IWA World Water Congress & Exhibition
11-15 SEPTEMBER 2022 | COPENHAGEN, DENMARK | www.worldwatercongress.org

# A Cyber-Physical all-hazard risk management approach: the case of the WWTP of Copenhagen

**C. Bosco*, G. Bour**, I. Selseth*, C. Thirsing***, D. Thornberg***, S. Lindberg****, M.G. Jaatun**, R.M. Ugarelli***

*SINTEF Community, S.P. Andersens vei 3, Trondheim, Norway, camillo.bosco@sintef.no
**SINTEF Digital, Stindvegen 4, Trondheim, Norway
***BIOFOS A/S, Refshalevej 250, 1432 Copenhagen K, Denmark
****DHI, Agern Alle 5, 2970 Hørsholm, Denmark

**Abstract:** The ongoing digitalization in the water sector enables more efficient processes, but also comes with new challenges related to potential cyber-physical attacks on the water systems. To manage the associated risk, a precise and systematic framework should be adopted. This paper describes a methodology that is consistent with the Risk Management ISO (31000-2018) and builds on specific tools developed within the H2020 Digital Water City (DWC) project (https://www.digital-water.city). The demonstration of the approach concerns a digital solution of the DWC project which allows to visualize inflow's predictions at the Waste Water Treatment Plant (WWTP) in the city of Copenhagen. Specifically, the risk assessment and risk treatment options are demonstrated in the case of the spoofing of the web interface where forecast data are visualized by operators, leading to a wrong flow prediction and thus to a wrong maintenance schedule.

**Keywords**: cyber-security; risk management; water system

## 1. Introduction

As part of the planning and implementation of digital solutions to support water industry processes, risk management plays a fundamental role in limiting the risk associated with economic, social, and environmental losses. In fact, through risk management the threats that can emerge from digital tools can be addressed in a systematic way, according to the four steps of risk management in ISO standard 31000-2018 (Identification, Analysis, Evaluation, and Treatment) shown in Figure 1.1. The presented approach extends and customizes the work of STOP-IT (https://stop-it-project.eu/) to the DWC solutions.

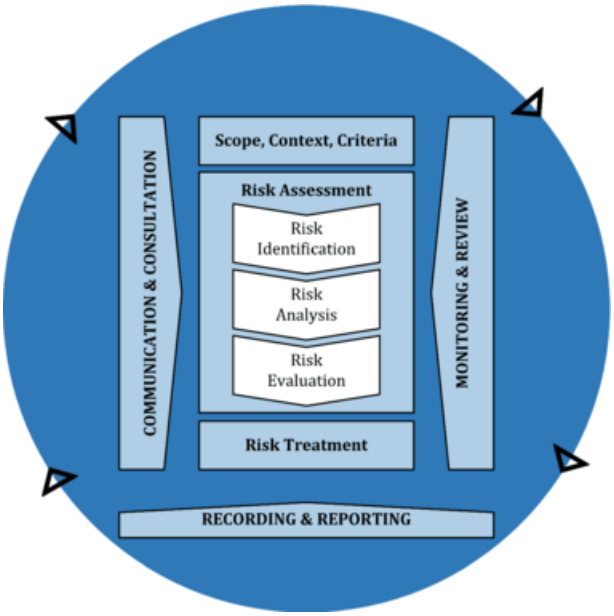


**Figure 1.1** Steps of Risk Management (ISO 31000-2018)

## 2. Methods

To address the various steps of Risk Management, specific methods and tools have been developed as part of the DWC Project. The Risk Identification Database (RIDB) was designed to support water organizations in the first step of the Risk Assessment (Ostfeld et al., 2018). It covers the events identified by DWC partners as the most relevant risks related to their digital solutions developed in the project. The sentence's structure is the same for each record to ensure consistency, as shown in Figure 2.1

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

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

**Figure 2.1** Records structure in the RIDB

According to the Risk Management framework, the Risk Analysis part should focus on estimating probabilities and consequences. Given a digital twin of the analysed system, stress testing can be adopted to compute the expected consequences for the selected Key Performance Indicators (KPIs) under a wide range of scenarios, once the cyber-attack was successful (Nikolopoulos et al., 2020). On the other hand, the probability of a successful cyber-attack could be estimated by historical data or by structured subjective assessment. Resulting KPIs are compared with target values in the Risk Evaluation phase, and potential decisions to take actions to mitigate the risk might be taken accordingly.

