted under 5 specific attributes of the implication goals.

1. Description of sensors' characteristics: The type of sensor, sampling process and/or detection limits etc.

2. Definition of the design threat: A contamination scenario with specific contaminant injection identity, density, time, location and customer behavior.

3. Selection of impact measures: It can be a set of metrics such as “number of people exposed”, “volume of contaminated water consumed”, “length of contaminated pipes” etc. (Berry et al., 2012)

4. Planning response to sensor detection: Actions to be taken or time aspect of identification and verification of contamination

5. Identification of feasible sensor locations: User defined parameter, including the choice of fixed sensor’s location

1.5 Cyber-physical layer modelling and testbeds

SCADA systems are vital to the operations of CI in a society, thus their protection against cyber-attacks should be a priority considering the multiple vulnerabilities associated with their hardware and software components. There is a need to analyse security risks of a specific SCADA system and develop applicable security measures and solutions to minimize risk and impacts of an attack. Real SCADA systems cannot be easily utilized for cyber-security experiments, as any interruption in their operation is totally unacceptable since these systems control critical infrastructure (Queiroz et al., 2011). However, testing a replica of a real SCADA system is cost-prohibitive and impractical due to the high prices of the specialized software/hardware involved and also their large scale. Therefore, models of the real SCADA system installed in a CI must be created and then tested against simulated threats. Due to their complex cyber-physical nature, there is difficulty in creating a unified generic methodology and tools for SCADA/NCS systems in order to provide cyber-physical stress-testing platforms and many researchers in literature try to address this with modelling frameworks.

Generally, the cyber element is modelled through two paradigms: emulation/virtualization (i.e. setting up virtual instances of the complete cyber network and their operation) and simulation (a more abstract way of modelling the behaviour of the individual components) (Chertov et al., 2006). Simulation is a less sensitive and detailed modelling paradigm but is generally faster, simpler and easier to set up than emulation. A SCADA simulation/emulation framework would enable the creation of integrated models of SCADA systems (along with the physical system) with the additional benefit of testing real attacks and trying different security solutions. Several tools/frameworks/platforms have been proposed and tested in literature and are summarized in Table 5. Three features are considered necessary:

a. Ability to simulate/emulate standard control system devices, such as RTUs, PLCs, IEDS
b. Ability to emulate/simulate standard networking and communication protocols between devices, including connection over Internet (IP Protocols), as well as standard SCADA protocols (e.g. Modbus, DNP3)
c. Ability to connect its elements with a physical model (e.g. EPANET)

Furthermore, the elements of Table 5 are categorized as:

CS – (Embedded) Control Systems models, SIMULINK-like, where the focus is on modelling control units.

NS – Network Systems Simulation models, where the focus is on network protocols simulation (packet simulation-modelling).

NS.CS – Combined model that includes network and control system simulation.

Table 5: List of tools/platforms for cyber-physical systems simulation or emulation

Modelling Environment	Features:			Possible pitfalls:	Category	Availability	Source
	a	b	c				
SCADAvt	Yes	Yes	Yes	Is based on CORE, many dependencies, only Modbus and DNP3 Protocols	NS.CS	Open	(Almalawi et al., 2013)
SCADASim	Yes	Yes	?	Based on OMNet++, simulation of Control units with Simulink	NS.CS	Open	(Queiroz et al., 2011)
VCSE	Yes	Yes	Yes	Very limited documentation about its case studies/use	NS	Commercial	Sandia
JRC-EPIC	Yes	Yes	Yes	Primarily used for scenario-based microscale modelling of CPS.	NS.CS	Open	(Siaterlis et al., 2013)
Modelica	Yes	Ltd	Ltd	Embedded control systems modelling tool	CS	Open, some libraries commercial	(Tang Junjie et al., 2012)
TrueTime (MATLAB)	Yes	Ltd	?	Limited support for network simulation. Possible limitations for physical systems integration.	CS	Open	(Cervin et al., 2003)
Ptolemy (Java)	Yes	Ltd	Ltd	Embedded control systems engineering tool, limited simulation of network protocols and physical parts.	CS	Open	https://ptolemy.berkeley.edu/
OMNet++ (C++)	Ltd	Yes	?	Networks simulation software, packet-level simulation of protocols, limited in its integration	NS	Open	https://omnetpp.org/

				with control and physical units.			
Ns-2 (C++)	?	Yes	?	Networks simulation software, packet-level simulation of protocols, limited in its integration with control and physical units.	NS	Open	https://www.isi.edu/nsnam/ns/
PiccSIM (MATLAB-SIMULINK)	Yes	Yes	?	SIMULINK + Ns-2 combined control/network model Possibly limited in its integration potential with physical parts.	NS.CS	Open also has an extension for TrueTime	http://wsn.aalto.fi/en/tools/piccsim/
NCSWT	Yes	Yes	?	Ensemble of control models used for networked control systems, limited use for physical systems, complicated architecture	NS.CS	Not directly available	
iSEE	Yes	Yes	?	Network emulation + control system simulation combination model	NS.CS	Website down. Presently not directly available	
OpenPLC	Yes	Yes	?	Fully functional standardized open source PLC (software and hardware). Is a framework for industrial cyber security research	NS.CS	Open	https://www.openplcproject.com/
epanetCPA	Ltd	No	Yes	Open-source object-oriented MATLAB® toolbox for modelling the hydraulic response of water distribution systems to cyber-physical attacks	CS	Open	(Taormina et al, 2016)

Some of the most promising tools identified for modelling the cyber elements pf CPS are discussed briefly in the following section, whereas Table 6 sums up the purpose of each tool with regards to the ISO steps and focus, following the same structure as Table 1.

Table 6: Promising tools for cyber-physical layer modelling

Name	Approach	Purpose	Water sector CI	Focus
Cyber-physical layer modelling				
OpenPLC	Cyber Physical simulation	Risk Identification and Risk Analysis	✓	Mainly deliberate attacks
SCADAVT	Cyber Physical emulation	Risk Identification and Risk Analysis	✓	Mainly deliberate attacks
SCADASim	Cyber Physical simulation	Risk Identification and Risk Analysis	✓	Mainly deliberate attacks
epanetCPA	Cyber Physical simulation	Risk Analysis	✓	Mainly deliberate attacks

1.5.1 OpenPLC

OpenPLC is an open-source Programmable Logic Controller that is based on an easy to use software. It includes a program development environment, supports popular SCADA protocols such as Modbus/TCP and DNP3, and also includes an open source Human Machine Interface (HMI) editor called ScadaBR. The OpenPLC project was created in accordance with the IEC 61131-3 standard, which defines the basic software architecture and programming languages for PLCs. This means that OpenPLC can be programmed in any of the five standardized languages: Ladder Diagram (LD), Function Block Diagram (FBD), Structured Text (ST), Instruction List (IL), and Sequential Function Chart (SFC). Since the early 70s, PLC (Programmable Logic Controller) has dominated industrial automation by replacing the relay logic circuits. OpenPLC is mainly used on industrial and home automation, internet of things and SCADA research ("Hackers Arise!: SCADA Hacking: SCADA/ICS Communication Protocols (Modbus)," 2017). The interface of OpenPLC is presented in Figure 17.

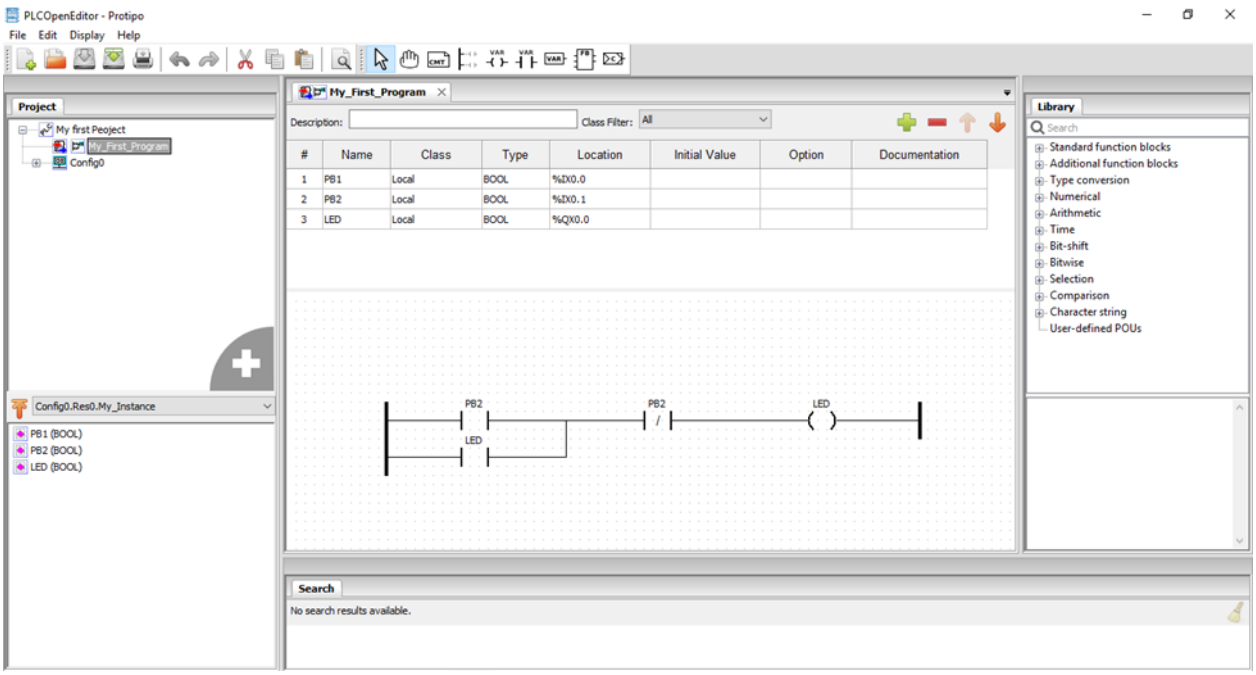


Figure 17: OpenPLC - Ladder Diagram (LD) programming interface

1.5.2 SCADAVT

SCADAVT is a user-friendly interface able to create SCADA systems based on the CORE emulator. It is also able to connect to real SCADA devices for evaluation. SCADAVT uses the Modbus protocol and extends CORE functionality with the implementation of new components: Modbus/TCP slave and master simulators and Modbus/TCP HMI server. Using the DLL of EPANET, the user is able to simulate the effects of cyber-attacks to the physical system via scripting the output of SCADAVT (Almalawi et al., 2013).

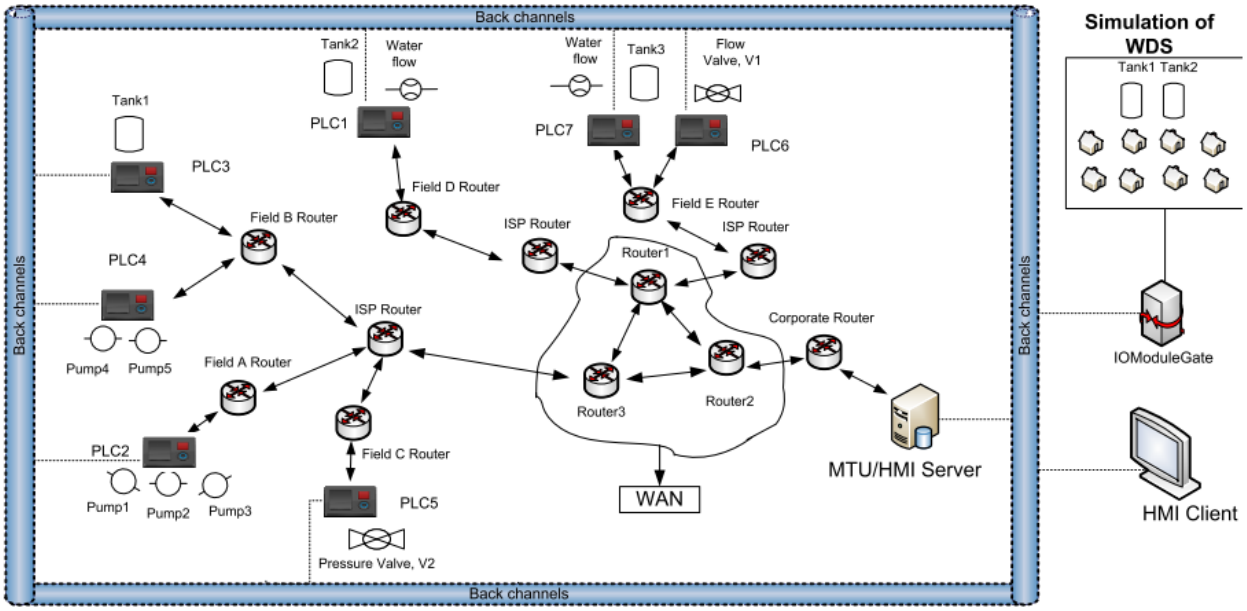


Figure 18: SCADAVT schematic of cyber layer assets and WDN connection (Almalawi et al., 2013)

1.5.3 SCADASim

SCADASim is based on the OMNET++ simulation environment and also allows real world devices to be attached to the simulator. Its architecture consists of the following abstract classes that extend OMNET++ functionality: SSScheduler that sends and receives messages to /from the environment, SSGate that implements a Protocol (Modbus, DNP3, HTTP) and the SSProxy that simulates a device such as a Programmable Logic Controller (PLC) or an Remote Terminal Unit (RTU). Devices can be simulated by Simulink functions. SCADASim allows the testing of various cyber-attacks on the behaviour of the simulated SCADA system.

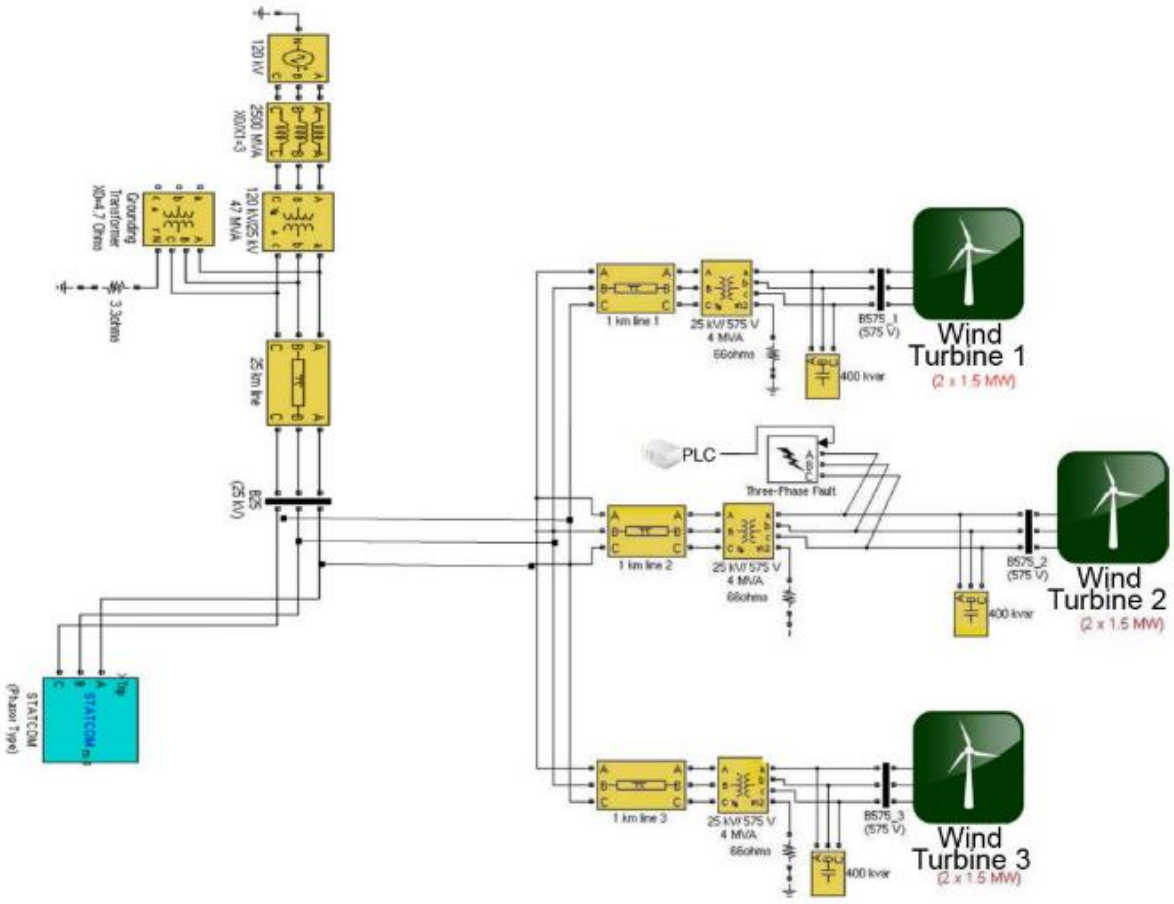


Figure 19: SCADASIM interface with connected elements of the model (Queiroz et al., 2011)

1.5.4 epanetCPA

EPANET2 (Rossman, 2000) is a free licence program designed and distributed from Environmental Protection Agency (EPA) capable of simulating hydraulic systems under pressure such as Water Distribution Networks. Through a Users' Interface, the user can create a network topology or modify an existing one, prior to simulation. The "assets" included in the model are:

- Reservoirs
- Tanks
- Pipes
- Pumps
- Valves
- Emitters
- Junctions (demand nodes)

A set of attributes is associated with each asset, including a unique ID and location information (X, Y, Z). EPANET is a widely accepted tool based on a demand-driven approach in the hydraulic simulation of the distribution networks. Extensions to EPANET such as

EPANET-MSX and PDX have been developed in order to solve previous limitations of the model with regards to multiple agent interaction and pressure driven hydraulics. The latter is a key progress in hydraulics simulation since the demand-driven approach, which EPANET originally uses, poses limitations in low pressure condition simulations (Chmielewski et al., 2016). This is due to the fact that in demand-driven modelling "consumer demands are always satisfied regardless of the pressure" (Taormina et al., 2016).

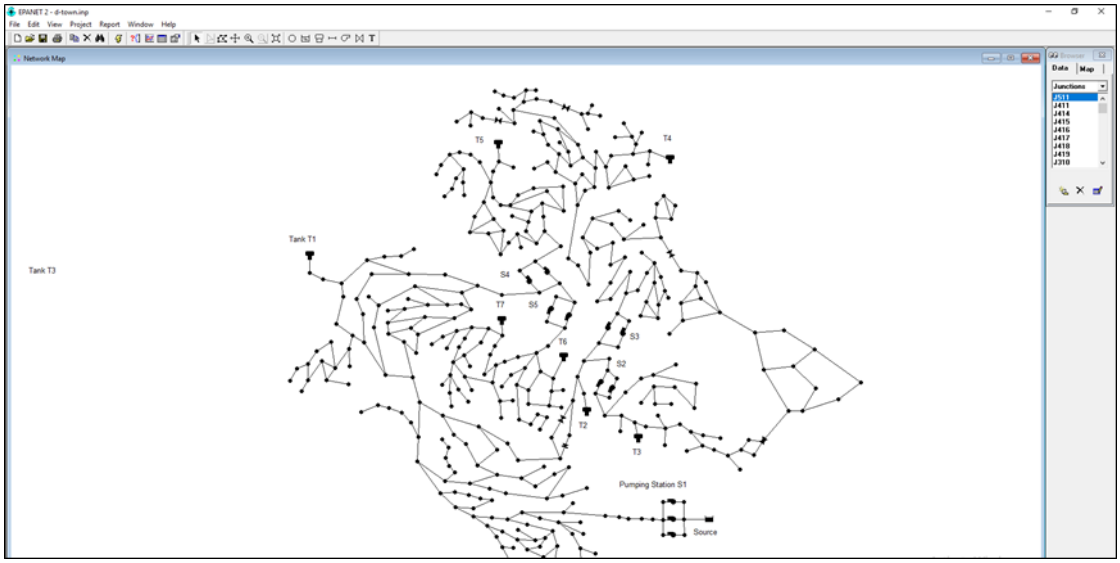


Figure 20: EPANET interface with C-Town network example

The OpenSource EPANET Initiative was established in 2015, promoting the interested parties (academics, industry etc.) to continue development and enhancement of the tool. Eliades et al. in 2016 presented an open-source software to establish a well-organised interface between EPANET and Matlab, allowing the transfer of the programs capabilities from a standalone software to a programming environment researchers use for evaluation of new methodologies (Eliades et al., 2016).

The first attempt to model cyber-physical attacks on WDNs using EPANET was done by Taormina et al. (2016), by altering control statements in the network. In 2017 Taormina et al. contributed further to the subject of hydraulic modelling of cyber-physical attacks by developing the epanetCPA toolbox. In order to model cyber-attacks with a physical expansion, epanetCPA uses an input file (.cpa expansion) that contains connectivity information between PLCs, sensors and actuators. The .cpa file also contains the "attack" information and the control changes to be implemented in the system as part of the cyber-attack. The epanetCPA does not have a UI, but a rather structured way of importing the attack scenario to the simulator that utilizes the EPANET dll the EPANET Matlab interface.

The latest version of epanetCPA can simulate (Taormina et al., 2018):

- 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
- Attack on communication

In addition to the multiple CP attack modes available and the system's control override, a quasi-dynamic pressure driven analysis capability was added to the toolbox, allowing the users to select between a demand-driven and a pressure-driven option by setting appropriate parameters in the .cpa file.

1.6 Agent Based Models

The complex adaptive nature of the socio-technical interactions of the urban water system is better modelled using Agent Based Modelling (ABM) as proposed by several researchers (Borshchev and Filippov, 2004; Koutiva and Makropoulos, 2016; Nilsson and Darley, 2006; Railsback, 2001; Tesfatsion, 2003; Van Dam et al., 2012). Similarly, the emergent need of simulating complex cyber-physical systems resulted in ABM application within risk management processes.

Agent Based Modelling is a computational intelligence application that is based on agents which are "computer systems situated in some environment, capable of autonomous action in this environment in order to meet its design objectives" (Wooldridge, 1999). Agents consist of states and rules and have clearly defined boundaries and interfaces (van Dam et al., 2013). They are able to act on their own based on the input they receive from both their environment and other agents and these actions may alter their own state or that of the environment or even of other agents based on the behavioural rules they follow (Van Dam et al., 2013). ABM reduces the complexity of a problem by representing a system using sub-groups, associating an independent intelligent agent to each group, providing rules for action to each agent and coordinating their activities and interactions (Bousquet et al., 1999). Agent based modelling (ABM) may address problems that concern emergence arising from interactions between a system's individual components and their environment (Grimm and Railsback, 2013).

Agent Based Modelling may be applied to enhance the capabilities of risk assessment to estimate the likelihood of successful threats to avoid the use of subjective opinions. The agents are able to follow given rules and define their autonomous behaviour thus allowing us to explore the relationship between the CPA and the target. It is thus possible to define environment rules and links that may be described using FTs, in order to extract emergent behaviours using ABMs that allow to define likelihood of threats. The following examples present some ABMs developed to deal with this type of problems.

Based on Burns et al. (2017) information systems security can be regarded as complex adaptive system and the role of humans in security efforts may be simulated using ABM to exhibit system-emergent properties. To prove this, they designed three different ABMs, where the first one dealt with phishing attacks credibility, aiming to determine the probability that a user will be phished, and the second and the third ABM were built to map the overall security of the information system as the proportion of secure to insecure patches. This work proved the applicability of ABM to information systems security and the need for sensitivity analyses to examine the parameters of ABMs showcasing in their examples the influence of population parameters (e.g., culture) and environmental parameters (e.g., hostility) on the effectiveness of information security approaches.

An ABM was created by Sandia National Laboratory in 1997, to identify and assess risks through the interdependencies of the banking sector and the telecommunication infrastructures, called CommAspen. In addition, CommAspen can perform analyses of cross-sectoral cascading effects (effects of telecommunication sector disruption on the economic sector) by modelling the behaviour of the sectors as integrated layers (Giannopoulos et al., 2012). Additionally, this tool assesses economic impacts of threats and measure effectiveness of the security, without addressing resilience (Barton et al., 2004).

As an enhancement of CommAspen, collaboration between Sandia and Los Alamos under a common contract with NISAC (National Infrastructure Simulation and Analysis Center), produced the N-ABLE (Agent Based Laboratory for Economics) tool. The tool models the complex dynamics and interdependencies between economic and multiple infrastructure sectors. N-ABLE focuses on the identification of the most vulnerable sector to loss of infrastructures' functionality. While CommAspen only focused on telecommunication sector to economic, N-ABLE simulates and assesses vulnerabilities of multiple sectors, even with supply-chain structure (Eidson and Ehlen, 2005). More on the technical aspect can be found in Eidson and Ehlen (2005) overview of N-ABLE. As a summary, those tools only refer to vulnerability and consequence assessment and interdependencies of CIs. In that scope, used as a part of a Risk Assessment and Treatment approach, it can produce the much-needed information towards a holistic and more resilient management of threats.

Eom et al. (2008) designed a cyber-attack model to assess the vulnerability of a network. The aim was to identify the weakest point of the network and inspect security policy. The tool estimates attack success percent taking into account the ratio of all successful events that affect a sub-node over all nodes of the attack tree. The model simulates Intelligence, Surveillance and Reconnaissance (ISR) Agents and Attack Action (AA) Agents. AA are able to behave autonomously based on the set target system environment and attack process that are provided as a what-if scenario tree. AA main aim is to find the weakest point and attack there first before ISR agents are able to intersect them.

Chapman et al. (2014) created an ABM of an abstract hide-and-seek game as an allegorical simulation of the problems of attack attribution and attack pivoting in the cyber-attacks domain. The hider simulates the attacker, who has strategies regarding the attractiveness of the nodes of choice and might be biased regarding the course of hiding places. Additionally,

the seeker simulates the security, and tries to find the hider by traversing an Euclidian Path or engage in a random walk. The seeker aim is to find the hider by understanding the hider's strategies and biases which are facilitated through the recording of a hider's behaviour and the production of predictive information regarding the hiding strategy. In this study the strategies of the hider and the seeker are not dynamically connected, however the researchers identify the requirement for evaluating the dynamic co-evolution and co-adaptation of strategies.

The above ABMs present an example of available tools that explore effects such as the likelihood of an attack to a network, the strategies of attackers and how security may control them, cross sectoral cascading effects etc. These tools use either explicit representations of the system i.e. a simple model of the network under attack or simplified allegorical representations of the attributes of the system i.e. hide and seek game to simulate attackers and security.

Table 7 completes Table 1 and sums up the ABM examples referred with regard to ISO step and focus.

Table 7: ABM examples in respect to risk management processes

Name	Approach	Purpose	Water sector CI	Focus
Agent Based Models				
COMMASPEN	Agent Based model	Risk Identification, Consequences analysis		Interdependency effects
N-ABLE	Agent Based Model	Risk Identification, Vulnerability Assessment, Consequences analysis		All-Hazards
Eom et al. (2008) ABM	Agent Based Model	Risk Identification, Vulnerability Assessment		Deliberate Attacks
Chapman et al. (2014) ABM	Agent Based Model	Risk Identification, Vulnerability Assessment		Deliberate Attacks

1.7 Performance Indicators

As proven in the previous chapters, managing and keeping an overview of the behaviour of CI can be very difficult. Systems that contain thousands of interconnected nodes, with

multiple functions and various limits and characteristics of operation are simulated through models or monitored via a sensor network. But clearly perceiving the performance of a system by looking through the sheer volume of data is almost impossible. For this reason, and in order to keep track of an organisation's goals and services, Performance Indicators (PI) can be used, translating raw data and measurements to a set of compact and well-aimed information: "Ultimately, an effective performance measurement system should support informed decision making about the allocation of resources within and by an organization" (Cable, 2005).

According to Parmenter (2015), the performance measures can be separated into two major groups, Result Indicators and Performance Indicators. The first, answer the question of "what has been achieved so far", while the second indicate "what is to be achieved to increase performance". As identified by Popova and Sharpanskykh (2010), PI "is a quantitative or qualitative indicator that reflects the state/progress of the company, unit or individual". In more detail, Alegre, (2000) defined PIs as "measures of the efficiency and effectiveness of the delivery of the services that result from the combination of several variables. The information provided by a performance indicator is the result of a comparison (to a target value, previous values of the same indicator, or values of the same indicator from other utilities)". Using the word *key* before PIs indicates the importance of those factors in achieving the company's goals. In other words, it reveals the critical success factors. Due to the complexity of each company, it's goals, processes, infrastructure etc., KPIs should be designed to match the needs of each company (Cable, 2005). As found in Nogueira Vilanova et al. (2014) work on the effectiveness of performance measurements, PIs should maintain a level of relevance to the organization's objectives.

Focusing on PIs of the water sector, they are found to be very similar across countries and companies (Nogueira Vilanova et al., 2014). The similarity emerges from the common basic processes, assets and overall goals of the water companies. Usually, the PIs focus on 5 main categories of management interest:

- Quality of service, that includes both quantity and quality delivered to the customers
- Asset, that includes the physical performance of the infrastructure
- Operational, related with daily monitoring and maintenance of the system
- Personnel, that focuses on human resources
- Financial, that keeps track of the financial soundness and economic prosperity of the company

Among the available PIs, the sector established and widely used set of IBNET and IWA PIs were selected to be presented for the purposes of this literature review. In addition to those indicators, resilience measures are also presented, due to their importance in a strong CI and their relevance to the purposes of assessing a system after a stress event has occurred.

1.7.1 IBNET Indicators

Helping utility experts and managers identify weakness and strengths of their organisation, International Benchmarking Network of Water and Sanitation Utilities (IBNET) (Danilenko et al., 2014) includes a number of indicators, categorized in the following manner:

Table 8: Summary of IBNET Indicators structure

Category	Number of PIs	Category	Number of PIs
Service Coverage	2	**Operating Costs and Staff**	16
Water Consumption and Production	6	**Quality of Service**	8
Nonrevenue water	1	**Billings and Collections**	23
Meters	2	**Financial Performance**	2
Network Performance	3	**Assets**	3

The full list of IBNET PIs can be found in the respective publication.

Through the use of sets of the above indicators, the user can produce focused, comparative reports of the performance of the Water and Wastewater sector, from local system, up to national level. Such a report example is the one produced by EBC (2017), demonstrating part of the above indicators and their benchmarking. Most importantly, the above indicators can be produced with little data, which is one of the main targets of constructing PIs or PI sets.

Usage of the indicators within the IBNET framework, can be performed either through calculating single indicators for the system, or by forming the so-called Overall Performance Indicator (OPI). Because the use of single indicators cannot produce a comprehensive image for the system, IBNET proposes the construction of Specific Core Indices. An index is

produced through a number of individual Partial Indicators. Combining various, process aimed indices, the user can create a single PI that represents, in a unique perspective, the performance of the system. Such an OPI can be used e.g. for each sub-system of the WDS such as the treatment plant, composing a simple set of KPIs for the company.

1.7.2 IWA Performance Indicators

According to Alegre et al. (2016), the same set of PIs can be used, but at the same time serve each differently. E.g. for a water sector CI, PIs can serve in maintaining or improving the quality of service, ease monitoring and decision making, detect strengths and weaknesses but most importantly provide key information that supports pro-active management. On the other hand, e.g. regulatory agencies can use the same PIs a key monitoring tool.

PIs offer information as a result of comparison to a target value, in an un-biased and comprehensive manner. They represent an actual performance achieved in the system of part of it, in a specific time-frame. In that context, IWA categorized the PIs in 6 categories:

- Water Resources (WR)
- Personnel (Pe)
- Physical (Ph)
- Operational (Op)
- Quality of Service (QS)
- Economic and Financial (Fi)

Each of the above categories represent the main purpose of a PI (Alegre et al., 2016) and a unique letter code for each group. Each of those “supersets” is divided to more subsets of PIs. The structure of the IWA PIs is presented in the table that follows.

Table 9: Summary of IWA PI structure

Group	Subgroup	Number of PIs
Water Resources	Water resources	4
Personnel	Total personnel	2
	Personnel per main function	7
	Technical services personnel per activity	6
	Personnel qualification	3
	Personnel training	3
	Personnel health and safety	4
	Overtime work	1
	Water treatment	1

Physical	Water storage	2
	Pumping	4
	Valve, hydrant and meter availability	6
	Automation and control	2
Operational	Inspection and maintenance	6
	Instrumentation calibration	5
	Electrical and signal transmission equipment inspection	3
	Vehicle availability	1
	Rehabilitation	7
	Operational water losses	7
	Failure	6
	Water metering	4
	Water quality monitoring	5
Quality of Service	Service coverage	5
	Public taps and standpipes	4
	Pressure and continuity of supply	8
	Quality of supplied water	5
	Service connection and meter installation and repair	3
	Customer complaints	9
Economic & Financial	Revenue	3
	Cost	3
	Composition of running costs per type of costs	5
	Composition of running costs per main function of the water undertaking	5
	Composition of running costs per technical function activity	6
	Composition of capital costs	2
	Investment	3
	Average water charges	2
	Efficiency	9

	Leverage	2
	Liquidity	1
	Profitability	4
	Economic water losses	2

In Alegre et al. (2016) the interested parties can find the new set of PIs, different than the previously proposed (Alegre, 2000), but in the same structure and spirit. The newest set also tries to assess the performance of bulk supply systems, previously not done.

The entire list of the IWA PIs, including units and details can be found in the respective publication.

1.7.3 Resilience Measures

Resilience is a term that currently dominates the policy discourse. Being a relatively recent term in the water industry, there are many definitions used among scholars (Francis and Bekera, 2014). The variations are mostly subtle (Butler et al., 2017), as dominant and fundamental in the literature is the definition given in Holling's early work (1973) and later refinements (1996), where resilience is a measure of " the persistence of systems and of their ability to absorb change and disturbance and still maintain the same relationships between population or state variables", as an expansion to the view of the system's stability, which "represents the ability of a system to return to an equilibrium state after a temporary disturbance". A large lineage of definitions stems from Holling's seminal work (Francis and Bekera, 2014), although there are definitions of resilience that are based on the theme of "The return time to a stable state following a perturbation" (Pizzol, 2015). Todini (2000) likewise recognized that resilience is "the capability of the designed system to react and to overcome stress conditions" and "...sudden failures", while referring to WDNs. A definition of resilience that seems very close to a measure of a CI system's performance is "the ability of the system to meet its intended performance and functions in the community through prevention (mitigation), design, and recovery plans and actions" (Chmielewski et al., 2016). Focused on the characteristics of the source of failure, National Infrastructure Advisory Council (NIAC, 2009) characterizes "infrastructure resilience" as "the ability to reduce the magnitude and/or duration of disruptive events". A visual representation of the above defined "resilience" characteristic of a system can be seen in Figure 21. F(t) is a theoretical performance function of the system, which in a WDN could represent "the number of nodes with sufficient supply". Note that t_a, in the time axis, can also represent the end of the actual event, and not only the activation of a pure resilience action. In general, resilience is viewed as the inverse of the duration unsatisfactory state of the system, in regards to any of the multiple functions. Hashimoto et al. (1982) used the inverse of the expected time the system's performance remains unsatisfactory, as the average recovery time of the systems, hence a measure of resilience.

A more holistic approach regarding water systems as a whole and not specific elements or CIs is given in Makropoulos et al, (2018), where resilience is defined as “the degree to which an urban water system continues to perform under progressively increasing disturbance” and quantified via the use of the resilience profile graph, as seen in Figure 22. The element of increasing disturbance is given on the x-axis with different scenarios, and performance is measured through reliability on the y-axis. Resilience is quantified through the area under the curve.

In general, resilience is viewed as the inverse of the duration during which the system has an unsatisfactory state, with regards to any of the multiple functions. Hashimoto et al. (1982) used the inverse of the expected time the system’s performance remains unsatisfactory, as the average recovery time of the systems, hence a measure of resilience.

A list of resilience indexes for WDS and assets, description and reference can be found in the work of Shin et al. (2018) which also includes resilience indexes regarding water resources systems.

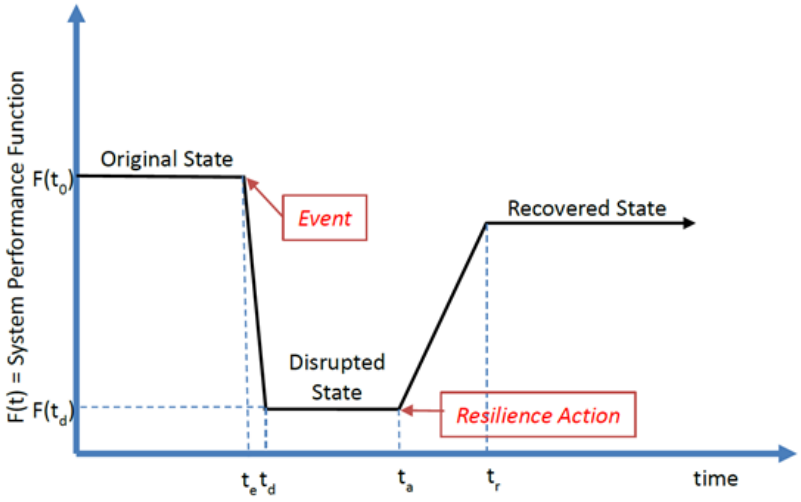


Figure 21: System performance function F(t) before, during and after an event (EPA, 2015)

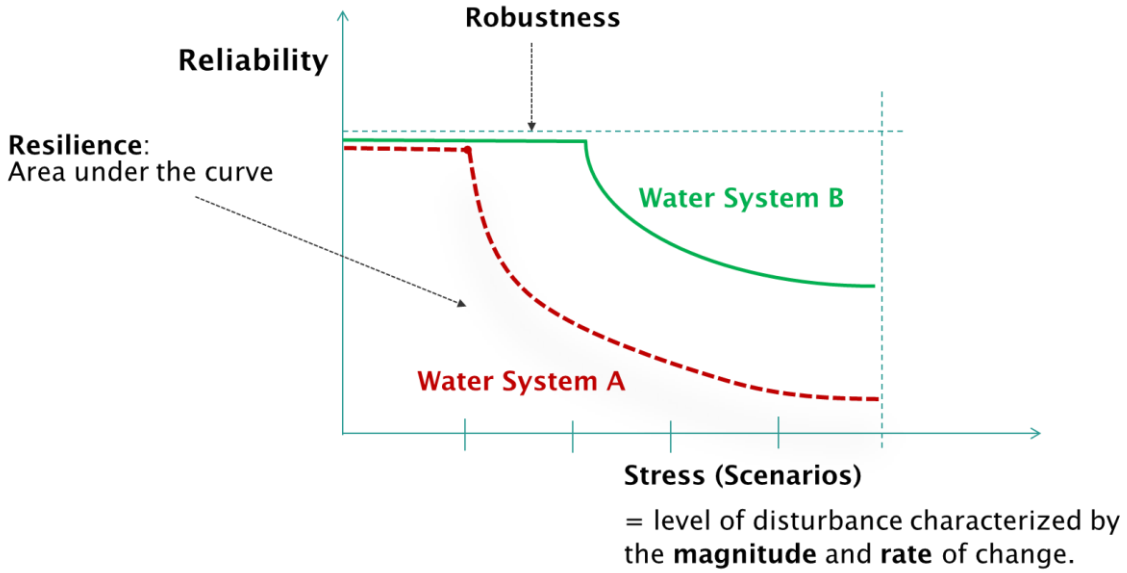


Figure 22: The concept of resilience profile graph (Makropoulos et al, 2018)

Part B: STOP-IT Risk Assessment and Treatment Framework

2.1 Introduction

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. One of the modular components of the STOP-IT risk management platform is the Risk Assessment and Treatment Framework of WP4. The aforementioned integral component of the project's outcomes is being deployed by developing several autonomous, yet interoperable, tools towards the tactical and strategic risk assessment and intervention planning. Those tools are: the Risk Identification Database (RIDB) of Task 3.2, a step-by-step guide for vulnerability assessment implemented through the Asset Vulnerability Assessment Tool (AVAT) (T4.1), the Risk Analysis and Evaluation Toolkit (RAET) on state-of-art models and tools, for the analysis and evaluation of risk (from physical, cyber and combined events perspective) to the water systems (T4.2) linkable to a Scenario Planner (SP) and a Probabilistic Safety Assessment tool i.e. Fault Trees Explorer/Editor (FT Editor), a Risk Reduction Measure Database (RRMD)(T4.3) recommending actions to avoid or mitigate the occurrence and consequences of risk events for water CIs, a Stress-Testing Platform (STP) to conduct simulations but also to evaluate system's performance or the effectiveness of risk reduction measures (T4.4) with the use of Key Performance Indicators (KPIs) (T4.2).

This foreword discusses the approach of STOP-IT Risk Assessment and Treatment Framework and its alignment to experts' accepted standards and approaches in order to ensure the delivery of ISO compatible outcomes. The suggested STOP-IT methodology and tools are based on the ISO 31000 Risk management Standards family, with the necessary adaptation to meet the needs of the water sector Critical Infrastructures under cyber-physical threats. Nevertheless, the developed framework and tools are applicable to any utility/end-user either having its processes/services aligned to the aforementioned standard or not. Before presenting the individual tools and their application, it is useful to introduce a Risk vocabulary, in order to best communicate knowledge, practices or information within the STOP-IT project among partners, Front Runners (FRs) and Followers (FLs). The adoption of ISO Standard terms and definitions (ISO 73:2009) is perceived as a solid step towards the creation of a common, comprehensive and clear vocabulary regarding risk assessment. The detailed glossary can be found in ANNEX A.

The ISO 31000:2009 methodology has been reviewed in Chapter 1.3 of Part A of this document and its primary process can be seen in Figure 2. As proposed by ISO, the core process of assessing and treating risks can be divided in the following steps:

i. Risk Identification
ii. Risk Analysis
iii. Risk Evaluation

iv. Risk Treatment

Setting side by side the STOP-IT Risk Assessment and Treatment methodology processes with the ones corresponding to ISO, they follow the same structure flow and terminology. The 7 key-step procedure of the STOP-IT methodology, and its relation to the tasks, as found in the Description of Work , is comprised of:

i. Risk Identification (Task 3.2)
ii. Asset Vulnerability assessment (Task 4.1)
iii. Consequences analysis (Task 4.2, Task 4.4)
iv. Risk level identification (Task 4.2, Task 4.4)
v. Risk Evaluation (Task4.2, Task 4.4)
vi. Treatment analysis (Task 4.3, Task 4.2, Task 4.4)
vii. Treatment effectiveness assessment (Task 4.2, Task 4.4)

Note: Although considered as key part of the chain, the Risk Treatment steps can be "skipped" only in case Risk Evaluation step leads to the conclusion of tolerable risk under the existing control measures and company's risk perception.

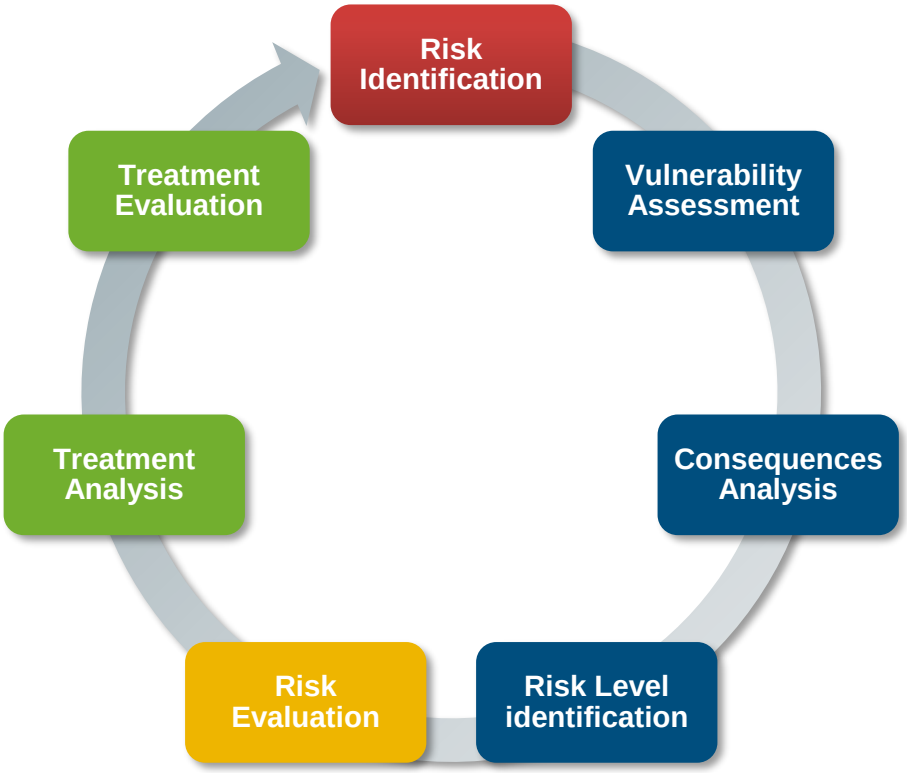


Figure 23: STOP-IT Risk Assessment and Treatment process

In the following table (Table 10), equivalent steps between ISO and STOP-IT methodology are being listed and coloured matched.

Table 10: STOP-IT process in regards to ISO 31000:2009

ISO 31000	STOP-IT
Risk Identification	Risk Identification
Risk Analysis	Asset Vulnerability Assessment
	Consequences Analysis
	Risk Level identification
Risk Evaluation	Risk Evaluation
Risk Treatment	Treatment Analysis
	Treatment Evaluation

The step of Risk Identification provides a pool of threats, i.e. a knowledge base from which information is derived for the next steps. The risk management team, with the help of experts from other fields (e.g. IT experts, penetrators, infrastructure managers etc.) create and enrich a list of potential threats to be further examined. This step is the creation of a database with all identified risks and their potential outcomes in the form of the Risk Identification Database (RIDB). This is in line with ISO guides that sets risk identification goals to “generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives” (ISO 31000:2009). In addition to the RIDB, generic Fault Trees for water quality and quantity issues assist the users in the risk identification step, providing also better insights on the cascading and interconnected events for both cyber and physical threats as well their combinations.

Asset Vulnerability Assessment detects the “intrinsic properties of an asset or control that create susceptibility to a source of risk and could potentially be exploited by one or more threats” (ISO 31000:2009), hence delivering a list of weaker points of the system against specific threats under current conditions (measures, controls etc.), based on the asset’s criticality and “attractiveness“.

Consequences Analysis is the step taken towards creating a better understanding of the behaviour of the system under specific threats/events, revealing valuable additional information about the threat. The RAET contains valuable tools, able to simulate cyber-physical parts of the system at multiple levels (e.g. with epanetCPA, Infrarisk-CP), providing the means to “consider the causes and sources of risk, their positive and negative consequences” (ISO 31000:2009).

Following the vulnerability and consequences analysis steps, the magnitude of risk can be identified/estimated for each threat/scenario. ISO 31000 refers to the estimation of risk magnitude as combination of only consequences and likelihood.

The step of risk evaluation is common to both ISO and STOP-IT processes. Based on the outcomes of the analysis, the organisation should be able to compare the system's behaviour under stress to the desired level, using a set of predefined Performance Indicators (PIs). Using a set of STOP-IT designed KPIs (found in RAET), consequences are mapped on and risks are evaluated as acceptable under existing measures or not, promoting the need for treatment. Based on the scores of the KPIs and the Risk Level, Risk Prioritisation sorting could indicate the major risks to be treated before others.

Treatment Analysis is the first part of the Risk Treatment procedure, as defined in the ISO 31000. All the risks identified from the previous step can be treated in regards to:

i. Impact mitigation
ii. Likelihood mitigation
iii. Increasing reliability/resilience

A set of predefined Risk Reduction Measures, with appropriate attributes that couple the controls with attributes of the Identified Risks, serving as a database (Risk Reduction Measure Database - RRMD for STOP-IT), can provide a solid step towards a comprehensive and structured treatment approach but also as a common base for the EU water sector. Once a treatment option is chosen from the RRMD, the system behaviour should be reassessed, consequences (re-)analysed for the new assumptions and new PIs must be estimated/calculated, following the same logic as in the previous steps.

Treatment evaluation is the comparison of the set of new KPIs to the KPIs of the stressed system under the existing measures and the target values. If the set of new KPIs indicated an acceptable behaviour of the system then the treatment measure should be indicated as effective. The treatment measures that are indicated as effective can be assigned an attribute of "preference" in the RRMD for the specific nature of threat, assisting the knowledge base of effective Risk Reduction Measures. Those can serve as Best Options in case the user needs an informative approach on the treatment of a risk/threat identified, prior to fully analysing it.

Note: The effectiveness of a measure does not mean that the organisation is going to adopt it. For various reasons, such as the cost of the measure, the organization can make an informed decision to retain the risk.

It is important to set the approach of the risk management process for the water CIs under CP threats, before delving into detail on the toolkit to facilitate the aforementioned steps. There are 3 main pillars on which the methodology is built.

STOP-IT Risk Assessment and Treatment methodology is designed to be an ***all-hazards*** approach, since the proposed framework refers to water CIs, aiming to achieve or maintain a high level of preparedness against threats of all nature (natural and man-made, accidental and malevolent, physical and cyber etc.). The second pillar is the use of threat ***scenarios***, reflecting a set or combination of possible threats and characteristics, creating a larger picture of the potential outcomes. This also allows the imaginative creation of multiple possible "future" conditions and reveals weaknesses which were previously unexplored. Due to the criticality of the CI system's response and bounce-back, countering threats should not only be approached with regards to avoidance, but also by retaining damage and minimizing responding/bounce-back time, hence addressing ***resilience***.

The STOP-IT methodology and toolkit is designed to serve multiple levels of analysis (generic or site-specific analysis, expert-opinion-based or model-based, qualitative, semi-quantitative or quantitative analysis, deterministic or stochastic analysis). Within that context, if multiple levels of analysis are chosen, it might be necessary to employ different ways of likelihood estimation. Regarding the examination of risks and consequences, it is done under the perspectives of water quality and quantity, natural environment, economics and reputation of the company.

2.2 STOP-IT components

The framework and scope of each of the aforementioned parts leads to the need of appropriate tools that can serve the risk management implementation and specifically the deployment of STOP-IT Risk Assessment and Treatment process. WP4 STOP-IT components (as well as others developed in other WPs which interoperate with them) are designed to cover the needs of each step of the process, as well as ensure their cooperation by keeping compatibility of data transferring among them. In the following chapters, the STOP-IT Toolkit is presented, including additional details on the processes within each tool.

In the following table (Table 11), the tools are linked to the corresponding Risk Assessment and Treatment process step.

Table 11: Matching of STOP-IT tools with procedural steps

STOP-IT tool	Corresponding step
Risk Identification DataBase (RIDB)	Risk Identification
InfraRisk-CP	Risk Analysis / Risk Evaluation / Treatment Analysis
Asset Vulnerability Assessment Tool (AVAT)	Vulnerability Assessment
Fault Trees & FT Editor	Risk Identification / Consequences Analysis
Scenario Planner (SP)	Risk Identification / Consequences Analysis
Risk Analysis and Evaluation Toolkit (RAET)	Risk Analysis / Risk Evaluation
Cyber-Physical Stress Testing Platform (STP)	Consequences Analysis / Risk Level Identification Treatment Analysis
Key Performance Indicators (KPIs)	Risk Evaluation / Treatment Evaluation
Risk Reduction Measure Database (RRMD)	Treatment Analysis

2.2.1. Risk Identification Database (RIDB)

The Risk Identification Database (RIDB), developed under Task 3.2 and documented in D3.2 with TECHN partner as the leading author, is essentially a list of risk events i.e. examples that assist the users in the Risk Identification step (as per ISO) and allow them to commence the process and draw their attention to some possibilities that should be investigated. Risk events are related to physical and/or cyber threats, which can occur in water distribution systems/water utilities. The RIDB identifies the type of threats, the sources of risk, the description of the events and the type of consequences produced. It is noted that the events included in the RIDB are not the result of a comprehensive review, but rather a list of events considered more relevant to the FRs.

The content of the RIDB should be considered as individual “building blocks" from which the various risk scenarios can be derived by their combination within the tasks performed in WP4 while exploiting the developed tools. Each event holds a unique ID for which a general description has been given, whereas several specific examples characterising further the risk have been matched for each general description. To ensure coherence between the different events composing the RIDB, a specific sentence structure has been designed for the general description of the event. The general description is formed by combining the attributes that characterise the event with the following encoding of sentence structure:

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

Where:

A: Type of risk source,

B: Type of threat,

C: Type of event,

D: Specific asset,

E: Type of asset,

F: Consequences dimension.

Using the above fixed structure, the following description of the event can be obtained as an example:

*"*External attacker generates a physical caused pollution of groundwater affecting raw water bodies; which might lead to a quality issue*".*

One of the specific examples giving additional information to aforementioned generic event might be "Substances are applied to the wells by addition to monitoring pipes".

As described in the following paragraphs e.g. section 2.3 (STOP-IT Methodological approach), the RIDB and its content is considered as the starting point for the different levels of analysis described under the Risk Assessment and Treatment Framework. In addition, it provides input to the several developed autonomous, yet interoperable, tools which are considered as integral components of the RAET. Indicative example of use is the exploitation of the RIDB structure and content during the Fault Trees creation while using the FT Editor.

Further information related the content and structure of the RIDB can be found under the D3.2 report of the project.

2.2.2. Asset Vulnerability Assessment Tool (AVAT)

Within this task, a methodology and a tool have been developed (D4.1) by TECHNION which serves as a procedural "step-by-step" guide for assessing asset vulnerability to risk events. The methodology takes into account specific asset characteristics, the importance of the components for water supply, their attractiveness and is aligned with security standards for their protection.

A well-defined methodology has been documented and suggested by SINTEF too, which estimates an overall Vulnerability Index through a two-step procedure. Within the first step, the so-called component vulnerability contributing index is estimated, which tries to capture the vulnerability from the system perspective, i.e. identify components (assets or subsystems) that contribute to the system vulnerability (system inability to withstand deficiencies in those components). In the second step of the above-mentioned methodology, vulnerability of components contributing to system vulnerability is further investigated through the estimation of the inherent vulnerability index. The latter index combines the likelihood of attack or other types of hostile environments that threaten the component and the inability to withstand such an attack. Moreover, through the incorporation of general system but also component-specific factors, the specification of vulnerability scores is achieved related to the frequency

of attack for the system and/or components, but also to the probability of specific component to fail to withstand the attack.

Parallel to SINTEF's work, TECHNION also delivered an asset vulnerability assessment methodology. Specifically, TECHNION worked on applying two system-wide measures: the Todini's Resilience Index (Todini, 2000) (which requires a steady state water distribution system hydraulic model), and Connectivity (which requires the system topology). In addition, complementing the system approach, the metric of Reachability was used to compute critical demand nodes vulnerabilities and critical network components. TECHNION's methodology is being deployed through the delivered Asset Vulnerability Assessment Tool (AVAT).

Further information related the developed methodologies for assessing vulnerability and the AVAT can be found under the D4.1 report of the project.

2.2.3. InfraRisk-CP

InfraRisk-CP consists a novel tool developed within STOP-IT project, aiming at assisting in the risk analysis of CI under cyber-physical (CP) threats, with focus on cascading effects. It is an extension of the previously developed InfraRisk tool, initiated within the DECRIS project[1], and its use is focused for the generic scenarios assessments as part of WP4 (and secondarily for the single scenario assessments). The CP risk assessments of water infrastructures in InfraRisk-CP are mainly based on expert judgments of the vulnerabilities and risks affecting on specific assets. The tool is designed to be independent from other models (such as system models; e.g., EPANET) yet supports information transferring (when appropriate) from the STOP-IT tools for the specific assessments. Particularly, the tool can be coupled (when necessary) with, the generic cyber-physical scenarios given in the risk identification data base (RIDB), the prescribed risk reduction measures in the risk reduction measure database (RRMD) and the Asset Vulnerability Assessment Tool (AVAT) developed in STOP-IT (D4.1). These may be imported in InfraRisk-CP as templates for further assessments. Each water utility (FR) car carry out assessments of single hazards and/or cyber events related to their own water infrastructure and systems.

More specifically, InfraRisk-CP implements two levels of analysis. On the first level, similar to a preliminary hazard analysis (PHA), cyber-physical scenarios are specified and analysed by the user in a very direct approach. The starting point is a predefined hierarchical list of so-called "main events" related to critical infrastructures (natural hazards, technical events, malicious acts and so on), and then the associated risk is analysed (based on their specified frequencies and consequences).

In the second, more comprehensive level, explicit linking between Societal Critical Functions (SCFs often corresponding to the physical asset) and the main events are established. One

[1] Norwegian research project financed by the Norwegian Research Council, 2008-2009.

or more SCFs could be chosen from a hierarchical structure of SCFs for each scenario. Similarly, one or more vulnerability factors may be linked to the main event. A conceptual bow-tie model holds the structure of the SCFs and vulnerability factors. In this level, formal assessment of the frequencies and consequences is achieved by applying fault tree analysis (FTA), reliability block diagrams (RBDs) and event tree analysis (ETA).

In summary, InfraRisk-CP can be viewed as a qualitative assessment tool for critical infrastructures and interdependencies, including the water supply and waste water treatment. The tool handles scenarios that could harm interdependent infrastructures and/or societal functions, and involve multiple infrastructures interactions.

2.2.4. Fault Trees and FT Editor

Fault Trees Analysis, as introduced in section 1.4.11 of Part A of the current document is a top-down approach to failure analysis, starting with a potential undesirable occurrence (hazardous event) called a top event, and then determining the ways it can happen. The analysis proceeds by determining how the top event can be caused by individual or combined lower level failures. FTs provide means to schematise the ways an event can occur and is considered as a necessity in the risk identification step and the initial steps of risk analysis, since the scenario's designed and eventually assessed by the end-users will be derived by them.

Taking advantage of the well-defined structure of the RIDB and having as primary aim to utilise its content for the Faults Trees (manual) creation, a step-by-step process was created in order to ensure that there will be no different interpretation of RIDB risk events from each FT designer. Following the structure of the RIDB ("*A generates a B C of D affecting E, which might lead to a F"* issue, as presented in 2.2.1 section) and specifically by reading its content backwards (from F to A), FT creation is achieved as presented in Figure 24. The different attributes of the RIDB i.e. the Type of Source (A), Type of Threat (B), Type of Event (C), the Specific Asset (D), the Type of Asset (F), and eventually the Consequence (F) are structured in a pre-defined and converse order, so as to form the different parts of a FT i.e. the Top events, the Intermediate Events and finally the Basic Events.

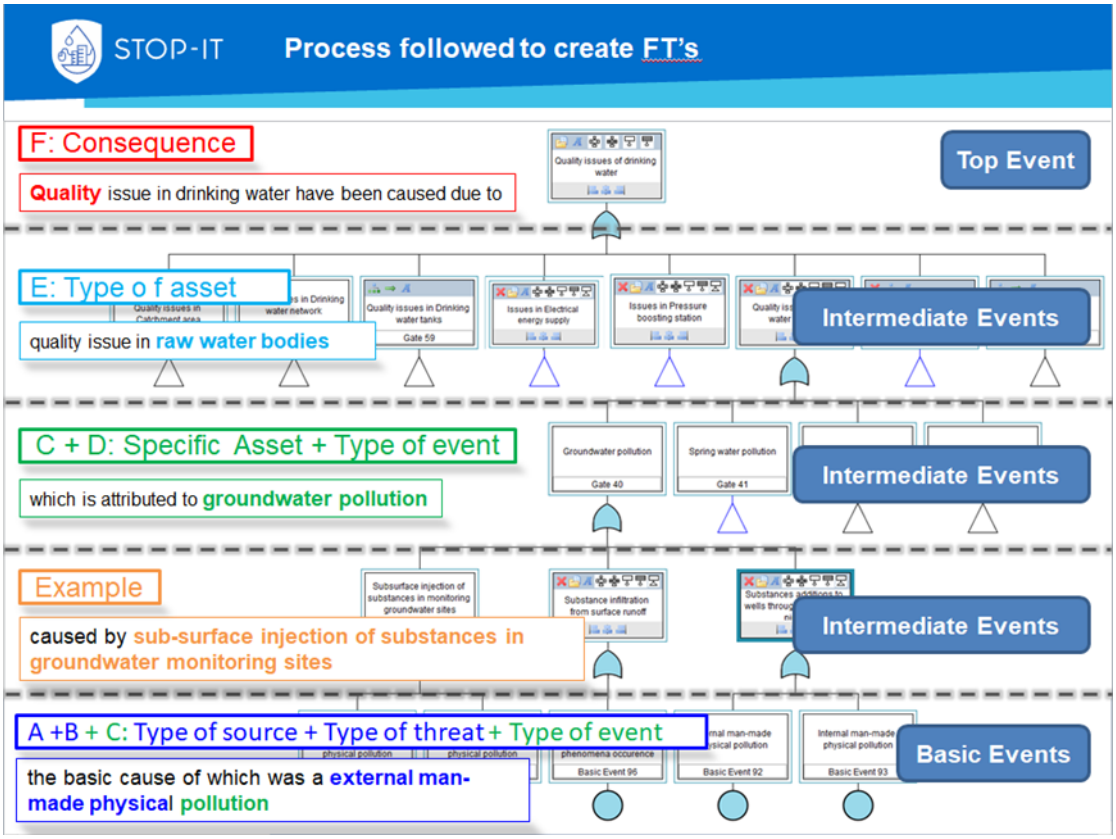


Figure 24: Process followed to create FT's from RIDB

Figure 25 attempts to clarify how FTs' creation is achieved by providing an RIDB example (with general description and its additional information) and how it has been "transformed" to a FT.

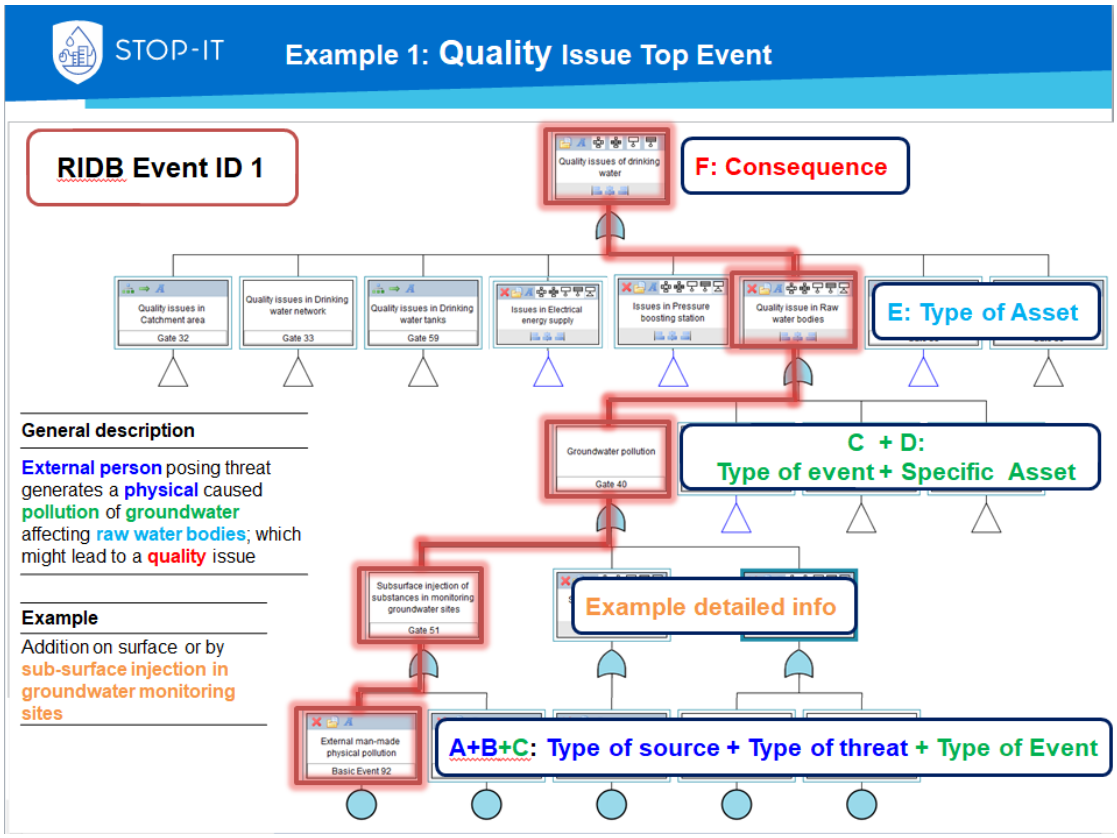


Figure 25: Example of RIDB event transformation to FT

It is highlighted that after following the above suggested process, two FTs have been derived based on the defined RIDB's consequences, having as Top Event "Quality Issues" and "Quantity Issues" in drinking water. The Financial, Reputation and Disruption type of consequences defined in the RIDB could be used at a later step to expand the 2 above-mentioned FTs and define new starting point of analysis for each company, since financial and media communication management processes are not sector-specific. In case there is an exception e.g. a reputation event which is not linked with any quantity or a quality issue, it will be taken into account as well and perhaps translated into an autonomous FT if needed.

Having implemented the above methodology, the RIDB was translated into Fault Trees. The derived FTs were then modified in order to more accurately represent the paths of cascading failures within under the holistic view of Urban Water Cycle. Joining cyber-physical operations within the Urban Water Cycle created a new, enhanced version of the structure to be used in the tactical and strategic planning of water sector CIs.

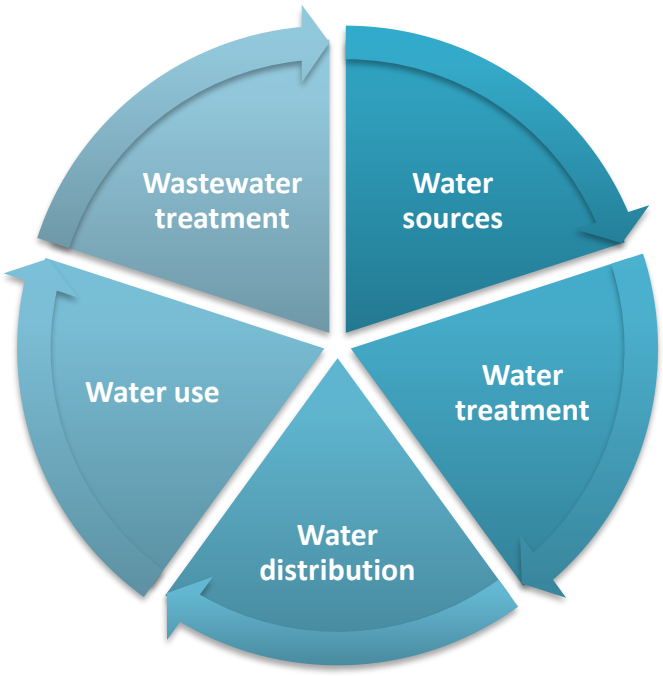


Figure 26: Urban Water Cycle

In fact, and for the purposes of the use of the enhanced FTs in building scenarios, the basic architecture and structure, as seen in Figure 27, is not a closed loop of the UWC, but rather the process from the output of wastewater treatment to sources, to withdrawal and water treatment plant up to the water distribution network and the consumers. CP attacks can occur at any level, and possibly cascade upwards, if the required conditions occur. Besides RIDB translation, the latest FTs are enriched with additional cyber-physical failure paths and key natural threats, identified in PREPARED project (FP7). Incorporating the FTs of the PREPARED project into the newly developed FTs of STOP-IT, including additional cyber elements, results in comprehensive descriptions of both cyber-physical events visualised through STOP-IT FTs. Undoubtedly, considering cyber-physical security aspects as a whole and not separately is one of the major objectives of the STOP-IT project.

The new UWC CP Fault Trees are made available through the RAET.

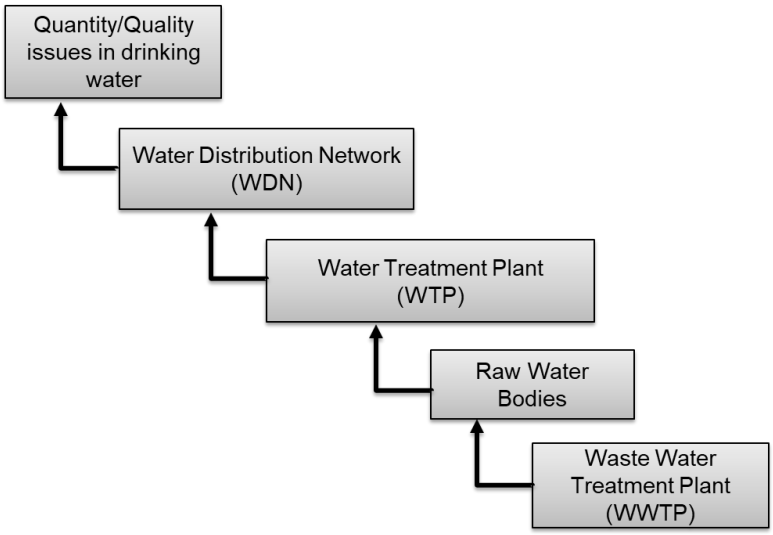


Figure 27: Enhanced UWC Fault Tree structure used

The primary User Interface of creating the FTs (by utilising the RIDB's content) is the Fault Tree (FT) Editor tool developed by RISA. The FT Editor tool is a graphical fault tree editor which has been developed for the WP6 of the project. The latest version of the tool used (V1.1.6) supports, among other, the calculation of failure probabilities in case probabilities of basic events have been defined. Identifying cut sets of the FTs designed, but also the minimal cut set are functionalities that will be sought to be developed since they will give additional functionalities to the SP tool (refer to section 2.2.5), hence, assist end-users in scenarios' exploration. Further, in order to assist integration with other tools of the RAET, RIDB attributes have been added to the Fault Trees. Each event contains information, as an inner dimension, through the related attributes and (if applicable) the ID of the threat recognised in RIDB. The new threat events and paths were also assigned those attributes, providing links and continuity within the developments. That attribute assignment is being utilised to link RIDB, scenarios and related measures in RRMD, while they are also providing identification parameters for the tool suggestion in RAET.

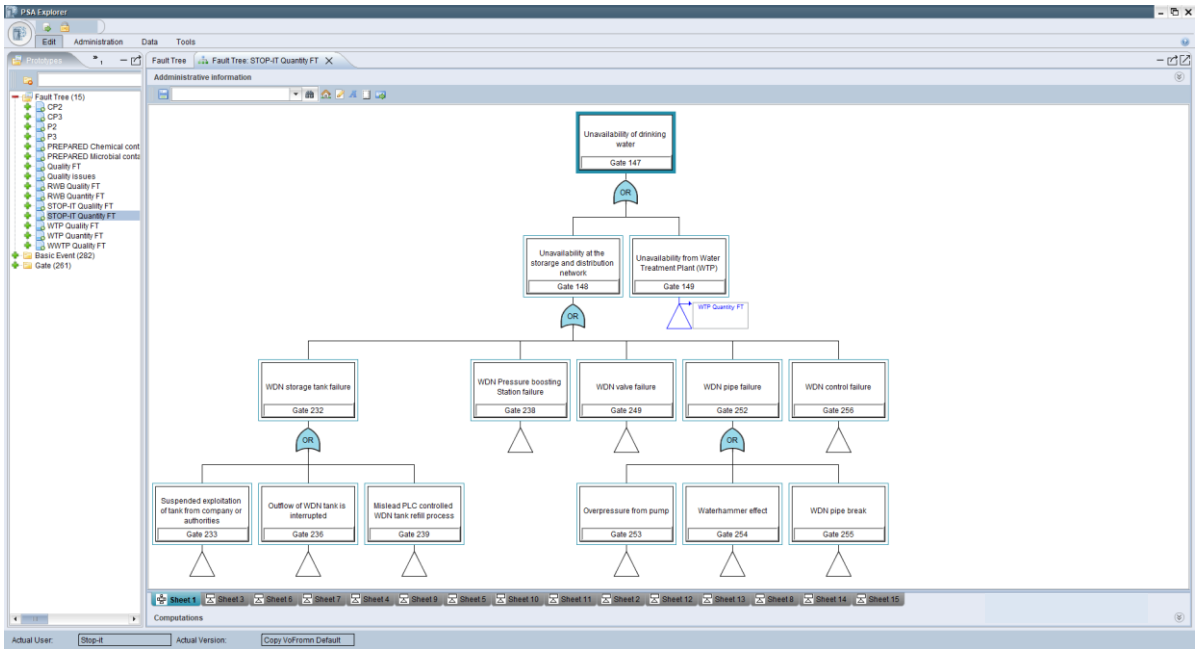


Figure 28: User's Interface and FT's example available in the FT Editor

In earlier version's, the FT Editor' content was stored in an access database (psa.accdb file) stored locally in each PC as defined in a configuration file (COODEXX.INI). In order to facilitate collaborative work and ensure that one common database is used by the STOP-IT partners, a Postgres database was set up in a server which is accessed remotely. In this way, simultaneous creation of FTs is achieved by different users of the FT Editor tool. In order to ensure integrity of the database, only authorised users can access the server, read and edit the FTs, while a back-up plan is applied (administrator can return to any version).

2.2.5. Scenario Planner (SP) tool

As addressed in the proposed methodology, and rather important in the All-Hazard approach and the investigation of complex system behaviour under multiple threats is the use of the threat scenarios. The Scenario Planner, a RAET embedded tool, is designed to assist the user by creating the graphical environment to decide the threats to be examined, based on the RIDB content and the designed generic STOP-IT FTs and enable users to build scenarios of their interest in order to be examined and simulated within the Stress Testing Platform or any other user selected model. The SP is primary consisted of two modules, an FT viewer and a scenario manager module developed to assist the above-mentioned workflow. Further details on its use and developments are being documented in the sections that follow in the current document.

2.2.6. Risk Analysis and Evaluation Toolkit (RAET)

The Risk Analysis and Evaluation Toolkit (RAET) aims at providing users with information and access to tools suitable to analyse and calculate water related problems. It is especially

useful when it comes to identifying those tools which are suitable to address a specific threat selected by the user according to chosen scenario. Appropriate tools can be selected depending on the **Type of infrastructure** to be analysed and the **Event/Threat** under consideration. Various filters, such as the **Technology Readiness Level (TRL)** of the tool, the **license type** associated with it, the usage **costs** etc., help the user to narrow down the list of possible options. Tools, selected to be used for simulation are associated with the **scenario**. RAET supports the users in obtaining, installing and executing the tools by providing documentation and links to the relevant sites.

Detailed information on the RAET's use and actual developments are provided in the sections that follow in the current document.

2.2.7. Stress Testing Platform (STP)

From the Stress Testing Platform, the user has access to a number of available modelling tools that can be used to simulate system behaviour under various threat scenarios, integrated with other STOP-IT components (e.g. the Scenario Planner). The integrated models are able to simulate the cyber layer information flow and control logic, as well as the physical layer's processes. The STP includes the following models:

- EpanetCPA, which models the distribution network (pumps, valves, pipes, tanks, reservoirs, consumers) and the connected cyber layer (sensors, actuators, PLCs) under physical or cyber-attacks. EpanetCPA is currently undergoing a customization that includes the ability to perform Pressure-Driven-Analysis (epanetCPA-PDA). In the case of simple demand driven analysis under extreme cases, such as pipe rapture, the false assumption of fully meeting the demand until complete pressure loss is made. The PDA enhancement provides a better, more accurate estimation model with results that bear resemblance to the actual conditions under extreme cases. The PDA analysis approach though should be evaluated against a ground truth or against a truth dataset, e.g. provided by a FR. The latest version of the epanetCPA enhancement developed within the project includes the coupling of a Pressure-Driven-Demand (PDD) version of the EPANET engine (.dll file) with various pressure-driven formulas that can be used with this expansion. This creates a new version of the epanetCPA (STOP-IT enhanced version), substituting the .dll file used to simulate the network with a new expansion (2.2+), but keeping the basic architecture behind the cyber layer of the network. The 2.2+ expansion of EPANET engine used in the STOP-IT version offers a dynamic alternative engine to explore CP attacks leading to pressure deficiency and low flow cases. It combines the features of EPANET 2.2 (the newest engine version available in OWA) with features of the Morley PDD engine, thus allowing for an assignment of PDD variables per node, which makes it a more adjustable and realistic approach. Proof of concept work on this development has been done on widely used "fictional" WDNs such as the C-town network. In addition to this, a visual representation of the cyber-network on top of the physical (WDN) is accomplished by extracting relationship information from the .cpa file and topological attributes from the .inp file. Moreover, a new version was

developed to include additional relations between cyber elements, including the communication channel (i.e. optic fiber, Wi-Fi etc.). The objects created are class type, encapsulating data and methods that can be inherited between class and sub-class objects, giving a direct link of connection. In order to discretely and dynamically represent the functionality of the cyber layer (control logic behind the system) a graph-based network algorithm is being developed, separating control logic from the hydraulic simulation. This algorithm assimilates the control logic from the EPANET file and creates the logical connection between PLCs, sensors and actuators. The control logic (rules) are represented as intermediate nodes between the connected objects, via connection paths that represent and carry information of communication channels, such as fibers. The properties of the cyber network elements, will enable the interconnection with variables set by the scenario planner. The EPANET simulation is controlled step-wise from the cyber layer, resembling a true real-time control infrastructure. Further enhancing this tool, we will create a CPA-Wizard with visual representation of the cyber layer and options to explore cyber-attacks to the related infrastructure. Through this expansion, the user will be able to run any CP attack scenario with site-specific reference using the wizard's UI.

