RISKNOUGHT: Stress-testing platform for cyber-physical water distribution networks HS5.2.3-Water resources policy and management: digital water and interconnected urban infrastruct...

Conference Paper · May 2020

DOI: 10.5194/egusphere-egu2020-19647

Dionysios Nikolopoulos
National Technical University of Athens

Georgios Moraitis
National Technical University of Athens

European Geosciences Union General Assembly

Vienna, Austria, 5 May 2020

HS5.2.3- Water resources policy and management: digital water and interconnected urban infrastructure

RISKNOUGHT: Stress-testing platform for cyber-physical water distribution networks

D. Nikolopoulos[1], G. Moraitis[1], D. Bouziotas[2],

A. Lykou[1], G. Karavokiros[1], C. Makropoulos[1,2]

(1) School of Civil Engineering, National Technical University of Athens

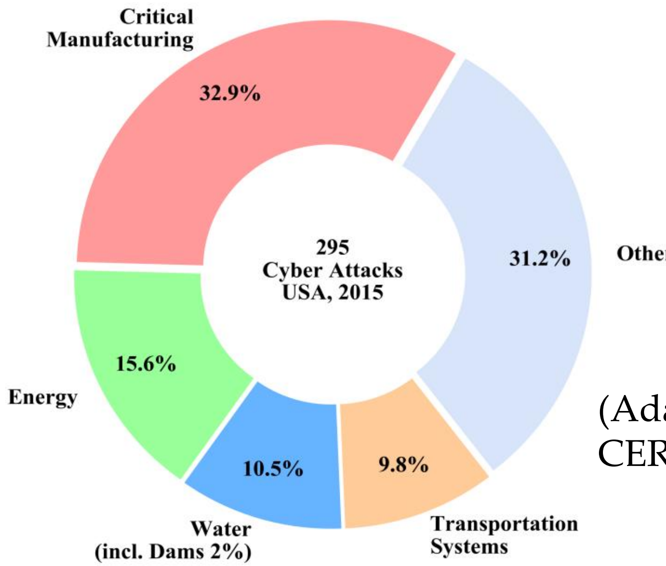
(2) KWR, Water Cycle Research Institute

Water Cyber-Physical Systems

- Modern water distribution systems are **Cyber-Physical Systems** (CPSs): integration of physical processes with computational engineered systems (SCADA)
- Advantages: increased automation, adaptability, efficiency, functionality, reliability, safety, and usability of large systems (Chen, 2017) due to the networking and communication capabilities
- **Drawback**: Exposure to an expanded attack surface (Rasekh *et al.*, 2017), including **physical and cyber attacks** (Taormina *et al.*, 2017)

- Indeed, water CPS are **very attractive** for perpetrators!

- We need to rethink water systems as CPSs in resilience oriented stress-testing procedures! (Nikolopoulos *et al.*, 2019)



(Adapted from ICS-CERT, 2016)

