Webinar – Managing risks from digitalisation in the Water sector
1st April 2020

Questions and Answers:

Q: Are there recorded incidents of DOS incidents, ransomware or malicious operation of water systems in the water sector? Are there any specific issues related to standardization in cyber security in water sector?

A: Please see some examples: www.cyberscoop.com/ransomware-hits-onwasa-computer-network-north-carolina-water-utility/; www.ajc.com/news/local/rockdale-water-customers-can-make-payments-again-after-ransomware-attack/4GshKfGFW0w8yjCOh376SM/; https://ascelibrary.org/doi/abs/10.1061/%28ASCE%29EE.1943-7870.0001686

(The last one is an extensive review of cybersecurity attacks on the water sector, including ransomware and cryptojacking suggested by an attendee of the webinar)

Regarding standardization, specific for the water sector, there is not much. We have created a task force under the ICT4Water cluster (the 'cybersecurity action group') to focus specifically on this aspect of cybersecurity.

There is a need to be aware of what's happening with other utility services also. This article discusses a ransomware attack on a power company in South Africa**:** www.welivesecurity.com/2019/07/26/south-africa-johannesburg-ransomware/

Q: It is a good idea to make the existing centralised water and wastewater system more smart, but it needs lot of further investment. Why are we not moving to distributed water systems? These are easier to operate and digital technologies can be used to operate them and can be more sustainable.

A: Yes, there will initial investment costs, but we believe these costs will be recovered within a short time (i.e. savings associated with the examples discussed in the presentation). It is also believed that it is only a matter of time before more and more utilities begin using digital water technologies, especially as they develop new infrastructure.

It is certainly a good idea to consider integrating digital water solutions when planning and implementing the rehabilitation of deficient water systems. Decisions on the incorporation of new and improved technologies into a water system are specific to the local system. As discussed in the webinar, one way to consider the viability of tools and capabilities is benefit-risk assessment.

We have discussed the specific issue of distributed water systems and cybersecurity in a recent technical paper on resilience.[1] We argue that although distributed solutions allow for a spreading and minimization of (spatial) risks, there are important (often hidden) ways in which even the most distributed configurations remain "centralized". A case in point is cybersecurity: More often than not several distributed water systems in a given area, will be controlled through a central SCADA system, and thus, still be vulnerable to cyber-attacks –

[1] Nikolopoulos, D., van Alphen, H.J., Vries, D., Palmen, L., Koop, S., van Thienen, P., Medema, G. and Makropoulos, C., 2019. Tackling the "New Normal": A resilience assessment method applied to real-world urban water systems. *Water*, *11*(2), p.330.

and perhaps, even more vulnerable than a single, well-protected centralised water infrastructure system.

Q: From your analysis, how best would this platform have dealt with the case of Israel and the cyber attack on their waste system?

A: MEKOROT is a partner in STOP-IT. I think this is a question they are in a much better position to answer: www.mekorot.co.il/Eng/newsite/Pages/default.aspx

Q: How do we obtain the software and is it free?

A: The software is not available yet. The project is ongoing, though we expect to have a solution with a clear exploitation model within the next few months. Please contact us through the STOP-IT website and register your interest. We will come back to you with updated information as it is available.

Q: Can we use KPI-TOLL to develop a Water Safety Plan?

A: In principle yes. But this activity does require a level of 'mapping' between results and the requirements for a WSP. This is of interest and Dr, Patrick Smeets of KWR is exploring this potential application.

Q: Is the platform commercially available?

A: Not yet. The project is ongoing, though we expect to have a solution with a clear exploitation model within the next few months. Please contact us through the STOP-IT website to register your interest and we will come back to you.

Q: Is the hybrid system (digital and analog) able to reduce the risk rather than merely digital system?

A: Our point was that a water system is always a hybrid system: pipes are analog whereas controls are digital. You need tools and models that can simulate both in various combinations.

Q: So the solution to mitigate digital risks is again using digital tools?

A: There is a combination of tools that can be used to solve various problems. However, there should always be the option to manually override some operations (e.g. the control of certain treatment and disinfection processes).

Q: Which part of the world has been tested with this technologies?

A: This is an EU-funded project. The main urban systems tested were in: Oslo (NO), Barcelona (ES), BWB (DE) and Mekorot (IL). Additional utilities in these countries were also involved, though mainly with co-development of training materials and participation in training activities. We are very interested in looking at systems and preparing case studies across other world regions.

Q: How it will help to integrate water quality at the Treatment plant?

A: We have not yet addressed water quality within a WTP within STOP-IT, only water quality within a water distribution network. It is of importance to also integrate treatment and disinfection processes, but this falls outside the scope of the current project.

Q: Why don't we have an alarm kind of provision when something goes abnormal?

A: We are developing this feature in another module within STOP-IT (stop-it-project.eu/). In addition to Module I (featured in the webinar), which supports strategic and tactical planning, we have developed the following additional modules:

Module 2: Secure wireless sensor communications module

Module 3: Toolbox of technologies for securing IT and SCADA

Module 4: Toolbox of technologies for protecting against physical threats in CI

Module 5: Cyber Threat Incident Service

Module 6: Real-Time anomaly detection system

Module 7: Public Warning System-Secure Information Exchange Technologies

Module 8: Reasoning Engine

Module 9: Enhanced Visualisation Interface for the water utilities

Q: At the cyber level, the tools look at the effect of the attack on the system, what measures need to be taken at the cloud security level to ensure the cyber-attacks are kept to a minimum in the first place?

A: Within STOP-IT, we are developing (purely) cyber security risk minimisation tools in other modules. However, these modules are mostly looking into raising alerts (in real time) whenever something suspicious happens - in the cyber realm. Cloud security per se is not part of the work we are currently focused on.

Q: Why does the impact and likelihood map not have any values associated with it?

A: For those interested, you can read more about the concept here:

1) maps.groupmap.com/workspaces/fOwX84XymYnc/maps/X5OlgqZEWvj0/participants/XFvxm68qIbL8
2) www.groupmap.com/map-templates/risk-assessment/

Q: Navigation and allocation of risks in the domain of Impact and likelihood depend upon the perception which varies from person to person. How do you standardise it?

A: For those interested, you can read more about the methodology used here:

1) reports.weforum.org/global-risks-report-2020/appendix-b-methodology/
2) www.groupmap.com/map-templates/risk-assessment/

Panellists’ contact information:

Harsha Ratnaweera harsha.ratnaweera@nmbu.no

Rita Ugarelli Rita.Ugarelli@sintef.no

Christos Makropoulos cmakro@mail.ntua.gr

Zakhar Maletskyi zakhar.maletskyi@nmbu.no

David Tipping david.tipping@hotmail.com