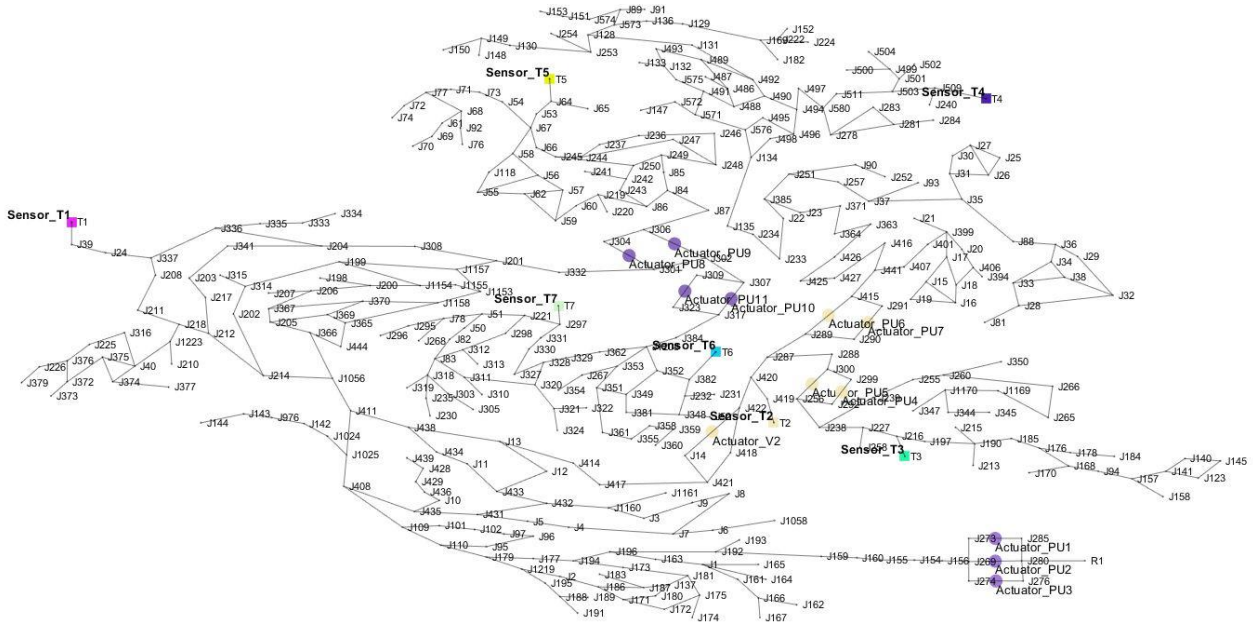


Figure 29: Cyber-physical network simulation representation (Matlab environment) with different color of sensors and actuators for each SCADA

- EPANET-MSX (Multi Species Extension) (Shang et al. 2008) is an extension to EPANET that allows for the consideration of multiple interacting species in the bulk flow and on the pipe walls. This greatly enhances the software's capability to track chemicals' fate in the network through diffusion mechanisms and chemical/biological reactions. With EPANET-MSX users are able to model complex physical

contamination (chemical or biological) threats and events in the water distribution networks. The toolkit library of functions is incorporated in the STOP-IT customized STP.

- RISKNOUGHT (Nikolopoulos et al. 2019) is a modelling framework developed within the STOP-IT project to serve as an innovative stress-test platform of cyber physical risks. For the physical layer, RISKNOUGHT uses the WNTR toolbox (Klise eta al 2017) which employs a custom made EPANET-like solver as well EPANET bindings. RISKNOUGHT also incorporates the EPANET-MSX solver for water quality modelling. On top of the physical layer, we develop the cyber infrastructure objects: sensors, actuators, Programmable Logic Controllers (PLC), central SCADA and Historian (the database of the SCADA) and their respective connections (wireless, optical fibre etc.). These objects form the control logic of the network by interacting with each other. The control logic explicitly and directly controls the state of the physical layer in each simulation time step. For example: A sensor in a tank senses its level (the actual tank head of the hydraulic simulation in this particular time-step) transmits this information to a PLC, which accordingly to its specified set of instructions sends a signal to an actuator to turn a pump off (setting the pump to off in the hydraulic network). The actuator transmits an ACK ("acknowledged") signal back to the PLC and the PLC reports all inputs and actions to the supervisory SCADA, which stores data in the Historian. We have developed methods of various interactions between both layers that can simulate a comprehensive list of cyber-physical threat scenarios on a wide range of attack vectors throughout the CPS. This includes:
    - Attacks that target sensors, like manipulating readings, making them appear offline or physically destroy them etc.
    - Attacks that target actuators, like intercepting signal from PLCs and sending fake ACK messages, making them offline, performing Denial of Service attacks, alter behaviour etc.
    - Attacks on PLCs, like altering/deleting the instruction sets, making them offline etc.
    - Attacks on master SCADA and Historian units, like disrupting communications with the slave PLCs, making the whole cyber system offline, altering database values etc.
    - Physical attacks on the hydraulic system, like destroying pumps, valves, pipes etc.

  More than one attacks are possible to affect multiple components of the system, and start times and duration of the events can be described, using a novel scenario planner tool that sets the environment for the cyber-physical simulation. By using the scenario planner, we can conduct a thorough stress-testing of the system with a multitude of different attack combinations and system states in order to identify vulnerabilities and assess performance. Consequences of the cyber-physical attacks, including cascading effects on the physical layer, can be quantified through the use of the KPI tool (see part E of this report).

All the above tools are also described as Stress Test Platforms and provide the appropriate modelling environment to estimate consequences with known assumptions and limitations. The results of each model are consequence metrics. Detailed information on the STP will be documented in Deliverable 4.4 which is due on M30.

2.2.8. KPIs

As each WDN requires its unique network model and scenario set-up to perform stress-testing, so does for the evaluation of their output in order to properly map consequences. Either stress-testing the system under a CP attack that affects the network's supply quantity or in terms of quality, each CI operates under unique internal and external environment, while that environment can also change. In this spirit, STOP-IT Key Performance Indicators are a set of adjustable multidimensional, quantitative metrics deployed for both Risk and Treatment evaluation. They are designed to filter and map the results of stress testing simulations and allow the comparison of the system's behaviour under stress to the desired behaviour. The latter also applies in the evaluation of risk treatment effectiveness, while specific metric families are designed to capture and reveal the effectiveness for different type of measures, designed to mitigate risk, boost system's recovery or increase robustness and improve resilience of the system against CP threats.

With system dynamics affecting failure characteristics in various dimensions, and the volume of simulation results, even for skeletonized networks and large timesteps, creating additional complexity, STOP-IT KPI framework provides the structure for a simple and efficient overview of the system under stress, through a set of metrics that explore failure in the dimensions of supply, nodes, customers and time.

Detailed information on the STOP-IT KPIs and tool developed are provided in Part E below.

2.2.9. Risk Reduction Measure Database (RRMD)

The Risk Reduction Measures Database assists users in their aim to find suitable measures for an identified risk. The aim of the database is not to support a fully prepared and formulated plan for risk treatment, but to point out measures which may address existing risks. The database is being developed in a generic way which allows its use by users from different regions and under very different conditions. Thus, it is up to the user to finally select those measures that are appropriate for the specific case and adapt them to the specific site conditions.

The main measure attributes supported by the RRMD are the following:

- Name: A short name of the measure
- Description: An optional textual field containing a description of the measure
- Type of Measure: The type of measure which defines the main principle under which the measure is able to reduce risk, such as physical barriers, cyber barriers, redundancy, control systems, economic policy etc.
- Type of Asset: Asset types which can be treated by this measure.
- Type of Event: Type of the event to be addressed

- Characteristics of Reduction: Characterization of the event in terms of whether it is reducing the likelihood of an event happening or if it is reducing the consequences of the event.
- Consequence Dimension: Selection from a list of consequences such as Financial, Water quantity, Water quality etc.
- Risk Source: External or internal source of the threat or human failure
- Characteristics of Action: Specification whether the measure acts proactive, reactive or both
- Comments: Viability, advantages, disadvantages

Measures from the RRMD have to be related with identified risks of the RIDB. The interpretation of this relationship is that the specific threats/risks can potentially be treated with the related measures. This information is important when it comes to select appropriate measures for a potential threat. However, establishing and maintaining such a relationship may pose a significant problem since both databases, the RIDB as well as the RRMD are expected to be updated continuously.

Detailed information on the RRMD are documented in the D4.3 report leaded by IWW and submitted on M24.

2.3 STOP-IT Methodological approach

Following the overview of STOP-IT Module I components, the proposed methodology flow for STOP-IT is presented in this chapter, taking into account the end-user perspective and implementing a three (3) level procedure, according to specific levels of analysis for an all-hazard risk assessment and treatment of CP threats in water systems. The levels of analysis are based on the needs or perception of the end user as well as on the data availability and are further specified in steps.

In the next subsections, a step-by-step guide of the methodological steps is presented, also illustrated in schematic representations. Table 12 summarizes the methodological approach for each level.

The end user can implement all three levels subsequently or can omit one or more according to the needs.

Table 12: Levels of analysis and steps proposed in the STOP-IT risk assessment and treatment methodology

Methodological levels of analysis and steps	Link with ISO	STOP-IT Tools	WPs/Tasks*
1. Generic assessment			
1.a Identify risk criteria	Risk Criteria Identification	N/A	WP3 (T3.1)
1.b Create threat scenarios	Risk Identification & initial step for Risk Analysis	RIDB, Scenario Planner	WP3 (T3.2), WP4 (T4.2)
1.c Conduct generic risk analysis & risk level estimation	Part of the Risk Analysis	InfraRisk-CP	WP4 (T4.2)
1.d Examine initial set of measures	Part of the Risk Treatment	RRMD	WP4 (T4.3)
2. Single scenario assessment			
2.a Create threat scenario	Risk Identification & initial step for Risk Analysis	RIDB, SP	WP3 (T3.2), WP4 (T4.2)
2.b Assess asset vulnerability	Part of the Risk Analysis	AVAT	WP4 (T4.1)
2.c Assess performance and perform risk evaluation	Part of the Risk Analysis and Risk Evaluation	SP, RAET, KPIs, STP with the appropriate simulation model	WP4 (T4.2, T4.4)
2.d Select the set of measures for given scenarios	Part of the Risk Treatment	RRMD, KPIs, STP with the appropriate simulation model	WP4 (T4.2, T4.3, T4.4)
2.e Evaluation of solutions	Part of the Risk Treatment	SP	WP4 (T4.2)
3. Multiple scenarios simulations			
3.a. Assess overall performance (KPI) of utility network	Risk Identification, Risk Analysis, Risk Evaluation	RIDB, SP, RAET, STP, KPIs	WP3 (T3.2), WP4 (T4.2, T4.4)

3.b Identify most serious threats	Part of Risk Evaluation	N/A	N/A
3.c Identify most appropriate measures	Risk Treatment	RRMD, KPIs, STP with the appropriate simulation model	WP4 (T4.2, T4.3, T4.4)
* Where “WP” is the Work Package and “T” is the Task			

2.3.1. Generic assessment

This is a generic approach, for which no specific data of a utility network is needed. The user can have a first assessment of risks and vulnerability of the infrastructure and identify potential risk reduction measures based only on what is known for infrastructures of his type and his knowledge about the site.

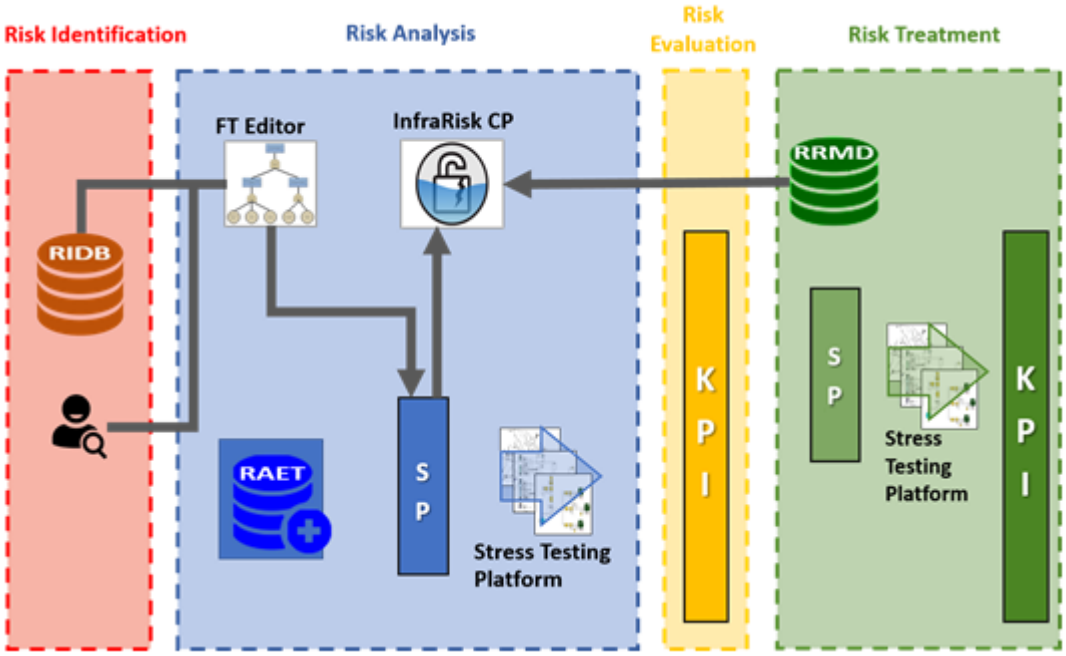


Figure 30: Schematic representation of the 1st level of analysis

1.a. Risk criteria identification

The first level of analysis would be the most generic one, serving the purpose of providing the end user with a general overview of risk assessment in water systems. The definition of risk criteria consists on establishing the level of risk that is acceptable and tolerable (or not) and it will support the step of risk evaluation. The process of defining risk criteria followed in the STOP-IT project was part of the step “Establishing the context” which has been described in Deliverable 3.1.

Tools: N/A
In regards to ISO: Risk Criteria Identification
WPs connected: WP3 (T3.1)

1.b. Create threat scenarios

The RIDB events have been translated into FTs by using the FT Editor developed by the RISA partner. During this process the event information included in the RIDB has been enriched with causal relationships and dependences. Taking advantage of the defined FTs, with the FR experts' opinion assigned values of likelihood, the user can simply choose, through the FT viewing capabilities of the SP the threats (basic, intermediate or top events in the FTs) for investigation.

After the selection of the desired threats to be triggered, the activated paths/parts of the FTs are being highlighted based on the user's choices and information is being extracted regarding the likelihood the experts have assigned and calculated through the PSA Explorer. Besides the user defined scenario, SP also has the ability to visualise the most likely to happen scenario or the minimum cut scenarios of the FT.

Tools: RIDB, FT Editor, SP
In regards to ISO: Risk Identification + initial step for Risk Analysis
WPs connected: WP3 (T.3.2), WP4 (T4.2)

1.c. Conduct Generic risk analysis and risk level estimation

After the use of SP tool (or even prior), the user can select to explore a desired event selected possibly by the RIDB and proceed with a Preliminary Hazard Analysis, through InfraRisk-CP. This procedure is based on expert's judgment and has little if any request for input. The first step towards assessment through InfraRisk-CP is to insert the scenario and select main events with appropriate categorization. The user can link to RIDBs specific elements such as "type of threat" for more comprehensive work-flow between elements of the process. Main events are then linked to Societal Critical Functions embedded in the tool's lists. Vulnerability factors related to the threat, main event and linked Critical Societal Factors must be assigned by the user as well as a Probability Factor for each consequence dimension. For the adjustment of frequency or consequences, consider the vulnerability factors acting on SCFs, either prior, after or both prior/after the main event. The user can then select a class value (e.g. "2" in a 1 to 5 scale) for the potential consequences in respect to:

1. Life and Health
2. Environment
3. Economy
4. Manageability
5. Political trust
6. Lifeline quality

Based on those user-defined semi-qualitative attributes that demonstrate expert's perspective and knowledge of the network's current state and the examined threat, the Risk Picture can be defined.

The overall process is a preliminary hazard analysis based on expert judgment and no request for simulations or data, giving the user a first approach of the threat in the system.

Tools: InfraRisk CP
In regards to ISO: Part of the Risk Analysis
WPs connected: WP4 (T4.2)

1.d. Examine initial set of measures

The next possible step for the user is to address the risks and request for possible Risk Treatment options regarding the scenario. All threats documented in the RIDB will have been related with suitable measures identified in the RRMD. The user will be able to review the measures which correspond to the threats according to chosen scenario. For the matched measures additional information will be retrieved from the RRMD and provided to the user such as conditions and cost range. In case documented applications of the measures are known additional information about the case studies can be provided (lessons learned etc.). Since the goal of this approach is the examination of possible behaviours of water CIs and the corresponding treatment options, no evaluation of the selected treatment will be made at this stage.

Tools: RRMD
In regards to ISO: Part of the Risk Treatment
WPs connected: WP4 (T4.3)

The threats/events, the vulnerability scores, risk characteristics and treatment options proposed are registered as a scenario with unique ID within the SP database, allowing the user to keep track of all the examined scenarios and treatment options.

All of the above steps compose a fully generic, not dependent on data, site-agnostic examination of Risk Assessment and Treatment procedure in any water sector CI. This is a robust way to have an initial approach to the procedure and the expected outcomes, with no need for site specific data or expertise in modelling. It can be used for a water company challenged by the municipality regarding risk issues for the water distribution network.

2.3.2. Single scenario assessment

After having the initial overview of the CI system response to a set of generic threats, the user might decide to proceed with the examination of a specific network as described in this section. Here vulnerability is assessed for specific assets and risk assessment is performed by simulations against identified threats, giving a concise picture on how the utility network performs on given event or event combinations. After that, appropriate risk reduction

measures may be identified and their performance against the given threats can be analysed. Comparison between RRMS ensues.

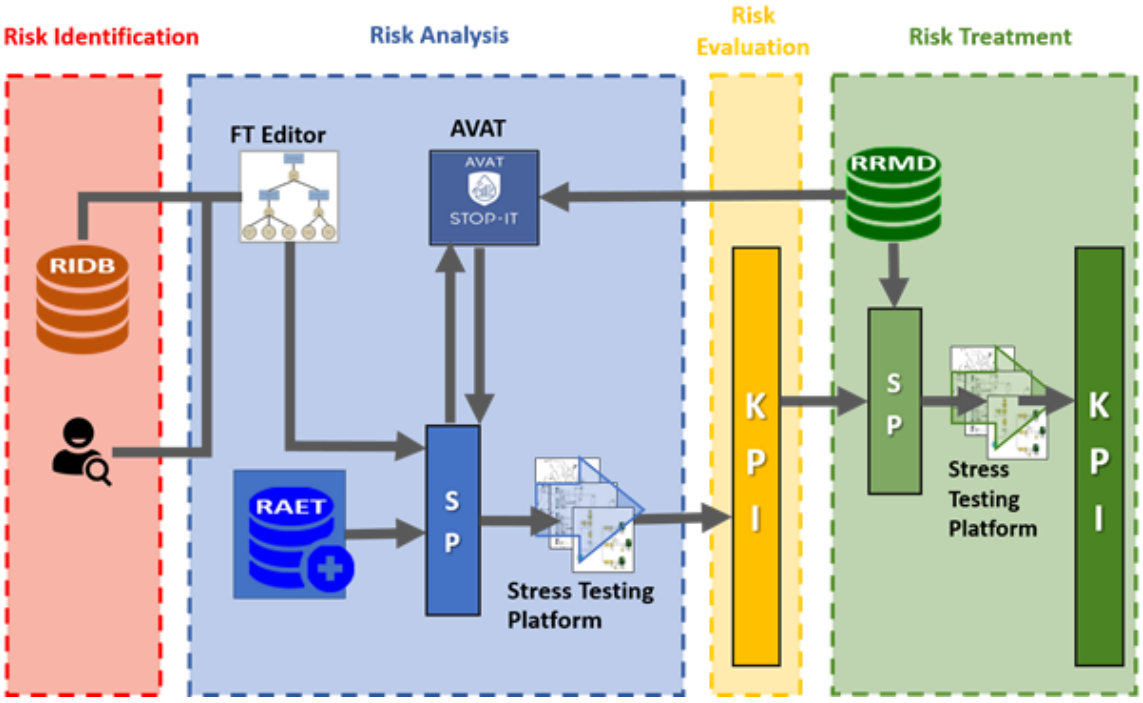


Figure 31: Schematic representation of the 2nd level of analysis

2.a. Create threat scenario

Taking advantage of the UWC defined FTs, the user can simply choose, through the FT viewing capabilities of the SP, the threats (basic, intermediate or top events in the FTs) for investigation. The system will support the user in the selection of the threat for the scenario by providing him useful information and assisting him in refining the initial selection. The SP also has the ability detect if conditions for path activation are met and visualise the activated paths of the events selected.

Tools: RIDB, FT Editor, SP
In regards to ISO: Risk Identification + initial step for Risk Analysis
WPs connected: WP3 (T.3.2), WP4 (T4.2)

2.b. Assess asset vulnerability

After the selection of the scenario, the user can proceed with the vulnerability assessment against the chosen threats. In contrast to the previous level of analysis (Level 1) where InfraRisk-CP was used, in Level 2 a step-by-step procedure is employed through the development and use of the Asset Vulnerability Assessment Tool which estimates the overall Vulnerability Index of the system. The key difference here is that a formal vulnerability

assessment process is utilized which takes into account the vulnerability of each component, contributing to the overall vulnerability of the WDN system. Further, it incorporates the inherent vulnerability i.e. the part indicating the likelihood of an attack and other types of hostile environments that threaten a specific component and the inability to withstand such an attack. Considering that there are several factors affecting vulnerability, some system-wise and others component- specific, the methodological process uses vulnerability factors so as to enable the users to take into account the specific characteristics of the assets, the importance of the components for water supply and its attractiveness to be attacked (further information regarding the AVAT has been provided in 2.2.2 section and the D4.1 report). In this level of analysis, data include the topology of the network and it is understood that some of the required input will be provided by the user through an input file (.xls format), and some will be calculated by the tool itself. The use of importance measures for asset types affected by the threat contained in the scenario could facilitate an asset-specific vulnerability scoring, without taking into account scenario-specific modelled consequences. Such asset specific scoring is also provided by the user in the input file required by the tool.

The output will be a vulnerability report that indicates the assets of the system that are more vulnerable to the generic threat scenarios. As such a user is be able to prioritize assets for more close examination. This step turns the generic scenario into prioritized site-specific scenarios.

Tools: AVAT
In regards to ISO: Part of the Risk Analysis
WPs connected: WP4 (T4.1)

2.c. Assess performance and evaluate risk through simulations

In step 2.a. the users have created scenarios of their interest by utilising the RIDB content, the outputs of the FT Editor i.e. the FTs and the SP which enabled them to visualise and filter parts of the FTs i.e. possible path of failures which need to be further analysed. In addition, prior to this step, the overall vulnerability of the actual system was assessed by implementing the AVAT (step 2.b.). All of the aforementioned information and produced results serve as input to the SP which assists the users in running their developed scenario in the Stress Testing Platform. In case the user hasn't previously used the tool, there is available access through Risk Analysis and Evaluation Toolkit (RAET) for more information. The user, having access to the RAET, can review the characteristics and requirements of the available tools and choose the ones to be deployed. The selected tools are internally associated with the given scenario and RAET can support the user in the preparation of the tool for execution (documentation, download link, installation process etc.). In this process, several models can be used, e.g. a PLC hack can be simulated in a cyber-level first, before modelling the hydraulic effects of that event, with a water distribution model such as the EPANET-based models of STP. After simulating the scenario, the results are mapped to the appropriate KPIs (e.g. a contamination threat must de facto be mapped with regards to a water quality KPI) and the Risk Level. As the consequences are a result of a model (pressure, demand met,

density of chemical component, hours out-of-service etc.), the KPIs can be calculated by formulas after evaluation of the simulation results, thus, providing a more precise metric of system performance under the specific threat scenario (further information on KPI's has been presented in section 2.2.8 of this document, Part E and ANNEX C). On the other hand, the mapping function that translates simulation results to KPIs is model/tool specific, based on results output format and needs to be developed for each model separately. Therefore, this function is implemented only for a limited number of models/tools in this project. The user can choose to create additional multiple scenarios and run the simulation again or decide to proceed with the treatment of the evaluated ones. All defined and simulated scenarios, as well as the set of KPIs are stored in the RAET database for future use.

Tools: SP, RAET, KPIs, STP with the appropriate simulation model
In regards to ISO: Part of the Risk Analysis and Risk Evaluation
WPs connected: WP4 (T4.2, T4.4)

2.d. Select the set of measures for the given scenarios

After the risk evaluation, the RRMD can again provide a set of possible generic measures. This time, as the vulnerability assessment has transformed the generic scenario to one that is asset-specific, any generic measure can also be converted to asset specific. For example, in the informative approach, a possible Risk Reduction Measure (RRM) against pipe burst could be the addition of a regulatory valve. In this approach, the RRM of adding a regulatory valve is assigned to a specific location, e.g. Pipe-128 of the network. This way, the measure can not only be integrated and simulated within the network, but the specific costs can be estimated by the company given the diameter of the valve. After selecting one or a set of measures, the user recreates the new conditions of the network, creating a new scenario to be simulated with the selected model. In the case of an epanetCPA model, the user inserts, to the initial. inp, the identified measure in this case the valve and reassesses the behaviour of the system under the same threat scenario. The new results from this simulation run are again mapped to KPIs. New sets of consequences are estimated, since the system is different, and the SP maps the new set of KPIs.

Tools: RRMD, SP, KPIs, STP with the appropriate simulation model
In regards to ISO: Part of the Risk Treatment
WPs connected: WP4 (T4.2, T4.3, T4.4)

2.e. Evaluation of solutions

In order to facilitate the evaluation, as stated before, the previously assessed and evaluated scenarios are associated with the resulting KPIs which are stored in the SP's database. Same applies for the new scenario that includes the RRM, and the new KPIs which were calculated in the previous step. In case the user decides to run multiple scenarios with different measures each time, the same procedure can be repeated for each scenario. The SP will

support the user to compare the performances of the scenarios determining which measures improve the system performance under the specific threat.

Tools: SP
In regards to ISO: Part of the Risk Treatment
WPs connected: WP4 (T4.2)

2.3.3. Multiple scenarios simulations

In the previous approach a single threat or a combination of threats has been evaluated through simulations. In an All-Hazards approach however, a large number of various threats has to be considered. The combination between them with different attribute values each time, such as e.g. duration of threat, can lead to a vast number of possible scenarios with different magnitude of consequences. In this approach a methodology is proposed which takes into account the dimensionality of the problem and examines various scenarios by running a series of simulations. Risk identification and evaluation are implemented by SP, the STP and RAET in a single procedure which may give answers to the following questions:

- Which is the overall performance (KPI) of a utility network?
- Which are the most serious threats or combination of threats?

After that, another procedure may be initiated for the treatment analysis and evaluation providing the most appropriate risk reduction measures.

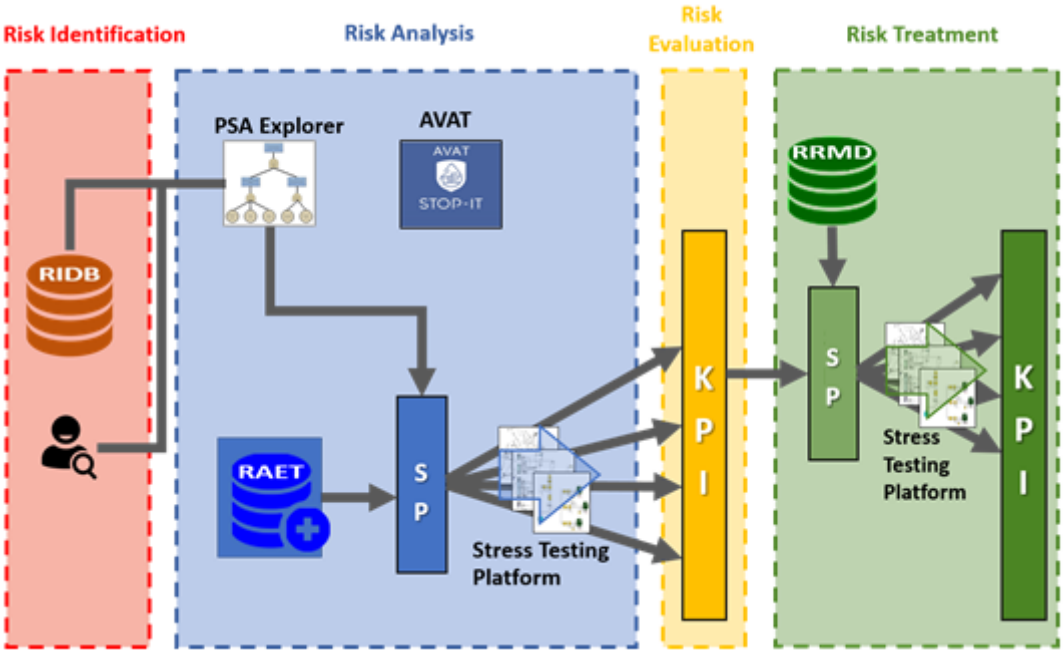


Figure 32: Schematic representation of the 3rd level of analysis

3.a. Assess the overall performance (KPI) of utility network through simulations

It is generally accepted that the initial assessment (based on expert judgment) on the performance and vulnerability of a network is relatively vague. Simulation results based on scenarios can give more precise and accurate information for a given threat or combination of threats. However, they are valid only for the specific scenario. In order to gain an objective performance assessment against CP threats of the utility network as a whole, a series of scenarios has to be simulated. The events and their weightings applied in the scenario each time must reflect the FT for the specific infrastructure type. The KPIs can then be assessed from the combination of all simulation results. This procedure can be analysed in the following steps:

- Based on the infrastructure type of the utility network the system retrieves its FT(s) and the corresponding events/threats.
- Each event leads to one or several scenarios which differ from the baseline (business-as-usual) scenario in the characteristics of the network (e.g. defect asset) or the initial conditions (e.g. water contamination). Other scenarios can be created by applying the same type of modifications at different parts of the network each time (e.g. another defect asset of the same type) or different attribute values for an event (e.g. duration of event, starting time etc.). A set of randomly generated scenarios (like a Monte Carlo approach) is proposed by the SP that covers a wide range of possible threats and configurations. The advantage of such approach is the combined investigation of threats, including low probability threats which might result in severe impacts, not foreseen previously.
- RAET proposes a list of suitable tools to simulate the network, based on the types of events and assets which are affected according to the scenario. From the list one or many tools/models are selected by the user.
- For each scenario and tool that has been selected, the input data are created. This step can be automated by the Stress Testing Platform only for a limited number of tools/models and event types. Scripts feeding the models with input data according to each scenario are developed for most of the other tools/models as well to avoid manual creation of the input files when possible.
- Through the Stress Testing Platform fed by the SP the simulations are executed with the selected tool, one for each scenario.
- The Stress Testing Platform examines the results of each simulation and maps them to KPIs. The Stress Testing Platform will support automated mapping only for a limited number of tools.
- The overall KPI and the KPI for each dimension are calculated by the SP taking into account the whole set of simulation results.

Tools: RIDB, SP, RAET, STP, KPIs
In regards to ISO: Risk Identification, Risk Analysis, Risk evaluation
WPs connected: WP4 (T4.2, T.4.4)

3.b. Identify the most serious threats

Based on the above simulation results of the stress test for various scenarios the user will be able to directly compare the results of a number of scenarios and thus assess the performance of the network under various conditions which may lead to answering question which single event or combination of events and under which conditions pose the most serious threats for the infrastructure.

3.c. Identify the most appropriate measures

A number of measures may be provided by the RRMD capable to address risk events identified in the previous step. Following a similar approach as described in previous sections the SP can support the user to identify the most appropriate measure(s) for a given threat or combination of threats:

- Either based on FTs or as a result of the previous simulations showing the most serious threats, the user selects an event or combination of events that poses a significant threat to mitigate
- The RRMD lists all known measures that potentially can address the threat providing additional information for each one of them
- The user selects a subset (or all) of them for further evaluation
- A set of randomly generated scenarios is proposed by the SP based on the selected set of RRM
- The RAET proposes a list of suitable tools to simulate the network or the same set of tools as for the simulation in previous steps is used.
- A script is utilized which creates or modifies the input files for the selected simulation tool(s) in a way that that corresponds to one scenario each time. Again, in this project this step can be automated by the Stress Testing Platform only for a limited number of tools/models.
- Through the Stress Testing Platform fed by the SPT a series of simulations are executed, one for each scenario.
- The Stress Testing Platform examines the simulation results for each simulation and maps the results to KPIs.

The SP lists the performance of all simulated scenarios. Next to the performance evaluation of the scenario, additional characteristics of the measure applied (e.g. costs, installation time, type of measure) may be presented and taken into account for the final selection of the most appropriate measure(s).

Tools: RRMD, RAET, KPIs, STP with the appropriate simulation model
In regards to ISO: Risk Treatment
WPs connected: WP4 (T4.2, T4.3, T4.4)

2.4 User's perspective and examples of use

2.4.1. Generic assessment – 1st level of analysis

The first level of analysis consists a generic assessment and analysis of CP scenarios for CIs implemented using the InfraRisk-CP tool. A detailed description of the InfraRisk-CP methodology is given in Part C, while herein we provide a brief description of its main functionalities.

The starting point in an InfraRisk-CP risk assessment is to add the 'Type of source' or 'Main event' based on a scenario description. There is a predefined list of main events related to different critical infrastructures. For each main event it is possible to link societal critical functions (SCFs) that are most relevant for the events been considered.

The main analysis screen of InfraRisk-CP is shown in Figure 33, where the main-event levels are shown in the top middle, the SCFs to the left, and the consequence dimensions to the right, similar to a 'bow-tie' approach.

To some extent the frequencies, and to a large extent the consequences of the main events, are influenced by one or more vulnerability factors. These are assessed in the bottom middle of the screen. Based on assessment of the vulnerability factors and the SCFs the frequency of the main event is set at the upper left corner.

The following points illustrate in a step-by-step manner the risk assessment analysis carried out in InfraRisk-CP (in accordance with the numbered bubbles of Figure 33):

1. Start the analysis by describing or importing the scenario description from the RIDB.
2. The next step is to press the 'New event' or 'Change event' buttons (shown in the middle of Figure 33). The latter is chosen if the analysis will be based on a previous entry, or a generic record. The main event is chosen from the hierarchy menu given Figure 35.
3. When a simplified analysis mode is chosen, the frequency and consequence assessments are made directly according to procedures in Section 3.2.2.
4. In the left part of the screen it is possible to add SCFs relevant for the risk scenario by clicking the Add button. A new SCF is chosen from the hierarchical menu (Figure 36 and Figure 37). When a new SCF is added the type and strength of relation between the SCF and the main event should be defined according to values shown in Table 13. It should be stated whether the SCF occurs before (initiating event) or after (barrier function) the main event.
5. Vulnerabilities or risk factors are defined in the browser in the middle of the screen in Figure 33. To add a new vulnerability or risk factor move to the New record (*) row and choose a factor from the list. It should be indicated whether the vulnerability or risk factors act before or after the main event. The value of the factor is chosen from a list corresponding to Table 22 (see ANNEX D).
6. The probabilities (worst case) for each of the consequence dimensions are assessed.

7. Select the consequence class for the respective consequence dimension. The risk for each consequence dimension is calculated according to the current calibration of the risk matrix in Table 19 (see ANNEX D).
8. Pick the correct classification of the "type of event" and relation to cyber.
9. Describe causes as basis for suggesting improvement measures.
10. Pick risk reduction measures from the risk reduction measure database (RRMD).

The frequencies, probabilities and consequences are assessed by experts and entered into InfraRisk-CP from predefined drop-down lists. Alternatively, the assessments/values could be based on specific information provided from the other STOP-IT tools.

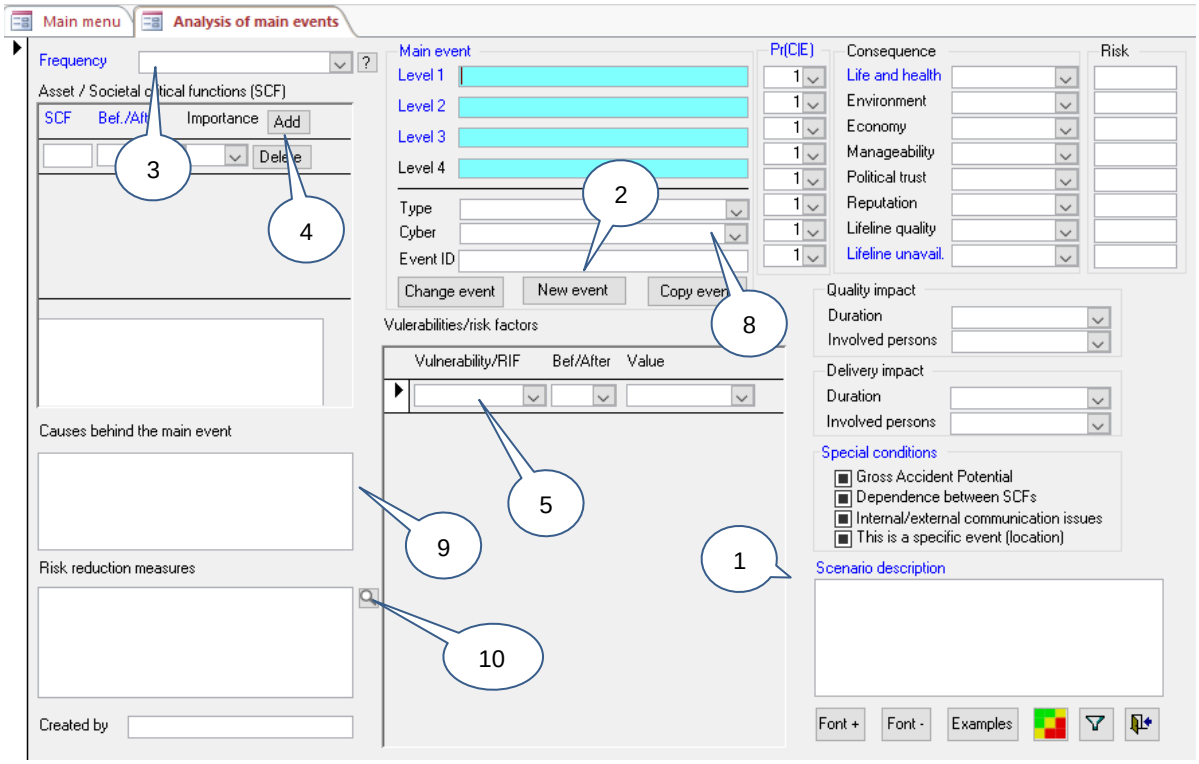


Figure 33: The InfraRisk-CP tool with its Input fields.

By clicking the lower 'risk-matrix' illustrated button in the bottom right corner of Figure 33, the risk matrix in Figure 34 appears. The lifeline quality and unavailability dimensions could either be specified directly or calculated from the 'Duration' and 'Involved persons' assessment. The consequences are determined by the current calibration of matrixes for duration and involved persons (see Table 18 in ANNEX D). By clicking the View risk matrix button (▪) in Figure 33 all (filtered) main events are plotted in the risk matrix as exemplified in Figure 34. By clicking in one of the cells in the risk matrix, the corresponding main events are filtered out and viewed. Note that the risk matrix is presented for one consequence dimension at the time. The buttons at the bottom of the screen are used to move between the various consequence dimensions.

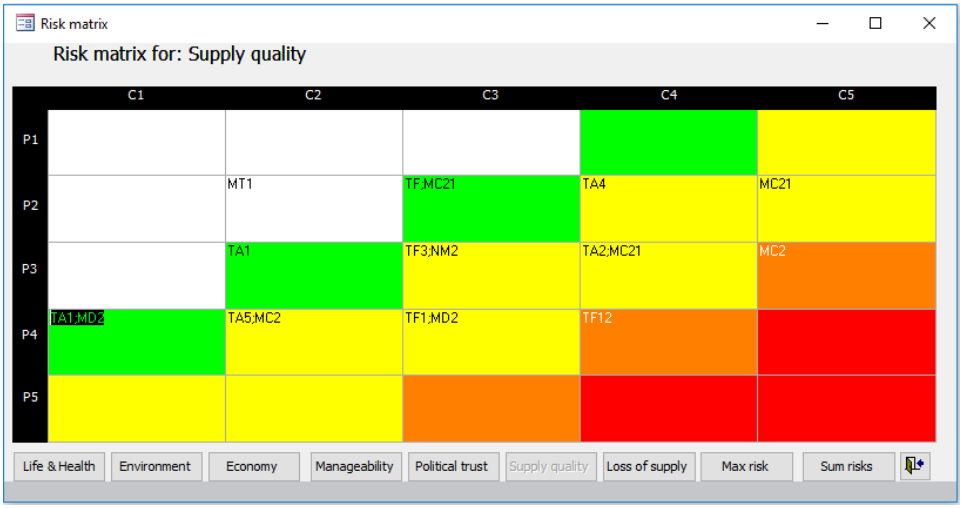


Figure 34: Risk matrix.

Main events

Main focal points of risk analyses in InfraRisk-CP are the Main events (or Type of source) that describe the nature of risk by structuring 'What can go wrong? in the hierarchical structure of events.

The upper two levels in the main-event structure are shown in Figure 35:

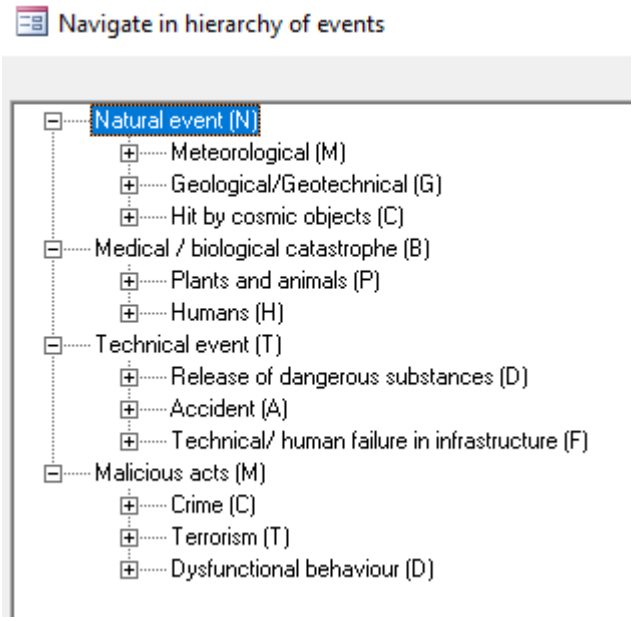


Figure 35: Structure of Main Events in InfraRisk-CP.

For a complete list of main events reference is made to Table 20 of ANNEX D.

The most evident events are found under Technical event – Technical/human failure in infrastructure, but also some other types of events are relevant in STOP-IT.

As mentioned, the main events are the starting point of the risk analysis conducted in the InfraRisk-CP. The analysts may choose an event from any level of the hierarchy, but usually level four would be the most precise starting point. Note, that component failures are not the starting point. Component failures are rather addressed by listing one or more of the so-called *societal critical functions* (SCFs) related to the main events.

The following options are available related to the main events:

- **Change event:** This means to navigate in the hierarchy of main events to find a more appropriate event, see Figure 35.
- **New event:** Add a new event to the InfraRisk-CP database. An event is a record in the database. When a new event is to be added to the database, the first step is to navigate in the hierarchy of main events to find an appropriate event (Figure 35).
- **Copy event:** Copy the current event to a new event. You are prompted to add a new event identifier. Note that InfraRisk-CP comes with the 81 risk elements from the RIDB. A typical working procedure will be to identify a generic risk element from the 81 RIDB events, then copy it to a new Infra Risk CP record representing a site-specific risk element. For such a site-specific element it is natural to assess probability and consequences.

Main events societal critical functions (asset)

The SCFs are generic components or functions in the critical infrastructure[2]. The SCFs are functions that if they fail to deliver the required output this will reduce the quality of life. The SCFs may be linked to main events in three different manners:

- Loss of, or reduction in the performance of the SCFs could be *the cause* of a main event. In this situation we say that the SCF works “before” the main event. An example is “Pipes” in relation to the main event 'Failure to deliver (critical infrastructure like water supply)'
- The loss of, or reduction in the performance of the SCFs will *increase the consequences* if the main event occurs. In this situation we say that the SCF works “after” the main event, i.e., it operates as a barrier or a mitigating measure. An example is “Backup systems for water” in relation to the main event 'Failure to deliver (critical infrastructure, water supply)'.
- The occurrence of the main event will threaten the performance of the SCF. An example is “Failure to deliver (critical infrastructure, cooling water)” in relation to the SCF “Transformer (in hydro power production)”.

In InfraRisk CP, the SCFs are structured in a four-level hierarchy. In addition to other infrastructures, Figure 36 shows the underneath level for Critical infrastructure, remaining C, Water and sewage systems (1) as it appears in the tool:

[2] See also: *ISO 55000 Standards for asset management* - Assets, and value realized from them, are the basis for any organisation delivering what it aims to do.

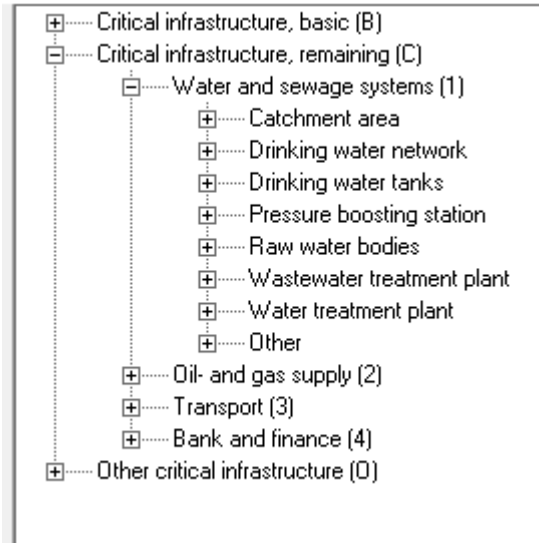


Figure 36: Societal Critical Functions (SCF) to third level.

Note that STOP-IT has introduced a specific notation corresponding to level 3 and 4 in the SCF structure. Level 3 corresponds to *Type of asset* and level 4 corresponds to *Specific asset*. Figure 37 shows a snapshot of this structure for the two first types of assets (catchment and network) with corresponding specific asset. For a complete list for all types of assets related to water distribution systems (see Table 21 in of ANNEX D).

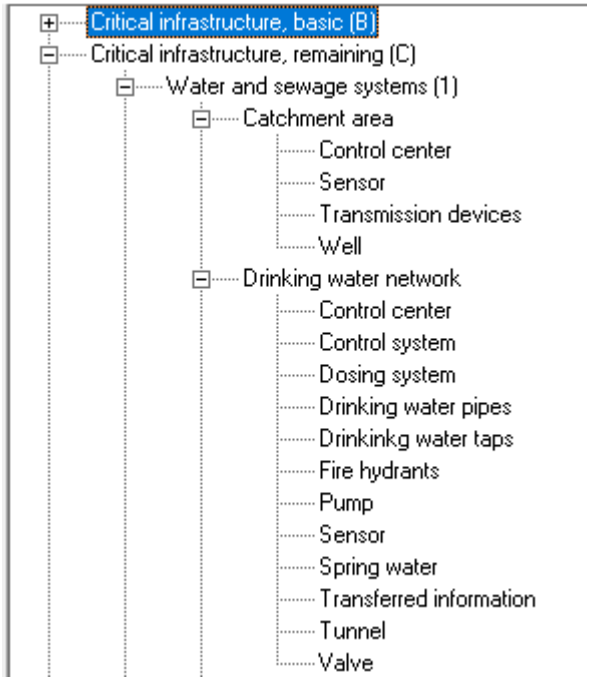


Figure 37: SCF at level four for Catchment area and Drinking water network.

It is noted that the term “function” is used rather than “component” to emphasize that there are *functions* to be carried out, for example “pumping water”, “store water”, “control water flow” and so on. In most cases there are components installed to carry out these functions, i.e., pumps, water tanks and valves, respectively.

Note that there is a many-to-many relation between the *main events* and the *SCFs*.

In the analysis it is possible to establish several main events with the same name, and then make a one to one relation between each SCF and one of the main events. But a more efficient way could be to only have one main event, and then list some, or all the relevant SCFs to that main event.

For each SCF linked to the main event the type and strength of relation to the main event should be specified by using one of the codes in Table 13.

Table 13: Type and strength of relation between the SCF and the main event.

Code	Text
I100	Loss of SCF is the initiating event in the scenario
B100	SCF acts as a complete barrier
R90	SCF is very important for the scenario
R60	SCF is important for the scenario
R40	SCF is medium important for the scenario
R15	SCF is not very important for the scenario
R05	SCF is hardly important for the scenario
V90	SCF is very vulnerable wrt the main event
V60	SCF is vulnerable wrt the main event
V40	SCF is medium vulnerable wrt the main event
V15	SCF is not very vulnerable wrt the main event
V05	SCF is hardly vulnerable wrt the main event

The numbers in the code field represent the importance of the SCF with respect to the scenario being analysed. When a criticality measure is established, this number is used to give a score of the SCF.

Vulnerability factors

Vulnerability factors are factors that need attention when assigning probabilities and consequences to the main events. In ANNEX D, Table 22 the full overview of vulnerability factors and their values is presented. Some of the key aspects covered by the vulnerability factors are as follows:

- Area

- Geographic scope
- Population density pr 1 km²
- Outdoor temperature
- Time of day
- Duration
- Dependency with other social critical functions
- Substitution opportunities for infrastructure
- Degree of coupling
- Culture
- Mental preparedness

Frequencies, probabilities and consequences

A 5-point scale is used In InfraRisk-CP to assign a frequency to each main event:

1. Very unlikely Less than once per 100 year
2. Remote Once per 10-100 year
3. Occasional Once per 1-10 year
4. Probable 1 to 10 times a year
5. Frequent More than once a month

For malicious acts a procedure with use of scores has been developed to assess the frequency (see section 3.2.2 for further details).

Given the occurrence of the main event, one or more consequence dimensions could be specified:

- Life and health
- Environment
- Economy
- Manageability
- Political Trust
- Reputation
- Lifeline quality
- Lifeline unavailability

In InfraRisk-CP (according to STOP-IT aims), the term 'lifeline' means important means for the public welfare, typically like 'drinking water'.

Note that in the STOP-IT RIDB it is only possible to specify one consequence dimension for each event, whereas InfraRisk-CP allows to use any combinations of consequence dimensions.

A five-point scale is used to assign the severity for each consequence dimension relevant for the main event:

1. Delimited
2. Some damage

3. Serious
4. Critical
5. Catastrophic

With regards to assigning a severity number given the occurrence of the main event, the severity should be seen as a random variable which in principle could take all possible values. Since only one value could be specified at a time in InfraRisk CP, it is common to assign a (reasonable) “worst case” value. With “reasonable” we here mean a value where the probability of a severity of higher intensity is very low. The severity assigned is thus, a conservative number. To compensate for this conservatism, a probability of experiencing the “worst case” is assigned to each consequence dimension by using the following five-point scale:

1. Very unlikely One out of 1000
2. Remote One out of 100
3. Occasional One out of 10
4. Probable One out of 2
5. For sure Occurs with certainty

As an example, consider a pipe breakage. The failure frequency is assigned to *Probable* = *Once per 1-10 year*. Due to redundancy in the network the lifeline unavailability is usually *Delimited*. However, in a few cases, say *Remote* = *One out of 100*, the redundancy is lost due to one or more other failures in the system. If this happens, the lifeline unavailability is considered *Serious*. The occurrence of an event with serious impact on the lifeline unavailability will then be once per 100 to 1 000 years.

It should also be noted that a component failure (loss of a societal critical function - SCF) will not always result in the main event due to effective barrier(s) or system redundancy.

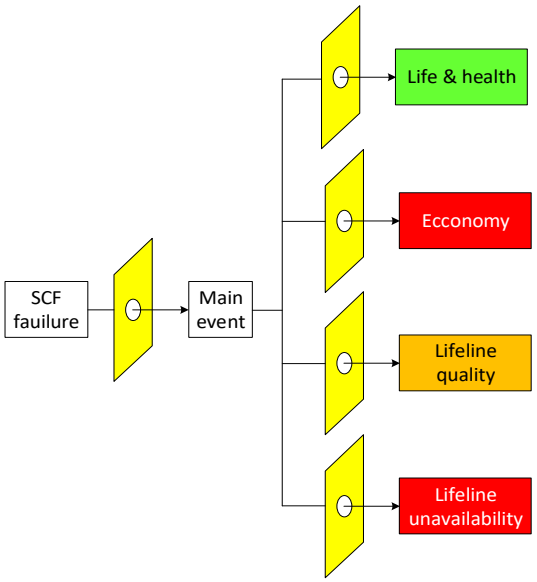


Figure 38: Relations between SCFs, main event and consequence dimensions

Figure 38 illustrates the situation. A failure in an SCF will not necessarily result in a main event. For example, a critical pipe failure can be harmless if a water thank will provide water during the upset, or until the pipe failure is repaired. This is illustrated by the yellow "barrier" ( ) between the SCF and the main event in Figure 38. Further the impact of the main event on "life & health" could be eliminated by preparedness measures (e.g., each family has a stock of bottles with drinking water). The example shows a higher impact on "economy" where it could be more difficult to implement preparedness measures. The "strength" of the various "barriers" between the main event and the various consequence dimensions could vary. In InfraRisk-CP this is accomplished by allowing different probabilities for the "worst case" event to occur, as mentioned above.

Risk reduction measures

To add or modify selected risk reduction measures select the magnifier ( ) to the right of the risk reduction measure field (Figure 33). A new tab opens where it is possible to tick of the selected risk reduction measure (Figure 39). The list depends on the specified specific assets (SCF's) and the type of event. Press the "Save and close" button to save the selected measures. In the risk measure field, the short names of the selected measures are shown.

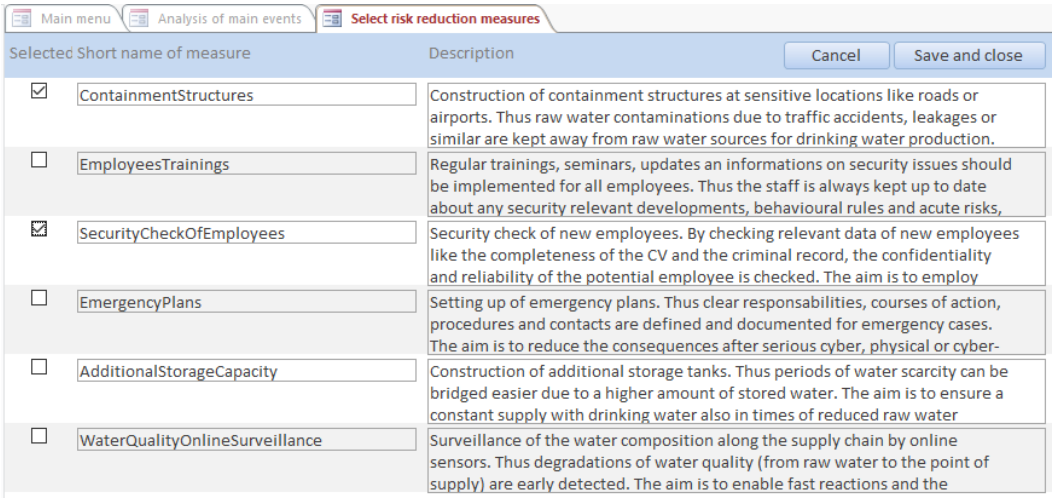


Figure 39: Selection of risk reduction measures

2.4.2. Single scenario assessment – 2nd level of analysis

In this chapter we demonstrate the end-user's perspective through a step-by-step narrative for the single scenario assessment level.

When the end user selects the single threat scenario assessment, he usually wishes to get a better picture of the network performance under a selected threat. In order to create the threat scenario, the user must have a structured and comprehensive overview of those threats and their characteristics. More specifically, he may want to analyse the path of

cascading events that are triggered when selecting a particular threat. To facilitate those needs, the Fault Tree Viewer has been developed as part of the RAET (see Part D for details). It visualises fault trees that lead to an undesired state of the system, currently a water quality or quantity issue as seen in Figure 40.

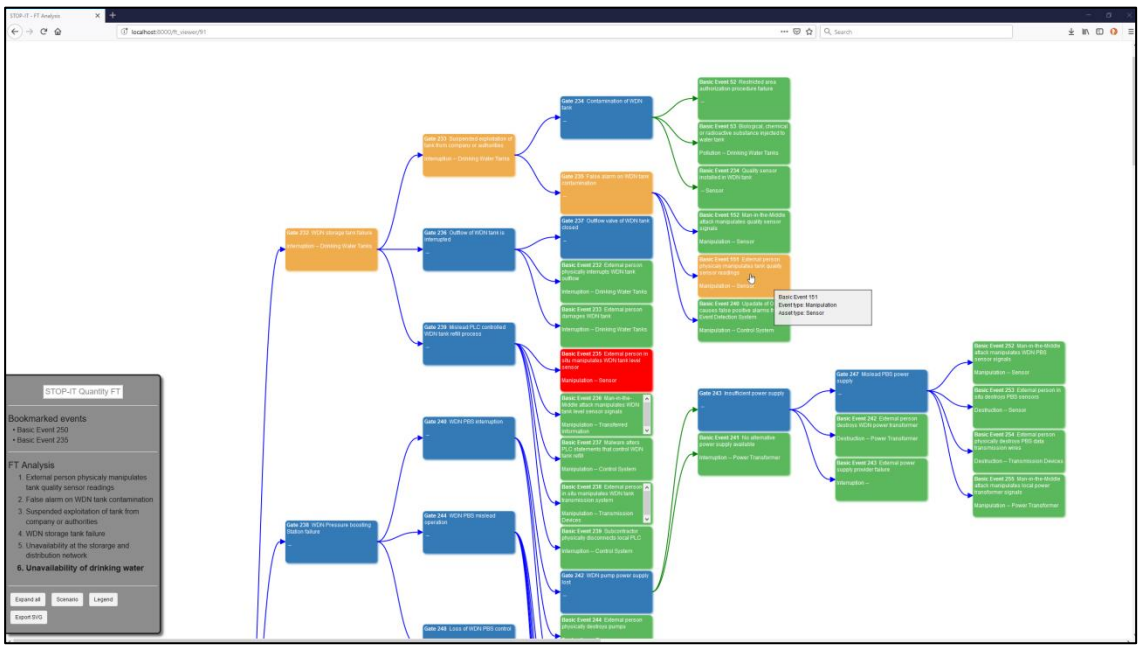


Figure 40: Fault Tree viewer - Overview of identified potential risks in FT structure

The user may explore the FT zooming in and out the FT and analysing possible cascading effects of specific events. When hovering over an event (intermediate or basic) all events that are triggered directly or indirectly by this event are highlighted and the names of all affected events up to the top event are listed. Additionally, the FT Viewer indicates if another condition is required to trigger an event.

After exploring the FT, the user may want to bookmark certain events for further use as part of a scenario, regardless whether they represent basic or intermediate events. The user may then switch to another FT to explore events of another category, e.g. water quantity or water quality. In case he has developed customized FTs using the FT Editor, these can also be projected and selected events of these FTs can be bookmarked as well.

After visualizing the events and cascading effects of undesired states of the system and having identified potential threats that need to be examined further, the user can assess the vulnerability of his infrastructure by calling the Asset Vulnerability Assessment Tool. It will calculate the vulnerability of the system as a whole and will provide an estimation of the vulnerability of the water network at the level of nodes and links. Results of vulnerability assessment enable prioritisation of assets, based on the scenario and the current conditions of the system.

Having a more precise view of potential threats and the most vulnerable assets of the CI, the user may now start with the specification of the threat scenario. This process will be assisted

by a wizard of the Scenario Planner in the following way:

1. The wizard provides filters to narrow down the list of events that will be part of the scenario (Figure 41). One filter refers to the previously bookmarked events. However, other additional filters may be used referring to the event type, the related asset type, the Fault Tree and the tool capable to simulate the event. As a result of this step a single event will be selected by the user.
2. The selected event may be applied to a number of assets, i.e. components of the CP infrastructure of the water utility. The wizard recognizes those assets and lets the user select the one that will be affected.
3. Depending on the nature of the event (event type) the asset type and the tool selected to simulate the scenario, a number of additional parameters will be presented, the values of which must be specified by the user. These may be related with the simulation process (start time and duration of the event) or the event itself (e.g. for the pollution of a tank: which pollutant, the quantity, the way of injection).

The above steps can be repeated in order to add multiple events to the same scenario.

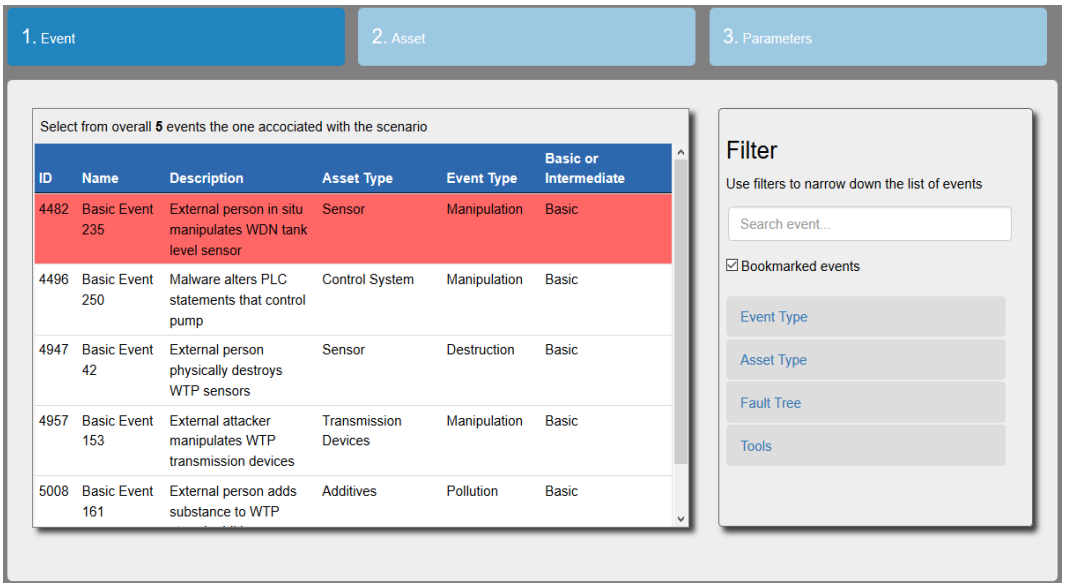


Figure 41: Scenario Wizard – Event selection

The SP database contains additional information related to the saved scenarios, and is capable to manage a large number of scenarios for CI of a water sector. In order to facilitate the task of managing the scenarios, the SP is designed to provide a number of functionalities. The user can gain access to the database through the SP, as seen in Figure 42, and, through that interface, have an overview of the scenarios contained in it. But managing a list of scenarios, based only on names or triggered events would not be useful. For this reason, the interface provides additional information, such as: a) known tools that are capable to simulate the scenario, b) the reference (base) scenario c) the number of events defined in this scenario

d) whether the scenario has been executed and scenario results are available and e) the exact date and time when the scenario has been created and executed.

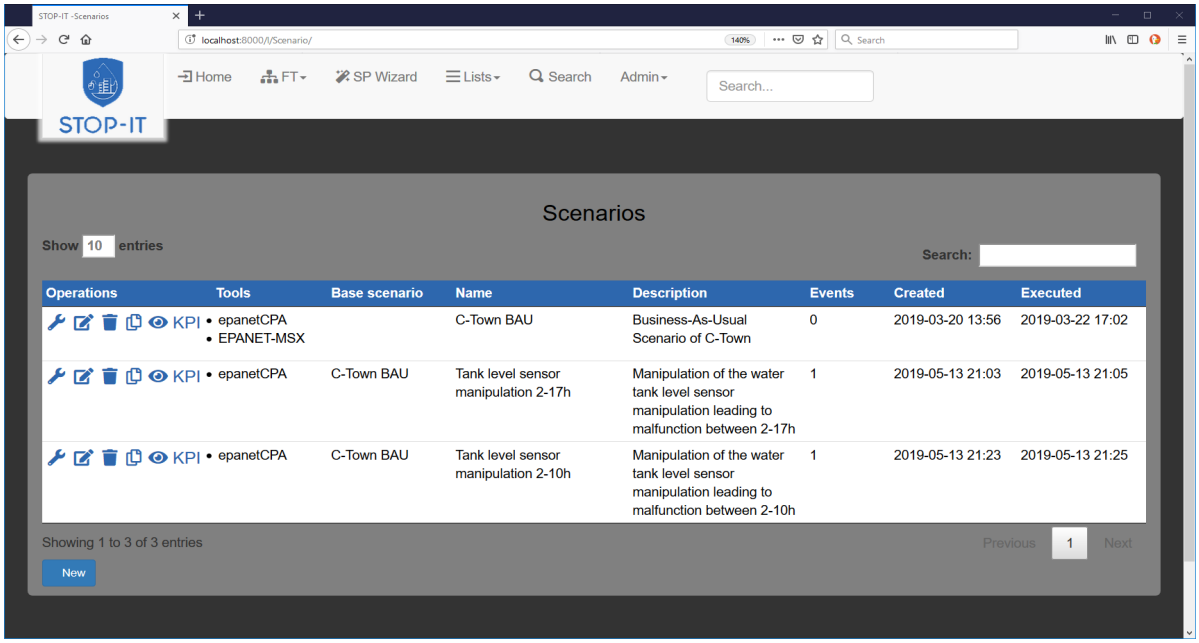


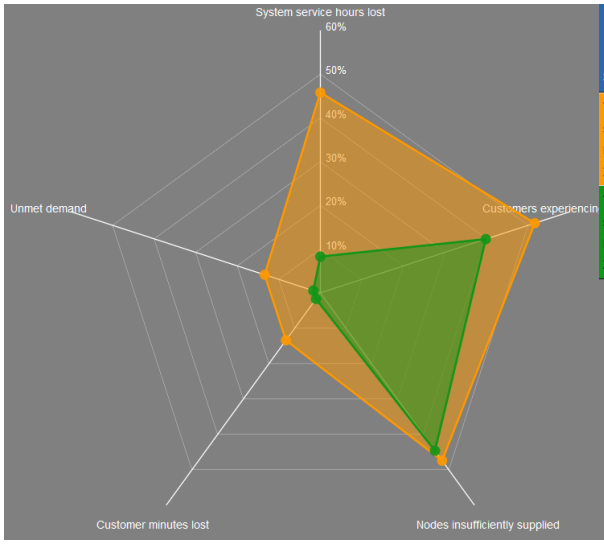
Figure 42: Scenario Planner Tool – Scenario list view containing saved scenarios, related information and available operation buttons

After having created asset specific threat scenarios for the system, the user must select the simulation platform to assess performance and evaluate risk. In order to facilitate this procedure, the Toolkit Library (TL) can be used. Navigating through TL, the user can see a number of useful information related to the cyber-physical protection of water sector CIs. Most notably, he can search for the capabilities of the tools, identifying those tools which are capable to simulate specific scenarios. Even if the selected tools are not supported by the RAET and thus they cannot be executed from the platform, the user can retrieve useful information regarding the usability, licensing, potential costs etc. of the tool and navigate to the tool's page for further information and download. Since the STOP-IT project is focused on cyber-physical attacks, it would be common for TL to propose not one, but a set of tools in order to simulate both cyber and physical layer.

Using the TL, the user has successfully identified, downloaded and set-up the tools most appropriate to the threat scenario and must now prepare the simulation data. Different tools require different data and input format, making the step of simulation model dependent and the user's perspective different for each tool.

Some tools are directly supported by RAET, i.e. they are integrated in the platform and relevant scenarios can use these tools for simulation and assessment of the results. These tools are displayed in the Scenario list view. A runner icon next to the tool indicates that the scenarios are ready to be simulated by these tools. The process begins by clicking on the icon and may take a while to complete, depending on the selected model and the data.

Simulation results are presented in a common way using well defined KPIs and metrics. Graphical elements (charts, tables) facilitate comparisons between scenarios (Figure 43).



Scenario	Unmet demand (litres)	Nodes insufficiently supplied	Customers experiencing insufficient service	Customer minutes lost	System service hours lost
Tank level sensor manipulation 2-17h	2041030	184	51691	14666168	11.0
Tank level sensor manipulation 2-10h	261877	173	39869	1875543	2.0

Figure 43: Comparing scenario results

RAET's provides the possibility to navigate through the RRMD and search for suitable risk reduction measures. A first match is made by the system based on the characteristics of risks and measures and the results are presented to the user for the final selection

After having selected the RRMs, a new treatment scenario is created. Similarly, to the Risk Analysis and Evaluation steps, the user must now simulate the behaviour of the system against the threat scenario, but this time under new conditions in the system. Since the system under examination and the threat remain the same, the appropriate tools for simulation remain the same. Changes must be made to the input data of the models, in order to include the new conditions created by the RRMs selected. After running the simulations, the output results are mapped in KPI dimensions, similar to the procedure of the threat scenario analysis.

2.4.3. Multiple scenario assessment – 3rd level of analysis

Having analysed the overall procedure of exploring, simulating and evaluating a risk in a single scenario step, the multiple scenario assessment follows in principle the same steps. The 3rd level of analysis is the enhanced procedure of evaluating cyber-physical threats through the WP4 tactical and strategic planning tools. This process is designed to minimize uncertainty of risk assessment linked with the subjective view of a plausible threat scenario. A multiple scenario approach can also reveal which threat is more serious/critical for the given system configuration under current risk criteria. In this spirit, 2 approaches in the multiple scenario assessment level can be identified.

The first approach refers to a set of scenarios created in a random manner. At first, a basic threat scenario is identified, through the available FTs. The user can narrow down the

selection using filters and finally select an event for the scenario. Having selected the event, the user is requested to specify the asset upon which the event will be applied, as well as additional specific parameters. The user must now define ranges for those parameters for which values will be randomly specified by the system. Those ranges are utilised to define the boundary conditions for each new threat scenario. An appropriate algorithm is utilized in order to randomly vary and assign parameters values and create a new scenario each time. The SP will subsequently create the input files according to the scenarios and call the STP in a batch mode. This configuration creates a scenario relationship, resembled in the next figure.

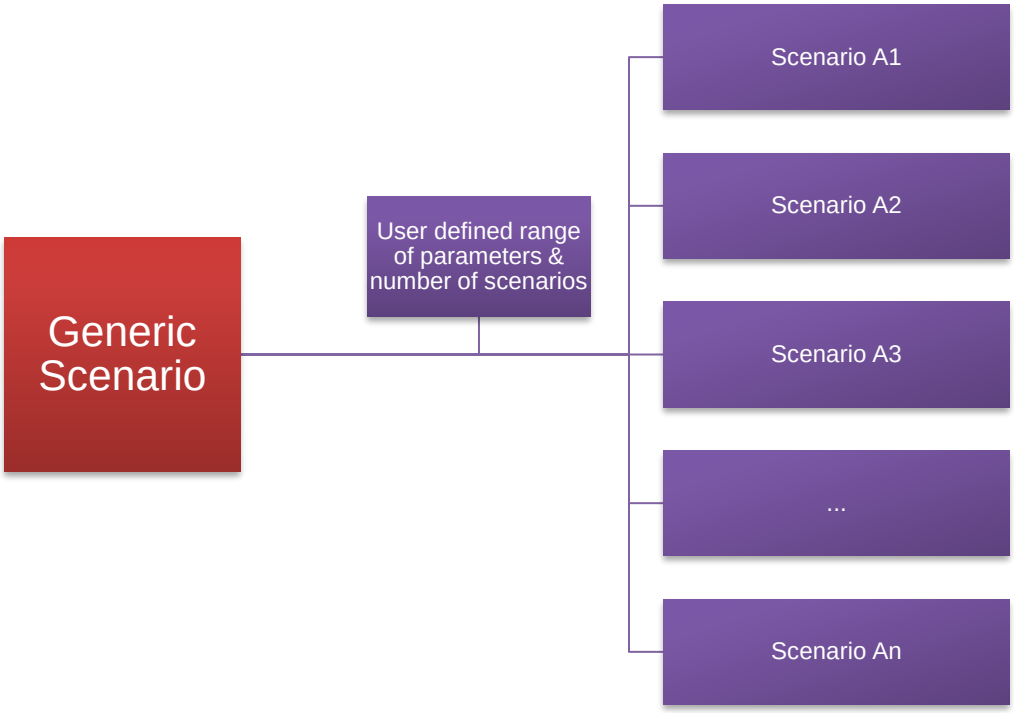


Figure 44: Randomised Scenario generation schematic

This structure demonstrates that all scenarios are linked to a parent generic scenario, on which random parameterisation is applied. For this approach, the scenario generation is independent from the results of the previous scenario.

The second approach is an optimization procedure where the creation of a new scenario is based on the results of the previous ones. This is achieved by applying an optimization algorithm and defining an objective function, based on the available STOP-IT KPIs. Note that the metrics are specifically designed to serve the purpose of optimization by directly referring to the loss of performance quantitatively. As described in the paragraphs dedicated to the KPI Framework, the metrics are built to reflect the risk criteria of a company, thus allow for a flexible adaptation. One way to define the goal of the optimization algorithm is to maximize the value of the objective function, a process which will identify the events with the maximum risk.

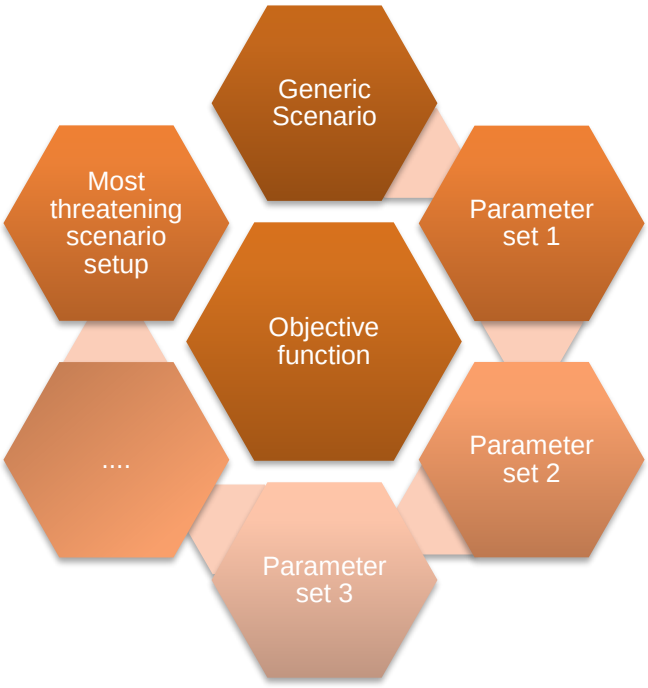


Figure 45: Optimization Scenario Generation schematic

For a given generic scenario and the user defined parameter ranges, the process of the single scenario is applied to every new instance, simulating and mapping results to the appropriate KPIs. The functionalities used for the multiple scenario level are linked with processes in Task 4.4 (STP), for which the development has not been completed yet. Due to this dependency, the user's perspective on the 3rd level of assessment will be updated after submission of D4.4.

3.1 Introduction

3.1.1. Background

The InfraRisk-CP tool is based on the previous InfraRisk developed in the DECRIS project[3]. The original scope of InfraRisk was analysing different risk scenarios and consequences across various interlinked infrastructures. Although the cyber-physical (CP) threat to infra-structures was not a part of the original InfraRisk, it was indirectly addressed by the code structure that was developed. By bringing InfraRisk towards the STOP-IT aims, the InfraRisk-CP explicitly addresses the cyber-physical threats to water systems and corresponding risk assessments. The tool is mainly intended for the generic (and secondarily single) scenario assessments as part of the WP4 framework. In addition to InfraRisk-CP, the Asset Vulnerability Assessment Tool (AVAT) developed in STOP-IT (D4.1) supports the initial risk and vulnerability assessments of specific water distribution networks.