Existing CPS simulation methodologies

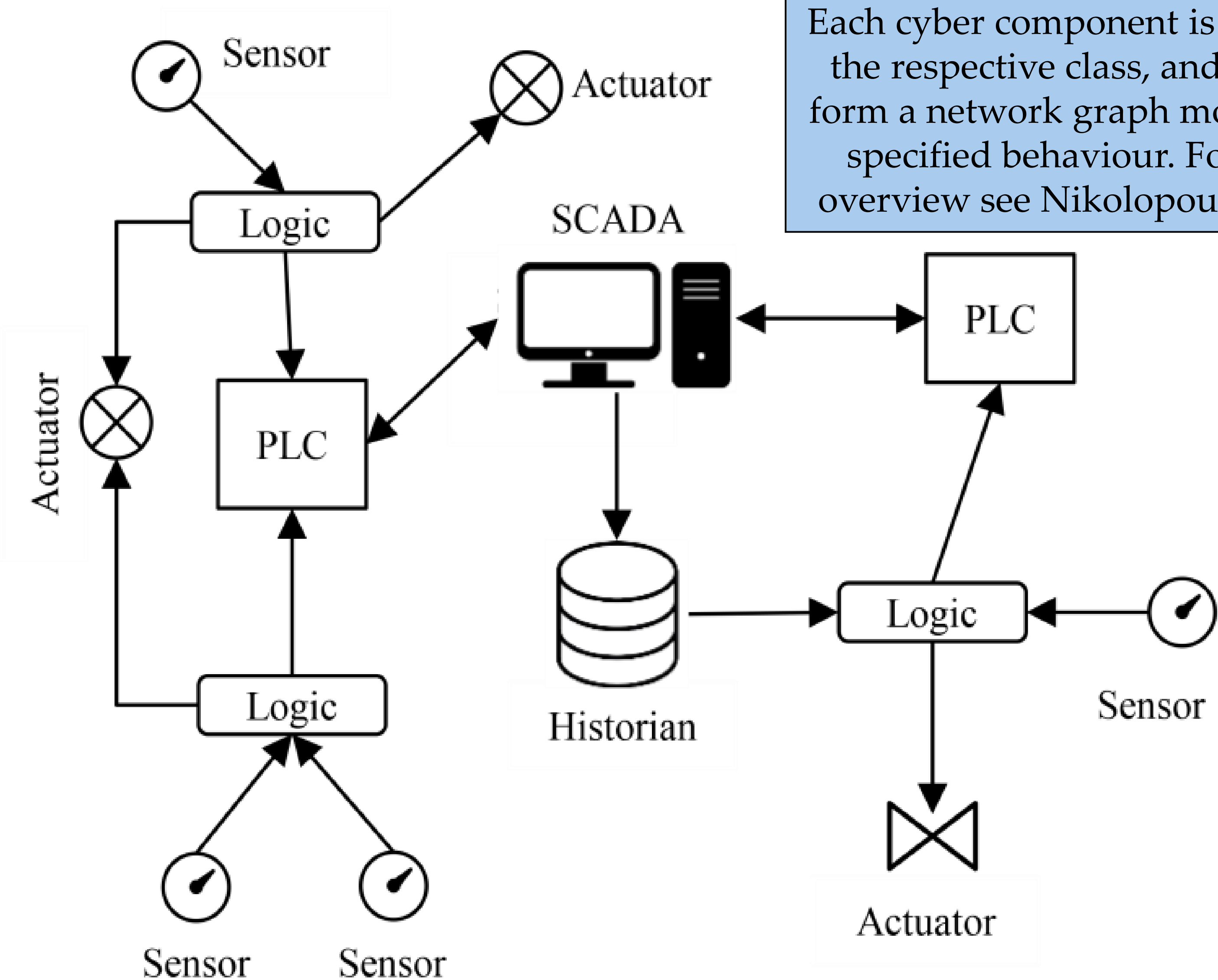
- Emulators of SCADA systems (OMNeT++, NS3), Virtual Machines (VMs) or software defined networks (SDNs)
  - Precise representation of the cyber layer
  - Difficult interconnection with physical processes
  - Simulation of cyber-attacks is not straight-forward (penetration testing) (Nikolopoulos *et al.*, 2020)
- Purely simulation based tools for both cyber and physical processes
  - **Lower fidelity** in the information flow of the cyber layer **but straight-forward modeling** of various types of cyber-physical attacks and their outcomes
  - Easier coupling to models of the physical processes
  - **Influential** work on WDN CPS systems: *epanetCPA* (Taormina *et al.*, 2017)

RISKNOUGHT modelling platform

risk + nought = “to risk nothing”

