Digital Water .City

Risk Identification Database

&

Risk Reduction Measures Database

RIDB & RRMD

digital-water.city
digitalwater_eu

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

Deliverable N° 4.2	RIDB & RRMD
Related Work Package	4
Deliverable lead	SINTEF
Author(s)	Guillaume Bour, Ingrid Selseth, Martin Jaatun, Rita Ugarelli
Contact for queries	Guillaume Bour
Grant Agreement Number	n° 820954
Instrument	HORIZON 2020
Start date of the project	01 June 2019
Duration of the project	42 months
Website	www.digital-water.city
License	This work is licensed under a Creative Commons Attribution 4.0 International License
Abstract	This report describes the Risk Identification Database (RIDB) and Risk Reduction Measures Database (RRMD). The databases gather the generic risk events associated with the implementation of the digital solutions of DWC by the cities and the associated risk reduction measures. The process of the creation of the databases is described, along with a detailed explanation of the fields composing the databases. Finally, a description of the companion tool of the databases, the "RIDB & RRMD Explorer", is provided.

Dissemination level of the document

X	PU	Public
	PP	Restricted to other programme participants
	RE	Restricted to a group specified by the consortium
	CO	Confidential, only for members of the consortium

Versioning and contribution history

Version	Date	Modified by	Modification reasons
D1	14/09/2021	Ingrid Selseth	Proposed structure.
D2	October 2021	SINTEF	Contributions from the authors.
R1	15/10/2021	Guillaume Bour	Sent for internal review.
R2	22/11/2021	Guillaume Bour	Final deliverable.
R3	23/11/2021	Nico Caradot	Review by coordinator.
S	29/11/2021	Guillaume Bour	Final version ready for submission.

* The version convention of the deliverables is described in the Project Management Handbook (D7.1). *D* for draft, *R* for draft following internal review, *S* for submitted to the EC and *V* for approved by the EC.

Note that previous versions to *V* are draft since they are not yet approved by the EC.

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

Table of content

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

List of figures

List of tables

Glossary

CI	Critical Infrastructure
CoP	Community of Practice
DWC	Digital Water City
D	Deliverable
JSON	JavaScript Object Notation
RIDB	Risk Identification Database
RRM	Risk Reduction Measure
RRMD	Risk Reduction Measures Database
UWC	Urban Water Cycle
WP	Work Package
WTP	Water Treatment Plant
WWTP	Waste Water Treatment Plant

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

Executive summary

This report introduces two new databases for urban water management developed within Digital Water City: a Risk Identification Database (RIDB) and a Risk Reduction Measure Database (RRMD). This report is a supporting document providing background information, identifying information requirements for the RIDB and the RRMD and presenting the databases structure.

The databases have been first implemented in MS Excel to facilitate the process of co-creation and interaction with the DWC cities and then converted into a web-based explorer, which allows for an easy visualisation of the two databases. In addition, it is complemented by exploring features that facilitate navigating through risk events and risk treatment measures. The explorer application is accessible at https://risk-explorer.digital-water.city.

The RIDB is a catalogue of risk events, related to physical and cyber threats, which could happen in the case of a cyber and/or physical attack affecting the solutions adopted in DWC by the cities that contributed to the creation of the RIDB. The RIDB identifies the type of threats, the sources of risk, the description of the events and the type of consequences produced. The purpose of the RIDB is not to substitute the comprehensive identification of risk events for each application. Instead, the examples given in the RIDB allow the users to commence with the process and draw its attention to some possibilities that should be investigated, when local conditions evolve, indicating that an event might occur.

The RRMD assists risk managers in the process of finding suitable measures for an appropriate risk treatment. The RRMD lists potential measures to reduce risks included in the RIDB. The database shall not replace a fully formulated plan for risk treatment, but rather show to the users options on how risks could be treated by choosing and implementing one or several measures from the database.

The databases have been created to specifically address the DWC solutions. However, given the wide range of digital technologies (e.g. sensors, modelling, AR, etc.) considered along the urban water cycle, we are confident that both databases could be of strong relevance for European utilities in charge of the management of water and sewer infrastructures.

The creation of the RIDB and RRMD started with a project CoP with the DWC cities to present the scope of the work and the methodology adopted, followed by several meetings with the DWC cities. Based on the knowledge of their systems, of the DWC solutions adopted and the practices in use for risk assessments, potential risks and corresponding measures have been described in general terms during those meetings. Utility's site-specific risks or assets were not included in order to avoid a leak of sensitive information. Therefore, the databases have been populated with generally described risk events and Risk Reduction Measures (RRM) avoiding site-specific information.

This report, which summarizes the RIDB and the RRMD features, holds the following structure: introduction (Section 1), the detailed description of the two databases (Section 2 for the RIDB and Section 3 for the RRMD), the presentation of the RIDB & RRMD explorer (Section 4) and conclusions (Section 5).

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

1. Introduction

Task 4.2 "Cyber-physical security of flow of information in operational, tactical and strategic dimensions" covers all the steps of the risk management process described by the ISO 31000:2009: risk identification, risk analysis, risk evaluation and risk treatment ().

This deliverable presents the DWC contribution to the steps "risk identification" and "risk treatment" through the creation of two databases, the RIDB (Task 4.2.1) and the RRMD (Task 4.2.2), as catalogues of risk events and connected RRMs related to cyber and/or physical threats connected to the DWC solutions adopted by the DWC cities. The steps of risk analysis and evaluation are covered by Task 4.2.3 and the results will be included in D4.3 at M36. D4.3 will provide instructions on how to analyse and evaluate risks related to selected risk events through a concept of system-stress-testing and will provide a risk guide on how to complete a full risk management process from risk identification to risk treatment (i.e. including and building from the RIDB and the RRMD).

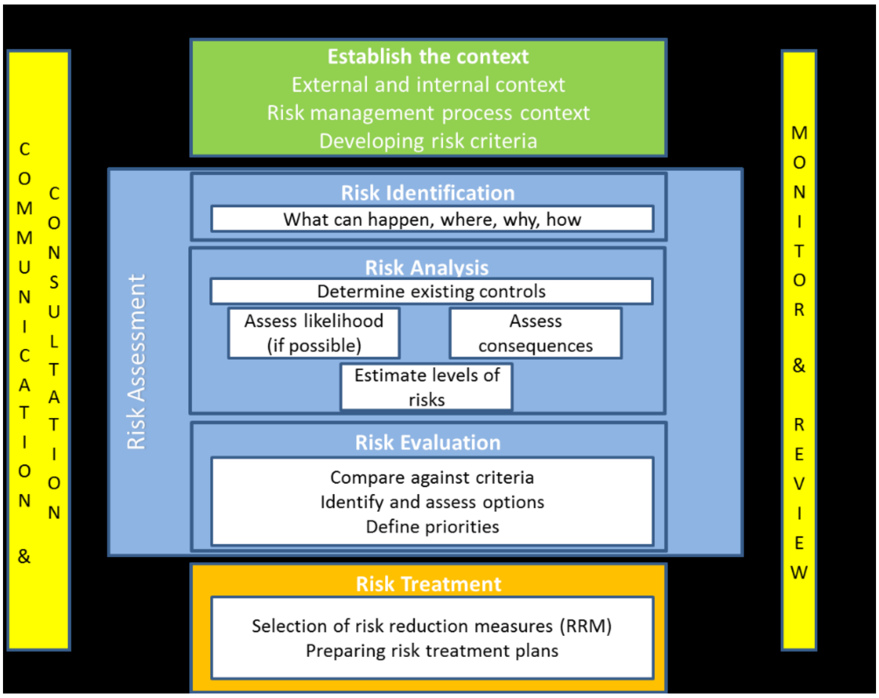

Establish the context
External and internal context
Risk management process context
Developing risk criteria
COMMUNICATION & CONSULTATION
MONITOR & REVIEW
Risk Assessment
Risk Identification
What can happen, where, why, how
Risk Analysis
Determine existing controls
Assess likelihood (if possible)
Assess consequences
Estimate levels of risks
Risk Evaluation
Compare against criteria
Identify and assess options
Define priorities
Risk Treatment
Selection of risk reduction measures (RRM)
Preparing risk treatment plans

Figure 1 Risk management process as defined in ISO 31000:2009

Risk identification

Task 4.2.1 has generated a comprehensive list of potential risk events that may affect a DWC city in relation to the adopted DWC solutions. The outcome from this phase is a RIDB covering the identified risks at strategic, tactical, and operational level of planning. The RIDB is intended to be a source of information to facilitate the task of identifying potential events relevant for the following steps of risk analysis, evaluation (Task 4.2.3) and treatment (Task 4.2.4).

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

Risk analysis and evaluation

Risk analysis consists in assessing the magnitude of risk, by estimating the probability of the selected event to happen and the consequences created. Risk evaluation involves comparing the magnitude of risk estimated during the risk analysis with set risk criteria defining the level of risk that is acceptable, tolerable, or not acceptable. Risk events can therefore be ranked in terms of severity. The result of this step is used to make decisions about future actions on risks events that need to be treated with the adoption of adequate risk reduction measures (which in DWC can be selected for further assessment from the RRMD).

The RIDB cannot substitute the comprehensive identification of risks for each application; however, the examples given allow the users to commence the process and draw their attention to some possibilities that should be investigated, when local conditions indicate that a hazardous event is somehow likely to happen. Furthermore, events considered in the database are not necessarily realistic for each application and others might exist that are not included.

Following the ISO 31000:2009 risk management process, the risk manager should assess the risk level related to the selected risk events (risk analysis) and identify the risk events that are not acceptable given a pre-set criteria for risk acceptance (risk evaluation).

Risk treatment

The Risk Reduction Measures Database (RRMD) is a tool to assist risk managers in the process of finding suitable measures for the appropriate risk treatment of the risk events, included in the DWC-RIDB, assessed as not acceptable. To perform an appropriate risk treatment plan, the main key actions are:

- Identification of risk reduction measures;
- Assessment, prioritization and selection of risk reduction measures;
- Assessment of residual risk;
- Development of a risk treatment program.

To decide on the best risk reduction program, all possible risk reduction measures for the events aligned with the risks requiring treatment need to be identified at first. For this purpose, the DWC - RRMD should be consulted first. For the selected measures, appropriate methods should be used to assess and prioritize them. The final decision will result in a selected set of measures to be implemented, and a final estimation of risk allows a verification of acceptable or at least tolerable residual risk. For some risks, multiple measures can be identified and be used individually or in combination (“multiple barriers”) to accomplish a more effective risk reduction. Situations that could lead to simultaneous failure of multiple barriers should be taken into account. For each measure, appropriate actions needed for its implementation should also be described in the plan since they are relevant in terms not only of implementation effort but also for effectiveness and efficiency of implementation.

In some systems, some RRM may already be implemented but might need improvements. In these cases, these RRM should be assessed (e.g., by site inspection or using monitoring data) to determine its effectiveness in controlling risk. When identifying measures, their potential to continue to be effective considering uncertain future scenarios should also be balanced in terms of measures adaptability.

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

Characterisation of each risk reduction measure should include information that can be classified in four main groups:

- Characterisation and applicability;
- Potential for risk reduction;
- Implementation strategy;
- Analysis of viability.

This information is essential to proceed with the assessment, prioritisation and, finally, selection of the measures to be implemented as well as to produce an adequate risk treatment programme. The DWC - RRMD was developed to support the application of this step.

