11th World Congress of the European Water Resources Association on “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]**

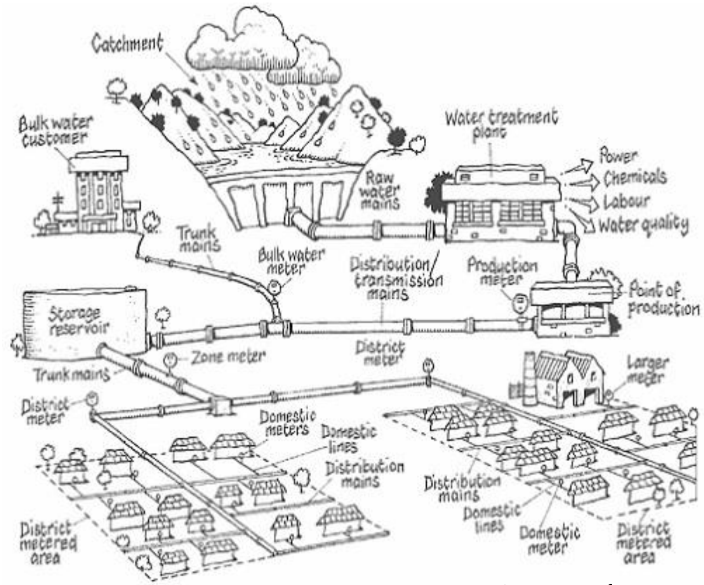
(1) School of Civil Engineering, National Technical University of Athens

(2) KWR, Water Cycle Research Institute

# Cyber-Physical Systems (CPS)

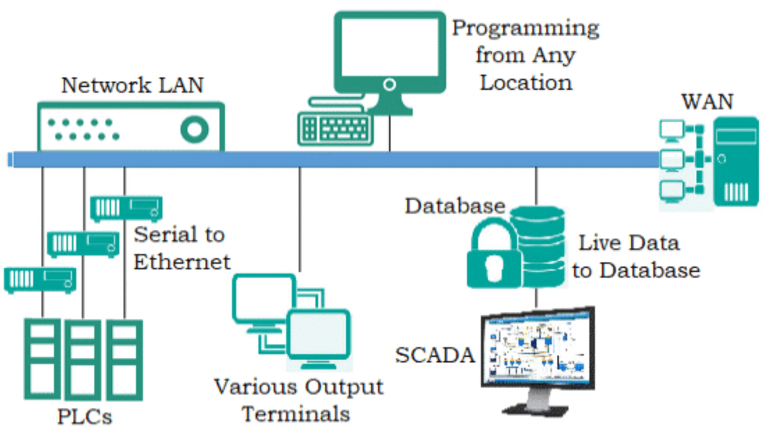
Systems with 2 layers:

- Physical Processes




(image from pacificwater.org)

- Control, Communication, Computation




(image from electricalfundablog.com)