A brief description of the main elements of InfraRisk-CP follows. Special attention is put on the cyber-physical aspects of water infrastructures and the risk assessment of such. The risk assessments in InfraRisk-CP are mainly based on expert judgments of the vulnerabilities and risks affecting on specific assets. The tool is independent of system models such as EPANET, FTA, RBD, etc. but information from such tools may be applied for the specific assessments. Information from other tools developed in WP4, such as e.g., the generic risk identification data base (RIDB), the risk reduction measure database (RRMD), and the AVAT-tool (D4.1) are applied when found relevant, or convenient when conducting risk and vulnerability assessments by use of InfraRisk-CP.

The former InfraRisk tool basically supported two analysis levels. At overall level, the tool worked very much as a so-called preliminary hazard analysis (PHA). Risk is directly assessed by specifying the frequencies and consequences of main events.

More comprehensive risk analysis was possible in the former InfraRisk with modelling of the explicit linkage between the SCFs and main events. Formal assessment of the frequencies and consequences was achieved by applying fault tree analysis (FTA), reliability block diagrams (RBDs) and event tree analysis (ETA). Some functionalities to support these types of analyses methods are available as sub-modules in the former InfraRisk tool also. These functionalities are not further developed in InfraRisk-CP.

[3] Norwegian research project financed by the Norwegian Research Council, 2008-2009.

3.1.2. Installation and setup

InfraRisk-CP is implemented in MS Access. This means that the program runs on a personal computer where MS Access is installed. Note that Mac does not support MS Access, hence InfraRisk-CP cannot be run on a Mac.

InfraRisk-CP comprises two separate files:

InfraRiskCP.accdb: This is the program file. In addition to visual basic code it contains data tables with predefined codes, hierarchical structures for assets and events and so one.

InfraRiskCP_RIDBdata.inr: This is the data file with all risk elements. The first time InfraRisk-CP is installed, this file contains the 81 RIDB events. But as the user runs cite specific analyses, the datafile will be extended. Therefore, if an update of the program file is launched in the future, this make sure that the datafile is not overwritten.

The files are zipped into one zip file, **InfraRiskCP.zip**. The program and data files may be unzipped to any folder, but it is recommended to download the files to a trusted area because the program file contains code.

Note that an InfraRisk-CP datafile has the extension **.inr**. The user may copy the original datafile and give it an appropriate name, for example by using the name of a town and the year the analysis is conducted. File extension should always be **.inr.**

To run InfraRisk-CP just double-click on **InfraRiskCP.accdb**, or open the file from within MS Access. Unless **InfraRiskCP.accdb** is downloaded to a “trusted area”, MS Access will complain the first time **InfraRiskCP.accdb** opens because the file contains code. To activate the code, click on the yellow bar stating “Enable content”.

InfraRiskCP.accdb creates a link to the data file being last used. This means that it is not necessary to load the appropriate datafile from time to time. However, if the link is broken, the user is asked to specify a new file from the standard file selection menu. Navigate to the appropriate file folder, and select a valid InfraRisk-CP datafile. From the main menu the user may at any time change the project, i.e., load a new datafile.

3.2 Methodology

3.2.1 Risk assessment in InfraRisk-CP

3.2.1.1 Direct assessment

The risk identification database (RIDB) has been established as part of WP3 in STOP-IT, also based on a direct assessment approach. Event descriptions in the RIDB could be seen as generic events independent of any water distributions network, system configuration, vulnerability factors, and so on. Direct assessments without any support from calculations are regarded as generic assessment. As discussed in Part B the similarities between the RIDB and InfraRisk-CP databases are evident, and little effort is required to import

information from one to the other (e.g. putting data from RIDB and RRMD into the InfraRisk-CP format).

The current version of RIDB contains 81 events. These events are already loaded in InfraRisk-CP and could be used as generic templates for the specific analyses to be carried out.

3.2.1.2 Calculations and scoring approach based on vulnerabilities

For a specific site and network structure, given a set of vulnerability factors, it is to some extent, possible to calculate the risk of the generic events imported to InfraRisk-CP from RIDB. Note that the risk elements in RIDB are not quantified in terms of frequencies nor consequences. But when the generic RIDB risk elements are imported into InfraRisk-CP the values for the frequencies are set to (3) Occasional, and the values for the consequences are set to (3) Serious.

A simple way to calculate the risk numbers from the generic RIDB is to establish a scoring approach. The scores are established based on assessment of the vulnerability factors. In InfraRisk-CP the vulnerability factors will have the following impact:

- Prior to main event
- After main event
- Both prior to, and after main event

Further, each vulnerability factor is given a value on a five-point scale:

1. Very favourable
2. Favourable
3. Medium
4. Un-favourable
5. Very un-favourable

A simple regime for scoring and updating the result from the generic RIDB is as follows:

It is assumed that for the generic values on probabilities and consequences in RIDB, these values have been assessed under the assumption that the vulnerability factors all have a value of 3 = Medium.

For the adjustment of frequency of in event, consider vulnerability factors that either act prior to the main event, or both prior and after the main event. For these factors calculate the average values from the five-point scale and subtract 3 (corresponding to medium). This number is added to the frequency of the main event from the generic RIDB.

For the adjustment of consequences, the vulnerability factors that either act after, or prior to the main event, or both after and prior is used to find an average score where we also here subtract 3. This score is then consequence number.

Note, that calculating a score for the vulnerability factors will give a real number, and the nearest integer should be found to adjust the frequencies and consequences which are on integer levels.

3.2.2 Frequency assessments of physical and cyber attacks

A method for assigning frequencies to malicious attacks where it is hard to use pure statistical data for assessment is expected. Thus, only a qualitative or semi-quantitative determination of the frequency is possible. IWW has proposed a method for assessment of physical attacks based on DVGW (German Technical and Scientific Association for Gas and Water) Information Water No. 80. In STOP-IT deliverable D4.1 Asset Vulnerability Assessment to Risk Events, and in NTNU memo STOPIT-8, an approach for cyber-attack was proposed. The objective has been to unify the two approaches for implementation in InfraRisk-CP.

To assess the frequency of a successful attack to the water distribution system the following approach is followed:

1. To find the frequency of an attack attempt (sometimes referred to as likelihood of threat happening) a set of questions is provided

2. For each question there is a predefined list of answers, where each answer is associated with a score. A low score means that there is not much support for an attack attempt and a high score means that there is support for expecting an attack attempt.

3. The scores are aggregated to give a total score for the frequency of an attempt

4. To transform the score to a frequency number a low value, f_L, and a high value f_H are defined. f_L represents the frequency of an attack attempt if all scores for the attack attempt questions have the lowest possible values, and f_H represents the frequency of an attack attempt if all scores have the highest possible values. As default values f_L = 1/100 (one per hundred years) and f_H = 20 (20 per year) are used. The user of InfraRisk-CP may change these values, but they remain constant for all assessments.

5. To find the probability of the success of an attack attempt (sometimes referred to as likelihood of threat succeeding) another set of questions is provided

6. For each of these questions there is also a predefined list of answers, where each answer is associated with a score. A low score means that there is not much support for a successful attack attempt and a high score means that there is support for expecting the attack attempt to succeed.

7. To transform the score to a probability number a low value, p_L , and a high value p_H are defined. p_L represents the probability of a successful attack attempt if all scores have the lowest possible values, and p_H represents the probability if all scores have the highest possible values. As default values p_L = 1/100 and p_H = 0.5. The user of InfraRisk-CP may change these values, but they remain constant for all assessments.

To find the frequency of a successful attack attempt, the frequency of an attack attempt is multiplied with the probability of success.

3.2.2.1 Physical attacks

Frequency of physical attack

For physical attacks, the following questions with possible answers are provided for the estimation of the frequency:

Q1: How attractive is the asset to the perpetrator?

1=Very low attractivity
2=Low attractivity
3=Medium attractivity
4=High attractivity
5=Very high attractivity

The attractivity is influenced by the possible damage potential, the political, social and economic importance, the psychological effects as well as by the affected end-users (military institutions, parliaments, chemical industry, residence of important people like a president or similar). The classification of the attractivity is done subjectively as for example the perpetrator is not known at the time the assessment is done.

Q2: How is the actual security situation evaluated by the security authorities?

1=Police intelligence does not expect any threats
3=Evidences for a threat exist
4=The asset is endangered, an attack cannot be excluded
5=The asset is in significant danger, an attack should be expected

Information about the actual security situation can usually be gained at the responsible police authority.

Q3: How relevant is the asset for the overall water supply?

1=Low
2=Medium
3=High
4=Very high
5=Critical

A systematic can be applied to answer this question. For example, each answer can be matched to a certain percentage of end-users/people (e.g. Low -> <10 %, Medium -> <25 %, etc.). Other possibilities could be the matching of answers with percentages of the overall drinking water amount affected or similar. It might often be true that the asset is e.g. very relevant for a certain part of the network but only medium relevant for the overall network. In these cases, the relevance of the asset should be rated with regard to its importance for the affected part of the network.

Q4: How difficult is it to carry out a criminal act?

1=Extremely high effort necessary (1 point)
2=Medium effort necessary (2 points)

3=Little to no effort necessary (3 points)

The choice of an answer is based on the assumed effort of the perpetrator and the possibility to be successful with that assumed effort. For the evaluation the attack path of “lowest resistance” should be considered.

Q5: Do special environmental conditions exist that temporarily increase the need for protection?

1=No special conditions (1 point)
2=Few special conditions (2 points)
3=Substantial special conditions (3 points)

Here special temporarily occurring events or conditions are regarded. Examples could be government visits, major events, festivals, etc.

Now let L* be the sum of scores achieved for questions Q1 to Q5. L* can take values in the range 5 to 21, and a standardized score between 0 and 1 is given by: *L = (L*-5)/(21-5) = (L*-5)/16*. The frequency of a physical attack is now calculated as:

$$f = f_L \left(\frac{f_H}{f_L}\right)^L \quad (1)$$

Where f_L and f_H are defined as limiting values for the frequency, see section 3.3.1.2 for how to change these values.

Probability of physical attack succeeding

The following questions with possible answers are provided for the probability of a successful attack:

Q6: How is the asset built? Is it easily visible for the public?

3=Object not visible for public
2=Object visible without restrictions
1=Object only accessible by interruptions of the public life (railway, streets, etc.)

For example, if an asset is built in a very enlivened area of a city an attack is more likely to be detected by people and thus, not succeeding compared to an attack on an asset that is built in a forest where a perpetrator is more or less undisturbed.

Q7: In which resistance class is the perimeter protection built?

2=RC1-RC2
1=RC3-RC4
0=RC5-RC6

The different resistance classes used in the possible answers are defined in DIN EN 1627. (DIN 2011). If there is any gap or similar in the perimeter protection, the score of 2 is given.

Q8: In which resistance classes are the walls of the buildings including their integrated integrations?

2=RC1-RC2

1=RC3-RC4
0=RC5-RC6

The different resistance classes used in the possible answers are defined in DIN EN 1627. (DIN 2011). If there is any gap or similar in the protection like unprotected windows lower than the first floor, the score of 2 is given.

Q9: How is the sensory surveillance realized?

2=No sensory surveillance
1=Binary Contacts, e.g. open/closed
0=Measured value-based surveillance, e.g. sensitivity of sensor can be regulated

The evaluation of the sensory surveillance should be realized at the weakest position of the barriers.

Q10: How are organizational measures implemented?

2=No organizational measures exist
1=Primary dissuasive measures are implemented like alarms, only irregular patrolling
0=Organizational measures ensure, that a direct defensive reaction is initiated (e.g. the police is called, the system is shut down)

Now let Q^* denote the sum of scores for questions Q6-Q10. Q^* can take values in the range 1 to 11, and a standardized score between 0 and 1 is given by: $Q = (Q^*-1) / (11-1) = (Q^*-1)/10$. The probability of success of an attempt is given by:

$$p = p_L \left(\frac{p_H}{p_L}\right)^Q \quad (2)$$

Where p_L and p_H are defined as limiting values for the probability, see section 3.3.1.2 for how to change these values.

Frequency of successful physical attack

The frequency of a successful attack is given by:

$$f_A = f \times p \quad (3)$$

The frequency in equation (3) gives directly a frequency per year. In some situation it is desirable to assign the frequency of successful attack to a likelihood category. In InfraRisk-CP the following likelihood categories are defined:

1. Very unlikely Less than once per 100 year
2. Remote Once per 10-100 year
3. Occasional Once per 1-10 year
4. Probable 1 to 12 times a year
5. Frequent More than once a month

These categories are used to transform the frequency in equation (3) to a category number. An example of frequency assessment of physical attacks is shown in Figure 46.

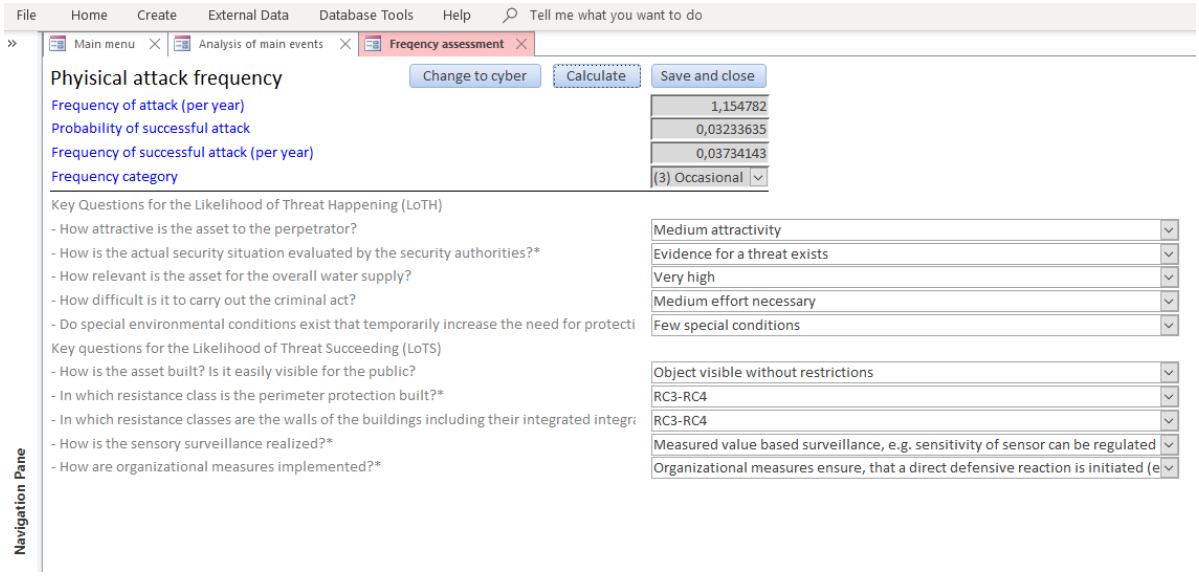


Figure 46: Frequency assessment of physical attacks

3.2.2.2 Cyber attacks

Frequency of cyber attack

For assessing frequencies of cyber-attacks, a list of questions is provided, where scores are obtained for each sub question (s1, s2, etc). The scores marked by a star (*) are common to all component conditions considered as global conditions for the critical infrastructure under consideration. Scores not marked with a star are considered as component specific conditions. If no information is available a score of 3 is given. If a question is not considered relevant, the score excluded from the aggregation. The scores are grouped under some headlines:

How attractive it is to make an attempt to attack the water distribution system?

s_1 = ..in terms of Recognisability (1=very low,2=low,3=medium,4=high,5=very high) *
s_2 = .. in terms of Symbolism (1=very low,2=low,3=medium,4=high,5=very high) *
s_3 = .. in terms of Potential for economic profit (ransom) (1=very low, 2=low, 3=medium, 4=high,5=very high) *
s_4 = in terms of Potential for political profit (1=very low,2=low,3=medium,4=high,5=very high) *

Note: Recognisability deals with attackers having a desired to be recognized within a community. Typically, this could be individual hackers. Symbolism could be relevant for terrorist groups which often have an objective to cause fear and uncertainty. Economic profit would relate to organized crime. Political issues could relate to foreign nations or political groups within one nation.

Organizational issues:

s_5 = Measures implemented towards insiders (1=very high,2=high, 3=medium, 4=low,5=very low)*

s_6 = Quality of internal surveillance and intelligence systems (1=very high,2=high, 3=medium, 4=low,5=very low) *

s_7 = Systematic preparedness exercises, investigation and learning (1=very high, 2=high,3=medium, 4=low,5=very low) *

s_8 = Security focus in agreements with vendors and contractors (1=very high,2=high, 3=medium, 4=low,5=very low) *

Conditions affecting if an attacker will make an attack attempt for a specific component:

s_9 = How vulnerable the component seems from the attacker's point of view (1=very low, 2=low, 3=medium,4=high,5=very high)

s_{10} = Visible protective measures by the utility manager for the specific component (1=high, 5=low)

s_{11} = How critical the component seems from the attacker's point of view (1=very low,2=low, 3=medium,4=high,5=very high)

s_{12} = Accessibility of the particular component (1=very low,2=low, 3=medium, 4=high,5=very high)

s_{13} = Attacker's capability vs required capability to make an attempt (1=very low, 2=low,3=medium, 4=high,5=very high) *

s_{14} = Attacker's available resources vs required resources to make an attempt (1=very low, 2=low, 3=medium,4=high,5=very high) *

Evidence with respect to possible attacks:

s_{15} = How is the actual cyber security situation evaluated by the security authorities (police, intelligence etc., 1=very low,2=low, 3=medium, 4=high,5=very high) *

s_{16} = Evidence from internal surveillance (computerized monitoring tools). This quantity is measured in terms of number of attack attempts per time unit, typically per year.

To combine the scores into a frequency of attack the following arguments are made:

The scores s_1 – s_4 could be seen as competing scores, and we let $S_A = \max(s_1, s_2, s_3, s_4) + \Delta_A$ be a total attractiveness score. Here[4] $\Delta_A = 0.25 \ln n$, where n counts the number of scores equal the maximum score. $\Delta_A = 0$ if the maximum score is 1 or 5. Thus Δ_A accounts for very many scores equal to the maximum score.

For the organizational factors affecting the frequency of attack we calculate an average score: $S_O = (s_5 + s_6 + s_7 + s_9)/4$

For the conditions influencing willingness of an attacker to make an attempt an average score is also proposed: $S_W = (s_9 + s_{10} + s_{11} + s_{12} + s_{13} + s_{14})/6$

[4] The argument for the adjustment is as follows. Assume that for each of the questions, the frequency of attack is given on the form $f = a \cdot b^S$, where a and b are constants, and S is the score. Given that n questions get the highest score, say S, then the total frequency is $f_{Tot} = n \cdot a \cdot b^S$. To "account" for multiple answers getting the highest score, we seek an adjusted score: $S+\Delta$. Δ is then determined by: $f_{Tot} = a \cdot b^{S+\Delta} = n \cdot a \cdot b^S$. This gives $\Delta = (1/b) \ln n$. Here ln n is the natural logarithm of n. Note that b is a factor determining the increase in the frequency when the score increases with a nominal value of 1. Typical values for b would be in the interval 3 to 10, and we pragmatically choose $b = 4$.

To obtain a total normalized score for the likelihood of an attack, we take the average of S_A, S_O, S_W and s_{15} (national evidence) and standardize between 0 and 1: $L = (S_A + S_O + S_W + s_{15} - 4) / (20-4)$.

The frequency of an attack based on the influencing conditions is given by:

$$f = f_L \left(\frac{f_H}{f_L}\right)^L \quad (4)$$

The yearly frequency f_S based on the assessment of conditions should be compared to the observed frequency, s_{16}. A natural approach to obtain a combined yearly frequency measure is to calculate a weighted average of f_S and s_{16}. With equal weights this yields:

$$f = (f_S + s_{16})/2 \quad (5)$$

Note that f_S would normally be updated rather seldom, for example every 5 years. On the other side, s_{16} would in principle be available in real-time. This is crucial for real-time update of the risk profile.

Probability of cyber-attack succeeding

For the probability assessment of a successful attack another set of questions are provided:

Likelihood of succeeding in an attempt

s_{17} = Attacker's capability vs required capability to succeed in an attempt (1=very low,2=low, 3=medium,4=high,5=very high) *

s_{18} = Attacker's available resources vs required resources to succeed in an attempt (1=very low,2=low, 3=medium,4=high,5=very high) *

s_{19} = Explicit protective measures (1=very high,2=high,3=medium,4=low,5=very low) *

Comments: For explicit protective measures one should take into account (i) use of encryption, (ii) regular updates of software (safety patches), (iii) avoiding possibility to send control commands "from home" to the control systems of the water distribution system (iv) proper governance of emerging technologies like IoT when integrated into the control systems and (v) well design software architecture.

To obtain a probability measure for success of the attack, we first calculate a standardised score $Q = (s_{17} + s_{18} + s_{19} + s_6 + s_7 - 5)/20$, where Q is in the interval from 0 to 1.

Note that in this score we have included two of the organizational conditions which also were "counted" in the likelihood assessment. It could be argued that this will give "double counting", but since we always "normalize", this is considered not to be a big problem. The probability of a successful attack is given by:

$$p = p_L \left(\frac{p_H}{p_L}\right)^Q \quad (6)$$

Frequency of successful cyber attack

The frequency of a successful attack is given by:

$$f_A = f \times p \quad (7)$$

The frequency in equation (7) gives directly a frequency per year. In some situation it is desirable to assign the frequency of successful attack to a likelihood category. In InfraRisk the following likelihood categories are defined:

1. Very unlikely Less than once per 100 year
2. Remote Once per 10-100 year
3. Occasional Once per 1-10 year
4. Probable 1 to 12 times a year
5. Frequent More than once a month

These categories are used to transform the frequency in equation (7) to a category number. An example of frequency assessment of cyber-attacks is shown in Figure 47.

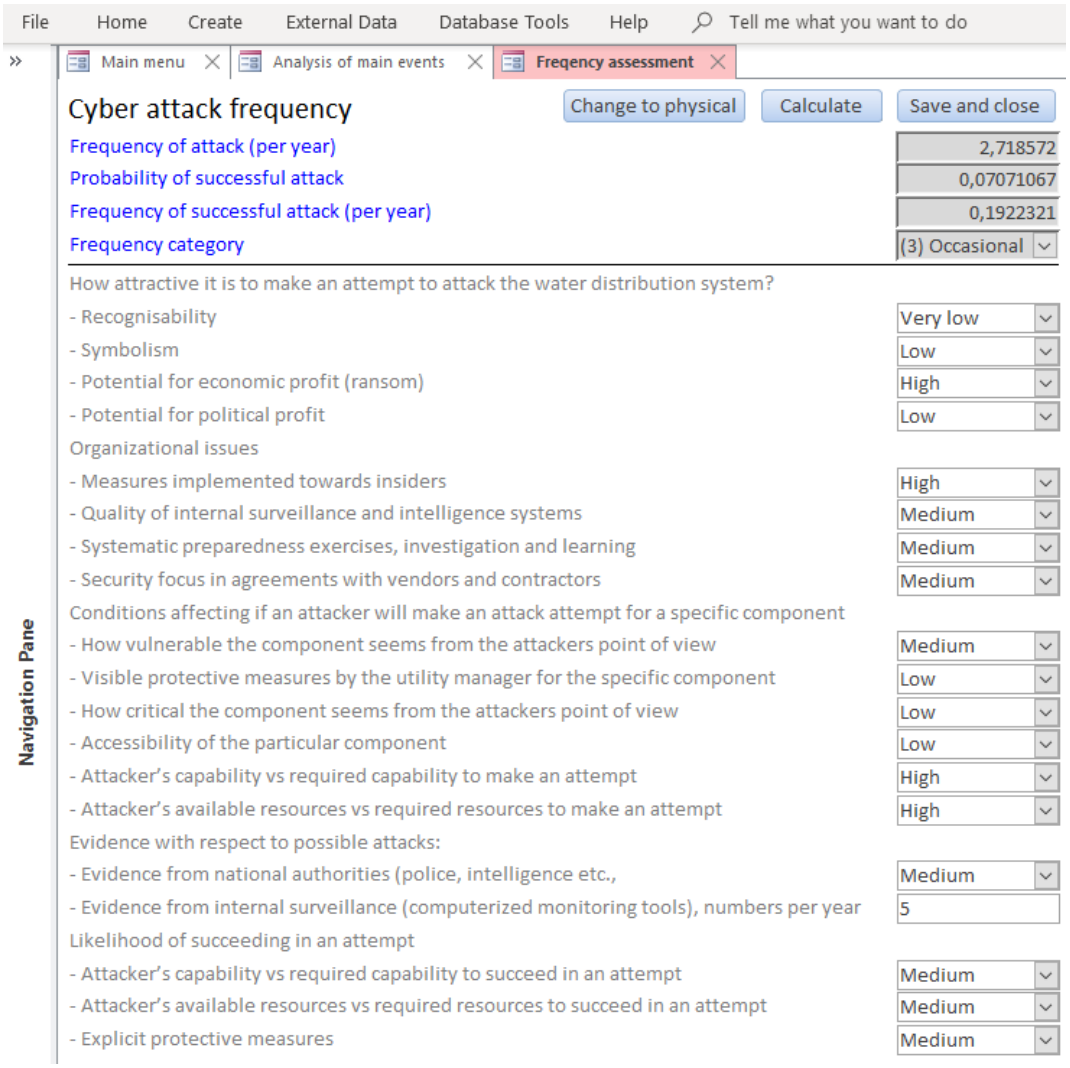


Figure 47: Frequency assessment of cyber attacks

3.3 Configuration and analysis

3.3.1 Configuration

The Configuration menu is found under the InfraRisk-CP Main menu, seen at the opening view of the tool, illustrated in Figure 48.

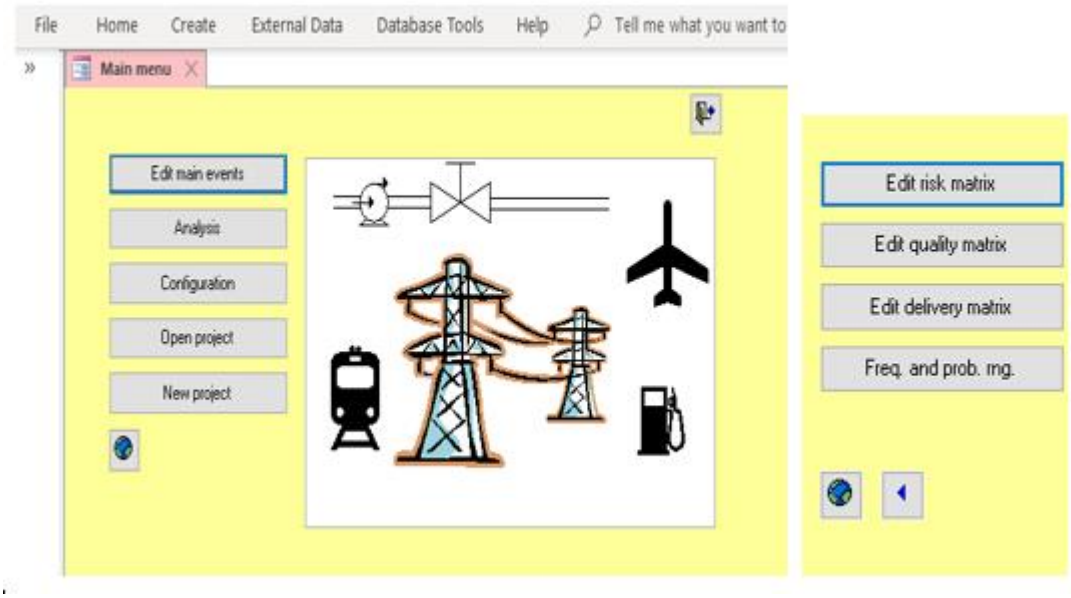


Figure 48: InfraRisk-CP, Main menu and configuration.

3.3.1.1 Risk Matrices

The various matrixes used in InfraRisk may be calibrated from the Configuration menu available from the main menu. For example, press the Edit risk matrix from the configuration matrix. In the risk matrix you now click on a cell, and then you could change the colour/text of the cell as shown in Figure 49:

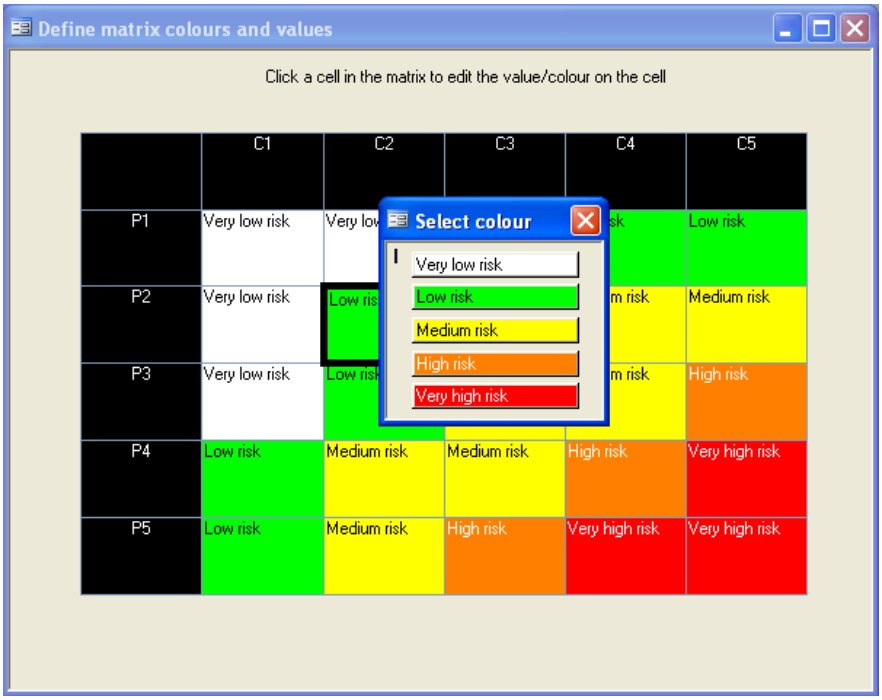


Figure 49: Calibration of risk matrixes.

Similarly, the consequence dimensions for lifeline quality and unavailability (quantity) also could be calibrated from the configuration menu.

3.3.1.2 Attack ranges

Click Attack ranges from the configuration menu to specify the following quantities:

- f_L = Lowest attack frequency (default = one per hundred years)
- f_H = Highest attack frequency (default = 10 per year)
- p_L = Lowest attack success probability (default = one out of hundred)
- p_H = Highest attack success probability (default = one out of two)

The frequencies should reflect the best and worst case respectively. With the best case we mean a situation where all risk factors (scores) take the values considered to give the lowest frequency of attacks, and where the worst case means that all factors take the values considered to give the highest frequency of attacks. Similarly, for the probabilities. Default values are given. These values are used when actual frequencies and probabilities are calculated based on scores.

3.3.2 Analysis

From the main menu, press the Analysis button to get access to the various analysis available in the InfraRisk-CP program. The following options are available:

Asset / SCF ranking. The assets / SCFs are linked according to their importance. The importance depends both on how many events they are linked to, how strong these links are, and the total risk for the corresponding events.

Asset / SCF listing. This option lists all the assets / SCFs with the corresponding events where the asset/SCF are listed.

Print events. The events are populated into a printable report. It is possible to select a subset of the events by filtering.

3.3.2.1 SCF ranking

The SCF ranking is based on the result from the quantification of frequency and consequence of events. For each main event where a SCF is involved, the risk is calculated by multiplying the frequency with the sum of consequences. Then each SCF achieves a score which is the importance contribution times the risk. The importance contribution of an SCF wrt a given event is shown as the "number" in Table 13, for example R90 gives an importance score of 90%. By summing over all main events for all SCFs it is possible to establish a ranking of SCFs. Note that the frequency and consequence values are given on a logarithmic scale, hence it is necessary to use the exponential function during the calculation in InfraRisk CP.

3.3.2.2 SCF listing

In the SCF listing, all SCFs are listed with a sub-list of all main events for which the SCF is included.

3.3.2.3 Print events

Pressing the Print events button from the analysis menu will create a formatted report for selected events. The report is opened in standard MS Access format, and may be sent to the printer from the MS Access Print Preview ribbon menu. It is possible to filter a subset of the events by specifying an SQL statement, see section 3.3.2.4.

3.3.2.4 Filtering events

Press the filter button ( ) at the bottom of Main Event specification form in Figure 33 to activate the filter prompt. Enter the WHERE clause of the SQL statement to filter out selected records. Note that the same syntax for filtering events also applies for the print event menu under the analysis menu. Some special functions/statements will be described below, and these are:

```
SCF(<SCF code 1>,[SCF code 2], [SCF code 3], …)
MainEvent(<Event code 1>, [Event code 2], [Event code 3], … )
TypeOfEvent = <EventType>
TypeOfThreat = <ThreatType>
```

To filter specific societal critical functions the **SCF()** function is used. See Table 21 (ANNEX D) for a list of SCFs related to water distribution systems. For example to filter out events for the *catchment area* and the (specific asset) *control center,* the following statement is entered:

```
SCF ("C111")
```

Note that several code values may be specified as arguments in the **SCF()** function, for example:

```
SCF("C111","C121")
```

will filter out events with associated (specific asset) *control center* for *catchment area* and *drinking water network*. Up to 10 arguments may be specified in the **SCF()** function.

Table 20 shows the hierarchical structure of the main events. For example, the statement:

```
MainEvent("MC21")
```

will filter out events with the following criteria:

Malicious acts (M)
Crime (C)
Sabotage (2)
Attack against installations (1)

In the STOP-IT project a further elaboration of the nature of the event is given by the type of event and the type of threat. Note that **TypeOfEvent** and **TypeOfThreat** are represented as coded values in the InfraRisk-CP data table. To filter these events both the code values and the full text may be used. The values must be enclosed in double quotes. For example, the following statements will give the same results:

```
TypeOfEvent = "I"
TypeOfEvent = "Interruption"
```

Table 14 shows code values used for **TypeOfEvent**:

Table 14: Code values for TypeOfEvent.

Code	Description
D	Destruction
I	Interruption
M	Manipulation
P	Pollution

Similarly, to filter out a specific **TypeOfThreat** the following statements are equivalent:

```
TypeOfThreat = "C"
```

```
TypeOfThreat = "Cyber"
```

Table 15 shows code values for **TypeOfThreat**:

Table 15: Code values for TypeOfThreat.

Code	Description
C	Cyber
P	Physical
B	Cyber-physical

Note that the filter commands above may be combined by **AND** or **OR** statements, for example:

```
TypeOfThreat = "C" AND TypeOfEvent = "I"
```

In order to clear the filter, i.e., select all events in the database, specify:

```
True
```

Advanced filtering requires understanding of the name structure of the **tblMainEvents** in InfraRisk CP.

Part D: Risk Analysis and Evaluation Toolkit

4.1 Introduction

The Risk Analysis and Evaluation Toolkit (RAET) provides a platform for the analysis and evaluation of risks from physical, cyber and combined CP events to the water system. It supports users throughout all stages of analysis and evaluation, i.e. the identification of CP risks and vulnerabilities, the elaboration of attack scenarios and their simulation, the analysis of the results and the search for appropriate risk reduction measures. It consists of or is connected with the following components:

- A database of cascading events which may lead to water quality or quantity issues. The events are based on risks, initially stored in the **Risk Identification Database** (RIDB) in Task 3.2 and enhanced with additional cyber-physical threats.
- A **Fault Tree Editor** (FT Editor) for creating, editing and modifying fault trees, initially developed for the needs of WP6.
- A **Fault Tree Viewer** (FT Viewer) which enables FT analysis and supports the identification and selection of risks for further use in the Scenario Planner
- An **Asset Vulnerability Assessment Tool** (AVAT) developed in Task 4.1 for the identification of the most vulnerable components of an infrastructure.
- The **Scenario Planner** (SP) 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.
- A **Toolkit Library** (TL) providing access to information about tools, mathematical models and methodologies related CP risk analysis and evaluation in the water infrastructure.
- A **Risk Reduction Measures Database** (RRMD) developed in Task 4.3.
- **Tools** for the simulation of elaborated scenarios i.e. Epanet CPA, Epanet MSX
- The **Key Performance Indicator Tool** (KPI Tool), analysing simulation results
- **Advanced search** (AS) functionality, for querying within the RRMD, the RIDB and the related data, based on user defined criteria.

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). Others are autonomous Windows applications which have been developed in other work packages and 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, EPAMET-MSX). Both databases, RIDB and RRMD, have been developed in other Tasks of the project and have been integrated in the RAET database.

In the following subsections the conceptual data model capable to support the framework for WP4 is briefly introduced. A detailed Conceptual Data Model (CDM) is provided in ANNEX

E. In the Entity-Relationship diagram (E-R-diagram) entities in red background are tool specific, while the others are considered to be generic.

For the purpose of demonstrating the functionality of RAET and testing the software prototypes according to MS14, the development team has installed the latest version of RAET on a Windows server.

RAET is a web application and its core components can be accessed over HTTP using a common browser (i.e. http://raet.itia.civil.ntua.gr:8001/). However, because RAET can invoke components which are Windows desktop applications requiring interaction with the user, direct access to the Windows desktop must be provided. This can be achieved using a common remote desktop sharing tool. Unfortunately, one of the components (MATLAB) has some known compatibility issues when using it via Windows Remote Desktop Connection and cannot be started from this terminal server[5]. Therefore, users need to access RAET using another tool such as TeamViewer. On the server side, Teamviewer and a development web server will normally start on Windows start-up and therefore should always be running, even after a power outage. To access certain functionality of RAET, login to the system is required. Credentials for accessing both, the remote desktop and RAET can be obtained from Dr. Christos Makropoulos (Christos.Makropoulos@kwrwater.nl or cmakro@chi.civil.ntua.gr).

As AVAT is considered to be classified, it is not available in the demo version. Additionally, other components and functionalities are still under development in other tasks (e.g. the Stress Testing Platform in T4.4) and will be added in later stages of the project.

4.2 System Architecture

RAET has been developed as three-tier architecture consisting of the following modules:

- A **Web server**, serving static and dynamic content based on requests sent by an HTTP client (browser). The browser will then render the content and present the information to the user, usually in form of a web page.
- The **Application server**, realizing the logical tier of the system. It receives requests from the presentation layer, controls an application's functionality by performing detailed processing, communicates with the data layer and responds to the requests returning processed data. The application server is implemented with the Django framework which follows the Model-View-Controller (MVC) architectural pattern.
- A **Back-end database**, comprising both data sets and the database management system software (DBMS) that manages and provides access to the data. In RAET the DBMS is implemented with the open source software SQLite as single-file embedded database. This is possible because the volume of data stored in the database is expected to be limited and allows a more simple and flexible installation procedure.

[5] Issue documented here: https://se.mathworks.com/matlabcentral/answers/91874-why-do-i-receive-license-manager-error-103

The FT Viewer, the Scenario Planner the Toolkit library and the Advanced search functionality are integral parts of RAET and follow the above architecture. Other components which are external desktop applications can be invoked by RAET. For most of them, interfaces have been defined for data exchange e.g. for importing fault trees developed by the FT Editor or for receiving simulation results of scenarios calculated by a stress-testing tool (epanetCPA, EPANET-MSX). The risks documented in the RIDB have been integrated in the RAET database as events of fault trees, while risk reduction measures, initially stored in the RRMD, have been imported and linked with events. Import routines have been developed so that any future updates of these databases can be easily incorporated in the RIDB database. Figure 50 depicts the system architecture of RAET.

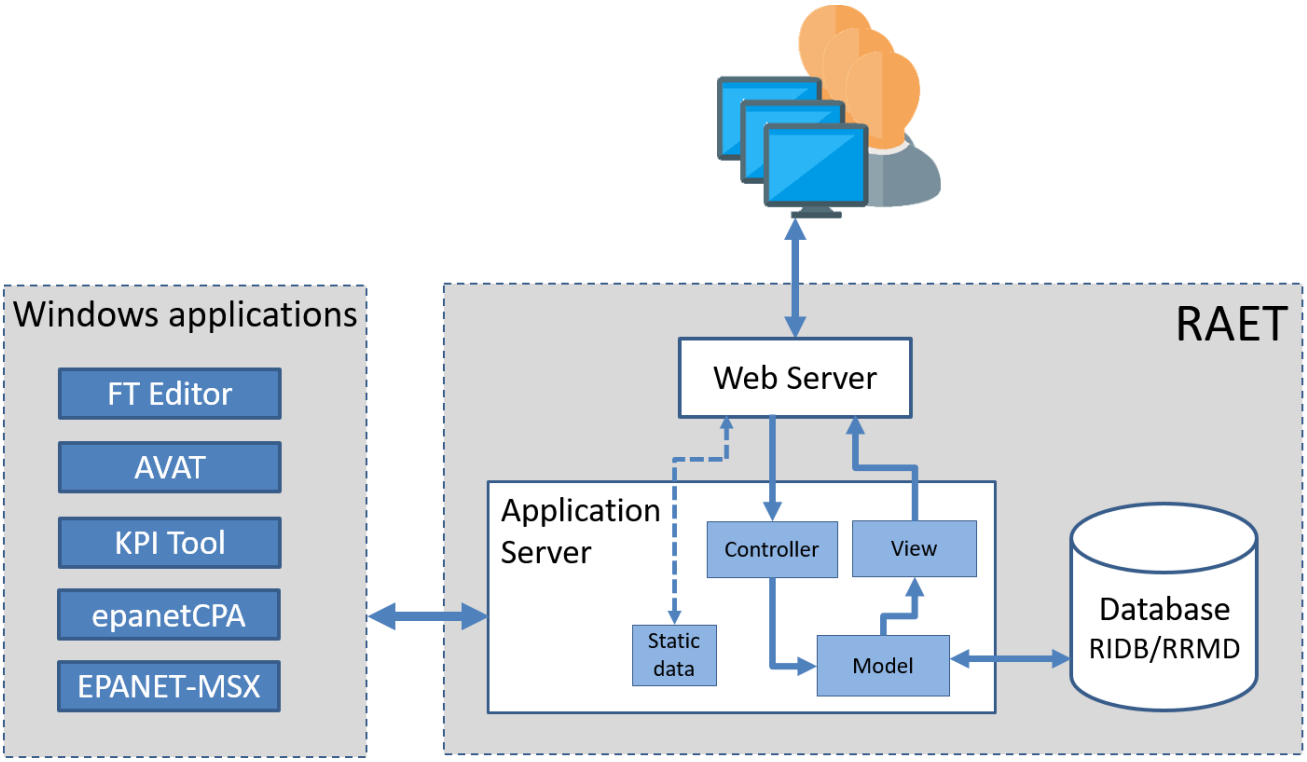


Figure 50: System architecture of RAET

Interfaces of RAET to other external Windows components include the following files:

- Open PSA file for importing fault trees created by the FT Editor.
- Two files (.inp and .cpa) for the feeding EPANET CPA with the network file and cyber-physical attack according to the specified scenario
- Two files (.inp and .msx) for the feeding EPANET MSX with the network file and the pollution dynamics according to the specified scenario
- A file in JSON format containing simulation results calculated by EPANET CPA or EPANET MSX
- A CSV file with detailed simulation results to be evaluated by the KPI Tool

RAET can be installed in the Intranet of a water utility and accessed through a browser. Since all interactions with the user are made at the SP level, RAET is capable to support desktop applications which can be executed in batch mode. RAET will create a new process on the server for each simulation run, will observe its progress and read the simulation results when the process has terminated. This way, several users in the same utility can collaborate in a project jointly developing and executing common scenarios.

4.3 Conceptual Data Model

In the following subsections the conceptual data model capable to support the framework for WP4 is briefly introduced. A detailed Conceptual Data Model (CDM) is provided in ANNEX E. In the Entity-Relationship diagram (E-R-diagram) entities in red background are tool specific, while the others are considered to be generic.

4.3.1 Events

Events described in this context are risks or threats that can occur in a cyber-physical water infrastructure. In WP4, events are always considered generic, i.e. there are infrastructure specific events but no site-specific ones. A list of general risks has been initially defined in the Risk Identification Database (RIDB) in Task 3.2. After that, they have been enhanced with additional ones and transformed into Fault Trees (FT). FTs are hierarchical trees of cascading events connected through boolean logic. Events may be *Basic* and *Intermediate*. Intermediate events are triggered by other events (basic or intermediate) through gates which describe the relationship between input and output events and represent boolean logic operations. In this work, the basic gates AND and OR are supported.

Events may be applied to assets of a specific asset type. Assets, within this context, always consider specific asset types/ groups and not individual components of a specific network. Possible asset types defined in the RIDB are the following:

- Additives
- Control centre
- Control system
- Dosing system
- Drinking water pipes
- Drinking water tanks
- Drinking water taps
- Fire hydrants
- Groundwater
- Media channels
- Power transformer
- Pressure boosting station
- Pump
- Sensor
- Server

- Spring water
- Surface water
- Transferred information
- Transmission devices
- Transmission pipes and equipment
- Treatment unit process
- Valve
- Water under treatment
- Well

Events may also be related to one of the following event types:

- Destruction
- Interruption
- Manipulation
- Pollution

Although events are unique instances in the database, they may appear in several places in a FT. In order to identify the node in the FT which has triggered an event, the entity *node* has been introduced. Thus, a number of nodes may be related to a single event.

The aforementioned concepts and their relationships are depicted in Figure 51.

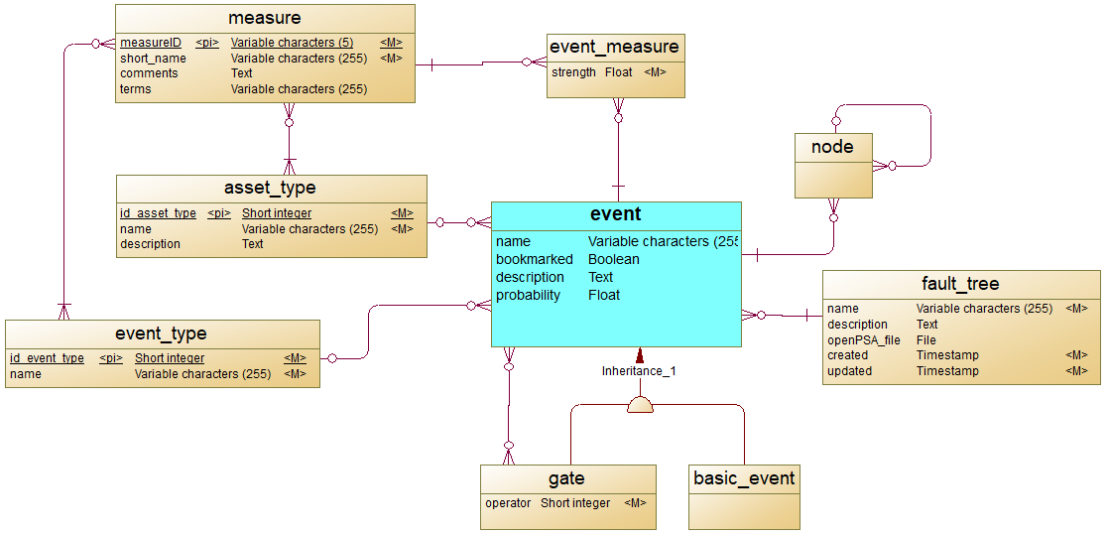


Figure 51: ER-diagram of concepts related with Events

4.3.2 Measures

Risk reduction **Measures** can be specified which may address one or several identified risks. Measures have been specified in T4.3 and documented in the RRMD. The categorization of measures is also defined in T4.3 and adopted in T4.2. As an example, possible action

characteristics of a measure may be *Proactive, Reactive* or *Proactive & Reactive*. Another categorization refers to the measure type that can be selected from the following list:

- Physical Barriers
- Cyber Barriers
- Redundancy
- Control System
- Consequence Mitigation
- Economic Policy
- Action and Crisis Management Plans and Training

Just as for events, measures are related to one or several event types and asset types. Through these two common data categories an initial association between events and measures can be established. However, in order to capture with better precision, the measures which potentially can address specific threats, another matching table has been introduced (event_measure). A procedure involving a custom algorithm and possibly expert opinions will be developed in T4.5 in order to populate this table. As a result of this procedure the strength of the relationship between an event and a measure will be estimated and quantified.

The diagram in Figure 52 depicts the relationships of measures with other entities.

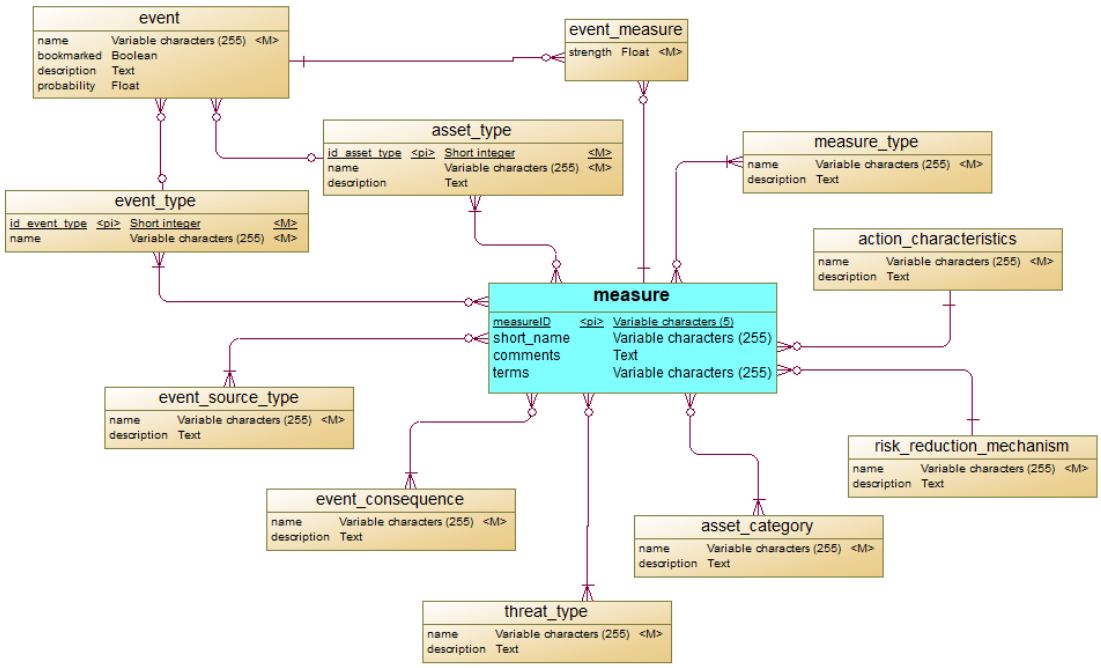


Figure 52: ER-diagram of concepts related with Measures

4.3.3 Tools

The Risk Analysis and Evaluation Toolkit (RAET) supports stakeholders in their aim to:

- Get informed about state-of-the-art tools, i.e. software, models, methodologies and algorithms capable analyse and evaluate the risks and vulnerabilities which have been identified in Tasks 3.2 and 4.1.
- Navigate to external sources providing additional information on selected tools
- Depending on their license type, obtain and execute the tools.

The tool attributes as well as the relationships with other data categories are described in detail in section 4.6. Tools supported by this platform are related with the scenario through the table supported_tool. Figure 53 shows the ER-diagram of Tools.

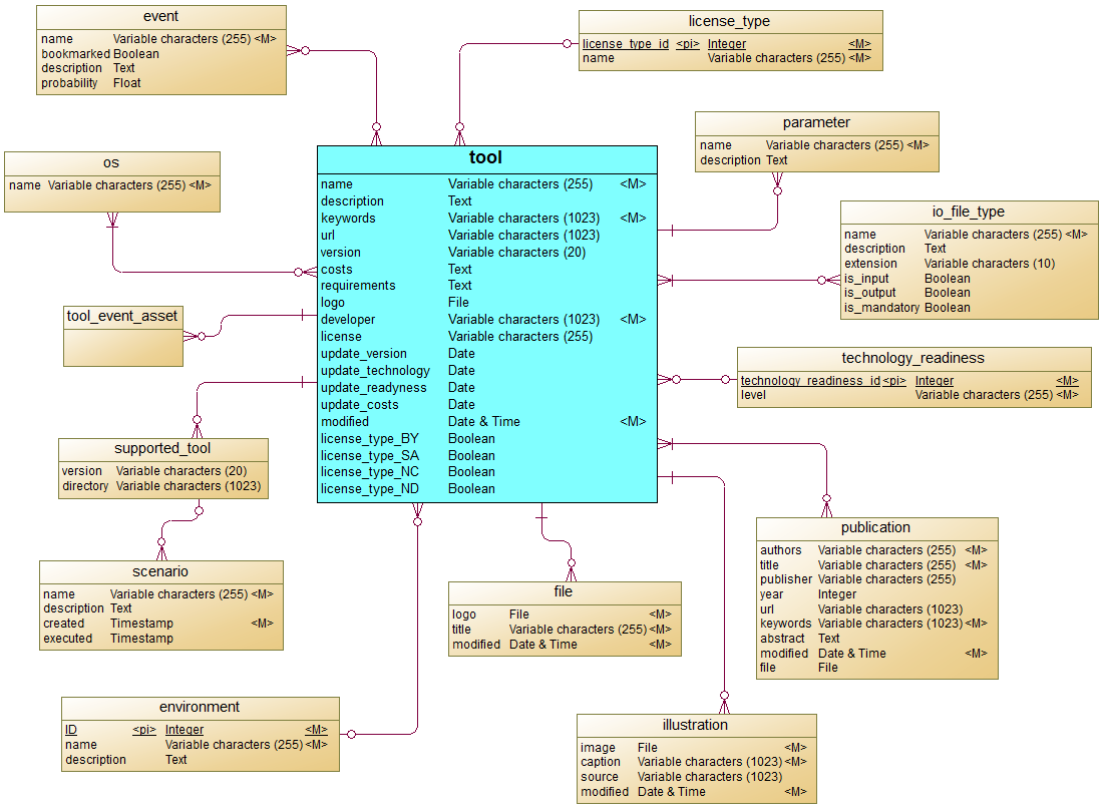


Figure 53: ER-diagram of concepts related with Tools

4.3.4 Scenarios

A given scenario includes the following components:

- **Tools** capable to simulate CP processes. Currently, the platform supports the tools EPANET CPA and EPANR MSX.
- A **utility network**, its characteristics and initial conditions given by the tool specific files.
- A series of **events** which are triggered on specific assets according to the stress test scenario

- 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.

In Figure 54 the concepts which are directly related with Scenarios are shown.

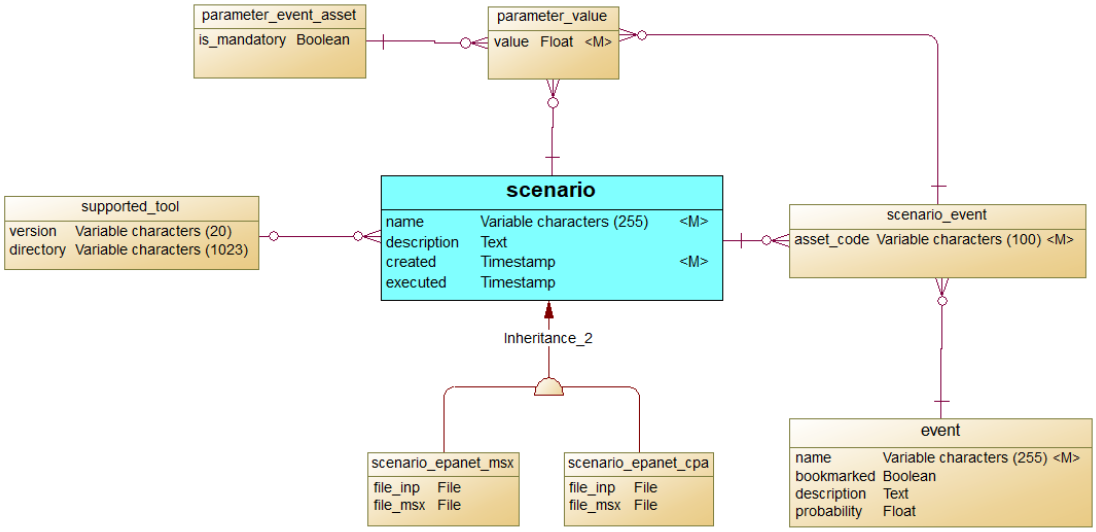


Figure 54: ER-diagram of concepts related with Scenarios

4.4 User roles

Typically, users will install the RAET on their personal computer, together with all the other components included in Module I. This decision is based on security reasons because of the sensitive nature of the data and may be accompanied by additional measures such as operating the application in an isolated environment. However, RAET provides the possibility for multiple user access over a local network (Intranet) using the HTTP protocol. Users will then be able to access the application with a typical browser and work on common projects and scenarios. Therefore, it is important for the system to recognize user roles and associated rights as follows:

Simple user: A simple user can view and navigate to any part of the application for which authentication is not required. This includes listing and displaying stored risks/events, risk reduction measures, related tools, scenarios and scenario results.

Fault Tree Manager: A Fault Tree Manager is authorized to manage Fault Trees, i.e. create new Fault Trees and modify existing ones using the FT Editor and import them into the RAET or delete FTs created by him or by other users.

Tools Manager: In addition to the rights of a simple user, a Tools Manager is authorized to add, modify and delete tools stored in the Tools library.

Modeler: A Modeler can create scenarios based on an identified risk and a selected tool. He is able to modify base scenarios, develop a variation of it or create from scratch a new one and import it in RAET. He can then execute scenarios and view the results.

Administrator: An administrator has unlimited access to all RAET functionality, including adding new users and assigning roles to users. The initial user after installing RAET is always an administrator.

A user may hold more than one role. Table 16 summarizes the allowed basic operations by user role.

Table 16: Permissions by user role

Operation	Simple user	Fault Tree Manager	Tools Manager	Modeler	Admini-strator
Add user account					**Yes**
Delete user account					**Yes**
Modify account attributes					**Yes**
Add Tool			**Yes**		**Yes**
Modify Tool			**Yes**		**Yes**
Delete Tool			**Yes**		**Yes**
View Tools	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**
Import Fault Tree		**Yes**			**Yes**
Delete Fault Tree		**Yes**			**Yes**
View Fault Tree	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**
Create Scenario				**Yes**	**Yes**
Modify Scenario				**Yes**	**Yes**
Run Scenario				**Yes**	**Yes**
Delete Scenario				**Yes**	**Yes**
View scenario results	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**
Advanced search	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**

A detailed description of the functionality which is available by the RAET to users in accordance to their roles is given in the user guide in section 4.7.

4.5 Scenario Planner

In this document, a **scenario** is defined as a set of input data which are required to run a simulation using a model (tool). Typically, a scenario will include data from the following categories:

- A network topology of the water infrastructure.
- The characteristics of all assets of the CP infrastructure.
- A set of events identified as possible threats.

- Possibly measures capable to address identified CP risks.
- Other simulation parameters, required by the selected tool.

The Scenario Planner supports the user to define the aforementioned data which comprise the scenario, to manage scenarios, to select appropriate models and to run simulations and assess their results. By employing the Scenario Planner, RAET introduces a higher level of abstraction to the end user, hiding the underlying data files needed by a model to run the simulation. In most cases, the user has to develop from scratch only once the base scenario, i.e. a reference scenario such as the business-as-usual scenario and then for any variation to the base scenario he has to specify only (small) differences. The SP would then implement all required modifications in the related files of the supported tool in accordance to the scenario.

Next to the scenario data, the SP hides also the simulation model from the user. Based on the declared capabilities of each tool, the SP is able to recognize which tools support the simulation of user defined events. Thus, only tools (models) which are integrated in RAET and can simulate the scenario are offered for further processing. In order to run the simulation, there is no need to interact with the user interface of the tool as all aspects needed for the simulation have been defined in the SP. The tool is used only as an engine and is executed in batch mode.

Once the user has identified possible risks for further investigation using the Fault Tree analysis, a wizard may be called, guiding the user to specify the way the identified threat will be applied on his infrastructure (see also section 2.3.2). This specification may involve several additional parameters, e.g. individual assets, the involved pollutants, the expected duration of the event etc. which will clearly define the scenario and will be used to feed the Stress Testing Platform. The procedure may be repeated several times, adding a number of events of the same general category (e.g. destruction of several pipes simultaneously) or of different categories (e.g. pollution of drinking water tanks and manipulation of the corresponding tank sensors) to the scenario. The parameters are dependent on the **model** (tool) to use for the simulation, the **type of event** and the affected **asset types**.

The matching algorithm which relates events specified in the RIDB with measures imported from the RRMD is based on the event type and specific asset type attributes. It is assumed that risk reduction measures will more likely be able to address events documented in the RIDB if they are applied on assets and support events of the same type. A more sophisticated algorithm for matchmaking will be developed in Task 4.5 and will be incorporated in RAET.

4.6 Toolkit library

In the following text, by using the term *Tools* we mean Software tools such as models, applications and algorithms that can be used to analyse and evaluate CP risks in the water infrastructure.

The Toolkit library can be updated by authorized users based on the following concepts:

- An online application has been developed guiding the user to provide information on new Tools and related data and managing existing ones.
- New entries can be added by authorized users upon login to the system. Attributes and relationships to other entities must be provided as stated in the following sections
- The Toolkit shall be connected to the Scenario Planner in the following way: The data provider must specify which event/threat and asset types the tool supports, i.e. event and asset types that, in a way, can be modelled by the tool. On the other hand. Based on this information the Scenario Planner can propose appropriate tools which are able to address CP threats identified by the user. Restrictions and conditions under which a tool can be applied in relation with event and asset type shall also be provided.
- The official instance of the Toolkit library will be publicly available and can be constantly updated by authorized users. However, a snapshot of the Toolkit can be taken in order to be used in an isolated environment e.g. in the Intranet of water utilities.

Additional information on how to enhance the Toolkit library is provided in the user manual in section 4.7.6.

4.6.1 Tool attributes

Attribute	Type	Mandatory	Description
Name	Char (255)	Yes	Name of the tool
Description	Text	Yes	A short description for the tool
Keywords	Char (1024)	Yes	Comma separated keywords related with the tool
Developer/ Owner	Char (1024)	Yes	Institution, contact person, address, phone, email (mandatory is at least the name of the institution)
Technology readiness	Integer [1,9]	Yes	Estimate in a scale from 1 to 9 the level of technology readiness (see Section 0)
URL	Char (1023)		URL providing further information about the tool or/and can be used to navigate to the download page.
Version	Char (20)		Current stable version number or name of the software
OS	List	Yes	Operating environment in which the tool can run. Select at least one or more options from the provided list of Operating Systems (see Section 4.6.6).
Requirements	Text		Minimum hardware and software requirements, including 3rd party software applications, libraries etc. needed to run the tool such as Matlab, EPANET, MS Excel
Logo	File		The logo of the tool. One of the following image formats is accepted: jpeg, png
Illustrations	Files		One or more characteristic screenshots, including a legend for each one of them. One of the following image formats is accepted: jpeg, png
Publications	List		List of publications (reference list) related with this tool (see section 0)

Files	Files		Additional files related with the tool can be uploaded to the Toolkit, e.g. user manual.
Event types	List	Yes	Event types supported by the tool, i.e. the event types which the tool is capable to address and/or which can be modelled in a way by the tool. Select one or more options from the list (see section 4.6.3)
Asset types	List	Yes	Asset types supported by the tool. Is the tool suitable to address CP problems related with this kind of asset types? Select one or more options from the list (see section 4.6.4)
License type	List	Yes	Specify the general license type: • Commercial or • FOSS (Free and open-source software) This is relevant not only for the main tool but also any additional software needed to run the tool.
License	Char (255)		If applicable, name the license associated with the tool (e.g. GPL 3 or MIT), not only for the main tool but also for any other software necessary to run the tool.
Costs	Text		If applicable, describe the costs and conditions for obtaining a license (e.g. purchase vs. SAAS, floating license, packages, editions)
CC license type[6]			
Attribution (BY)	Yes, No, Unknown		Licensees may copy, distribute, display and perform the work and make derivative works and remixes based on it only if they give the author or licensor the credits (attribution) in the manner specified by these.
Share-alike (SA)	Yes, No, Unknown		Licensees may distribute derivative works only under a license identical ("not more restrictive") to the license that governs the original work. Without share-alike, derivative works might be sublicensed with compatible but more restrictive license clauses, e.g. CC BY to CC BY-NC.
Non-commercial (NC)	Yes, No, Unknown		Licensees may copy, distribute, display, and perform the work and make derivative works and remixes based on it only for non-commercial purposes.
No Derivative Works (ND)	Yes, No, Unknown		Licensees may copy, distribute, display and perform only verbatim copies of the work, not derivative works and remixes based on it.

[6] In case of FOSS, these are the main license types recommended by Creative Commons, in addition to the "baseline rights" (see also: https://en.wikipedia.org/wiki/Creative_Commons_license). Indicate the application of each one of them with "Yes" (condition applies), "No" (condition does not apply) or “Unknown". If all four conditions are answered with "No" this means that the tool is public domain i.e. available globally without restrictions (CC0).

In addition to the above user-defined attributes, a timestamp will be taken automatically every time a record is modified. Other read-only timestamps will document the time when selected attributes will be modified such as version, technology readiness, license and costs. This way, selected information that may change over time will always have a reference to the time they have been provided or modified.

Data categories related with tools are briefly introduced in the following subsections.

4.6.2 Publications

Publications related with tools.

Attribute	Type	Mandatory	Description
Authors	Char (255)	Yes	Authors/owner of the publication
Title	Char (255)	Yes	Title of the entity
Publication	Char (255)		
Publisher	Char (255)		Name of the publisher
Year	Integer		Year of the publication
Url	Char (1023)		URL providing further information about this entity
Keywords	Char (1024)	Yes	Comma separated keywords related with the publication
Abstract	Text		Abstract of the publication
File	File		A file related to the reference (e.g. a PDF document or an image)

4.6.3 Event types

List of possible event types elaborated in Task 3.2 for the RIDB and used also in the RRMD.

Destruction
Interruption
Manipulation
Pollution

4.6.4 Specific asset types

List of possible specific asset types elaborated in Task 3.2 for the RIDB and used also in the RRMD.

Additives
Control centre
Control system
Dosing system
Drinking water pipes
Drinking water tanks
Drinking water taps
Fire hydrants

Groundwater
Media channels
Power transformer
Pressure boosting station
Pump
Sensor
Server
Spring water
Surface water
Transferred information
Transmission devices
Transmission Pipes and Equipment
Treatment Unit Process
Valve
Water under treatment
Well

4.6.5 Technology readiness

The following levels are in use by the EU to describe the technology readiness of products and will be used also for tools in the RAET.

Level	Description
Level 1 - Basic Research: basic principles are observed and reported	Lowest level of technology readiness. Scientific research begins to be translated into applied research and development. Examples might include fundamental investigations and paper studies.
Level 2 – Applied Research: technology concept and/or application formulated	Once basic principles are observed, practical applications can be formulated. Examples are limited to analytic studies and experimentation.
Level 3 – Critical function, proof of concept established	Active research and development is initiated. Laboratory studies aim to validate analytical predictions of separate components of the technology. Examples include components that are not yet integrated or representative.
Level 4 – Laboratory testing of prototype component or process	Design, development and lab testing of technological components are performed. Here, basic technological components are integrated to establish that they will work together. This is a relatively “low fidelity” prototype in comparison with the eventual system.
Level 5 – Laboratory testing of integrated system	The basic technological components are integrated together with realistic supporting elements to be tested in a simulated environment. This is a “high fidelity” prototype compared to the eventual system.
Level 6 – Prototype system verified	The prototype, which is well beyond that of level 5, is tested in a relevant environment. The system or process demonstration is carried out in an operational environment.
Level 7 – Integrated pilot system demonstrated	Prototype is near, or at, planned operational system level. The final design is virtually complete. The goal of this stage is to remove engineering and manufacturing risk.
Level 8 – System incorporated in commercial design	Technology has been proven to work in its final form under the expected conditions. In most of the cases, this level represents the end of true system development.
Level 9 – System ready for full scale deployment	Here, the technology in its final form is ready for commercial deployment.
Level beyond 9 - Market introduction	The product, process or service is launched commercially, marketed to and adopted by a group of customers (including public authorities).

4.6.6 Operating Systems

Possible options of operating systems:

- Windows
- Linux
- macOS
- Android
- iOS
- Other

4.7 User's guide

This section provides information for the installation of the core RAET components. Other components which are invoked from RAET are installed separately as described in their user manuals. However, the deployment of RAET including Module I components, pre-configured and ready for use on-site by the stakeholders is planned in WP7 for the demonstration purposes.

RAET is a cross-platform application and can be installed on any common operating system. Other components of Module I, which are autonomous applications (AVAT, KPI Tool) but can be invoked from RAET, require a Microsoft Windows environment to run and therefore installing RAET in a Microsoft Windows environment is recommended in order for the user to have full access to all applications from a single workstation.

RAET has been developed based on the Python/Django web framework and therefore Python 2.7.X has to be installed prior to all other installations. After that, a number of software, libraries and packages have to be installed, preferably within a virtual environment. The dependencies are documented in file requirements.txt and can be downloaded and installed in one process using python's package installer (pip), calling pip from a shell (command line) as follows:

```
pip install -r requirements.txt
```

This will install the following dependencies:

Software	Recommended version
django	1.10
beautifulsoup4	4.6
djangorestframework	3.7
django-filter	1.1.0
pillow	4.3.0
openpyxl	2.6
numpy	1.16
scipy	1.2
networkx	2.2
pandas	0.24
enum34	1.1
wntr	0.1.6

The following components can be installed separately as documented in their user manuals:

- FT Editor
- AVAT
- KPI Tool

In order to connect them with RAET the absolute path of the executable file has to be declared in the file `\spindle_project\settings\local.py` as follows:

```
TOOL_FTEDITOR_EXE = r"<path to FT Editor>\psa.exe"
if not os.path.isfile(TOOL_FTEDITOR_EXE):
    TOOL_FTEDITOR_EXE = None
TOOL_AVAT_EXE = r"<path to AVAT>\AVAT.exe"
if not os.path.isfile(TOOL_AVAT_EXE):
    TOOL_AVAT_EXE = None
KPI_TOOL_EXE = r"<path to KPI Tool>\WP4_KPI_tool.exe"
if not os.path.isfile(KPI_TOOL_EXE):
    KPI_TOOL_EXE = None
```

RAET is a web application and therefore it needs a web server for accessing it. In a single user environment or event in a small multiuser environment like an Intranet, this could be *runserver*, Django's own development server. It can be started with the following command:

```
Python manage.py runserver 0.0.0.0:8000
```

REAT can then be accessed from a common browser under the URL *<host IP or name>*:8000. Windows desktop applications are is executed on the local machine and can be controlled only by the Windows user even if they are invoked by RAET over the network. Remote users can gain control through a remote control or desktop sharing software such as TeamViewer or Windows Remote Desktop.

4.7.1. Simple User guide

Simple, unregistered users can retrieve data of various resources stored in the RAET. However, in order to modify any data they have to log into the system first, by clicking on the `Login` option from the main menu. The RAET home page is shown in Figure 55, which is common for all user roles. The main operations represented by pictures of animals are the following:

Identify Risks	Identify risks based on Fault Tree Analysis.
Identify Vulnerabilities	Identify the most vulnerable components of your infrastructure.
Check for Tools	Check the library for appropriate tools capable to simulate events.
Create your Scenario	Create a new threat scenario for your utility and run a simulation with the model of your choice.

Secure your Network	Check for possible risk reduction measures that address the identified risks.
Optimize the Operation	Optimize the operation of your network. This connects to the Stress Testing Platform which is under development in Task 4.4.

The pictures of operations that are not available are grayed out. This is the case when an external application is not installed or under development (Optimization). By clicking on a picture, the user is navigated to the respective website.

The main menu is on the header of all pages, from which the user can directly access the following pages: Fault Trees (list of available FTs, importing FTs, access to specific FT), Scenario wizard, Lists of data categories (Measures, Events, Scenarios, FTs, Tools), Search.

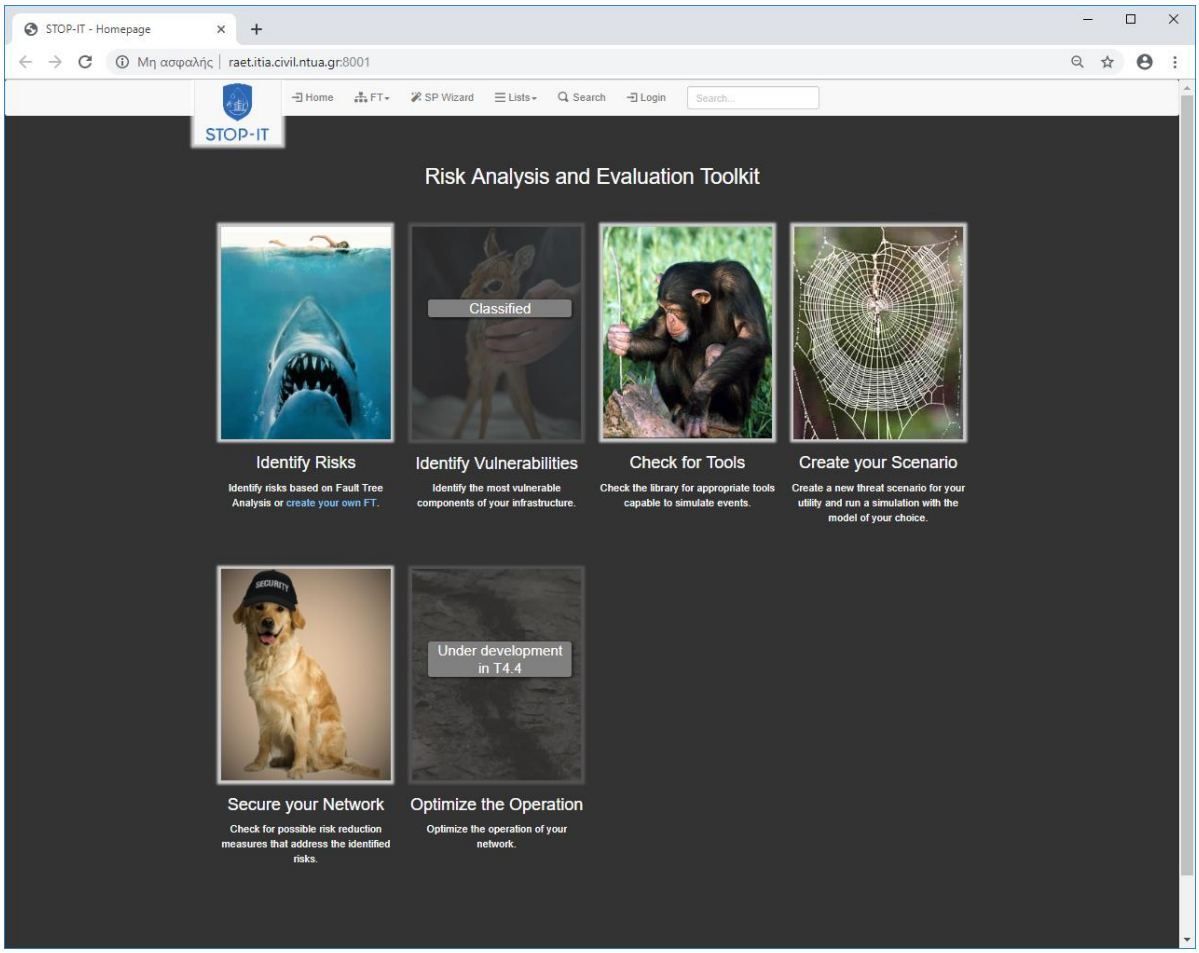


Figure 55: Homepage of the Risk Analysis and Evaluation Toolkit

4.7.2. Fault Tree Viewer (FT Viewer)

The user can navigate to the FT Viewer a) by clicking on a fault tree icon ( ) from the FT list page or b) by selecting an existing FT from the main menu under the option `FT`. Authorized users (FT Manager) may also import a new FT, either from the FT list page (button `New FT`)

or from the main menu (`FT/Import`), after which the newly imported FT is immediately displayed.

The Fault Tree (FT) describes risks in a more structured way than the RIDB as it captures cascading effects between events. The way the FT is displayed by the FT viewer is shown in Figure 56. The root of the FT is to the left, while the FT is developed from the left to the right, in contrast to the typical top-down view of common FT viewers. Additionally, the gate symbols are here replaced by arrows, the colour of which represents a gate type: green for AND gates and blue for OR gates. Only Basic and Intermediate Events and OR/AND Gates are supported by this version of the FT viewer.