1.1. Building on existing knowledge

Risk assessment and risk management have been a core activity of water utilities for decades. The DWC project therefore builds on the existing risk identification and RRM databases that have been developed through various projects including TECHNEAU, PREPARED, TRUST and more recently STOP-IT (https://stop-it-project.eu).

The TECHNEAU project introduced the risk-based approach to protect the water supply. A major outcome was the TECHNEAU Hazard Database, which provided an overview of hazards in all stages of water supply (Beuken *et al.,* 2007). The PREPARED project built on this by creating the PREPARED Risk Identification Database. This expanded the risk identification to the entire Urban Water Cycle (UWC) with a focus on risks from climate change (Almeida *et al*., 2013). Here a RRMD was introduced to guide the selection and evaluation of risk reduction measures at UWC level and in relation to climate change related risks (Almeida *et al*., 2014). Within the TRUST project, the effect of new technologies and concepts on the resilience of water supply under various future scenarios of risk was studied (Ugarelli *et al.,* 2014). In the STOP-IT project, the focus has been on the cyber-physical related risks to protect water supply critical infrastructure. How various cyber threat scenarios could lead to the physical risks already identified in the previous projects has been addressed in STOP-IT and dedicated new RIDB and RRMD have been produced (Ostfeld *et al*., 2018; Mälzer *et al*., 2019). In DWC, the STOP-IT RIDB and RRMD are adapted and enhanced in structure and usability to consider additional parts of the urban water cycle addressed by DWC solutions, namely sewer network, WWTP and water bodies.

1.2. The approach used to create the RIDB and the RRMD

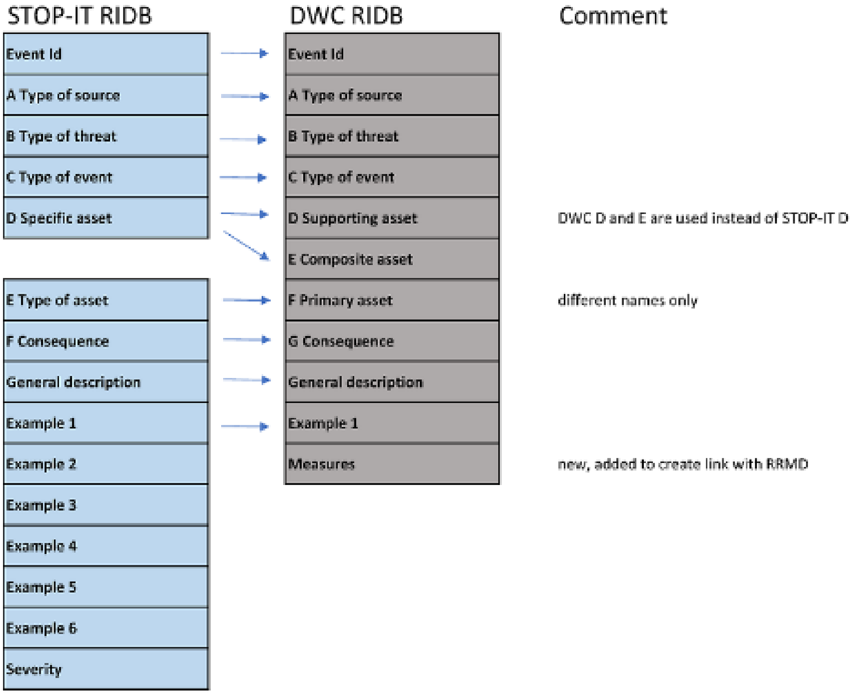
To create a list of risk events and associated risk reduction measures that are as exhaustive as possible, the information was collected by different means and over almost a year, with the contribution of different partners and stakeholders of the project. In addition, as mentioned above, the databases were built based on the experience acquired in the STOP-IT project.

1.2.1. Risk Identification Database

The process of identifying risk events started almost at the beginning of the project when security researchers from SINTEF participated in meetings with the digital solution providers to better understand the technologies used and their potential vulnerabilities. This was for instance the case with Fluidion and their ALERT system (sensors for real-time in situ E.coli and enterococci measurements).

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

Afterwards, the work on designing the RIDB to reflect the new requirements related to the DWC users (i.e. the DWC cities) started. The database's structure was adapted from the STOP-IT RIDB: i.e., a new column "composite asset" (the digital solution the risk applies to) was added, and the original asset column was split between "primary asset" (the main impacted asset) and "supporting asset" (what components are impacted, e.g., sensors, servers, etc.). As a consequence, the description of a risk event, which is automatically created on the basis of the entries in the database columns, was also adapted, as it is described below in chapter 2.



STOP-IT RIDB	DWC RIDB	Comment
Event Id	Event Id	
A Type of source	A Type of source	
B Type of threat	B Type of threat	
C Type of event	C Type of event	
D Specific asset	D Supporting asset	DWC D and E are used instead of STOP-IT D
	E Composite asset	
E Type of asset	F Primary asset	different names only
F Consequence	G Consequence	
General description	General description	
Example 1	Example 1	
Example 2	Measures	new, added to create link with RRMD
Example 3		
Example 4		
Example 5		
Example 6		
Severity		

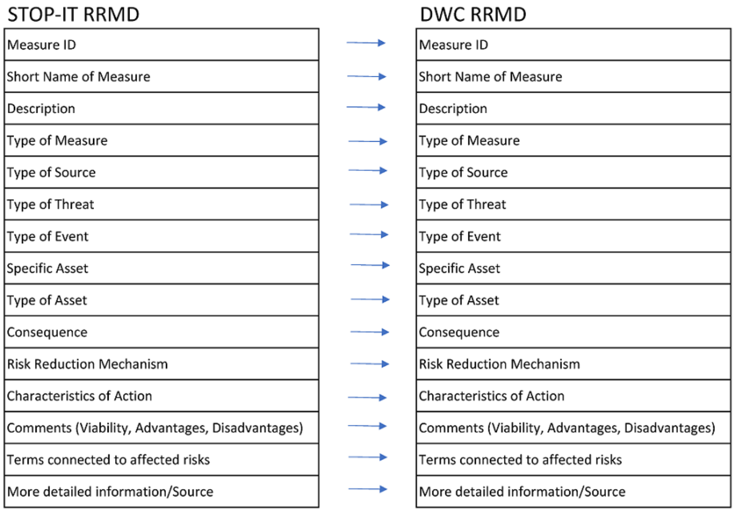
Figure 2. The RIDB database structure

Prior to the Community of Practice (CoP) of October 2020, the empty RIDB was sent to the cities and technology providers with a step-by-step guide including instructions on how to fill it. During the CoP, a RIDB workshop was held by SINTEF. It involved a brainstorming session, which aimed at reviewing the already identified risk events by the cities and possible new risk events (cities were invited to think not only about their own solutions but about others' as well). Online tools such as Slido and GroupMap were used to collect initial information and the results of the brainstorming sessions. As a result of the CoP, SINTEF consolidated the RIDB and sent it again to the cities for review and comments. In January 2021, a second meeting took place with the cities (Paris, Copenhagen, Sofia and Milan) to review and complete the obtained database. At the end of this process, a first usable version of the RIDB was ready. Although all meetings have been held digitally, the communication between partners has been constructive and active; therefore, it can be considered that the RIDB is the actual result of a co-creation process among the project's partners involved. Furthermore, the DWC-RIDB has been shared among the ICT4Water Cluster projects for feedback and eventual new entries in February 2021, through the secretariat of the Cluster. Although the response from the Cluster has been limited to two projects, the proposed new events have been considered relevant for the DWC-RIDB and therefore included.

Eventual identified new risk events can always be added in the RIDB, which has therefore to be considered as a live tool which can be enriched during the project and beyond it.

1.2.2. Risk Reduction Measures Database

Similarly to the RIDB, the Risk Reduction Measures Database (RRMD) developed in STOP-IT was used as a starting point for the DWC version, the difference being that for the RRMD, many measures were kept from STOP-IT as they are generic and could apply to DWC as well. The RRMD is closely linked to the RIDB as it covers measures that allows to reduce the risk of a given event.



STOP-IT RRMD		DWC RRMD
Measure ID	→	Measure ID
Short Name of Measure	→	Short Name of Measure
Description	→	Description
Type of Measure	→	Type of Measure
Type of Source	→	Type of Source
Type of Threat	→	Type of Threat
Type of Event	→	Type of Event
Specific Asset	→	Specific Asset
Type of Asset	→	Type of Asset
Consequence	→	Consequence
Risk Reduction Mechanism	→	Risk Reduction Mechanism
Characteristics of Action	→	Characteristics of Action
Comments (Viability, Advantages, Disadvantages)	→	Comments (Viability, Advantages, Disadvantages)
Terms connected to affected risks	→	Terms connected to affected risks
More detailed information/Source	→	More detailed information/Source

Figure 3. The RRMD database structure

The databases being in practice two Excel files, the process of maintaining them without introducing errors is cumbersome. It was decided to develop a script to update the RRMD based on the RIDB (see 4.1).

To create the RRMD, SINTEF took a first round in identifying risk reduction measures for the different risk events listed in the RIDB. The file was then sent to the cities for review and for them to complete it with the measures they had identified or already in place at their premises. Finally, in April 2021, one-to-one meetings were organized with Paris, Copenhagen, and Milan to further discuss existing measures and brainstorm on the possible new ones. These discussions also lead to improvements of the RIDB. SINTEF consolidated the database afterward, identifying in both the RIDB and RRMD the missing information and incoherent lines so that the cities could fix them. The first version of the RRMD was finished in early June 2021.

Since the RRMD is conceived as a live tool where new entries can be entered on need, the SINTEF team plans to continue populating it along the project life. It is envisaged that new measures (and maybe events) can be identified along the work performed under the sub-task 4.2.4 which is meant to propose tailored recommendations for cyber security to the DWC technology providers.

2. The DWC Risk Identification Database – RIDB

2.1. Information requirements for the RIDB

The aim of the risk identification steps is to identify the events that can occur, specifying where, why and how they can happen. Therefore, the objective of risk identification is to identify all possible risks, not to eliminate risks from consideration or to identify solutions for mitigating risks—those functions are carried out during the risk analysis, evaluation, and risk treatment steps.

Comprehensive identification of risk events using a systematic process is critical since if not identified at this stage relevant risks might be excluded from subsequent analysis (AS/NZS, 2005). Proper risk description should include four elements, namely, sources, events, causes and consequences (ISO, 2009a).

Information sources useful to support risk identification includes (AS/NZS, 2005):

- Expert knowledge and judgement,
- Personal and organisational experience,
- Checklists,
- Historical records, incident databases and previous risk registers,
- Reports from previous risk assessments.

Several methods allowing identifying risks exist. ISO 3100: 2009 (ISO, 2009b) lists and classifies different methods for this purpose, providing an indication of the applicability of the method and whether quantitative output can be provided.

Within DWC, the RIDB includes information on (not intending to be exhaustive):

- Threat (cyber or physical),
- Risk sources,
- Dimensions of consequence expected,
- Typical causes,
- Typical events.

The event comprises the progress from the threat to the accident and associated consequences. The DWC project builds on the general approach provided by the STOP-IT project; however, the application here is focused on the effects of physical-cyber threats to the DWC adopted solutions in the DWC cities. The selected criteria used to describe the data are presented in the following sections. This information allows the user to proceed with the risk identification steps, providing background information that can be used together with the selected approach for risk identification. If no other more complex method is adopted, the database can be used as a checklist.