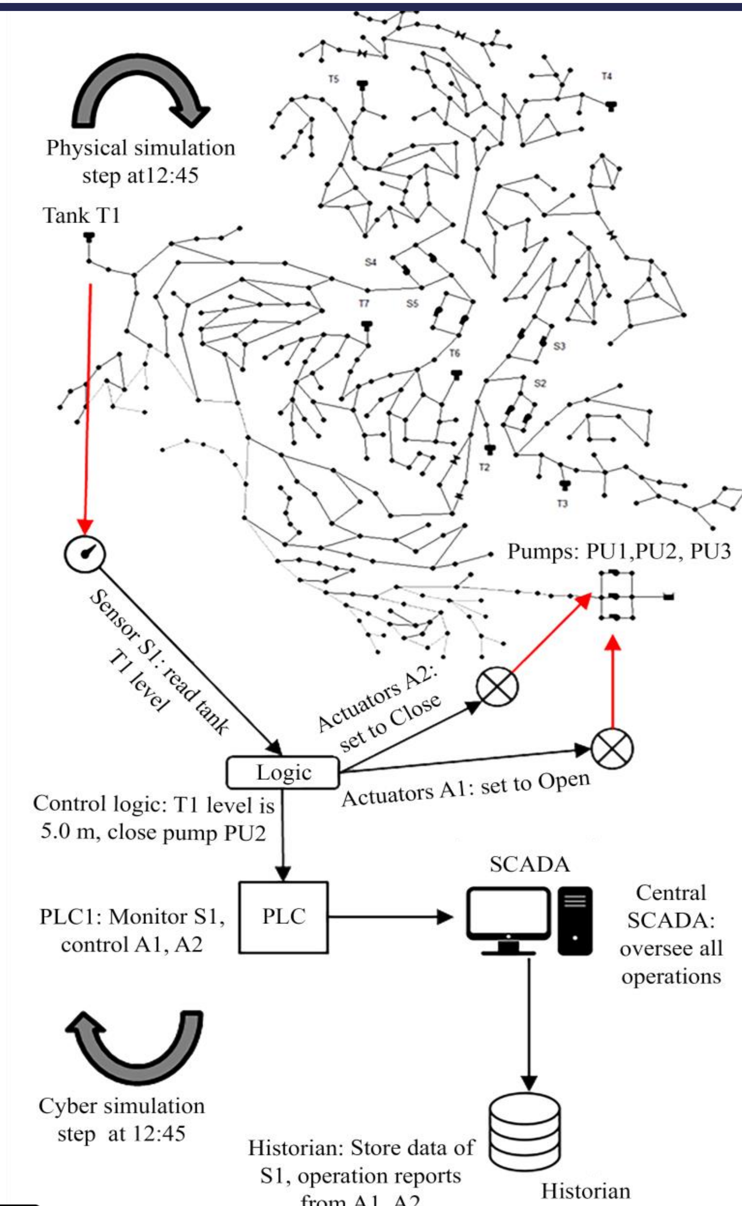
- RISKNOUGHT (Nikolopoulos et al., 2020) aims to be a complete Python-based modelling framework for water CPS stress-testing and a **risk management tool** of water utilities
- Ability to simulate the flow of information within the cyber layer (SCADA) and the interconnection with physical processes (hydraulic model)
- Control logic of the WDN is explicitly formulated
- Hydraulics are solved interactively with EPANET solver via the WNTR Python package (Klise *et al.*, 2017) with Pressure Driven Analysis equations
- Water quality modelling for reactive or conservative species is handled currently with EPANET quality solver whereas the EPANET-MSX extension coupling is in development (coming soon)

RISKNOUGHT cyber layer model



Each cyber component is an instance of the respective class, and all elements form a network graph model with user specified behaviour. For a detailed overview see Nikolopoulos *et al.*, 2020

RISKNOUGHT cyber-physical loop



Example of Coupling of the cyber and physical models :

- The hydraulic model is run at step 12:44 with commands from the cyber layer – next time step is 12:45
- *SCADA* oversees *PLC1* with a slave/master protocol : sends command to perform operations
- *PLC1* implements the control Logic rule if tank *T1* level is >5.0 close pump *PU2*
- *PLC1* monitors sensor *S1* (tank level sensor) and sends signals to actuators *A1* and *A2*
- At time 12:45, *S1* reads *T1* level and sends the value to Logic part of *PLC1*
- The control Logic decides to send the "Close" command to *A2* and "Open" to *A1*
- *PLC1* sends the information of inputs and actions back to *SCADA*
- *SCADA* sends the information to the *Historian* for archiving
- The next hydraulic simulation step @12:45 runs with pump *PU2* closed

