*11th World Congress on Water Resources and Environment (EWRA 2019)*
*"Managing Water Resources for a Sustainable Future"*
*Madrid, Spain, 25-29 June 2019*

# RISKNOUGHT: A Cyber-Physical Stress-Testing Platform For Water Distribution Networks

D. Nikolopoulos[1*], G. Moraitis[1], D. Bouziotas[2], A. Lykou[1], G. Karavokiros[1], C. Makropoulos[1,2]
[1] *Department of Water Resources and Environmental Engineering, School of Civil Engineering, National Technical University of Athens, Iroon Politechniou 5, 157 80 Zografou, Athens, Greece*
[2] *KWR, Water Cycle Research Institute, Groningenhaven 7, 3433 PE Nieuwegein, the Netherlands*
** e-mail: nikolopoulos.dio@gmail.com*

## Introduction

Cyber-Physical systems (CPS) consist of two layers, one comprised of the physical processes, and one computational and networking layer (Lee 2008). Modern water systems (distribution network, treatment plants, etc.) are CPS, as the physical system is supervised and operated by sensors and actuators through SCADA (Supervisory Control And Data Acquisition) in real-time. Advantages of CPS are automation, increased reliability and efficiency. However, a major disadvantage of the networking, communication and remote control of CPS is the susceptibility to cyber and physical attacks (or combinations) (Rasekh et al. 2016). Indeed, various incidents of cyber-physical attacks have threatened real-world water CPS, making them among the most targeted critical infrastructure (ICS-CERT 2016), e.g. like the 2000 Maroochy Water Services incident.

As water CPS are critical for human society, life and health, there is an immediate need of developing robust tools able to assess performance under cyber-physical threat scenarios. Influential work in this new field is implemented by Taormina et al. (2017), with the characterization of cyber-physical attacks in water distribution systems and the development of an EPANET-based modelling environment of such attacks.

In this work, we present the development of a stress-testing modelling platform for Cyber-Physical water distribution systems, able to simulate both the cyber layer information flow and the physical processes.

## Materials and methods

Our modelling platform called RISKNOUGHT (*risk + nought, to risk nothing*) is EPANET-based as it is a proven tool for water distribution network simulations. We use the WNTR toolbox (Klise et al. 2017) which provides the functionality of simulating and analysing systems and model input/output. WNTR has a built-in hydraulic simulation engine using the same equations as EPANET and is also able to use EPANET's engine. The advantage of WNTR simulation engine is the ability to perform Pressure Driven Analysis, which is essential for simulating the inability of meeting demands due to disrupted system operation under a cyber-physical attack. Hence, we use WNTR's simulation engine as the basis of the physical layer of the system.

On top of the physical layer we develop the cyber infrastructure objects: sensors, actuators, Programmable Logic Controllers (PLC), central SCADA and Historian (the database of the SCADA) and their respective connections (wireless, optical fiber etc.). These objects form the control logic of the network by interacting with each other. The control logic explicitly and directly controls the state of the physical layer in each simulation time step. For example: A sensor in a tank senses its level (the actual tank head of the hydraulic simulation in this particular time-step) transmits this information to a PLC, which accordingly to its specified set of instructions sends a signal to an actuator to turn a pump off (setting the pump to off in the hydraulic network). The actuator transmits an ACK ("acknowledged") signal back to the PLC and the PLC reports all inputs and actions to the supervisory SCADA, which stores data in the Historian.

We have developed methods of various interactions between both layers that can simulate a comprehensive list of cyber-physical threat scenarios on a wide range of attack vectors throughout the CPS. This includes:

- Attacks that target sensors, like manipulating readings, making them appear offline or physically destroy them etc.
- Attacks that target actuators, like intercepting signal from PLCs and sending fake ACK messages, making them offline, performing Denial Of Service attacks, alter behaviour etc.
- Attacks on PLCs, like altering/deleting the instruction sets, making them offline etc.
- Attacks on master SCADA and Historian units, like disrupting communications with the slave PLCs, making the whole cyber system offline, altering database values etc.
- Physical attacks on the hydraulic system, like destroying pumps, valves, pipes etc.

More than one attacks are possible to affect multiple components of the system, and start times and duration of the events can be described, using a novel scenario planner tool that sets the environment for the cyber-physical simulation. By using the scenario planner we can conduct a thorough stress-testing of the system with a multitude of different attack combinations and system states in order to identify vulnerabilities and assess performance.

Consequences of the cyber-physical attacks, including cascading effects on the physical layer, can be quantified through the use of selected Key Performance Indicators, in multiple dimensions (e.g. demand coverage, recovery time, Customer Minutes lost), depicting the criticality of the CPS service failure.

## Results and concluding remarks

We present a cyber-physical stress-testing platform able to simulate both the cyber and physical layers of a water distribution network and assess performance versus a wide range of cyber-physical attacks. The use of the platform is presented by utilizing the C-Town water distribution system, which is based on a real-world medium-sized network (Ostfeld et al. 2012), already used as benchmark for similar purposes. It is suggested that such tools are crucial for preparing water utilities to shield their systems from potential threats of the evolving digital landscape.

**Acknowledgments:** STOP-IT has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740610. The publication reflects only the authors' views and the European Union is not liable for any use that may be made of the information contained therein.

## References

ICS-CERT (Industrial Control Systems-Cyber Emergency Response Team) (2016). NCCIC/ICS-CERT year in review: FY 2015. Rep. No. 15-50569. DC: ICS-CERT, Washington.

Klise KA., Hart DB, Moriarty D, Bynum M, Murray R, Burkhardt J, Haxton T (2017). A software framework for assessing the resilience of drinking water systems to disasters with an example earthquake case study. Environmental Modelling and Software 95(1): 420-431. http://doi.org/10.1016/j.envsoft.2017.06.022.

Lee EA (2008) Cyber physical systems: Design challenges. 11th IEEE Int. Symp. on Object Oriented Real-Time Distributed Computing (ISORC), IEEE, New York, 363. http://doi.org/10.1109/ISORC.2008.25.

Ostfeld, A, Salomons E, Ormsbee L, Uber JG (2012) Battle of the water calibration networks. Journal of Water Resources Planning and Management 138(5): 523-532 https://doi.org/10.1061/(ASCE)WR.1943-5452.0000191

Rasekh A, Hassanzadeh A, Mulchandani S, Modi S, Banks MK (2016) Smart water networks and cyber security. Journal of Water Resources Planning and Management 142(7): 01816004. http://doi.org/10.1061/(ASCE)WR.1943-5452.0000646

Taormina R, Galelli S, Tippenhauer NO, Salomons E, Ostfeld A (2017). Characterizing cyber-physical attacks on water distribution systems. Journal of Water Resources Planning and Management 143(5): 04017009. https://doi.org/10.1061/(ASCE)WR.1943-5452.0000749.