The application of the risk identification step to a specific system should be carried out using a purpose made form allowing reporting the specific events characteristics and other relevant information. The RIDB structure can be an inspiration to this form, but it is not intended for that purpose. As mentioned previously, the RIDB is a checklist to help the comprehensive identification of risks in each specific application; the examples given in the database allow the users to commence the process and draw their attention to some possibilities that should be investigated, when local conditions indicate that it is somehow likely to happen. Furthermore, events considered in the database are not necessarily applicable for each application and others might exist that are not included.

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

2.2. How to describe a risk event?

The RIDB is considered as an evolving deliverable along the DWC project life and beyond. It is envisaged that additional events identified when developing other WP4 tasks will be added. Besides, it is expected that users of the RIDB will contribute to add new events (even after the end of the project). It is therefore important to provide instructions on how an event should be described.

A risk can be more effectively managed if it is clearly articulated: risk events should be synthetic but information-rich to ensure that the risk statements have an impact and support effective risk management. A good quality risk event statement should answer the following questions:

- What could happen?
- Why could it happen?
- Why do we care?

There is no specific formula to describe a risk event; however, there is guidance provided in the ISO 31000:2009 Risk management—Principles and guidelines (ISO, 2009a) that can help to better articulate risk events as a structured and concise explanation of what occurs in the event, usually including the pathway of the event.

Example of a bad statement: *Water treatment fails.*

Example of a good statement: *Microbiological contamination of treated water due to faulty UV lights in the water treatment PROCESS, resulting in health problems to consumers.*

To avoid repetitions, the DWC RIDB categorizes risk events at general level (general description of the event) and then provides examples, for each general description, where risks are further characterized.

In addition, 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 characterize the event with the following sentence structure:

A generates a **B** threat causing a **C** of the **D** of the **E** which affects **F** and might lead to a **G** issue.

Where:

A Type of source	**B** Type of threat	**C** Type of event	**D** Supporting asset	**E** Composite asset	**F** Primary asset	**G** Consequence

A list of fix words to choose from for each item (A-G) is provided in the file. Using these fix words, the general description of the event can be obtained.

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

2.3. The DWC - RIDB structure

The RIDB is available for public access at risk-explorer.digital-water.city/download/.

The RIDB has been originally implemented in Microsoft Excel files in order to facilitate its creation, and as such it was planned as project deliverable. The excel version remains at value for water utilities interested to create their own versions of it beyond the project or to import the information on their own risk management tools. However, as further contribution to the project, also an online version was created to facilitate the navigation through the two databases as they result at the end of the project. The excel file consists of three data sheets. While the major information is given in the sheet "DWC - Database", the other two sheets contain supporting information, i.e., a front-page introducing the RIDB and a sheet containing the options that can be chosen in the main database sheet. The structure of the RIDB file is given in Table 1.

Table 1. The structure of the RIDB file

Sheet number	Sheet name	Description
1	Description	Front page of the RIDB with a list of RIDB fields
2	DWC - Database	Main database sheet
3	DWC - Options	Option list for fields

2.4. The DWC – RIDB Database sheet

In the main database sheet (sheet n. 2), the identified risk events are listed and characterized. With the help of this table, it is possible for the user to answer when, why and in which manner the risks can occur as well as which type of consequences can be expected if the risks are occurring. Therefore, the following different columns are implemented to describe different characteristics of the listed risks to enable a comprehensive understanding of risks. A short description of all implemented columns of the RIDB is given in Table 2.

Table 2. List of attributes and descriptions of the DWC RIDB

Name	Description
Event ID	Unique numeric identifier
Type of source	Element which alone or in combination has the intrinsic potential to give rise to risk
Type of threat	The type/nature of the threat that within the DWC context could be cyber, physical or cyber-physical.
Type of event	The nature of the event
Supporting asset	The specific element (physical or virtual) where the risk source or exposure to it occurs
Composite asset	The DWC solution where the risk source or exposure to it occurs, composed of supporting assets

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

Name	Description
Primary asset	Infrastructure of the water cycle where the risk event occurs
Consequence	The type of impact caused by the undesired event if materialised (outcome of an event affecting objectives).
General description	A short description of the risk event (fixed sentence structure).
Example	Further characterization of the risk event (free text).
Measures	List of relevant risk reduction measures (comma separated)

2.5. Detailed description of the attributes in the DWC RIDB database sheet

The description of the attributes and the entries is shown in Table 2 **Fehler! Verweisquelle konnte nicht gefunden werden.** and explained in detail in the following.

2.5.1. Event ID

Each entry in the RIDB is connected to a specific “Event ID” facilitating the reference to specific risks from the RIDB. The event ID may be a consecutive number, which allows a clear identification of an event.

2.5.2. Type of source

Risk sources are necessary to describe how the event may initiate and propagate. The risk source defines the cause that leads to the undesired event. This differentiation can help the user to gain a better understanding of the risk that also leads to a facilitated selection of suitable risk reduction measures. The options are:

External attacker: A failure in delivering the service occurs due to a deliberate or accidental action by external people generating a cyber and/or physical threat.

External supplier: Attackers often do not attack their target directly but use a “weaker” link as entry point. In the context of water utilities, it can be an external IT supplier, or simply a technology provider that is targeted to leverage and attack against a digital solution.

Human fault: A failure of the water system occurs due to a human fault (e.g., wrong operation, wrong maintenance, wrong design, wrong action). System failures in this case is not caused by a cyber or physical attack. The effect on the service provided may be similar to an attack, but the risk reduction measures will be completely different.

Internal attacker: A failure in delivering the service occurs due to a deliberate or accidental action by people from the water utility’s staff generating a cyber and/or physical threat

2.5.3. Type of threat

The following entries describe the type of threats. The options are:

Cyber: Voluntary or not, the intent of individuals or groups to electronically corrupt or seize control of data or information essential to system operations. People attempting an attack via cyber mechanisms may also seek out information that contains highly sensitive knowledge about a system’s vulnerabilities.

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

Physical: By the physical type of threats, assets or technical devices of the system will be damaged or manipulated. The physical threat may also destroy or damage sensors, data transmission lines or the process control/SCADA system in a way that the normal function is no longer possible.

Cyber-Physical: The threat has a combined cyber-physical nature. It can generate in different ways, as for instance:

- **Combined cyber-physical threats**: coordinated and long-term attacks on the infrastructure to reach and compromise the normal functioning. Some of the latest attacks have been a combination of social engineering, actions in the physical environment and actions in the cyber area. Being developed along a period of time and with several phases.
- **Cyber threat to any of the physical component of the water infrastructure,** e.g., monitoring devices (including e.g., IP cameras, networked sensors, AMR/AMI) that become more vulnerable to cyber-attacks due to their higher automation/networking level
- **Physical threats to the "cyber" environment** of the utilities, e.g. Intrusion of attackers to the utilities control & operation centres (access to computers) or SCADA devices, etc.

2.5.4. Type of event

The type of event specifies the character of how the risk event is generated. Knowing the "type of event" will help to define risk reduction measures to reduce the probability of the event to happen.

The main options are:

Eavesdropping: An eavesdropping attack, also known as a sniffing or snooping attack, is a theft of information as it is transmitted over a network by a computer, smartphone, or another connected device. The attack takes advantage of unsecured network communications to access data as it is being sent or received by its user.

Denial of Service: A denial-of-service (DoS) attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor.

Manipulation of the data: An attacker modifies the data of the system, either directly (modification of a database for instance) or during a communication exchange between two entities (via a Man-in-the-Middle attack for instance).

Destruction: Destruction of an asset or composite asset of the solution. This includes for instance destruction of sensors, communication infrastructures, etc.

Spoofing: Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source. Spoofing can apply to emails, phone calls, and websites, or can be more technical, such as a computer spoofing an IP address, Address Resolution Protocol (ARP), or Domain Name System (DNS) server.

Discharge of pollutants: Discharge of pollutants means (A) any addition of any pollutant to navigable waters from any point source, (B) any addition of any pollutant to the waters of the contiguous zone or the ocean from any point source other than a vessel or other floating craft.

2.5.5. Supporting asset

This field includes a list of fixed words to be selected to indicate the specific asset where the risk source or exposure to it occurs.

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

The main options are:

Sensors: A device which detects or measures a physical property and records, indicates, or otherwise responds to it. In the context of DWC, sensors will also often have a way to communicate the measured data.

Servers: A computer or computer program that manages access to a centralized resource or service in a network.

Web application: An application software that runs on a web server. Web applications are usually accessed through a web browser.

Web API: A Web API (Application Programming Interface) is, as its name indicates, an interface that gives access to a web application functionality.

2.5.6. Composite supporting asset

Composite supporting assets are the digital solutions implemented.

The options are:

- Sensors for real-time in situ E.coli and enterococci measurements
- Machine-learning based Early Warning System for bathing water quality
- Early Warning System for safe reuse of treated wastewater for agricultural irrigation
- WebGIS platform for improved decision making in water reuse
- Active unmanned aerial vehicle for analysis of irrigation efficiency
- Match making tool between water demand for irrigation and safe water availability
- Serious game on the water reuse, carbon, energy, food and climatic nexus
- Mobile application for asset management of drinking water wells
- DTS sensor for tracking illicit sewer connections
- Sensors and smart analytics for tracking illicit sewer connections hotspots
- Augmented reality (AR) mobile application for groundwater visualisation
- Sewer flow forecast toolbox
- Interoperable Decision Support System (DSS) and real-time control algorithms for stormwater management
- Web platform for integrated sewer and wastewater treatment plant control
- Low-cost temperature sensors for real-time combined sewer overflow (CSO) and flood monitoring
- Smart sewer cleaning system with HD camera and wireless communication

2.5.7. Primary asset

The primary assets are the water assets that are affected by the attack. As similar risk sources might lead to different risk events at different assets, this specification is necessary for further risk assessment process.

The main options are:

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

Raw water bodies: The raw water bodies comprise the catchment areas of groundwater as well as springs, the water body and inflows of reservoirs used for drinking water supply and the river upstream of the abstraction point of river water used for drinking water supply.

Water abstraction points: Under this type of asset, the wells and abstraction pumps of surface waters (dams, rivers, and springs) are summarized. If the water is abstracted by gravity pipelines, the entrance of water into the pipeline is to be considered as well (e.g., feed hopper, intake tower, spring building).

Water Treatment Plants (WTPs): Drinking water treatment plants are considered as integral units. There is no specification made amongst the possible components of a plant (e.g., ozonation, flocculation, sedimentation, filtration, intermediate tanks and pumps, valves and sensors). Chemical or physical disinfection is considered as a treatment.

Drinking water distribution network: The drinking water distribution network is the network of smaller pipes that supply water to the customers. A differentiation of individual pipes is not made. Manholes and valve chambers are also part of the distribution network.

Drinking water tanks: Drinking water tanks are all tanks in which drinking water is stored before distribution. Drinking water tanks may comprise tanks at ground level and elevated tanks as well as water towers. In addition, small inflow tanks for pumps or intermediate tanks in water treatment plants are to be considered as they might be vulnerable to pollutions too.

Pressure boosting stations: They may be located between Drinking water main pipes or in the distribution network and allow the supply of higher elevated regions with drinking water.

Sewer network or Wastewater treatment plants: In a sewage treatment plant, waste or contaminated substances are treated with various means and produce purified substances that are safe and reusable in the process or discharged to the environment.