Finally, the purpose of the Risk Treatment is to select and implement the best options for addressing the identified risk (Mälzer et al., 2019). The DWC project provides a Risk Reduction Measures Database (RRMD) where several risk reduction measures were gathered and associated to related risks events of the RIDB (https://zenodo.org/record/5735537).

## 3. Results and discussion

The DWC Digital Solution "*Web platform for integrated sewer and wastewater treatment plant control*" was selected to demonstrate the discussed methodology. The solution allows the manager of the WWTP of Copenhagen to visualize the predictions of the inflow at the WWTP, up to 48 hours in advance. Since the water organization performs periodically maintenance on one of the four parallel lines of the WWTP, an internal attacker could manipulate the data visualization, leading to a wrong flow prediction and thus to a wrong maintenance schedule. In the cyber-attack scenario, the actual rain information has been hidden, leading to an unexpected discharge overload in the three lines left in operation. The reduced capacity might be compensated to a certain extent by the existing equalization tanks which may adsorb the generated flow overloads. The characteristics of the considered water system and risk event are shown in Table 3.1 and Figure 3.1, respectively.

**Table 3.1** Characterization of the analysed water system

| Characteristics of the System | Values | Units |
|---|---|---|
| Number of Treatment Lines of the WWTP | 4 | [-] |
| Capacity of each Treatment Line | 2.500 | [$m^3/h$] |
| Total Volume of the Equalization Tanks | 44.000 | [$m^3$] |

**Internal attacker** generates a **cyber** threat causing a **Spoofing** of the **Web application** of the **Web platform for integrated sewer and wastewater treatment plant control** which affects **Sewers or Wastewater treatment plant** and might lead to a **Quantity** issue

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

**Figure 3.1** Structure of the selected event in the RIDB

The consequences, illustrated in Figure 3.2, have been assessed in terms of a selected KPI (cubic meters of biologically untreated wastewater) through the stress testing of a digital twin of the water system with reduced capacity, by considering the historical inflows of 2020.

