Developing a stress-testing platform for cyber-physical water infrastructure

Dionysios Nikolopoulos
Department of Water Resources & Environmental Engineering
National Technical University of Athens
Athens, Greece
nikolopoulos.dio@gmail.com

Christos Makropoulos
Department of Water Resources & Environmental Engineering,
National Technical University of Athens
Athens, Greece
cmakro@chi.civil.ntua.gr

Dimitrios Kalogeras
Institute of Communication and Computer Systems (ICCS)
National Technical University of Athens
Athens, Greece
D.Kalogeras@noc.ntua.gr

Klio Monokrousou
Department of Water Resources & Environmental Engineering,
National Technical University of Athens
Athens, Greece
kmonokrousou@gmail.com

Ioannis Tsoukalas
Department of Water Resources & Environmental Engineering,
National Technical University of Athens
Athens, Greece
jtsoukalas@hotmail.com

***Abstract*—Water supply and sanitation infrastructures are essential for our welfare, but vulnerable to several attacks, typically of physical and cyber types. Cyber-physical attacks on critical infrastructures include chemical and/or biological contamination, physical or communications disruption between the network elements and the supervisory SCADA. Due to the ever-changing landscape of the digital world and the rising concerns about security, there is an emerging need for conceptualizing critical infrastructure as cyber-physical systems and develop a holistic risk management framework for its physical and cyber protection. The framework aims to strengthen the capacities of water utilities to systematically protect their systems, determine gaps in security technologies and improve risk management approaches. Our work envisions the development of a stress testing modelling platform, able to simulate the water system as a complete cyber-physical infrastructure and investigate attack scenarios and possible mitigation measures.**

Keywords—cyber-physical water systems, cyber attacks, stress-testing platform, cyber security

I. Motivation: The security concerns of critical infrastructure

Water supply and sanitation are critical infrastructures (CI) essential for human society, life and health. Despite little publicity or knowledge on risks associated with these critical infrastructures, the fact is that they can be endangered, disrupted or destroyed by events related to physical and cyber threats. These include, but are not restricted to, deliberate attacks, like for example the growing terrorist activities with disastrous consequences for society or hacking attempts for activist/political/ransomware reasons. Such attacks could take various forms, for example chemical contamination, biological contamination, physical component disruption and disruptions of the communication between the network elements and its supervisor/monitoring layer (sensors, actuators, SCADA, data servers, etc.). A successful attack resulting in consequences in one of these areas could effectively cause major damage e.g. long periods of operational downtime, financial losses, loss of trust for water utilities, loss of life, a direct threat to public health, societal and political instability. Promising conceptual and technological solutions to water systems security and resilience do exist [1] but further work is required to bring them together in an overarching risk management framework, strengthen the capacities of water utilities to protect their systems in a systematic way, determine gaps in security technologies and improve their risk management approaches and technologies [2]. In particular, the water industry lacks adaptable/flexible solutions for prevention, detection and mitigation of consequences due to physical and cyber threats, their combination and even the cascading effects from attacks to other CI (e.g. energy). Some large utilities employ some ambitious existing solutions, but these are typically proprietary and not scalable to Small and Medium-sized Utilities (SMU), which also lack the personal/technical and financial resources to test and adapt promising solutions. Hence, there is (i) an urgent need to efficiently tackle cyber-physical security threats, (ii) an existing risk management gap in utilities' practices and (iii) an un-tapped technology market potential for strategic, tactical and operational protection solutions for water infrastructure.

II. Coupling Cyber and Physical Models

Our methodology revolves around coupling cyber systems with physical systems in an integrated model, as part of the

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.

978-1-5386-6744-6/18/$31.00 ©2018 IEEE
DOI 10.1109/CySWater.2018.00009

STOP-IT H2020 project, funded by the European Commission. The challenge here is to make tools that are built for specific purposes (i.e. cyber system emulation and water system simulation) to communicate with each other, operate in-sync and provide feedback. Useful tools/models that could be included in an integrated model include for example MiniCPS [3] which is based on the cyber tool Mininet, EPANET, UWOT [4] and/or possibly others. One possible approach is to use a cyber-oriented tool (like MiniCPS) to define the cyber layer of the model and simulate an attack, explore the physical system's complete water cycle for cascading effects using UWOT and assess the specific effect of the attack on a higher resolution physical model (e.g. EPANET for the distribution network). Figures 1 to 3 depict the usual environment of the three aforementioned tools.