2.5.8. Consequence dimension

The consequence dimension describes the outcome of an event in terms of potential type of impact created. A quantitative assessment of the impact extend is not required at this place, as the general RIDB will not contain individual information of the utility and the assessment will only be possible under consideration of the individual and specific conditions of each Service provider.

The options are:

Quantity: An event may lead to a disturbance in terms of “quantity” to the service to be provided, for instance the event may result in an insufficient availability of drinking water.

Quality: An event may lead to a disturbance of the quality of supplied water. This may result in chemical, biological or radiological aberrations from the acceptable levels.

Financial: Due to an event, actions to remove the causes and to re-establish the normal estate will be necessary, which will need financial resources.

Reputation: Consequences dimension for events that, not having any consequence on the service, end up in a loss of reputation by the company (i.e. loss of sensitive information).

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

2.5.9. General description (based on a fixed syntax)

This field includes the general description of the event, which is formulated automatically by entering words characterizing the fields:

A Type of source	B Type of threat	C Type of event	D Supporting asset	E Composite asset	F Primary asset	G Consequence

By entering words per each A-G cell a general description of the event will be formulated according to the following syntax:

A generates a **B** threat causing a **C** of the **D** of the **E** which affects **F** and might lead to a **G** issue

Example of a general description:

External Attacker *generates a* ***cyber threat*** *causing a* ***Denial of Service*** *of the* ***Sensors*** *of the* ***Sensors for real-time in situ E.coli and enterococci measurements*** *which affects* ***Raw water bodies*** *and might lead to a* ***Quality*** *issue.*

2.5.10. Example 1

The user should possibly provide a more detailed example but following as close as possible the RISK event definition syntax provided in 2.5.4 2.2. In the example, the user can further elaborate without being limited to the fix words.

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

3. The DWC - Risk Reduction Database – RRMD

The RRMD is available for public access at risk-explorer.digital-water.city/download/.

In this chapter, the overall methodology of the RRMD is described. The RRMD is generally oriented towards the risk reduction measures database designed in the EU-project "PREPARED" (Almeida *et al.*, 2014).

Adding to the PREPARED database, additional sources for the RRMD have been the measures developed in the STOP-IT and DWC projects or the measures described in regulations and guidelines, specific for the DWC application scope. The aim of the database is to provide generally described measures avoiding site-specific information. Thus, the applicability of the proposed measures at different locations and under varying conditions shall be ensured. It must be kept in mind that the aim of the RRMD is not to supply the user with a fully prepared strategy for risk reduction that can be simply taken over and applied in the end-user's utility. Instead, measures that can potentially reduce previously identified risks are proposed and their effectiveness still need to be evaluated in the specific cases by simulations, expert judgement or similar.

In its initial state, the RRMD is implemented in Microsoft Excel. Using standard software, an easy population with a first set of measures by different partners is enabled. The RRMD must be seen as strongly connected to the deliverable RIDB. The excel files of both databases contain the initial content of the finally programmed versions of the database.

3.1. The DWC – RRMD Database Structure

The RRMD is implemented in Microsoft Excel files and consists of five data sheets. While the major information is given in the sheet "RRMD", the other sheets contain supporting information, i.e., a front-page introducing the RRMD and a sheet containing the options that can be chosen in the main database sheet. The structure of the RRMD file is given in Table 3.

Table 3. The structure of the RRMD file

Sheet number	Sheet name	Description
1	Cover	Front page of the RRMD
2	Instructions for use	List and description of RRMD fields
3	Definitions	Definition of the options for field no 4-10
4	RRMD	Main database sheet
5	Options Lists	Option lists for field no 4-12

3.2. The RRMD Database sheet

The worksheet "RRMD" represents the main part of the database where risk reduction measures are listed and generally described with respect to their characteristics, mechanisms, and primary aims. Therefore, different data categories were implemented in the database which are explained individually in the following part.

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

Table 4. List of attributes and descriptions of the DWC RRMD

Name	Description
ID	Unique Identifier
Short Name of Measure	Short name
Description	General information on which action is connected to the measure
Type of Measure	The main principle according to which the measure reduces a risk
Type of Source	The sources of risk events for which the measure is able to reduce the risk
Type of Threat	The nature of the reduced risk
Type of Event	The type of event treated by the measure
Specific Asset	Which specific asset is directly affected by the risk event
Type of Asset	Which type of asset is affected by the outcomes of the risk event for which the risk shall be reduced
Consequence	Which consequence dimensions are affected if the treated risk event occurs
Risk Reduction Mechanism	Define if the frequency/likelihood of a risk event occurring, its consequences or both are reduced
Characteristics of Action	Specify if a measure operates as proactive, reactive or both.
Comments (Viability, Advantages, Disadvantages)	Notes or a short-written text
Terms connected to affected risks	Several terms that are connected to the risk that shall be reduced by the risk reduction measure can be noted
More detailed information/Source	Free text

For a record to be valid and included into the database, data from all categories must be provided. For those data categories that represent a list of predefined options, multiple choices can be made. However, at least one selection is required.

Since many measures can be described by different terms (options) of the same category, it is possible to enter more than one term in all columns that represent a selection from a list. By this mean, many-to-many relationships between risk events and measures can be realized. Thus, an event of the RIDB may be associated to several suitable measures of the RRMD. On the other hand, a measure from the RRMD may address several risks documented in the RIDB.

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

3.3. Detailed description of the attributes in the RRMD database sheet

The description of the attributes and the entries is shown in Table 4 and explained in detail in the following.

3.3.1. Measure ID

In this column each measure is connected to a specific Measure ID. The ID is a unique number, which allows the clear identification of a measure.

3.3.2. Short name of Measure

To ease the recognition of the RRMs, a short name for each measure is defined. The short name is written in CamelCase format.

3.3.3. Description

General information is given on which action is connected to the measure. It is helpful to use meaningful and informative notes to give the user a clear and fast understanding of the main working principle of the measure. Furthermore, the description should be as universal as possible to ensure the suitability of the measure in many cases with varying conditions, e.g. different countries, varying environmental conditions or similar.

The description of a RRM might answer the following questions:

- Which technique/method/kind of asset is used as RRM?
- How does it work?
- What is the overall aim of the measure?

3.3.4. Type of measure

The type of measure defines the main principle according to which the measure reduces a risk. This categorization shall give the user a basic idea of the working principle of the measure.

The options are:

Action and crisis management plans and training: With appropriate action and crisis management plans and trainings, the staff of a utility can be taught how to behave and work in a way that the risk events like accidents and attacks are reduced to a minimum. Furthermore, the correct behaviour after the occurrence of a risk event might be taught to ensure the reduction of negative consequences to a minimum. The training of the utilities' staff's behaviour in crisis situations and after attacks is one possible example for this type of measure. Giving advice to the population about the correct behaviour in case of attacks or water shortages is also an important activity of this measure type (e.g. by preparation of flyers in advance or by broadcasting announcements).

Consequence mitigation: The mitigation of consequences reduces the risk without having an impact on the probability or frequency of risk events occurring. Therefore, this kind of RRMs is suitable for the reduction of the negative consequences of risk events. Examples for consequence mitigation measures could be a) the construction of connection pipes to neighbouring water supplier(s) to be prepared in a case such as the breakdown of the own water supply, b) the construction of wells for emergency supply or c) the signing of contracts with organizations providing small mobile emergency water treatment plants.

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

Control Systems: Risks can be reduced if a threat is recognized and indicated in an early stage before the negative consequences really occur or before the negative consequences aggravate. Therefore, control systems can help to reduce the risk of unidentified incidents by warning the operating staff early enough to take action to prevent hazardous incidents from happening or aggravating. Examples for control systems are pressure sensors in pipes or alarm systems at water treatment sites. Control systems in the field of cyber threats are for example firewalls inspecting in-going and out-going data for viruses, Trojans or similar. However, sometimes it can be difficult to distinguish between control systems and barriers. For example, firewalls can be seen as barriers if they directly prevent access of malware to data, but they can also be seen as control systems if they just warn the user about potentially dangerous incidents.

Cyber Barriers: Cyber barriers reduce risks by introducing a cyber-barrier between software or hardware components of a system like the process control/SCADA system and the risk source. This could for example be a firewall. In addition, encryption processes can be seen as cyber barriers as the encryption represents a barrier between the attacker and the sensitive content of the stolen data.

Economic Policy: Financial risks can be reduced by building financial reserves or by contracting an insurance policy. Thus, the risk of insolvency or similar can be reduced, especially if a high amount of money will be necessary for the restauration of the water supply after an attack resulting in cost-intensive damages like damages to wells, pumps, networks, treatment plants or reservoirs. Economic Policy often may be seen also as a kind of Consequence Mitigation.

Physical Barriers: Physical barriers reduce risks by introducing a barrier between the protected good and the risk source. It could e.g. be a fence to keep out unauthorized people from a sensitive site, bars at the windows, burglar-proof doors, locks or similar.

Redundancy: With the help of redundancies, risks based on the possibility of failing infrastructure, treatment equipment etc. shall be compensated. Redundant infrastructures (at least partially) keep on working in the desired manner if one of the redundantly constructed parts fails. Examples could be the construction of a second pipeline to ensure water supply if one of the pipelines is destroyed, mirrored (double) process control systems, additional pumping wells or additional treatment plants.

3.3.5. Type of source

In this category, the sources of risk events for which the measure is able to reduce the risk are specified. To enable the process of semantic mapping, measures are characterized according to the type of source in alignment to the RIDB, refer chapter 2.5.2.

3.3.6. Type of threat

The “Type of Threat” defines the nature of the reduced risk and is divided into three options. To enable the process of semantic mapping, the possible options are similar to the ones specified in the RIDB, refer to chapter 2.5.3.

3.3.7. Type of event

As similarly implemented in the RIDB, in this column the type of event treated by the measure is defined. To enable the process of semantic mapping, the possible options are similar to the ones in the RIDB, refer to chapter 2.5.4.

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

3.3.8. Specific asset

Here is defined, which specific asset is directly affected by the risk event. To enable the process of semantic mapping, for the column "Specific Asset" the same options can be chosen as it is possible in the RIDB. The column "specific asset" is filled with both the supporting and composite assets from the RIDB, refer to chapter 2.5.5 and 2.5.6.

3.3.9. Type of asset

The "Type of Asset" defines which type of asset is affected by the outcomes of the risk event for which the risk shall be reduced. To enable the process of semantic mapping, the possible options are similar to the ones in the RIDB, refer to chapter 2.5.7.

3.3.10. Consequences

The "Consequence" options define which consequence dimensions are affected if the treated risk event occurs. To enable the process of semantic mapping, the possible options are similar to the ones in the RIDB, refer to chapter 2.5.8.

3.3.11. Risk Reduction Mechanism

Here it is defined, if the frequency/likelihood of a risk event occurring, its consequences or both are reduced.

- Consequences
- Frequency/Likelihood
- Frequency/Likelihood & Consequences

3.3.12. Characteristics of action

In this column it is specified if a measure operates as proactive, reactive or both. For example, the flushing of the piping system after an observed contamination is a reactive measure while the implementation of a functioning management system or the building of fences are proactive measures.

- Proactive
- Proactive & Reactive
- Reactive

3.3.13. Comments

This column may be filled with notes or a short-written text. Special properties of a measure like site specific features, advantages, disadvantages, experiences, additional explanations or similar might be entered.