# Emerging threats on CPS

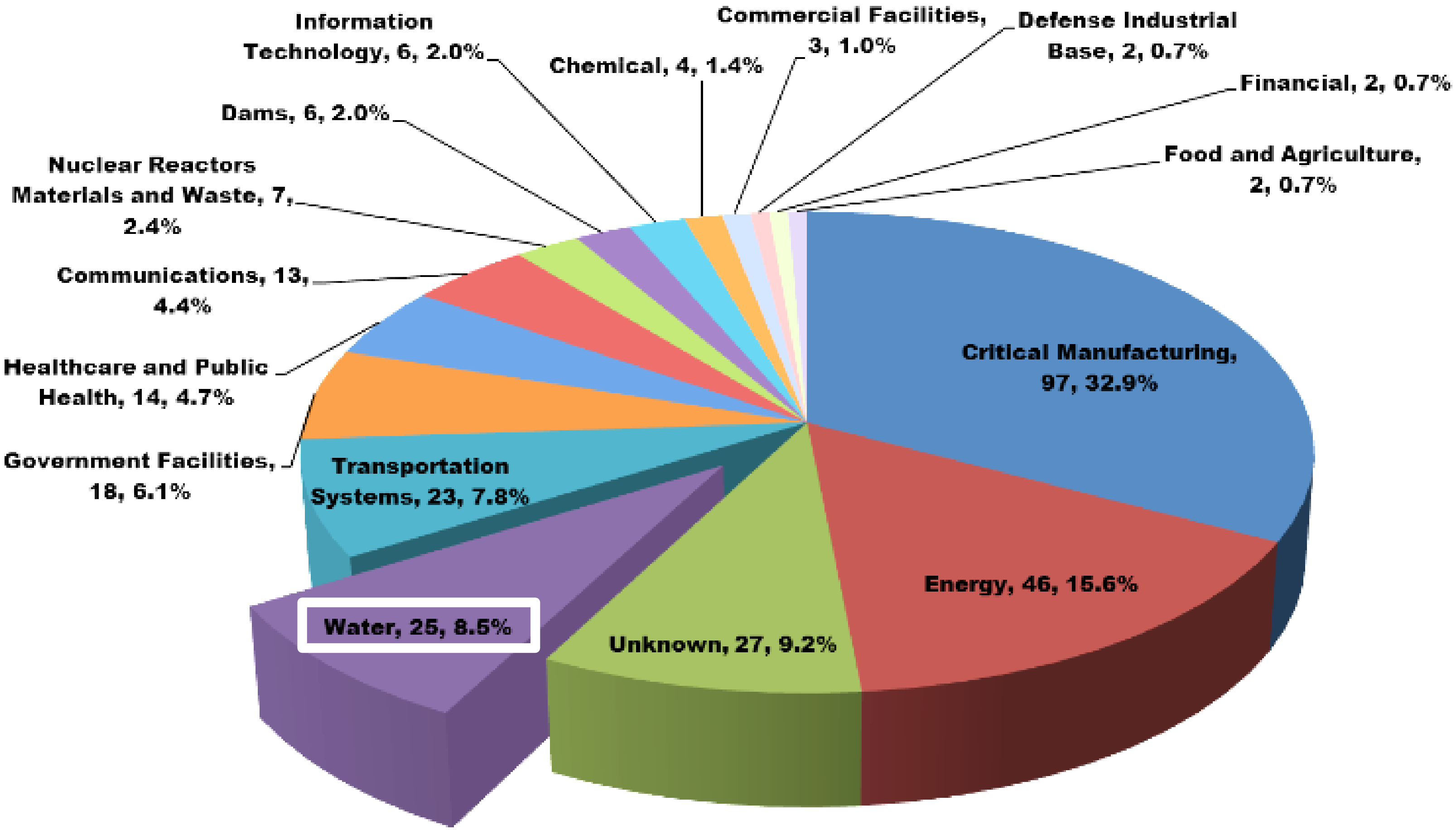
- CPS susceptible to a wide range of cyber, physical or a combination of attacks (CPA)
- Famous examples of cyber-attacks to CPS:
  - Stuxnet worm that targets SCADA units
  - Hacking of Maroochy Shire WWTP

*CS 5032 Case study Stuxnet worm, 2013*

*CS 5032 Case study Maroochy breech, 2013*

# Water CPS as targets?

WDNs are a prominent critical infrastructure (CI) target!!! (ICS-CERT 2016)




Cyber attack incidents in USA, 2015 (DHS, 2016)