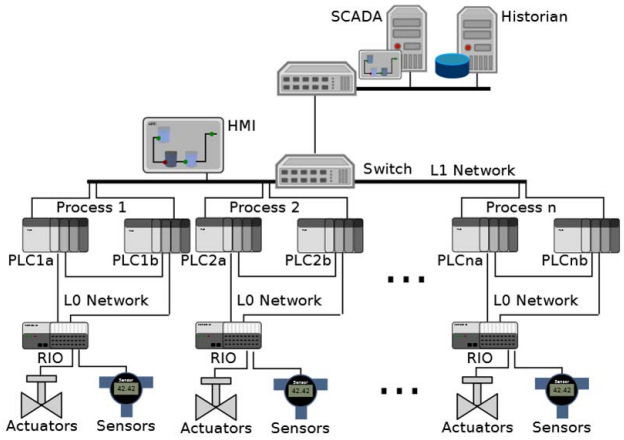

Fig. 1. MiniCPS [4]: Cyber-physical tool build on Mininet, able to simulate cyber attacks.

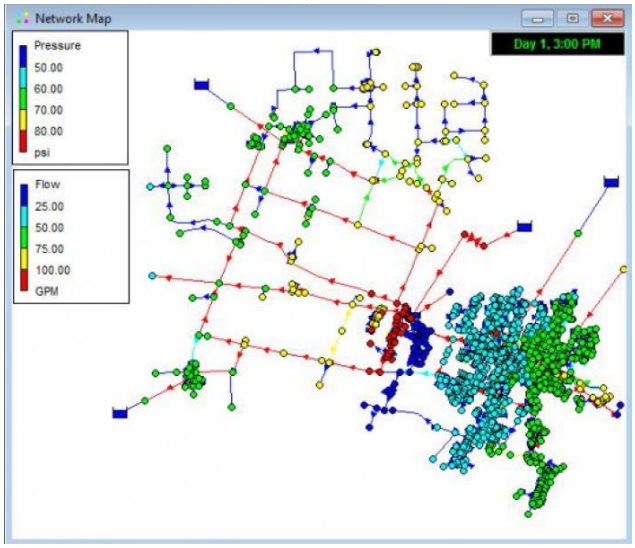

Fig. 2. Epanet, a well known and robust tool for the simulation of distribution networks.

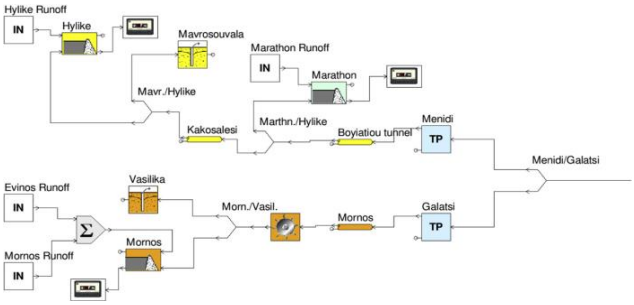

Fig. 3. UWOT [2], an optioneering tool able to simulate the complete urban water cycle.

III. The STOP-IT Stress Testing Platform

The core of STOP-IT is its stress testing platform that provides a test bed for alternative risk treatment options. It is supplement by a toolkit that includes a scenario planner used to define attack scenarios, the models (solvers) for all cyber and physical parts of the water system, a Risk Reduction Measures (RRMs) database and a set of Key Performance Indicators (KPIs) against which the performance (and loss thereof) of the water system will be assessed. The functionality of the stress testing platform includes:

- Deliberately stressing the system under different threat and pressure scenarios generated by the scenario planner and assess its behaviour, including combinations of low probability –high consequence events
- Employment of applicable RRMs to the aforementioned events as prescribed by the database and assessment of their performance against threat scenarios using the KPIs.

The schematic overview of the stress-testing platform is shown in Fig. 4.