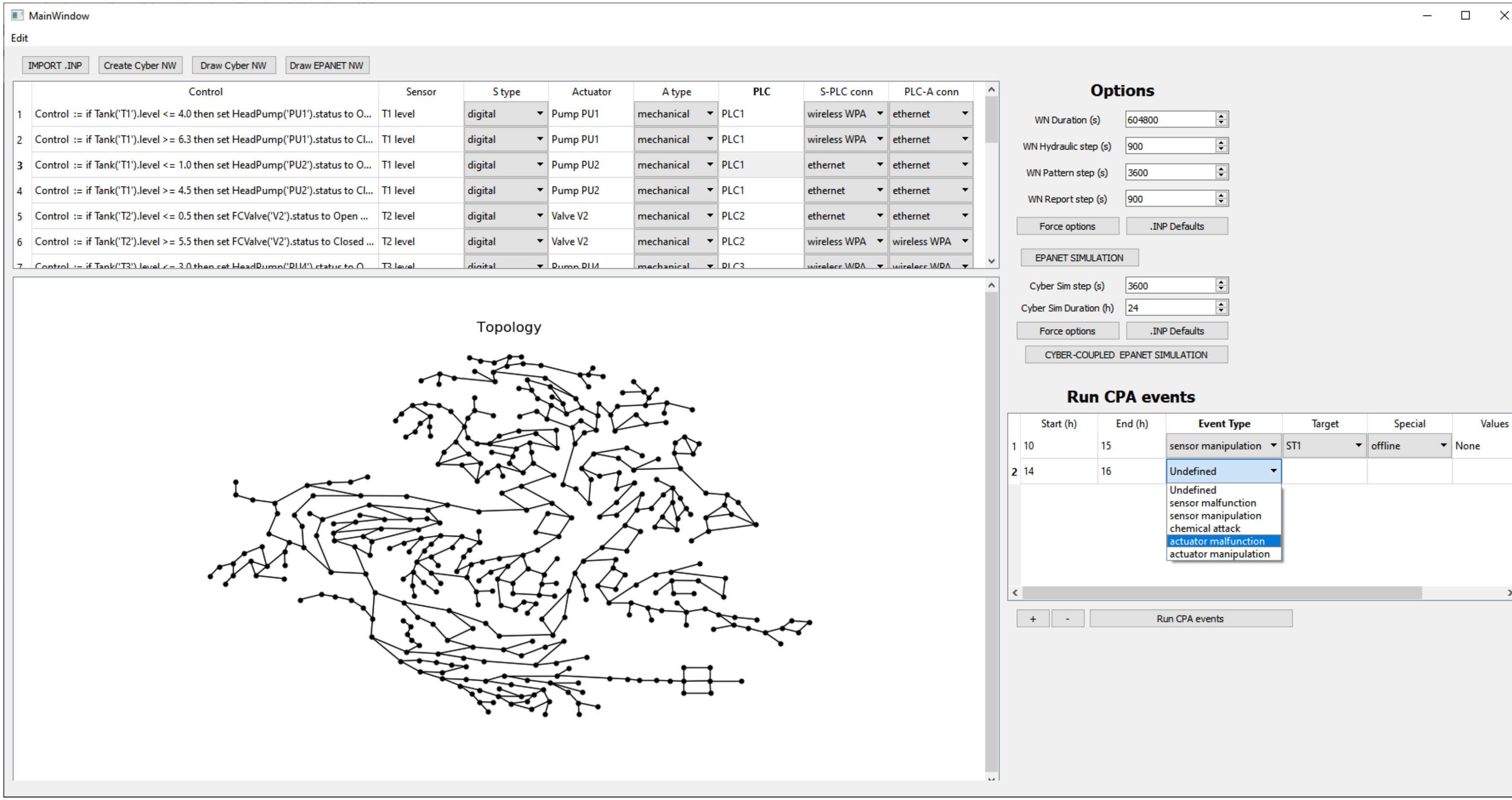
RISKNOUGHT modelling capabilities

- Modeling of various sensors exposing various hydraulic aspects, such as:
  - tank level
  - node pressure
  - link velocity
  - link flow
  - concentration of a species etc.
- Actuators acting on:
  - pumps
  - valves
  - isolation of pipes
  - flushing units /hydrants (quality related actuators) etc.