The user can scroll up/down and left/right the screen to inspect all parts of the FT. Using the zoom capabilities of the browser (by holding the control key down and rolling the mouse wheel) the user can zoom in and out. In order to pan the view, the user has to hold down the mouse button and drag the mouse. Figure 56 gives an example of a FT as shown by the FT viewer.

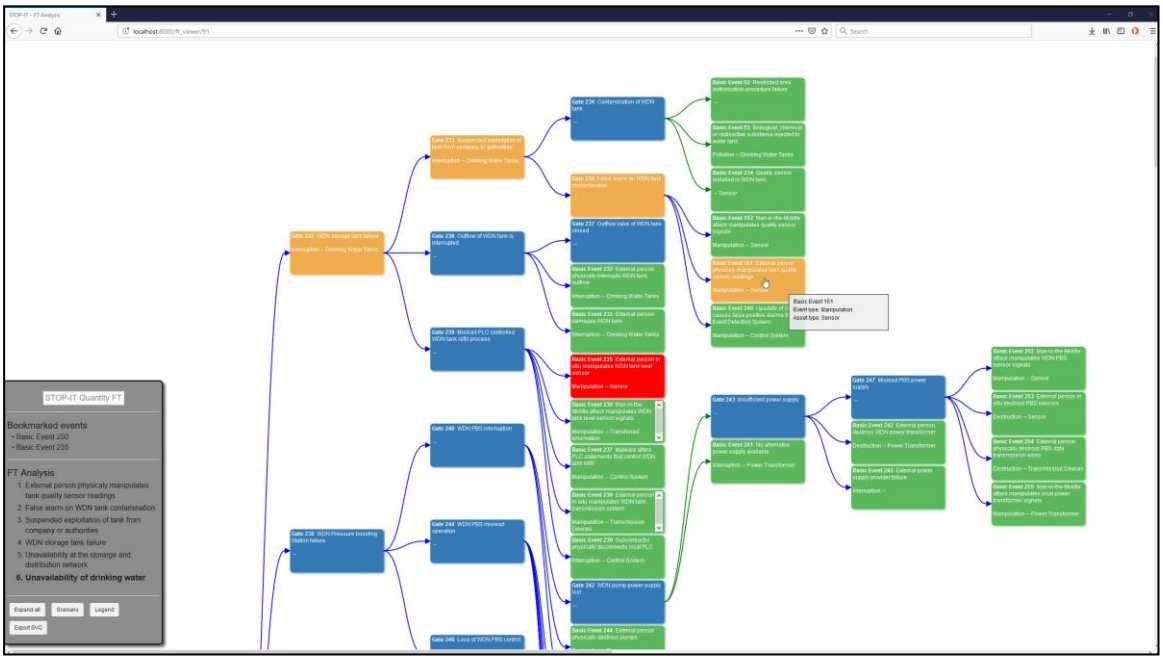
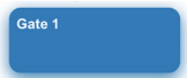
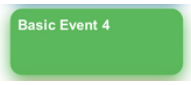
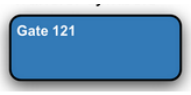
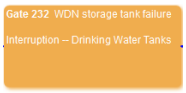


Figure 56: Fault Tree viewer

The symbols in the FT have the following interpretation:

OR Gate  An OR gate symbol represents the Boolean OR operation in the relationship between input and output events.

AND Gate  An AND gate symbol represents the Boolean AND operation in the relationship between input and output events.

Intermediate Event		An intermediate event is triggered by another event (basic or intermediate) of the FT
Basic event		Basic events are the leaves of a hierarchical tree and are not further developed.
Bookmarked event		By clicking on an event box once the colour of the box turns to red, indicating that it has been bookmarked for further use in later stages of the process. At the same time, the list of bookmarked events in the control pane of the FT viewer is updated.
Transfer event		Similar to a transfer symbol of a fault tree, this box of an intermediate event having thick border symbolizes that the fault tree of a subsystem is hidden. It will be shown by double clicking with the mouse on the box. To hide the subsystem, double click on the box again.
Triggered event		On hovering over an event all events that may be triggered by cascade up to the root event are highlighted. The list of cascading events is shown on the control pane. If triggering of an event depends on one or several conditions, i.e. if input and output events are connected with an AND gate, then this event and all subsequent events in the list of cascading events are greyed out.

4.7.3. Vulnerability Assessment with AVAT

In this version of RAET vulnerability assessment is performed by AVAT (Figure 57), developed by TECHNION in Task 4.1 of WP4. AVAT is a Windows desktop application which can be invoked from the RAET homepage by clicking on the Vulnerability picture, provided that AVAT is installed on the PC and the user has access to it. As this is a Windows desktop application, it is executed on the local machine and can be controlled only by the Windows user. Remote users can gain control of AVAT through a remote control or desktop sharing software such as TeamViewer or Windows Remote Desktop.

Additional information on the methodology and use of AVAT is provided in deliverable D4.1.

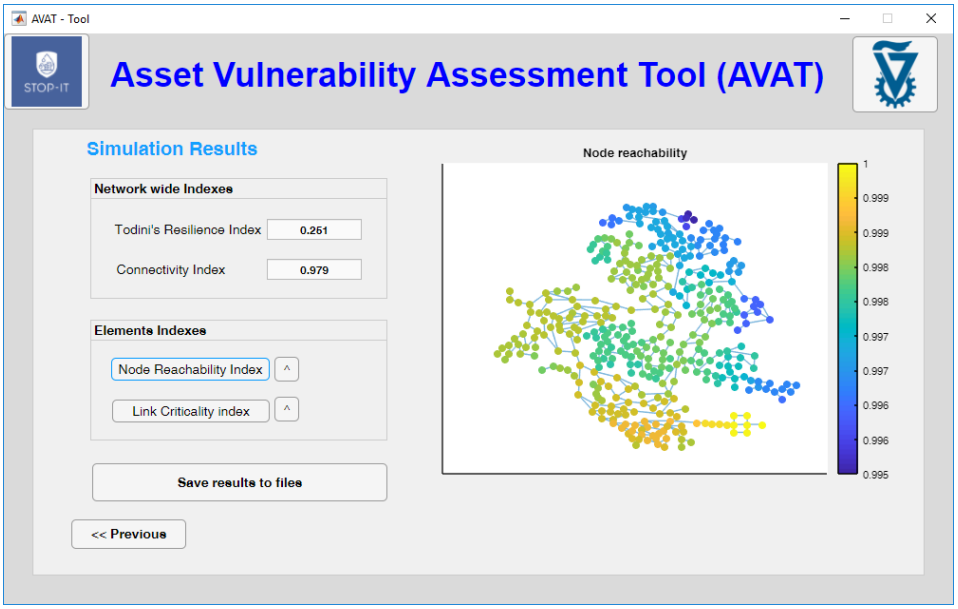


Figure 57: Example of simulation results as shown by AVAT

4.7.4. Search capabilities

Full text search

The RAET provides full text search functionality to all kinds of stored textual information, including names of entities, classes, descriptions, etc. The search algorithm is based on Levenshtein Distance for approximate string matching (Levenshtein, 1966), i.e. finding strings within a longer text that match a given keyword approximately. The results are presented as an excerpt of the text in which the given keyword has been encountered, along with the names of the relevant object and property including a link to the object's detail page (Figure 58).

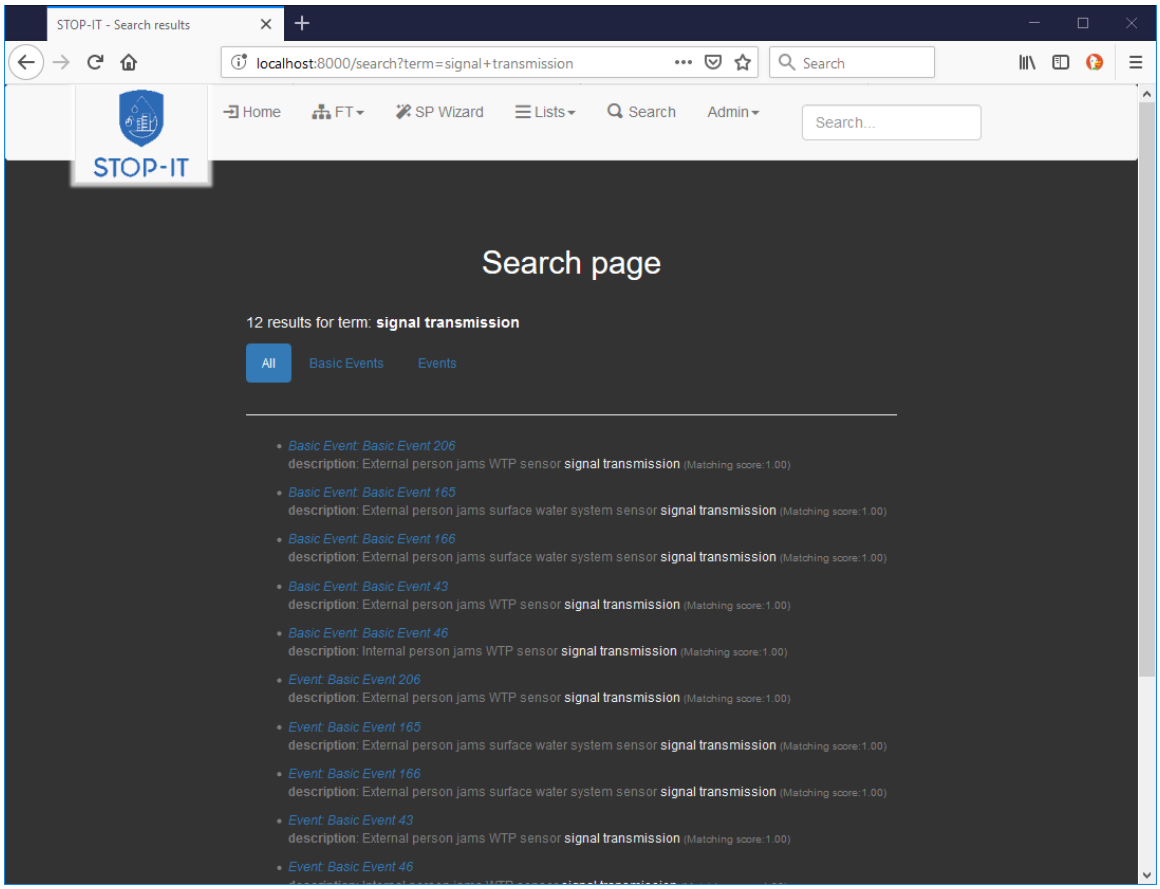


Figure 58: Results from full text search

Search in the RIDB

In addition to the full text search, RAET provides the means for the user to search within the RIDB, i.e. the risks and events database. The events list page (Figure 59), accessed by selecting `Lists/Events` from the main menu, lists in tabular form all events stored in the database, regardless of the related FT. Each row of the table provides some basic attributes (ID, name, description, asset type, event type, FT event category) and the number of associated measures which can potentially address the event. By clicking with the mouse on the number, the user is navigated to the measures list.

On the right pane the following filters are provided which narrow down the listed events:

- Filter by keyword. The keyword entered by the user is checked on-the-fly against the event attributes. Only those rows having at least one match are shown in the list.
- Filter by event type. These are the event types as specified in the RIDB.
- Filter by asset type. The asset types are defined as specific asset types in the RIDB.
- Filter by fault tree. Keeps only those events which appear in the selected FT.
- Filter by tools. Keeps only those events which are supported by the selected tools.

Multiple selections are possible. The actual number of selections is provided in brackets next to the name of the filter category.

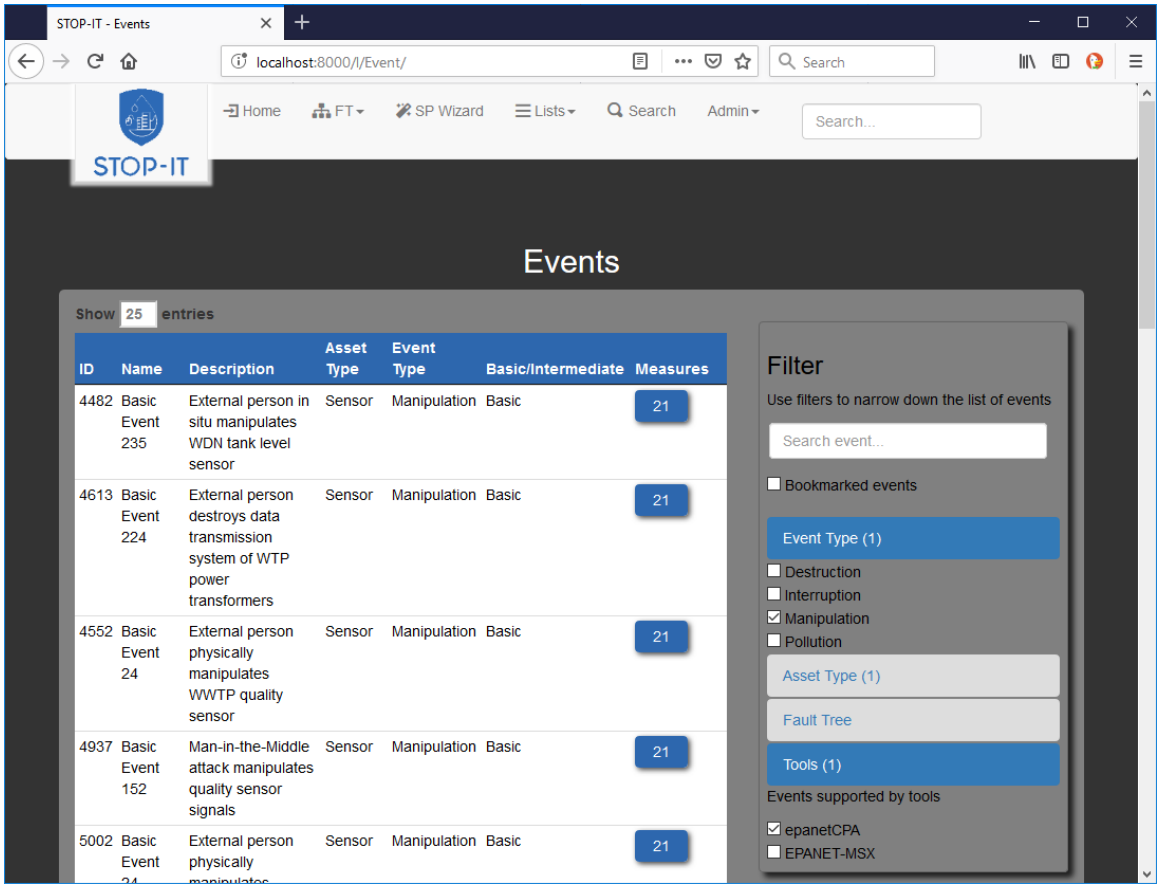


Figure 59: Events list page

Search in the RRMD

Similar to the RIDB, the user can search the RRMD from the risk reduction measures list page (Figure 60). The user can access it by selecting `Lists/Measures` from the main menu.

When pressing the button `Reassess relations`, all existing relations between risks (events) and suitable measures will be deleted and reassessed according to the matching algorithm. This procedure may take several minutes to complete and should be initiated a) if either the Risk Identification Database (RIDB) or the Risk Reduction Measures Database (RRMD) has been modified or b) if the methodology for the calculation of relationships has changed.

When clicking with the mouse on a row, the user is navigated to the detail page of the specific risk reduction measure (Figure 61), providing data on the attributes of the measure and the

relationships to other objects with the name of the related object as hyperlink. By clicking on the name, the user is navigated to the detail page of the related object.

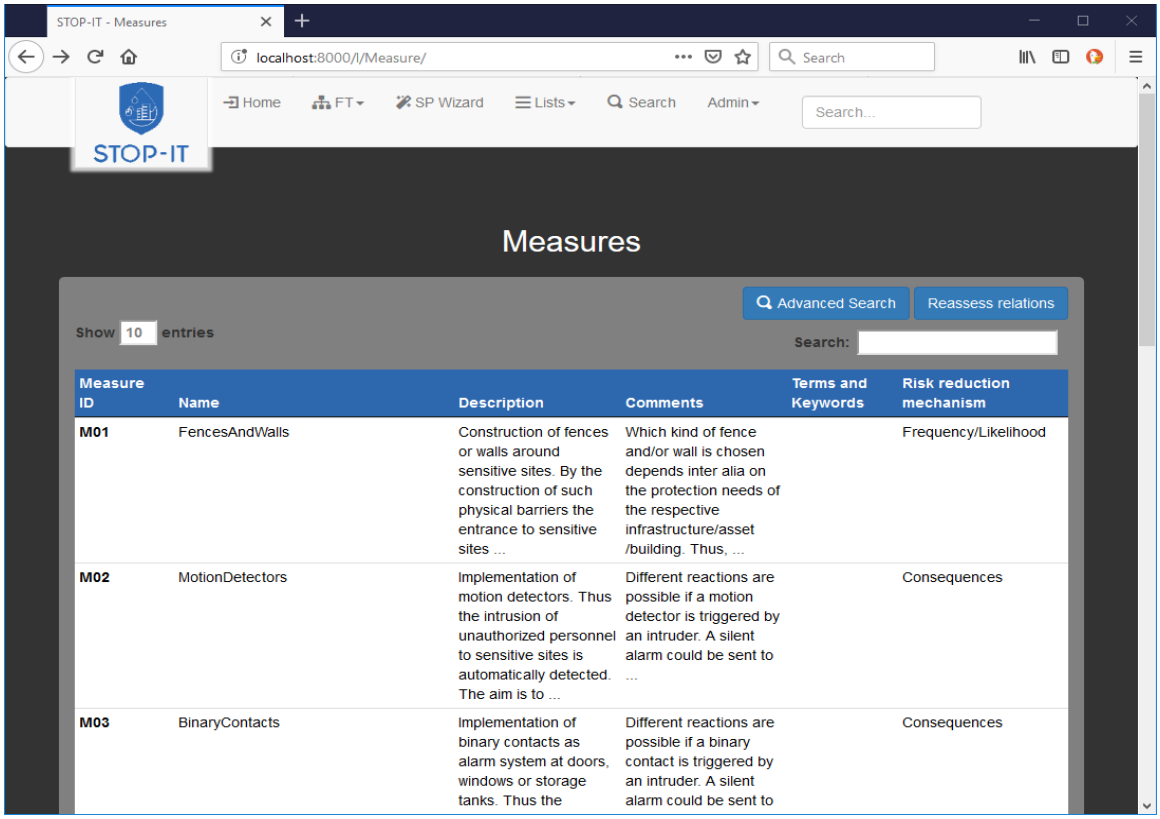


Figure 60: Risk reduction measures list page

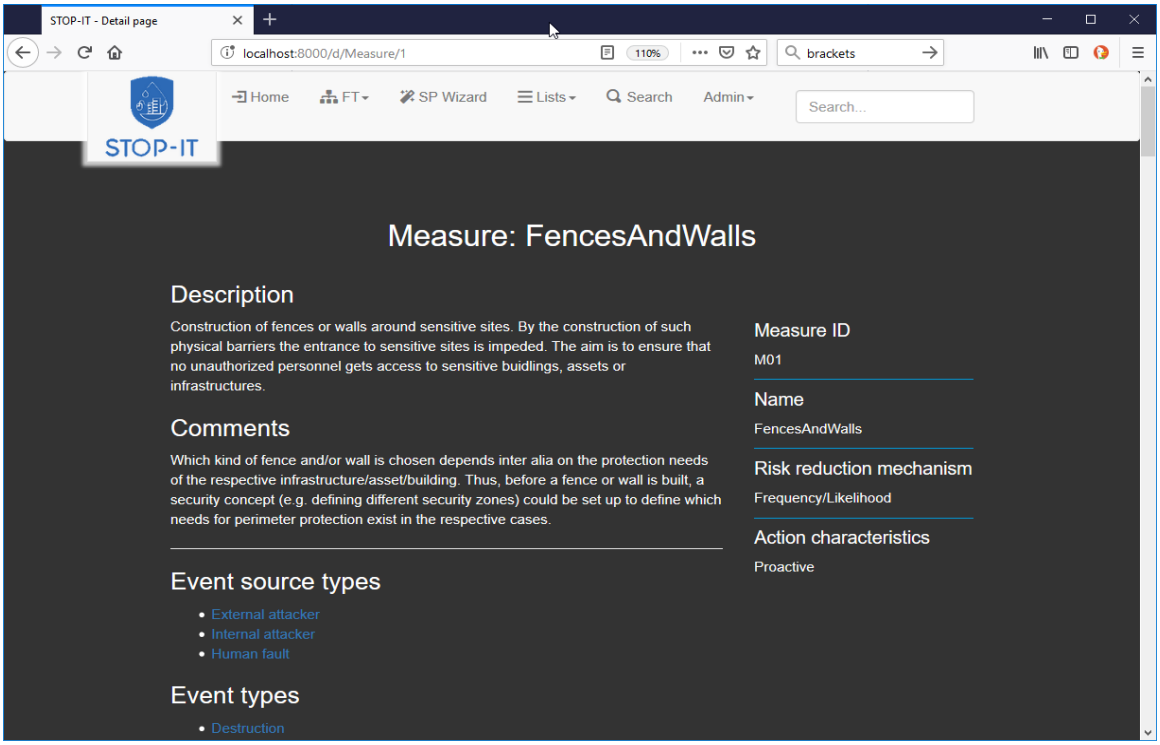


Figure 61: Risk reduction measure detail page

By clicking on the button `Advanced Search`, the advanced search page for measures appears (Figure 62). It provides a way to query the RRMD with user defined criteria. A narrative for better understanding of the query is formulated on-the-fly and presented in the yellow box. In the same box a number is displayed corresponding to the number of items which comply with the criteria. When clicking on the button `Show me`, the user is navigated to the risk reduction measures list page, listing those measures which match the criteria.

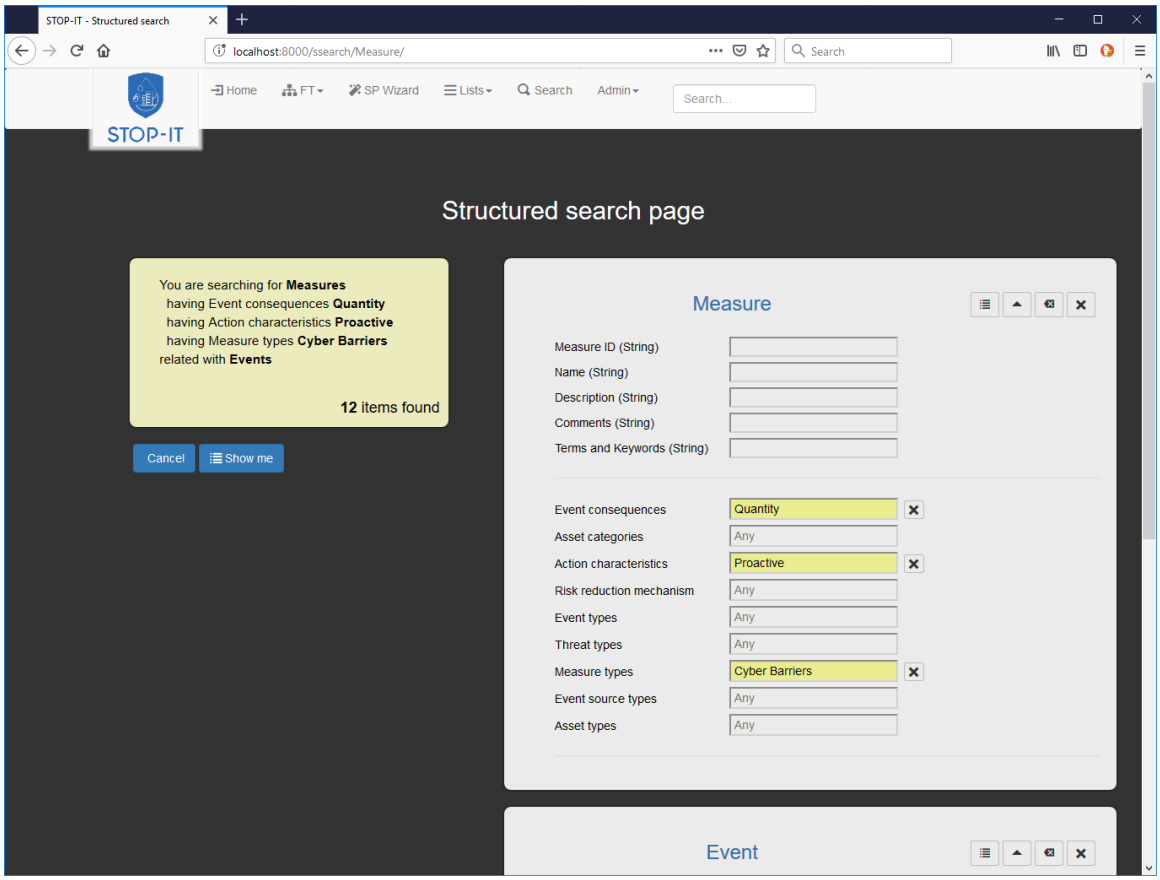


Figure 62: Advanced search page

4.7.5. Fault Tree Manager

The Fault Tree Manager is responsible for importing into RAET Fault trees of cascading events and deleting existing ones from the RAET database. These operations are managed through operations provided in the Fault Tree list page (see section 4.7.2). In order to create a new FT, the FT Editor has to be called from the homepage, provided that this application and its database are installed and properly connected to the RAET (see section 4.7.1). Figure 63 shows the main view of the FT Editor. Further information on the creation and management of FTs using the FT Editor will be provided in deliverable D6.3.

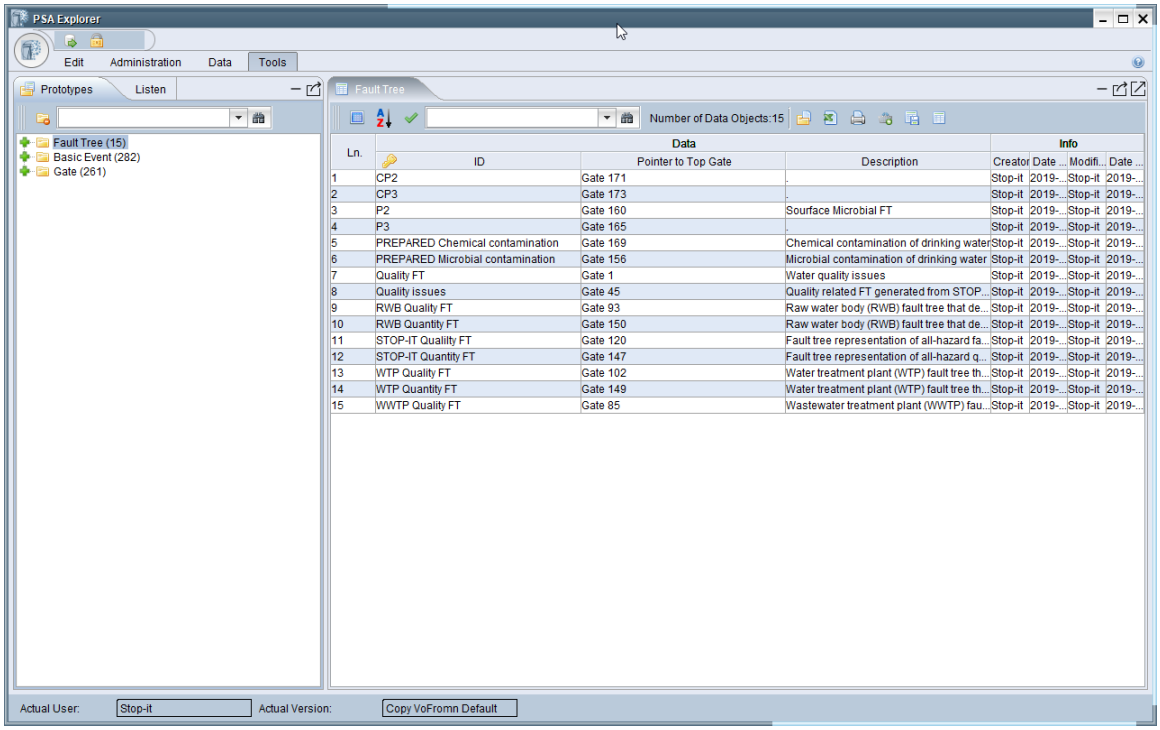


Figure 63: Main view of the FT Editor

Once a fault tree has been created, it can be exported in the Open PSA format by right-clicking on the FT name on the left pane and then selecting `PSA Export` from the pop-up menu (Figure 64).

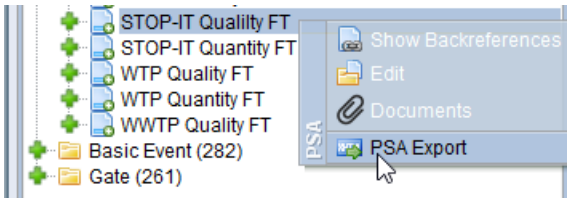


Figure 64: Exporting FT in Open PSA format

After that, the XML file can be imported as a new FT from the RAET. By clicking the button New FT, the FT detail page appears from where the user can select the file to import and give the FT a name and optionally a description (Figure 65).

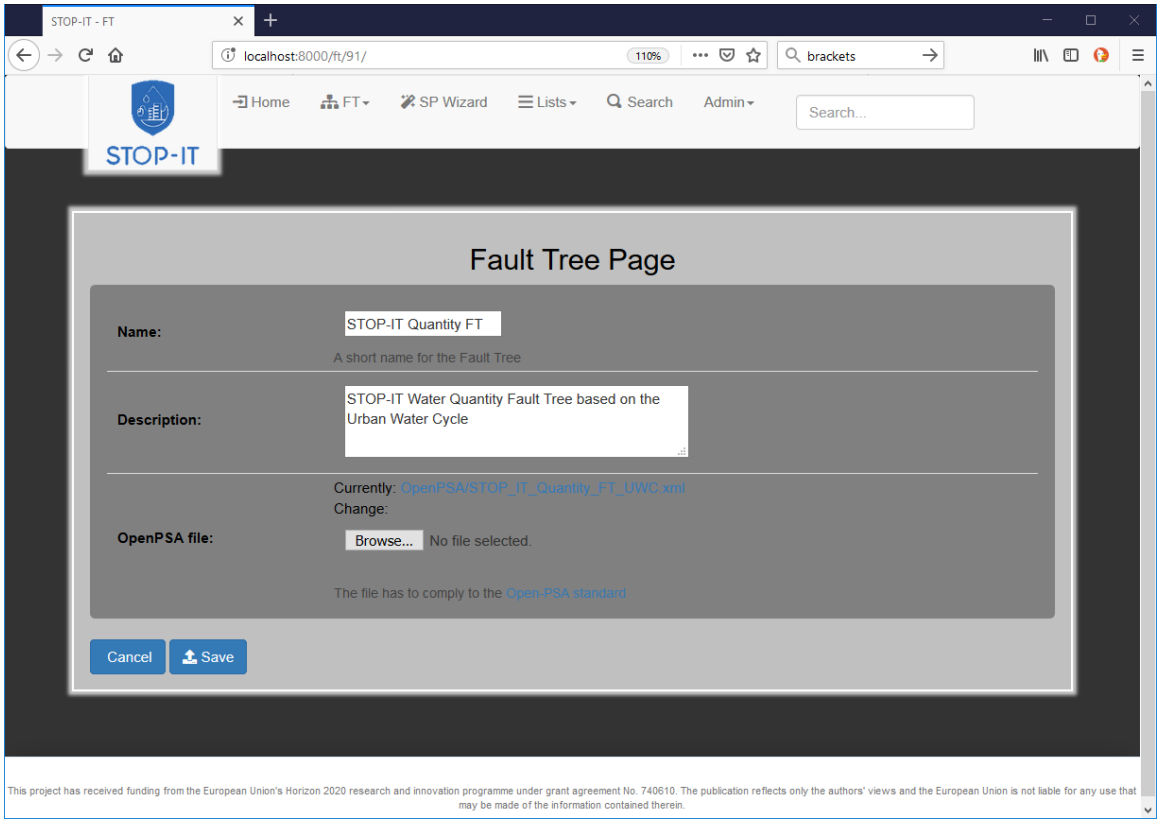


Figure 65: FT detail page

Another way to import a FT through the FT detail page is by selecting from the main menu `FT/Import` as shown in Figure 66.

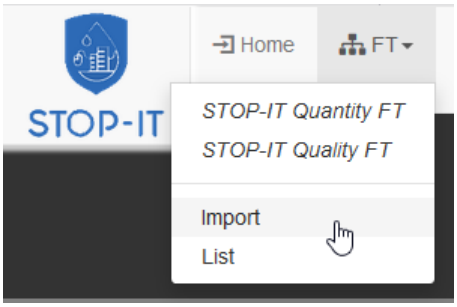


Figure 66: Menu option which navigates to the page for importing a new FT

Trying to delete an existing FT will require a confirmation by the FT Manager. On the delete confirmation page all related items are listed which will be deleted as well (Figure 67).

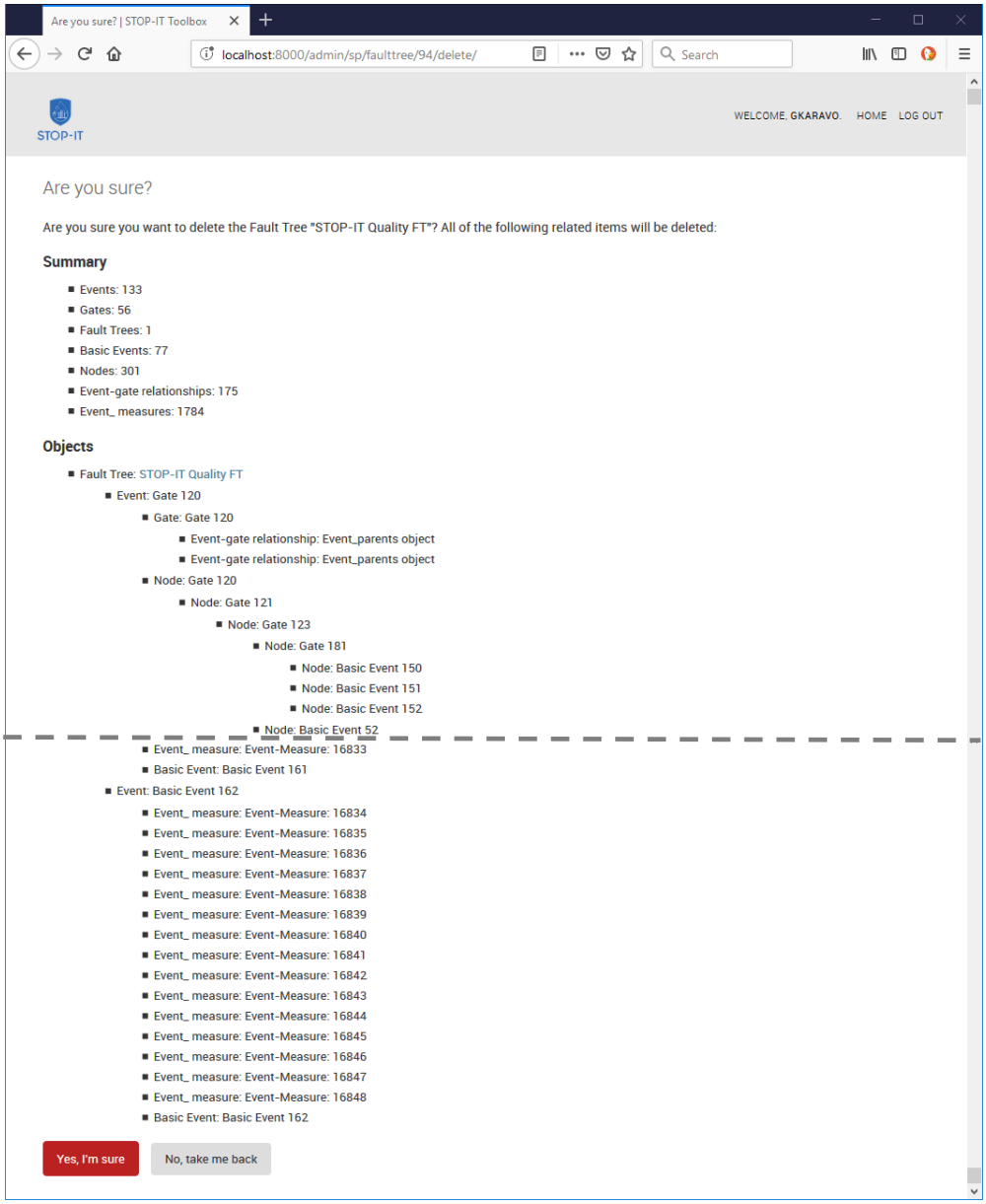


Figure 67: FT delete confirmation page

4.7.6. Tools Manager

The Tools Manager is responsible for managing the tools library in the RAET. This can be done from the Tools list page (Figure 68), which can be called a) from the homepage by clicking on the related figure or b) by selecting from the main menu `Lists/Tools`.

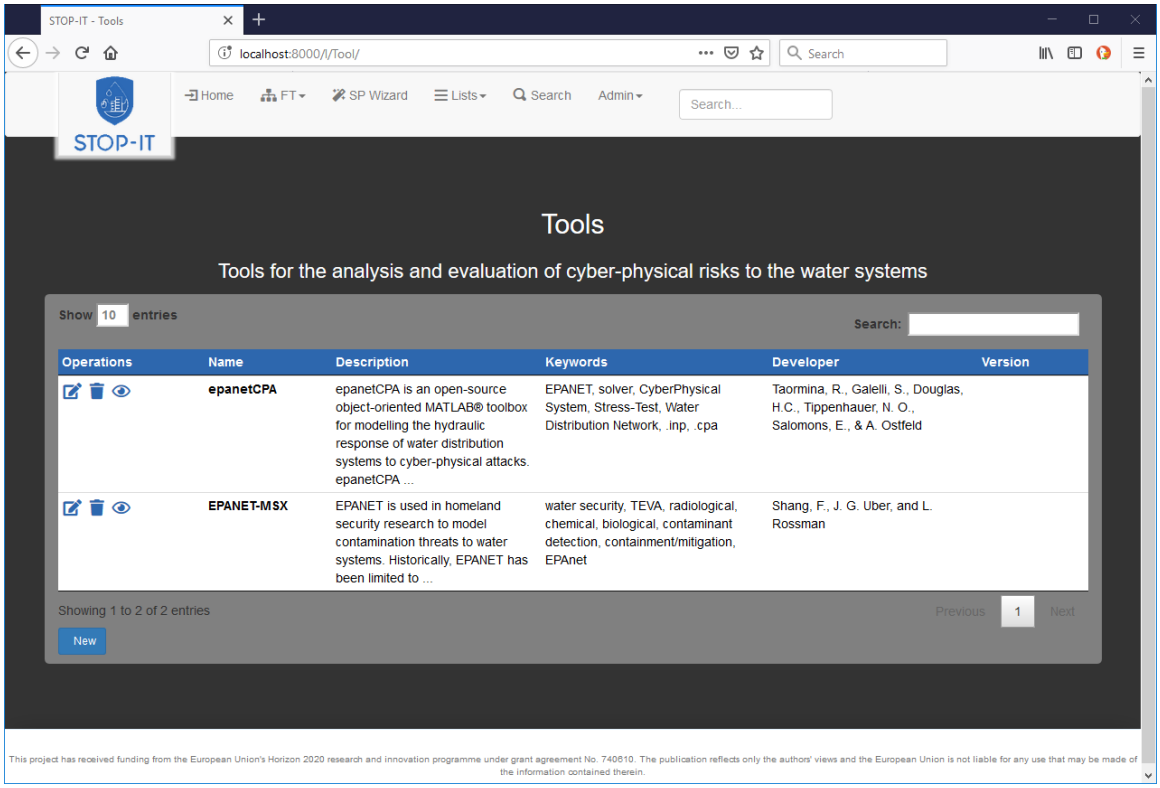
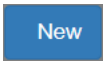
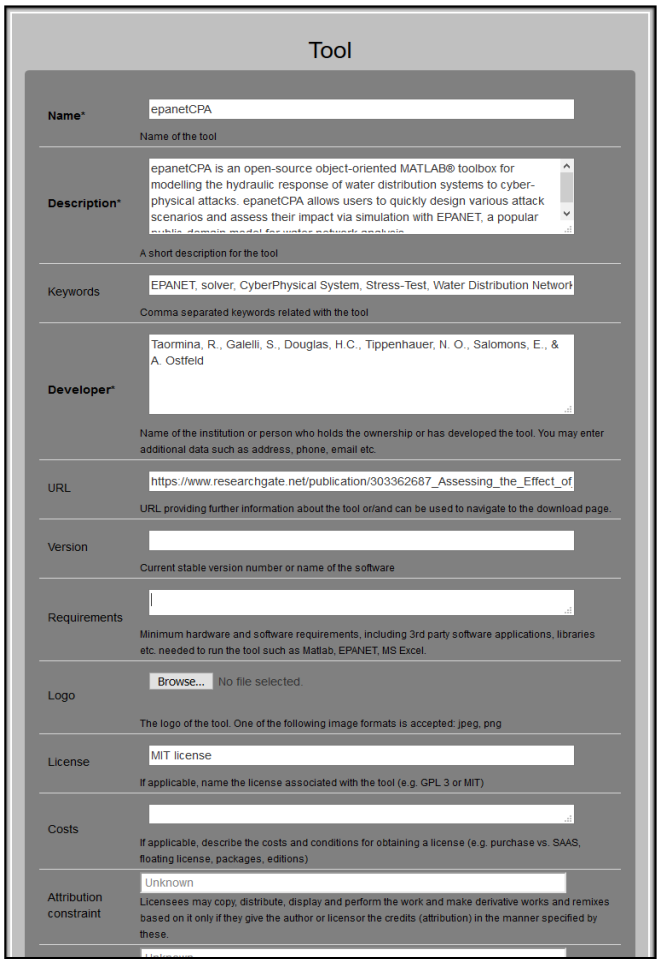


Figure 68: Tools list page

Possible operations are the following

Icon	Description of the operation
	Opens the tool form for editing (Figure 69)
	Opens the delete tool page which enables the permanent removal of the tool from the database after confirmation by the user.
	Shows the tool detail page (Figure 70). This operation is available to all users
Button	
	Opens a blank tool form for creating a new tool.



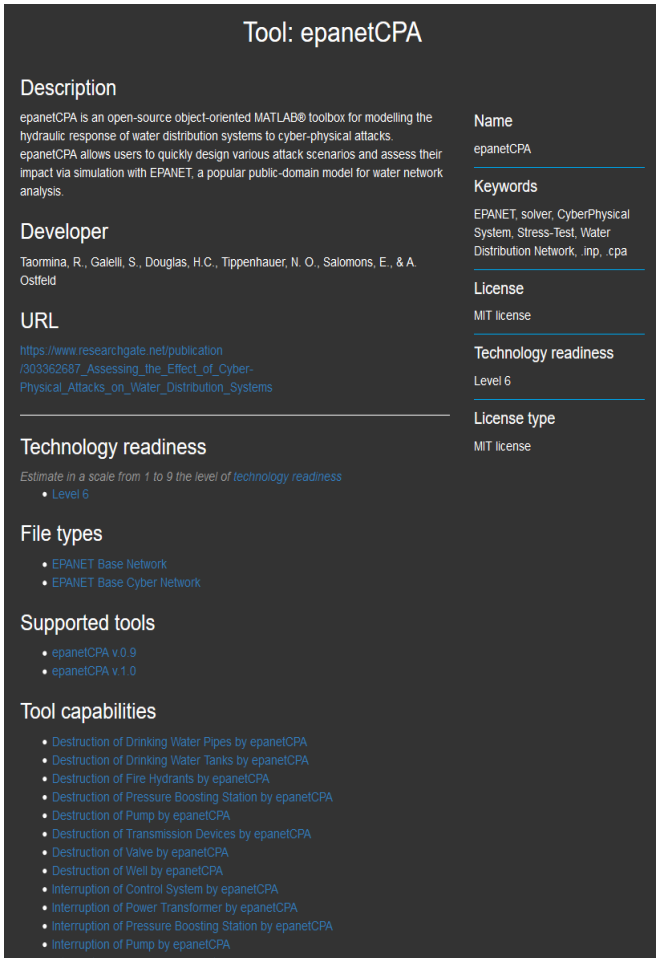


Figure 69: Tool edit form

Figure 70: Tool detail page

4.7.7. Modeler

A Modeler is responsible for creating, managing and simulating scenarios. After analysing the FTs, the user will identify the threat(s) based which the scenario will be developed, select the assets upon which the event(s) will be applied and can select risk reduction measures along with a tool to simulate the scenario. After that the user initiates the simulation and evaluate the results in comparison with other scenarios.

This can be done from the scenario list page (Figure 71), which can be called a) from the homepage by clicking on the related figure or b) by selecting from the main menu `Lists/Scenarios`. The scenario list page provides an overview of the existing scenarios and some of their main characteristics in a tabular form:

Tools	List of tools capable to simulate the scenario
Base scenario	The reference scenario. This scenario is a variation of the reference scenario.
Name	The name of the scenario

Description	A short description for the scenario
Events	Number of events (CP threats) associated with the scenario
Created	Date on which the scenario is created
Executed	If applicable, date on which the scenario simulation has been executed

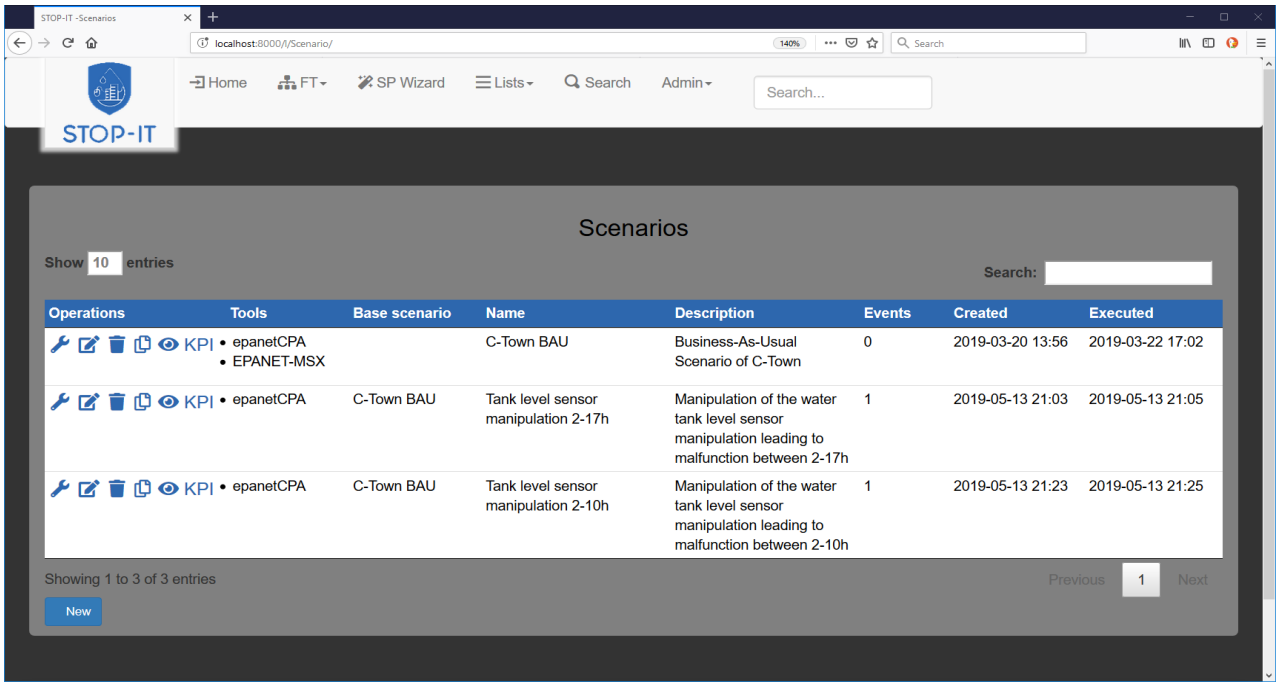


Figure 71: Scenarios list page

The following list shows the available operations represented by icons.

Icon	Description of the operation
	Navigates to the related default tool
	Opens the scenario form for editing (Figure 72)
	Opens the delete scenario page which enables the permanent removal of the scenario from the database after confirmation by the user.
	Clones the scenario
	Shows simulation results (available only if the scenario simulation has been executed, Figure 76)
KPI	Invokes the KPI Tool for detailed results analysis (available only if the scenario simulation has been executed)

	A runner next to a tool name indicates that this scenario has not been simulated yet and that the simulation is supported by the particular tool. This option is not available in case the simulation has been executed once.

By clicking on the edit icon or by pressing the `New` button, the user is navigated to the Scenario edit page (Figure 72). Here the user can provide or modify the main attributes of the scenario (name, description, base scenario, default tool) and after saving it, can specify the events associated with the scenario using the scenario wizard.

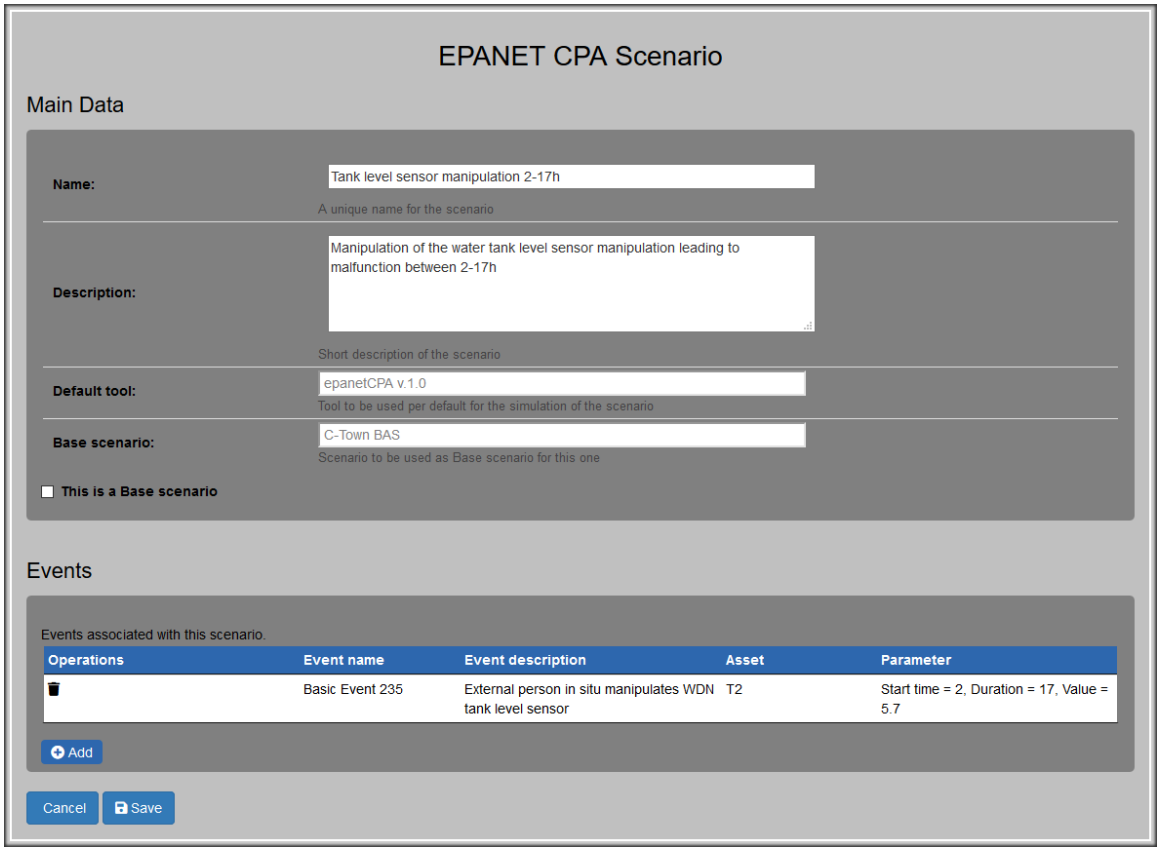


Figure 72: Scenario edit page

The first screen of the scenario wizard (Figure 73) shows a list of all known CP events. The user can filter out events and narrow down the selection using filters in the same way as for the RIDB described in the events list page (see Figure 59). The user selects an event to be associated with the scenario by clicking on any part of the event row. The background of the row turns red, indicating that the event is selected.

After that, the user may proceed to the next screen of the wizard which is the asset selection (Figure 74). Here, all assets are listed which may be affected by the selected event. In order to do so, RAET loads all assets from the network file, defined by the scenario (.inp file in EPANET), and identifies possible affected assets based on the characteristics of the asset

type attribute of the event. Again, the user is requested to select the asset affected by the event.

In the third and last stage, a form with additional parameters is shown and the user is requested to fill in values (Figure 75). These parameters specify the details for the simulation and the event and depend on the selected event type, asset type and tool.

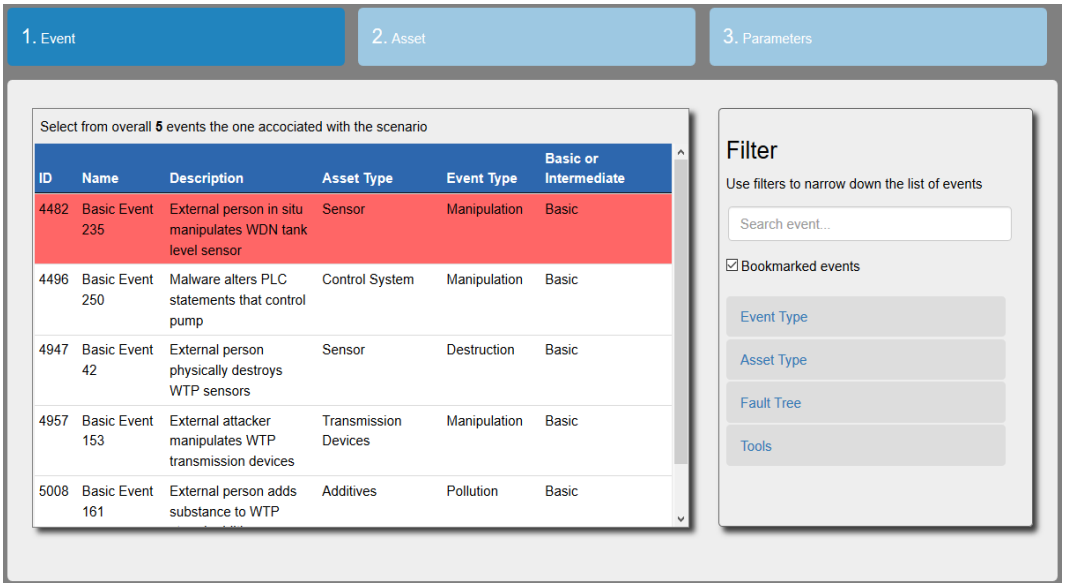


Figure 73: Scenario Wizard – Event selection

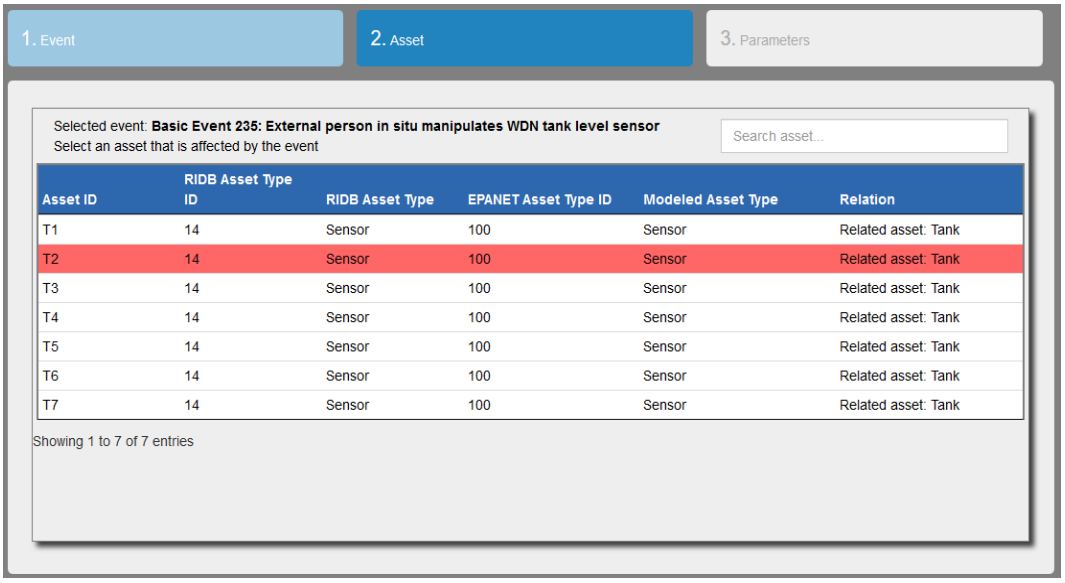


Figure 74: Scenario Wizard –Asset selection

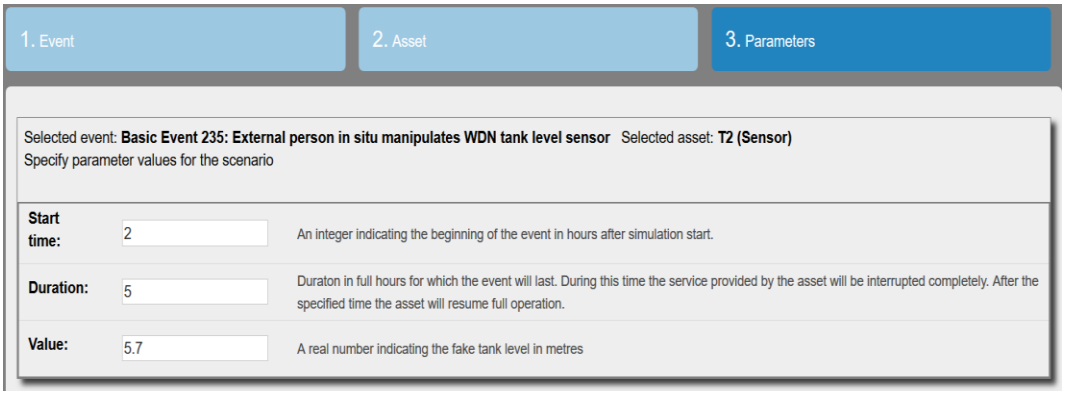
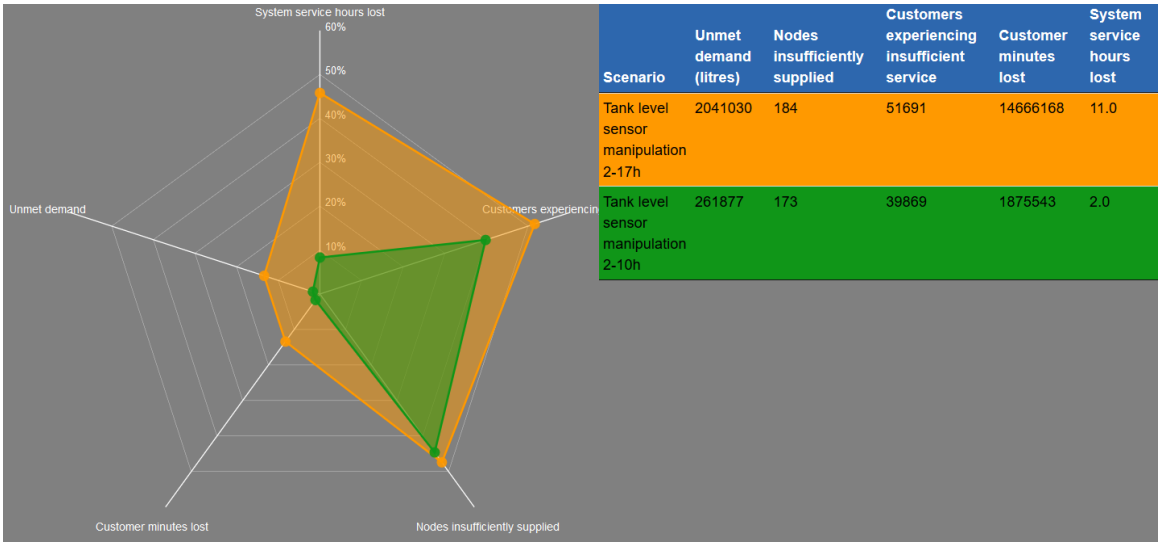


Figure 75: Scenario Wizard –Specification of parameter values

After completing the specification of the scenario, the user can run the simulation by clicking on the runner icon ( ), next to the selected tool. The simulation may take several minutes to complete, upon which the execution date and time appears in the scenario row. The main results of the simulation can be viewed by clicking on the eye icon ( ). In this version of RAET the results documenting water quantity issues are shown the following five dimensions in tabular form in absolute numbers and as a radar chart in percentages: a) Unmet demand, b) Nodes insufficiently supplied, c) Customers experiencing insufficient service, d) Customer minutes lost and e) System service hours lost (Figure 76).



Scenario	Unmet demand (litres)	Nodes insufficiently supplied	Customers experiencing insufficient service	Customer minutes lost	System service hours lost
Tank level sensor manipulation 2-17h	2041030	184	51691	14666168	11.0
Tank level sensor manipulation 2-10h	261877	173	39869	1875543	2.0

Figure 76: Comparing scenario results

Once a scenario simulation has been executed, it cannot be modified, as this would introduce inconsistencies between the scenario data and simulation results. For the same reason it is not possible to run the scenario again. However, a new scenario can be created by cloning an existing one (click on icon).

More detailed analysis of the simulation results is provided by the KPI Tool (see PART E) which can be invoked by clicking on the icon KPI provided that this tool is installed and properly connected to the RAET.

4.7.8. Administrator's guide

Administrators are capable to access any functionality of the RAET, but their main responsibility is the user management, i.e. adding new user accounts to the system, giving them roles as specified in section 4.4, specify their characteristics and removing them from the system. The administrator role becomes even more important if the RAET is installed in an Intranet and accessed by several users over the network.

After logging into the system, an Administrator can navigate to the Users management page (Figure 77) from which is possible to add/delete/filter user accounts. A selected account can be further specified in the user's page (Figure 78). In this page user roles are given (indicated as Groups).

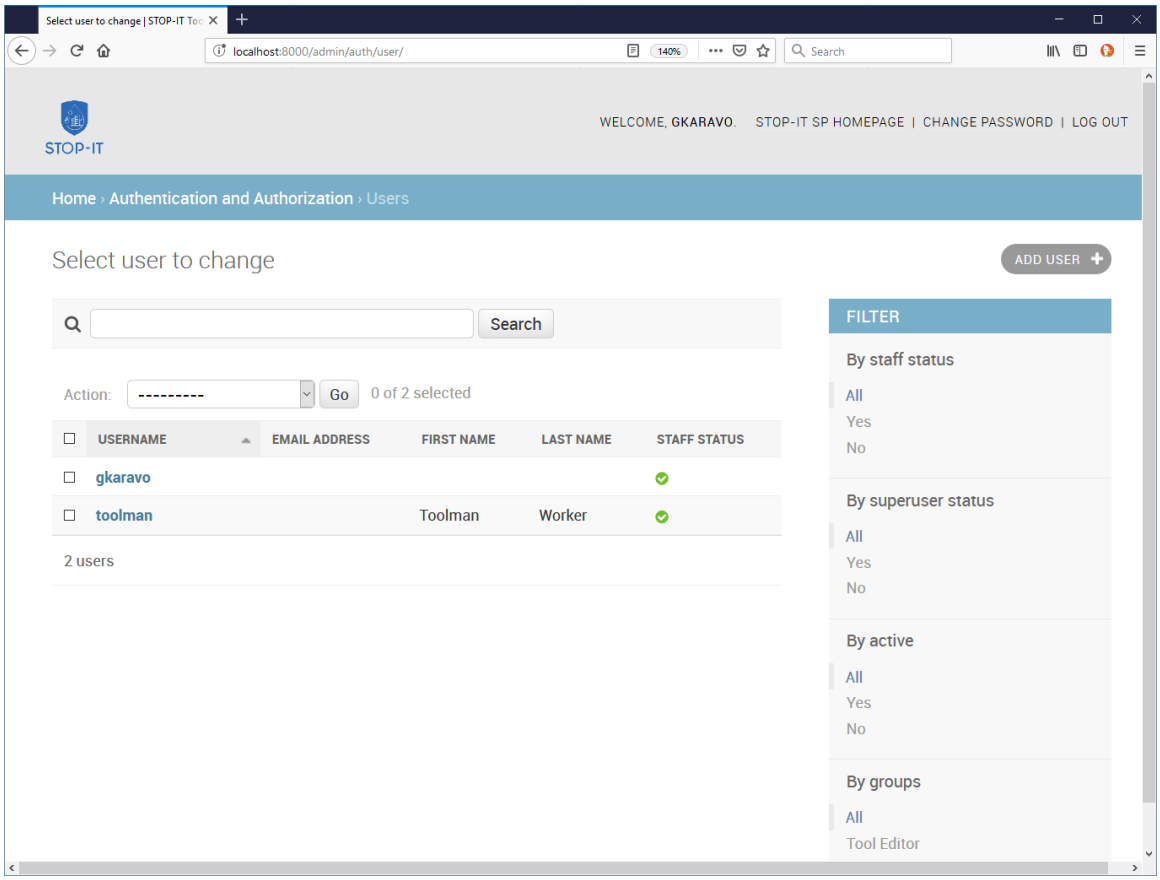


Figure 77: Users management page

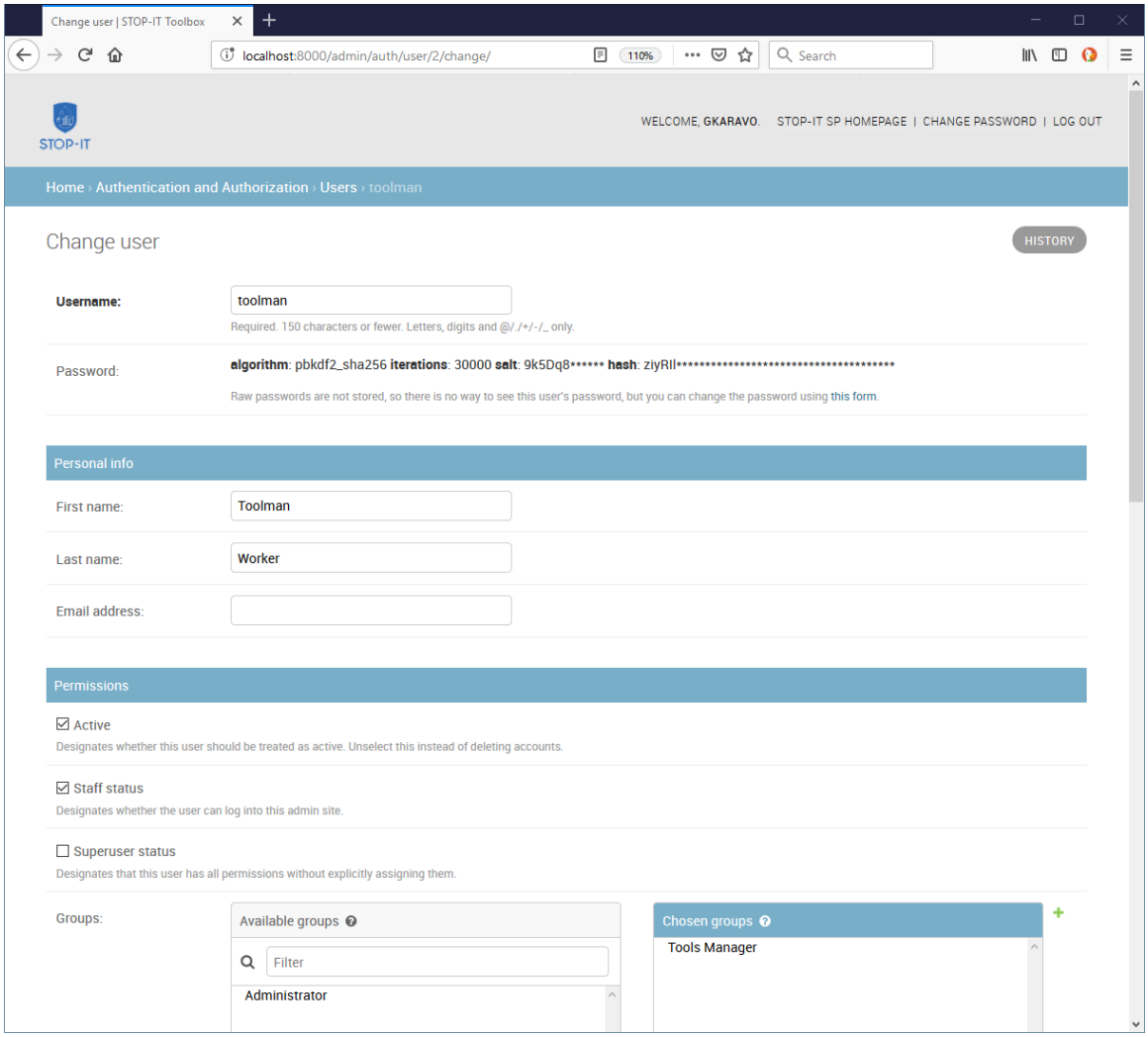


Figure 78: User's page

Part E: KPI Framework and Tool

In the following sections the actual development of the Key Performance Indicators foreseen under Task 4.2 and a corresponding tool is documented giving the users more information related to its design, content, scope and architecture as well as the technologies used for its development.

5.1 STOP-IT Key Performance Indicators Framework

5.1.1 KPI approach in tactical and strategic planning

A water sector CI under optimal conditions is designed to provide sufficient quantity and quality of water, covering customer's needs (and expectations) without interruptions for the entire network. By default, stress testing conditions (as real-time disruption events) are less than optimal, decreasing service levels and generating consequences that affect quantity or quality of supplied water to customers at specific areas of the network for a period of time. Thus, the goal of performing stress-testing simulation is to assess this loss of performance. The results of the Stress Testing Platform (STP) simulations are the raw consequence data pool from which the user gets this vital information. Translating raw data and keeping an overview of the simulated behaviour of a water CI is a difficult task due to the large volume of data. Real water network models contain thousands of nodes and connections, with multiple functions and constraints in addition to dynamically temporally and spatially varying characteristics of operation over the defined simulation period. Even skeletonized network models, with known limitations and shortcomings (Davis and Janke, 2018), produce large sets of data for the included assets and multiple operational dimensions (pressure, pipe flow, tank head, valve setting etc.) over a simulation period, while timestep is also adding to the detail and volume of results as well. Therefore, making sense of stress-test results in a simple, structured and efficient way, to assist risk-informed decision-making (Hansson and Aven, 2014), is of paramount importance, and can be achieved by mapping results to suitable indicators.

In literature, several performance indicators of water supply systems are metrics used to compare companies in the same sector (e.g. customers/km of pipe, valves/km of network etc.), as well as to show the performance of the management practices (e.g. hours of training per personnel, number of inspections per year etc.). In STOP-IT and in Risk Management in general, PIs need to indicate the change of network's performance under various attacks or measures. The goal of the STOP-IT KPIs must be the representation of the impact and the response of the system in different dimensions of interest, enabling the comparison between attacks or measures implementation, through simulation results' mapping. Specifically for the dimensions of interest, according to STOP-IT DoW, KPIs must 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. According to the European Standard BS EN 15975-2:2013 for security of drinking water supply (referenced by Commission Directive (EU) 2015/1787), system integrity is achieved when the system can "meet specified quality, quantity, continuity and pressure targets in accordance with legal/regulatory requirements and the drinking water supplier's objectives". The above dimensions are in line with the answers provided by the FRs in Task 3.1, responsible for identifying risk criteria against which risk is evaluated (D 3.1) and the DoW description of the KPI dimensions.

In order to assess its network's loss of performance under attack, the users must be able to immediately get a sense of the type, the level, the extent and the rate of impact in the services provided. For this reason, we propose a 3-step logic approach for the creation of STOP-IT KPIs. The first step is categorizing the services provided by the company to the customers and those are the supply of adequate quantity and quality of water. For both those services, we can identify 2 failure levels (step 2). The first level is related to the minimum acceptable requirements of service (company's operational environment, regulation, standards etc) and the other related to what can be considered as a tolerable level of service, which can be associated with mild discomfort of customers and, inevitably, reputational damage to the company. For both services (quality and quantity) and failure types (complete and partial), metrics related to physical aspects, spatial characteristics and dynamics of the system are used. The following figure demonstrates the previously mentioned logic.

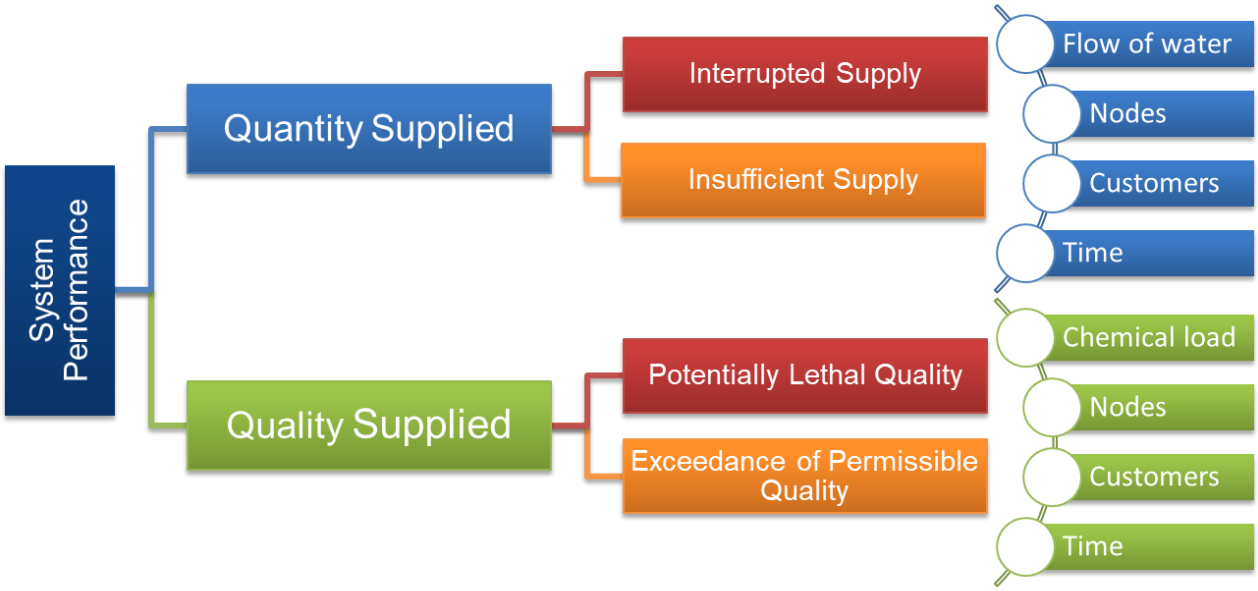


Figure 79: 3-step logic of STOP-IT KPIs development

Note that all indicators that were created in STOP-IT under this structure are directly referring to the loss of performance, in order to avoid misleading evaluation perspectives in the context of "how well the system is performing under stress", but rather approach the true meaning of

evaluating risks and treatment options through stress testing, that is “how critical are the consequences in the system under the examined threat”.

Based on the above structure of Figure 79, two sets of indicators can be recognized based on the water CI services: those related to the sufficiency of quantity and those related to the quality of water supplied. It is worth mentioning that for each of those sets, service level is adjustable, making the metrics representative to each company’s risk criteria and encapsulating the company’s risk perspective, internal and external environment in which the organization seeks to achieve its objectives, as proposed in ISO 31000. Those service levels can be viewed with a “traffic lights” of risks analogy. Complete failure levels (Supply interruption and potentially lethal quality) are a potentially harmful and operationally critical state of the system, for which special attention should be given (red light). Partially inadequate service levels (Insufficient or substandard supply) are a non-harmful and more reputation-oriented failure level, raising a caution flag (yellow light). Any service that meets the requirements above inadequate level, up to optimal service performance is considered as normal performance (green light). The above process can be seen as an intermediate classification of failure, important to the separation between critical and less critical levels, and apply indicators on each separately to better comprehend the profile of failure.