3.3.14. Terms connected to affected risks

In this column several terms that are connected to the risk that shall be reduced by the risk reduction measure can be noted. Thus, the search for suitable risk reduction measures might be improved. The possible terms for the list should be chosen from the ontology. The addition of terms in this field is optional, thus the user is free to leave this field empty.

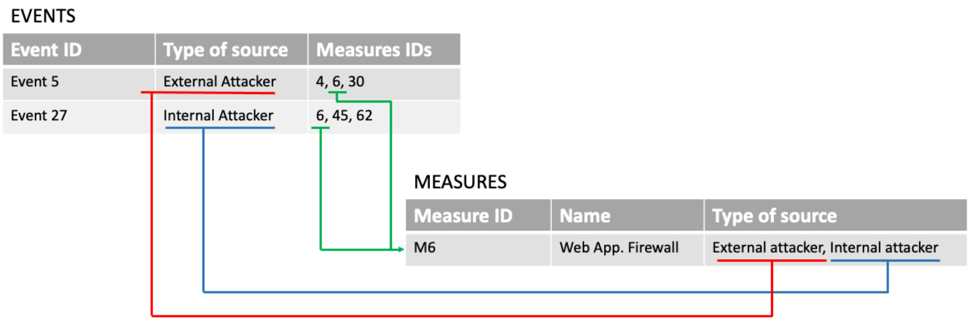
digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

4. The RIDB & RRMD Explorer

Navigating the Excel databases to identify risk events and possible risk reduction measures that apply to a given solution or assets is not practical. It was thus decided to develop a companion application, called the “RIDB & RRMD Explorer” which allows for an easy visualisation of the two databases. The development of this application was done in august 2021 and it is accessible at https://*risk-explorer.digital-water.city*.

4.1. RIDB & RRMD processing

As already mentioned in the previous section, maintaining the two databases without forgetting information or introducing mistakes is a cumbersome task. To prevent that from happening and to help updating the two databases along the way without having to freeze the RIDB, a script was developed (available in Appendix). For the script to function, a new column “measures” was added to the RIDB. This column contains the applicable risk reduction measures’ ID. This ID is used to link the events to the measures explicitly. The measures on the other hand are not linked directly to specific events: for a given measure, each field is a set in which are inserted the values of the corresponding field of the events the measure is applicable for, as shown in Figure 4.



EVENTS

Event ID	Type of source	Measures IDs
Event 5	External Attacker	4, 6, 30
Event 27	Internal Attacker	6, 45, 62

MEASURES

Measure ID	Name	Type of source
M6	Web App. Firewall	External attacker, Internal attacker

Figure 4 Mapping between the risk events and the risk reduction measures

Afterwards, two other scripts (one for each of the databases) parse the files and produce two JSON files: *events.json* and *measures.json*. The update scripts should be used by anyone who wishes to update the databases (see 4.3 for the detailed update procedure). These two files are then used by the web application to display the risk events and risk reduction measures in an easy-to-navigate and friendly manner.

4.2. RIDB & RRMD Explorer Functionalities

The RIDB & RRMD Explorer is not a complex application: it simply provides the user with an easy way to navigate the risk events identified for the different solutions in digital-water.city.

It provides a direct mapping between the events and the measures, i.e., for each event, the user can see what the identified risk reduction measures are and click on them to have more details if necessary. It is also possible to see all the identified risk reduction measures and see to which type of assets, type of threats, etc. they apply to.

In addition, filtering options were added to both the events and the measures to ease the lookup up of a risk and/or measure. Filters can be combined to refine a search.

4.3. Adding risks and events to the databases

The RIDB & RRMD Explorer is a frontend-only application. That means there is no backend server nor databases. The risk events and risk reduction measures are thus fixed to the deployed version. To enable the application to live after the end of the project, it was made open source on GitHub[1]. This allows anyone to access the latest version of the databases/Excel files, but also to locally deploy the application and contribute to the project.

Updating the databases will also be done using GitHub. As an external contributor, there are two ways to suggest an update:

1. Updating the project directly (preferred solution)
    a. Fetch the project at https://github.com/SINTEF-Infosec/dwc-risk-explorer
    b. Update the RIDB & RRMD files found in the *data* folder
    c. Run the update script (found in the *scripts* folder)
    d. Commit the changes and submit a pull request
    e. The pull request will then be reviewed and accepted by SINTEF
2. Open an issue
    a. You can open an issue on GitHub directly describing the changes to be made to the database. To do so, use the provided templates.
    b. The proposed changes will then be reviewed, implemented, and added to the main branch of the project by someone in the SINTEF team.

4.4. Future development of the risk explorer

By open sourcing the code of the risk explorer, the intention is to ensure that companies and individuals will use it to expand the databases, but also to facilitate the further development of the tool. While the explorer is currently only a façade for the Excel files, it could be used as a starting point for a self-contained tool for risks identification and management. Possible functionalities include adding a way for external contributors to suggest risks events and risk reduction measures that could then be reviewed and validated by a team of administrators.

4.5. RIDB & RRMD Explorer user guide

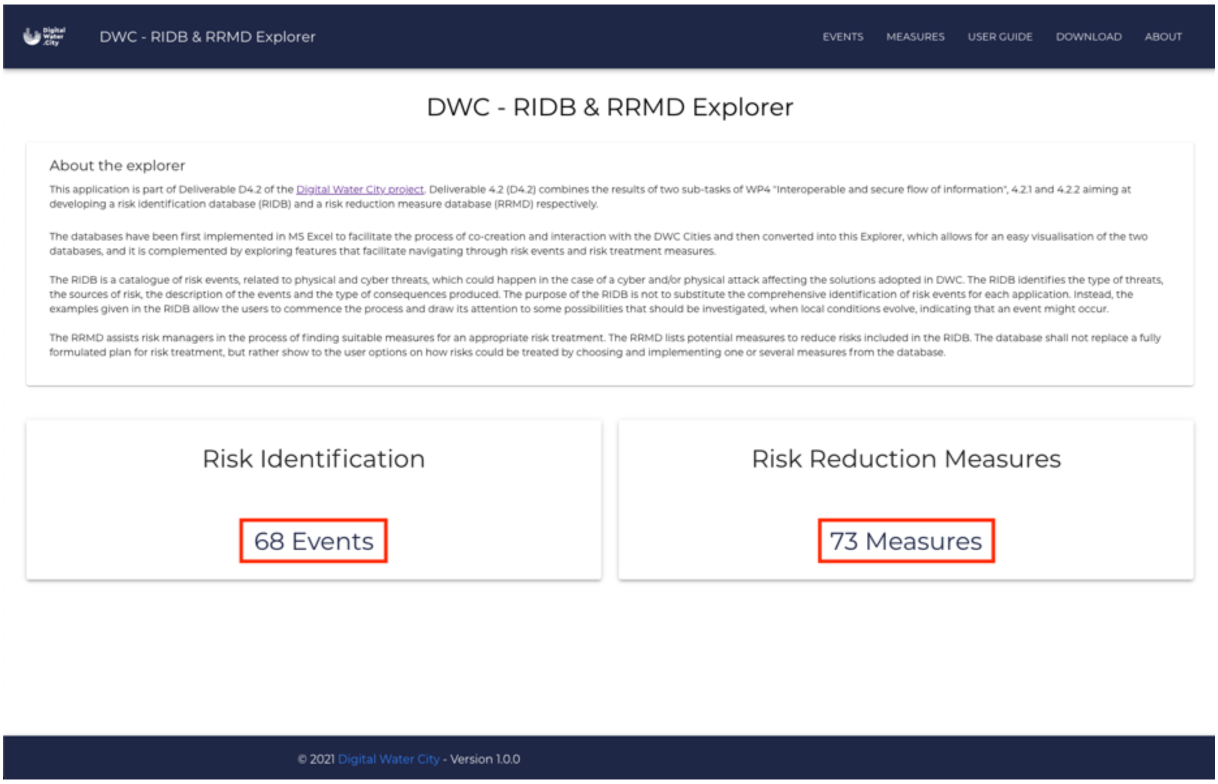
A user guide was created to explain how to use the explorer and it can be read directly on the explorer website, at the following address: https://risk-explorer.digital-water.city/user-guide. The content is similar to what is presented below.

4.5.1. The dashboard

The dashboard provides information about the number of events and measures available in the application. Clicking on the links redirects to the events and measures' pages respectively.

[1] GitHub is a code hosting platform for version control and collaboration. It lets you and others work together on projects from anywhere.

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.



DWC - RIDB & RRMD Explorer

About the explorer

This application is part of Deliverable D4.2 of the Digital Water City project. Deliverable 4.2 (D4.2) combines the results of two sub-tasks of WP4 "Interoperable and secure flow of information", 4.2.1 and 4.2.2 aiming at developing a risk identification database (RIDB) and a risk reduction measure database (RRMD) respectively.

The databases have been first implemented in MS Excel to facilitate the process of co-creation and interaction with the DWC Cities and then converted into this Explorer, which allows for an easy visualisation of the two databases, and it is complemented by exploring features that facilitate navigating through risk events and risk treatment measures.

The RIDB is a catalogue of risk events, related to physical and cyber threats, which could happen in the case of a cyber and/or physical attack affecting the solutions adopted in DWC. The RIDB identifies the type of threats, the sources of risk, the description of the events and the type of consequences produced. The purpose of the RIDB is not to substitute the comprehensive identification of risk events for each application. Instead, the examples given in the RIDB allow the users to commence the process and draw its attention to some possibilities that should be investigated, when local conditions evolve, indicating that an event might occur.

The RRMD assists risk managers in the process of finding suitable measures for an appropriate risk treatment. The RRMD lists potential measures to reduce risks included in the RIDB. The database shall not replace a fully formulated plan for risk treatment, but rather show to the user options on how risks could be treated by choosing and implementing one or several measures from the database.