RISKNOUGHT modelling capabilities

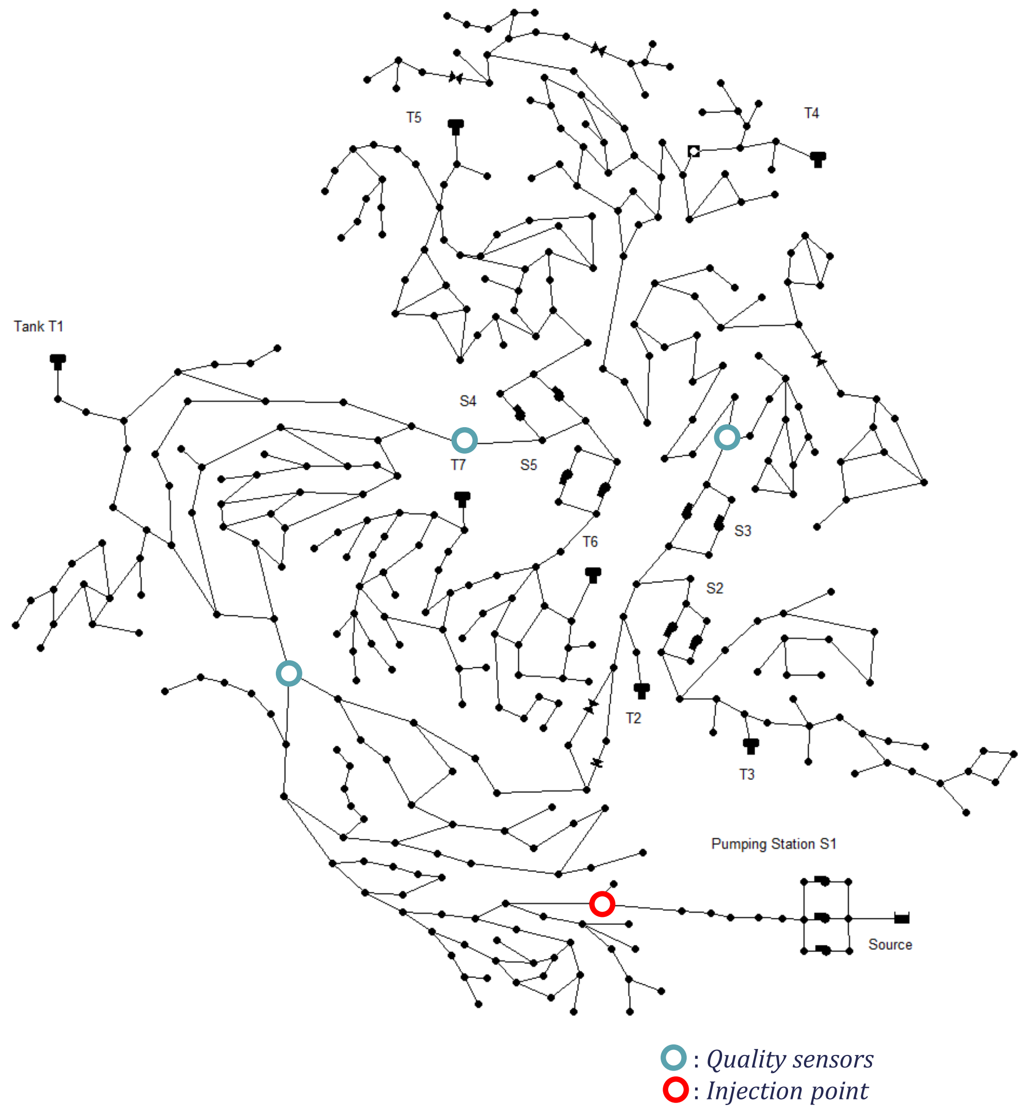
- Simulation of acknowledged signals (ACK) behavior and reporting of remote actuators
- Augmenting EPANET control logic based on complex rules, past timeseries (from Historian unit), quality related controls (isolation of specific areas, activation of flushing units)
- Simulation of interconnecting PLCs, Master-Slave protocols, autonomous operations of PLCs, multiple distributed SCADA systems on the same WDN
- Alerts, flags and warnings on SCADA & HMI (human – machine interface) level
- Sensor/actuator manipulation/malfunction, denial of service (DoS) attacks on SCADA/PLCs and connections, chemical/microbial attacks and the fate of the contaminant in the network
- Communication link attributes (e.g. fiber, wireless etc.)
- Pipe endurance ratings, simulation of bursting, leaks etc.

RISKNOUGHT GUI (work in progress)