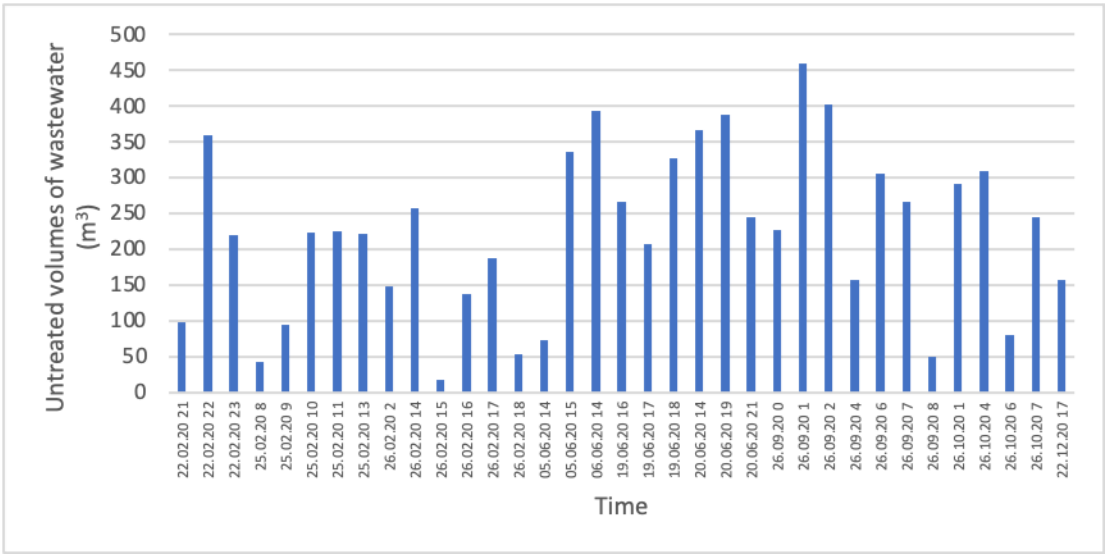


**Figure 3.2** Consequences resulting from the stress-testing procedure

The outcome of the Risk Assessment can lead to the adoption of some mitigation measures which should be further investigated through a cost-benefit analysis. From the RRMD, the following measures depicted in Figure 3.3, linked to the identified risk, are suggested.

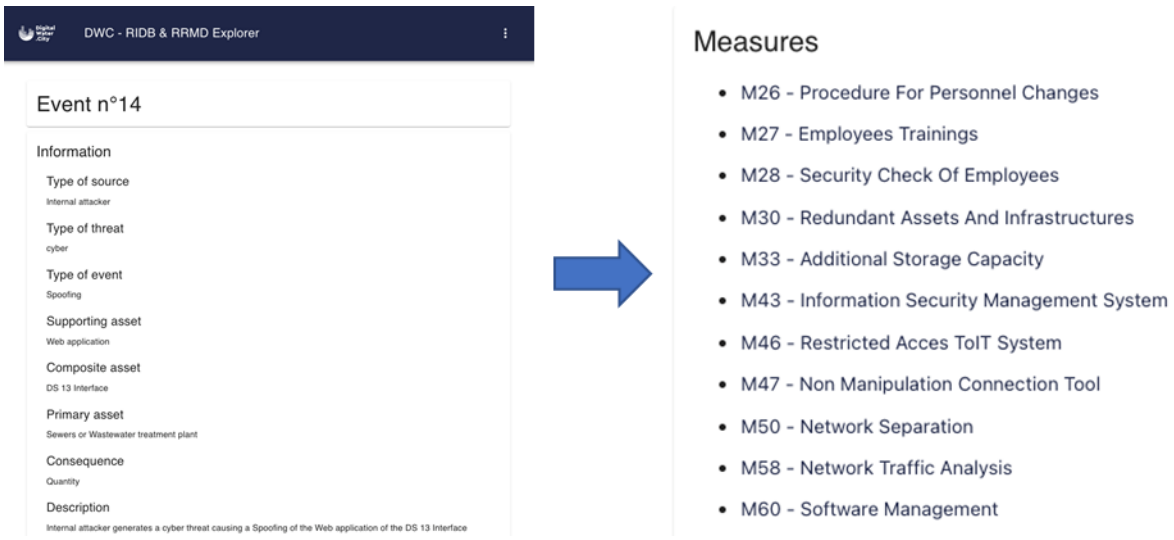


**Figure 3.3** Risk reduction measures in the RRMD associated with the identified risk in the RIDB

## 4. Conclusions

The described methodology supports the adoption of a risk management process covering both safety and cyber security. Due to the increased level of digitalization of the operations in water systems, new vulnerabilities are introduced and must be addressed. To limit the undesirable effects that digital tools may bring, a set of tools and methods developed as a part of the DWC project serves as a guide for other water utilities that need to assess the risks associated with digital solutions.

## REFERENCES

ISO (2018). ISO 31 000:2018 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.

Nikolopoulos, D., Moraitis, G., Bouziotas, D., Lykou, A., Karavokiros, G., & Makropoulos, C. (2020). Cyber-physical stress-testing platform for water distribution networks. Journal of Environmental Engineering, 146(7), 04020061.

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

## Funding

The work reported in this paper has received funding from the DWC project, European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.