Risk Identification

68 Events

Risk Reduction Measures

73 Measures

© 2021 Digital Water City - Version 1.0.0

Figure 5 Dashboard of the RIDB & RRMD Explorer

4.5.2. Events & measures pages

Both risk events and risks measures are presented in a similar manner in the explorer: a paginated table with the main information about an event or a measure. For the events, the fields are:

- ID
- Type of source
- Type of threat
- Type of event
- Supporting asset
- Composite asset
- Primary asset
- Consequence
- Description
- Example
- Number of measures (this field is calculated automatically based on the measures associated to this event)

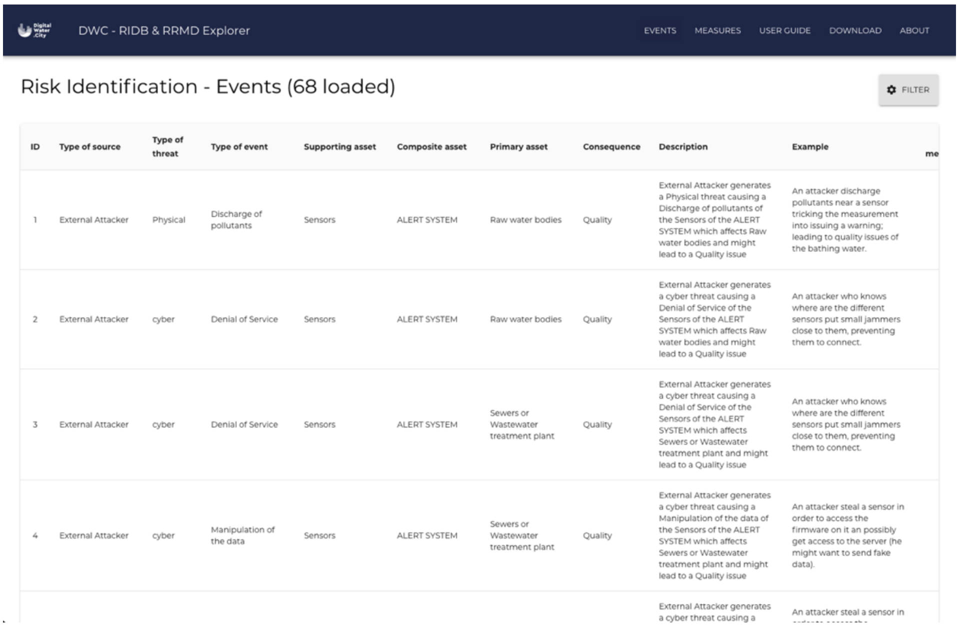
For the measures, the fields are:

- ID
- Name
- Description
- Type of measures

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

- Type of source
- Type of threat
- Specific asset
- Consequence
- Risk reduction mechanism

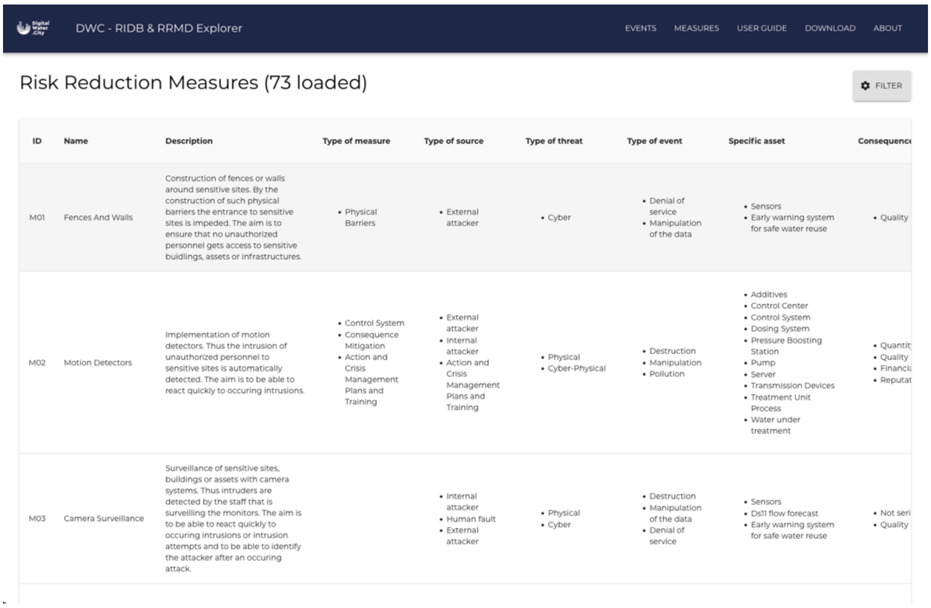
For a detailed explanation of those fields, please refer to sections 2 (RIDB) and 3 (RRMD).



Risk Identification - Events (68 loaded)

ID	Type of source	Type of threat	Type of event	Supporting asset	Composite asset	Primary asset	Consequence	Description	Example	me
1	External Attacker	Physical	Discharge of pollutants	Sensors	ALERT SYSTEM	Raw water bodies	Quality	External Attacker generates a Physical threat causing a Discharge of pollutants of the Sensors of the ALERT SYSTEM which affects Raw water bodies and might lead to a Quality issue	An attacker discharge pollutants near a sensor tricking the measurement into issuing a warning; leading to quality issues of the bathing water.	
2	External Attacker	cyber	Denial of Service	Sensors	ALERT SYSTEM	Raw water bodies	Quality	External Attacker generates a cyber threat causing a Denial of Service of the Sensors of the ALERT SYSTEM which affects Raw water bodies and might lead to a Quality issue	An attacker who knows where are the different sensors put small jammers close to them, preventing them to connect.	
3	External Attacker	cyber	Denial of Service	Sensors	ALERT SYSTEM	Sewers or Wastewater treatment plant	Quality	External Attacker generates a cyber threat causing a Denial of Service of the Sensors of the ALERT SYSTEM which affects Sewers or Wastewater treatment plant and might lead to a Quality issue	An attacker who knows where are the different sensors put small jammers close to them, preventing them to connect.	
4	External Attacker	cyber	Manipulation of the data	Sensors	ALERT SYSTEM	Sewers or Wastewater treatment plant	Quality	External Attacker generates a cyber threat causing a Manipulation of the data of the Sensors of the ALERT SYSTEM which affects Sewers or Wastewater treatment plant and might lead to a Quality issue	An attacker steal a sensor in order to access the firmware on it an possibly get access to the server (he might want to send fake data).	
								External Attacker generates a cyber threat causing a	An attacker steal a sensor in	

Figure 6 Risk events page



Risk Reduction Measures (73 loaded)

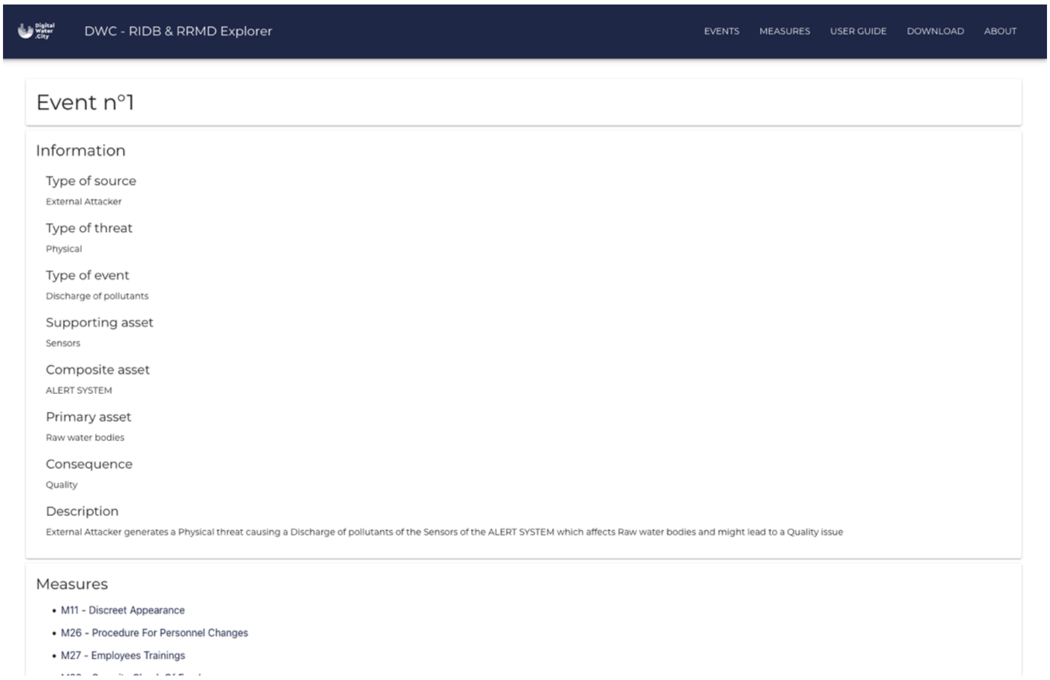
ID	Name	Description	Type of measure	Type of source	Type of threat	Type of event	Specific asset	Consequenc
M01	Fences And Walls	Construction of fences or walls around sensitive sites. By the construction of such physical barriers the entrance to sensitive sites is impeded. The aim is to ensure that no unauthorized personnel gets access to sensitive buidlings, assets or infrastructures.	• Physical Barriers	• External attacker	• Cyber	• Denial of service • Manipulation of the data	• Sensors • Early warning system for safe water reuse	• Quality
M02	Motion Detectors	Implementation of motion detectors. Thus the intrusion of unauthorized personnel to sensitive sites is automatically detected. The aim is to be able to react quickly to occuring intrusions.	• Control System • Consequence Mitigation • Action and Crisis Management Plans and Training	• External attacker • Internal attacker • Action and Crisis Management Plans and Training	• Physical • Cyber-Physical	• Destruction • Manipulation • Pollution	• Additives • Control Center • Control System • Dosing System • Pressure Boosting Station • Pump • Server • Transmission Devices • Treatment Unit Process • Water under treatment	• Quantit • Quality • Financi • Reputat
M03	Camera Surveillance	Surveillance of sensitive sites, buildings or assets with camera systems. Thus intruders are detected by the staff that is surveilling the monitors. The aim is to be able to react quickly to occuring intrusions or intrusion attempts and to be able to identify the attacker after an occuring attack.		• Internal attacker • Human fault • External attacker	• Physical • Cyber	• Destruction • Manipulation of the data • Denial of service	• Sensors • Ds11 flow forecast • Early warning system for safe water reuse	• Not seri • Quality

Figure 7 Risk reduction measures page

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

4.5.3. Detailed events & detailed measures pages

Clicking on an event or a measure shows the detailed page for that element with all the attributes entered in the database. When looking at a specific event, the list of applicable measures is available and can be used to navigate to the measures' detailed pages directly.



Event n°1

Information

Type of source
External Attacker

Type of threat
Physical

Type of event
Discharge of pollutants

Supporting asset
Sensors

Composite asset
ALERT SYSTEM

Primary asset
Raw water bodies

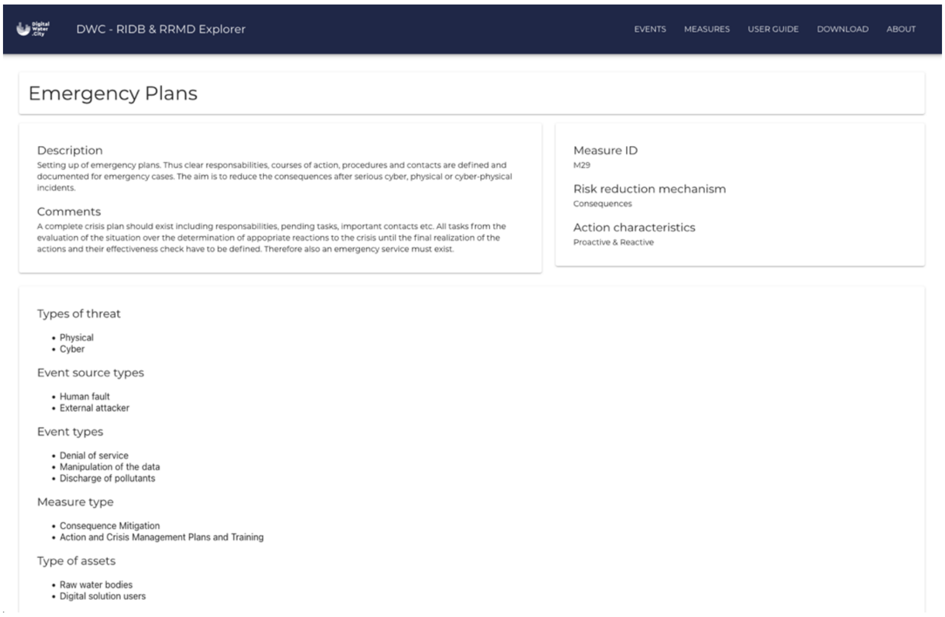
Consequence
Quality

Description
External Attacker generates a Physical threat causing a Discharge of pollutants of the Sensors of the ALERT SYSTEM which affects Raw water bodies and might lead to a Quality issue