# Existing (limitations of) CPS simulation tools

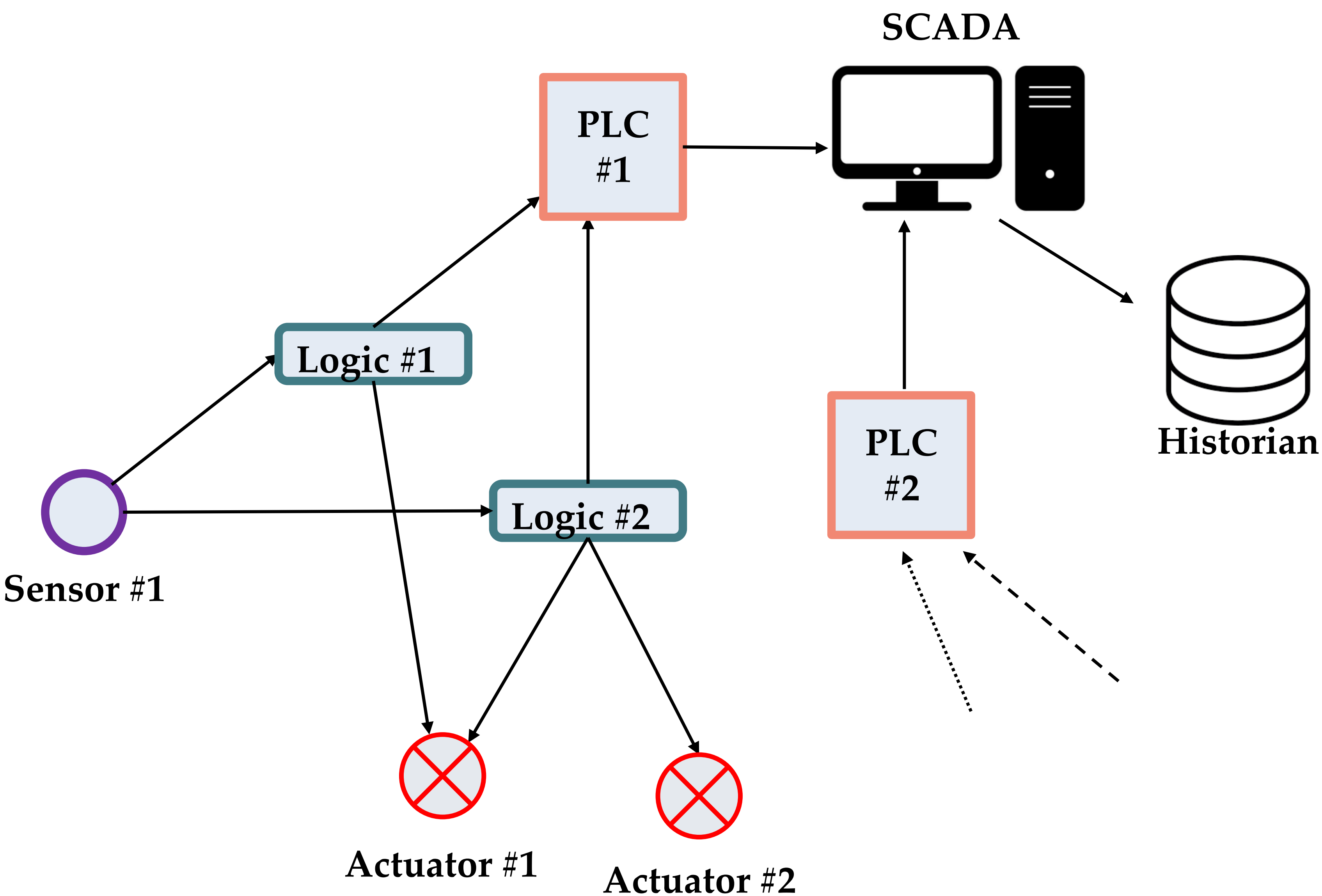
- Emulators of SCADA systems (e.g. OMNeT++, NS3) or Virtual Machines (VMs)
  - Precise representation of the cyber layer
  - Difficult interconnection with physical processes
  - Simulation of cyber-attacks is not straight-forward (penetration testing)
- EPANET-CPA (Taormina et. Al, 2017)
  - **Influential** work on WDN CPS systems
  - Depends on EPANET control logic
  - Representation of the information flow of the cyber layer, however options are limited
  - No quality modelling