As the KPIs are used to map simulated results of the CI network, besides the service level filter previously described, as second data filter is applied. STOP-IT KPIs, as seen in step 3 of the process, are exploring 4 dimensions of system consequences under a CP attack and allow users to explore connections or hidden characteristics. In general, the STOP-IT designed metrics are providing answers, for each service level, to the questions:

- How much performance is lost? (Supply & Chemical load dimension)
- What part of the network? (Nodes dimension)
- How many were affected (Customers dimension)
- For how long? (Time dimension)

In addition to the previous dimensions that are used to map the consequences of the simulated threat, one additional key information is also added, that of available time. This information dimension applies not to the duration of the effects, but to key critical times of the system in respect to the start of the simulated threat, representing available time windows for action to be taken into consideration and assist emergency planning. Those indicators are capable to address resilience related evaluation in terms of time.

In order to detect and interpret key attack consequences’ characteristics for each dimension mentioned before, a 4th step is needed, applied to every branch of the STOP-IT KPI Framework structure. In this step, metrics families are built, each demonstrating a specific failure characteristic, e.g. magnitude of failure, peak temporal effect etc.

It is a known fact that water CI systems service multiple customers, some of which can be considered critical based on the societal impact the disruption of service can have.

Specifically, in the case of stress-testing against CP attacks, that specific category of customers should be taken under special consideration. Such critical customers can be:

- Hospitals,
- Schools,
- Government buildings,
- Military buildings,
- Industry,
- Fire hydrants,

as well as, any other infrastructure/asset found critical by experts. In this spirit, the company should create one or multiple Critical Customer Districts (CCD) that contains the nodes that service critical customers, and assess performance explicitly for those areas. For each CCD, different service level thresholds can be selected, demonstrating the importance or specific limitations and uniqueness for each part of the network under examination. This allows for a second level of adjustability that of spatial customization of metrics, to account for important operational gears of community and provide a more realistic overview of the simulated risk consequences.

From the above, it is obvious that the STOP-IT KPI Framework is a failure-oriented set of metrics, addressing multiple dimensions of failure customizable to each company's risk attitude that can be used to evaluate risk and treatment options under the lenses of various failure characteristics and spatial variations for critical customers. This dynamic set of quantitative failure KPIs is independent from the units used in simulation. More details for each process step and the produced STOP-IT KPIs can be found in the next sections.

5.1.2 System failure levels

As mentioned in the general structure developed for the STOP-IT KPI Framework, Risk and Treatment evaluation is performed in respect to specific system service levels. Assuming a stress testing scenario that leads to pressure deficient conditions, if only complete service interruption was considered as failure, the spatial image of consequences (and what the KPIs would later demonstrate) could be represented by Figure 80 (a), with 8 nodes being affected. Following this approach, system failure and the corresponding consequences would be produced by comparing the results of those nodes against desired behaviour of the system.

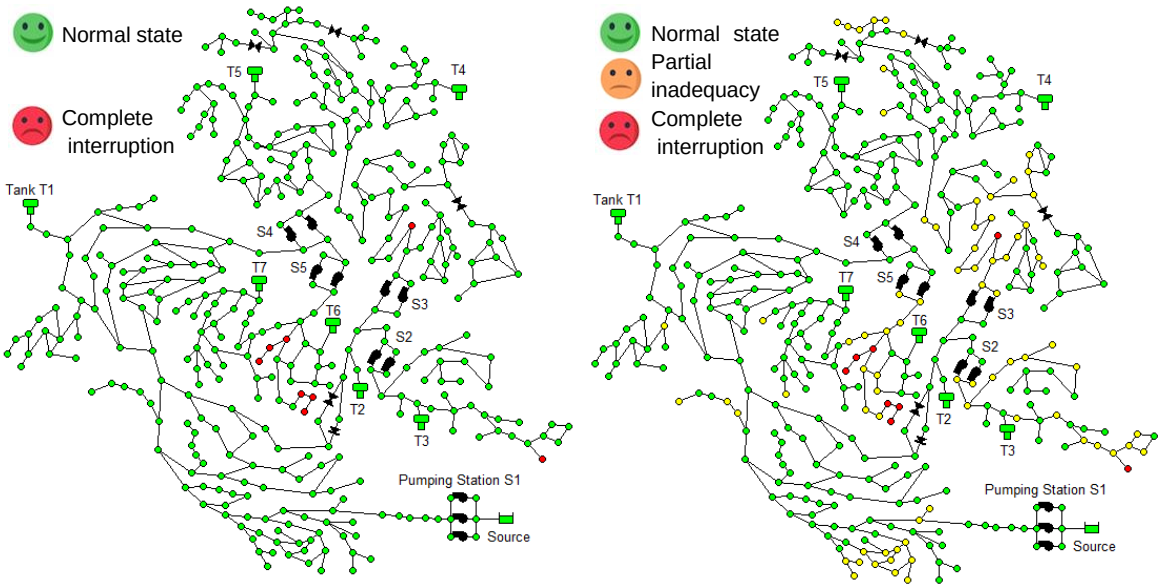


Figure 80: Visual representation of a) complete interruption failure level (left) and b) combination with partial inadequacy service failure level (right)

But in reality, the network failure would be closer to Figure 80 (b), since pressure drops and only partial supply of water would not be acceptable from customers. By adding this intermediate level of service in the evaluation process, company is able to identify consequences that may only bring minor discomfort to customers but affect its reputation. Different levels of failure also allow the exploration of those "hidden", less critical impacts prior to complete failure. This adaptation of the risk evaluation context to better reflect the company's perspective in terms of service also allows exploration of the treatment measure dynamics and effectiveness. This applies for both types of service recognized in step 1 of the process.

The first service towards customers is the supply of adequate water to customers (quantity). For this service we identify 2 levels of failure. The first is what is perceived as the most "critical" state, which is the complete interruption of service to nodes and customers, with 0-supply conditions. Those conditions can be found not only when the strict rule of "$Supply_{i,t}$=0" is found in the simulation results. Many companies would agree that, supplying only a small percentage l of demand in the simulation (even in pressure driven analysis configurations) is in fact zero-supply-equivalent in real life. In order to define this "threshold", each company can select a lowest acceptable percentage of demand, below which the customers would not open their taps. This percentage l is defined by and for each company and can vary per CCD, representing the importance of those customer nodes.

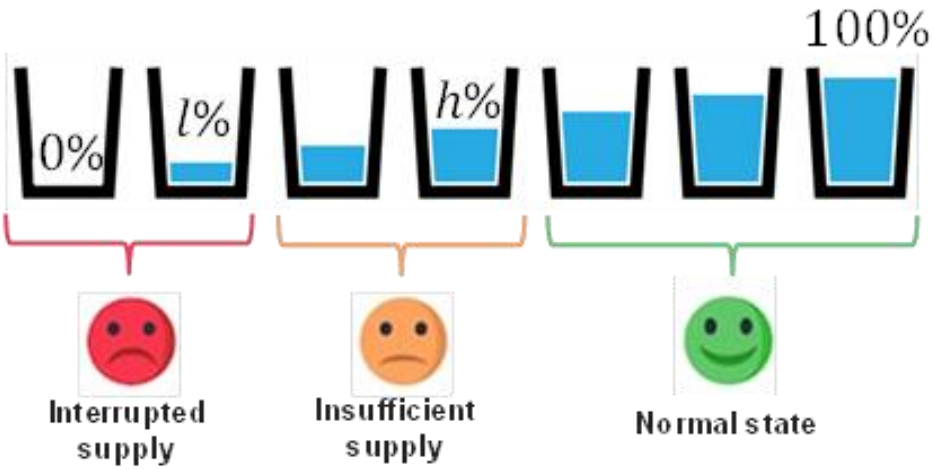


Figure 81: Visual representation of service level thresholds for quantity related failures

For example, supplying only 5% of the total demand of a node can be the threshold for one area, but in a CCD that includes hospitals, supplying more, e.g. 15% can also be viewed as a critical state and equivalent to complete service interruption, since it affects an infrastructure related to public health and vital for society. This threshold (adjustable for each user and CCD of the network) is denoted l throughout our document. The second state of failure in regards to quantity is that of insufficient supply. The lowest acceptable percentage of supply (l) is now the lower boundary condition for that failure state and the upper boundary is related to the sense of fulfilment, or satisfaction the customers feel for the quantity of supply. As such, upper boundary h is what the company perceives as the lowest acceptable percentage of demand provided to the customers before affecting reputation. Such a failure state can be seen a degraded state of the system related directly to customer satisfaction. Again, the upper boundary threshold is adjustable to the company's operational environment, especially since customers' expectations, needs and sense of fulfilment vary even within different districts of the serviced community. Any part of the system supplied with demand satisfaction ratio above threshold h, is considered to be in a business-as-usual operating state, normally operating and servicing customers. For both failure states, the obvious level of impact is the total unmet demand (or percentage of demand unmet). The number of nodes that fail can give a raw image on the extent of supply impact over the network and the number of customers affected. The survival of the system can be seen not only through unmet demand, but also through failure duration or rate of impact, which can be found in the rate of nodes being cut-off supply.

The second service of a water sector CI is the supply of high-quality water. There is no question that the water sector companies continuously work towards safe and high-quality water supply to their customers. In addition, quality standards and legal frameworks provide guidance in setting the minimum acceptable quality, towards customer's safety. Both biological and chemical contaminations directly affect human health, hence it is important to maintain high performance levels.

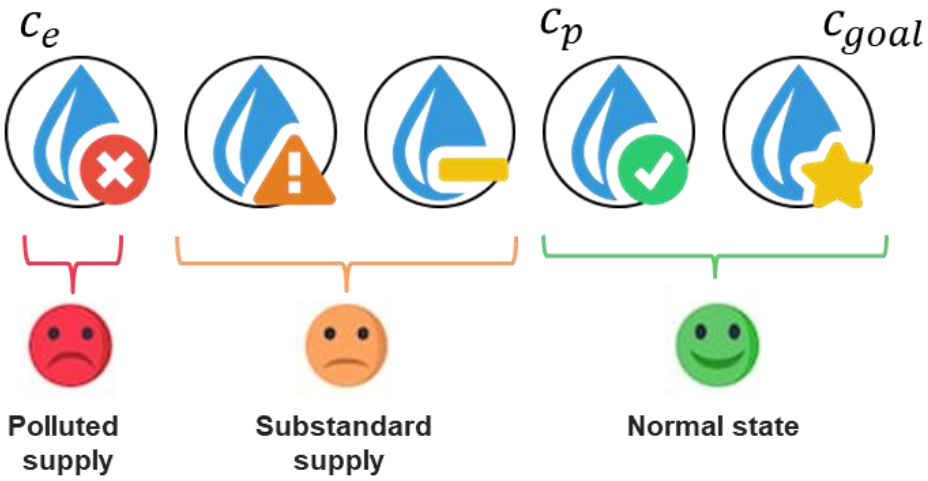


Figure 82: Visual representation of service level thresholds for quality related failures

Since different chemical or microbial substances can be simulated in stress testing process, so must, based on their "criticality", different minimum levels be applied for the evaluation of results. Specifically, for EU water companies, minimum acceptable levels for drinking water, can be adopted from various legislative documents, such as EU DIRECTIVE 98/83/EC for drinking water. Only standard compliant supply is acceptable. But a (minimum) 2 level approach can also be applied for the evaluation of quality related consequences. Assuming the team can determine a value that is considered excessive, an extremely hazardous environment in the system can be detected, thus a state of emergency. In the presence of such extreme conditions in the system, potential life losses from the consumption of polluted water could occur. Although such concentrations are difficult to occur, since attempting to evaluate the system under various scenarios, a low probability- high impact deliberate attack should be accordingly identified and mapped! Such a concentration, for a given substance, can be considered as "excessive", causing toxicity of the supplied water. Polluted supply, can be related to the Lethal Concentration of the substance, since at this level potential life losses could occur due to high toxicity. Since it is a sensitive level of failure in risk assessment and emergency planning, lower values could be used, such as LC_{50}, which is the concentration of a substance for which 50% of the population that consumed it is expected to die.

The second level of failure would be more related in a "discomfort" or "displeasure" of customers, little or no possibility for minor illness but not life-threatening. This failure state is certainly less critical than life-threatening concentrations, but still affects customers' well-being. It can be more related to a "reputational" impact of an incident, since it can also refer to an effect to the "aesthetics" of the product and create the sense of "unsafe water" due to e.g. taste or odour. Certainly, the objective of the water company is determined in higher standards than this, and higher than "usually acceptable" values of concentrations in the delivered water. Such a state of failure that refers to substandard supply can be found for concentrations below the value previously defined as excessive and higher than a concentration considered permissible (c_p). The later threshold can be the upper acceptable

concentration of a substance as found in drinking water regulations or company's defined concentration. The values of permissible and excessive concentrations for the various substances are adjustable, as different legislation or standards may apply to each supplier. Regardless of those service levels though, the company should always take into account the severity of potential health impacts from either short (usual case for microbial load) or long term (common for most chemical substances) exposure of the customers. Permissible concentration c_P can never exceed the calculated concentration at which none of the population is expected to die (LC_0) or the Maximum Contaminant Level Goal ($MCLG$) for which there is no known or expected risk to customers health (PL 93-523; SDWA, 1974), while excessive concentration c_f is usually the threshold at which many regulations demand supply interruption or use restriction! In conclusion to this approach, the previous limits define the water supplied as a) fit and b) safe for consumption.

By determining, for a given substance, the 2 levels of concentration "Permissible" (c_P) and "Excessive" (c_f), a set of metrics to assess the performance of the system in respect to quality and safety of supply can be determined. We denote the potentially lethal concentration with subscript f and exceedance of "permissible" concentration with subscript p.

The above categorization of failure levels is intended to reveal, in a structured way, secondary effects of a threat that are deemed less critical. By creating an intermediate level of failure between complete failure and normal operation, the users can also detect marginal situations of the failing system. The number of intermediate levels can also increase, in order to better describe the company's risk attitude and quantify consequences for multiple service levels before complete failure.

5.1.3 System Consequences dimensions

Twisting the idea of ideal performance for a WDN, that is a continuous supply of sufficient quantity and quality of water to customers in the entire network, we can see the dimensions on which integrity of service, and failure thereof, should be built upon. Categorizing and separating service failure in terms of quantity and quality was the scope of the previous step. For each service, the dimension of KPIs are defined, providing answers to the consequence and risk related questions of:

- how much?
- where?
- how many?
- for how long?

Each service of the system is based on a physical aspect, either quantity (volume) or quality (concentration), and so must consequences for each. Answering the first question of "how much", users seek information in a dimension relative to the operation of the system.

According to BS EN 15975-2:2013 for security of drinking water supply, sufficient pressure is a parameter that also define integrity of supply. Simulation models, stimulated by threat scenarios, react based on a set of predefined rules and adjust assets' behaviour accordingly.

Such a behaviour change can also be seen in the use of Pressure Driven Analysis in quantity related threats. As low-pressure conditions are met in the system, the model adjusts flow and reduces supply to the nodes, via the selected pressure-driven formulation. This direct coupling of pressure and supply in the stress testing models allows us to reduce dimensions of consequences by one, simplifying the overview without losing information.

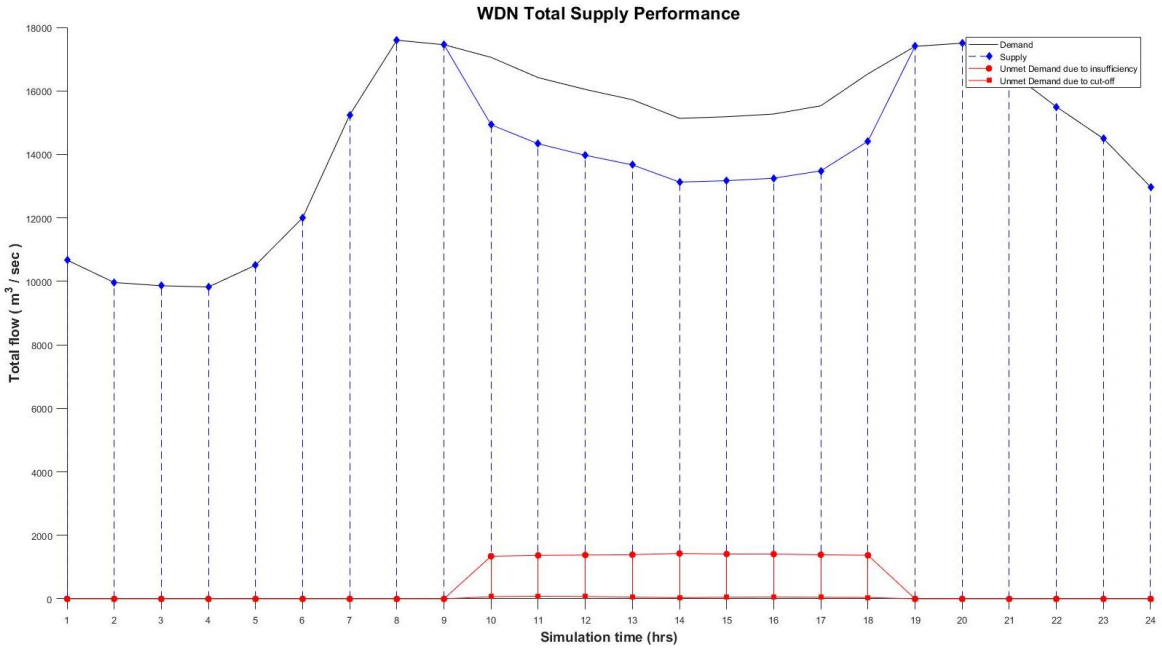


Figure 83: Example of physical dimension failure timeseries for a WDN under CP stress

Providing the physical meaning of service consequences, the flow of water is selected. This dimension is used to provide a clear reference to the aim of the network's services in a familiar manner (known terminology, values, units etc.). Providing a familiar and sector established dimension to quantify failure ensures better comprehension of the results but also allow better information sharing and communication on the examined threat scenario results. In quantity related simulations, physical dimension of failure is demonstrated through the unmet demand, which is the difference of demand (optimal state) and the actual supply (stress test results). In quality related simulations, the physical dimension of failure is the supply of water with concentration (stress test results) above allowable operating limits (optimal state).

As simulation is based on a system network model, the above physical dimension is actually located in parts of it. In order to understand the extent of the service failure over the network, the spatial dimension of failure must be explored. In the simulation model, supply points or districts (group of points) are represented by demand nodes.

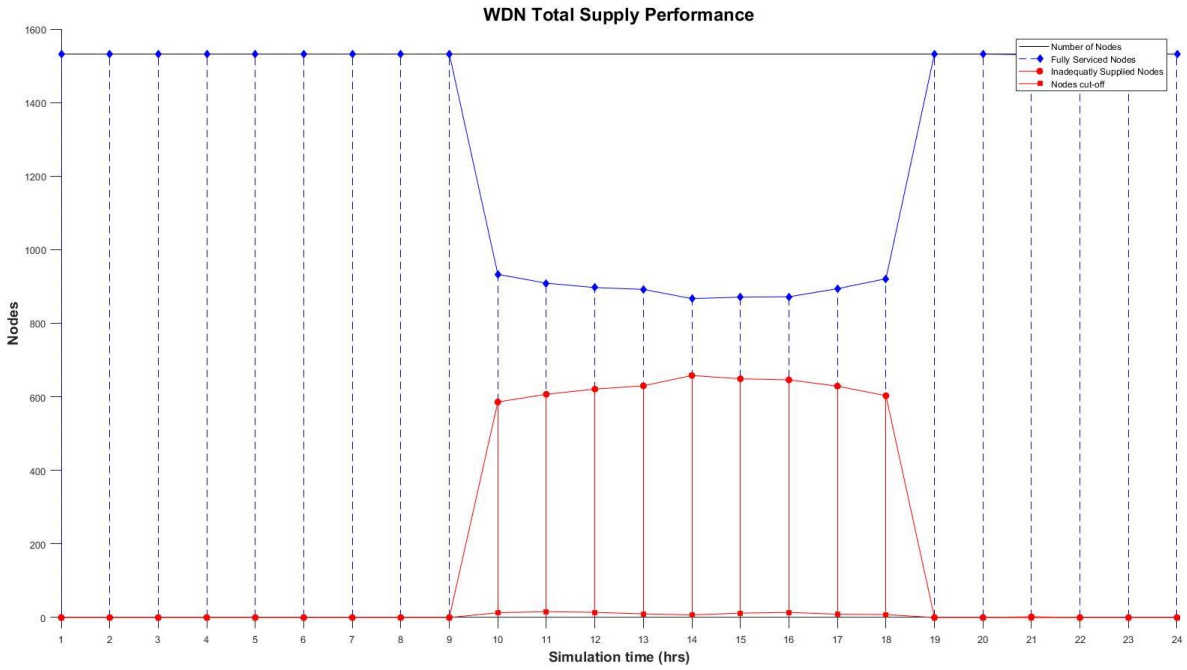


Figure 84: Example of spatial dimension failure timeseries for a WDN under CP stress

Those nodes can represent a single property supply point (high resolution network) or a supplied district like a number of blocks (skeletonized network). Regardless of the degree of skeletonization, spatial extent of failure is related to the connectivity and dynamics of the system. Spatial dimension of failure is an important characteristic, as the company needs to know if the threat under examination cascades through the network or is isolated on a part of the network, and estimate the loss in service coverage. This is highly related to the examination of potential risk reduction measures, as the company through this information can decide to explore metrics designed to isolate failure and decrease its propagating dynamics or making an informed decision of retaining risk.

But the water supply service is a service towards customers, i.e. people. A WDN model, such as the ones created in EPANET, can simulate an area with a demand node, but no 2 nodes are the same. Area density can vary significantly, thus, spatial dimension is one side of the coin. It is only normal that the spatial difference of population density is considered crucial when assessing impact. Also, a real city, thus a real WDN, is an ever-moving system, dynamic in its internal flows, with people working, living or entertaining in different areas within the city web. The WDN, with its fixed nodes must change accordingly. This temporal change in a node is seen via demand curves in models. Spatial-temporal distribution of customers in the model directly affects multiple hydraulic characteristics, e.g. tank available storage, refill, pump speed etc. This dynamic value, changing over time based on the demand curve, will assist assessing impacts during different critical hours e.g. peak demand hours (more people affected) and night hours (less people affected). In order to assess the system's

integrity in that dynamic, a third dimension linked to the number of customers affected is used. Based on the demand value of each node in the system, assuming a common average value of per capita consumption, (200 l/day, average European consumption) a raw estimate for customers can be exported, i.e. people, affected in each node of the network at each time t of the simulation. This allows to assume (if no other validated information exists) each i node will serve:

$$C_{i,t} = \frac{Demand_{i,t}}{per\ capita\ consumption}$$

Note that the above equation includes the time varying demand for each node ($Demand_{i,t}$), thus it accounts for the spatial-temporal distribution and dynamics of the system.

A water CI network must be assessed in regards to another critical characteristic as well, that of duration of failure. Time dimension is crucial in the risk management process as it, indirectly, defines a level of criticality in terms of exposure to consequences. Duration of failure is important since e.g. assuming a fictional network topology having N nodes affected for 1 hour is no comparison to the same "spatial" impact that lasts 4, 8 or 12 hours. This information can also be used as a guide to select risk reduction measures that allow the system to maintain service longer, or recover faster from a critical service failure, complete failure duration can be proven very important while evaluating measures, since minimizing 0-supply or polluted supply duration significantly increases quality of service.

5.1.4 Metrics families and impact characteristics

While consequences can be manifested in different dimensions, there are inner characteristics that define the profile of each failure. Reversing the generic system performance after an attack, found in Figure 21, the failure curve can be exported. The shape of the produced curve strongly resembles the shape of a flood hydrograph.

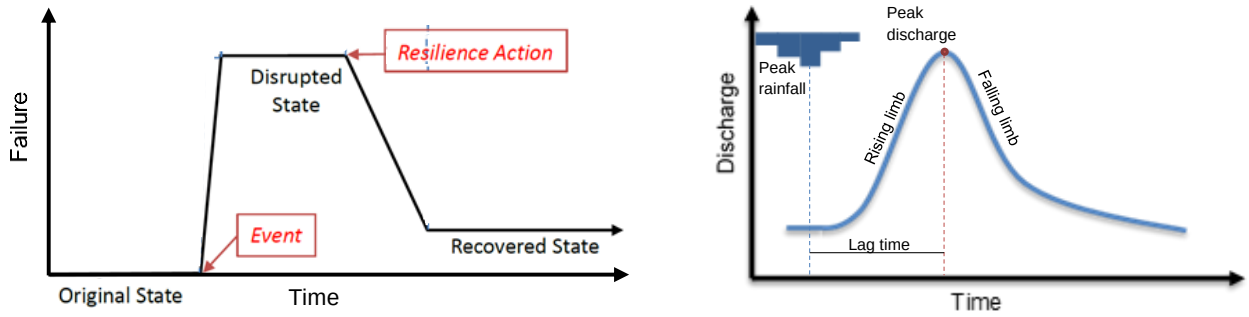


Figure 85: Generic failure curve after an attack event and flood hydrograph after a rain event

Creating an analogy between rain event and CP attack as causes of an incident, key information that are found in a flood hydrograph can be translated to detect key characteristics of a system failure under CP attack. The rising limb represents the beginning of WDN failure from original state to the disrupted. While the falling limb is representing the

system recovering, the new base flow of the hydrograph on the right side of the curve is equal to the recovered state of the system, as it is possible to have a new state before reaching optimum performance.

While assessing a flood event, one of the first key characteristics is that of total runoff volume. In a sense, the total volume of runoff is the magnitude of the flood, a characteristic that is directly linked to the rain event itself and the ability of the catchment area to absorb part of the precipitation. The area under the flood curve is the total runoff volume for the flood. Bringing that characteristic to our approach, the magnitude of failure is the total effect it has on each dimension. In terms of supply, the magnitude of failure is the total volume of unmet demand or substandard supply, which is the area under the curve. In terms of nodes and customers, magnitude of failure is the total number of nodes and customers that experienced the failure throughout the total duration of service failure. This is the sum of hours for which even 1 demand node of the system experiences service failure. Magnitude of failure can also be represented as a percentage of optimal state, where the total volume of supply is delivered at high quality (total volume of demand), to all the demand nodes (total number of demand nodes), satisfying all customers (total number of customers) with no interruption (total simulation hours). In this family of metrics, we see fit to add a water sector used failure metric that of customer minutes lost (CML). It is the sum of customers experiencing 0-supply conditions, times the duration of that failure in minutes. But since we explore multiple levels of service failure levels, a new variation of that metric should be added as well. Since the intermediate level in quantity related simulation is the partial inadequacy of supply, related more on the fulfilment of customers' need we propose the Reputational Customer Minutes Lost (RCML) which refers to the number of customers and duration of that level.

Another characteristic of the timeseries is the average propagation profile. How a flood is propagating through time, can be seen in the average discharge among other. The average image of the propagation profile can be a valuable first image, knowing of course that the average value is not the accurate representation of truth but only a part of it. Bringing the propagation dynamics in the failure of a WDN, the average profile for each dimension can be estimated as an absolute number. Since the propagation profile is averaged against time for the 3 dimensions of flow, nodes and customers, we propose the exploration of average duration against a dynamically varying value of the model, that of customers. Average duration of failure per customer is able to demonstrate the experience an affected customer in the network would have. In fact, this family of metrics, is designed to create a narrative of such nature, referring to a representative picture of an average system experience. Since average numbers can be misleading, for the purposes of the STOP-IT KPIs the arithmetic non-zero mean of the consequences is used. This is the mean values of the timeseries profiles only for the duration of failure (at each service level) excluding zero-values. Estimating the mean in failure duration instead of the total duration of the system, prevents dependency of the metrics on the simulation duration.

But magnitude and average propagation are not uniquely defining an event. For example, in the case of two flood events, the total runoff volume and average propagation can be similar,

but the actual events and their severity can be very different. Such an analogy can be found in the next figure.

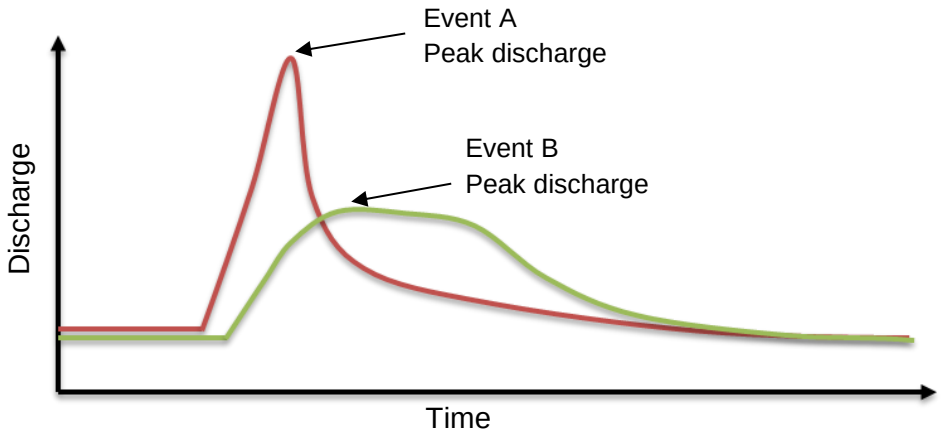


Figure 86: Representation of flood hydrographs with similar runoff volume and average flow

It is obvious from the two events that the difference is found on the peak discharge. It is a well-established and widely used characteristic of floods that represents the severity. Severity of a system failure is also a key characteristic that is highly valuable in creating a consequence profile of a threat. As peak temporal effect of an event can have a severe impact, even for a short period, it can also be used to compare scenarios, against the climax of events. In addition to comparing threat scenarios, this metric is crucial for assessing risk mitigating measures, to indicate their ability to blunt the peak effect. For example, peak spatial extent of service failure is extremely relevant to measures aiming to contain the expansion of the impact over the network, such as local boosters, or back-up pump activation plan and activation of isolation valves for quality issues. Those measure can create a ceiling on the failure propagation, thus reducing peak effect. Measures can also be targeting the mitigation of specific level of service, as peak temporal failure of supply interruption or pollution can be viewed as more critically severe by companies. The KPIs are designed to provide the necessary information behind consequences to allow for better informed risk decisions.

In Figure 86, event A is an event that escalates quickly reaching its peak discharge and dropping rapidly as well. This type of flood events is known as flash floods. Event B has a “steadier” state of discharge after peak is reached, meaning that values near peak are maintained throughout the event. Both types can damage an area, either due to inability to quickly respond to peak impact or retain discharges near peak for a long duration. The key characteristic that separates those is the load factor. Load factor is a parameter used in planning and assessing a system design. The effect of a lower peak temporal effect can be amplified due to its sudden occurrence, creating a larger gap between the average propagation and the extreme state. This is why the peak-to-average ratio (PAR) family of metrics is introduced in STOP-IT KPIs. Those metrics are quantitative but unitless, demonstrating the scale factor of peak and how extreme is the peak effect in respect to the average propagating profile. PAR metrics are magnitude-independent and larger values imply spike-like failure, while as PAR is getting closer to 1 the failure is approaching a steady-

state profile. This information can be used to evaluate a risk reduction measure in respect to the effect on the consequence profile type (in reference to the event profiles of Figure 86).

So far, consequences are evaluated in respect to 2 service categories (quantity & quality) in 4 dimensions (supply, customers, spatial and temporal) for 4 key characteristics (magnitude, propagation, severity & load factor). This process is applied in both service levels (complete & partial failure) recognizing the consequence profiles in each separately, as one service level is more related to reputational damage than the other. Considering complete service failure as more critical than the intermediate service, a comparison between the consequences found must be provided. This weighing between service level is allowing the measurement of criticality of consequence. The prevailing failure ratio (PF) family of metrics is the weighing between critical and moderate consequences previously calculated, allowing the users to see if and which dimension is presenting more critical behaviour and guide risk and treatment evaluation.

One of the most important aspect though, after recognizing the key characteristics and creating the consequences profile for a threat scenario, is the identification of key critical states and the available time from the start of the threat event. Defining critical reaction thresholds (could be more than 1) and recognizing available reaction time for each is important in emergency response plans. As the final step, and perhaps the most important, in strategic and tactical planning against CP attacks, key times and expected consequences define the emergency call and also allows companies to re-evaluate their emergency plans against a previously unexplored threat scenario and the available times. Company's resources allocation, mobilization of units and communication protocols are based on available time and criticality of state. Such states in STOP-IT KPI Framework are defined for the 3 dimensions of supply, nodes and customers and all service levels. Critical states are again company defined, adjusting to any risk attitude or available resources and action plans. Those can be the loss of performance in percentage for the dimensions of supply and nodes, as physical and spatial dimensions can, and usually are, viewed as part of a total. This does not apply to the customers dimensions though. In STOP-IT KPIs Framework, critical states in customers' dimension are expressed only in absolute numbers, as It would be unacceptable to consider evaluation of critical time of e.g. polluted supply against a percentage of people. Critical state can refer to a specific service level as well, since different resources or response plans can be selected to address them. This creates the Time from Event to Critical state (TEC) metrics for the dimensions mentioned before. This set-up provides the answer to the question "How much time after the attack is available before X number of customers or 2.5% of the network experiences supply interruption?". By calculating available time before a number of customers experiences supply inadequacy (reputational failure level), the company can also get a rough estimate of the expected complains. It is obvious that the thresholds defined can and should be different between quantity and quality threat scenarios, but also based on the examined chemical or biological species simulated. Other than the company defined critical levels, STOP-IT KPIs include the calculation of the available time to respond from the start of the event until peak temporal effect is reached, similarly to the lag-time of a flood, identifying the available timeslot in which measures and

operational actions that aim to blunt the peak effect are to be applied. Time from Event to Peak (TEP) metrics are similarly applied to dimensions and service levels. The last key time metric family is the Time from Event to Restoration (TER), representing the equivalent falling limb of failure, estimating time from the end of attack to the system restoration. This time metric may not be addressing measure implementation related times but it can be used to evaluate the performance of a metric implementation in assisting the systems bounce-back back ability by reducing time until restoration is achieved. All of the above reflect the key survival time of the system after an attack has occurred.

The above analysed KPI families are the stress-test simulation profilers, working also as a series of filters for the consequence exploration providing key information on how much service is lost, at what extent, affecting how many customers and for how long.

5.1.5 STOP-IT KPIs

Following the structure presented in the previous chapters, the list of STOP-IT KPIs is presented in ANNEX C. The first categorization is in respect to services, creating a separate section for quantity and quality KPIs. To each of those sections, KPIs for all dimensions are presented based on the families of metrics, i.e. magnitude, propagation, peak, PAR, PF, TEC, TEP and TER, dimensions and service level, as analysed.

5.2 KPI tool

The KPI tool is a MATLAB®-based standalone executable designed to assist in the evaluation process of a threat scenario within the WP4 tactical and strategic planning of water sector CIs against CP attacks. The aim of the tool is not to export any ranking or final decision on criticality of a threat, but rather present a user-friendly environment to deploy the STOP-IT KPI Framework in a structured way. The main concept behind the KPI tool is a sequential application of user-defined selections as filters to visually present only selected parts of consequence information. The adjustability of the KPIs to the company's risk attitude is the main pillar of the tool development, while additional functionalities were added to assist the risk informed decisions for the threat scenarios examined. This was a necessary additional development in order to make better use of the KPI structure for the RAET users. As a whole, KPI tool enhances the single scenario assessment, presented in previous chapters. It allows users to select scenario results and a number of configurations of the system to create a deeper analysis of the stress test simulation results and identify key information for the tactical and strategic planning.

In the following paragraphs, the methodology, components and user manual of the latest version of the tool are presented.

5.2.1 Methodology and functionalities

The KPI tool is oriented towards the actual implementation of the STOP-IT KPI Framework in multiple aspects. As such, the core methodology of the framework is implemented as part of the tool's overall process, presented here and is constructed on 3 pillars.

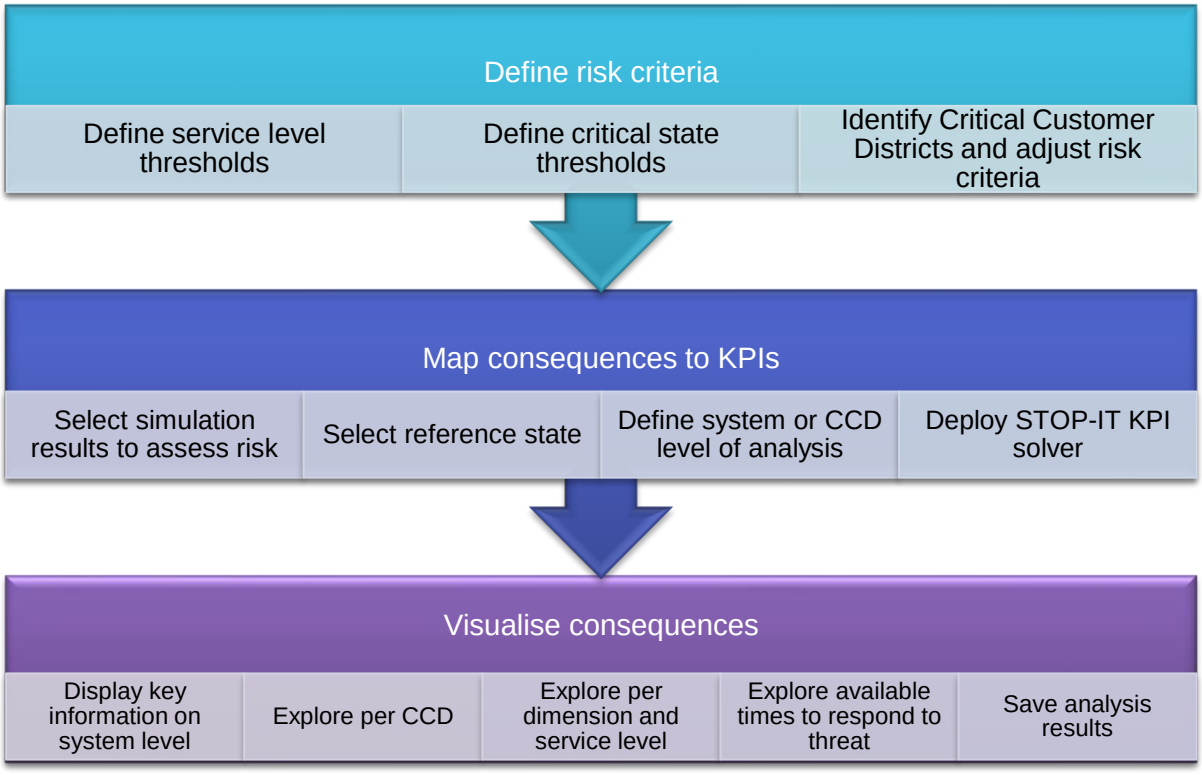


Figure 87: KPI tool methodology in process overview

The first pillar is what ISO 31000 recognizes as “defining risk criteria” for a company. Risk criteria are a set of terms against which the significance of risk is evaluated. As part of this process, risk criteria in respect to the KPI framework are the threshold values that define the service levels (complete and partial inadequacy of service) for each service type. Each WDN operates under different internal and external context, serving customers with different needs and expectations. Such a diverse perspective in the system operation should be captured. Besides service thresholds, as described before, STOP-IT KPIs are adjustable to the company’s risk attitude as well. A set of terms to evaluate significance of risk is obviously the critical state thresholds. Defining the loss of supply, the spatial extend or the number of customers above which, the company recognizes a critical state of operation and seeks to allocate resources, design and deploy measures and identify the time window is obviously setting a value of significance. But those are not the only terms against significance of risk should be evaluated in a network. In order to link a model’s results to reality for the purposes of risk assessment, the actual significance of several parts of the network must be recognized. Those are described previously as critical customers and may refer to:

- Hospitals,
- Schools,
- Government buildings,
- Military buildings,
- Industry,

- Fire hydrants,

as well as, any other infrastructure/asset found critical by experts. Critical customers are expected to be served with “higher” expectations, thus higher levels of service. For example, an area with hospitals or government facilities, due to their importance to societal functions, are expected to have higher service levels, while critical state is expected to be much more sensitive than other areas. In that spirit, the KPI tool perceives critical customers as an additional set of terms for risk significance. Since such information is not included in any hydraulic model, since hydraulic operations are not directly defined by the type of customer but are simple seen as a demand node to be served. For this reason, KPI tool is designed with a functionality that allows users to select critical customers in the network and create what was defined as Critical Customer Districts (CCD) to assess risk in those areas. Demonstrating the selected network topology, in a dedicated window, the user creates a polygon to define the CCD and sets the threshold and critical state variables to represent the risk attitude for the specified district. The district must include at least 1 demand node. In the latest case, is a direct assessment of the critical customer as a unit. For each CCD the threshold parameters are defined, adjusting the risk assessment process for the district. Multiple CCDs can cover the network or only part of it, according to the user’s selection. All of the above process defines risk criteria of the company, and since are not threat specific, are to be used multiple times. In addition, a company can have multiple CCD configurations, not because it refers to specific critical customers, but because it can include future city topologies (construction of a new hospital) or the creation of a CCD for a densely populated area, or the city centre because of an international event. Note that a CCD can be part of or overlap with other CCDs, enabling users to select an area of interest and then explore risk assessment information in lower CCD scale. Regardless of the background for the CCD creation, the configuration may not be edited at a later stage for integrity reasons. Assessing a risk against tempered risk criteria can create a faulty risk evaluation and skip or propose an unnecessary measure.

The second pillar of the KPI tool is the actual solver for the KPI calculation based on the user’s selections and the above analysed framework. In order to calculate KPIs, a reference file and the result file must be defined. For quantity related simulations, reference file is the normal state of the system, under no attack, while for quality simulations, reference file should contain acceptable levels of concentration. This need for reference files has been foreseen in RAET process, where the user can create a no attack scenario and export normal state reference results and a .csv file in addition to the results for quality simulations. The later .csv formatted file that is provided for each simulation, includes the concentration thresholds for each of the chemical species in the simulation. Those files, in combination to the user defined parameters. For each service type service levels and thresholds are used based on user’s selection. If the user has imported CCDs and selects to evaluate risk per district, the thresholds are imported accordingly in the calculations, for each district. As STOP-IT KPIs are making reference to an optimal situation, in the case of district calculation, the optimal state of the part of the system is found and exported from the reference file. Following this, a set of functions dedicated to the KPI calculation per district and for the system are put to use.

The third pillar of the tool is the visualisation of selected KPIs for the user. The main concept and value behind the KPI tool, besides calculating the metrics, is a metric exploration in a user defined way. Continuing with a user-controlled process, the profile picture of the risk must be presented in an efficient way, while filters for the exploration can lead to a conclusion. The visualisation process follows the sequential exploration for families of metrics for the system or districts. The first step in the series of filtering information, is to present the overall key consequences for the system, setting the scene on which a second level exploration per district is performed, possibly guiding the user to undertake the next step of assessment for a specific selection of the used CCDs. In assessing the risk, the first question to be answered is “what is the magnitude of failure?” in the multiple dimensions of service in the system. Regardless if the CCD KPI estimation is selected or not, the first picture of risk must be reference to the entire system, as this is the highest available level. For the entire system, absolute values of magnitude KPIs, with their corresponding units, are presenting the consequences size, while the percentage form, in respect to optimal service provide a sense of scale, for the gap of service to be covered. Knowing the magnitude of the failure, the peak temporal effect and overall propagation of the failure must be presented for the entire simulation. Time of occurrence and value are clearly depicted for key dimensions of supply and nodes, while the cumulative behaviour of Customer Minutes (a metric widely used in supply companies to measure failure) allowing the user to see if peak effects are occurring simultaneously, amplifying the significance of consequences. In customers dimension, it is important to also see the spatial-temporal effect of the complete service inadequacy on the network, thus the first part of visualisation is complete with a spatial image of duration of failure weighted per customer (to take into account temporal density of each area). Exploring the same set for each critical customer allows the user to compare consequences characteristics in multiple dimension per district, and guide the next step of exploration perhaps to a specific CCD. Now the user has seen the system consequences and has selected the critical customers that need to be further explored. After this first filtering process and for the selected CCD, the user explores peak effect in the multiple dimensions and service levels defined in the calculation process. At this stage, the user can either explore all dimension and service levels, or decide (based on experience and the previous visualisation step) to focus attention on a specific service level or dimension. This can be done for multiple CCDs, so for example user can explore the spatial extent of service interruption in CCD A that includes e.g. the city centre and for CCD B that e.g. includes hospitals and government facilities, the user explores the peak effect in terms of polluted supply. This allows information exploration to adjust to user’s decision and provide the requested class of information. In this view, the peak temporal effect is demonstrated as value and percentage, while in respect to the start of the simulated threat, the TEP metrics are presented, giving information of available time in respect to the selected dimension and service level explored. After this, the third part of visualisation follows. With the user having understood the main characteristics of failure, the areas of effect and how this is reflected to critical customers, it is time to also explore the critical states defined in risk criteria and, if those are reached, the available time to act. It is important to allow user to readjust evaluation (return to pillar 1 processes) at any time and create or import a new set of CCD or/and risk criteria and explore the selected

scenario consequences under the new set-up. The final step of the tool methodology and process is to save the produced KPI metrics under the latest risk criteria configuration.

5.2.2 User manual

In the following paragraph, the tool's user manual is presented, following a step-by-step process of running the tool and applying the tools methodology while also demonstrating additional functionalities. Note that this manual refers to the latest version of the tool, as demonstrated in the latest local CoP in Berlin (STOP-IT WP4,5,6,7-meeting on IT security, May 15th 2019). Additional developments are expected by the end of the project, based on the feedback of future demonstration activities, and are expected to be documented accordingly in WP7.

Installing KPI tool

Install the KPI tool by deploying the app installer executable, proceed with default path of installation and select folder for the MATLAB Runtime (tool dependency) installation. The tool is designed for Windows OS, and the minimum hardware requirement (known at this point) is an 8GB RAM.

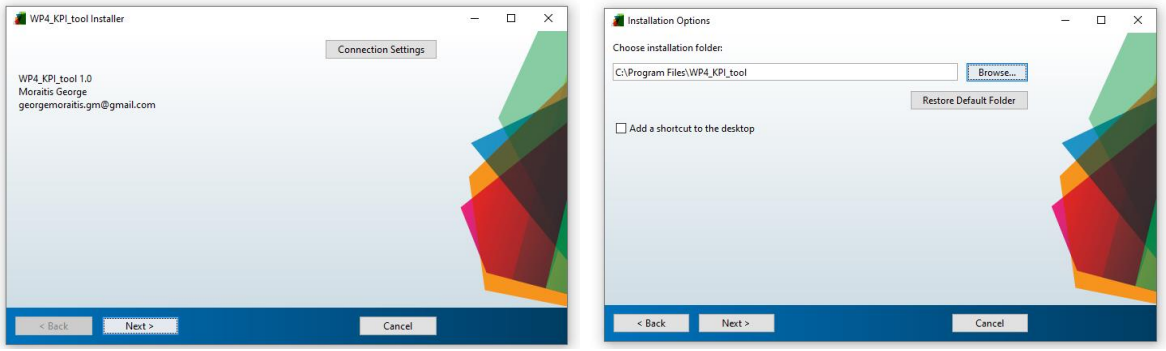


Figure 88: Installation executable windows

After the installation is finished, run the tool.

KPI tool user manual

In the next figure, the main window of the KPI tool is presented. It contains the plot of the latest network topology used (field 1), the paths to the latest reference (field 2) and results (field 3) files used. The user can select to explore the current topology though pan and zoom options available (button 4). In the topology plot (field 1), tanks are illustrated as magenta circles and reservoirs as blue rectangles. This is to assist the user and visually separate the assets related to the system storage. On top of each node, the unique ID label is assigned as found in the EPANET

The user can select to import a different reference (button 5) and scenario results (button 6) file, and navigate through a file explorer to find the desired files. In case the above scenario

refers to a different topology, the user can import the correct ".inp" from the file explorer that appears after pressing button (button 7).

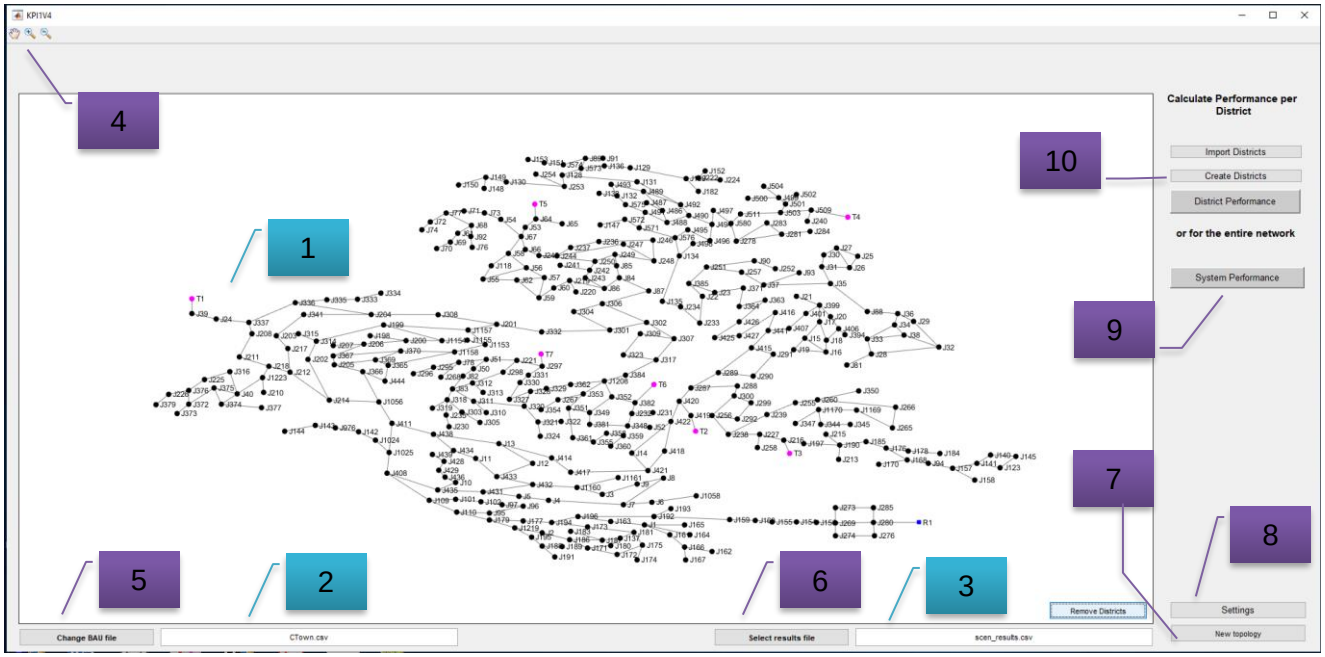


Figure 89: KPI tool main window and first user actions in setting the evaluation configuration

After having selected the scenario configuration to be assessed, the user must set the risk criteria. The risk criteria for the system can be found in Settings (button 8).

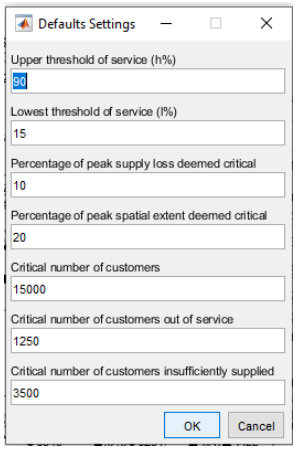


Figure 90: Risk criteria settings window for the system level

After altering in the appropriate manner, the values of risk criteria found in the window and pressing "OK", the new default risk criteria parameters for the system are applied and saved.

After this, the user can select to run the KPI tool for assessment at system level (button 9).

In order to evaluate risk in respect to critical customers, the user can create a new set of Critical Customer Districts (CCDs) (button 10). After this, a new component, dedicated to the creation of CCDs is deployed. Field and button numbers in this manual are reset for the purposes of the new component.

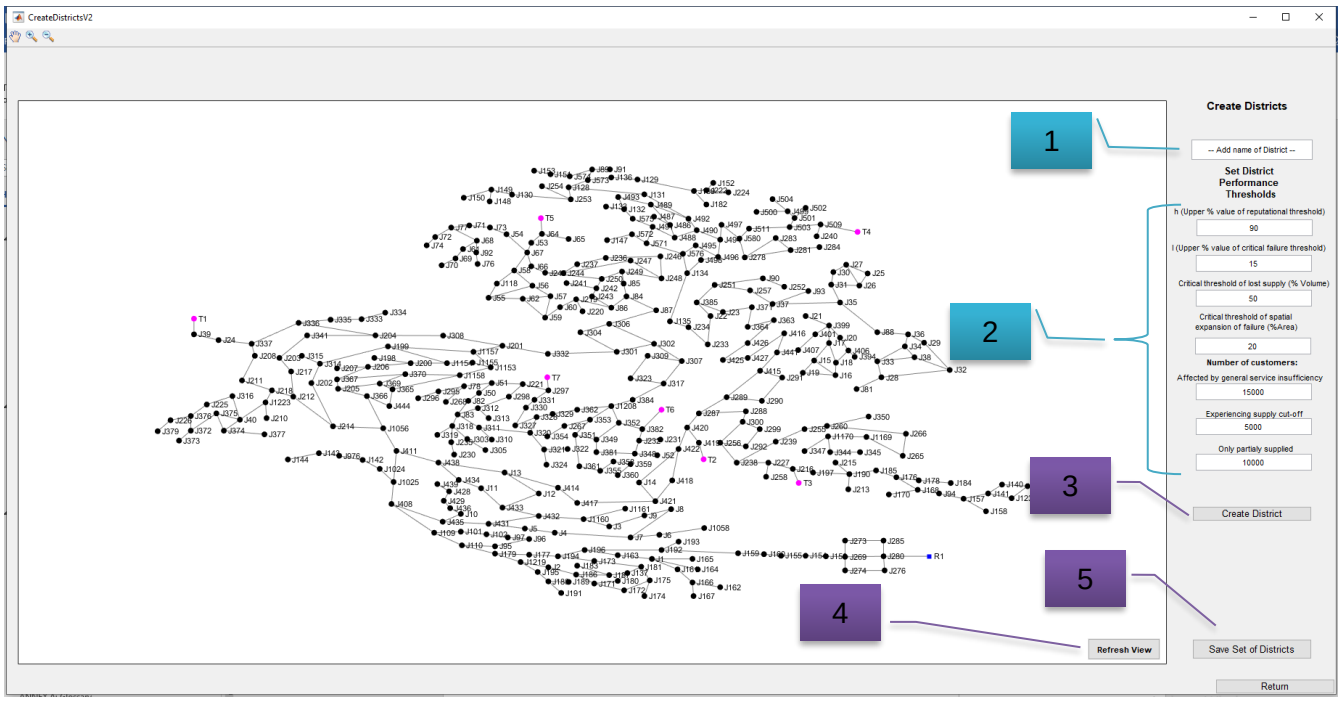


Figure 91: Critical Customer District constructor window

The CCD constructor component uses the same topology, as the one found in the main window. In order to create a CCD, the user has to first define the name of the CCD (field 1). Since this is used in naming parameters and files, the CCD name must contain no special characters, including space. After inserting the unique ID of the CCD, the user can edit the default threshold values and adjust it to represent the company's risk attitude in respect to the specific CCD (fields 2). Having set the parameters for the CCD creation, the user must define the spatial coverage of the area. In order to create the CCD boarders, user must press button 3 and the CCD polygon constructor is deployed.

The user creates the polygon that encloses the CCD as shown in Figure 92, by joining the last edge with the starting point. Note that the starting point is used to assign the ID ladel of the CCD. The polygon is not finalised yet, and is dragable while the user can select to relocate edges to include or exclude parts of the network. This extra functionality was found very useful in correcting edge point locations without the need to start the process from scratch.

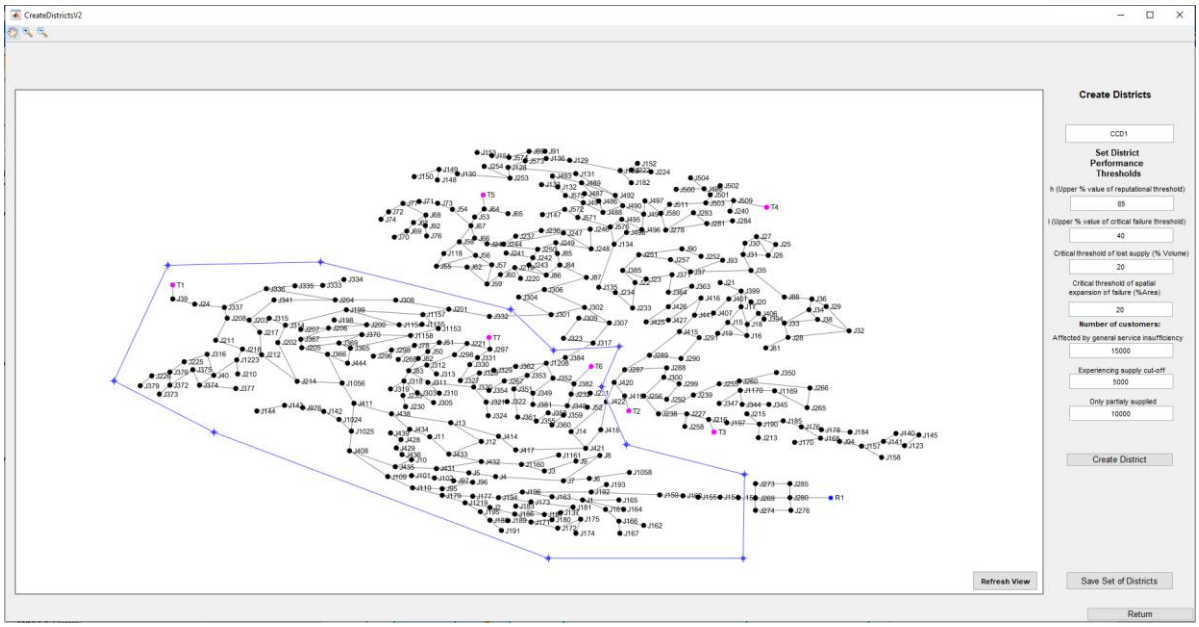


Figure 92: Polygon constructed to enclose user defined CCD

Additional functionalities on the polygon creation can be seen in Figure 93. Customizing the colour of the CCD can be useful in creating an easy to detect set of CCDs, allowing users to have a colour-based overview of the selected area and can be later used for reporting.

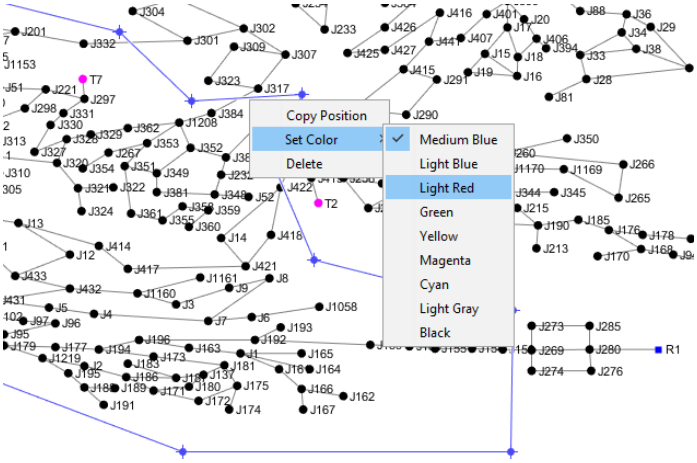


Figure 93: Additional functionalities on CCD creation and colour customization

After customizing, relocating or reshaping the CCD, the user can again check the corresponding parameters and readjust them to the latest selections. In order to verify the creation of the CCD and the corresponding risk criteria the user double clicks on the polygon. The CCD is registered to a temporary file, and the ID field 1, is refreshed and the process is ready to be repeated in order to create the full set of CCDs. Note that the colour customization can be done even after the creation of the CCDs and is applied simply by clicking the “refresh view” button 4. Having finalized the CCD creation, the user selects to save the configuration

(button 5). A save file window appears and is used to set the name and location of the configuration. Note that the CCD configuration is non editable by the tool after it is exported.

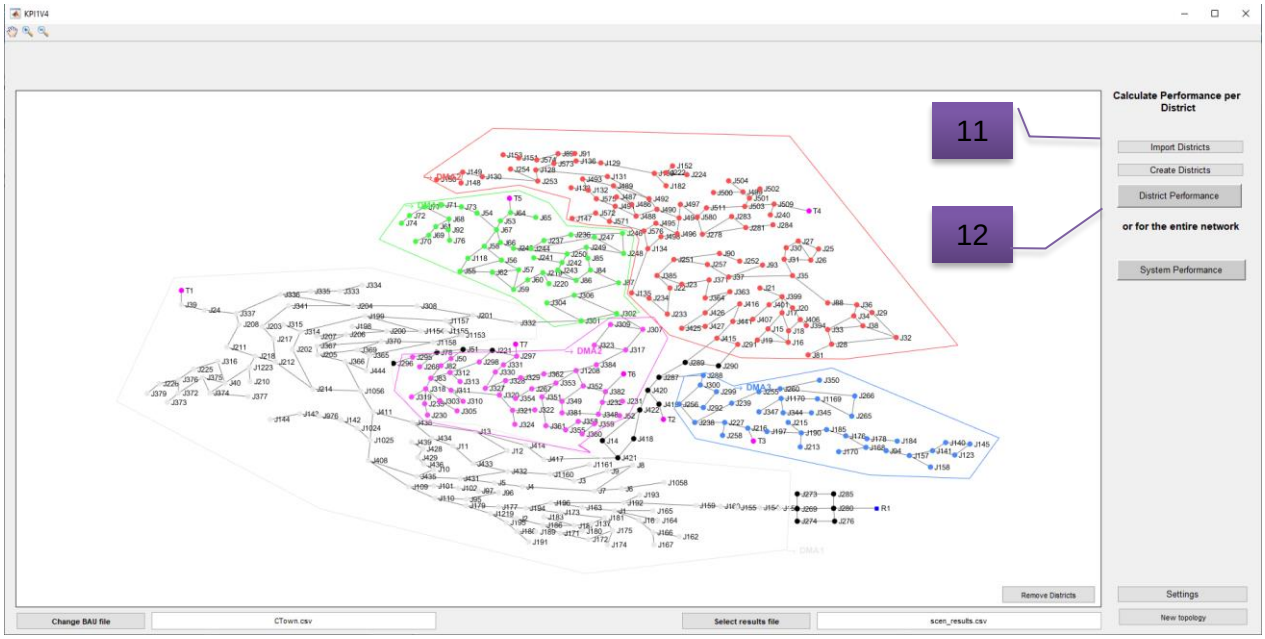


Figure 94: KPI tool main window with a CCD set added

After returning to the main window of the tool, the latest CCD created is loaded by default as seen in the above figure. Component data are linked, requiring less user actions for some operations, creating a more user-friendly experience. Note that the saved configuration can be later sent to any other tool users, in order to be used. The receiver can simply choose the “import District” button 11. Any other previously created or shared CCD configuration can be selected and loaded via this way.

For the selected CCD configuration, the user has imported, the tool is ready to deploy the STOP-IT KPI solver for a CCD analysis (button 12).

For both System (button 9) and CCD (button 12) analysis, the back-end operation of the tool automatically recognizes if the results file is a quality or quantity related simulation and invokes the necessary algorithm of the solver. During the KPI solver running, no interface is available, but a progress bar displays the performed actions running on the back. After the solver processes are complete, data are imported to the visualisation component of the tool.

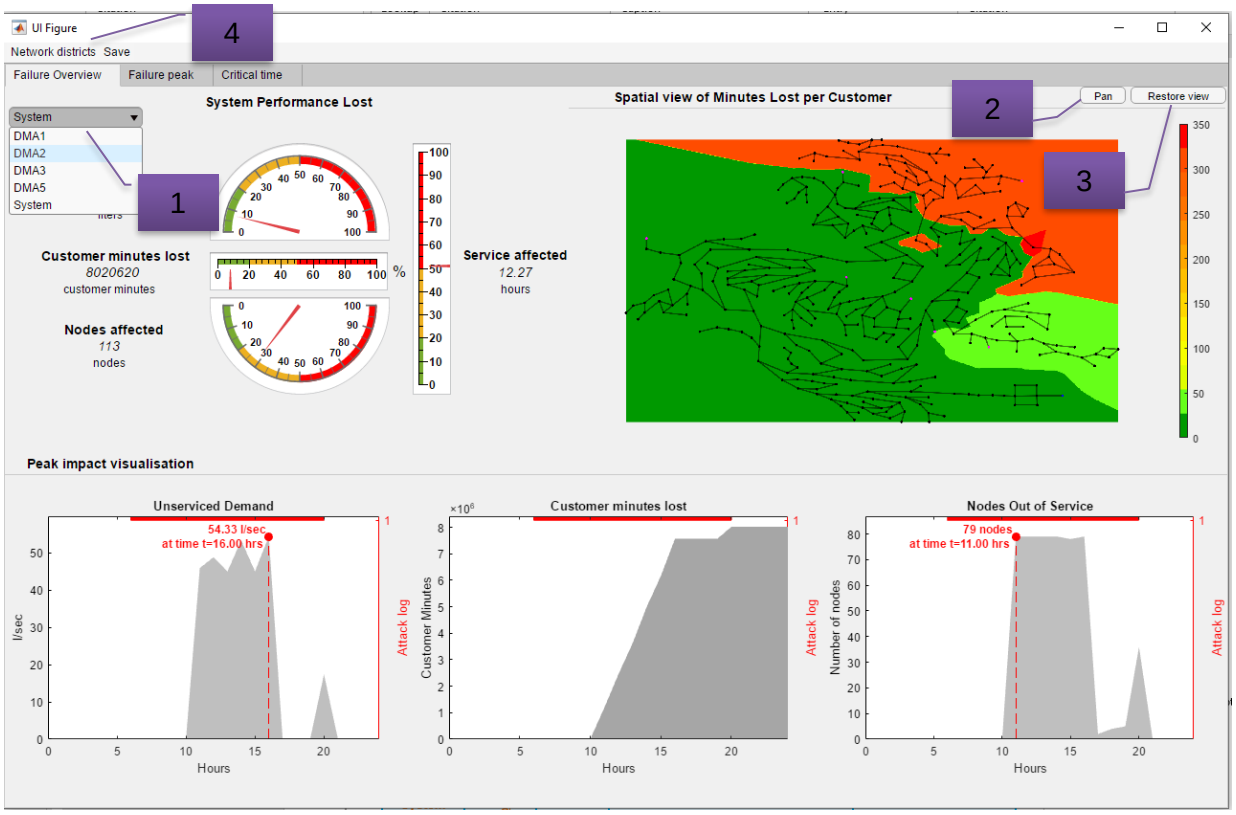


Figure 95: Consequence visualisation component main window

In the main window of visualisation component, the user can see the information described in previous chapters, at system or CCD level (dropdown 1). The charts are explorable, allowing zoom (by default) or pan (button 2). For a more friendly use of this tab, KPI tool includes a “restore view” button (button 3) to restore all charts and the spatial figure to their default display.

Since real network topologies can be composed of numerous CCDs, the tool was enhanced with an additional functionality. Through menu button 4, the user can select the “remind district” option and a pop-up window with the CCD set used will appear. The window includes interactive functionalities and besides the purposes of a reminder window, it can also be used to export the CCD set in relation to the network to be used in reports (image or pdf format).

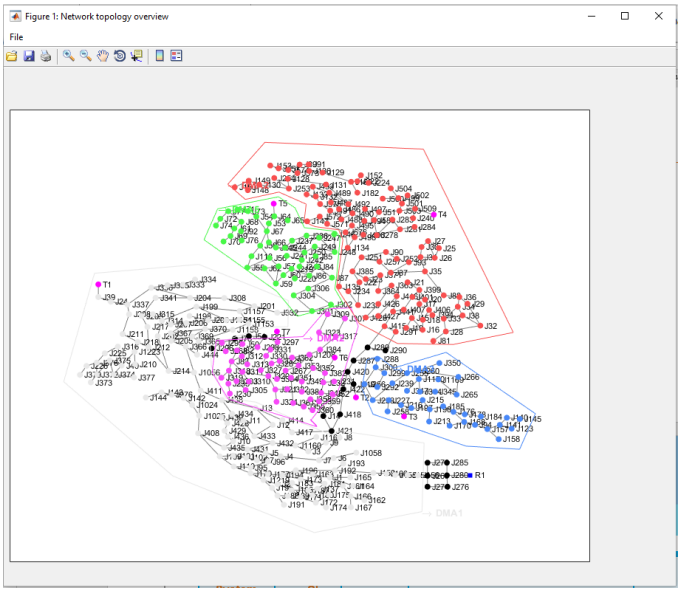


Figure 96: Pop-up CCD reminder window of KPI tool with example CCD set

The second tab of the visualisation component window can be seen in Figure 97. In this window the user selects the spatial level of assessment from the dropdown menu (dropdown 1). The district selection is intentionally treated separately in each tab of the tool, as the user might wish to explore different characteristics for different districts simultaneously.

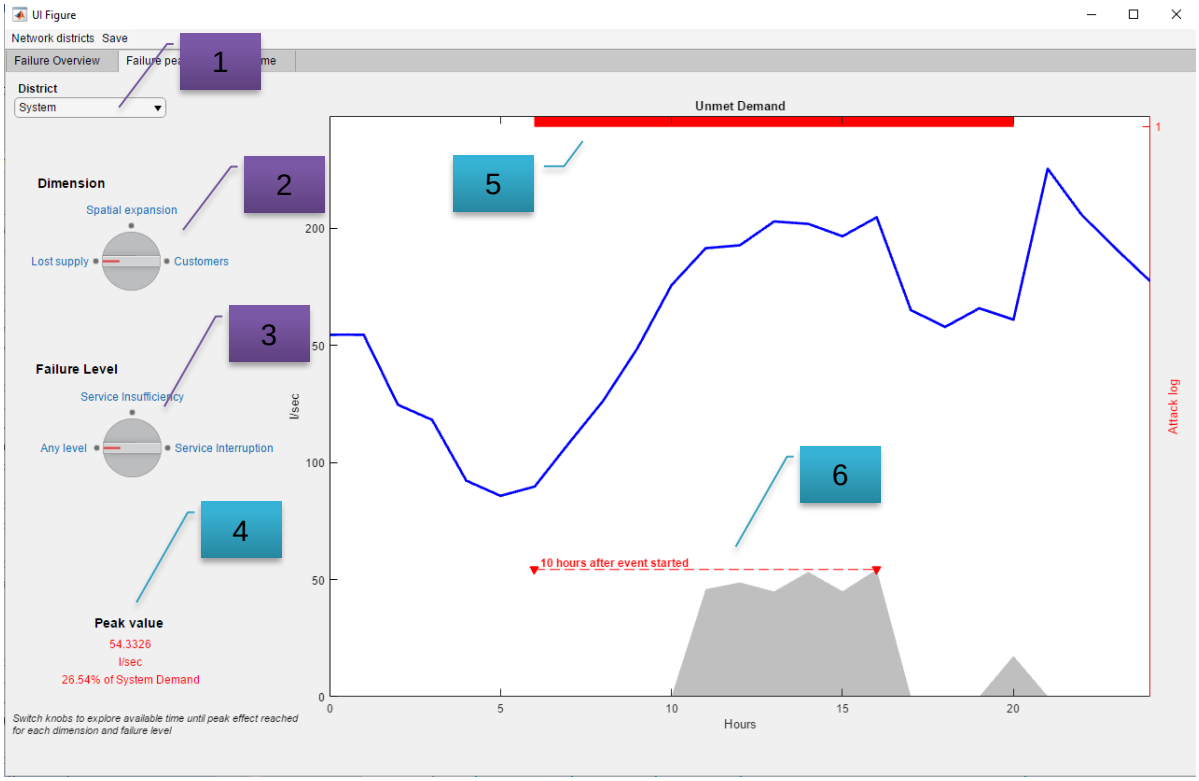


Figure 97: Peak impact tab in visualisation component window

Using knob 2, the user switches and selects the dimension of consequences and with knob 3 the service level for that dimension. This allows an easy and structured navigation over 9 system consequence severity profile. In field 4, text dynamically adjusts to represent the absolute value, the corresponding units and the percentage of reference. In the figure area, the user can see the attack log (attack start and duration) (field 5) and the available time, from event start to peak effect (TEP) in a dashed line (field 6).

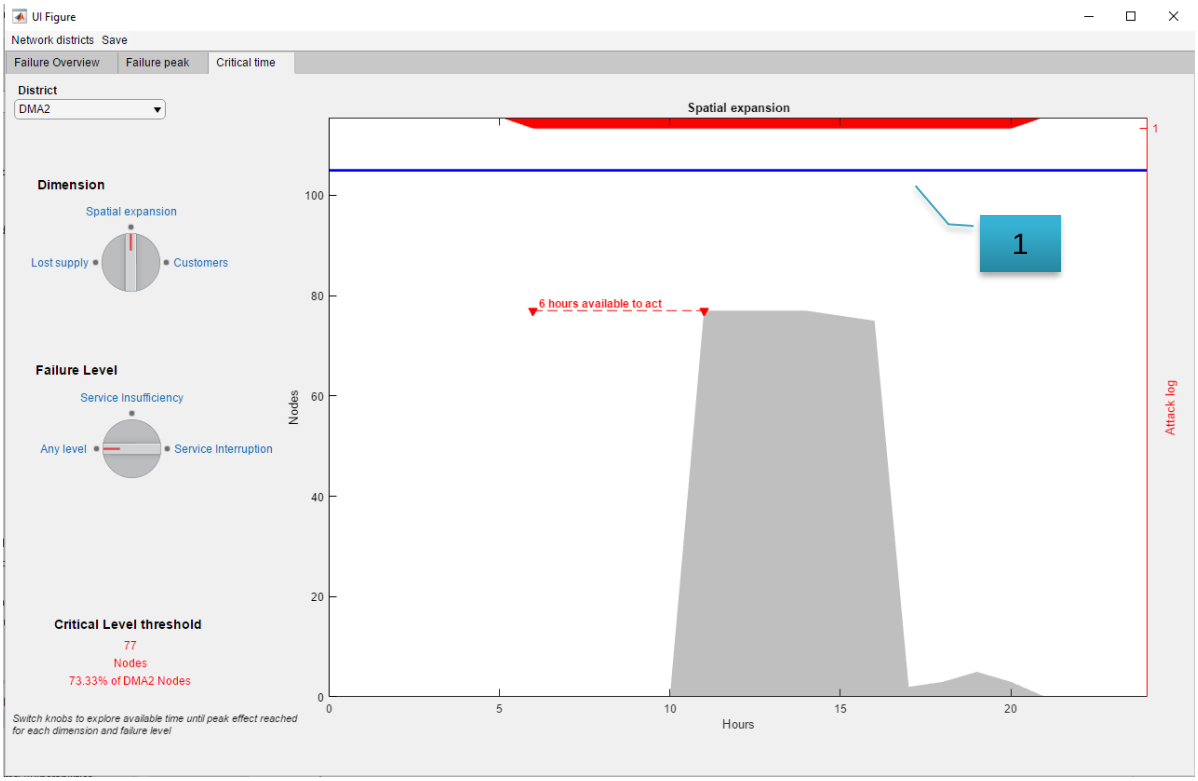


Figure 98: Critical state tab in visualisation component window

As seen in Figure 98, the critical state tab of the visualisation component can be utilised using the same logic as before. Note that reference value for each dimension (line 1), is also adjusting to the user's selection, demonstrating the reference value for the district selected. Accordingly, the supporting dynamic text, also "reminds" the district selection made, in order to avoid faults.

In the case of quality stress testing results assessment, an additional drop-down menu is presented (see in each tab of the visualisation component that allows the user to select the chemical species as an additional variable. Multispecies stress testing analysis information must be maintained for the user to explore.