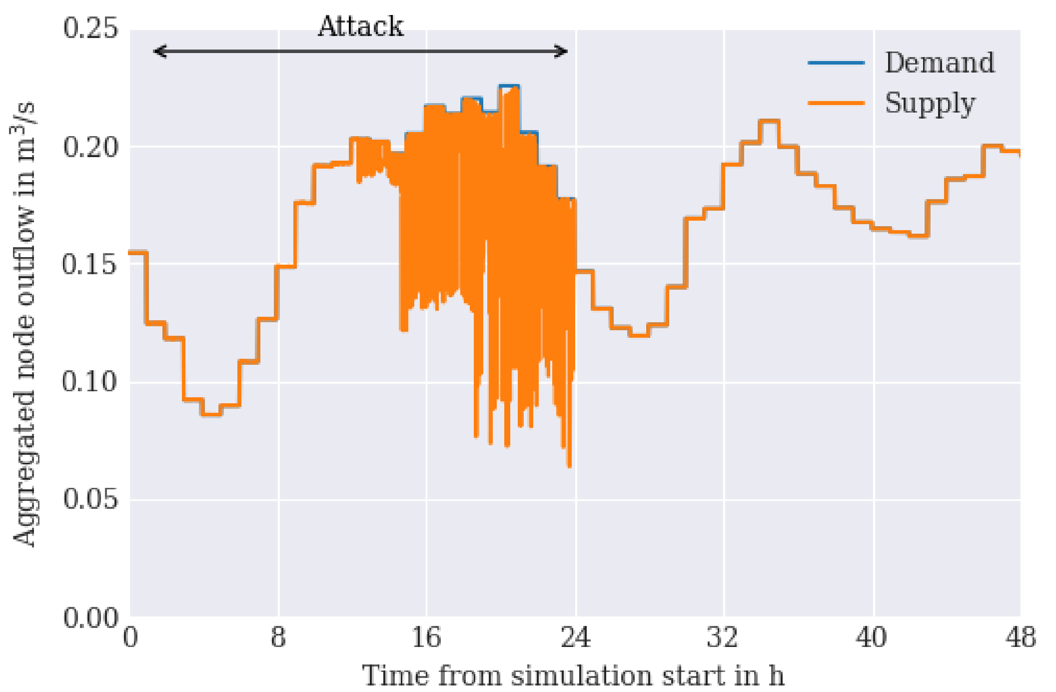
Benchmark network: C-Town

- Based on a real-world medium sized network (Ostfeld *et al.*, 2002)
- 388 demand nodes, 7 tanks, 11 pumps, 4 valves
- One source of drinking water
- Some branched service areas
- Controls based on tank levels: Sensors at each tank, actuators on all pumps
- Quality sensors at nodes J411, J332 and J441, if an anomaly is detected all DMAs are isolated
- For the attack scenarios 3 and 4, the injection point is J192



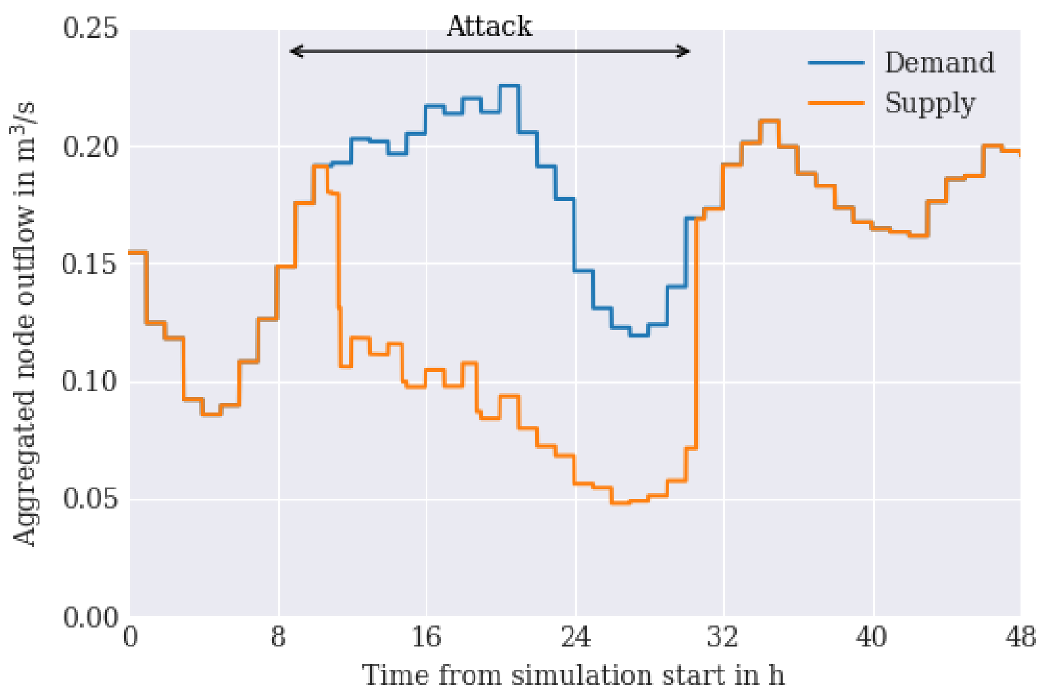
Cyber Attack scenario #1

- **Type**: Exploitation of actuators
- Attacker exploits a vulnerability in the PLC controlling all pumps in the network and issues repeating random commands (open/close) for an extended period while actuators send deceitful ACK signals. Supply in the network becomes intermittent.