# RISKNOUGHT modelling platform

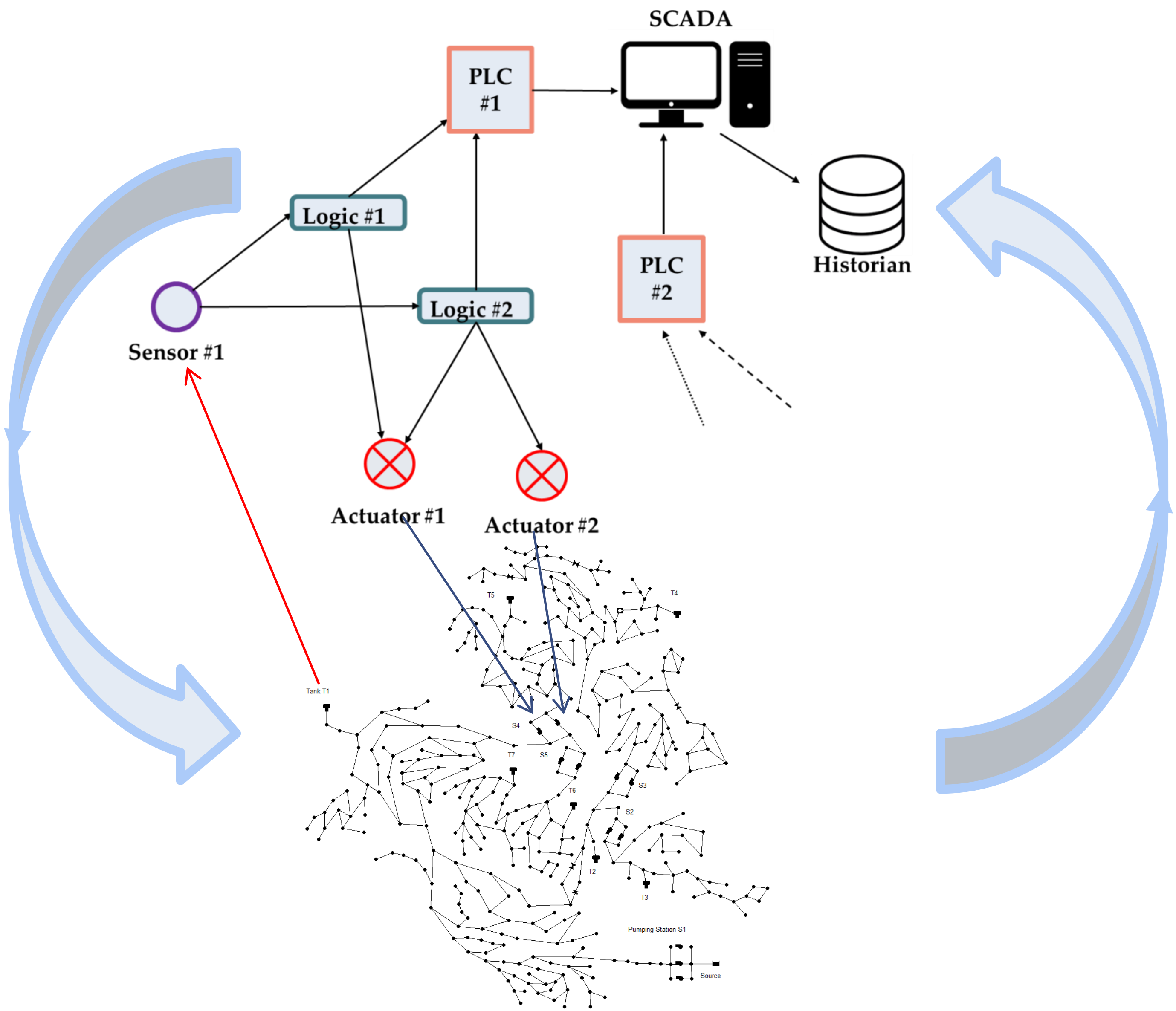
*risk + nought = "to risk nothing"*

- RISKNOUGHT aims to be a complete modelling framework for water systems cyber-physical stress-testing and part of **risk management** 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 model
- WNTR python package (Klise et al., 2017) is utilized, as it couples EPANET with Pressure Driven Analysis equations
- Water quality modelling is handled with EPANET-MSX extension (reactive and conservative species)