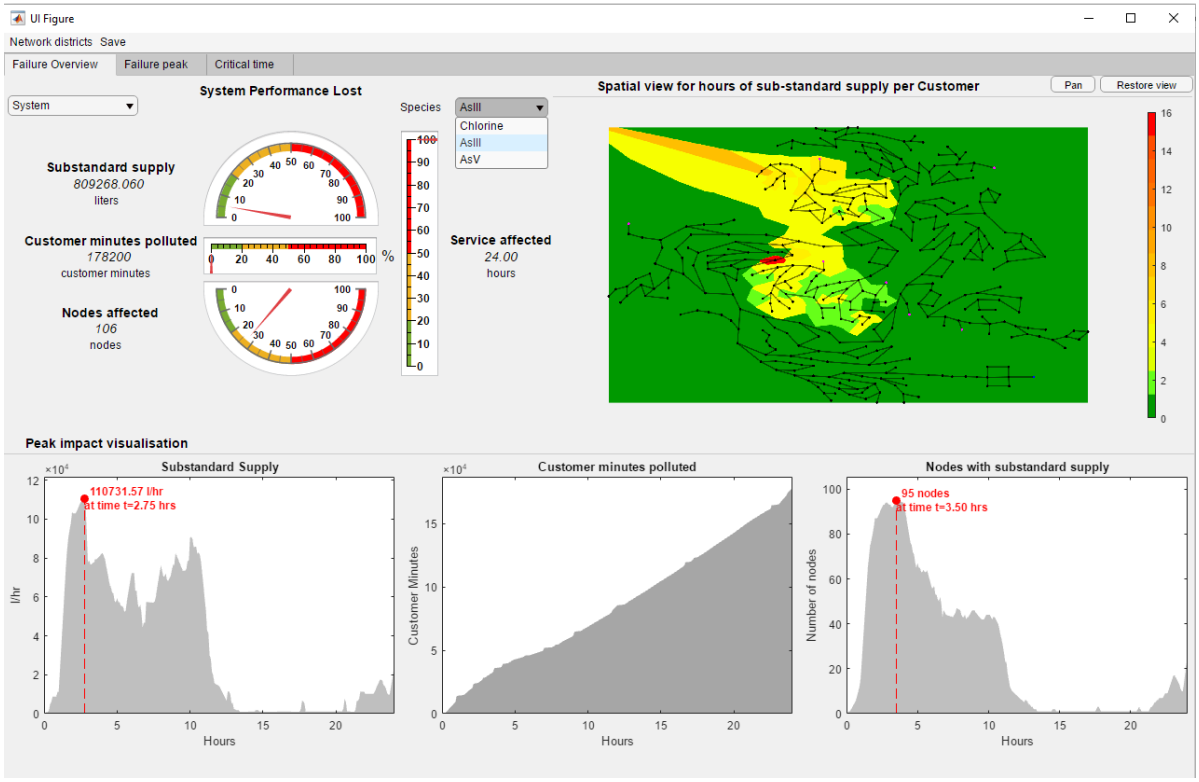


Figure 99: Main window of visualisation component for quality consequences assessment

As the methodology of the tool is not a one-way process, the tool is designed to serve some direct "previous step" functionalities. Those are (a) the selection of different CCD configuration that already exists (import CCD to the scenario) or (b) Create a new set of CCD to be used.

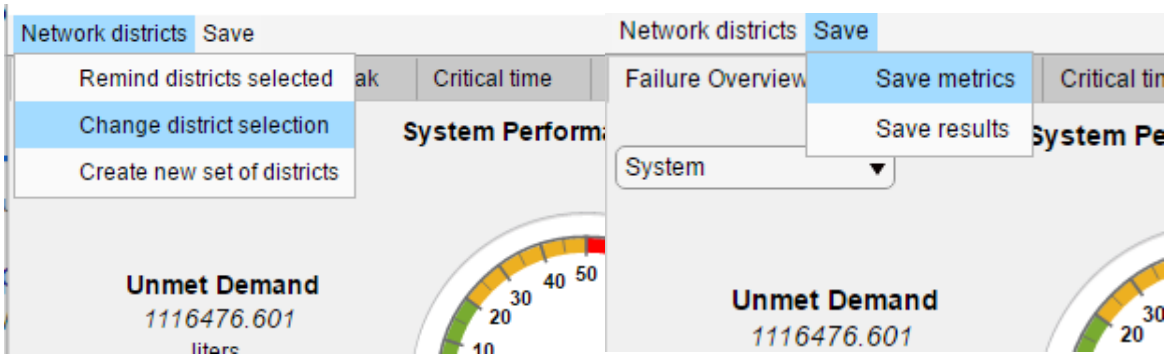


Figure 100: Menu options in the visualisation component

Adjusting the CCD configuration or creating a new set can be very useful to the user since, a specific scenario might need to be further investigated under a different spatial perspective.

After the user has decided on the risk criteria (including the CCDs) and has explored the consequences profile, the option of saving the produced metrics can be selected. This option

automatically detects the results file used and stores the produced metrics (from the KPI solver) in the same folder. This is done to create a consistent data storing structure, with simulation results and corresponding KPIs stored in the same folder, avoiding misplacement and serious errors in the risk and treatment evaluation process. In addition, the user can save the “results” of the KPI tool analysis that also include the selected risk assessment configuration, risk criteria and file paths. All of the above are functionalities that aim to increase integrity and reduce errors in the strategic and tactical planning against the CP threats examined.

The design and performance of the tool were tested in both demo and real network simulation, with various configurations, including large simulation duration and fine timestep. This manual refers to the latest version of the tool, as demonstrated in the latest L-CoP in Berlin.

Conclusions

Risk Analysis and Evaluation Toolkit (RAET) is a collection of various tools that aid in the identification, analysis and evaluation of cyber-physical threats to the water systems. RAET is aligned with and applies the STOP-IT Risk Assessment and Treatment Framework (WP4) i.e. Module I of STOP-IT. The developed framework is compatible with ISO 31000:2009, hence, certifies acceptance and interoperability of the STOP-IT framework with existing risk management procedures in the water sector without posing any constraints on whether the users/utilities are aligned to the abovementioned standard. The methodological approach employs three levels of analysis, for an all-hazard risk assessment and treatment of cyber-physical threats in water systems. The levels of analysis are based on the needs or perception of the end user as well as on the data availability. The levels are interoperable, meaning the end user can apply all levels sequentially or select the relevant level(s) for specific purposes. Those level are:

- **1st level, Generic assessment**: Initial overview of a CI, with no specific data of a utility network needed. The user can have a first assessment of risks and vulnerability of the infrastructure and identify potential risk reduction measures based only on what is known for infrastructures of his type and his knowledge about the site. The tools RIDB, FT Editor and Scenario Planner are used in order to create or visualise possible threat scenario and InfraRisk CP is used for Generic risk analysis and risk level estimation. The RRMD (Risk Reduction Measures Database) is utilized (either through the InfraRisk-CP, the SP or accessed independently) to examine an initial set of measures.
- **2nd level, Single scenario assessment**: In this level, after the creation of a threat scenario (using RIDB, SP, FT Editor capabilities) vulnerability is assessed for specific assets (using AVAT tool) and risk assessment is performed by simulations of the utility network (using the Stress Testing Platform (STP)) against identified threats benchmarking performance with the use of KPIs (via the respective KPI tool). Appropriate risk reduction measures from RRMD can be identified and their performance against the given threats can be analysed by KPIs.
- **3rd level, Multiple scenarios simulations**: Expanding the single scenario assessment, this level comprises multiple scenarios with a large number of various threats with different magnitude of consequences, stress-testing the system, by running a series of simulations.

STOP-IT Risk Assessment and Treatment Framework is scalable, adaptable and flexible. Adopter Utilities are able to support strategic/tactical planning, real-time/operational decision making and post-action assessment for the key parts of the water infrastructure, moving towards a resilient, cyber-physical-wise and safe water sector.

References

Alegre, H., 2000. Performance Indicators for Water Supply Services.

Alegre, H., Baptista, J.M., Jr, E.C., Cubillo, F., Duarte, P., Hirner, W., Merkel, W., Parena, R., 2016. Performance Indicators for Water Supply Services.

Almalawi, A., Tari, Z., Khalil, I., Fahad, A., 2013. SCADAVT-A framework for SCADA security testbed based on virtualization technology. Proc. - Conf. Local Comput. Networks, LCN 639–646. https://doi.org/10.1109/LCN.2013.6761301

Amin, S., Litrico, X., Sastry, S., Bayen, A.M., 2013. Cyber security of water scada systems-part I: Analysis and experimentation of stealthy deception attacks. IEEE Trans. Control Syst. Technol. 21, 1963–1970. https://doi.org/10.1109/TCST.2012.2211873

ASME-ITI, 2009. All-hazards risk and resilience: Prioritizing Critical Infrastructures Using the RAMCAP Plus Approach.

AWWA, 2010. Risk and Resilience Management of Water and Wastewater Systems 10.

Ayala, L., 2016. Cybersecurity Lexicon. https://doi.org/10.1007/978-1-4842-2068-9

Baker, G.H., Redwine, S., Blandino, J., 2003. Network Security Risk Assessment Modeling Tools for Critical Infrastructure Assessment. Crit. Infrastruct. Prot. Proj. Work.

Berry, J., Boman, E., Riesen, L.A., 2012. User's Manual TEVA-SPOT Toolkit 2.5.2. U.S. Environmental Protection Agency, Cincinnati.

Borshchev, A., Filippov, A., 2004. From system dynamics and discrete event to practical agent based modeling: reasons, techniques, tools, in: Proceedings of the 22nd International Conference of the System Dynamics Society. Citeseer.

Bouchon, S., Di Mauro, C., Logtmeijer, C., Nordvik, J.-P., Pride, R., Schupp, B., Thornton, M., 2008. Non-binding guidelines for application of the Council Directive on the identification and designation of European critical infrastructure and the assessment of the need to improve their protection. Luxemb. Off. Off. Publ. Eur. Communities, Italy.

Bousquet, F., Barreteau, O., Le Page, C., Mullon, C., Weber, J., 1999. An environmental modelling approach: the use of multi-agent simulations. Adv. Environ. Ecol. Model. 113, 122.

BS EN, 2013. BSI Standards Publication 15975-2 Security of drinking water supply — Guidelines for risk and crisis management Part 2 : Risk management.

BS EN. (2013). BSI Standards Publication 15975-2 Security of drinking water supply — Guidelines for risk and crisis management Part 2 : Risk management.

Burns, A.J., Posey, C., Courtney, J.F., Roberts, T.L., Nanayakkara, P., 2017. Organizational information security as a complex adaptive system: insights from three agent-based models. Inf. Syst. Front. 19, 509–524.

Butler, D., Ward, S., Sweetapple, C., Astaraie-Imani, M., Diao, K., Farmani, R., Fu, G., 2017. Reliable, resilient and sustainable water management: the Safe & SuRe approach. Glob. Challenges 1, 63–77.

Cervin, A., Henriksson, D., Lincoln, B., Eker, J., Arzen, K.E., 2003. How does control timing affect performance? Analysis and simulation of timing using Jitterbug and TrueTime. IEEE Control Syst.

23, 16–30. https://doi.org/10.1109/MCS.2003.1200240

Chapman, M., Tyson, G., McBurney, P., Luck, M., Parsons, S., 2014. Playing hide-and-seek: an abstract game for cyber security, in: Proceedings of the 1st International Workshop on Agents and CyberSecurity. ACM, p. 3.

Chertov, R., Fahmy, S., Shroff, N.B., 2006. Emulation versus simulation: A case study of TCP-targeted denial of service attacks. 2nd Int. Conf. Testbeds Res. Infrastructures Dev. Networks Communities, TRIDENTCOM 2006 2006, 316–325. https://doi.org/10.1109/TRIDNT.2006.1649164

Chmielewski, H., Guidotti, R., McAllister, T., Gardoni, P., 2016. Response of Water Systems under Extreme Events: A Comprehensive Approach to Modeling Water System Resilience, in: World Environmental and Water Resources Congress 2016. American Society of Civil Engineers: Reston, VA, USA, 2016, West Palm Beach, FL, USA, pp. 658–667.

COUNTERACT, 2009. PT4: Generic Guidelines for Conducting Risk Assessment in Public Transit Networks, Final Report 4.

Danilenko, A., Van der Berg, C., Macheve, B., Moffitt, J., 2014. The IBNET Water Supply and Sanitation Blue Book, The World Bank.

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.

East, S., Butts, J., Papa, M., Shenoi, S., 2009. A taxonomy of attacks on the DNP3 protocol. IFIP Adv. Inf. Commun. Technol. 311, 67–81. https://doi.org/10.1007/978-3-642-04798-5_5

EBC, 2017. Learning from International Best Practicies, 2017 WATER & WASTEWATER BENCHMARK.

Eidson, E. D., and Ehlen, M. A. (2005). “NISAC Agent-Based Laboratory for Economics (N-ABLETM): Overview of Agent and Simulation Architectures.” Sandia National Laboratories Technical Report SAND2005-0263, (February).

Eliades, D.G., Kyriakou, M., Vrachimis, S.G., Polycarpou, M.M., 2016. EPANET-MATLAB Toolkit : An Open-Source Software for Interfacing EPANET with MATLAB. 14th Comput. Control Water Ind. Conf. CCWI 2016 1–8. https://doi.org/10.5281/ZENODO.437751

Eom, J., Han, Y.-J., Park, S.-H., Chung, T.-M., 2008. Active cyber attack model for network system’s vulnerability assessment, in: Information Science and Security, 2008. ICISS. International Conference On. IEEE, pp. 153–158.

EURACOM, 2011. D--20.1 Final Publishable Summary 1–23.

Falliere, N., Murchu, L.O., Chien, E., 2011. W32.Stuxnet Dossier. Symantec-Security Response Version 1., 1–69. https://doi.org/20 September 2015

Francis, R., Bekera, B., 2014. A metric and frameworks for resilience analysis of engineered and infrastructure systems. Reliab. Eng. Syst. Saf. 121, 90–103.

Giannopoulos, G., Filippini, R., Schimmer, M., 2012. Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art., European Commission JRC (Joint Research Center) Technical notes. https://doi.org/10.2788/22260

Gillette, J.L., Fisher, R.E., Peerenboom, J.P., Whitfield, R.G., 2002. Analysing water/wastewater

infrastructure interdependencies. Argonne National Lab., IL (US).

Grimm, V., Railsback, S.F., 2013. Individual-based modeling and ecology. Princeton university press.

Hackers Arise!: SCADA Hacking: SCADA/ICS Communication Protocols (Modbus) [WWW Document], 2017. URL https://www.hackers-arise.com/single-post/2017/01/05/SCADA-Hacking-SCADAICS-Communication-Protocols-Modbus (accessed 8.3.18).

Hansson, S. O., and Aven, T. (2014). “Is Risk Analysis Scientific?” Risk Analysis, 34(7), 1173–1183.

Hashimoto, T., Stedinger, J. R., and Loucks, D. P. (1982). “Reliability, resiliency, and vulnerability criteria for water resource system performance evaluation.” Water Resources Research.

Holling, C.S., 1996. Engineering resilience versus ecological resilience. Eng. within Ecol. constraints 31, 32.

ICS-CERT (Industrial Control Systems-Cyber Emergency Response Team) (2016). NCCIC/ICS-CERT year in review: FY 2015. Rep. No. 15-50569. DC: ICS-CERT, Washington.

International Telecommunication Union, 1994. X.200: Data Networks and open system communications.

ISO 31000, 2009. ISO 31000:2009 Risk management - Principles and guidelines. Risk Manag. 31000, 24. https://doi.org/ISBN 978-1-86975-127-2

ISO, 2009. Risk management - Vocabulary. ISO Guid. 732009.

ISO, 2011. ISO 27005:2011 - Information security risk management. Iso 270052011 2011.

ISO/IEC 31010:2009, 2009. Risk Management- Risk Assessment Techniques.

Jaeger, C.D., Roehrig, N.S., Torres, T., 2008. Development of an Automated Security Risk Assessment Methodology Tool for Critical Infrastructures. Sandia National Laboratories.

Jain, P., Tripathi, P., 2013. SCADA security: a review and enhancement for DNP3 based systems. CSI Trans. ICT 1, 301–308. https://doi.org/10.1007/s40012-013-0024-2

John H Cable, J.S.D., 2005. Key Performance Indicators for Federal Facilities Portfolios: Federal Facilities Council Technical Report Number 147.

Kelic, A., Warren, D.E., Phillips, L.R., 2008. Cyber and physical infrastructure interdependencies. Sandia Natl. Lab. Rep.

Klise KA., Hart DB, Moriarty D, Bynum M, Murray R, Burkhardt J, Haxton T (2017). A software framework for assessing the resilience of drinking water systems to disasters with an example earthquake case study. Environmental Modelling and Software 95(1): 420-431. http://doi.org/10.1016/j.envsoft.2017.06.022

Koutiva, I., Makropoulos, C., 2016. Modelling domestic water demand: an agent based approach. Environ. Model. Softw. 79, 35–54.

Langner, R., 2013. To Kill a Centrifuge 1–36.

Makropoulos, C., Nikolopoulos, D., Palmen, L., Kools, S., Segrave, A., Vries, D., Koop, S., van Alphen, H.J., Vonk, E., van Thienen, P., 2018. A resilience assessment method for urban water systems. Urban Water J. 1–13.

McPherson, T.N., Burian, S.J., 2005. The water infrastructure simulation environment (wise) project.

World Water Congr. 2005 Impacts Glob. Clim. Chang. - Proc. 2005 World Water Environ. Resour. Congr. 58-. https://doi.org/doi:10.1061/40792(173)58

Murray, R., Janke, R., Uber, J., 2012. The Threat Ensemble Vulnerability Assessment (TEVA) Program for Drinking Water Distribution System Security 1–7. https://doi.org/10.1093/icb/icy006/4989945

Nai Fovino, I., Masera, M., De Cian, A., 2009. Integrating cyber attacks within fault trees. Reliab. Eng. Syst. Saf. 94, 1394–1402. https://doi.org/10.1016/j.ress.2009.02.020

NIAC. (2009). "Critical Infrastructure Resilience Final Report and Recommendations." 1–43.

Nikolopoulos D., Moraitis G., Bouziotas D., Lykou A., Karavokiros G., Makropoulos C.(2019). 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, 25-29 June 2019

Nilsson, F., Darley, V., 2006. On complex adaptive systems and agent-based modelling for improving decision-making in manufacturing and logistics settings: Experiences from a packaging company. Int. J. Oper. Prod. Manag. 26, 1351–1373.

NIST, 2012. Guide for conducting risk assessments. NIST Spec. Publ. 95. https://doi.org/10.6028/NIST.SP.800-30r1

Nogueira Vilanova, M.R., Filho, P.M., Perrella Balestieri, J.A., 2014. Performance measurement and indicators for water supply management: Review and international cases. Renew. Sustain. Energy Rev. 43, 1–12. https://doi.org/10.1016/j.rser.2014.11.043

Ostefeld, R.M.C.S.H.A., 2011. Hand book of water and wastewater systems protection.

Parmenter, D., 2015. Key Performance Indicators: Developing, Implementing, ans Using Winning KPIs, John Wiley & Sons. https://doi.org/10.1017/CBO9781107415324.004

Pizzol, M., 2015. Life cycle assessment and the resilience of product systems. J. Ind. Ecol. 19, 296–306.

Popova, V., Sharpanskykh, A., 2010. Modeling organizational performance indicators. Inf. Syst. 35, 505–527. https://doi.org/10.1016/j.is.2009.12.001

Queiroz, C., Mahmood, A., Tari, Z., 2011. SCADASimA framework for building SCADA simulations. IEEE Trans. Smart Grid 2, 589–597. https://doi.org/10.1109/TSG.2011.2162432

Railsback, S.F., 2001. Concepts from complex adaptive systems as a framework for individual-based modelling. Ecol. Modell. 139, 47–62.

Ralston, P.A.S., Graham, J.H., Hieb, J.L., 2007. Cyber security risk assessment for SCADA and DCS networks. ISA Trans. 46, 583–594. https://doi.org/10.1016/j.isatra.2007.04.003

Rasekh, A., Hassanzadeh, A., Mulchandani, S., Modi, S., Banks, M.K., 2016. Smart Water Networks and Cyber Security. J. Water Resour. Plan. Manag. 142, 01816004. https://doi.org/10.1061/(ASCE)WR.1943-5452.0000646

Rossman, L. a, 2000. EPANET Programmer's Toolkit 1–74.

Samsa, M.E., Kuiken, J. Van, Jusko, M.J., 2008. Critical infrastructure protection decision support system decision model: overview and quick-start user's guide. Decision and Information Sciences Division, Argonne National Lab.

Schnaubelt, C.M., Larson, E. V., Boye, M.E., 2014. Vulnerability Assessment Method Pocket Guide: a tool for center of gravity analysis, RAND Arroyo Center.

Shang, F., J. G. Uber, AND L. Rossman. EPANET Multi-Species Extension Software and User's Manual. U.S. Environmental Protection Agency, Washington, DC, EPA/600/C-10/002, 2008.

Shin, S., Lee, S., Judi, D., Parvania, M., Goharian, E., McPherson, T., and Burian, S. (2018). "A Systematic Review of Quantitative Resilience Measures for Water Infrastructure Systems." Water, 10(2), 164.

Siaterlis, C., Genge, B., Hohenadel, M., 2013. EPIC: A testbed for scientifically rigorous cyber-physical security experimentation. IEEE Trans. Emerg. Top. Comput. 1, 319–330. https://doi.org/10.1109/TETC.2013.2287188

Silberschatz, A., Galvin, P.B., Gagne, G., 2005. Operating Systeme Concepts. Wiley 32, 575. https://doi.org/10.1016/0950-5849(90)90158-N

Stergiopoulos, G., Vasilellis, E., Lykou, G., Kotzanikolaou, P., Gritzalis, D., Security, I., Protection, C.I., Ave, P., St, D., 2016. Critical Infrastructure Protection Tools: Classification and Comparison Critical Infrastructure Protection Tools :

Tang Junjie, Zhao Jianjun, Ding Jianwan, Chen Liping, Xie Gang, Gu Bin, Yang Mengfei, 2012. Cyber-physical systems modeling method based on Modelica. 2012 IEEE Sixth Int. Conf. Softw. Secur. Reliab. Companion 188–191. https://doi.org/10.1109/SERE-C.2012.49

Taormina, R., Galelli, S., Douglas, H.C., Tippenhauer, N.O., Salomons, E., Ostfeld, A., 2018. Modeling Cyber-Physical Attacks on Water Networks with epanetCPA Overview of epanetCPA toolbox.

Taormina, R., Galelli, S., Tippenhauer, N.O., Salomons, E., Ostfeld, A., 2017. Characterizing Cyber-Physical Attacks on Water Distribution Systems. J. Water Resour. Plan. Manag. 143, 04017009. https://doi.org/10.1061/(ASCE)WR.1943-5452.0000749

Taormina, R., Galelli, S., Tippenhauer, N.O., Salomons, E., Ostfeld, A., 2016. Simulation of cyber-physical attacks on water distribution systems with EPANET. Cryptol. Inf. Secur. Ser. 14, 123–130. https://doi.org/10.3233/978-1-61499-617-0-123

Tesfatsion, L., 2003. Agent-based computational economics: modeling economies as complex adaptive systems. Inf. Sci. (Ny). 149, 262–268.

Todini, E. (2000). Looped water distribution networks design using a resilience index based heuristic approach. Urban Water, 2(2), 115-122.

Utne, IB., Hokstad, P., Kjølle, G., Vatn, J., Tøndel, IA., Bertelsen, D., Fridheim, H. Røstum, J. Risk and Vulnerability Analysis of Critical Infrastructures - The DECRIS Approach. Presented at the SAMRISK conference in Oslo, SINTEF, September 2008.

Valis, D., Koucky, M., 2009. Selected Overview. Tech. Univ. Lib. 19–32.

Van Dam, K.H., Nikolic, I., Lukszo, Z., 2012. Agent-based modelling of socio-technical systems. Springer Science & Business Media.

Wikipedia, T. F. E. (n.d.). "SCADA." <https://en.wikipedia.org/wiki/SCADA> (Apr. 6, 2019).

Wooldridge, M., 1999. Intelligent agents. InWeiss G. editor Multiagent systems: A modern approach to Distributed Artificial Intelligence. MIT Press.

Yusta, J.M., Correa, G.J., Lacal-Arántegui, R., 2011. Methodologies and applications for critical

infrastructure protection: State-of-the-art. Energy Policy 39, 6100–6119. https://doi.org/10.1016/j.enpol.2011.07.010

Zhu, B., Joseph, A., Sastry, S., 2011. A taxonomy of cyber attacks on SCADA systems. Proc. - 2011 IEEE Int. Conf. Internet Things Cyber, Phys. Soc. Comput. iThings/CPSCom 2011. https://doi.org/10.1109/iThings/CPSCom.2011.34

ANNEX A: Glossary

Risk Management terms

Asset: Any tangible or intangible thing or characteristic that has value to an organization.

Communication and consultation: Continual and iterative processes that an organization conducts to provide, share or obtain information, and to engage in dialogue with stakeholders regarding the management of risk**.** The information can relate to the existence, nature, form, likelihood, significance, evaluation, acceptability and treatment of the management of risk.

Consequences: Outcome of an event affecting objectives.

Control: Any administrative, managerial, technical, or legal method that can be used to modify or manage risk.

Criticality: The relative importance of the asset to the production and service continuity of the organization.

Effect: Positive and/or negative deviation from the expected.

Establishing the context: Defining the external and internal parameters to be taken into account when managing risk, and setting the scope and risk criteria for the risk management policy.

Event: Occurrence or change of a particular set of circumstances.

Exposure: Extent to which an organization is subject to an event.

External context: External environment in which the organization seeks to achieve its objectives. External context can include:

- The cultural, social, political, legal, regulatory, financial, ecological, economic, natural and competitive environment, whether international, national, regional or local;
- Key drivers and trends having impact on the objectives of the organization; and
- Relationships with, and perceptions and values of external stakeholders

Frequency: Measure of likelihood of an event expressed as a number of events or outcomes per defined unit of time.

Hazard: Source of potential harm.

Internal context: Internal environment in which the organization seeks to achieve its objectives. Internal context can include:

- Governance, organizational structure, roles and accountabilities;

- Policies, objectives, and the strategies that are in place to achieve them;
- The capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
- Information systems, information flows and decision-making processes (both formal and informal);
- Relationships with, and perceptions and values of internal stakeholders;
- The organization's culture;

Level of risk: Magnitude of a risk expressed in terms of the combination of consequences and their likelihood.

Likelihood: Chance of something happening.

Monitoring: Continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected.

Residual risk: Risk remaining after risk treatment.

Residual Risk: Risk remaining after risk treatment.

Resilience: Adaptive capacity of an organization in a complex and changing environment.

Review: Activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives.

Risk acceptance: Informed decision to take a particular risk**.** Risk acceptance can occur without risk treatment or during the process of risk treatment. Accepted risks are subject to monitoring and review.

Risk aggregation: Combination of a number of risks into one risk to develop a more complete understanding of the overall risk.

Risk analysis: Process to comprehend the nature of risk and to determine the level of risk.

Risk appetite: Amount and type of risk that an organization is willing to pursue or retain.

Risk assessment: The overall process of risk identification, risk analysis and risk evaluation.

Risk attitude: Organization’s approach to assess and eventually pursue, retain, take or turn away from risk.

Risk aversion: Attitude to turn away from risk.

Risk avoidance: Informed decision not to be involved in, or to withdraw from, an activity in order not to be exposed to a particular risk.

Risk criteria: Terms of reference against which the significance of a risk is evaluated.

Risk description: Structured statement of risk usually containing four elements: sources, events, causes and consequences.

Risk evaluation: Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.

Risk financing: Form of risk treatment involving contingent arrangements for the provision of funds to meet or modify the financial consequences should they occur.

Risk identification: The process of finding, recognizing and describing risks.

Risk management framework: Set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization.

Risk management plan: Scheme within the risk management framework specifying the approach, the management components and resources to be applied to the management of risk.

Risk management policy: Statement of the overall intentions and direction of an organization related to risk management.

Risk management process: Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk.

Risk management: Coordinated activities to direct and control an organization with regard to risk.

Risk matrix: Tool for ranking and displaying risks by defining ranges for consequence and likelihood.

Risk owner: Person or entity with the accountability and authority to manage a risk.

Risk perception: stakeholder's view on a risk.

Risk Profile: Description of any set of risks.

Risk Register: Record of information about identified risks. The term “risk log” is sometimes used instead of “risk register”.

Risk Reporting: Form of communication intended to inform particular internal or external stakeholders by providing information regarding the current state of risk and its management.

Risk retention: Acceptance of the potential benefit of gain, or burden of loss, from a particular risk.

Risk source: Element which alone or in combination has the intrinsic potential to give rise to risk.

Risk tolerance: Organization's or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives. Risk tolerance can be influenced by legal or regulatory requirements.

Risk treatment: Process to modify risk. Risk treatment can involve:

- Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk.
- Taking or increasing risk in order to pursue an opportunity.
- Removing the risk source.
- Changing the likelihood.
- Changing the consequence.
- Sharing the risk with another party or parties [including contracts and risk financing].
- Retaining the risk by informed decision.

Risk: Effect of uncertainty on objectives.

Stakeholder: Person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity.

Threat: Any potential event that could harm an organization or system.

Uncertainty: State, even partial, of deficiency of information related to or understanding or knowledge of an event, its consequences or likelihood.

Vulnerability: Intrinsic properties of an asset or control that create susceptibility to a source of risk and could potentially be exploited by one or more threats.

Cyber-Physical attacks terms

Account harvesting attack: The process of collecting all the user account names on a computer network. Often used to refer to computer spammers, individuals who try to sell or seduce others through e-mail advertising or solicitation. Account harvesting involves using computer programs to search areas on the Internet in order to gather lists of e-mail addresses from a number of sources, including chat rooms, domain names, instant message users, message boards, newsgroups, online directories for web pages, web pages, and other online destinations.

ACK piggybacking attack: Is an active form of wiretapping when a hacker sends an ACK inside another packet to the same destination. ACK signal is used in some protocols as a signal of data receipt, sent from the receiving station. After the source gets the ACK signal, it transmits the next block of data.

Active cyber-attack: An intentional cyber-attack perpetrated that attempts to alter a SCADA (supervisory control and data acquisition) system, its resources, its data, or its operations.

Active attack: An attack on the authentication protocol where the attacker transmits data to the claimant, credential service provider, verifier, or relying party. Examples of active attacks include man-in-the-middle, impersonation, and session hijacking.

Address space probe attack: An attacker first attempts to map IP address space before searching for security holes.

Advanced Persistent Threats (APT): An adversary that possesses sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat (1) pursues its objectives repeatedly over an extended period of time; (2) adapts to defenders' efforts to resist it; and (3) is determined to maintain the level of interaction needed to execute its objectives. An unauthorized person gains undetected access to a system and stays for a long period of time. The intent is to steal data. A persistent presence is sometimes called consolidation. APTs can wait a long time before becoming active. By performing a gap analysis of the network configuration, hidden APTs can be made to show themselves either by detection methods or making them become visible by exposing themselves through their designed behaviour.

Amplification attack: A reflected DDoS attack when a single UDP packet generates tens or hundreds of times the bandwidth to overwhelm a control system with DNS response traffic. A denial-of-service technique that uses numerous hosts.

(Java) **applet attack:** The Java Applet Attack is considered as one of the most successful and popular methods for compromising a system. Spoofs a Java certificate, delivers a Metasploit-based payload and disables the Java security sandbox.

Aircrack-Ng: A set of tools for auditing wireless networks. Aircrack-ng is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. Aircrack-ng implements the standard FMS attack, making the attack much faster compared to other WEP cracking tools.

Airdrop-Ng: A program used for targeted, rule-based deauthentication of users. It can target based on MAC address, type of hardware, or completely deauthenticate ALL users by the transmission of deauthentication packets.

ARP spoofing attack: A technique by which an attacker sends (spoofed) Address Resolution Protocol (ARP) messages onto a local area network. Generally, the aim is to associate the attacker's MAC address with the IP address of another host, such as the default gateway, causing any traffic meant for that IP address to be sent to the attacker instead. ARP spoofing may allow an attacker to intercept data frames on a network, modify the traffic, or stop all traffic. Often the attack is used as an opening for other attacks, such as denial- of-service, man in the middle, or session hijacking attacks. Also called ARP cache poisoning or ARP poison routing.

NFS Misconfiguration: NFS stands for Network File System and it is a service that can be found in Unix systems. The purpose of NFS is to allow users to access shared directories in a network .However special effort needs to be done from system administrators in order to configure properly an NFS share. From the security perspective this can be catastrophic as any attacker can mount the whole directory and can view the contents in a local directory.

Auto-hacking attack: An easy-to-use device with the auto-hacking function will hack into a Wi-Fi network without a computer. Simply turn on the device, select a network and the device will hack it automatically. It is a standalone machine and does not require boot from disc or computer.

Backdoor attack: A backdoor is a means of access to a computer program that bypasses security mechanisms. A programmer may sometimes install a backdoor so that the program can be accessed for troubleshooting or other purposes. Also, it can be a hidden method for bypassing control system authentication. Two types are:

- **Beachhead backdoors**: Used to retrieve files, gather control system information, and trigger execution of other capabilities.
- **Standard backdoors**: Communicate using HTTP protocol to blend in with legitimate web traffic or a custom protocol and allow a hacker to upload/download, modify/ delete/execute programs, modify the registry, capture keystrokes, harvest passwords and take screenshots.

Banner grabbing attack: Capturing banner information (the information displayed to a remote user trying to connect to a service: this may include version information, control system information, or a warning about unauthorized use) that is transmitted when a connection is initiated.

Beacon channel: A stealthy method to transfer a large amount of information to or from a target network without being detected, because small packets are overlooked by most IDS software. The small packets are then reassembled to a file that can be many megabytes in size. Only deep packet inspection can ferret these out.

Behavior monitoring hack: Observing activities of users, control systems, and processes and measuring the activities against organizational policies and rules, baselines of normal activity, thresholds and trends.

Birthday attack: a type of cryptographic attack that exploits the mathematics behind the birthday problem in probability theory. This attack can be used to abuse communication between two or more parties. The attack depends on the higher likelihood of collisions found between random attack attempts and a fixed degree of permutations (pigeonholes). The attack depends on the higher likelihood of collisions found between random attack attempts and a fixed degree of permutations. Given a function f, the goal of the attack is to find two different inputs—x1, x2—such that f(x1) = f(x2). Such a pair x1, x2 is called a collision. With a birthday attack, it is possible to find a collision of a hash function in $2^{n/2}$ trials, n being the classical preimage resistance security. There is a general speculation that quantum computers can perform birthday attacks, thus breaking collision resistance, in $2^{n/3}$ trials.

Bit-flipping attack: An attack on a cryptographic cipher in which the attacker can change the ciphertext in such a way as to result in a predictable change of the plaintext, although the attacker is not able to learn the plaintext itself. Note that this type of attack is not directly against the cipher itself (as cryptanalysis of it would be), but against a particular message or series of messages. The attack is especially dangerous when the attacker knows the format of the message. In such a situation, the attacker can turn it into a similar message but one in which some important information is altered. For example, a change in the destination address might alter the message route in a way that will force re-encryption with a weaker cipher, thus possibly making it easier for an attacker to decipher the message.

Black hole attack: A type of denial-of-service attack in which a router that is supposed to relay packets instead discards them. This usually occurs from a router becoming compromised from a number of different causes. Also called a packet drop attack. One cause mentioned in research is through a denial-of-service attack on the router using a known DDoS tool. Because packets are routinely dropped from a lossy network, the packet drop attack is very hard to detect and prevent. The malicious router can also accomplish this attack selectively; for example, by dropping packets for a particular network destination, at a certain time of the day, a packet every n packets or every t seconds, or a randomly selected portion of the packets. This is rather called a gray hole attack.

Black start hack: The black start is the process of restoring electric power to a building without relying on the commercial power grid. Some power stations have small diesel generators, normally called the black start diesel generator (BSDG), which can be used to start larger generators (of several megawatts capacity), which in turn can be used to start the main power station generators. Hacking a black start generator will prevent the large generators from restarting.

Blended threat attack: A hostile action to spread malicious code via multiple methods. For example, sending a malicious URL by e-mail, with text that encourages the recipient to click the link, is a blended threat attack.

Boot sector virus: A virus that plants itself in a system's boot sector and infects the master boot record.

Boot record infector attack: Malware that inserts malicious code into the boot sector of a disk.

Bot attack: An application that runs automated cyber-attacks over the Internet. Bots perform simple and repetitive tasks at a faster rate than humans can.

Botnet attack: A group of computers taken over by malicious software and controlled across a network. The compromised computers are commonly known as zombies. These computers, which have been infected with malware, allow the attacker to control them.

Brute-force attack: A method of accessing an obstructed device through attempting multiple combinations of numeric and/or alphanumeric passwords. An attacker tries to use all possible combinations of letters, numbers, and symbols to enter a correct password. Programs exist to do this, such as Zip Password Cracker Pro. Any password can be cracked using the brute-force method, but it can take a very long time.

Buffer overflow attack: A method of overloading a predefined amount of space in a buffer, which can potentially overwrite and corrupt data in memory. Hackers exploit such a condition to crash a control system or to insert specially crafted code that allows them to gain control of the control system.

Byzantine failure hack: The loss of a control system service due to a Byzantine fault in systems that require consensus. Failure occurs when components of a control system fail with symptoms that prevent some components of the control system from reaching agreement among themselves, where such agreement is needed for the correct operation of the control system.

Cache cramming attack: The technique of tricking a computer browser to run cached Java code from the local disk, instead of the Internet zone, so it runs with less restrictive permissions.

Cache poisoning attack: Bad data from a remote name server is cached by another name server. Typically used with DNS cyber-attacks.

Cache stampede attack: A type of cascading failure that can occur when control systems with caching mechanisms come under very high load. Sometimes also called dog-piling.

Cascading failure hack: A failure in a control system of interconnected parts in which the failure of one part can trigger the failure of successive parts. When one part of the control system fails, nearby nodes must take up the slack for the failed component. This overloads these nodes, causing them to fail as well, prompting additional nodes to fail one after another.

Chain/loop attack: A chain of connections through many nodes as the attacker moves across multiple nodes to hide own origin and identity. In case of a loop attack, the chain of connections is in a loop making it more difficult to track down the origin.

Cinderella attack: A cyber-attack that disables security software by manipulating the network internal clock time so a security software license expires prematurely rendering the target network vulnerable to cyber-attack.

Click-jacking: Concealing hyperlinks beneath legitimate clickable content which, when clicked, causes a user to unknowingly perform actions, such as downloading malware, or sending your ID to a site. Numerous click-jacking scams have employed Like and Share buttons on social networking sites.

Collision attack: In cryptography, a collision attack on a cryptographic hash tries to find two inputs producing the same hash value, such as a hash collision.

Computer network attack (CNA): Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. A category of fires employed for offensive purposes in which actions are taken through the use of computer networks to disrupt, deny, degrade, manipulate, or destroy information resident in the target information system or computer networks, or the systems/networks themselves. The ultimate intended effect is not necessarily on the target system itself, but may support a larger effort, such as information operations or counter-terrorism; for example, altering or spoofing specific communications or gaining or denying access to adversary communications or logistics channels. The term fires means the use of weapon systems to create specific lethal or nonlethal effects on a target.

Computer virus attack: A program “infects” control systems in much the same way as a biological virus infects humans. The typical virus makes copies of itself and inserts them into the code of other programs.

CMMS cyber-attack: Computerized Maintenance Management System (CMMS) depends heavily on connectivity to the Internet as well as wireless communications to work efficiently. Building maintenance personnel are notified by the CMMS when equipment needs attention such as when a pump or valve malfunctions by generating and sending a work order to a mobile device. Personnel can access information wirelessly such as past maintenance history, preventive maintenance performed, all the specifications for the device including capacity, normal operating parameters and even whether spare parts are on hand and where

they are located in the storage room. Some CMMS databases include tenant information such as who requested maintenance, the room number, and telephone number. Some databases contain information such as security clearance for staff, labor rates, vacation schedule and contact information. The CMMS would be a great tool to target maintenance personnel for spear phishing attacks. When a hacker breaks into the CMMS, it is possible to acquire a great deal of information about the building and how it is operated. A hacker can see which pieces of equipment are high-priority assets, which can be considered safety hazards and the trigger points for failure alarms and automatic shutdown. A hacker can see whether spare parts are on hand in order to target equipment that would take longer to repair. Another thing to consider is that the CMMS is typically tied directly to the BCS network making the CMMS a possible attack vector for hackers.

Congestion collapse attack: A condition that a packet-switched computer network can reach, when little or no useful communication is happening due to congestion. Generally, occurs at “choke points” in the network, where the total incoming traffic to a node exceeds the outgoing bandwidth

Covert channel attack: An unauthorized communication path that manipulates a communications medium in an unexpected, unconventional, or unforeseen way in order to transmit information without detection by anyone other than the entities operating the covert channel.

Cross-site scripting (XSS) attack: A type of computer security vulnerability typically found in web applications. XSS vulnerabilities enable attackers to inject client-side script (typically Java) into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy. The effect may range from a petty nuisance to a significant security risk, depending on the sensitivity of the data handled by the vulnerable site and the nature of any security mitigation implemented by the site’s owner.

Cross-site request forgery (CSRF): A type of malicious exploit of a web site where unauthorized commands are transmitted from a user that the web site trusts. Unlike cross-site scripting (XSS), which exploits the trust a user has for a particular site, CSRF exploits the trust that a site has in a user’s browser. Also known as one- click attack or session riding.

Cycle timer hack: A timing device that can be preset to turn off and on at specific intervals. Hack this and an attacker can cause things to turn off when they should be on and vice versa.

Data loss attack: The result intentionally deleting data.

DC servo drive hack: A type of drive that works specifically with servo motors. It transmits commands to the motor and receives feedback from the servo motor resolver or encoder. A hacker can cause the drive to transmit false commands to servo motors or ignore feedback from the motors.

Deauthentication packet attack: This attack sends disassociating packets to one or more clients that are currently associated with a particular Wi-Fi access point thereby breaking the connection. The deauthentication packets are sent directly from a PC to the clients, so the attacker must be physically close enough to the clients for wireless transmissions to reach them.

Denial-of-service (DoS) attack: An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources. The following are some of the different forms of DoS attack:

- Teardrop: Sending irregularly shaped network data packets.
- Buffer Overflow: Flooding a server with an overwhelming amount data.
- Smurf: Tricking computers to reply to a fake request, causing much traffic.
- Physical: Disrupting a physical connection, such as a cable or power source.

Diagnostic server attacks: An attacker can execute the following attacks without any authentication required while maintaining stealthiness such as remote memory dump, remote memory patch, remote calls to functions and remote task management.

Dictionary attack: When a cyber-attack utilizes a dictionary to crack a password. Words from the dictionary are input in the password field to try to guess the password. Programs and tools allow hackers to easily try combinations of words in the dictionary to crack a user's password.

Direct-access attack: A direct-access attack means gaining physical access to a control system and performing various functions or installing various types of devices to compromise building operations. The attacker can install a virus, worm, or Trojan horse, download building operations data, survey building activity, or change the operating parameters of building equipment to the point of equipment failure.

Direct Digital Controls (DDC) hack: DDC is the automated control of a condition or process by a computer. All instrumentation is gathered by various analog and digital devices that use the network to transport these signals to the central controller. The central computer then follows all of its production rules and causes action requests to be sent via the same network to valves, actuators, and other HVAC components that can be adjusted. By hacking the DDC, an attacker controls all processes.

Distributed denial-of-service (DDoS) attack: A denial-of-service technique that uses numerous hosts to perform the attack.

DNS forgery attack: A hacker with access to a network can easily forge responses to the computer's DNS requests.

DNS sinkhole: Also known as a sinkhole server, Internet sinkhole, or BlackholeDNS. A DNS server that gives out false information, to prevent the use of the domain names it represents. A sinkhole is a standard DNS server that has been configured to hand out non-routable addresses for all domains in the sinkhole, so that every computer that uses it will fail to get access to the real web site. The higher up the DNS server is, the more computers it will block. Some of the larger botnets have been made unusable by TLD sinkholes that span the entire Internet. DNS Sinkholes are effective at detecting and blocking malicious traffic, and used to combat bots and other unwanted traffic.

DNS spoofing: A computer hacking attack, whereby data is introduced into a Domain Name System (DNS) resolver's cache, causing the name server to return an incorrect IP address, diverting traffic to the attacker's computer (or any other computer). Also called DNS cache poisoning.

Domain hijacking attack: A cyber-attack that takes over a domain by first blocking access to the domain's DNS server and then putting the hacker's server in its place.

Doorknob-rattling attack: A hacker attempts a very few common username and password combinations on several computers resulting in very few failed login attempts. This attack can go undetected unless the data related to login failures from all the hosts are collected and aggregated to check for doorknob-rattling from any remote destination.

Drive-by download attack: Malware installed on a target computer or other device as soon as a user visits a compromised web site.

Dropper attack: Computer malware that allows attackers to open a backdoor to install another malware program to an infected machine to implement additional functionality.

Fast flux: A DNS technique used by botnets to hide phishing and malware delivery sites behind an ever- changing network of compromised hosts acting as proxies.

Fault line attacks: Exploit gaps in coverage between interfaces of control systems.

Field device hack: Equipment that is connected to the field side on a ICS. Types of field devices include RTUs, PLCs, HMIs, actuators, sensors, and associated communications. All can be hacked.

Flame virus: This computer virus can record audio, screenshots, keyboard activity, and network traffic. It can record Skype conversations and can turn infected computers into Bluetooth beacons that attempt to download contact information from nearby Bluetooth-enabled devices. Also known as Flamer, Da Flame, sKyWIper, and Skywiper. Flame supports a "kill" command that wipes all traces of the malware from the computer. Due to the size and complexity of the program (20 MB), it is described as "twenty times" more complicated than Stuxnet.

Flooding attack: Cyber-attack that attempts to cause a failure in the security of a building control system or industrial control device by providing more input than the device can process properly.

Fork bomb attack: A cyber-attack that works by using the fork () call to create a new process which is a copy of the original. By doing this repeatedly, all available processes on the machine can be taken up.

Fragment overlap attack: The IP fragment overlapped exploit occurs when two fragments contained within the same IP datagram have offsets that indicate that they overlap each other in positioning within the datagram. This could mean that either fragment A is being completely overwritten by fragment B, or that fragment A is partially being overwritten by fragment B. Some operating systems do not properly handle fragments that overlap in this manner and may throw exceptions or behave in other undesirable ways upon receipt of overlapping fragments. Overlapping fragments may be used in an attempt to bypass Intrusion Detection Systems. In this exploit, part of an attack is sent in fragments along with additional random data; future fragments may overwrite the random data with the remainder of the attack. If the completed datagram is not properly reassembled at the IDS, the cyber-attack will go undetected.

Function pointer attack: A buffer overflow by overwriting a function pointer or exception handler, which is subsequently executed.

Fuzzing attack: A cyber-attack when indiscriminate data is transmitted to a server in an attempt to override controls.

Ghostware: “Stealth” programs—usually for monitoring, like Trojans, keyloggers, and so forth—that reside in a system and are not readily detectible by the user. They transmit information to the person that installed the programs without the PC user being able to tell that it’s there. Software designed to rid a system of adware, viruses, and the like, may not be able to tell if ghostware is on a PC.

Gray hole attack: A type of packet drop attack in which a router that is supposed to relay packets instead discards them for a particular network destination, at a certain time of the day, a packet every n packets or every t seconds, or a randomly selected portion of the packets. This usually occurs from a router becoming compromised from a number of different causes. Because packets are routinely dropped from a lossy network, the packet drop attack is very hard to detect and prevent.

Hijack attack: Active wiretapping in which a hacker seizes control of a previously established communication connection.

Hybrid cyber-attack: A cyber-attack that builds on the dictionary attack method by adding numerals and symbols to dictionary words.

Inference attack: A data mining technique performed by analysing data in order to illegitimately gain knowledge about a subject or database. Sensitive information can be considered leaked if an adversary can infer its real value with a high degree of confidence.

Input validation attack: A cyber-attack when a hacker sends unexpected input to a server in the hopes of confusing a building controls system.

Insider attack: An entity inside the security perimeter that is authorized to access control system resources, but uses them in a way not approved by those who granted the authorization.

IP flood attack: A denial-of-service attack that sends a host more “ping” packets than the protocol can handle.

IP masquerading (IPMASQ): Network address translation (NAT) that allows internal computers that don’t have an officially assigned IP address to communicate to other networks and the Internet. It allows one machine to act on behalf of other machines. Also called MASQ.

Jamming attack: An attack in which a device is used to emit electromagnetic energy on a wireless network’s frequency to make it unusable.

Keystroke logger attack: A program or USB device designed to record which keys are pressed on a computer keyboard used to obtain passwords or encryption keys and thus bypass other security measures. Another type of keystroke logger uses the accelerometer in a smartphone to capture keystrokes.

Kinetic cyber-attack: A cyber-physical attack that is intended to cause physical damage in the real world to people, buildings, equipment, infrastructure or a nation’s way of life. Not a virtual attack or theft of data.

LAND attack: LAND (Local Area Network Denial) attack is a DoS (denial-of-service) attack that consists of sending a special poison spoofed packet to a computer, causing it to lock up. The attack involves sending a spoofed TCP SYN packet (connection initiation) with the target host’s IP address to an open port as both source and destination. This causes the machine to reply to itself continuously. Most firewalls should intercept and discard the poison packet thus protecting the host from this attack. Some operating systems released updates fixing this security hole. In addition, routers should be configured with both ingress and egress filters to block all traffic destined for a destination in the source’s address space, which would include packets where the source and destination IP addresses are the same.

Log clipping: Selective removal of control system log entries to hide a compromise.

Macro virus: A type of malicious code that attaches itself to documents and uses the macro programming capabilities of the document’s application to execute, replicate, and spread or propagate itself.

Malicious applet attack: A small application program that is automatically downloaded and executed and that performs an unauthorized function on a control system.

Malicious code attack: Program code intended to perform an unauthorized function or process that will have adverse impact on the confidentiality, integrity, or availability of a control system.

Malicious logic attack: Hardware, firmware, or software that is intentionally included or inserted in a control system to perform an unauthorized function or process that will have adverse impact on the confidentiality, integrity, or availability of a control system.

Malware attack: Malicious software designed to infiltrate or damage a building control system. Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of a building control system. Malware types include virus, worm, Trojan horse, root kit, spyware and adware designed to infect a host. Spyware and some forms of adware are also examples of malicious code (malware). SOURCE:

Man-in-the-middle (MITM) attack: A cyber-attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

Manipulated variable attack: In a process that is intended to regulate some condition, a quantity or a condition that the control alters to initiate a change in the value of the regulated condition such as a setpoint.

Masquerade attack: A cyber-attack in which one system entity illegitimately poses as another entity. Also called a spoofing attack.

Metamorphic and polymorphic malware attack: This category of malware keeps changing its code so each of its succeeding versions is different from the previous one. Metamorphic and polymorphic malware evades detection and conventional antivirus programs. It is difficult to write since it requires complicated techniques.

Network weaving: Penetration technique in which different communication networks are linked to access a control system to avoid detection and trace-back.

Offline attack: An attack where the hacker obtains some data (typically by eavesdropping on an authentication protocol run, or by penetrating a building control system and stealing security files). Then the attacker can proceed to analyse data in a building control system of own choice.

Online attack: An attack against an authentication protocol where the Attacker either assumes the role of a Claimant with a genuine Verifier or actively alters the authentication channel. The goal of the attack may be to gain authenticated access or learn authentication secrets.

Overload attack: In an overload cyber-attack, a shared resource or service is overloaded with requests to such a point that it's unable to satisfy requests from other users.

Pass the Hash Attack: A hacking technique that allows an attacker to authenticate to a remote server/ service by using the underlying NTLM and/or LanMan hash of a user's password, instead of requiring the associated plaintext password as is normally the case. The attack exploits an implementation weakness in the authentication protocol in that the password hashes are not salted, and therefore remain static from session to session until the password is next changed.

Pharming attack: A sophisticated MITM cyber- attack intended to redirect a web site's traffic to another, fake site. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software. DNS servers are computers responsible for resolving Internet names into their real IP addresses. Compromised DNS servers are sometimes referred to as poisoned. Pharming requires unprotected access to target a computer, such as altering a customer's home computer, rather than a corporate business server.

Phishing attack: Tricking individuals into disclosing sensitive personal information by claiming to be a trustworthy entity in an electronic communication (e.g., Internet web sites). A digital form of social engineering that uses authentic-looking—but bogus—e-mails to request information from users or direct them to a fake web site that requests information.

Ping of Death Attack: A cyber-attack that sends a large echo request packet with to overflow the input buffers of the building control system causing it to crash.

Ping scan attack: A passive cyber-attack looking for machines responding to pings.

Ping sweep attack: A cyber-attack that pings a range of IP addresses, with the goal of finding building control system hosts that can be probed for vulnerabilities.

Port scanning attack: Using a program to remotely determine which ports on a control system are open (e.g., whether building control systems allow connections through those ports).

Power over Ethernet (PoE) hack: Technology that uses unused conductors on Ethernet cabling to power low voltage devices. Up to 44 volts 350 ma is available. POE Plus can provide up to 25.5 Watts. An attacker that hacks into a security network and causes a power surge on the Ethernet cabling may be able to cause devices to fail.

Preimage attack: In cryptography, a preimage attack on cryptographic hash functions tries to find a message that has a specific hash value. A cryptographic hash function should resist attacks on its preimage. Some significant preimage attacks have already been discovered, but they are not yet practical. If a practical preimage attack is discovered, it would drastically affect many Internet protocols. In this case, "practical" means that it could be executed by an

attacker with a reasonable amount of resources (one that costs a few thousand dollars and takes a few weeks might be very practical).

Privilege escalation attack: Privilege escalation describes a cyber-attack where an attacker with some level of restricted access is able to, without authorization, elevate their privileges or access level. So, for example, a standard computer user may be able to fool the system into giving them access to restricted data; or even to "become root" and have full, unrestricted access to a system.

Probing attack: To attempt to connect to well-known services that may be running on a control system; done to see if the control system exists, and potentially to identify the software it is running.

Program infector attack: Malware that attaches itself to existing program files.

Promiscuous mode: A configuration setting for a network interface card that causes it to accept all incoming packets that it sees, regardless of their intended destinations.

Protocol fuzzing attack: A testing technique used to generate valid and invalid packets with "random" header field values. The purpose is to analyse the behavior of a specific protocol by injecting unexpectedly malformed input parameter values. Random fuzzing is less effective, than smart fuzzing (tests based on the target specifications that require knowledge of the building control system).

Radiation monitoring: The process of receiving images, data, or audio from an unprotected source by searching for radiation signals.

Ransomware: A type of malware that restricts access to a computer system that it infects in some way, and demands that the user pay a ransom to the operators of the malware to remove the restriction. Some forms of ransomware systematically encrypt files on the system's hard drive (cryptoviral extortion) using a large key that may be technologically infeasible to breach without paying the ransom, while some may simply lock the system and display messages intended to coax the user into paying. Ransomware typically propagates as a Trojan horse, whose payload is disguised as a seemingly legitimate file.

Remote access tool (RAT): A piece of software that allows a remote "operator" to control a building control system as if physical access to that building control system is granted. While desktop sharing and remote administration have many legal uses, RAT software is usually associated with criminal or malicious activity. Malicious RAT software is typically installed without the victim's knowledge, often as payload of a Trojan horse, and tries to hide its operation from the victim and from security software. Such tools provide an operator the following capabilities:

- Screen/camera capture, image control or microphone control
- File management (download/upload/execute, etc.)

- Shell control (from command prompt)
- Computer control (power off/on/log off if remote feature is supported)
- Registry management (query/add/delete/modify)
- Hardware Destroyer (overclocker)

Remote code execution vulnerability: Could enable an attacker to execute PHP code on a web server and bypass security mechanisms. Can allow the attacker to gain administrative access to the building control system.

Remote-to-local user (R2L) cyber-attack: When a hacker has the ability to send packets over a building control system network (but who does not have a valid user account) exploits a system vulnerability to gain access as a user.

Replay attack: Cyber-attack that involves capturing traffic sent over the network, and then reinjecting it again later, causing commands to be executed twice. A variety of mechanisms are designed to prevent replay attacks such as by using timestamps or session tokens.

Repudiation attack: When a user denies the action performed or a transaction. Utilities need defense mechanisms in place to ensure that all user activity can be tracked and recorded. Otherwise, a user can simply deny having knowledge of the transaction or communication and later claim that such transaction or communication never took place.

Resource exhaustion attack: Resource exhaustion cyber-attacks involve tying up limited resources on a control system, making them unavailable to other users. Related to **Resource starvation**: A condition where a computer process cannot be supported by available computer resources. Resource starvation can occur due to the lack of computer resources or the existence of multiple processes that are competing for the same computer resources.

Rogue access point: A rogue access point is a wireless access point that has been installed on a secure network without explicit authorization from a local network administrator, whether added by a well- meaning employee or by a malicious insider. Although it is technically easy for a well-meaning employee to install a “soft access point” or an inexpensive wireless router: perhaps to make access from mobile devices easier: it is likely that they will configure this as “open,” or with poor security, and potentially allow access to unauthorized parties. If an attacker installs a rogue access point they are able to run various types of vulnerability scanners, and rather than having to be physically inside the building, a hacker can attack remotely: perhaps from a reception area, adjacent building, or car parking lot.

Rootkit: A set of tools used by an attacker after gaining root-level access to a host to conceal the attacker’s activities on the host and permit the attacker to maintain root-level access to the host through covert means.

Scanning: Sending packets or requests to another system to gain information to be used in a subsequent attack. Scanning attack: Any of the following:

- active port scanning: Actively send network packets to enumerate all open ports of a device, including both TCP and UDP.
- passive traffic mapping/scanning: Passively record network traffic. Discover ports that are normally used, without detecting open ports not actively used.
- version scanning: Actively attempt to discover the protocol by connecting to open ports.
- vulnerability scanning: Actively connect to a remote device and exploit known vulnerabilities.

Scavenging attack: Unauthorized searching through data in a BCS, ICS, or SCADA system to gain knowledge of sensitive data. Searching through object residue to acquire data.

Sensory malware: Malware designed to hijack data collected surreptitiously from sensors on a networked device.

Session hijacking attack: Taking over a session that someone else established.

Smurf attack: A cyber-attack that spoofs the target address and sends a ping to the broadcast address for a remote network, which results in a large amount of ping replies being sent to the target.

Sniffer: Is a computer program or piece of computer hardware that can intercept and log traffic that passes over a digital network or part of a network. As data streams flow across the network, the sniffer captures each packet and, if needed, decodes the packet's raw data, showing the values of various fields in the packet, and analyses its content according to the appropriate RFC or other specifications.

Spear phishing attack: Phishing attempts directed at specific individuals or companies with the sole purpose of obtaining unauthorized access to victim's sensitive data such as network access credentials. Attackers may initially gather personal information about their target to increase the probability of success. This technique is, by far, the most successful on the Internet today, accounting for 91% of cyber-attacks.

Spoofing: (1) Faking the sending address (IP, Caller ID, GPS, e-mail address) of a transmission to gain illegal (unauthorized) entry into a secure building control system. (2) Spoofing can also refer to legitimate copyright holders placing distorted or unlistenable versions of their works on file-sharing networks. SOURCE: SP 800-48

Spoofing attack: Generation of outbound network traffic pretending to be from somewhere else, typically used in a denial-of-service attack. See Masquerading Attack.

Spyware: Software that aims to gather information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge. Spyware

is mostly classified into four types: system monitors, Trojan horse, adware, and tracking cookies. Spyware is mostly used for the purposes of tracking and storing Internet users' movements on the web and serving up pop-up ads to Internet users. Whenever spyware is used for malicious purposes, its presence is typically hidden from the user and can be difficult to detect. Some spyware, such as keyloggers, may be installed by the owner of a shared, corporate, or public computer intentionally in order to monitor users. While the term spyware suggests software that monitors a user's computing, the functions of spyware can extend beyond simple monitoring. Spyware can collect almost any type of data, including personal information like Internet surfing habits, user logins, and bank or credit account information. Spyware can also interfere with user control of a computer by installing additional software or redirecting web browsers. Some spyware can change computer settings, which can result in slow Internet connection speeds, unauthorized changes in browser settings, or changes to software settings. Spyware does not necessarily spread in the same way as a virus or worm because infected systems generally do not attempt to transmit or copy the software to other computers.

Spy-phishing: Defined as "crimeware," spy-phishing capitalizes on the trend of "blended threats." It borrows techniques from both phishing and spyware. The downloaded applications sit silently on the user's system until the targeted URL is visited wherein it activates, sending information to the malicious third party. Through the use of spyware and other Trojans, spy-phishing attempts to prolong the initial phishing attacks beyond the point at which the phishing site is available.

SQL injection attack: A type of input validation attack where SQL code is inserted into database-driven application queries to manipulate the database.

Stack smashing attack: A cyber-attack using a buffer overflow to trick a computer into executing arbitrary code.

Stealth strategy attack: Some viruses try to avoid detection by killing the tasks associated with antivirus software before it can detect them (for example, Conficker worm, also known as Downup, Downadup, and Kido).

Supply chain attack: Attacks that allow the adversary to utilize implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate hardware, software, operating systems, peripherals (information technology products) or services at any point during the life cycle. For example, including a tiny microphone in millions of thermostats manufactured in a foreign country so when they are installed in sensitive rooms, they can be used to eavesdrop on conversations.

Sybil cyber-attack: A Sybil cyber-attack is the forging of multiple identities for malicious intent, named after "Sybil," the famous multiple personality disorder patient. A spammer may create multiple web sites at different domain names that all link to each other.

Tampering attack: Tampering is a web-based cyber-attack where certain parameters in the URL are changed without the customer's knowledge; and when the customer keys in that URL, it looks and appears exactly the same. Tampering is basically done by hackers and criminals to steal the identity and obtain illegal access to information.

Tethering attack: Connecting one device to another. In the context of mobile phones and tablet computers, tethering allows sharing the Internet connection of the phone or tablet with other devices such as laptops. Connection of the phone or tablet with other devices can be done over wireless LAN (Wi-Fi), over Bluetooth or by physical connection using a cable, for example through USB.

Tiny fragment attack: To impose an unusually small fragment size on outgoing packets. If the fragment size is small enough, a disallowed packet might be passed because it didn't hit a match in the filter.

Trojan horse attack: A non-self-replicating program that seems to have a useful purpose, but in reality has a different, malicious purpose. A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

User-to-Root (U2R) Attack: This cyber-attack occurs when an attacker with access to a normal user account is able to exploit a control system vulnerability to gain root access.

Vampire tap: A device for physically connecting a station (e.g., a computer or printer) to a network that uses 10BASE5 cabling. This device clamps onto and "bites" into the cable (hence the vampire name), forcing a spike through a hole drilled through the outer shielding to contact the inner conductor while other spikes bite into the outer conductor. Vampire taps allow new connections to be made on a given physical cable while the cable is in use. Also called a piercing tap.

Verifier impersonation attack: An attack where the attacker impersonates the verifier in an authentication protocol, usually to learn a password.

Virtual Private Network (VPN): A virtual network—built on top of existing physical networks—that provides a secure communications tunnel for data and other information transmitted between networks. Protected information system link utilizing tunneling, security controls (see information assurance), and endpoint address translation giving the impression of a dedicated line.

Virus attack: Software buried within an existing program designed to infect a computer. A code segment that replicates by attaching copies of itself to existing executable programs. This is usually done in such a manner that the copies will be executed when the file is loaded into memory, allowing them to infect still other files. The new copy of the virus is executed when a user executes the new host program. The virus may include any additional "payload" that is triggered when specific conditions are met. For example, some viruses display a text

string on a particular date. There are many types of viruses including variants, overwriting, resident, stealth, and polymorphic. Viruses often have damaging side effects, sometimes intentionally, sometimes not.

War dialing attack: Dialing all the telephone numbers in a given area code to locate control system devices connected by a modem.

War droning attack: Use of a cyber-drone to search for Wi-Fi wireless networks connected to a control system at a facility and hack into networks when they are found. A cyber-drone can also shut down computer systems and other nearby electronic systems from the sky through targeted emission of microwaves.

War driving/walking Attack: The act of searching for Wi-Fi wireless networks by a hacker in a moving vehicle/on foot, using a portable computer, smartphone or personal digital assistant (PDA). Also called access point mapping.

Webcam hack: Most webcams can be hacked. A hacker can watch your facility without your knowledge. This is a fairly simple hack made possible by a Trojan horse called Blackshades that even a script kiddie can master. What's worse is a hacker may be able to hack into your CS through IP-enabled cameras.

Whaling attack: Spear phishing targeting high-profile executives, politicians, and celebrities. Whaling e-mails are highly-personalized and appear to come from a trusted source. Once opened, the target is directed to a web site that was created specifically for that individual's attack. Successful whaling targets are referred to as having been harpooned.

Wireless Sensor Network (WSN) cyber-attack: These cyber-attacks prevent sensors from detecting and transmitting data through the network infrastructure.

Worm attack: A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself that harms the network and consumes bandwidth.

ZeroAccess attack: A Trojan horse bot used to download other malware on an infected machine from a botnet, while remaining hidden on a control system using rootkit techniques.

Zero-day exploit attack: A worm, virus, or other cyber-threat that hits users on the same day the vulnerability is announced

Cyber-Physical measures terms

Anti-jam: Countermeasures ensuring that transmitted information can be received despite deliberate jamming attempts.

Anti-router: A device that detects Wi-Fi surveillance devices and blocks them from accessing your Wi-Fi network. Every wireless device has a unique hardware signature assigned to it by the manufacturer. These signatures are broadcast by wireless devices as they probe for, connect to, and use wireless networks. An anti-router “sniffs” the airwaves for these signatures, looking for surveillance devices such as a drone. If a banned device is discovered an alarm is triggered and if that device is connected to a network that the anti- router is trained to defend, a stream of “de-authentication packets” are sent automatically to disconnect the rogue device.

Anti-spoof: Countermeasures taken to prevent the unauthorized use of legitimate identification and authentication (I&A) data, however it was obtained, to mimic a subject different from the attacker.

Antispyware software: A program that specializes in detecting both malware and non-malware forms of spyware.

Antivirus software: A program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents.

Application Whitelisting (AWL): AWL can detect and prevent attempted execution of malware uploaded by adversaries. The static nature of BCS and SCADA systems make them ideal candidates for AWL. Whitelist stands for a list or register of entities that are being provided a particular privilege, service, mobility, access, or recognition. Entities on the list will be accepted, approved, and/or recognized. Whitelisting is the reverse of blacklisting, the practice of identifying entities that are denied, unrecognized, or ostracized.

Asymmetric keys: Two related keys, a public key and a private key that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification.

Authentication mechanism: Hardware-or software-based mechanisms that force users to prove their identity before accessing data on a device.

Automated password generator: An algorithm that creates random passwords that have no association with a particular user

Big red button: A kill switch, also known as an emergency stop or e-stop, is a safety mechanism used to shut off a device in an emergency situation in which it cannot be shut down in the usual manner. Unlike a normal shutdown switch/procedure, which shuts down all control systems in an orderly fashion and turns the machine off without damaging it, a kill switch is designed and configured to (1) completely and as quickly as possible abort the operation, even if this damages equipment; (2) be operable in a manner that is quick, simple

(so that even a panicking operator can activate it); and, usually, (3) be obvious even to an untrained operator or a bystander.

Black hole filtering: Black hole filtering refers specifically to dropping packets at the routing level, usually using a routing protocol to implement the filtering on several routers at once, often dynamically to respond quickly to distributed denial-of-service attacks.

Boundary protection: Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communication, through the use of boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels).

Boundary protection device: A device with appropriate mechanisms that (1) facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system); and/or (2) provides information system boundary protection. SOURCE: SP 800-53 A device with appropriate mechanisms that facilitates the adjudication of different security policies for interconnected systems.

Building operations recovery: The component of recovery after a cyber-physical attack which deals specifically with the relocation of key personnel, provision of equipment, supplies, work space, communication facilities, computer processing capability, records and so forth.

Burp suite: A scanner with a limited “intruder” tool for cyber-attacks. Many security-testing specialists use this effective tool for penetration testing.

Canary: Anything that can send up an observable alert if something happens. For example, you can set up a computer on a subnet such that no other computer should ever access that. If something touches it, you know it’s from outside normal behavior. Also called a tripwire.

Certificate policy (CP): A specialized form of administrative policy tuned to electronic transactions performed during certificate management. A certificate policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery, and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.

Certificate Revocation List (CRL): A list of revoked public key certificates created and digitally signed by a certification authority.

Challenge and reply authentication: Prearranged procedure in which a subject requests authentication of another and the latter establishes validity with a correct reply.

Challenge-Handshake Authentication Protocol: An authentication protocol where the verifier sends the claimant a challenge (usually a random value or a nonce) that the claimant combines with a shared secret (often by hashing the challenge and secret together) to

generate a response that is sent to the verifier. The verifier knows the shared secret and can independently compute the response and compare it with the response generated by the claimant. If the two are the same, the claimant is considered to have successfully authenticated himself. When the shared secret is a cryptographic key, such protocols are generally secure against eavesdroppers. When the shared secret is a password, an eavesdropper does not directly intercept the password itself, but the eavesdropper may be able to find the password with an off-line password guessing attack.

Character Generator Protocol (CHARGEN) attack: A service of the Internet Protocol Suite intended for testing, debugging, and measurement purposes that is rarely used, as its design flaws allow misuse. UDP CHARGEN is commonly used in denial-of-service attacks. By using a fake source address, the attacker can send bounce traffic off a UDP CHARGEN application to the victim. UDP CHARGEN sends 200 to 1,000 times more data than it receives, depending upon the implementation. This “traffic multiplication” is attractive to an attacker. Also attractive is the obscuring of the attacker’s IP address from the victim. CHARGEN was widely implemented on network-connected printers. As printer firmware was rarely updated on older models before CHARGEN and other security concerns were known, there may still be many network-connected printers that implement the protocol. Where these are visible to the Internet, they are invariably misused as denial-of-service vectors. Potential attackers often scan networks looking for UDP port 19 CHARGEN sources. So notorious is the availability of CHARGEN in printers that some distributed denial-of-service Trojans now use UDP port 19 for their attack traffic. The supposed aim is to throw investigators off the track; to have them looking for old printers rather than subverted computers.

Checksum: Value computed on data to detect error or manipulation.

Ciphony: Process of enciphering audio information, resulting in encrypted speech.

Common Misuse Scoring System (CMSS): A set of measures of the severity of software feature misuse vulnerabilities. A software feature is a functional capability provided by software. A software feature misuse vulnerability is a vulnerability in which the feature also provides an avenue to compromise the security of a control system.

Communications cover: Concealing or altering of characteristic communications patterns to hide information that could be of value to an adversary.

Communications deception: Deliberate transmission, retransmission, or alteration of communications to mislead an adversary’s interpretation of the communications.

Compartmented mode: Mode of operation wherein each user with direct or indirect access to a system, its peripherals, remote terminals, or remote hosts has all of the following: (1) valid security clearance for the most restricted information processed in the system; (2) formal access approval and signed nondisclosure agreements for that information which a user is to have access; and (3) valid need-to-know for information which a user is to have access.

Configuration control: Process of controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modification prior to, during, and after system implementation.

Content filtering: The process of monitoring communications such as e-mail and web pages, analysing them for suspicious content, and preventing the delivery of suspicious content to users. SOURCE: SP 800-114

Contingency plan: A plan for emergency response, back-up operations, and post- cyber-attack recovery for control systems and installations. The contingency plan ensures minimal impact upon building operations in the event the control system or facility is damaged or destroyed.

Contingency planning: A plan that addresses how to keep an organization's building functions operating in the event of a cyber-physical attack.

Cover-coding: A technique to reduce the risks of eavesdropping by obscuring the information that is transmitted.

Cyclic redundancy check (CRC): An error-detecting code commonly used in digital networks and storage devices to detect accidental changes to raw data. Blocks of data entering these systems get a short check value attached, based on the remainder of a polynomial division of their contents. On retrieval, the calculation is repeated and corrective action can be taken against presumed data corruption if the check values do not match.

Deep packet inspection (DPI): A form of computer network packet filtering that examines the data part (and possibly also the header) of a packet as it passes an inspection point, searching for protocol non- compliance, viruses, spam, intrusions, or defined criteria to decide whether the packet may pass or if it needs to be routed to a different destination, or, for the purpose of collecting statistical information. Also called complete packet inspection.

DumpSec: A security tool that dumps a variety of information about a control system's users, file system, registry, permissions, password policy, and services.

Egress filtering: Filtering outbound network traffic.

Encryption: Conversion of plaintext to ciphertext through the use of a cryptographic algorithm. The process of changing plaintext into ciphertext for the purpose of security or privacy.

End-to-end encryption: Communications encryption in which data is encrypted when being passed through a network, but routing information remains visible.

Explicit messaging: A proprietary vendor method of communication between devices where each message contains a message code that identifies the type of message and determines the action to be taken when received.

Failover protection: The transfer of operation from a failed component (e.g., controller, disk drive, pump) to a redundant component to ensure uninterrupted equipment operations.

File integrity monitoring (FIM): Host-based intrusion detection software installed on an asset that analyses control system behaviour and configuration status to track user access and activity as well as identify potential security exposures such as:

- Control system compromise
- Modification of critical configuration files (e.g., registry settings, password, etc.)
- Common rootkits
- Rogue processes

Forward recovery: Recovering a control system to the point of failure by applying active data to current backup files of the database.

Frequency hopping: Repeated switching of frequencies during radio transmission according to a specified algorithm, to minimize unauthorized interception or jamming of telecommunications.

Full-disk encryption (FDE): The process of encrypting all the data on the hard disk drive used to boot a computer, including the computer's operating system, and permitting access to the data only after successful authentication with the full disk encryption product.

Graduated security: A security system that provides several levels (e.g., low, moderate, high) of protection based on threats, risks, available technology, support services, time, human concerns, and economics.

Hardening: Configuring a host's operating systems and applications to reduce the host's security weaknesses.

High-assurance guard (HAG): An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance. A guard that has two basic functional capabilities: a message guard and a directory guard. The message guard provides filter service for message traffic traversing the guard between adjacent security domains. The directory guard provides filter service for directory access and updates traversing the guard between adjacent security domains.

Host-based intrusion detection system (HIDS): Detects malicious activity on a host from characteristics such as change of files (file system integrity checker) or operating system profiles.

Identity-based access control: Access control based on the identity of the user (typically relayed as a characteristic of the process acting on behalf of that user) where access authorizations to specific objects are assigned based on user identity.

Information Security Continuous Monitoring (ISCM): Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. The terms continuous and ongoing in this context mean that security controls and organizational risks are assessed and analysed at a frequency sufficient to support risk-based security decisions to adequately protect organization information.

Ingress filtering: The process of blocking incoming packets that use obviously false IP addresses, such as reserved source addresses.

Intrusion detection system (IDS): Hardware or software product that gathers and analyses information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from within the organizations):

- Host-based IDS operate on information collected from within an individual computer system. This vantage point allows host-based IDSs to determine exactly which processes and user accounts are involved in a particular attack on the Operating System. Furthermore, unlike network-based IDSs, host-based IDSs can more readily "see" the intended outcome of an attempted attack, because they can directly access and monitor the data files and system processes usually targeted by attacks.
- Network-based IDS detect attacks by capturing and analysing network packets. Listening on a network segment or switch, one network-based IDS can monitor the network traffic affecting multiple hosts that are connected to the network segment.

Intrusion prevention system (IPS): System(s) detect an intrusive activity and can attempt to stop the activity, ideally before it reaches its targets. SOURCE:

Least privilege: The security objective of granting users only those accesses they need to perform their official duties.

Manipulative communications deception: Alteration or simulation of friendly telecommunications for the purpose of deception.

Manual override switch: Manual override switches and potentiometers of output modules support direct operation. The positions of the manual override switches and potentiometers directly control outputs: independently. When a manual override switch or potentiometer is not in its default position ("auto"), the corresponding output LED will blink continuously, and the output module will send a feedback signal with the status "manual override" and the given override position to the Controller (which will then also store this information in its alarm memory).

Misnamed files: A technique used to disguise a file's content by changing the file's name to something innocuous or altering its extension to a different type of file, forcing the examiner to identify the files by file signature versus file extension.

Multifactor authentication: Authentication using two or more factors to achieve authentication. Factors include (1) something you know (e.g., password/PIN); (2) something you have (e.g., cryptographic identification device, token); or (3) something you are (e.g., biometric).

Network intrusion detection system (NIDS): A device or software that monitors for malicious activity and rule violations and reports incidences.

Network sniffing: A passive technique that monitors network communication, decodes protocols, and examines headers and payloads for information of interest. It is both a review technique and a target identification and analysis technique.

Periods processing: The processing of various levels of classified and unclassified information at distinctly different times. Under the concept of periods processing, the building control system must be purged of all information from one processing period before transitioning to the next.

Physically isolated network: A network that is not connected to entities or systems outside a physically controlled space.

Polyinstantiation: The ability of a database to maintain multiple records with the same key. Used to prevent inference attacks.

Protected distribution system (PDS): Wire line or fiber optic system that includes adequate safeguards and/or countermeasures (e.g., acoustic, electric, electromagnetic, and physical) to permit its use for the transmission of unencrypted information through an area of lesser classification or control.