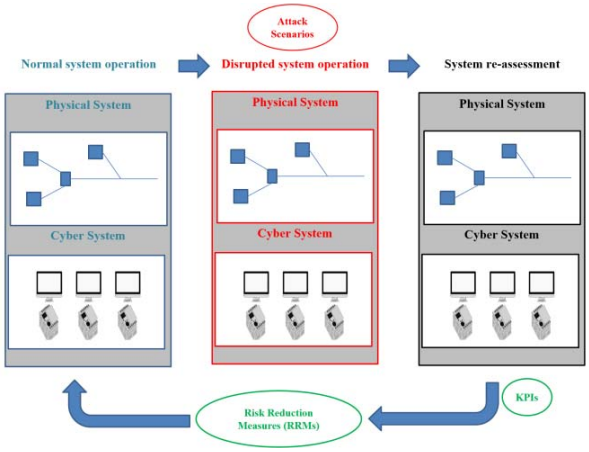

Fig. 4. Schematic overview of the stress testing platform and the connection between components.

IV. Scalable Modelling Approach of the Cyber-Physical System

We aim to make our cyber-physical modelling approach scalable to SMU followers by providing two options for the integrated cyber –physical system, as showcased in Fig. 5. These approaches can be benchmarked against the use of a real legacy SCADA system connected to a simulation of a physical system which should provide the best resolution in terms of monitoring and control of the cyber layer but at a prohibitive cost (monetary or computational) for most stress-testing security applications. The first option, termed S-S (simulation - simulation) is a modelling approach of simulation of both the cyber and physical system, thus being low cost but lower resolution. Still, this scheme provides useful insight of system dynamics in both the cyber and physical layer. The second approach termed S-E-S (simulation – emulation – simulation) implements emulation of the critical cyber elements on top of the S-S approach. This scheme is of higher cost but offers better resolution of the cyber layer i.e. a better exploration of possible threat "pathways" and behaviour of the critical components..

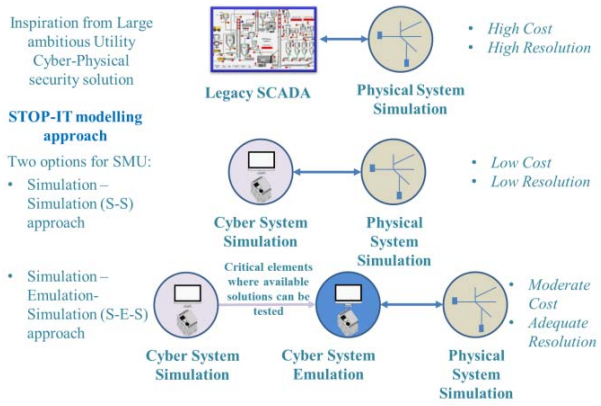

Fig. 5. The modelling aproaches of S-S and S-E-S in the context of cyber-physical security solutions.

V. Discussion

We present an early schematic prototype of a cyber-physical stress-testing platform able to simulate the water system as a complete cyber-physical infrastructure, and investigate physical attack scenarios, cyber-attack scenarios and their combination, while assessing the efficacy of possible mitigation measures. It is suggested that such modelling and testing environments are crucial for preparing water utilities to shield their systems against a dynamically changing digital world landscape, which brings with it significant opportunities but also potential threats that need to be taken seriously (and urgently) into account in the Water Sector's long-term planning process.

References

[1] C. Cook, and K. Bakker, "Water security: Debating an emerging paradigm," Glob. Environ. Chang, vol. 22, pp. 94–102, February 2012.

[2] S. Mittelstädt, X. Wang, T. Eaglin, D. Thom, D. Keim, W. Tolone, and W. Ribarsky, "An integrated in-situ approach to impacts from natural disasters on critical infrastructures," 48th Hawaii International Conference on System Sciences, pp 1118-1127, January 2015.

[3] D. Antonioli, D., and N. O. Tippenhauer, "MiniCPS: A Toolkit for Security Research on CPS Networks,", Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or Privacy, pp. 91-100, October 2015.

[4] E. Rozos, and C. Makropoulos, "Source to tap urban water cycle modelling," Environ. Model Softw., vol. 41, pp. 139–150, March 2013.