# RISKNOUGHT cyber layer model



# RISKNOUGHT cyber-physical loop



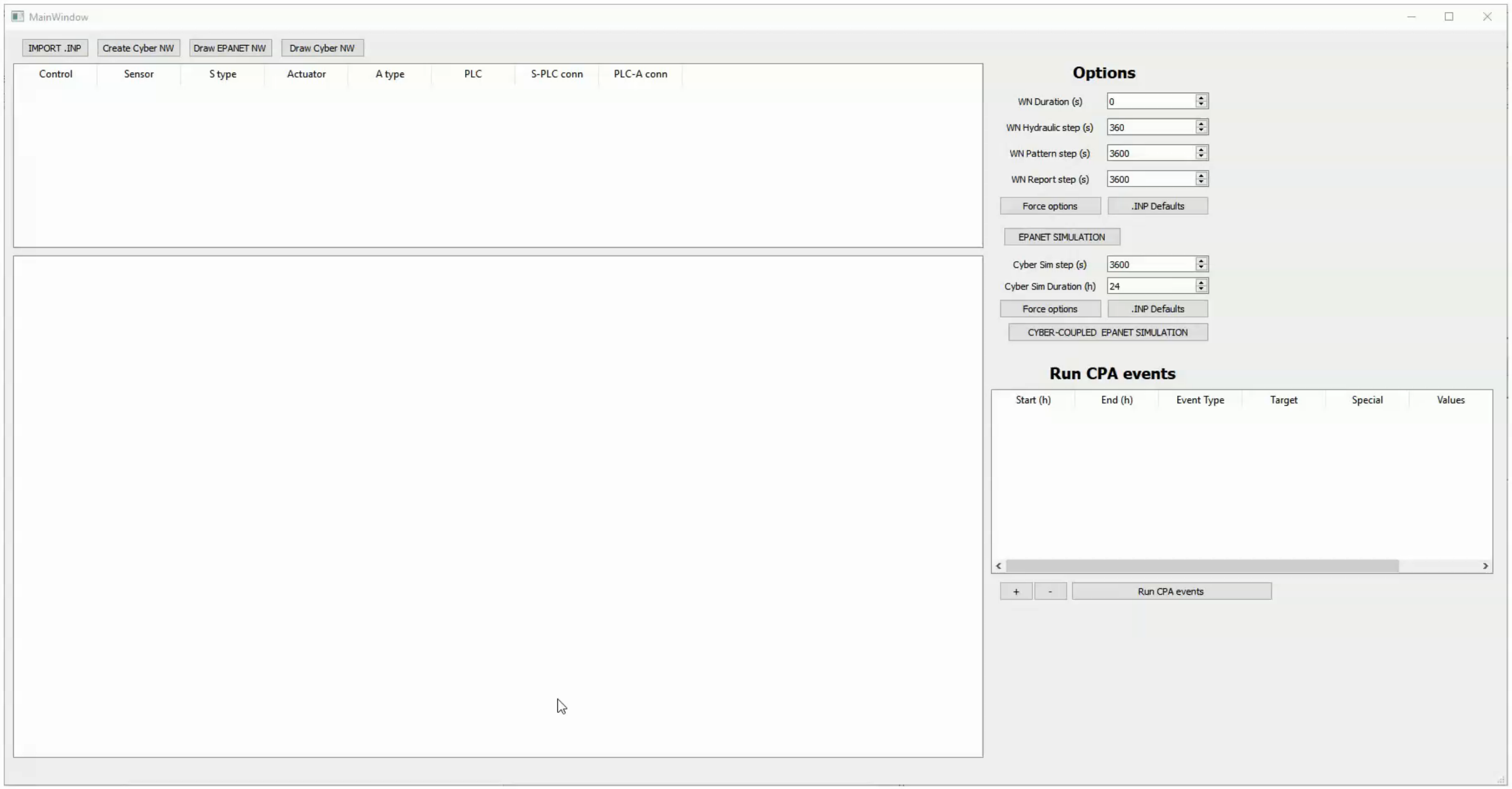
# RISKNOUGHT modelling capabilities

- 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 (Historian unit), quality related controls
- 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, DoS attacks on SCADA/PLCs and connections, chemical/microbial attacks
- Communication link attributes (e.g. fiber, wireless etc.)
- Pipe endurance ratings, simulation of bursting, leaks etc.