Measures

- M11 - Discreet Appearance
- M26 - Procedure For Personnel Changes
- M27 - Employees Trainings

Figure 8 Detailed view of a risk event



Emergency Plans

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

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

Measure ID
M29

Risk reduction mechanism
Consequences

Action characteristics
Proactive & Reactive

Types of threat

- Physical
- Cyber

Event source types

- Human fault
- External attacker

Event types

- Denial of service
- Manipulation of the data
- Discharge of pollutants

Measure type

- Consequence Mitigation
- Action and Crisis Management Plans and Training

Type of assets

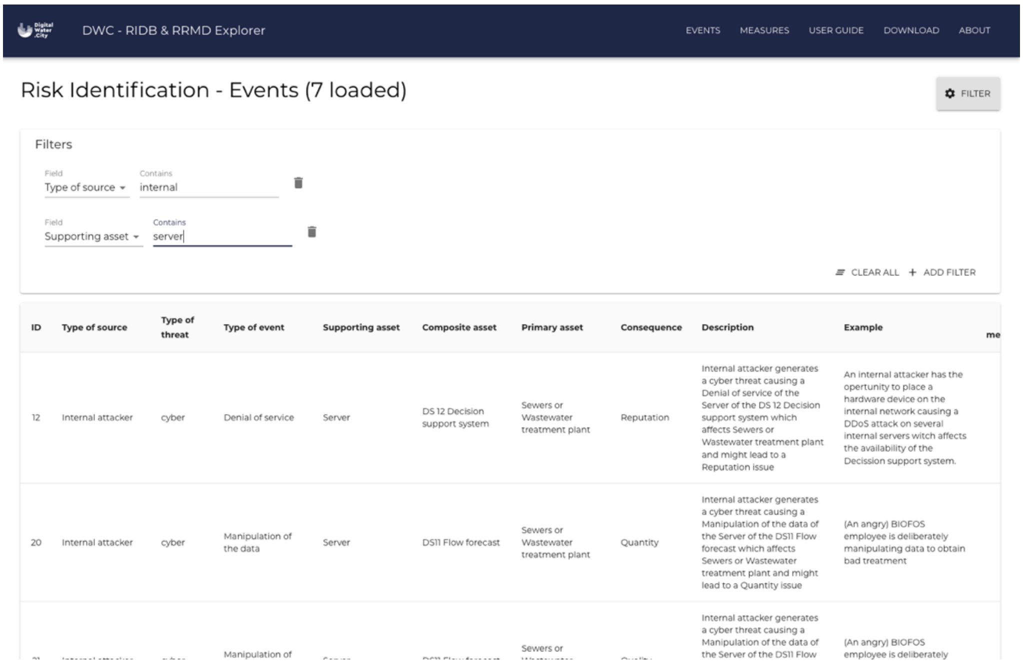
- Raw water bodies
- Digital solution users

Figure 9 Detailed view of a risk reduction measure

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

4.5.4. Filtering

Both the events and measures pages have basic filtering capabilities. One can add consecutive filters on specific fields.



Risk Identification - Events (7 loaded)

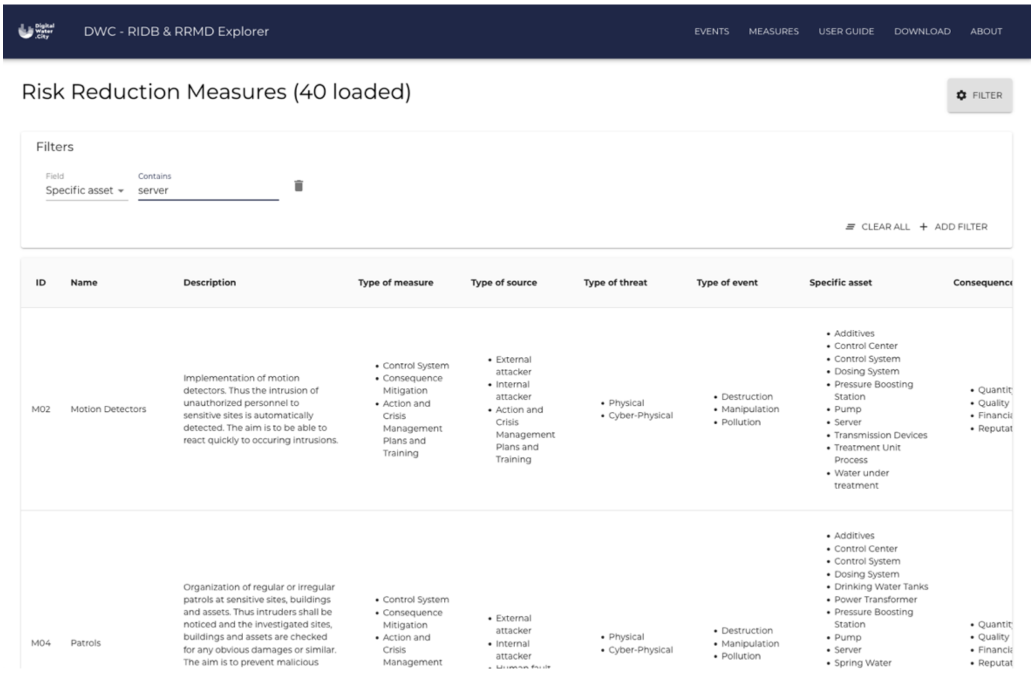
Filters

Field: Type of source — Contains: internal

Field: Supporting asset — Contains: server

ID	Type of source	Type of threat	Type of event	Supporting asset	Composite asset	Primary asset	Consequence	Description	Example	me
12	Internal attacker	cyber	Denial of service	Server	DS 12 Decision support system	Sewers or Wastewater treatment plant	Reputation	Internal attacker generates a cyber threat causing a Denial of service of the Server of the DS 12 Decision support system which affects Sewers or Wastewater treatment plant and might lead to a Reputation issue	An internal attacker has the opertunity to place a hardware device on the internal network causing a DDoS attack on several internal servers witch affects the availability of the Decission support system.	
20	Internal attacker	cyber	Manipulation of the data	Server	DS11 Flow forecast	Sewers or Wastewater treatment plant	Quantity	Internal attacker generates a cyber threat causing a Manipulation of the data of the Server of the DS11 Flow forecast which affects Sewers or Wastewater treatment plant and might lead to a Quantity issue	(An angry) BIOFOS employee is deliberately manipulating data to obtain bad treatment	
			Manipulation of			Sewers or		Internal attacker generates a cyber threat causing a Manipulation of the data of the Server of the DS11 Flow	(An angry) BIOFOS employee is deliberately	

Figure 10 Filtering example on the risk events



Risk Reduction Measures (40 loaded)

Filters

Field: Specific asset — Contains: server

ID	Name	Description	Type of measure	Type of source	Type of threat	Type of event	Specific asset	Consequence
M02	Motion Detectors	Implementation of motion detectors. Thus the intrusion of unauthorized personnel to sensitive sites is automatically detected. The aim is to be able to react quickly to occuring intrusions.	• Control System • Consequence Mitigation • Action and Crisis Management Plans and Training	• External attacker • Internal attacker • Action and Crisis Management Plans and Training	• Physical • Cyber-Physical	• Destruction • Manipulation • Pollution	• Additives • Control Center • Control System • Dosing System • Pressure Boosting Station • Pump • Server • Transmission Devices • Treatment Unit Process • Water under treatment	• Quantit • Quality • Financi • Reputat
M04	Patrols	Organization of regular or irregular patrols at sensitive sites, buildings and assets. Thus intruders shall be noticed and the investigated sites, buildings and assets are checked for any obvious damages or similar. The aim is to prevent malicious	• Control System • Consequence Mitigation • Action and Crisis Management	• External attacker • Internal attacker	• Physical • Cyber-Physical	• Destruction • Manipulation • Pollution	• Additives • Control Center • Control System • Dosing System • Drinking Water Tanks • Power Transformer • Pressure Boosting Station • Pump • Server • Spring Water	• Quantit • Quality • Financi • Reputat

Figure 11 Filtering example on the risk reduction measures

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

5. Conclusions

Deliverable 4.2 consists of the RIDB and the RRMD databases, available as excel data at risk-explorer.digital-water.city/download/ and as online version at risk-explorer.digital-water.city. The databases are supported by this report that presents the scope of the work and its contribution to the implementation of a risk management process in relation to cyber-physical protection of the DWC cities' infrastructure when adopting the DWC solutions.

The report also explains the methodology adopted in developing the databases and it provides an in-depth description of the attributes of each database. Finally, both RIDB and RRMD have been merged, resulting in the creation of a web-based explorer, which facilitates the navigation through events and RRMs and vice versa.

The RIDB and the RRMD databases were built on previous work performed in other EC funded projects where similar databases related to risks due to other threats, as climate impact and water contamination. They proved to be considered a valuable supporting tool by water utilities in the process of starting the steps of risk identification and risk treatment as source of inspiration for further in-depth analysis steps.

In DWC, the RIDB and the RRMD have been adapted to the scope of identifying and treating risks induced by new cyber and physical vulnerabilities created by the adoption of the DWC solutions. Furthermore, the structure of the existing databases has been enhanced to capture the requirements of the DWC potential users (the DWC cities) and an explorer has been created to facilitate the search. Both databases are designed to be enriched with new entries during and beyond the project.

The databases have been created to specifically address the DWC solutions: However, given the wide range of digital technologies (e.g. sensors, modelling, AR, etc.) considered along the urban water cycle, we are confident that both databases could be of strong relevance for European utilities in charge of the management of water and sewer infrastructures.

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

6. References

Almeida M.C, Ugarelli R., Vieira P., Cardoso M.A., (2013). Risk identification database. Guidance on hazard selection and use on WCSP - D 2.2.4

Almeida, M.d.C., Strehl, C., Vieira, P., Mälzer, H.-J. and Cardoso, M.A. (2014) D2.4.3: Risk reduction of climate change related risks in water systems. Guidance to risk treatment step., PREPARED.

Beuken, R., S. Sturm, J. Kiefer, M. Bondelind, J. Åström, A. Lindhe, I. Machenbach, E. Melin, T. Thorsen, B. Eikebrokk, C. Niewersch, D. Kirchner, F. Kozisek, D. W. Gari, and C. Swartz (2007), Identification and description of hazards for water supply systems - A catalogue of today's hazards and possible future hazards, TECHNEAU, Deliverable no. D 4.1.1, D 4.1.2.

ISO (2009a). ISO 31 000:2009 Risk management. Principles and guidelines. International Standards Organization.

ISO (2009b). ISO 31 010:2009 Risk management. Risk assessment techniques. International Standards Organization.

Ostfeld, A., Salomons, E., Smeets, P., Makropoulos, C., Bonet, E., Meseguer, J., Mälzer, H.-J., Vollmer, F. and Ugarelli, R. (2018) D3.2 Risk Identification Database (RIDB), STOP-IT.