Quadrant: Short name referring to technology that provides tamper-resistant protection to cryptographic equipment.

Redundant control server: A backup to the control system server that maintains the current state of the control server at all times.

Redundant data path (RDP): Technology that creates an alternate data path between the server and the storage system in the event of control system component failures to ensure continuous access to data.

Resource encapsulation: Method by which the reference monitor mediates accesses to an information system resource. Resource is protected and not directly accessible by a subject. Satisfies requirement for accurate auditing of resource usage.

Rogue scanner: A network security tool to automatically discover rogue access points.

Salt: A non-secret value that is used in a cryptographic process, usually to ensure that the results of computations for one instance cannot be reused by an attacker.

Samhain sensor: Frequently checks the critical control system files for additions, modifications and deletions. All changes are immediately logged locally or reported to a remote log server. These include timestamps of changes, file names, violation type, and changes in the building control system kernel.

Sandboxing: A method of isolating application modules into distinct fault domains enforced by software. The technique allows untrusted programs written in an unsafe language, such as C, to be executed safely within the single virtual address space of an application. Untrusted machine interpretable code modules are transformed so that all memory accesses are confined to code and data segments within their fault domain. Access to building control system resources can also be controlled through a unique identifier associated with each domain.

Secure configuration: Restricting the functionality of every device, operating system, and application to the minimum needed for the building control system to operate properly. A secure configuration minimizes the information that Internet-connected devices disclose about their configuration and software version and ensure they cannot be probed for vulnerabilities.

Security appliance: A server that is designed to protect control system networks from unwanted traffic. It is a simple and cost-effective way to segment a control system network into security zones. The user defines rules that specify exactly which devices are allowed to communicate, what protocols they may use, and what actions those protocols perform. Any communication that is not on the “allowed” list is automatically blocked and reported.

Shadow password file: A control system file in which encrypted user passwords are stored so that they aren’t available to people who try to break into the control system.

Shadow file processing: An approach to data backup in which real-time duplicates of critical files are maintained at a remote processing site.

Snort and dragon sensors: Signature-matching intrusion detection applications that report alerts and provide information on source and destination IP, and port, and which rule or signature was violated.

Social engineering attack: Social engineering is the art and science of getting people to do something you want them to do that they might not do in the normal course of action. Instead of collecting information by technical means, intruders might also apply methods of social engineering such as impersonating individuals on the telephone, or using other persuasive means (e.g., tricking, convincing, inducing, enticing, provoking) to encourage someone to disclose information. Attackers look for information about who the target does business with, both suppliers and customers and they are particularly interested in IT support. They gather this information to better understand roles and responsibilities. They use this information to

pose as someone from one of these companies. Attackers look for information such as birthdays, who was recently promoted or who just had a baby. Hackers do not discount any information they uncover. They will use bad relationships between IT department and other offices as a wedge to gain information.

Software-based fault isolation: A method of isolating application modules into distinct fault domains enforced by software. The technique allows untrusted programs written in an unsafe language, such as C, to be executed safely within the single virtual address space of an application. Untrusted machine interpretable code modules are transformed so that all memory accesses are confined to code and data segments within their fault domain. Access to system resources can also be controlled through a unique identifier associated with each domain.

Split-horizon: A method of preventing routing loops in distance-vector routing protocols by prohibiting a router from advertising a route back onto the interface from which it was learned.

Strong authentication: The requirement to use multiple factors for authentication and advanced technology, such as dynamic passwords or digital certificates, to verify an entity's identity.

Superencryption: Process of encrypting encrypted information. Occurs when a message, encrypted offline, is transmitted over a secured, online circuit, or when information encrypted by the originator is multiplexed onto a communications trunk, which is then bulk encrypted.

Time-dependent password: Password that is valid only at a certain time of day or during a specified interval of time.

Traffic padding: Generation of mock communications or data units to disguise the amount of real data units being sent. SOURCE:

Trampolining: In a buffer overflow attack, if the address of the user-supplied data is unknown, but the location is stored in a register, then the return address can be overwritten with the address of an opcode, which causes execution to jump to the user-supplied data. If the location is stored in a register R, then a jump to the location containing the opcode for a jump R, call R or similar instruction, will cause execution of user-supplied data.

Triple-wrapped: Data that has been signed with a digital signature, encrypted, and then signed again.

Tunneled password protocol: A protocol where a password is sent through a protected channel.

Two-Factor Authentication: Proof of identity by two independent means, such as knowing a password and using a smartcard.

Two-person control (TPC): Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect

and unauthorized procedures with respect to the task being performed and each familiar with established security and safety requirements.

Two-person integrity (TPI): System of storage and handling designed to prohibit individual access by requiring the presence of at least two authorized individuals, each capable of detecting incorrect or unauthorized security procedures with respect to the task being performed.

Virus detection software: Software written to scan machine-readable media on building control systems. There are a growing number of reputable software packages available that are designed to detect or remove viruses. In addition, many utility programs can search text files for virus signatures or potentially unsafe practices.

Voice intrusion prevention system (VIPS): A security management system for voice networks that monitors voice traffic for multiple calling patterns or cyber-attack signatures to detect anomalous behaviour.

CP systems components terms

Bus: The main electrical communication path in which signals are sent from one part of the computer to another.

Channel: A portion of the control network consisting of one or more segments connected by repeaters.

Common Industrial Protocol (CIP): An industrial protocol for industrial automation applications. CIP encompasses a comprehensive suite of messages and services for the collection of manufacturing automation applications: control, safety, synchronization, motion, configuration, and information. CIP allows users to integrate these manufacturing applications with enterprise-level Ethernet networks and the Internet. CIP is media-independent and provides a unified communication architecture throughout the manufacturing enterprise. These include application extensions to CIP: CIP Safety, CIP Motion, and CIP Sync.

Control loop: A combination of field devices and control functions arranged so that a control variable is compared to a set point and returns to the process in the form of a manipulated variable.

Control server: A computer server that hosts the supervisory control system, typically a commercially available BCS or SCADA application.

ControlNet: Open network protocol for industrial automation applications.

Data historian: A centralized database supporting data analysis using statistical process control (SPC).

Distributed I/O: Eliminates expensive point-to-point wires by networking process signals onto one digital communication link.

Ethernet: A local area network standard for hardware, communication, and cabling. Also is the most widely installed local area network (LAN) technology. Ethernet is a link layer protocol in the TCP/IP stack, describing how networked devices can format data for transmission to other network devices on the same network segment, and how to put that data out on the network connection.

Extensible Authentication Protocol (EAP): An authentication framework frequently used in wireless networks and point-to-point connections.

Exterior Gateway Protocol (EGP): The protocol that distributes routing information between two neighbour gateway routers that make up an autonomous control system.

Fiber channel (FC): A high-speed network technology (commonly running at 2-, 4-, 8- and 16-gigabit per second rates) primarily used to connect computer data storage.

Fiber channel-arbitrated loop (FC-AL): A fiber channel topology in which devices are connected in a one- way loop fashion in a ring topology common within data storage systems.

Fiber Distributed Data Interface (FDDI): A 100 Mbit/s ANSI standard LAN architecture, defined in X3T9.5. The underlying medium is optical fiber (though it can be copper cable, in which case it may be called CDDI) and the topology is a dual-attached, counter-rotating token ring.

Fieldbus: A digital, serial, multi-drop, two-way data bus or communication path or link between low-level industrial field equipment such as sensors, transducers, actuators, local controllers, and even control room devices. Use of fieldbus technologies eliminates the need of point-to-point wiring between the controller and each device. A protocol is used to define messages over the fieldbus network with each message identifying a particular sensor on the network.

Field Transfer Protocol (FTP): Internet standard for transferring files over the Internet.

File server: Central repository of shared files and applications in a building controls system.

Firewall: A hardware/software capability that limits access between networks and/or systems in accordance with a specific security policy.

Firewall control proxy: The component that controls a firewall's handling of a call. The firewall control proxy can instruct the firewall to open specific ports that are needed by a call, and direct the firewall to close these ports at call termination.

Frequency converter: An electronic device that converts alternating current of one frequency to another frequency and may also change the voltage. Frequency converters are typically used to control the speed of motors, primarily pumps and fans on industrial processing lines, where the control accuracy requirements can be very high.

General purpose programmable controller (GPPC): Unlike an ASC or AGC, a GPPC is not furnished with a fixed application program and does not have a fixed ProgramID or XIF file. A GPPC can be reprogrammed.

GSM base station: A cellular network. Cell phones connect to it by searching for cells in the immediate vicinity.

Hi-Link network devices: Hi-Link network devices are being designed to understand all the languages that connected devices use and be able to communicate with them in their own language. This approach is an attempt to unify the languages in which intelligent electronic devices communicate, but at the network level and not the device level.

Historian: A control system computer that stores values for various processes or states of interest to the control system. They are often the point of connection between the corporate network and the control system network.

Hub: A device that splits one network cable into a set of separate cables, each connecting to a different computer; used in a control system to create a small-scale network.

Human-machine interface (HMI): The computer hardware and software that enables a single operator to monitor and control equipment remotely.

Industrial Control System (ICS): An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems (SCADA) used to control geographically dispersed assets, as well as distributed control systems (DCS) and smaller control systems using programmable logic controllers to control localized processes.

Intelligent electronic device (IED): A device capable of two-way communication directly with a BCS, ICS, or SCADA computer that performs electrical functions such as sensors, actuators, servos, relays and circuit breakers. Any device incorporating one or more processors with the capability to receive or send data/ control from or to an external source (e.g., electronic multifunction meters, digital relays, controllers).

Inter-Control Center Communications Protocol (ICCP): The SCADA protocol used to exchange information with business partners or to exchange information between the corporate network and control center network.

Internet Control Message Protocol (ICMP): One of the main Internet protocols. Used by network devices to send error messages such as when a requested service is not available.

Internet Protocol (IP): A data-oriented protocol used for communicating data across a packet-switched inter-network. Data is sent in blocks referred to as packets. Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks.

I/O brick: A PLC storage system that handles a huge amount of I/O requests from machines and desktops.

IP-controlled device: An intelligent electronic device that can be controlled over the Internet. So, an IP controlled rack-mount power controller allows remote access, real-time monitoring and customer management from a phone, computer, or tablet. Such a device would be useful to reboot a server, but this represents a huge security risk.

Kernel: The core of an operating system such as Windows 98, Windows NT, Mac OS, or Unix; provides basic services for the other parts of the operating system, making it possible for it to run several programs at once (multitasking), read and write files and connect to networks and peripherals.

Key loader: A self-contained unit that is capable of storing at least one plaintext or encrypted cryptographic key or key component that can be transferred, upon request, into a cryptographic module.

Light fidelity (Li-Fi): Wireless data streaming using LED lights to transmit information. LEDs can communicate twice as fast (15 gigabits per second) as Wi-Fi. Li-Fi may be more secure because light can't go through walls, hackers would not be able to log on to Li-Fi networks in the same way that they're able to eavesdrop on Wi-Fi. Li-Fi may also be less secure.

Local area network (LAN): Computers connected together so that they can communicate with each other. A network of computers, within a limited area (e.g., a company or organization); computing equipment, in close proximity to each other, connected to a server which houses software that can be accessed by the users. This method does not utilize a public carrier.

Logical unit number (LUN): An addressing scheme used to define SCSI devices on a single SCSI bus.

Machine controller: A control system/motion network that electronically synchronizes drives within a machine system instead of relying on synchronization via mechanical linkage.

Mainframe computer: A high-end computer processor, with related peripheral devices, capable of supporting large volumes of batch processing, high performance on-line transaction processing systems, and extensive data storage and retrieval.

Manufacturing Message Specification (MMS): A messaging protocol for transferring real time process data and supervisory control information between networked field devices and computer applications.

Master-slave/token passing (MS/TP): Data link protocol as defined by the BACnet standard. Multiple speeds (data rates) are permitted by the BACnet MS/TP standard.

Master terminal unit (MTU): SCADA server.

Media access control (MAC) address: A sublayer of the data link layer. Provides addressing and channel access control mechanisms that make it possible for several terminals or nodes to communicate within an Ethernet network. A link between the sublayer and the physical layer.

Mobile ad hoc network (MANET): A continuously self-configuring, infrastructure-less network of mobile devices connected without wires. MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network. MANETs consist of a peer-to-peer, self- forming, self-healing network. MANETs typically communicate at radio frequencies (30 MHz: 5 GHz).

Modbus: A serial protocol for control network communications used in utility control systems. It was originally published by Modicon (now Schneider Electric) for use with programmable logic controllers. It is a de facto standard and it is a common means of connecting industrial electronic devices. Data type names came about from its use in driving relays: a single-bit physical output is called a coil, and a single-bit physical input is called a discrete input or a contact. Modbus is a master/slave protocol, there is no way for a field device to "report by

exception" (except over Ethernet TCP/IP, called open-mbus). Today Modbus is managed by the Modbus Organization.

Modbus Plus: A proprietary specification of Schneider Electric, normally implemented using a custom chipset. This is not a variant of Modbus. It is a different protocol, involving token passing.

Modulator demodulator unit (MODEM): Is a network hardware device that modulates one or more carrier wave signals to encode digital information for transmission and demodulation that demodulates signals to decode the transmitted information. The goal is to produce a signal that can be transmitted easily and decoded to reproduce the original digital data. Modems can be used with any means of transmitting analog signals, from light emitting diodes to radio. A common type of modem is one that turns the digital data of a computer into modulated electrical signal for transmission over telephone lines and demodulated by another modem at the receiver side to recover the digital data.

Mote: A sensor node in a wireless sensor network that is capable of performing some processing, gathering sensory information, and communicating with other connected nodes in the network. A mote is a node, but a node is not always a mote. Motes focus on providing the longest wireless range (dozens of km), the lowest energy consumption (a few uA) and the easiest development process for the user.

Motion control network: The network supporting the control applications that move parts in industrial settings, including sequencing, speed control, point-to-point control, and incremental motion.

Near field communication (NFC): A set of protocols that enable two electronic devices, one of which is usually a portable device such as a smartphone, to establish radio data communication with each other by bringing them closer than, typically, 4 inches from each other.

Network Access Control (NAC): A feature provided by some firewalls that allows access based on a user's credentials and the results of health checks performed on the telework client device.

Network Address Translation (NAT): A routing technology used by many firewalls to hide internal system addresses from an external network through use of an addressing schema.

Network front-end: Device implementing protocols that allow attachment of a computer system to a network.

Node (or network node): (1) Any device that is directly connected to the network, usually through Ethernet cable. Nodes include file servers and shared peripherals; the name used to designate a part of a network. This may be used to describe one of the links in the network, or a type of link in the network (for example, Host Node or Intercept Node). (2) A device that communicates using the CEA-709.1-C protocol and is connected to a CEA-709.1-C network.

Open-loop controller: A controller that does not use feedback to determine if its output has achieved the desired goal of the input. Also called a non-feedback controller.

Personal computer interconnect (PCI): An industry-standard bus used in PCs, workstations, and servers.

Piconet: A small Bluetooth network created on an ad hoc basis that includes two or more devices.

Profibus: A standard for field bus communication in automation technology.

Programmable logic controller (PLC): A digital computer used for automation of typically industrial electromechanical processes, such as control of machinery on factory assembly lines, building control systems, or light fixtures. PLCs are used in many machines, in many industries. PLCs are designed for multiple arrangements of digital and analog inputs and outputs, extended temperature ranges, immunity to electrical noise, and resistance to vibration and impact. Programs to control machine operation are typically stored in battery-backed-up or non-volatile memory. A PLC is an example of a “hard” real-time system since output results must be produced in response to input conditions within a limited time, otherwise unintended operation will result.

Process controller: A proprietary control system, typically rack-mounted, that processes sensor input, executes control algorithms, and computes actuator outputs. A process controller may either use feedback or it may be open loop, and control may be continuous or cause a sequence of discrete events. Processes can be characterized as one or more of the following forms:

- Discrete: Manufacturing, motion and packaging applications. Robotic assembly can be characterized as discrete process control. Most discrete manufacturing involves the production of discrete pieces of product, such as metal stamping.
- Batch: Some applications require that specific quantities of raw materials be combined in specific ways for particular durations to produce an end result. Examples are the production of food, beverages and medicine.
- Continuous: Often, a physical building control system is represented through variables that are smooth and uninterrupted in time. The control of the water temperature in a heating jacket, for example, is an example of continuous process control.
- Hybrid applications: These have elements of discrete, batch and continuous process control.

Protocol: A standard that specifies the format of data and rules to be followed in data communication and network environments. A set of rules (i.e., formats and procedures) to

implement and control some type of association (e.g., communication) between building control systems.

Protocol bridge: Translating one protocol to another, such as when TCP/IP traffic is converted to a proprietary control protocol such as Modbus.

Proximity sensor: A non-contact sensor with the ability to detect the presence of an object within a specified range.

Proxy: A proxy is an application that "breaks" the connection between client and server. The proxy accepts certain types of traffic entering or leaving a network and processes it and forwards it. This effectively closes the straight path between the internal and external networks making it more difficult for an attacker to obtain internal addresses and other details of the organization's internal network. Proxy servers are available for common Internet services; for example, a Hyper Text Transfer Protocol (HTTP) proxy used for web access, and a Simple Mail Transfer Protocol (SMTP) proxy used for e-mail. SOURCE: SP 800-44

Proxy agent: A software application running on a firewall or on a dedicated proxy server that is capable of filtering a protocol and routing it between the interfaces of the device.

Proxy server: A server that services the requests of its clients by forwarding those requests to other servers.

Push notification: A remote notifications feature. It is a highly efficient service for propagating information to intelligent, Internet-connected devices. Each device establishes an accredited and encrypted IP connection with the service and receives notifications over this persistent connection.

Radio frequency identification (RFID): A form of automatic identification and data capture (AIDC) that uses electric or magnetic fields at radio frequencies to transmit information.

Real-time operating system (RTOS): An operating system (OS) intended to serve real-time application process data as it comes in, typically without buffering delays. Processing time requirements is measured in tenths of seconds or shorter. A key characteristic of an RTOS is the level of its consistency concerning the amount of time it takes to accept and complete an application's task; the variability is jitter. A hard real-time operating system has less jitter than a soft real-time operating system. The chief design goal is not high throughput, but rather a guarantee of a soft or hard performance category. An RTOS that can usually or generally meet a deadline is a soft real-time OS, but if it can meet a deadline deterministically it is a hard real-time OS.

Relay: An electromechanical device that completes or interrupts an electrical circuit by physically moving conductive contacts. The resultant motion can be coupled to another mechanism such as a valve or a circuit breaker.

Remote I/O: A local area network designed to connect controllers to a variety of intelligent devices such as operator interfaces and AC or DC drives.

Remote terminal unit (RTU): A microprocessor-controlled electronic device that monitors analog and digital parameters and transmits data to the Central Monitoring Station. A RTU monitors and transmits values as input or output signals from I/O devices such as meters, pressure transducers, pump starter auxiliary contacts, and so forth, from within the SCADA System. Signals created from a device such as a water meter and sent to the RTU are called input signals. Signals created within the RTU and sent elsewhere are called output signals. Signals are of the following types:

- Digital: ON/OFF discrete signal such as an equipment contact closure wired to the isolated inputs of the RTU and is generally read as 0 or 1 in value. These values could be a RUN status from a pump starter auxiliary contact, pressure switch, and so forth.
- Analog: A continuous signal that changes smoothly over a given range is brought into the RTU via a 4 to 20 milliamp signal. These are real values such as water levels, pressure or turbidity and are not discrete signals such as ON/OFF.
- Counter: Pulse signals from flow meter or similar occurrence meters that count the number of times an event occurs.

Repeater: Hardware device that connects two network segments and retransmits information received on one side to the other.

Robust Security Network (RSN): A wireless security network that only allows the creation of Robust Security Network Associations (RSNAs).

Rogue device: An unauthorized node on a network.

Router: An electronic device connecting two or more networks that routes incoming data packets to the appropriate network by retransmitting signals received from one subnet onto the other.

RS-232: A standard for serial communication transmission of data. Many intelligent devices have an RS-232 port built into the device for troubleshooting by maintenance personnel, or to install software upgrades or patches. USB has largely displaced RS-232 from most of its peripheral interface roles.

SCADA server: The device that acts as the master controller in a SCADA system.

Scatternet: A type of ad hoc computer network consisting of two or more piconets. A chain of piconets created by allowing one or more Bluetooth devices to each be a slave in one piconet and act as the master for another piconet simultaneously. A scatternet allows several devices to be networked over an extended distance.

Segment: A “single” section of a network with a limited number of locally-powered devices (typically 64 devices) that contains no repeaters or routers. There is generally a limit on the number of devices on a segment, and this limit is dependent on the topology/media and

device type. For example, a TP/FT-10 segment with locally powered devices is limited to 64 devices, and a BACnet MS/TP segment is limited to 32 devices.

Sensor interface module (SIM): Interface between sensors such as occupancy sensors and the control system's network. Typically enables each sensor to be independently configured.

Smart meter: An electronic device that records consumption of electric energy in intervals of an hour or less and communicates that information at least daily back to the utility for monitoring and billing. Smart meters differ from traditional Automatic Meter Reading (AMR) in that smart meters enable two-way communications with the meter and the central system. Unlike home energy monitors, smart meters can gather data for remote reporting.

Solid-state relay (SSR): Provide a high degree of reliability, long life and reduced electromagnetic interference (EMI), together with fast response and high vibration resistance, as compared to an electromechanical relay (EMR). All the advantages of solid state circuitry, including consistency of operation and a typically longer usable lifetime because it has no moving parts to wear out or arcing contacts to deteriorate, which are primary causes of failure of an electromechanical relay.

Subnet: A logical grouping of up to 127 nodes, where the logical grouping is defined by node addressing. Each subnet is assigned a number that is unique within the domain.

Supervisory controller: A controller implementing a combination of supervisory logic (global control strategies or optimization strategies), scheduling, alarming, event management, trending, web services, or network management. Note this is defined by use; many supervisory controllers have the capability to also directly control equipment.

Supervisory gateway: A device that is both a supervisory controller and a gateway.

Transmission Control Protocol (TCP): TCP enables two hosts to establish a connection and exchange streams of data and ensures data delivery in the correct sequence.

Transmitter: Equipment that generates and transmits a message or signal.

Universal serial bus (USB): Standard for connecting electronic devices to a computer using a serial bus.

Universal software radio peripheral (USRP): A software-defined radio is an inexpensive hardware platform for software radio commonly used by research labs, universities, and hobbyists. A USRP can be used as a transmitter/receiver and decoder; an RFID reader; a GPS; a cellular GSM base station; a digital television (ATSC) decoder; and passive radar.

Utility Control System (UCS): A type of industrial control system. Used for field control of utility systems such as an electrical substation, sanitary sewer lift station, water pump station, and so forth. A UCS may include its own local front-end.

Valve: An in-line device in a fluid-flow system that can interrupt flow, regulate the rate of flow, or divert flow to another branch of the system. There are many different types and styles of valves, but all primarily serve the common purpose of balancing a system. Valve types include the following:

- Three-way valves. Most associated with constant volume systems, these devices are used to modulate water flow to the load without changing the constant volume of water flow to the system.
- Two-way valves. Most associated with variable speed/variable volume systems, these devices modulate flow to the load by changing the constant volume of water flow to the system.
- Manual balancing valves. These have an adjustable orifice that can be changed by hand to provide a specific pressure drop and flow.
- Flow-limiting valves. These valves vary the flow based on differential pressure to provide a specific flow rate.

Wide area network (WAN): A network that uses high-speed, long-distance communications technology (e.g., phone lines and satellites) to connect computers over long distances. Similar to a LAN, except that parts of a WAN are geographically separated, possibly in different cities or even on different continents. Telecommunications carriers are included in most WANs; very large WANs incorporate satellite stations or microwave towers.

Wi-Fi Direct: A Wi-Fi standard enabling devices to easily connect with each other without requiring a wireless access point.

Wireless Gigabit (WiGig): WiGig allows devices to communicate high performance wireless data, display and audio without wires at multi-gigabit speeds. WiGig tri-band enabled devices operate in the 2.4, 5 and 60 GHz bands and deliver data transfer rates up to 7 Gbit/s, while maintaining compatibility with existing Wi-Fi devices. The 60 GHz signal cannot typically penetrate walls but can propagate off reflections from walls, ceilings, floors and objects using beamforming built into the WiGig system. When roaming away from the main room the protocol can switch to make use of the other lower bands at a much lower rate, but which can propagate through walls.

General Glossary

Artifact: The digital remnants of a cyber-attack or incident activity. These could be software that was used by a hacker, a collection of tools, malicious code, logs, files, output from tools, or status of a control system after a cyber-attack. Examples range from Trojan-horse programs and computer viruses to programs that exploit vulnerabilities or objects of unknown type and purpose found on a compromised computer.

Attack: An attempt to gain unauthorized access to control system services, resources, or information, or an attempt to compromise control system integrity and availability.

Attack pattern: Similar cyber events or behaviors that may indicate that a cyber-attack is occurring or has occurred.

Attack sensing and warning (AS&W): Detection, correlation, identification, and characterization of intentional unauthorized activity with notification to decision makers so that an appropriate response can be developed. SOURCE: CNSSI-4009.

Attack signature: A specific sequence of events indicative of an unauthorized access attempt. A characteristic byte pattern used in malicious code or an indicator or set of indicators that allows the identification of malicious network activities. SOURCE: CNSSI-4009; SP 800-12.

Attack surface: The sum of all the attack vectors, where a hacker can attempt to enter or extract data from a control system.

Attack tools: Hackers use attack tools that leverage Google, Bing, and other search engines to find information and expose vulnerabilities of control systems.

Attack tree: A conceptual diagram showing how a computer system might be attacked by describing the threats and possible cyber-attacks to realize those threats. Cyber-attack trees lend themselves to defining an information assurance strategy and are increasingly being applied to industrial control systems and the electric power grid. Executing a strategy changes the attack tree.

Attack vectors: This is a path or means by which a hacker or cracker can gain access to a computer or network server in order to deliver a payload or malicious outcome. Ways in which your BCS or CMMS can be attacked:

- **Internet access**: If your BCS is connected, your network has already been scanned and mapped.
- **Wireless network**: If you use wireless devices on your BCS, it has already been scanned and mapped.
- **Insider threat**: Deliberate or inadvertent activity.
- **Direct-access attack**: Gaining physical access to a BCS network device.

- **Removable media**: USB, floppy, CD, laptop, anything that can connect directly to a BCS network device.
- **E-mail**: Malware delivered by phishing e-mail such as a virus, Trojan horse, worm.
- **Other networks**: A connection to the enterprise network can be one way to get into the BCS.
- **Supply chain**: If it's made overseas, it's probably got some hidden program you'll never find.
- **Improper installation or usage**: Deliberate or inadvertent activity.
- **Theft of equipment**: Lose a vital piece of equipment and your system can be left defenseless.
- **Cyber-drone**: A drone can monitor a facility seeking wireless signals such as from network printers.
- **Other**

Backdoor: Typically, unauthorized hidden software or hardware mechanism used to circumvent security controls.

Black holes (networking): Places in the network where incoming or outgoing traffic is silently discarded (or "dropped"), without informing the source that the data did not reach its intended recipient. When examining the topology of the network, the black holes themselves are invisible, and can only be detected by monitoring the lost traffic; hence the name. The most common form of black hole is simply an IP address that specifies a host machine that is not running or an address to which no host has been assigned. Even though TCP/IP provides means of communicating the delivery failure back to the sender via ICMP, traffic destined for such addresses is often just dropped. Note that a dead address will be undetectable only to protocols that are both connectionless and unreliable (e.g., UDP). Connection-oriented or reliable protocols (TCP, RUDP) will fail to connect to a dead address or will fail to receive expected acknowledgements.

Blinding: Generating network traffic that is likely to trigger many alerts in a short period of time, to conceal alerts triggered by a "real" attack performed simultaneously.

Block cipher: A symmetric key cryptographic algorithm that transforms one block of information at a time using a cryptographic key. For a block cipher algorithm, the length of the input block is the same as the length of the output block.

Byzantine fault: A fault presenting different symptoms to different observers.

Byzantine fault tolerance (BFT): The objective of BFT is to be able to provide the control system's service assuming there are not too many faulty components.

Client: A control system computer that requests and uses a service provided by a “server” computer. Sometimes the server may be a client of some other server.

Collision: Two or more distinct inputs produce the same output.

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Data breach: The unauthorized disclosure of sensitive information to a party that is not authorized to have the information.

Day Zero: The Day Zero or Zero Day is the day a new vulnerability is made known. In some cases, a “zero- day exploit” is referred to an exploit for which no patch is available yet.

Hash function: A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties:

- One-Way. It is computationally infeasible to find any input that maps to any pre-specified output.
- Collision Resistant. It is computationally infeasible to find any two distinct inputs that map to the same output.

Hash total: Value computed on data to detect error or manipulation.

Hash value: The result of applying a cryptographic hash function to data (e.g., a message).

Mesh network: A network topology in which each node relays data for the network. All mesh nodes cooperate in the distribution of data in the network. Mesh networks can relay messages using either a flooding technique or a routing technique. With routing, the message is propagated along a path by hopping from node to node until it reaches its destination. The network is typically quite reliable, as there is often more than one path between a source and a destination in the network.

Packet: A packet is the unit of data that is routed between an origin and a destination on the Internet or any other packet switched network.

Penetration test (pen test): A test methodology in which assessors, using all available documentation (e.g., system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system. Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability. The tools used for pen-testing can be

classified into two kinds—scanners and attackers. Some software/tools will show you the weak spots, some that show and attack.

Polling: A device requesting data from another device.

Ports (network): An interface for communicating with a computer program over a network.

Red/black concept: The careful segregation in cryptographic systems of signals that contain sensitive or classified plaintext information (red signals) from those that carry encrypted information, or ciphertext (black signals). Sometimes called the red-black architecture or red/black engineering. Encryption devices are often called blackers, because they convert red signals to black. Separation of electrical and electronic circuits, components, equipment, and systems that handle unencrypted information (red), in electrical form, from those that handle encrypted information (black) in the same form. SOURCE:

Residual risk: The remaining potential risk after all IT security measures are applied. There is a residual risk associated with each threat.

Rogue device: An unauthorized node on a network.

SCADA duration surface: Unlike most IT equipment found in a corporate network that is normally replaced every 2 to 3 years, a SCADA system typically has a “duration surface” of 25 years. This makes SCADA systems more vulnerable to persistent threats, allowing more time to develop exploits against these slow-changing systems.

System’s downtime: A planned interruption in building control system availability for scheduled building control system maintenance.

Trusted channel: A channel where the endpoints are known and data integrity is protected in transit. Depending on the communications protocol used, data privacy may be protected in transit. Examples include SSL, IPSEC, and secure physical connection.

Tunneling: Technology enabling one network to send its data via another network’s connections. Tunneling works by encapsulating a network protocol within packets carried by the second network.

Virtuous circle and vicious circle: A complex chains of events that reinforce themselves through a feedback loop. A virtuous circle has favorable results, while a vicious circle has detrimental results.

ANNEX B: Cyber – Physical Systems: Vulnerabilities and Testbeds

Key SCADA Components

The most important/critical components are:

- Sensors: They can be digital or analog and help users measure and collect data from various, usually remote locations. Sensor placement and allocation depends on the CPS complexity. Sensors can measure inputs (e.g. water filling up a tank) or outputs (e.g. pressure from the release of water). Digital sensors measure “discrete” inputs, or simple on/off signals. For example, digital sensors can tell you whether a light is on or an alarm has been tripped. Analog sensors can detect continuous changes at a site, and are often used for situations where an exact measurement is needed. Commons uses include checking water levels, temperature, and voltage.
- Conversion Units: These are connected to sensors and interpret the data collected. The conversion units convert the information they receive into digital information, which is then sent to the Master Units. The two most common types of conversion units used in a SCADA system are RTUs and PLCs.
    - RTUs (Remote Terminal Units) are electronic devices controlled by a microprocessor. Their main function is to interface a SCADA system with whatever objects or sensors the RTUs are connected to. Typically, they transmit information via wireless communication, and are considered best for functions covering a broad geographical area.
    - PLCs (Programmable Logic Controllers) or IEDs (Intelligent Electronic Devices) are ideal for situations requiring local control and automation, such as a factory setting. PLCs are essentially digital computers specially designed for output arrangements and multiple inputs. Sometimes they replace RTUs because of their versatility. PlCs can also control end devices like actuators.
- Master Units: The master unit is essentially the supervisory computer system. These units serve as the SCADA system’s central processor. They provide a human interface and automatically regulate the system based on information from the sensors. The Master Units are typically larger computer consoles, however several other SCADA components can be considered Master Units, such as software programs and HMIs (Human Machine Interface). HMIs are devices that allow an operator to view and interact with collected and processed data, usually through a graphical user interface. This interface is often used to perform tasks like collecting data, making reports, and sending out notifications. The HMI generally requests data from a data acquisition server, which is used to connect software services to conversion units out in the field (RTUs and PLCs). SCADA systems often also use a software service such as an Operational Historian. The Historian also requests data and creates a database of time-stamped data, available for auditing analysis of trends and other information related to the system’s processes over time.

- Communication Networks: The links between the RTUs, PLCs and Master Units. These include wired (telephone lines, WAN circuits, fiber-optic cables) and wireless connections (Wi-Fi, Bluetooth, radio, cellular, satellite).
- Communication Protocol: Protocols are important for ensuring communication between devices. Vendors often create specific protocols for their own products. Most of these are considered proprietary protocols, and only products created by that vendor use them (e.g. Seimens, Honeywell, Toshiba, Allen-Bradley, Mitsubishi, GE, Scheider Electric, Rockwell Automation etc.). There are also several non-proprietary protocols which are fairly common in SCADA systems:
    - Modbus was originally published in 1979 by a company called Modicon. It was created with industrial applications in mind, with the specific purpose of being used to connect PLCs/RTUs to a supervisory computer. Uses a Master/Slave topology. It is considered an industry standard and is widely accepted, despite having some shortcomings because it is very lightweight. It has difficulty handling large numbers (whether negative or positive) as the data limit is 253 bytes, and there is no way for field devices to report information unless it has been requested by the supervisory computer. There are, however, other Modbus variations (Modbus TCP, Modbus +) some of which can handle larger numbers and fix other problems found in the original protocol. Modbus has no encrpyption or other security measure implemented.
    - DNP (Distributed Network Protocol) is mainly used in utilities systems (like water or electricity), although it can be used in other industries. Similar to Modbus, DNP is typically used for communication between a master/supervisory computer and the devices in the field, such as RTUs and PLCs. It was specifically designed with reliability in mind, in order to protect against issues like electromagnetic interference and the aging of system components. It can hold 65000 devices under a single link. This protocol has gone through several changes and currently is widely employed in SCADA systems in its third version, DNP3. Like Modbus, DNP does not employ any security measures like encryption and authentication. DNPSec v5 has been developed in response to address security concerns such as spoofing, modification, replay attacks, and eavesdropping. However, this secure standard variant has yet to be widely accepted and implemented.
    - IEC 60870 (International Electrotechnical Commission 60780) is another set of standards sometimes used in SCADA systems. It is mostly used in power transmission and distribution systems, and is used in many countries around the world. Like Modbus and DNP, when IEC is used in a SCADA system application, it is generally to allow communication between RTUs, a supervisory computer and IEDs.
    - ICCP (Inter Control Center Protocol) The Inter-Control Center Protocol (ICCP) allows for data exchange over Wide Area Networks (WANs) between a utility control center and other control centers, other utilities, power pools, regional control centers, and Non-Utility Generators.
    - CIP (Common Industrial Protocol) with the following branches:

        - EtherNet/IP
        - CompoNet
        - ControlNet
        - DeviceNet
    - UCA, based on the Manufacturing Message Specification from ISO standard 9506
    - MMS, an implementation of Manufacturing Message Specification (MMS) protocol, an international standard (ISO 9506), dealing with messaging system for transferring real time process data and supervisory control information between networked field devices and/or computer applications.
    - OLE for Process Control (OPC)
    - PROFIBUS
    - Foundation Fieldbus H1

Security of modern SCADA systems

Early multi-site SCADA systems used closed communication networks, hard-wired electromechanical devices and propriety industrial communication protocols to control and monitor remote sites. Thus, such systems were somewhat more secure due to this limited connectivity. However, with time it has become more convenient, cost-effective (due to the recent software and hardware standardization trend) and reliable to connect them to the Internet and internal corporate networks and integrate information technology (IT) and computational capabilities with SCADA (Jain and Tripathi, 2013)(Amin et al., 2013). The benefits gained are multiple (Ostefeld, 2011):

- Shared Infrastructure: Business and SCADA systems in some cases share network (Metropolitan area or Wide Area) infrastructure to reduce the overall costs for leased or private lines
- Common architecture components such as network, database, and security can be managed by trained experts
- Cheaper Components: SCADA systems can use cheaper transmission control protocol/internet protocol (TCP/IP)-based components.
- Strategic Information Gains: Data for energy management, increased modeling capabilities with connections to LIMS/GIS databases, real-time water quality modeling, forecasting capability, management/regulatory reporting, and providing utility facility status information to Emergency Response Centers.
- Improved Overall Security Integration: Integration of physical security elements such as video monitoring with SCADA allows for 24/7 monitoring by SCADA operators

These innovations created the modern Networked Control Systems (NCSs) which are replacing old SCADA hardware at an increasing rate (Rasekh et al., 2016). However, Internet connections to modern SCADA induced new vulnerabilities: The benefits of using the Internet technology to carry SCADA communications come at the cost of compromised security since data transmission over the Internet can be an easy and prominent target for a cyber-attack. An attack can become matter of national security if these systems are power plants, water

treatment facilities, or other pieces of critical infrastructure. The vulnerabilities revolve around the following factors:

- SCADA systems were primarily designed with functionality rather than security (Ostefeld, 2011) (and unsurprisingly not with *internet* security) in mind in the first place and industrial communication protocols like DNP3 and Modbus, but also most other SCADA protocols, have no built-in security feature such as message authentication, which assures that a party to some computerized transaction is not an impostor, or data encryption
- Modern SCADA systems employ off-the-self IT devices and thus inherit their vulnerabilities(Amin et al., 2013)
- Open protocols enable possible cyber-attackers of the NCSs to learn about operations and commands (Amin et al., 2013)
- All sensor and control data is accessible to authorized users and operators via Internet or corporate network, thus making the NCSs subject to insider attack (Amin et al., 2013)
- The existence of organized cybercrime groups enhances attackers' capabilities to conduct intrusions into NCSs (Amin et al., 2013)

In fact, the threat posed to the critical infrastructure is far greater in terms of impact and scale of attack than common computer vulnerabilities (Queiroz et al., 2011), and many experts argue that the future of warfare will be organized cyber-attacks (Amin et al., 2013). Recent examples of cyber-attacks to SCADA/NCS systems and CIs include:

- An attack on a sewage treatment system in Maroochy Shire, Queensland, where 800 000 liters of raw sewage were released to spill out into local parks and rivers, causing death of marine life, stench, and discoloration of water (Queiroz et al., 2011)
- The Davis-Besse nuclear power plant in Oak Harbor, Ohio, was attacked by the Slammer SQL server worm, which disabled a safety monitoring system of the nuclear power plant for nearly 5 hours (Queiroz et al., 2011).
- Stuxnet, a worm that specifically targets NCSs (Falliere et al., 2011). Stuxnet is able to infect and reprogram PLCs and hide its activity by using a PLC rootkit. Some experts concluded that Stuxnet was specifically designed to damage nuclear power plants in Iran (Langner, 2013). More than 50 variants of Stuxnet are discovered in similar recent cyber-attacks (Zhu et al., 2011).

SCADA security vs IT Systems security

SCADA systems have many characteristics that differ from IT systems, including different risks and priorities. Thus, it is inherently difficult to implement the same security measures, traditionally engineered for IT systems, despite some similarities in hardware/protocols. By nature, SCADA/NCSs are hard real-time systems: a task (e.g. a command control) should be serviced by its deadline (Silberschatz et al., 2005); service after a deadline is not only

completely useless, but potentially harmful (Zhu et al., 2011) as cascading effects may take place. This differs from traditional soft real-time IT systems, which have less stringent time constraints (can endure significantly more latency). Latency in SCADA/NCSs may cause great loss of safety, threat to human life and complete physical system failure. Another issue is that timing task interruption and restarts for the physical processes prevents the use of encryption block algorithms commonly found in IT systems. Also, memory allocation is more critical in SCADA systems that in IT systems because devices operate years without rebooting, accumulating fragmentation. Other key technical challenges in security measures implementation revolve around the limitations of what can be installed and configured on the SCADA systems and the technical limitations of other components within the SCADA environment: The RTUs have limited computational capacity, limited memory and space capacity, and SCADA data transmission usually is very low (low bandwidth) (Jain and Tripathi, 2013).

Priorities also differ: For SCADA systems, 24/7 availability is top most priority followed by confidentiality and integrity. For IT systems, confidentiality is top most priority followed by integrity and availability (referred to as “CIA”)(Jain and Tripathi, 2013; Zhu et al., 2011) .The definitions of these priorities and how these affect security measures are as follows (Zhu et al., 2011):

- Availability: every SCADA component should be ready for use exactly when need and any outage/interruption/disruption is unacceptable. Security measures, such as the cryptographic system should not interfere with instant accessibility of operations and data in case of emergency.
- Confidentiality: Any unauthorized person should not have any information (layout maps, decryption keys, passwords etc.) related to the specific SCADA system. However, the continuous nature of operations and the simple, repetitive commands and messages employed are easy to predict.
- Integrity: requires data generated, transmitted, displayed and stored within a SCADA system to be genuine and intact without unauthorized intervention, including both its content, which may also include the header for its source, destination and time information besides the payload itself. The protocol implemented should prevent an adversary from constructing unauthentic messages, modifying messages that are in transit, reordering messages, replaying old messages, or destroying messages without detection.

Security goals for IT systems usually revolve around protecting the central host (server) and not an edge client. In contrast, PLCs, the typical edge client in SCADA, are equally (or even more, in life-threatening cases) important as a central host like the Operational Historian data server and should be protected (Zhu et al., 2011).

Taxonomy of SCADA cyber attacks

Cyber-attacks on SCADA/NCSs have a multitude of possible attack routes. These include Internet connections, corporate LAN, other control networks and the field devices. The most common attack vectors (path or means by which an attacker can gain access to a computer or network server in order to deliver a payload or malicious outcome (Ayala, 2016)) are (Zhu et al., 2011):

- Backdoors (unauthorized hidden software or hardware mechanism used to circumvent security controls (Ayala, 2016)) and security holes in network perimeter
- Vulnerabilities in common protocols
- Attacks on field devices through cyber means
- Database attacks like SQL injection (a type of input validation attack where SQL code is inserted into database-driven application queries to manipulate the database (Ayala, 2016))
- Communications hijacking and Man-in-the-middle attacks (a cyber-attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other (Ayala, 2016)).
- Cinderella attack on time provision and synchronization (a cyber-attack that disables security software by manipulating the network internal clock time so a security software license expires prematurely rendering the target network vulnerable to cyber-attack (Ayala, 2016))

As shown in Figure 101 an attacker through these attack vectors may have the purpose to interrupt, intercept, modify or fabricate data/messages or operations of the system. Thus, the attacker may accomplish any of the following outcomes:

- Feed bogus input data to a PLC by compromised sensors and/or exploited network link between PLC and sensors
- Manipulate output data to an actuator connected to a PLC due to compromised actuator and/or exploited network link between PLC and actuator
- Manipulate/exploit data of the Operational Historian
- Denial of Service (DOS): force the system to miss the deadlines of important task actions. Most SCADA use protocols that are extremely vulnerable to DOS (Modbus, DNP3).

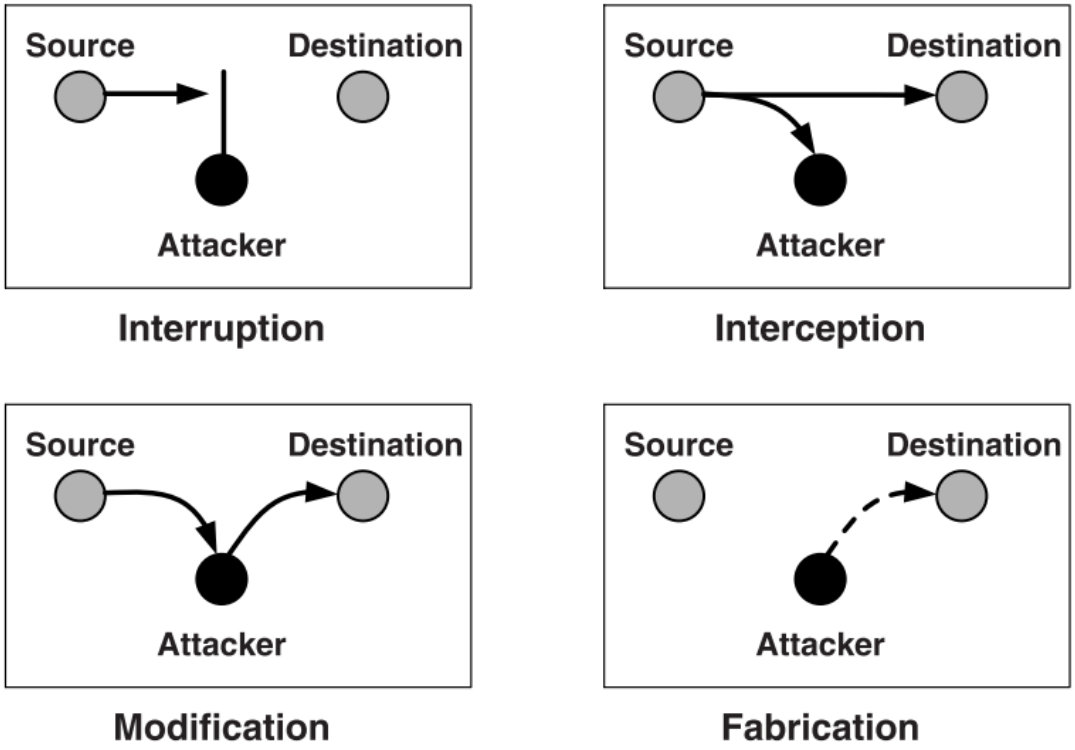


Figure 101: Possible threats to data/messages/operations of SCADA systems (East et al., 2009)

A hierarchical taxonomy of cyber-attacks can be visualized in Figure 102. The attacks on SCADA systems are classified by Zhu et al. (Zhu et al., 2011) in three main categories: attacks on hardware, attacks on software and attacks on the communication stack.

Attacks on hardware include unauthenticated remote access to devices and manipulation of their data, like changing threshold values for alarms, operations etc. Often this is performed with doorknob-rattling attacks (a hacker attempts a very few common username and password combinations on several computers resulting in very few failed login attempts. This attack can go undetected unless the data related to login failures from all the hosts are collected and aggregated to check for doorknob-rattling from any remote destination (Ayala, 2016)).

Attacks on software include exploits in vulnerabilities of specific software installed in the SCADA system like the database of the Operational Historian. Database manipulation is performed usually by SQL injection attacks as most databases use SQL language. If a command shell store procedure is enabled it is possible for an attacker to gain full control of the database and even execute operational commands. Another very common software vulnerability is induced buffer overflow as most SCADA software is written in C (format string, integer overflow etc.) as a means to corrupt a control program. Then, the system will behave unexpectedly. General methods of accomplishing it are stack smashing attacks (buffer overflow by tricking a computer into executing arbitrary code (Ayala, 2016)) and function

pointer attacks (buffer overflow by overwriting a function pointer or exception handler, which is subsequently executed (Ayala, 2016)). No privilege separation is another common vulnerability where monolithic kernels allow all tasks to run with high privileges and do not support memory protection between tasks.

Attacks on the communication stack can be broken down to four layers:

- Network layer:
  - Diagnostic Server Attacks (an attacker can execute the following attacks without any authentication required while maintaining stealthiness such as remote memory dump, remote memory patch, remote calls to functions and remote task management (Ayala, 2016)) through the UDP (User Datagram Protocol) back port.
  - Idle TCP Scan (consists of sending spoofed packets to a computer to find out what services are available. This is accomplished by impersonating another computer called a "zombie" (that is not transmitting or receiving information) and observing the behavior of the "zombie" system): Often a preparation step for an attack. Modbus and DNP3 are especially vulnerable to such attacks if running over TCP/IP.
  - Smurf: is a type of address spoofing, in general, by sending a continuous stream of modified Internet Control message Protocol(ICMP) packets to the target network with the sending address identical to one of the target computer addresses. If a PLC acts on the modified message, it may either crash or dangerously send out wrong commands to actuators.
  - Address Resolution Protocol (ARP) Spoofing/Poisoning: The ARP is primarily used to translate IP addresses to Ethernet Medium Access Control (MAC) addresses and to discover other connected interfaced device on the LAN. The ARP spoofing attack is to modify the cached address pair information. By sending fake ARP messages which contain false MAC addresses in SCADA systems, an attacker can confuse network devices, such as network switches. When these frames are sent to another node, packets can be sniffed; or to an unreachable host, DoS is launched; or intentionally to an host connected to different actuators, then physical disasters of different scales are initiated. Static MAC address is one of the counter measures. However, certain network switches do not allow static setting for a pair of MAC and IP address. Segmentation of the network may also be a method to alleviate the problem in that such attacks can only take place within same subnet.
  - Chain/Loop Attack: In a chain attack, there is a chain of connection through many nodes as the adversary moves across multiple nodes to hide own origin and identity. In case of a loop attack, the chain of connections is in a loop make it even harder to track down the origin in a wide SCADA system.
- Transport layer:

- Exploit vulnerabilities by a SYN Flood attack (a denial-of-service attack that sends a host more TCP SYN packets than the protocol can handle (Ayala, 2016))

- Application layer:
  - DNS forgery attack: a hacker with access to a network can easily forge responses to the computer's DNS requests (Ayala, 2016). The goal is to send a fake DNS reply with a matching source IP, destination port, request ID, but with an attacker manipulated information inside, so that this fake reply may be processed by the client before the real reply is received from the real DNS server.
  - SCADA specific attacks (e.g. attacks specific to DNP3)
- Attacks on specific implementation of protocols

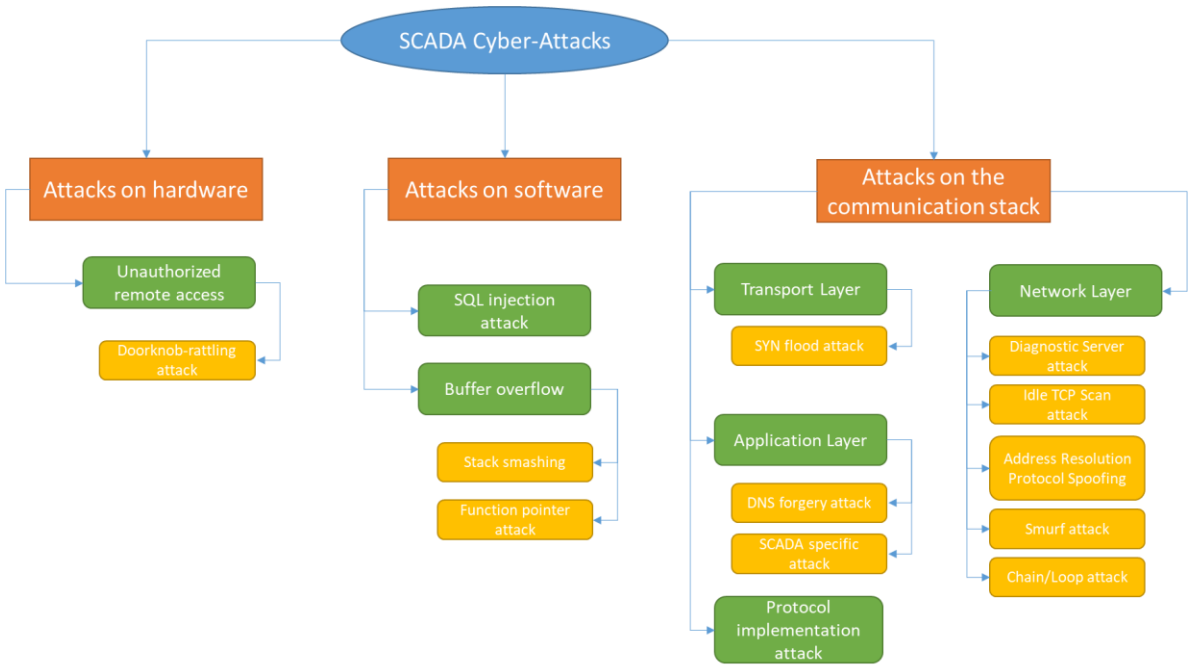


Figure 102: Taxonomy of common SCADA cyber-attacks, adapted from Zhu et al. (Zhu et al., 2011)

ANNEX C: Performance Indicators

Quantity of Supply Service

Indicator	UD & UD%		
Group	*KPI family*	*Dimension*	*Service level*
	Magnitude	Supply	Any
Description	Unmet demand is the total volume of supply not delivered to customers and its percentage against total volume of demand. UD% is complementary to Demand Satisfaction Ratio (DSR%) used by water companies. Where $D_{i,t}$ is the demand of node i at time t and $S_{i,t}$ its actual supply. N is the total number of demand nodes of the simulated network and T is the simulation duration.		
Formula	$$UD = \int_{t_0}^{T} (D - S) = \sum_{i=1}^{N} \sum_{t=t_0}^{T} (D_{i,t} - S_{i,t}) \quad (1)$$ $$UD_{\%} = \frac{\int_{t_0}^{T} (D - S)}{\int_{t_0}^{T} D} * 100\% = \frac{\sum_{i=1}^{N} \sum_{t=t_0}^{T} D_{i,t} - S_{i,t}}{\sum_{i=1}^{N} \sum_{t=t_0}^{T} D_{i,t}} * 100\% \quad (2)$$		

Indicator	ZS & ZS%		
Group	*KPI family*	*Dimension*	*Service level*
	Magnitude	Supply	Critical
Description	Interrupted supply is the total volume of supply not delivered to customers due to complete service interruption and its percentage against unmet demand. Where $ZS_{i,t} = \begin{cases} D_{i,t} \; for \; S_{i,t} \leq l * D_{i,t} \\ else \; 0 \end{cases}$ is the unmet demand due to supply below the low threshold percentage l of demand. We remind that supply below the lower threshold l is considered to be 0.		
Formula	$$ZS = \int_{t_0}^{T} ZS = \sum_{i=1}^{N} \sum_{t=t_0}^{T} ZS_{i,t} \quad (3)$$ $$ZS_{\%} = \frac{\int_{t_0}^{T} ZS}{UD} * 100\% = \frac{\sum_{i=1}^{N} \sum_{t=t_0}^{T} ZS_{i,t}}{\sum_{i=1}^{N} \sum_{t=t_0}^{T} (D_{i,t} - S_{i,t})} * 100\% \quad (4)$$		

Indicator	IS & IS%		
Group	*KPI family*	*Dimension*	*Service level*
	Magnitude	Supply	Moderate
Description	Supply insufficiency is the total volume of supply not delivered to customers due to only partial coverage of demand and its percentage against unmet demand. Where $IS_{i,t} = \begin{cases} (D_{i,t} - S_{i,t}) for\ h * D_{i,t} > S_{i,t} > l * D_{i,t} \\ else\ 0 \end{cases}$ is the unmet demand due to partial inadequacy of supply.		
Formula	$$IS = \int_{t_0}^{T} IS = \sum_{i=1}^{N} \sum_{t=t_0}^{T} IS_{i,t} \quad (5)$$ $$IS_{\%} = \frac{\int_{t_0}^{T} IS}{UD} = \frac{\sum_{i=1}^{N} \sum_{t=t_0}^{T} IS_{i,t}}{\sum_{i=1}^{N} \sum_{t=t_0}^{T} (D_{i,t} - S_{i,t})} * 100\% \quad (6)$$		

Indicator	$PF_{total\ supply}$		
Group	*KPI family*	*Dimension*	*Service level*
	Prevailing failure	Supply	Any
Description	Prevailing failure in total supply is the ratio of ZS and IS, used to detect the dominant type of failure in magnitude of supply.		
Formula	$$PF_{Total\ Supply} = \frac{ZS_{\%}}{IS_{\%}} \quad (7)$$		

Indicator	UD_{peak}		
Group	*KPI family*	*Dimension*	*Service level*
	Severity	Supply	Any
Description	Peak Unmet Demand is the peak temporal demand not supplied by the system during service hours		
Formula	$$UD_{peak} = \max_{t_0:T} \sum_{i=1}^{N} (D_{i,t} - S_{i,t}) \quad (8)$$		

Indicator	ZS_{peak}		
Group	*KPI family*	*Dimension*	*Service level*
	Severity	Supply	Critical
Description	Peak Interrupted Supply is the peak temporal demand not supplied by the system during service hours due to service interruption		
Formula	$$ZS_{peak} = \max_{t_0:T} \sum_{i=1}^{N} (ZS_{i,t})$$ (9)		

Indicator	IS_{peak}		
Group	*KPI family*	*Dimension*	*Service level*
	Severity	Supply	Moderate
Description	Peak Supply Insufficiency is the peak temporal demand not supplied by the system during service hours due to insufficient supply		
Formula	$$IS_{peak} = \max_{t_0:T} \sum_{i=1}^{N} (IS_{i,t})$$ (10)		

Indicator	$PF_{peak\ supply}$		
Group	*KPI family*	*Dimension*	*Service level*
	Prevailing failure	Supply	Any
Description	Prevailing failure in peak supply is the ratio of peak temporal effect to supply, used to detect the dominant type of failure in terms of severity.		
Formula	$$PF_{peak} = \frac{ZS_{peak}}{IS_{peak}}$$ (11)		

Indicator	UD_{PAR}		
Group	*KPI family*	*Dimension*	*Service level*
	PAR	Supply	Any
Description	The peak to average ratio of demand not met by the system for any type of service level. Where $\overline{UD}$ is the mean unmet demand, excluding 0 values, over the failure duration.		
Formula	$$UD_{PAR} = \frac{UD_{peak}}{\overline{UD}} \quad (12)$$		

Indicator	ZS_{PAR}		
Group	*KPI family*	*Dimension*	*Service level*
	PAR	Supply	Critical
Description	The peak to average ratio of demand not met by the system due to service interruption. Where $\overline{ZS}$ is the mean unmet demand due to service interruption, excluding 0 values, over the failure duration.		
Formula	$$ZS_{PAR} = \frac{ZS_{peak}}{\overline{ZS}} \quad (13)$$		

Indicator	TAN & $TAN\%$		
Group	*KPI family*	*Dimension*	*Service level*
	Magnitude	Nodes	Any
Description	Total affected nodes is the total number of nodes that experienced services below expectations for even 1 time during service hours and the percentage of total network's nodes they represent. Where $TAN_{i,T} = \begin{cases} 1 \; for \; S_{i,T} < h * D_{i,T} \\ else \; 0 \end{cases}$ is a logical index for the entire simulation duration T.		
Formula	$$TAN = \sum_{i=1}^{N} TAN_{i,T} \quad (14)$$		

	$$TAN\% = \frac{TAN}{N} * 100\% \quad (15)$$

Indicator	$\boldsymbol{TFN}$ & $\boldsymbol{TFN}\%$		
Group	*KPI family*	*Dimension*	*Service level*
	Magnitude	Nodes	Critical
Description	The total number of nodes that were cut-off supply for even 1 time during service hours and the percentage of total network's nodes (N) they represent. Where $TFN_{i,T} = \begin{cases} 1 \; for \; S_{i,T} < l * D_{i,T} \\ else \; 0 \end{cases}$ is a logical index for the entire simulation duration T.		
Formula	$$TFN = \sum_{i=1}^{N} TFN_{i,T} \quad (16)$$ $$TFN\% = \frac{TFN}{N} * 100\% \quad (17)$$		

Indicator	$\boldsymbol{TIN}$ & $\boldsymbol{TIN}\%$		
Group	*KPI family*	*Dimension*	*Service level*
	Magnitude	Nodes	Moderate
Description	The total number of nodes that were insufficiently supplied for even 1 time during service hours and the percentage of network's nodes (N) they represent. Where $TIN_{i,T} = \begin{cases} 1 \; for \; l * D_{i,T} < S_{i,T} < h * D_{i,T} \\ else \; 0 \end{cases}$ is a logical index for the entire simulation duration T.		
Formula	$$TIN = \sum_{i=1}^{N} TIN_{i,T} \quad (18)$$ $$TIN\% = \frac{TIN}{N} * 100\% \quad (19)$$		

Indicator	$PF_{Total\ nodes}$		
Group	*KPI family*	*Dimension*	*Service level*
	Prevailing Failure	Nodes	Any
Description	Prevailing failure in total spatial extent is the ratio of nodes cut-off and only partially supplied, used to detect the dominant type of failure in terms of magnitude.		
Formula	$PF_{Total\ nodes} = \frac{TFN}{TIN}$ (20)		

Indicator	$\overline{AN}$ & $\overline{AN}$%		
Group	*KPI family*	*Dimension*	*Service level*
	Propagation	Nodes	Any
Description	The average number of nodes of the system that experience supply failure over the failure time. Where $AN_{i,t} = \begin{cases} 1\ if\ S_{i,t} < h * D_{i,t} \\ else\ 0 \end{cases}$ is a logical index of affected node (1=affected and 0=not affected) and $t_{At} = \begin{cases} 0\ if\ \sum_{i=1}^{N} AN_t = 0 \\ else\ 1 \end{cases}$ is a logical index of the timestep where system is affected		
Formula	$\overline{AN} = \frac{\sum_{t=t_0}^{T} \sum_{i=1}^{N} AN_{i,t}}{\sum_{t=t_0}^{T} t_{At}}$ (21) $\overline{AN_{\%}} = \frac{\overline{AN}}{N}$ (22)		

Indicator	$\overline{FN}$ & $\overline{FN}$%		
Group	*KPI family*	*Dimension*	*Service level*
	Propagation	Nodes	Critical
Description	The average number of nodes of the system that experience supply cut-off over the failure time. Where $FN_{i,t} = \begin{cases} 1\ if\ S_{i,t} < l * D_{i,t} \\ else\ 0 \end{cases}$ is a logical index of node cut-off (1=affected and 0=not affected) and $t_{ft} = \begin{cases} 0\ if\ \sum_{i=1}^{N} FN_t = 0 \\ else\ 1 \end{cases}$ is a logical index of the timestep where system has nodes cut-off		

Formula	$\overline{FN} = \frac{\sum_{t=t_0}^{T}\sum_{i=1}^{N} FN_{i,t}}{\sum_{t=t_0}^{T} t_{ft}}$ (23) $\overline{FN}_{\%} = \frac{\overline{FN}}{N}$ (24)

Indicator	$\overline{IN}$ & $\overline{IN}$%		
Group	*KPI family*	*Dimension*	*Service level*
	Propagation	Nodes	Moderate
Description	The average number of nodes of the system that experience partial demand satisfaction over the failure time. Where $IN_{i,t} = \begin{cases} 1 \; if \; l * D_{i,t} < S_{i,t} < h * D_{i,t} \\ else \; 0 \end{cases}$ is a logical index of node partially supplied (1=affected and 0=not affected) and $t_{it} = \begin{cases} 0 \; if \; \sum_{i=1}^{N} IN_t = 0 \\ else \; 1 \end{cases}$ is a logical index of the timestep where system has nodes only partially supplied		
Formula	$\overline{IN} = \frac{\sum_{t=t_0}^{T}\sum_{i=1}^{N} IN_{i,t}}{\sum_{t=t_0}^{T} t_{it}}$ (25) $\overline{IN}_{\%} = \frac{\overline{IN}}{N}$ (26)		

Indicator	$PF_{\overline{nodes}}$		
Group	*KPI family*	*Dimension*	*Service level*
	Prevailing Failure	Nodes	Any
Description	Prevailing failure in average spatial extent is the ratio of average nodes cut-off and only partially supplied, used to detect the dominant type of failure in terms of propagation		
Formula	$PF_{\overline{nodes}} = \frac{\overline{FN}}{\overline{IN}}$ (27)		

Indicator	AN_{peak}		
Group	*KPI family*	*Dimension*	*Service level*
	Severity	Nodes	Any
Description	The maximum number of nodes simultaneously experiencing supply service failure.		
Formula	$AN_{peak} = \max_{t_0:T} \sum_{i=1}^{N} AN_{i,t}$ (28)		

Indicator	FN_{peak}		
Group	*KPI family*	*Dimension*	*Service level*
	Severity	Nodes	Critical
Description	The maximum number of nodes being simultaneously out of service. Where $FN_{i,t} = \begin{cases} 1 \; if \; S_{i,t} < l * D_{i,t} \\ else \; 0 \end{cases}$		
Formula	$FN_{peak} = \max_{t_0:T} \sum_{i=1}^{N} FN_{i,t}$ (29)		

Indicator	IN_{peak}		
Group	*KPI family*	*Dimension*	*Service level*
	Severity	Nodes	Moderate
Description	The maximum number of nodes simultaneously experiencing only partial demand satisfaction. Where $IN_{i,t} = \begin{cases} 1 \; if \; l * D_{i,t} < S_{i,t} < h * D_{i,t} \\ else \; 0 \end{cases}$		
Formula	$IN_{peak} = \max_{t_0:T} \sum_{i=1}^{N} IN_{i,t}$ (30)		

Indicator	$PF_{Peak\ nodes}$		
Group	*KPI family*	*Dimension*	*Service level*
	Prevailing Failure	Nodes	Any
Description	Prevailing failure in peak spatial extent is the ratio of nodes cut-off and only partially supplied, used to detect the dominant type of failure in terms of severity.		
Formula	$$PF_{Peak\ nodes} = \frac{FN_{peak}}{IN_{peak}}$$ (31)		

Indicator	AN_{PAR}		
Group	*KPI family*	*Dimension*	*Service level*
	PAR	Nodes	Any
Description	The peak to average ratio of node with supply not met for any type of service level.		
Formula	$$AN_{PAR} = \frac{AN_{peak}}{\overline{AN}}$$ (32)		

Indicator	FN_{PAR}		
Group	*KPI family*	*Dimension*	*Service level*
	PAR	Nodes	Critical
Description	The peak to average ratio of nodes with unmet demand due to service interruption		
Formula	$$FN_{PAR} = \frac{FN_{peak}}{\overline{FN}}$$ (33)		

Indicator	IN_{PAR}		
Group	*KPI family*	*Dimension*	*Service level*
	PAR	Nodes	Moderate
Description	The peak to average ratio of nodes only partially supplied by the system		
Formula	$IN_{PAR} = \frac{IN_{peak}}{\overline{IN}}$ (34)		

Indicator	AC		
Group	*KPI family*	*Dimension*	*Service level*
	Magnitude	Customers	Any
Description	The total number of customers that experienced services below expectations. Where $AC_{i,t} = \begin{cases} C_{i,t} \; if \; D_{i,t} > S_{i,t} \geq 0 \\ else \; 0 \end{cases}$ is the number of customers affected in each node in time t.		
Formula	$AC = \sum_{i=1}^{N} \max_{t_0:T}(AC_{i,t})$ (35)		

Indicator	FC		
Group	*KPI family*	*Dimension*	*Service level*
	Magnitude	Customers	Critical
Description	The total number of customers that experienced service interruption. Where $FC_{i,t} \begin{cases} C_{i,t} \; for \; S_{i,t} \leq l * D_{N,t} \\ else \; 0 \end{cases}$ is the number of customers experiencing 0-supply conditions in node i at time t.		
Formula	$FC = \sum_{i=1}^{N} \max_{t_0:T}(FC_{i,t})$ (36)		

Indicator	IC		
Group	*KPI family*	*Dimension*	*Service level*
	Magnitude	Customers	Moderate
Description	The total number of customers that experienced partial supply service. Where $IC_{i,t}\begin{cases} C_{i,t} \; for \; l * D_{i,t} < S_{i,t} < h * D_{i,t} \\ else \; 0 \end{cases}$ is the number of customers experiencing partial inadequacy of supply in node i at time t.		
Formula	$$IC = \sum_{i=1}^{N} \max_{t_0:T}(IC_{i,t})$$ (37)		

Indicator	$PF_{Total\ Customers}$		
Group	*KPI family*	*Dimension*	*Service level*
	Prevailing Failure	Customers	Any
Description	Prevailing failure in total number of customers dimension is the ratio of customers experiencing cut-off and only partially supplied, used to detect the dominant type of failure in terms of magnitude.		
Formula	$$PF_{Total\ customers} = \frac{FC}{IC}$$ (38)		

Indicator	AC_{peak}		
Group	*KPI family*	*Dimension*	*Service level*
	Severity	Customers	Any
Description	The maximum number of customers simultaneously experiencing supply service failure.		
Formula	$$AC_{peak} = \max_{t_0:T} \sum_{i=1}^{N} AC_{i,t}$$ (39)		

Indicator	FN_{peak}		
Group	*KPI family*	*Dimension*	*Service level*
	Severity	Customers	Critical
Description	The maximum number of customers being simultaneously out of service		
Formula	$$FC_{peak} = \max_{t_0:T} \sum_{i=1}^{N} FC_{i,t}$$ (40)		

Indicator	IN_{peak}		
Group	*KPI family*	*Dimension*	*Service level*
	Severity	Customers	Moderate
Description	The maximum number of customers simultaneously experiencing only partial demand satisfaction		
Formula	$$IC_{peak} = \max_{t_0:T} \sum_{i=1}^{N} IC_{i,t}$$ (41)		

Indicator	$PF_{Peak\ customers}$		
Group	*KPI family*	*Dimension*	*Service level*
	Prevailing Failure	Customers	Any
Description	Prevailing failure in number of customers simultaneously affected is the ratio of customers cut-off and only partially supplied, used to detect the dominant type of failure in terms of severity.		
Formula	$$PF_{Peak\ customers} = \frac{FC_{peak}}{IC_{peak}}$$ (42)		

Indicator	AC_{PAR}		
Group	*KPI family*	*Dimension*	*Service level*
	PAR	Customers	Any
Description	The peak to average ratio of customers with supply not met for any type of service level.		
Formula	$AC_{PAR} = \frac{AC_{peak}}{\overline{AC}}$ (43)		

Indicator	FC_{PAR}		
Group	*KPI family*	*Dimension*	*Service level*
	PAR	Customers	Critical
Description	The peak to average ratio of customers with unmet demand due to service interruption		
Formula	$FC_{PAR} = \frac{FC_{peak}}{\overline{FC}}$ (44)		

Indicator	IC_{PAR}		
Group	*KPI family*	*Dimension*	*Service level*
	PAR	Customers	Moderate
Description	The peak to average ratio of customers only partially supplied by the system		
Formula	$IC_{PAR} = \frac{IC_{peak}}{\overline{IC}}$ (45)		

Indicator	$\overline{AC}$		
Group	*KPI family*	*Dimension*	*Service level*
	Propagation	Customers	Any
Description	The average number of customers in the system that experience supply failure over the failure time. Where $AN_{i,t} = \begin{cases} 1 \ if \ S_{i,t} < h * D_{i,t} \\ else \ 0 \end{cases}$ is a logical index of affected node (1=affected and 0=not affected) and $t_{At} = \begin{cases} 0 \ if \ \sum_{i=1}^{N} AN_t = 0 \\ else \ 1 \end{cases}$ is a logical index of the timestep where system is affected		
Formula	$$\overline{AC} = \frac{\sum_{i=1}^{N} \sum_{t=t_0}^{T} \frac{AC_{i,t}}{t_{Ai}}}{\sum_{t=t_0}^{T} AN_t} \quad (46)$$		

Indicator	$\overline{FC}$		
Group	*KPI family*	*Dimension*	*Service level*
	Propagation	Customers	Critical
Description	The average number of customers in the system that experience supply cut-off over the failure time. Where $FN_{i,t} = \begin{cases} 1 \ if \ S_{i,t} < l * D_{i,t} \\ else \ 0 \end{cases}$ is a logical index of node cut-off (1=affected and 0=not affected) and $t_{Ft} = \begin{cases} 0 \ if \ \sum_{i=1}^{N} FN_t = 0 \\ else \ 1 \end{cases}$ is a logical index of the timestep where system has nodes cut-off		
Formula	$$\overline{FC} = \frac{\sum_{i=1}^{N} \sum_{t=t_0}^{T} \frac{FC_{i,t}}{t_{Fi}}}{\sum_{t=t_0}^{T} FN_t} \quad (47)$$		

Indicator	$\overline{IC}$		
Group	*KPI family*	*Dimension*	*Service level*
	Propagation	Customers	Moderate
Description	The average number of customers in the system that experience partial demand satisfaction over the failure time. Where $IN_{i,t} = \begin{cases} 1 \ if \ l * D_{i,t} < S_{i,t} < h * D_{i,t} \\ else \ 0 \end{cases}$ is a logical index of node partially supplied (1=affected and 0=not affected) and $t_{It} = \begin{cases} 0 \ if \ \sum_{i=1}^{N} IN_t = 0 \\ else \ 1 \end{cases}$ is a logical index of the timestep where system has nodes only partially supplied		

Formula	$\overline{IC} = \frac{\sum_{i=1}^{N}\sum_{t=t_0}^{T}\frac{IC_{i,t}}{t_{Ii}}}{\sum_{t=t_0}^{T} IN_t}$ (48)

Indicator	$\overline{PF_{customers}}$		
Group	*KPI family*	*Dimension*	*Service level*
	Prevailing Failure	Customers	Any
Description	Prevailing failure in average affect in customers dimension is the ratio of average customers experiencing cut-off and only partially supplied, used to detect the dominant type of failure in terms of propagation		
Formula	$\overline{PF_{customers}} = \frac{\overline{FC}}{\overline{IC}}$ (49)		

Indicator	$\boldsymbol{SAT}$ & $\boldsymbol{SAT}\%$		
Group	*KPI family*	*Dimension*	*Service level*
	Magnitude	Time	Any
Description	System Affected Time is the total duration the system services below expectations to even 1 node and its percentage against service hours. Where Δt_t is the timestep and and $t_{At} = \begin{cases} 0 \; if \; \sum_{i=1}^{N} AN_t = 0 \\ else \; 1 \end{cases}$ is a logical index of the timestep where system is affected		
Formula	$SAT = \sum_{i=1}^{N}\sum_{t=t_0}^{T} t_{At} * \Delta t_t$ (50) $SAT_{\%} = \frac{T_A}{T} * 100\%$ (51)		

Indicator	SDT & $SDT\%$		
Group	*KPI family*	*Dimension*	*Service level*
	Magnitude	Time	Critical
Description	System Down Time is the total duration the system services are interrupted to even 1 node and its percentage against service hours. Where Δt_t is the timestep and and $t_{Ft} = \begin{cases} 0 \; if \; \sum_{i=1}^{N} FN_t = 0 \\ else \; 1 \end{cases}$ is a logical index of the timestep where system is experiencing supply interruption		
Formula	$$SDT = \sum_{i=1}^{N} \sum_{t=t_0}^{T} t_{Fi,t} * \Delta t_t \quad (52)$$ $$SDT_{\%} = \frac{T_F}{T_A} * 100\% \quad (53)$$		

Indicator	SIT & $SIT\%$		
Group	*KPI family*	*Dimension*	*Service level*
	Magnitude	Time	Moderate
Description	The total duration the system services are only partially satisfying demand to even 1 node and its percentage against service hours. Where Δt_t is the timestep and and $t_{It} = \begin{cases} 0 \; if \; \sum_{i=1}^{N} FN_t = 0 \\ else \; 1 \end{cases}$ is a logical index of the timestep where system is experiencing supply service inadequacy		
Formula	$$SIT = \sum_{i=1}^{N} \sum_{t=t_0}^{T} t_{Ii,t} * \Delta t_t \quad (54)$$ $$SIT_{\%} = \frac{T_I}{T_A} * 100\% \quad (55)$$		

Indicator	$PF_{duration}$		
Group	*KPI family*	*Dimension*	*Service level*
	Prevailing Failure	Time	Any
Description	Prevailing failure in dimension of time is the ratio between SDT and SIT, used to explore the prevailing failure in terms of duration (magnitude).		
Formula	$$PF_{duration} = \frac{SDT}{SIT}$$ (56)		

Indicator	NAT		
Group	*KPI family*	*Dimension*	*Service level*
	Propagation	Time/Nodes	Any
Description	The average duration of failure per affected node		
Formula	$$NAT = \frac{\sum_{i=1}^{N}\sum_{t=t_0}^{T} t_{Ai}}{AN}$$ (57)		

Indicator	NDT		
Group	*KPI family*	*Dimension*	*Service level*
	Propagation	Time/Nodes	Critical
Description	The average duration of service interruption per affected node		
Formula	$$NDT = \frac{\sum_{i=1}^{N}\sum_{t=t_0}^{T} t_{Fi}}{FN}$$ (58)		

Indicator	NDT		
Group	KPI family	Dimension	Service level
	Propagation	Time/Nodes	Moderate
Description	The average duration of service insufficiency per affected node		
Formula	$NIT = \frac{\sum_{i=1}^{N} \sum_{t=t_0}^{T} t_{Ii}}{IN}$ (59)		

Indicator	CML		
Group	KPI family	Dimension	Service level
	Magnitude	Time/Customers	Critical
Description	The total customer minutes the system has not been able to supply services due to interruption		
Formula	$CML = \sum_{i=1}^{N} \sum_{t_0}^{T} C_{i,t} * t_{Fi,t} * \Delta t$ (60)		

Indicator	RCML		
Group	KPI family	Dimension	Service level
	Magnitude	Time/Customers	Moderate
Description	The total customer minutes the system has not been able to completely satisfy demand due to supply inadequacy (partial satisfaction)		
Formula	$RCML = \sum_{i=1}^{N} \sum_{t_0}^{T} C_{i,t} * t_{It} * \Delta t$ (61)		

Indicator	$\overline{CDT}$		
Group	*KPI family*	*Dimension*	*Service level*
	Propagation	Time/Customers	Critical
Description	The average duration of service interruption per affected customer		
Formula	$\overline{CDT} = \sum_{i=1}^{N} \sum_{t=t_0}^{T} \frac{C_{i,t} * t_{Fi,t} * \Delta t_t}{FC_i}$ (62)		

Indicator	$\overline{CIT}$		
Group	*KPI family*	*Dimension*	*Service level*
	Propagation	Time/Customers	Moderate
Description	The average duration of service inadequacy per affected customer		
Formula	$\overline{CIT} = \sum_{i=1}^{N} \sum_{t=t_0}^{T} \frac{C_{i,t} * t_{Fi,t} * \Delta t_t}{IC_i}$ (63)		

Indicator	TEP		
Group	*KPI family*	*Dimension*	*Service level*
	TEP	Any	Any
Description	The time between the initialization of threat event t_e and the time peak temporal value (t_{peak}) occurs.		
Formula	$TEP = t_{peak} - t_e$ (64)		

Indicator	TEC		
Group	*KPI family*	*Dimension*	*Service level*
	TEC	Any	Any
Description	The time between the initialization of threat event t_e and the time user defined critical state ($t_{critical}$) occurs. If critical state is not reached, $TEP = NaN$		
Formula	$$TEC = t_{critical} - t_e \quad (65)$$		

Indicator	TER		
Group	*KPI family*	*Dimension*	*Service level*
	TER	Any	Any
Description	The time between the end of threat event t_a and the time system service is restored t_R.		
Formula	$$TER = t_a - t_R \quad (66)$$		

Quality of Supply Service

Indicator	VLQS & VLQS%		
Group	*KPI family*	*Dimension*	*Service level*
	Magnitude	Supply	Any
Description	$VLQS$ is the total volume of sub-standard water delivered to the system's customers. $D_{i,t}$ is the demand of node i at time t and $PQS_{i,t}$ is the supply of water that meets the quality criteria set for c concentration of substance examined: $PQS_{i,t} = \begin{cases} S_{i,t} \; if \; c_{i,t} < c_p \\ else \; 0 \end{cases}$ N is the total number of demand nodes of the simulated network and T is the simulation duration. The percentage form of the ratio between the desired and sub-standard supply is expressed as $VLQS_{\%}$.		
Formula	$$VLQS = \int_{t_0}^{T} (D - PQS) = \sum_{i=1}^{N} \sum_{t=t_0}^{T} (D_{i,t} - PQS_{i,t}) \quad (1)$$ $$VLQS_{\%} = \frac{\int_{t_0}^{T} (D - PQS)}{\int_{t_0}^{T} D} * 100\% = \frac{\sum_{i=1}^{N} \sum_{t=t_0}^{T} (D_{i,t} - PQS_{i,t})}{\sum_{i=1}^{N} \sum_{t=t_0}^{T} D_{i,t}} * 100\% \quad (2)$$		

Indicator	VPS & VPS%		
Group	*KPI family*	*Dimension*	*Service level*
	Magnitude	Supply	Critical
Description	VPS, volume of polluted supply, is the volume of potentially unsafe/life-threatening supplied water by the company. In the expression, $PS_{i,t} = \begin{cases} S_{i,t} \; for \; c_{i,t} \geq c_{f_{i,t}} \\ else \; 0 \end{cases}$ is the supply in node i at time t of polluted water with substance concentration c above the upper threshold of excessive concentration c_f considered potentially life threatening. The ratio of supplied polluted water is given against the total volume of low-quality supplied water is $VPS_{\%}$.		
Formula	$$VPS = \int_{t_0}^{T} PS = \sum_{i=1}^{N} \sum_{t=t_0}^{T} PS_{i,t} \quad (3)$$ $$VPS_{\%} = \frac{\int_{t_0}^{T} PS}{VLQS} * 100\% = \frac{\sum_{i=1}^{N} \sum_{t=t_0}^{T} PS_{i,t}}{\sum_{i=1}^{N} \sum_{t=t_0}^{T} (D_{i,t} - PQS_{i,t})} * 100\% \quad (4)$$		

Indicator	$VSQS$ & $VSQS\%$		
Group	*KPI family*	*Dimension*	*Service level*
	Magnitude	Supply	Moderate
Description	Sub-Standard Quality Supply ($VSQS$) is the total volume of water supplied to customers that exceeded permissible (by legislation or standards) concentration c_p, but is still safe (not life-threatening) for use by the customers. In the expressions $SQS_{i,t} = \begin{cases} S_{i,t} \; for \; c_{f_{i,t}} > c_{i,t} \geq c_{p_{i,t}} \\ else \; 0 \end{cases}$ is the sub-standard quality supply of node i at time t. The ratio of supplied sub-standard quality water is given against the total volume of low-quality supplied water is $VSQS_{\%}$		
Formula	$$VSQS = \int_{t_0}^{T} SQS = \sum_{i=1}^{N} \sum_{t=t_0}^{T} SQS_{i,t} \quad (5)$$ $$VSQS_{\%} = \frac{\int_{t_0}^{T} SQS}{VLQS} * 100\% = \frac{\sum_{i=1}^{N} \sum_{t=t_0}^{T} SQS_{i,t}}{\sum_{i=1}^{N} \sum_{t=t_0}^{T} (D_{i,t} - PQS_{i,t})} * 100\% \quad (6)$$		

Indicator	$PF_{Supply\ quality}$		
Group	*KPI family*	*Dimension*	*Service level*
	Prevailing Failure	Supply	Any
Description	The ratio of Prevailing Failure (PF) in supply quality is a direct indication for the dominance of pollution in the supply chain of the water network.		
Formula	$$PF_{Supply\ quality} = \frac{VPS}{VSQS} \quad (7)$$		

Indicator	LQS_{peak}		
Group	*KPI family*	*Dimension*	*Service level*
	Severity	Supply	Any
Description	Low Quality Supply peak (LQS_{peak}) is the peak temporal value of low quality supplied water.		