# RISKNOUGHT interface (work in progress)

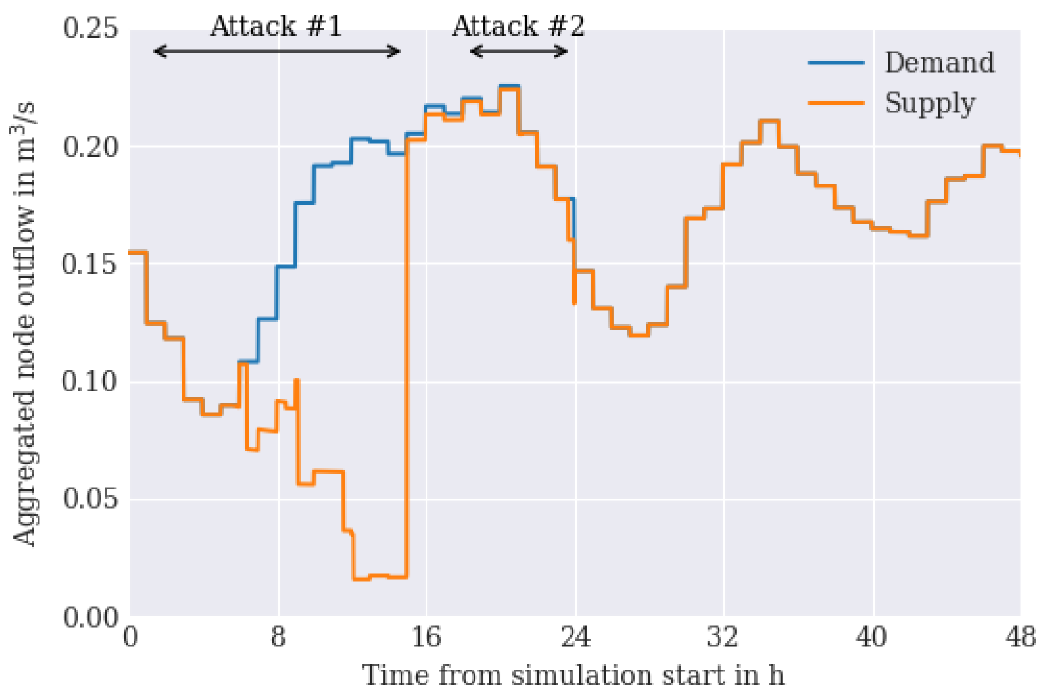


# Benchmark network: C-Town

- 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

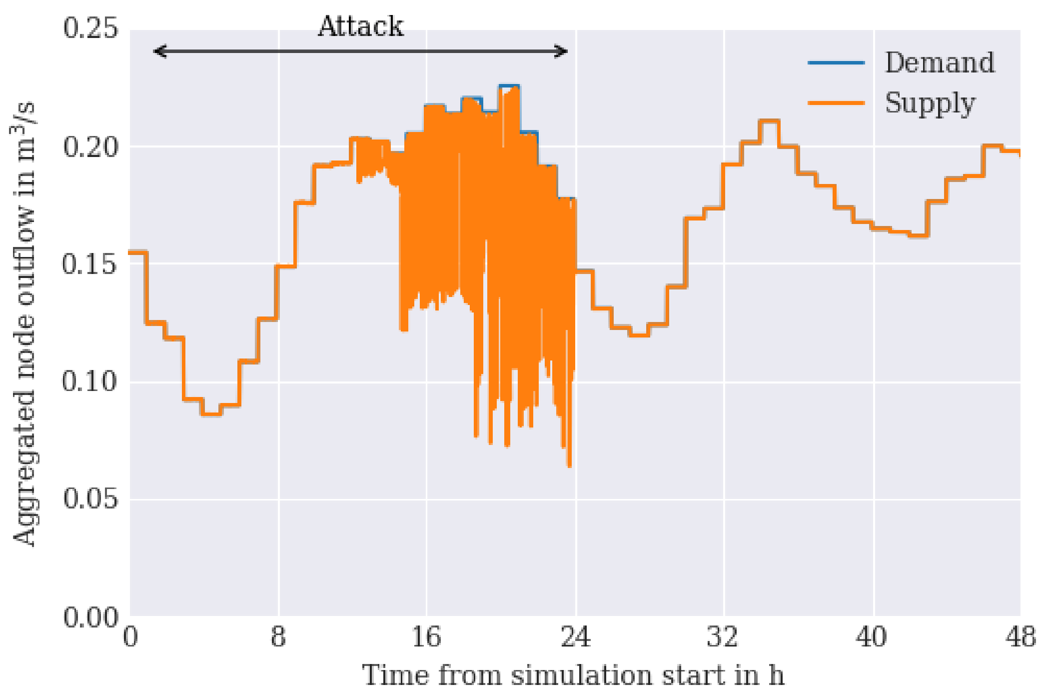
# Attack scenario #1

- **Type**: Manipulation of sensors