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

Ugarelli R. , M. C. Almeida, K. Behzadian, T. Liserra, P. Smeets, Z. Kapelan (2014). Sustainability risk based assessment of the integrated urban water system: a case study of Oslo. 11th International Conference on Hydroinfor-matics - HIC 2014, New York City, USA

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

7. Appendix

The RIDB and RRMD come with different Python scripts to automate the update of the RRMD based on the RIDB *(ridb_to_rrmd.py*), thus preventing errors and saving time, and to export the risk events and risk measures in a more machine friendly format (*ridb_to_json.py* and *rrmd_to_json.py*) to be used in the risk explorer application. A shell script (*update.sh*) automates the full process.

```
#!/usr/bin/env python3

"""
    File name: ridb_to_rrmd.py
    Version: 1.0
    Author: Guillaume Bour (guillaume.bour@sintef.no)
    Last modified: 2021/10/12
    License: MIT License
    Description: A script to update the RRMD based on the RIDB.
"""

from openpyxl import load_workbook
import json

RRMD_SPAN = 24

wb = load_workbook(filename="data/ridb.xlsx")
wb.active = 3  # Selection of the database sheet
ws = wb.active

wb2 = load_workbook(filename="data/rrmd.xlsx")
wb2.active = 3
ws2 = wb2.active


def read_event_and_update_measures(i, measures):

    print("[+] Handling event %d" % i)
    evt_id = str(ws["A{}".format(2 + i)].value)
    evt_type_of_source = ws["B{}".format(2 + i)].value
    evt_type_of_threat = ws["C{}".format(2 + i)].value
    evt_type_of_event = ws["D{}".format(2 + i)].value
    evt_supporting_asset = ws["E{}".format(2 + i)].value
    evt_composite_asset = ws["F{}".format(2 + i)].value
```

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

```python
    evt_primary_asset = ws["G{}".format(2 + i)].value
    evt_consequence = ws["H{}".format(2 + i)].value
    evt_description = ws["I{}".format(2 + i)].value
    evt_measures = [m.strip() for m in str(ws["K{}".format(2 + i)].value).split(",")]

    if evt_type_of_source == "" or evt_type_of_source == None:
        return False

    for measure_id in evt_measures:

        if measure_id not in measures.keys():
            measures[measure_id] = {
                "type_of_source": set(),
                "type_of_threat": set(),
                "type_of_event": set(),
                "specific_asset": set(),
                "type_of_asset": set(),
                "consequence": set(),
            }

        measures[measure_id]["type_of_source"].add(normalize_text(evt_type_of_source))
        measures[measure_id]["type_of_threat"].add(normalize_text(evt_type_of_threat))
        measures[measure_id]["type_of_event"].add(normalize_text(evt_type_of_event))
        measures[measure_id]["specific_asset"].add(normalize_text(evt_supporting_asset))
        measures[measure_id]["specific_asset"].add(normalize_text(evt_composite_asset))
        measures[measure_id]["type_of_asset"].add(normalize_text(evt_primary_asset))
        measures[measure_id]["consequence"].add(normalize_text(evt_consequence))

    return True


def update_rrmd(measures):
    s_c = 0
    u_c = 0

    for m_id, values in measures.items():
        start_row = 2 + RRMD_SPAN * (int(m_id) - 1)
        cell = "B{}".format(start_row)

        m_name = ws2[cell].value
        if m_name == "" or m_name == None:
            # we reached the end of the defined measures
            break

        if values["type_of_source"] == set():
            print("[-] Skipping measure %s" % m_id)
            s_c += 1
            continue
        print("[+] Updating %s" % m_name)

        # Cleaning first
        clean_cell("E", start_row)
        clean_cell("F", start_row)
        clean_cell("G", start_row)
        clean_cell("H", start_row)
        clean_cell("I", start_row)
        clean_cell("J", start_row)

        add_list_cell("E", start_row, values["type_of_source"])
        add_list_cell("F", start_row, values["type_of_threat"])
        add_list_cell("G", start_row, values["type_of_event"])
        add_list_cell("H", start_row, values["specific_asset"])
        add_list_cell("I", start_row, values["type_of_asset"])
        add_list_cell("J", start_row, values["consequence"])

        u_c += 1

    print("Done with the update: %s updated, %s skipped" % (u_c, s_c))


def clean_cell(column, start_row):
    for k in range(RRMD_SPAN):
        c = "{}{}".format(column, start_row + k)
        ws2[c] = ""


def add_list_cell(column, start_row, l):
    for idx, elt in enumerate(l):
        if idx >= RRMD_SPAN:
            print("********** TOO MANY ITEMS IN THE LIST, SKIPPING **********")
            break
        ws2["{}{}".format(column, start_row + idx)] = elt


def normalize_text(t):
    if t is None:
        return ""
    return t.lower().capitalize()


if __name__ == "__main__":
    measures = {}

    keep_reading = True
    k = 0

    while keep_reading:
        keep_reading = read_event_and_update_measures(k, measures)
        k += 1

    d = 0
    for mid, values in measures.items():
        if len(values["type_of_source"]) != 0:
            d += 1

    print("%d measures used" % d)
    update_rrmd(measures)
    wb2.save(filename="data/rrmd.xlsx")
```

ridb_to_rrmd.py

```
#!/usr/bin/env python3

"""
    File name: ridb_to_json.py
    Version: 1.0
    Author: Guillaume Bour (guillaume.bour@sintef.no)
    Last modified: 2021/10/12
    License: MIT License
    Description: A script to export the RIDB to JSON.
"""

```

```python
from openpyxl import load_workbook
import json

RIDB_FILE = "data/ridb.xlsx"
OUTPUT_FILE = "public/resources/events.json"

print("[+] Loading RIDB from %s" % RIDB_FILE)
wb = load_workbook(filename=RIDB_FILE)
wb.active = 3  # Selection of the database sheet
ws = wb.active


def read_event(i):
    print("[+] Handling event %d" % i)
    evt_id = str(ws["A{}".format(2 + i)].value)
    evt_type_of_source = ws["B{}".format(2 + i)].value
    evt_type_of_threat = ws["C{}".format(2 + i)].value
    evt_type_of_event = ws["D{}".format(2 + i)].value
    evt_supporting_asset = ws["E{}".format(2 + i)].value
    evt_composite_asset = ws["F{}".format(2 + i)].value
    evt_primary_asset = ws["G{}".format(2 + i)].value
    evt_consequence = ws["H{}".format(2 + i)].value
    evt_description = ws["I{}".format(2 + i)].value
    evt_example = ws["J{}".format(2 + i)].value
    evt_measures = [m.strip() for m in str(ws["K{}".format(2 + i)].value).split(",")]

    event = {}
    event["id"] = evt_id
    event["type_of_source"] = evt_type_of_source
    event["type_of_threat"] = evt_type_of_threat
    event["type_of_event"] = evt_type_of_event
    event["supporting_asset"] = evt_supporting_asset
    event["composite_asset"] = evt_composite_asset
    event["primary_asset"] = evt_primary_asset
    event["consequence"] = evt_consequence
    event[
        "description"
    ] = "%s generates a %s threat causing a %s of the %s of the %s which affects %s and might lead to a %s issue" % (
        evt_type_of_source,
        evt_type_of_threat,
```

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

```
        evt_type_of_event,
        evt_supporting_asset,
        evt_composite_asset,
        evt_primary_asset,
        evt_consequence,
    )
    event["example"] = evt_example
    event["measures"] = evt_measures

    return event


if __name__ == "__main__":
    events = []
    keep_reading = True
    k = 0
    while keep_reading:
        m = read_event(k)
        if m["type_of_source"] == "" or m["type_of_source"] == None:
            break
        events.append(m)
        k += 1

    with open(OUTPUT_FILE, "w") as of:
        json.dump(events, of)
```

ridb_to_json.py

```
#!/usr/bin/env python3

"""
    File name: rrmd_to_json.py
    Version: 1.0
    Author: Guillaume Bour (guillaume.bour@sintef.no)
    Last modified: 2021/10/12
    License: MIT License
    Description: A script to export the RRMD to JSON.
"""

from openpyxl import load_workbook
import json
```

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

```
RRMD_FILE = "data/rrmd.xlsx"
OUTPUT_FILE = "public/resources/measures.json"
RRMD_SPAN = 24

wb2 = load_workbook(filename="data/rrmd.xlsx")
wb2.active = 3
ws2 = wb2.active


def read_list(column, start_row, span):
    elts = []
    for k in range(span):
        elt = ws2["{}{}".format(column, start_row + k)].value
        if elt is not None:
            elts.append(elt)
    return elts


def read_measure(i):
    print("[+] Handling measure %d" % i)
    m_row = 2 + i * RRMD_SPAN
    measure_id = str(ws2["A{}".format(m_row)].value)
    measure_name = ws2["B{}".format(m_row)].value
    measure_description = ws2["C{}".format(m_row)].value
    measure_type = read_list("D", m_row, RRMD_SPAN)
    measure_type_of_source = read_list("E", m_row, RRMD_SPAN)
    measure_type_of_threat = read_list("F", m_row, RRMD_SPAN)
    measure_type_of_event = read_list("G", m_row, RRMD_SPAN)
    measure_specific_asset = read_list("H", m_row, RRMD_SPAN)
    measure_type_of_asset = read_list("I", m_row, RRMD_SPAN)
    measure_consequence = read_list("J", m_row, RRMD_SPAN)
    measure_risk_reduction_mechanism = ws2["K{}".format(m_row)].value
    measure_characteristic_of_action = ws2["L{}".format(m_row)].value
    measure_comments = ws2["M{}".format(m_row)].value
    measure_details = ws2["O{}".format(m_row)].value

    return {
        "id": measure_id,
        "short_name": measure_name,
        "description": measure_description,
```

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

```
        "type_of_measure": measure_type,
        "type_of_source": measure_type_of_source,
        "type_of_threat": measure_type_of_threat,
        "type_of_event": measure_type_of_event,
        "specific_asset": measure_specific_asset,
        "type_of_asset": measure_type_of_asset,
        "consequence": measure_consequence,
        "risk_reduction_mechanism": measure_risk_reduction_mechanism,
        "characteristics_of_action": measure_characteristic_of_action,
        "comments": measure_comments,
        "details": measure_details,
    }


if __name__ == "__main__":
    rrm = []
    keep_reading = True
    k = 0
    while keep_reading:
        m = read_measure(k)
        if m["short_name"] == None or m["short_name"] == "":
            break
        rrm.append(m)
        k += 1

    with open(OUTPUT_FILE, "w") as outfile:
        json.dump(rrm, outfile)
```

ridb_to_json.py

```
#! /bin/sh


RIDB_FILE=./data/ridb.xlsx
RRMD_FILE=./data/rrmd.xlsx


RIDB_PUBLIC=./public/resources/ridb.xlsx
RRMD_PUBLIC=./public/resources/rrmd.xlsx


RIDB_TMP_FILE=./data/~\$ridb.xlsx
RRMD_TMP_FILE=./data/~\$rrmd.xlsx
```

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

```
if test -f $RIDB_TMP_FILE; then
    echo "Please close the RIDB file before updating."
    exit -1
fi

if test -f $RRMD_TMP_FILE; then
    echo "Please close the RRMD file before updating."
    exit -1
fi

echo "Updating RRMD based on the RIDB..."
python3 scripts/ridb_to_rrmd.py


if [ $? -eq 0 ]
then
    echo "Exporting RIDB to JSON..."
    python3 scripts/ridb_to_json.py

    echo "Exporting RRMD to JSON..."
    python3 scripts/rrmd_to_json.py
else
    echo "Error during the update of the RRMD."
    exit -1
fi

cp $RIDB_FILE $RIDB_PUBLIC
cp $RRMD_FILE $RRMD_PUBLIC
```

update.sh

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

Digital Water .City

Leading urban water management to its digital future

digital-water.city
digitalwater_eu

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.