Formula	$LQS_{peak} = \max_{t_0:T} \sum_{i=1}^{N} (D_{i,t} - PQS_{i,t})$ (8)

Indicator	PS_{peak}		
Group	*KPI family*	*Dimension*	*Service level*
	Severity	Supply	Critical
Description	Polluted Supply peak (PS_{peak}) is the peak temporal value of polluted supplied water.		
Formula	$PS_{peak} = \max_{t_0:T} \sum_{i=1}^{N} (PS_{i,t})$ (9)		

Indicator	SQS_{peak}		
Group	*KPI family*	*Dimension*	*Service level*
	Severity	Supply	Moderate
Description	Sub-standard Quality Supply peak (SQS_{peak}) is the peak temporal value of sub-standard quality supplied water.		
Formula	$SQS_{peak} = \max_{t_0:T} \sum_{i=1}^{N} (SQS_{i,t})$ (10)		

Indicator	$PF_{quality\ peak}$		
Group	*KPI family*	*Dimension*	*Service level*
	Prevailing Failure	Supply	Any
Description	Prevailing Failure peak ($PF_{quality\ peak}$) is the ratio between Polluted Supply peak (PS_{peak}) and Sub-standard Quality Supply peak (SQS_{peak}) and demonstrates the prevailing failure in terms of severity.		
Formula	$PF_{quality\ peak} = \frac{PS_{peak}}{SQS_{peak}}$ (11)		

Indicator	LQS_{PAR}		
Group	*KPI family*	*Dimension*	*Service level*
	PAR	Supply	Any
Description	Low Quality Supply Peak to Average Ratio (LQS_{PAR}) exresses the ratio of peak to average failure in meeting quality threshold		
Formula	$$LQS_{PAR} = \frac{LQS_{peak}}{\overline{LQS}} \quad (12)$$		

Indicator	PS_{PAR}		
Group	*KPI family*	*Dimension*	*Service level*
	PAR	Supply	Critical
Description	Polluted Supply Peak to Average Ratio (LQS_{PAR}) exresses the ratio of peak to average failure in meeting quality threshold		
Formula	$$PS_{PAR} = \frac{PS_{peak}}{\overline{PS}} \quad (13)$$		

Indicator	SQS_{PAR}		
Group	*KPI family*	*Dimension*	*Service level*
	PAR	Supply	Moderate
Description	Sub-standard Quality Supply Peak to Average Ratio (LQS_{PAR}) exresses the ratio of peak to average failure in meeting quality threshold		
Formula	$$SQS_{PAR} = \frac{SQS_{peak}}{\overline{SQS}} \quad (14)$$		

Indicator	$\overline{LQN}$ & $\overline{LQN}_{\%}$		
Group	*KPI family*	*Dimension*	*Service level*

	Propagation	Nodes	Any
Description	Mean Low Quality Nodes $\overline{LQN}$ expresses the mean number of nodes supplied with low quality water over the failure duration. In the expression $LQN_{i,t} = \begin{cases} 1 \; if \; c_{i,t} > c_p \\ else \; 0 \end{cases}$ is a logical index of nodes supplied with low-quality water (1=affected and 0=not affected) and $t_{LQt} = \begin{cases} 0 \; if \; \sum_{i=1}^{N} LQN_t = 0 \\ else \; 1 \end{cases}$ is a logical index of the timesteps where system is supplying low-quality water or not. The ratio of Mean Low Quality Nodes to all nodes of the system is expressed as $\overline{LQN}_{\%}$.		
Formula	$$\overline{LQN} = \frac{\sum_{t=t_0}^{T} \sum_{i=1}^{N} LQN_{i,t}}{\sum_{t=t_0}^{T} t_{LQt}} \quad (15)$$ $$\overline{LQN}_{\%} = \frac{\overline{LQN}}{N} * 100\% \quad (16)$$		

Indicator	$\overline{PN}$ **&** $\overline{PN}_{\%}$		
Group	*KPI family*	*Dimension*	*Service level*
	Propagation	Nodes	Critical
Description	Mean Polluted Nodes ($\overline{PN}$) expresses the mean number of nodes supplied with polluted water over the failure duration. In the expression $PN_{n,t} = \begin{cases} 1 \; for \; c_{i,t} \geq c_f \\ else \; 0 \end{cases}$ is a logical index of nodes supplied with polluted water (1=polluted and 0=not affected) and $t_{Pt} = \begin{cases} 0 \; if \; \sum_{i=1}^{N} PN_t = 0 \\ else \; 1 \end{cases}$ is a logical index of the timesteps where system is supplying low-quality water or not. The ratio of Mean Polluted Nodes to all nodes of the system is expressed as $\overline{PN}_{\%}$.		
Formula	$$\overline{PQN} = \frac{\sum_{t=t_0}^{T} \sum_{i=1}^{N} PN_{i,t}}{\sum_{t=t_0}^{T} t_{LQt}} \quad (17)$$ $$\overline{PQN}_{\%} = \frac{\overline{PN}}{N} * 100\% \quad (18)$$		

Indicator	$\overline{SQN}$ **&** $\overline{SQN}_{\%}$		
Group	*KPI family*	*Dimension*	*Service level*
	Propagation	Nodes	Moderate
Description	Mean Sub-standard Quality Nodes ($\overline{SQN}$) expresses the mean number of nodes supplied with low quality water over the failure duration. In the expression $SQN_{i,t} = \begin{cases} 1 \; for \; c_p < c_{i,t} < c_f \\ else \; 0 \end{cases}$ is a logical index of sub-standard supplied nodes (1= sub-standard supply and 0=not affected) and $t_{SQt} = \begin{cases} 0 \; if \; \sum_{i=1}^{N} SQN_t = 0 \\ else \; 1 \end{cases}$ is a logical index of the timesteps where system is supplying sub-standard -quality water or not. The ratio of Mean Sub-standard Quality Nodes to all nodes of the system is expressed as $\overline{SQN}_{\%}$.		

Formula	$\overline{SQN} = \frac{\sum_{t=t_0}^{T}\sum_{i=1}^{N} SQN_{i,t}}{\sum_{t=t_0}^{T} t_{LQt}}$ (19) $\overline{SQN}_{\%} = \frac{\overline{SQN}}{N} * 100\%$ (20)

Indicator	PF_{Qnodes}		
Group	*KPI family*	*Dimension*	*Service level*
	Prevailing Failure	Nodes	Any
Description	Prevailing Failure of Quality Nodes ($PF_{quality\ peak}$) is the ratio between Mean Polluted Nodes ($\overline{PN}$) and Mean Sub-standard Quality Nodes ($\overline{SQN}$) and demonstrates the prevailing failure spatial characteristics.		
Formula	$PF_{Qnodes} = \frac{\overline{PN}}{\overline{SQN}}$ (21)		

Indicator	LQN_{peak}		
Group	*KPI family*	*Dimension*	*Service level*
	Severity	Nodes	Critical
Description	Maximum number of nodes with low quality of supplied water that are simultaneously affected (LQN_{peak}) is a measure of the threat's temporary spatial extremity.		
Formula	$LQN_{peak} = \max_{t_0:T} \sum_{i=1}^{N} LQN_{i,t}$ (22)		

Indicator	PN_{peak}		
Group	*KPI family*	*Dimension*	*Service level*
	Severity	Nodes	Any
Description	Maximum number of polluted nodes that are simultaneously affected (PN_{peak}) is a measure of the threat's temporal spatial extremity.		
Formula	$PN_{peak} = \max_{t_0:T} \sum_{i=1}^{N} PN_{i,t}$ (23)		

Indicator	SQN_{peak}		
Group	*KPI family*	*Dimension*	*Service level*
	Severity	Nodes	Any
Description	Maximum number of nodes supplied with water of sub-standard quality that are simultaneously affected (SQN_{peak}) is a measure of the threat's temporal spatial extremity.		
Formula	$$SQN_{peak} = \max_{t_0:T} \sum_{i=1}^{N} SQN_{i,t} \quad (24)$$		

Indicator	$PF_{peak\ nodes}$		
Group	*KPI family*	*Dimension*	*Service level*
	Prevailing Failure	Nodes	Any
Description	Prevailing Failure of maximum number of nodes ($PF_{peak\ nodes}$) is the ratio between maximum number of polluted nodes (PN_{peak}) and maximum number of sub-standard nodes (SQN_{peak}) and demonstrates spatial severity of the impact.		
Formula	$$PF_{Qnodes} = \frac{PN_{peak}}{SQN_{peak}} \quad (25)$$		

Indicator	LQN_{PAR}		
Group	*KPI family*	*Dimension*	*Service level*
	PAR	Nodes	Any
Description	Low Quality Node Peak to Average Ratio (LQN_{PAR}) exresses the ratio of maximum number of nodes to the average number of nodes in failure duration failing to meet quality threshold.		
Formula	$$LQN_{PAR} = \frac{LQN_{peak}}{\overline{LQN}} \quad (26)$$		

Indicator	PN_{PAR}		
Group	*KPI family*	*Dimension*	*Service level*
	PAR	Nodes	Critical
Description	Polluted Node Peak to Average Ratio (PN_{PAR}) exresses the ratio of maximum number of nodes to the average number of nodes in failure duration with polluted supply.		
Formula	$$PN_{PAR} = \frac{PN_{peak}}{\overline{PN}} \quad (27)$$		

Indicator	SQN_{PAR}		
Group	*KPI family*	*Dimension*	*Service level*
	PAR	Nodes	Moderate
Description	Sub-standard Node Peak to Average Ratio (SQN_{PAR}) the ratio of maximum number of nodes to the average number of nodes in failure duration with sub-standard quality supply.		
Formula	$$SQN_{PAR} = \frac{SQN_{peak}}{\overline{SQN}} \quad (28)$$		

Indicator	TLQN & TLQN%		
Group	*KPI family*	*Dimension*	*Service level*
	Magnitude	Nodes	Any
Description	$TLQN$ is the total number of nodes that are supplied with low quality water. The percentage form of the ratio is expressed as $TLQN_{\%}$. In the expression, $TLQN_{i,T} = \begin{cases} 1 \; for \; c_{i,t} > c_p \\ else \; 0 \end{cases}$ is a logical index for the entire simulation duration T. If node i has experienced supply with concentration higher than permissible for <u>any</u> step of the simulation, then the node is added to the list of affected system nodes		
Formula	$$TLQN = \sum_{i=1}^{N} TLQN_{i,T} \quad (29)$$ $$TLQN\% = \frac{TLQN}{N} * 100\% \quad (30)$$		

Indicator	TPN & $TPN\%$		
Group	*KPI family*	*Dimension*	*Service level*
	Magnitude	Nodes	Critical
Description	TPN is the total number of nodes that are supplied with polluted water. The percentage form of the ratio is expressed as $TPN_{\%}$. In the expression, $TPN_{i,T} = \begin{cases} 1 \; for \; c_{i,t} > c_f \\ else \; 0 \end{cases}$ is a logical index for the entire simulation duration T.		
Formula	$$TPN = \sum_{i=1}^{N} TPN_{i,T} \quad (31)$$ $$TPN\% = \frac{TPN}{N} * 100\% \quad (32)$$		

Indicator	$TSQN$ & $TSQN\%$		
Group	*KPI family*	*Dimension*	*Service level*
	Magnitude	Nodes	Moderate
Description	$TSQN$ is the total number of nodes that are supplied with sub-standard quality water. The percentage form of the ratio is expressed as $TSQN_{\%}$. In the expression, $TSQN_{i,T} = \begin{cases} 1 \; for \; c_{f_{i,t}} > c_{i,t} \geq c_{p_{i,t}} \\ else \; 0 \end{cases}$ is a logical index for the entire simulation duration T.		
Formula	$$TPN = \sum_{i=1}^{N} TPN_{i,T} \quad (33)$$ $$TPN\% = \frac{TPN}{N} * 100\% \quad (34)$$		

Indicator	$PF_{Total\ nodes}$		
Group	*KPI family*	*Dimension*	*Service level*
	Prevailing Failure	Nodes	Any
Description	Prevailing failure in total spatial extent is the ratio of total nodes supplied with polluted water and sub-standard quality, used to detect the dominant type of failure in terms of magnitude.		
Formula	$$PF_{Total\ nodes} = \frac{TPN}{TSQN} \quad (35)$$		

Indicator	LQC		
Group	*KPI family*	*Dimension*	*Service level*
	Magnitude	Customers	Any
Description	The number of customers that were serviced with, and therefor consumed, water of lower-quality than expected. Where $LQC_{i,t} = \begin{cases} C_{i,t} \; if \; c_{i,t} > c_p \\ else \; 0 \end{cases}$ is the number of customers serviced with low-quality water in each node in time t.		
Formula	$$LQC = \sum_{i=1}^{N} \max_{t_0:T}(LQC_{i,t})$$ (36)		

Indicator	PC		
Group	*KPI family*	*Dimension*	*Service level*
	Magnitude	Customers	Any
Description	The number of customers that were serviced with, and therefor consumed, polluted water. Where $PC_{i,t} \begin{cases} C_{i,t} \; if \; c_{i,t} > c_e \\ else \; 0 \end{cases}$ is the number of customers experiencing supply of polluted water in node i at time t.		
Formula	$$PC = \sum_{i=1}^{N} \max_{t_0:T}(PC_{i,t})$$ (37)		

Indicator	SQC		
Group	*KPI family*	*Dimension*	*Service level*
	Magnitude	Customers	Any
Description	The number of customers that were serviced with, and therefor consumed, sub-standard quality water. Where $SQC_{i,t} \begin{cases} C_{i,t} \; for \; c_p < c_{i,t} < c_e \\ else \; 0 \end{cases}$ is the number of customers supplied with water of sub-standard quality in node i at time t.		

Formula	$SQC = \sum_{i=1}^{N} \max_{t_0:T}(SQC_{i,t})$ (38)

Indicator	$PF_{Total\ Customers}$		
Group	*KPI family*	*Dimension*	*Service level*
	Prevailing Failure	Customers	Any
Description	Prevailing failure in total number of customers dimension is the ratio of customers supplied with polluted and sub-standard quality water, used to detect the dominant type of failure in terms of magnitude.		
Formula	$PF_{Customers} = \frac{PC}{SQC}$ (39)		

Indicator	$\overline{LQC}$		
Group	*KPI family*	*Dimension*	*Service level*
	Propagation	Customers	Any
Description	Mean Low Quality supplied Customers $\overline{LQC}$ expresses the mean number of customers supplied with low quality water over the failure duration. In the expression $LQN_{i,t} = \begin{cases} 1\ if\ c_{i,t} > c_p \\ else\ 0 \end{cases}$ is a logical index of nodes supplied with low-quality water (1=affected and 0=not affected) and $t_{LQt} = \begin{cases} 0\ if\ \sum_{i=1}^{N} LQN_t = 0 \\ else\ 1 \end{cases}$ is a logical index of the timesteps where system is supplying low-quality water or not.		
Formula	$\overline{LQC} = \frac{\sum_{i=1}^{N}\sum_{t=t_0}^{T} \frac{LQC_{i,t}}{t_{LQi}}}{\sum_{t=t_0}^{T} LQN_t}$ (40)		

Indicator	$\overline{PC}$		
Group	*KPI family*	*Dimension*	*Service level*
	Propagation	Customers	Critical

Description	Mean Polluted Customers ($\overline{PC}$) expresses the mean number of customers supplied with polluted water over the failure duration. In the expression $PN_{n,t} = \begin{cases} 1 \; for \; c_{i,t} \geq c_f \\ else \; 0 \end{cases}$ is a logical index of nodes supplied with polluted water (1=polluted and 0=not affected) and $t_{Pt} = \begin{cases} 0 \; if \; \sum_{i=1}^{N} PN_t = 0 \\ else \; 1 \end{cases}$ is a logical index of the timesteps where system is supplying low-quality water or not.
Formula	$$\overline{PC} = \frac{\sum_{i=1}^{N} \sum_{t=t_0}^{T} \frac{PC_{i,t}}{t_{Pi}}}{\sum_{t=t_0}^{T} PN_t} \quad (41)$$

Indicator	$\overline{SQC}$		
Group	*KPI family*	*Dimension*	*Service level*
	Propagation	Customers	Moderate
Description	Mean Sub-standard Quality supplied Customers ($\overline{SQC}$) expresses the mean number of customers supplied with low quality water over the failure duration. In the expression $SQN_{i,t} = \begin{cases} 1 \; for \; c_p < c_{i,t} < c_f \\ else \; 0 \end{cases}$ is a logical index of sub-standard supplied nodes (1= sub-standard supply and 0=not affected) and $t_{SQt} = \begin{cases} 0 \; if \; \sum_{i=1}^{N} SQN_t = 0 \\ else \; 1 \end{cases}$ is a logical index of the timesteps where system is supplying sub-standard -quality water or not.		
Formula	$$\overline{SQC} = \frac{\sum_{i=1}^{N} \sum_{t=t_0}^{T} \frac{SQC_{i,t}}{t_{SQi}}}{\sum_{t=t_0}^{T} SQN_t} \quad (42)$$		

Indicator	LQC_{peak}		
Group	*KPI family*	*Dimension*	*Service level*
	Severity	Customers	Critical
Description	Maximum number of customers supplied with low quality water that are simultaneously affected (LQC_{peak}) is a measure of the threat's temporary spatial extremity.		
Formula	$$LQC_{peak} = \max_{t_0:T} \sum_{i=1}^{N} LQC_{i,t} \quad (43)$$		

Indicator	PC_{peak}		
Group	*KPI family*	*Dimension*	*Service level*
	Severity	Customers	Any
Description	Maximum number of customers that are simultaneously supplied with polluted water (PC_{peak}) is a measure of the threat's temporal spatial extremity.		
Formula	$$PC_{peak} = \max_{t_0:T} \sum_{i=1}^{N} PC_{i,t} \quad (44)$$		

Indicator	SQC_{peak}		
Group	*KPI family*	*Dimension*	*Service level*
	Severity	Customers	Any
Description	Maximum number of customers supplied with water of sub-standard quality that are simultaneously affected (SQC_{peak}) is a measure of the threat's temporal spatial extremity.		
Formula	$$SQC_{peak} = \max_{t_0:T} \sum_{i=1}^{N} SQC_{i,t} \quad (45)$$		

Indicator	$PF_{peak\ customers}$		
Group	*KPI family*	*Dimension*	*Service level*
	Prevailing Failure	Customers	Any
Description	Prevailing failure of peak customers is the ratio of customers supplied with polluted and sub-standard water, used to detect the dominant type of failure in terms of severity.		
Formula	$$PF_{Peak\ customers} = \frac{PC_{peak}}{SQC_{peak}} \quad (46)$$		

Indicator	LQC_{PAR}		
Group	*KPI family*	*Dimension*	*Service level*
	PAR	Customers	Any
Description	The peak to average ratio of customers with supply not meeting minimum requirements of quality		
Formula	$LQC_{PAR} = \frac{LQC_{peak}}{\overline{LQC}}$ (47)		

Indicator	PC_{PAR}		
Group	*KPI family*	*Dimension*	*Service level*
	PAR	Customers	Critical
Description	The peak to average ratio of customers supplied, and thus having consumed, polluted water		
Formula	$PC_{PAR} = \frac{PC_{peak}}{\overline{PC}}$ (48)		

Indicator	SQC_{PAR}		
Group	*KPI family*	*Dimension*	*Service level*
	PAR	Customers	Moderate
Description	The peak to average ratio of customers supplied, and thus having consumed, sub-standard, but not toxic, water		
Formula	$SQC_{PAR} = \frac{SQC_{peak}}{\overline{SQC}}$ (49)		

Indicator	LQT & $LQT\%$		
Group	*KPI family*	*Dimension*	*Service level*
	Magnitude	Time	Any
Description	Low Quality Time is the total duration the system services water with quality lower than expectations to even 1 node and its percentage against service hours. Where Δt_t is the timestep and and $t_{LQt} = \begin{cases} 0 \ if \ \sum_{i=1}^{N} LQN_t = 0 \\ else \ 1 \end{cases}$ is a logical index of the timestep where system is affected		
Formula	$$LQT = \sum_{i=1}^{N} \sum_{t=t_0}^{T} t_{LQt} * \Delta t_t \quad (50)$$ $$LQT_{\%} = \frac{LQT}{T} * 100\% \quad (51)$$		

Indicator	PT & $PT\%$		
Group	*KPI family*	*Dimension*	*Service level*
	Magnitude	Time	Critical
Description	System Polluted time is the total duration the system supply has excessive concentration of a species and supplies it to even 1 node and its percentage against LQT hours. Where Δt_t is the timestep and and $t_{Pt} = \begin{cases} 0 \ if \ \sum_{i=1}^{N} PN_t = 0 \\ else \ 1 \end{cases}$ the timestep logical index where the system supplies polluted water to at least 1 node.		
Formula	$$PT = \sum_{i=1}^{N} \sum_{t=t_0}^{T} t_{Pt} * \Delta t_t \quad (52)$$ $$PT_{\%} = \frac{PT}{LQT} * 100\% \quad (53)$$		

Indicator	SIT & $SIT\%$		
Group	*KPI family*	*Dimension*	*Service level*
	Magnitude	Time	Moderate
Description	Sub-standard time is the total duration the system supply has above permissible concentration (but not toxic concentrations) of a species and supplies it to even 1 node and its percentage against LQT hours. Where Δt_t is the timestep and and $t_{SQt} = \begin{cases} 0 \; if \; \sum_{i=1}^{N} SQN_t = 0 \\ else \; 1 \end{cases}$ the timestep logical index where the system has at least 1 node experiencing supply of sub-standard quality.		
Formula	$$SQT = \sum_{i=1}^{N} \sum_{t=t_0}^{T} t_{SQt} * \Delta t_t \quad (54)$$ $$SQT_{\%} = \frac{SQT}{LQT} * 100\% \quad (55)$$		

Indicator	$PF_{duration}$		
Group	*KPI family*	*Dimension*	*Service level*
	Prevailing Failure	Time	Any
Description	Prevailing failure in dimension of time is the ratio between PT and SQT, used to explore the prevailing failure in terms of duration (magnitude).		
Formula	$$PF_{duration} = \frac{PT}{SQT} \quad (56)$$		

Indicator	CMP		
Group	*KPI family*	*Dimension*	*Service level*
	Magnitude	Time/Customers	Critical
Description	The total customer minutes the system supplies with polluted water		

Formula	$$CMP = \sum_{i=1}^{N} \sum_{t_0}^{T} C_{i,t} * t_{Pi,t} * \Delta t \quad (57)$$

Indicator	***CMS***		
Group	*KPI family*	*Dimension*	*Service level*
	Magnitude	Time/Customers	Moderate
Description	The total customer minutes the system supplies with sub-standard quality, but not excessive concentration		
Formula	$$CMS = \sum_{i=1}^{N} \sum_{t_0}^{T} C_{i,t} * t_{SQt} * \Delta t \quad (58)$$		

Indicator	$\overline{CPT}$		
Group	*KPI family*	*Dimension*	*Service level*
	Propagation	Time/Customers	Critical
Description	The average duration of exposure to polluted supply per affected customer		
Formula	$$\overline{CPT} = \sum_{i=1}^{N} \sum_{t=t_0}^{T} \frac{C_{i,t} * t_{Pi,t} * \Delta t_t}{PC_i} \quad (59)$$		

Indicator	$\overline{CST}$		
Group	*KPI family*	*Dimension*	*Service level*
	Propagation	Time/Customers	Moderate
Description	The average duration of exposure to sub-standard supply per affected customer		
Formula	$\overline{CST} = \sum_{i=1}^{N} \sum_{t=t_0}^{T} \frac{C_{i,t} * t_{SQi,t} * \Delta t_t}{SQC_i}$ (60)		

Indicator	TEP		
Group	*KPI family*	*Dimension*	*Service level*
	TEP	Any	Any
Description	The time between the initialization of threat event t_e and the time peak temporal value (t_{peak}) occurs.		
Formula	$TEP = t_{peak} - t_e$ (61)		

Indicator	TEC		
Group	*KPI family*	*Dimension*	*Service level*
	TEC	Any	Any
Description	The time between the initialization of threat event t_e and the time user defined critical state ($t_{critical}$) occurs. If critical state is not reached, $TEP = NaN$		
Formula	$TEC = t_{critical} - t_e$ (62)		

Indicator	TER		
Group	*KPI family*	*Dimension*	*Service level*
	TER	Any	Any
Description	The time between the end of threat event t_a and the time system service is restored t_R.		
Formula	$TER = t_a - t_R$ (63)		

ANNEX D: Supplementary material for InfraRisk-CP

Input tables

Consequence classes

The consequences of each main event should be assessed in terms of consequence classes in Table 17. The classes are the same for all consequence dimensions, but the narrative description varies between consequence dimensions.

Table 17: Consequence classes for each consequence dimension.

Consequence dim.	Class	Description
Life & Health	(1) Delimited	Up to 5 fatalities, Up to 20 injured
	(2) Some damage	Up to 50 fatalities, Up to 200 injured
	(3) Serious	Up to 300 fatalities, Up to 1200 injured
	(4) Critical	Up to 1000 fatalities, Up to 4000 injured
	(5) Catastrophic	More than 1000 fatalities, More than 4000 injured
Environment	(1) Delimited	Minor environmental changes
	(2) Some damage	Major environmental changes
	(3) Serious	Moderate environmental injurious to health changes
	(4) Critical	Store environmental injurious to health changes
	(5) Catastrophic	Destruction of human habitat
Economy	(1) Delimited	Up to 0.01 % of GNP
	(2) Some damg.	Up to 0.1 % of GNP
	(3) Serious	Up to 1 % of GNP
	(4) Critical	Up to 10 % of GNP
	(5) Catastrophic	More than 10 % of GNP
Manageability	(1) Delimited	No or minor disturbances
	(2) Some damage	Short disturbances
	(3) Serious	Major disturbances
	(4) Critical	Serious disturbances
	(5) Catastrophic	Critical disturbances, permanent changes
Political Trust	(1) Delimited	No significant effects
	(2) Some damage	Passively constructive, loyalty, adoption

	(3) Serious	Actively constructive, disturbances, protest, demanding changes
	(4) Critical	Passively destructive, non-participation, substitutional behavior
	(5) Catastrophic	Actively destructive, political exit, violence, system de-legitimating, system change
Lifeline Quality	(1) Delimited	
	(2) Some damage	
	(3) Serious	
	(4) Critical	
	(5) Catastrophic	
Lifeline unavailability	(1) Delimited	
	(2) Some damage	
	(3) Serious	
	(4) Critical	
	(5) Catastrophic	

Table 18 below shows a consequence matrix for quality and life line unavailability.

Table 18: Consequence matrix, quality and delivery of service.

	0 - 6 hours	6 - 24 hours	1 - 7 days	1 - 4 weeks	One to 6 months	More than 6 months
1 - 10 persons	Delimited	Delimited	Delimited	Some Damages	Some Damages	Serious
10 - 100 persons	Delimited	Delimited	Some Damages	Some Damages	Serious	Serious
100 - 1 000 persons	Delimited	Some Damages	Some Damages	Serious	Serious	Critical
1 000 - 10 000 pesons	Some Damages	Some Damages	Serious	Serious	Critical	Critical
10 000 - 100 000 persons	Some Damages	Serious	Serious	Critical	Critical	Catastrophic
More than 100 000 persons	Serious	Serious	Critical	Critical	Catastrophic	Catastrophic

Risk matrix

A risk matrix is used to visualize the result. The format of the risk matrix is shown in Table 19. Separate matrixes may be established for each consequence dimension, i.e., personal safety, environment, economy etc. It is also possible to plot the worst risk dimension for each main event to get an overall overview of the various events. Each event is given a unique identifier, which is plotted in the cells of the risk matrixes to visualize more than one event at a time.

Table 19: Proposed calibration of the risk matrix.

Probability	5)	More than once a month	Low risk	Medium risk	High risk	Very high risk	Very high risk
	4)	1 to 10 times a year	Low risk	Medium risk	Medium risk	High risk	Very high risk
	3)	Once per 1-10 year	Very low risk	Low risk	Medium risk	Medium risk	High risk
	2)	Once per 10-100 year	Very low risk	Low risk	Low risk	Medium risk	Medium risk
	1)	Less than once per 100 year	Very low risk	Very low risk	Very low risk	Low risk	Medium risk
			(1) Delimited	(2) Some damage	(3) Serious	(4) Critical	(5) Catastrophic
			Consequences				

Table 20 shows main elements with corresponding codes. The number in parentheses shows the level in the hierarchical structure.

Table 20: Main events with codes

Event (1)	Event (2)	Event (3)	Event (4)	Code (1)	Code (2)	Code (3)	Code (4)
Natural event (N)	Meteorological (M)	Strong wind (1)	Storm, hurricane (1)	N	NM	NM1	NM11
			Whirlwind, tornado (2)	N	NM	NM1	NM12
		Flooding (2)	Seasonal flooding (1)	N	NM	NM2	NM21

			Storm flooding (2)	N	NM	NM2	NM22
			Spring flooding (3)	N	NM	NM2	NM23
		Extreme precipitation (3)	Rain (1)	N	NM	NM3	NM31
			Snow (2)	N	NM	NM3	NM32
			Drought (3)	N	NM	NM3	NM33
		Extreme temperature (4)	High temperature (1)	N	NM	NM4	NM41
			Low temperature (2)	N	NM	NM4	NM42
		Stroke of lightening (5)	Lightening (1)	N	NM	NM5	NM51
	Geological/Geotechnical (G)	Snow slide (1)	Snow slide over infrastructure (1)	N	NG	NG1	NG11
			Snow slide over buildings (2)	N	NG	NG1	NG12
		Landslide (2)	Land slide over infrastructure (1)	N	NG	NG2	NG21
			Land slide over buildings (2)	N	NG	NG2	NG22
			Land slide into water (3)	N	NG	NG2	NG23

		Earthquake (3)	Less than 5 Richter (1)	N	NG	NG3	NG31
			5 Richter or more (2)	N	NG	NG3	NG32
		Tsunami (4)	National impact (1)	N	NG	NG4	NG41
			Regional impact (2)	N	NG	NG4	NG42
		Volcanism (5)	Not in use (1)	N	NG	NG5	NG51
			National downfall fallout (2)	N	NG	NG5	NG52
		Calderac explosion (6)	Not in use(1)	N	NG	NG6	NG61
			Global impact, national downfall fallout (2)	N	NG	NG6	NG62
	Hit by cosmic objects (C)	Meteorite (asteroid) (1)	National impact (1)	N	NC	NC1	NC11
			Regional impact (2)	N	NC	NC1	NC12
			Global impact (3)	N	NC	NC1	NC13
		Comet (2)	Urban impact (1)	N	NC	NC2	NC21
			National impact (2)	N	NC	NC2	NC22

Medical / biological catastrophe (B)	Plants and animals (P)	Transferable disease (1)	Zoonotic (between humans and animals) (1)	B	BP	BP1	BP11
			Non-zoonotic (2)	B	BP	BP1	BP12
	Humans (H)	Pandemic (1)	Flu (1)	B	BH	BH1	BH11
			SARS (2)	B	BH	BH1	BH12
			Not in use (3)	B	BH	BH1	BH13
		Non pandemic (2)	Other diseases (1)	B	BH	BH2	BH21
Technical event (T)	Release of dangerous substances (D)	Chemical (1)		T	TD	TD1	
		Biological (2)		T	TD	TD2	
		Radiological (3)		T	TD	TD3	
		Other (4)		T	TD	TD4	
	Accident (A)	Fire, industrial (1)		T	TA	TA1	
		Explosion, Industrial (2)		T	TA	TA2	
		Transportation accident (3)		T	TA	TA3	
		Structural collapse (4)		T	TA	TA4	

		ICT system failure (5)		T	TA	TA5	
		Other (6)		T	TA	TA6	
	Technical/ human failure in infrastructure (F)	Water supply (1)	Water source (1)	T	TF	TF1	TF11
			Waterworks and purification (2)	T	TF	TF1	TF12
			Pipelines (3)	T	TF	TF1	TF13
		Safe food (2)		T	TF	TF2	
		Sewage and refuse collection (3)	Sewer (1)	T	TF	TF3	TF31
			Surface Water (2)	T	TF	TF3	TF32
			Refuse collection (3)	T	TF	TF3	TF33
		Transportation services (4)		T	TF	TF4	
		Financial services (5)		T	TF	TF5	
		Energy supply (6)		T	TF	TF6	
		Communication (7)		T	TF	TF7	
Malicious acts (M)	Crime (C)	Organised crime (1)	Smuggling (1)	M	MC	MC1	MC11

			Drugs and weapon arm trade (2)	M	MC	MC1	MC12
			Trafficking (3)	M	MC	MC1	MC13
			Cybercrime (4)	M	MC	MC1	MC14
		Sabotage (2)	Attack against installations (1)	M	MC	MC2	MC21
			Forcible violent protest, "disturbance" (2)	M	MC	MC2	MC22
			Will full plundering (3)	M	MC	MC2	MC23
			Data hacking (4)	M	MC	MC2	MC24
		Espionage (3)	Political (1)	M	MC	MC3	MC31
			Military (2)	M	MC	MC3	MC32
			Industrial (3)	M	MC	MC3	MC33
	Terrorism (T)	Conventional terrorism (1)	Attack against persons (1)	M	MT	MT1	MT11
			Hostage-taking (2)	M	MT	MT1	MT12
			Explosives used against crowds (3)	M	MT	MT1	MT13
			Attack against	M	MT	MT1	MT14

			installations (4)				
		CBRN-terrorism (2)		M	MT	MT2	
	Dysfunctional behaviour (D)	Gangs (1)		M	MD	MD1	
		Individuals (2)		M	MD	MD2	

Table 21 shows code lists for societal critical functions relevant for water distribution systems. To be consistent with the RIDB structure the notations type of asset and specific asset are used.

Table 21: Code list for SCFs, water distribution systems

Type of asset	Specific asset	Code
Catchment area	Control center	C111
	Sensor	C112
	Transmission devices	C113
	Well	C114
Drinking water network	Control center	C121
	Control system	C122
	Dosing system	C123
	Drinking water pipes	C124
	Drinking water taps	C125
	Fire hydrants	C126
	Pump	C127
	Sensor	C128
	Spring water	C129
	Transferred information	C12A
	Tunnel	C12B
	Valve	C12C

Drinking water tanks	Control system	C131
	Drinking water tanks	C132
	Pump	C133
	Sensor	C134
	Transmission devices	C135
	Valve	C136
Pressure boosting station	Control system	C141
	Power transformer	C142
	Pressure boosting station	C143
	Sensor	C144
	Transferred information	C145
	Transmission devices	C146
Raw water bodies	Control system	C151
	Groundwater	C152
	Surface water	C153
Wastewater treatment plant	Control system	C161
	Power transformer	C162

Water treatment plant	Additives	C181
	Control system	C182
	Dosing system	C183
	Power transformer	C184
	Pump	C185
	Sensor	C186
	Transmission devices	C187
	Valve	C188
	Water under treatment	C189
Other	Media channels	C191
	Server	C192

Vulnerability factors

Vulnerability factors assessed in InfraRisk-CP with description of type and influences are given in Table 22.

Table 22: Vulnerability factors and their values

Vulnerability Factor	Influence	Comment
Area	(1) Minor	Open ground
	(2) Small	Transportation trace
	(3) Medium	Street in town, dens building mass, landslide risk area etc.
	(4) Huge	Close to dangerous installation, factors etc.
	(5) Very huge	Terminal for person traffic or tunnel
Geographic scope	(1) Local	+ neighborhood in large city or equivalent
	(2) City	+ Large city, major suburbia
	(3) Region	Limited to regions
	(4) National	+ Capital
	(5) International	If current country is affected

Population density pr 1 km²	(1) 1 - 4	Isolated village settlement
	(2) 5 - 29	Village settlement
	(3) 30 - 199	Open settlement
	(4) 200 - 499	Suburbia
	(5) 500 - 15200	Cities
Outdoor temperature	(1) +20 °C - +30 °C	No heating or cooling demand
	(2) +5 °C - + 20 °C	Some heating demand
	(3) -5 °C - +5 °C, > +30 °C	Significant heating or cooling demand
	(4) -20 °C - -5 °C	Large heating demand
	(5) < -20 °C	Heating critical for survival
Time of day	(1) Night	Silence
	(2) Evening	Most people are at home
	(3) Working hours	Most people are at work
	(4) Early morning	Early morning
	(5) Rush hours	From and to work, school, etc.
Duration	(1) < 1 day	Fast normalization
	(2) < 1 week	Normalization within weeks
	(3) > 1 month	Normalization takes more than one month
	(4) > 6 months	Normalization takes up to one year
	(5) Quasi permanent	Years or decades to normalize
Dependency with other social critical functions	(1) Very little	Small dependencies
	(2) Little	Medium asymmetric dependencies
	(3) Medium	Medium symmetric dependencies
	(4) Huge	Strong Medium symmetric dependencies
	(5) Very huge	Strong symmetric dependencies
Substitution opportunities for infrastructure	(1) Very huge	Easy substitution

	(4) Huge	Substitution with some problems
	(3) Medium	Substitution requires significant effort
	(4) Little	Substitution difficult
	(5) Very little	Indispensability
Degree of coupling	(1) Very little	Anarchism
	(2) Little	Simple set of rules sufficient for activity functions
	(3) Medium	Complex set of rules sufficient for activity functions
	(4) Huge	Operative governing functions necessary
	(5) Very huge	Strong centralized governed with small tolerance for deviations
Culture	(1) Very favourable	Frankness, humility, real competence, honesty
	(2) Favourable	Cooperation climate, looks for opportunities, consciousness
	(3) Medium	Caution, delays, naivety
	(4) Unfavourable	Reluctance, anxiety, isolation
	(5) Very unfavourable	Power struggle, closed, dishonesty
Mental preparedness	(1) Very favourable	Frequent targeted training
	(2) Favourable	Significant effective measures
	(3) Medium	Good risk consciousness, some measures
	(4) Unfavourable	Under communicated risk
	(5) Very unfavourable	Lack of potential risk consciousness

Mapping of RIDB against InfraRisk CP

Adaptation into InfraRisk CP

The former InfraRisk method was found appropriate for analysing different societal safety challenges related to critical infrastructures in the DECRIS-project[1]. Therefore, STOP-IT choose to apply the main structure of this tool in developing the new InfraRisk CP. The main adaptation was to make the 'Main event'- and SCF hierarchies more related to water supply systems and water systems. Next, to identify those SCFs and components being affected by the cyber-attack threat. Of that reason the RIDB and the RRMD was natural background information for making the necessary amendments and/or adjustments in the tool. Adaptation of InfraRisk-CP to cyber-physical threats is outlined in the following:

The relation of RIDB and RRMD - databases to InfraRisk CP

The risk Identification database (RIDB) was developed earlier in the STOP-IT project (Ref D3.2). In addition, a risk reduction measure database is under development (Ref. D4.3). Based on the issued versions of the RIDB and RRMD databases, a comparison between the structure of these databases against the structure of the original InfraRisk was made. The generic information in RIDB and RRMD is independent of cite, network layout, water tanks, vulnerability factors and so on. Table 23 shows the mapping of RIDB against InfraRisk CP. Based on this mapping, a recommendation regarding the field names in InfraRisk-CP is given in the same Table below.

Table 23: Mapping of the RIDB against InfraRIsk-CP

No	RIDB	Entry	InfraRIsk-CP
1	Event ID	Consecutive number	InfraRisk CP: Event ID
2	Type of source	External attacker External supplier Human fault Interdependent CI Internal attacker Natural phenomena	Some adjustment is required for the code list in InfraRisk CP InfraRisk CP: Main Event = Type of source
3	Type of threat	Cyber Cyber-physical Physical	Type of threat is added, i.e. the relation to cyber InfraRisk CP: Cyber
4	Type of event	Destruction Interruption Manipulation Pollution	Type of event is added with some additional entries for completeness.

			InfraRisk CP: Type
5	Specific asset	Additives Control center Control system Dosing system Drinking water pipes Drinking water tanks Drinkinkg water taps Fire hydrants Groundwater Media channels Power transformer Pressure boosting station Pump Sensor Server Spring water Surface water Transferred information Transmission devices Valve Water under treatment Well	Some amendments in order to make the relevant scenario combinations in InfraRIsk CP. InfraRisk CP: Specific asset at SCF level four.
6	Type of Asset	Catchment area Drinking water network Drinking water tanks Pressure boosting station Raw water bodies Wastewater treatment plant Water abstraction points Water treatment plants	Outline of the SCFs, level 3.The type of asset list used in RIDB is a subset of the SCF list in InfraRisk CP. InfraRisk CP: Type of asset
7	Consequence	Financial Quality Quantity Reputation	In RIDB only one consequence dimension is given for each event. In InfraRisk-CP more than one consequence dimension could be given.

			InfraRisk CP: Several consequence dimensions
8	General description	A short description of the risk event (fixed sentence structure). See section 2.4.2 of the D3.2 (RIDB report).	In InfraRisk-CP this is a free text field, in RIDB predefined values are given. InfraRisk CP: General description
9	Example	Free text entry with further characterization of the risk event	InfraRisk CP: None. However, predefined examples from RIDB may be viewed for the 81 RIDB events.
10	Severity	Blank column that can be used by used to prioritize the events according their specific conditions (see severity matrix)	Assigning severity for consequences in InfraRisk-CP by use of Pr (C|E) and scale for each of the consequence dimensions.

The RRMD has been included as a separate table in InfraRisk CP. The user of InfraRisk-CP may choose one or more measures from the RRMD for a given risk element. Some pre-processing was required to ensure that only relevant measures for a given risk element are shown.

Diagram RAET

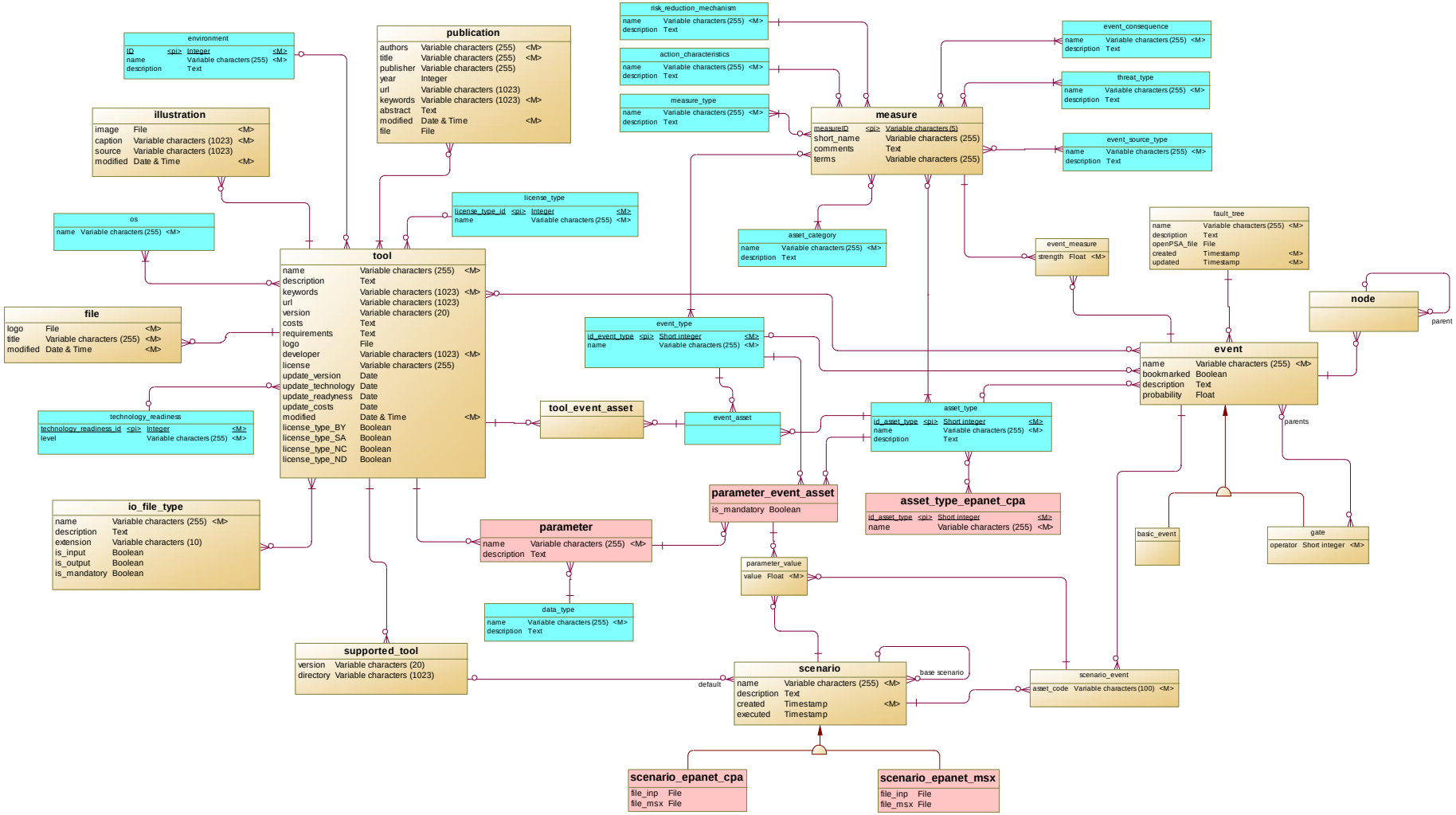


Figure 103: RAET Diagram

Entities

List of entities

Name
action_characteristics
asset_category
asset_type
asset_type_epanet_cpa
basic_event
data_type
environment
event
event_asset
event_consequence
event_measure
event_source_type
event_type
fault_tree
file
gate

illustration
io_file_type
license_type
measure
measure_type
node
os
parameter
parameter_event_asset
parameter_value
publication
risk_reduction_mechanism
scenario
scenario_epanet_cpa
scenario_epanet_msx
scenario_event
supported_tool
technology_readiness
threat_type
tool

tool_event_asset

action_characteristics

Description

Action characteristics:

Proactive

Reactive

Proactive & Reactive

Attributes

Name	Comment	Data Type	Mandatory
name		Variable characters (255)	X
description	Short description of the entity	Text	

Relationships

Entity 1	Entity 2	Entity 1 -> Entity 2 Role	Entity 1 -> Entity 2 Role Cardinality	Entity 2 -> Entity 1 Role	Entity 2 -> Entity 1 Role Cardinality	Entity 1 -> Entity 2 Role Mandatory	Entity 2 -> Entity 1 Role Mandatory
action_characteristics	measure		0,n		1, 1		X

asset_category

Attributes

Name	Comment	Data Type	Mandatory
name		Variable characters (255)	X
description	Short description of the entity	Text	

Relationships

Entity 1	Entity 2	Entity 1 -> Entity 2 Role	Entity 1 -> Entity 2 Role Cardinality	Entity 2 -> Entity 1 Role	Entity 2 -> Entity 1 Role Cardinality	Entity 1 -> Entity 2 Role Mandatory	Entity 2 -> Entity 1 Role Mandatory
asset_category	measure		0,n		1,n		X

asset_type

Description

Possible specific asset types

Attributes

Name	Comment	Data Type	Mandatory
id_asset_type		Short integer	X
name		Variable characters (255)	X
description	Short description of the entity	Text	

Relationships

Entity 1	Entity 2	Entity 1 -> Entity 2 Role	Entity 1 -> Entity 2 Role Cardinality	Entity 2 -> Entity 1 Role	Entity 2 -> Entity 1 Role Cardinality	Entity 1 -> Entity 2 Role Mandatory	Entity 2 -> Entity 1 Role Mandatory
asset_type	parameter_event_asset		0,n		1,1		X
asset_type	asset_type_epanet_cpa		0,n		0,n		
asset_type	event		0,n		0,1		
asset_type	measure		0,n		1,n		X
asset_type	event_asset		0,n		1,1		X

asset_type_epanet_cpa

Description

Asset types supported by Epanet CPA

Attributes

Name	Comment	Data Type	Mandatory
id_asset_type		Short integer	X
name		Variable characters (255)	X

Relationships

Entity 1	Entity 2	Entity 1 -> Entity 2 Role	Entity 1 -> Entity 2 Role Cardinality	Entity 2 -> Entity 1 Role	Entity 2 -> Entity 1 Role Cardinality	Entity 1 -> Entity 2 Role Mandatory	Entity 2 -> Entity 1 Role Mandatory
asset_type	asset_type_ epanet_cpa		0,n		0,n		

data_type

Description

Known data types:

Integer
Real
Date
Time
Boolean
Text

Attributes

Name	Comment	Data Type	Mandatory
name		Variable characters (255)	X
description	Short description of the entity	Text	

Relationships

Entity 1	Entity 2	Entity 1 -> Entity 2 Role	Entity 1 -> Entity 2 Role Cardinality	Entity 2 -> Entity 1 Role	Entity 2 -> Entity 1 Role Cardinality	Entity 1 -> Entity 2 Role Mandatory	Entity 2 -> Entity 1 Role Mandatory
data_type	parameter		0,n		1,1		X

environment

Attributes

Name	Comment	Data Type	Mandatory
ID	ID of the entity	Integer	X
name		Variable characters (255)	X
description	Short description of the entity	Text	

Relationships

Entity 1	Entity 2	Entity 1 -> Entity 2 Role	Entity 1 -> Entity 2 Role Cardinality	Entity 2 -> Entity 1 Role	Entity 2 -> Entity 1 Role Cardinality	Entity 1 -> Entity 2 Role Mandatory	Entity 2 -> Entity 1 Role Mandatory
environment	tool		0,n		0,1		

event

Attributes

Name	Comment	Data Type	Mandatory
name		Variable characters (255)	X
bookmarked		Boolean	
description	Short description of the entity	Text	
probability		Float	

Relationships

Entity 1	Entity 2	Entity 1 -> Entity 2 Role	Entity 1 -> Entity 2 Role Cardinality	Entity 2 -> Entity 1 Role	Entity 2 -> Entity 1 Role Cardinality	Entity 1 -> Entity 2 Role Mandatory	Entity 2 -> Entity 1 Role Mandatory
event	fault_tree		1,1		0,n	X	
tool	event		0,n		0,n		
gate	event		0,n	parents	0,n		
event	scenario_event		0,n		1,1		X
asset_type	event		0,n		0,1		
event_measure	event		1,1		0,n	X	
event_type	event		0,n		0,1		
event	node		0,n		1,1		X

event_asset

Description

Valid combinations of event and asset types

Relationships

Entity 1	Entity 2	Entity 1 -> Entity 2 Role	Entity 1 -> Entity 2 Role Cardinality	Entity 2 -> Entity 1 Role	Entity 2 -> Entity 1 Role Cardinality	Entity 1 -> Entity 2 Role Mandatory	Entity 2 -> Entity 1 Role Mandatory
event_asset	tool_event_asset		0,n		1,1		X
event_type	event_asset		0,n		1,1		X
asset_type	event_asset		0,n		1,1		X

event_consequence

Attributes

Name	Comment	Data Type	Mandatory
name		Variable characters (255)	X
description	Short description of the entity	Text	

Relationships

Entity 1	Entity 2	Entity 1 -> Entity 2 Role	Entity 1 -> Entity 2 Role Cardinality	Entity 2 -> Entity 1 Role	Entity 2 -> Entity 1 Role Cardinality	Entity 1 -> Entity 2 Role Mandatory	Entity 2 -> Entity 1 Role Mandatory
event_consequence	measure		0,n		1,n		X

event_measure

Attributes

Name	Comment	Data Type	Mandatory
strength		Float	X

Relationships

Entity 1	Entity 2	Entity 1 -> Entity 2 Role	Entity 1 -> Entity 2 Role Cardinality	Entity 2 -> Entity 1 Role	Entity 2 -> Entity 1 Role Cardinality	Entity 1 -> Entity 2 Role Mandatory	Entity 2 -> Entity 1 Role Mandatory
event_measure	event		1,1		0,n	X	

measure	event_measure		0,n		1,1		X

event_source_type

Attributes

Name	Comment	Data Type	Mandatory
name		Variable characters (255)	X
description	Short description of the entity	Text	

Relationships

Entity 1	Entity 2	Entity 1 -> Entity 2 Role	Entity 1 -> Entity 2 Role Cardinality	Entity 2 -> Entity 1 Role	Entity 2 -> Entity 1 Role Cardinality	Entity 1 -> Entity 2 Role Mandatory	Entity 2 -> Entity 1 Role Mandatory
event_source_type	measure		0,n		1,n		X

event_type

Description

Event types:

Destruction
Interruption
Manipulation
Pollution

Attributes

Name	Comment	Data Type	Mandatory
id_event_type		Short integer	X
name		Variable characters (255)	X

Relationships

Entity 1	Entity 2	Entity 1 -> Entity 2 Role	Entity 1 -> Entity 2 Role Cardinality	Entity 2 -> Entity 1 Role	Entity 2 -> Entity 1 Role Cardinality	Entity 1 -> Entity 2 Role Mandatory	Entity 2 -> Entity 1 Role Mandatory
parameter_event_asset	event_type		1,1		0,n	X	
event_type	measure		0,n		1,n		X
event_type	event		0,n		0,1		
event_type	event_asset		0,n		1,1		X

fault_tree

Attributes

Name	Comment	Data Type	Mandatory
name		Variable characters (255)	X
description	Short description of the entity	Text	
openPSA_file		File	
created		Timestamp	X
updated		Timestamp	X

Relationships

Entity 1	Entity 2	Entity 1 -> Entity 2 Role	Entity 1 -> Entity 2 Role Cardinality	Entity 2 -> Entity 1 Role	Entity 2 -> Entity 1 Role Cardinality	Entity 1 -> Entity 2 Role Mandatory	Entity 2 -> Entity 1 Role Mandatory
event	fault_tree		1,1		0,n	X	

file

Description

Files related to the tool

Attributes

Name	Comment	Data Type	Mandatory
logo		File	X
title	Title of the entity	Variable characters (255)	X
modified	Date in which this record has been updated. This is read-only information and will be automatically set by the DB.	Date & Time	X

Relationships

Entity 1	Entity 2	Entity 1 -> Entity 2 Role	Entity 1 -> Entity 2 Role Cardinality	Entity 2 -> Entity 1 Role	Entity 2 -> Entity 1 Role Cardinality	Entity 1 -> Entity 2 Role Mandatory	Entity 2 -> Entity 1 Role Mandatory
file	tool		1,1		0,n	X	

gate

Attributes

Name	Comment	Data Type	Mandatory
operator		Short integer	X

Relationships

Entity 1	Entity 2	Entity 1 -> Entity 2 Role	Entity 1 -> Entity 2 Role Cardinality	Entity 2 -> Entity 1 Role	Entity 2 -> Entity 1 Role Cardinality	Entity 1 -> Entity 2 Role Mandatory	Entity 2 -> Entity 1 Role Mandatory
gate	event		0,n	parents	0,n		

illustration

Attributes

Name	Comment	Data Type	Mandatory
image		File	X
caption		Variable characters (1023)	X
source		Variable characters (1023)	
modified	Date in which this record has been updated. This is read-only information and will be automatically set by the DB.	Date & Time	X

Relationships

Entity 1	Entity 2	Entity 1 -> Entity 2 Role	Entity 1 -> Entity 2 Role Cardinality	Entity 2 -> Entity 1 Role	Entity 2 -> Entity 1 Role Cardinality	Entity 1 -> Entity 2 Role Mandatory	Entity 2 -> Entity 1 Role Mandatory
tool	illustration		0,n		1,1		X

io_file_type

Description

File types needed for the calculations with a specific tool, e.g.:
e.g. Network file, Cyberphysical file, Pollutants file

Attributes

Name	Comment	Data Type	Mandatory
name		Variable characters (255)	X
description	Short description of the entity	Text	
extension		Variable characters (10)	
is_input		Boolean	
is_output		Boolean	
is_mandatory		Boolean	

Relationships

Entity 1	Entity 2	Entity 1 -> Entity 2 Role	Entity 1 -> Entity 2 Role Cardinality	Entity 2 -> Entity 1 Role	Entity 2 -> Entity 1 Role Cardinality	Entity 1 -> Entity 2 Role Mandatory	Entity 2 -> Entity 1 Role Mandatory
tool	io_file_type		0,n		1,n		X

license_type

Description

The license type of the tools (commercial, open source, etc.)

Attributes

Name	Comment	Data Type	Mandatory
license_type_id		Integer	X
name		Variable characters (255)	X

Relationships

Entity 1	Entity 2	Entity 1 -> Entity 2 Role	Entity 1 -> Entity 2 Role Cardinality	Entity 2 -> Entity 1 Role	Entity 2 -> Entity 1 Role Cardinality	Entity 1 -> Entity 2 Role Mandatory	Entity 2 -> Entity 1 Role Mandatory
license_ type	tool		0,n		0,1		

measure

Attributes

Name	Comment	Data Type	Mandatory
measureID		Variable characters (5)	X
short_name		Variable characters (255)	X
comments		Text	
terms	Comma separated synonyms of the term	Variable characters (255)	

Relationships

Entity 1	Entity 2	Entity 1 -> Entity 2 Role	Entity 1 -> Entity 2 Role Cardinality	Entity 2 -> Entity 1 Role	Entity 2 -> Entity 1 Role Cardinality	Entity 1 -> Entity 2 Role Mandatory	Entity 2 -> Entity 1 Role Mandatory
measure_t ype	measure		0,n		1,n		X
event_type	measure		0,n		1,n		X
asset_type	measure		0,n		1,n		X
measure	event_meas ure		0,n		1,1		X

action_characteristics	measure		0,n		1,1		X
risk_reduction_mechanism	measure		0,n		1,1		X
event_consequence	measure		0,n		1,n		X
asset_category	measure		0,n		1,n		X
threat_type	measure		0,n		1,n		X
event_source_type	measure		0,n		1,n		X

measure_type

Attributes

Name	Comment	Data Type	Mandatory
name		Variable characters (255)	X
description	Short description of the entity	Text	

Relationships

Entity 1	Entity 2	Entity 1 -> Entity 2 Role	Entity 1 -> Entity 2 Role Cardinality	Entity 2 -> Entity 1 Role	Entity 2 -> Entity 1 Role Cardinality	Entity 1 -> Entity 2 Role Mandatory	Entity 2 -> Entity 1 Role Mandatory
measure_type	measure		0,n		1,n		X

node

Description

Nodes in a Fault Tree

Relationships

Entity 1	Entity 2	Entity 1 -> Entity 2 Role	Entity 1 -> Entity 2 Role Cardinality	Entity 2 -> Entity 1 Role	Entity 2 -> Entity 1 Role Cardinality	Entity 1 -> Entity 2 Role Mandatory	Entity 2 -> Entity 1 Role Mandatory
event	node		0,n		1,1		X
node	node		0,n	parent	0,1		
node	node		0,n	parent	0,1		

os

Attributes

Name	Comment	Data Type	Mandatory
name		Variable characters (255)	X

Relationships

Entity 1	Entity 2	Entity 1 -> Entity 2 Role	Entity 1 -> Entity 2 Role Cardinality	Entity 2 -> Entity 1 Role	Entity 2 -> Entity 1 Role Cardinality	Entity 1 -> Entity 2 Role Mandatory	Entity 2 -> Entity 1 Role Mandatory
os	tool		0,n		1,n		X

parameter

Description

Parameters that must be further specified for the simulation of a specific event and asset with a given tool

Attributes

Name	Comment	Data Type	Mandatory
name		Variable characters (255)	X
description	Short description of the entity	Text	

Relationships

Entity 1	Entity 2	Entity 1 -> Entity 2 Role	Entity 1 -> Entity 2 Role Cardinality	Entity 2 -> Entity 1 Role	Entity 2 -> Entity 1 Role Cardinality	Entity 1 -> Entity 2 Role Mandatory	Entity 2 -> Entity 1 Role Mandatory
data_type	parameter		0,n		1,1		X
parameter_event_asset	parameter		1,1		0,n	X	
tool	parameter		0,n		1,1		X

parameter_event_asset

Description

Any tangible or intangible thing or characteristic that has value to an organization.

Attributes

Name	Comment	Data Type	Mandatory
is_mandatory		Boolean	

Relationships

Entity 1	Entity 2	Entity 1 -> Entity 2 Role	Entity 1 -> Entity 2 Role Cardinality	Entity 2 -> Entity 1 Role	Entity 2 -> Entity 1 Role Cardinality	Entity 1 -> Entity 2 Role Mandatory	Entity 2 -> Entity 1 Role Mandatory
asset_type	parameter_event_asset		0,n		1,1		X
parameter_event_asset	parameter		1,1		0,n	X	
parameter_event_asset	event_type		1,1		0,n	X	
parameter_event_asset	parameter_value		0,n		1,1		X

parameter_value

Attributes

Name	Comment	Data Type	Mandatory
value		Float	X

Relationships

Entity 1	Entity 2	Entity 1 -> Entity 2 Role	Entity 1 -> Entity 2 Role Cardinality	Entity 2 -> Entity 1 Role	Entity 2 -> Entity 1 Role Cardinality	Entity 1 -> Entity 2 Role Mandatory	Entity 2 -> Entity 1 Role Mandatory
scenario_event	parameter_value		0,n		1,1		X

parameter_event_asset	parameter_value		0,n		1,1		X
scenario	parameter_value		0,n		1,1		X

publication

Description

Publications related with tools

Attributes

Name	Comment	Data Type	Mandatory
authors	Authors/owner of the publication	Variable characters (255)	X
title	Title of the entity	Variable characters (255)	X
publisher	Name of the publisher	Variable characters (255)	
year	Year of the publication	Integer	
url	URL providing further information about this entity	Variable characters (1023)	
keywords	Comma-separated keywords	Variable characters (1023)	X
abstract	Abstract of the publication	Text	
modified	Date in which this record has been updated. This is read-only information and will be automatically set by the DB.	Date & Time	X
file		File	

Relationships

Entity 1	Entity 2	Entity 1 -> Entity 2 Role	Entity 1 -> Entity 2 Role Cardinality	Entity 2 -> Entity 1 Role	Entity 2 -> Entity 1 Role Cardinality	Entity 1 -> Entity 2 Role Mandatory	Entity 2 -> Entity 1 Role Mandatory
publication	tool		1,n		0,n	X	

risk_reduction_mechanism

Description

Risk reduction mechanisms:
Frequency/Likelihood
Consequences
Frequency/Likelihood & Consequences

Attributes

Name	Comment	Data Type	Mandatory
name		Variable characters (255)	X
description	Short description of the entity	Text	

Relationships

Entity 1	Entity 2	Entity 1 -> Entity 2 Role	Entity 1 -> Entity 2 Role Cardinality	Entity 2 -> Entity 1 Role	Entity 2 -> Entity 1 Role Cardinality	Entity 1 -> Entity 2 Role Mandatory	Entity 2 -> Entity 1 Role Mandatory
risk_reduction_mechanism	measure		0,n		1,1		X

scenario

Attributes

Name	Comment	Data Type	Mandatory
name		Variable characters (255)	X
description	Short description of the entity	Text	
created		Timestamp	X
executed		Timestamp	

Relationships

Entity 1	Entity 2	Entity 1 -> Entity 2 Role	Entity 1 -> Entity 2 Role Cardinality	Entity 2 -> Entity 1 Role	Entity 2 -> Entity 1 Role Cardinality	Entity 1 -> Entity 2 Role Mandatory	Entity 2 -> Entity 1 Role Mandatory
scenario	scenario_event		0,n		1,1		X
scenario	supported_tool	default	0,1		0,n		
scenario	parameter_value		0,n		1,1		X
scenario	scenario		0,n	base scenario	0,1		
scenario	scenario		0,n	base scenario	0,1		

scenario_epanet_cpa

Attributes

Name	Comment	Data Type	Mandatory
file_inp		File	
file_msx		File	

scenario_epanet_msx

Attributes

Name	Comment	Data Type	Mandatory
file_inp		File	
file_msx		File	

scenario_event

Attributes

Name	Comment	Data Type	Mandatory
asset_code		Variable characters (100)	X

Relationships

Entity 1	Entity 2	Entity 1 -> Entity 2 Role	Entity 1 -> Entity 2 Role Cardinality	Entity 2 -> Entity 1 Role	Entity 2 -> Entity 1 Role Cardinality	Entity 1 -> Entity 2 Role Mandatory	Entity 2 -> Entity 1 Role Mandatory
scenario_event	parameter_value		0,n		1,1		X
scenario	scenario_event		0,n		1,1		X
event	scenario_event		0,n		1,1		X

supported_tool

Description

Tools which are supported by the Scenario Planner,

Attributes

Name	Comment	Data Type	Mandatory
version	Optional field, relevant to software tools	Variable characters (20)	
directory		Variable characters (1023)	

Relationships

Entity 1	Entity 2	Entity 1 -> Entity 2 Role	Entity 1 -> Entity 2 Role Cardinality	Entity 2 -> Entity 1 Role	Entity 2 -> Entity 1 Role Cardinality	Entity 1 -> Entity 2 Role Mandatory	Entity 2 -> Entity 1 Role Mandatory
scenario	supported_tool	default	0,1		0,n		
tool	supported_tool		0,n		1,1		X

technology_readiness

Description

Technology readiness level giving an estimate of the technology maturity of the related tool.

Attributes

Name	Comment	Data Type	Mandatory
technology_readiness_id		Integer	X
level		Variable characters (255)	X

Relationships

Entity 1	Entity 2	Entity 1 -> Entity 2 Role	Entity 1 -> Entity 2 Role Cardinality	Entity 2 -> Entity 1 Role	Entity 2 -> Entity 1 Role Cardinality	Entity 1 -> Entity 2 Role Mandatory	Entity 2 -> Entity 1 Role Mandatory
technology_readiness	tool		0,n		0,1		

threat_type

Attributes

Name	Comment	Data Type	Mandatory
name		Variable characters (255)	X
description	Short description of the entity	Text	

Relationships

Entity 1	Entity 2	Entity 1 -> Entity 2 Role	Entity 1 -> Entity 2 Role Cardinality	Entity 2 -> Entity 1 Role	Entity 2 -> Entity 1 Role Cardinality	Entity 1 -> Entity 2 Role Mandatory	Entity 2 -> Entity 1 Role Mandatory
threat_type	measure		0,n		1,n		X

tool

Attributes

Name	Comment	Data Type	Mandatory
name	Name of the tool	Variable characters (255)	X

description	Short description of the entity	Text	
keywords	Comma-separated keywords	Variable characters (1023)	X
url	URL providing further information about the tool or/and can be used to navigate to the download page	Variable characters (1023)	
version	Current stable version number or name of the software	Variable characters (20)	
costs	If applicable, describe the costs and conditions for obtaining a license (e.g. purchase vs. SAAS, floating license, packages, editions)	Text	
requirements	Minimum hardware and software requirements, including 3rd party software applications, libraries etc. needed to run the tool such as Matlab, EPANET, MS Excel	Text	
logo	The logo of the tool. One of the following image formats is accepted: jpeg, png	File	
developer	Institution, contact person, address, phone, email (mandatory is at least the name of the institution)	Variable characters (1023)	X
license	If applicable, name the license associated with the tool (e.g. GPL 3 or MIT)	Variable characters (255)	
update_version	Date to which the given tool data refer	Date	
update_technology	Date to which the given tool data refer	Date	
update_readyness	Date to which the given tool data refer	Date	
update_costs	Date to which the given tool data refer	Date	
modified	Date in which this record has been updated. This is read-	Date & Time	X

	only information and will be automatically set by the DB.		
license_type_BY	Licensees may copy, distribute, display and perform the work and make derivative works and remixes based on it only if they give the author or licensor the credits (attribution) in the manner specified by these.	Boolean	
license_type_SA	Licensees may distribute derivative works only under a license identical ("not more restrictive") to the license that governs the original work. Without share-alike, derivative works might be sublicensed with compatible but more restrictive license clauses, e.g. CC BY to CC BY-NC.	Boolean	
license_type_NC	Licensees may copy, distribute, display, and perform the work and make derivative works and remixes based on it only for non-commercial purposes.	Boolean	
license_type_ND	Licensees may copy, distribute, display and perform only verbatim copies of the work, not derivative works and remixes based on it.	Boolean	

Relationships

Entity 1	Entity 2	Entity 1 -> Entity 2 Role	Entity 1 -> Entity 2 Role Cardinality	Entity 2 -> Entity 1 Role	Entity 2 -> Entity 1 Role Cardinality	Entity 1 -> Entity 2 Role Mandatory	Entity 2 -> Entity 1 Role Mandatory
tool	event		0,n		0,n		

tool	io_file_type		0,n		1,n		X
technology_readiness	tool		0,n		0,1		
license_type	tool		0,n		0,1		
publication	tool		1,n		0,n	X	
tool	supported_tool		0,n		1,1		X
os	tool		0,n		1,n		X
tool	parameter		0,n		1,1		X
file	tool		1,1		0,n	X	
tool	illustration		0,n		1,1		X
environment	tool		0,n		0,1		
tool	tool_event_asset		0,n		1,1		X

tool_event_asset

Description

Combinations of event types and asset types that are supported by the tool

Relationships

Entity 1	Entity 2	Entity 1 -> Entity 2 Role	Entity 1 -> Entity 2 Role Cardinality	Entity 2 -> Entity 1 Role	Entity 2 -> Entity 1 Role Cardinality	Entity 1 -> Entity 2 Role Mandatory	Entity 2 -> Entity 1 Role Mandatory
event_asset	tool_event_asset		0,n		1,1		X
tool	tool_event_asset		0,n		1,1		X

STOP-IT

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 740610.