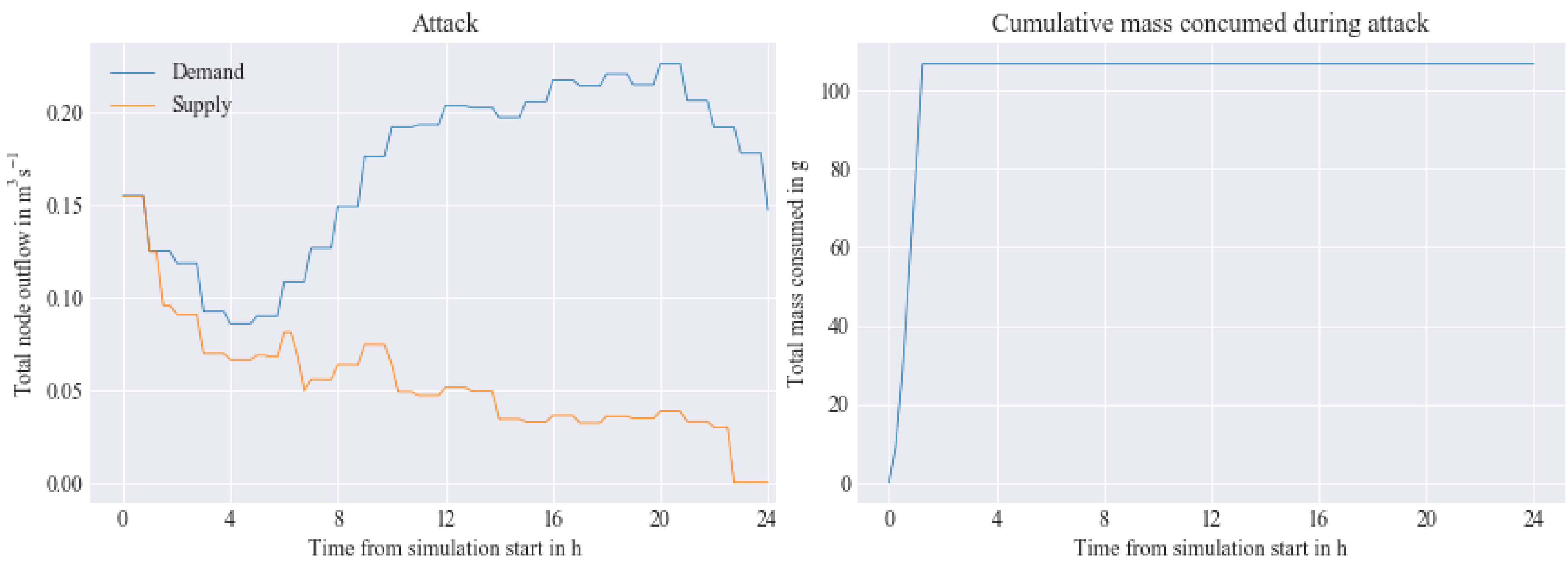
Cyber Attack scenario #2

- **Type**: SCADA DoS Attack, Master-Slave protocol, insider knowledge
- Attacker performs a similar DoS attack on the SCADA with a Master-Slave protocol and knows what time the attack consequences will be critical: The attack starts when most of the pumps are closed, and thus remain closed for an extended period.



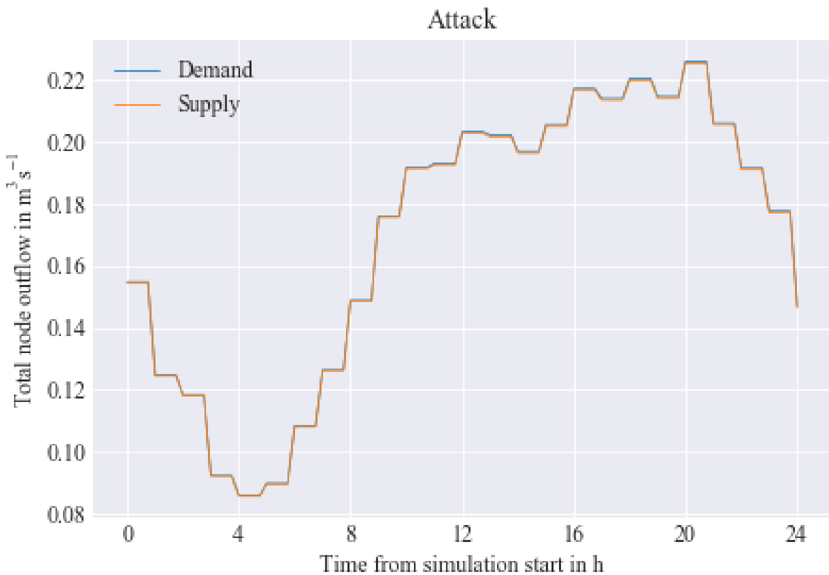
Physical Attack scenario #3

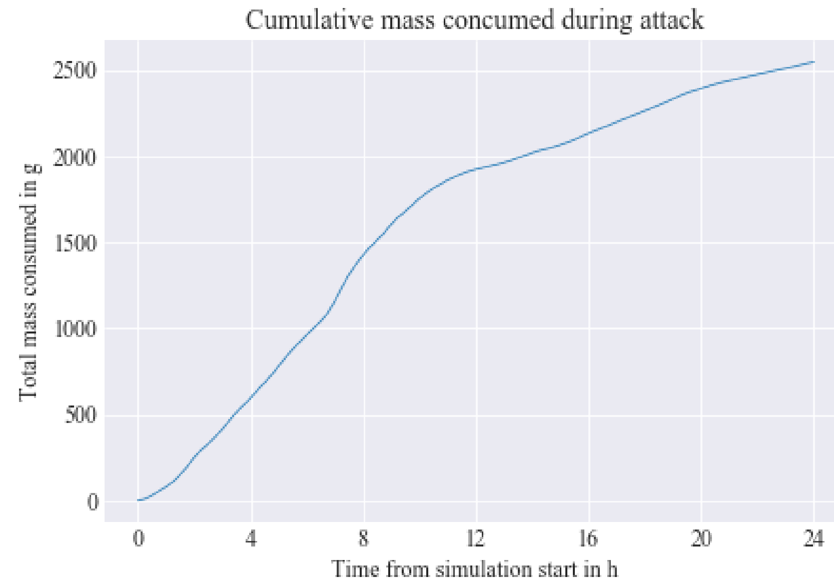
- **Type**: Contaminant injection at node J192
- Attacker contaminates the water distribution system between 0:00 to 01:00 with 3600 g of a conservative contaminant. The first quality sensor in the flow path of water reports the anomaly at time 01:30 and all DMAs are isolated. Consumed mass of the contaminant is low and the contamination extent is minimized.



Cyber-Physical Attack scenario #4

- **Type**: Contaminant injection at node J192 and cyber attacks on all quality sensors
- Attacker contaminates the water distribution system between 0:00 and 01:00 with 3600 g of a conservative contaminant and at the same time hacks the connection between quality sensors of the network for 24 h. The quality sensors reports “normal” readings. No alteration in water supply. The consumed mass in the same 24 h time window is 2.5x more than Scenario 3, and the contamination extents to the whole WDN.





Conclusions

- Water CPS are CIs vulnerable to a multitude of cyber-physical threats.
- RISKNOUGHT is able to simulate both the interplay between the cyber and physical layers of a WDN.
- RISKNOUGHT models a multitude of cyber-physical threat events and also mitigation and response measures, e.g. the isolation of DMAs in the event of a contamination event.
- Bridges the gap between *precise emulation* of SCADA systems and *simple simulation* of control logic rules of hydraulic operations.
- Supports quality related cyber-attacks.
- Extensive water quality modelling capabilities with multiple species and reactions using the EPANET-MSX extension is under way.

RISKNOUGHT is under active development and will be expanded with more functionality soon!

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 K.A., Hart D.B., 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. https://doi.org/10.1016/j.envsoft.2017.06.022
- 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. https://doi.org/10.1061/(ASCE)EE.1943-7870.0001722
- Nikolopoulos D., van Alphen H. J., Vries D., Palmen L., Koop S., van Thienen, P., Medema, G., Makropoulos C. (2019). Tackling the “new normal”: A resilience assessment method applied to real-world urban water systems. Water, 11 (2), 330. https://doi.org/10.3390/w11020330
- Ostfeld, A., Salomons E., Ormsbee L.., Uber J.G. (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 M.K. (2016) Smart water networks and cyber security. Journal of Water Resources Planning and Management 142(7): 01816004. https://doi.org/10.1061/(ASCE)WR.1943-5452.0000646
- Taormina R., Galelli S., Tippenhauer N.O., 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

Acknowledgments

STOP-IT

www.stop-it-project.eu

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.