- Attacker manipulates readings of two different sensors (different start/end/durations and some overlap in the two cyber attacks).



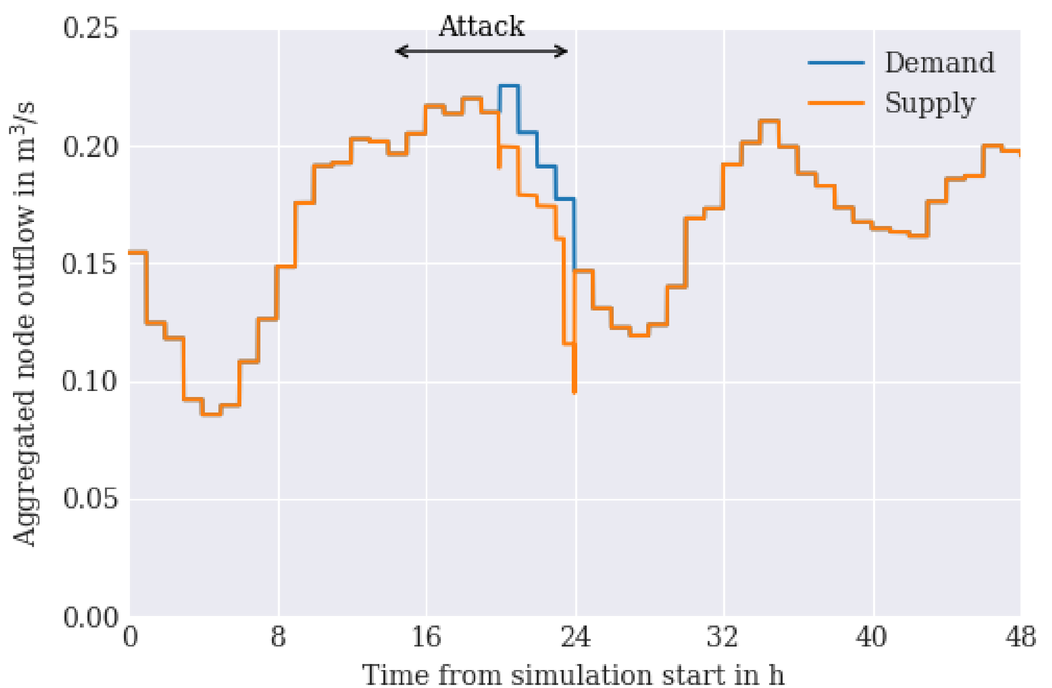
# Attack scenario #2

- **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 of time, actuators send ACK signals.



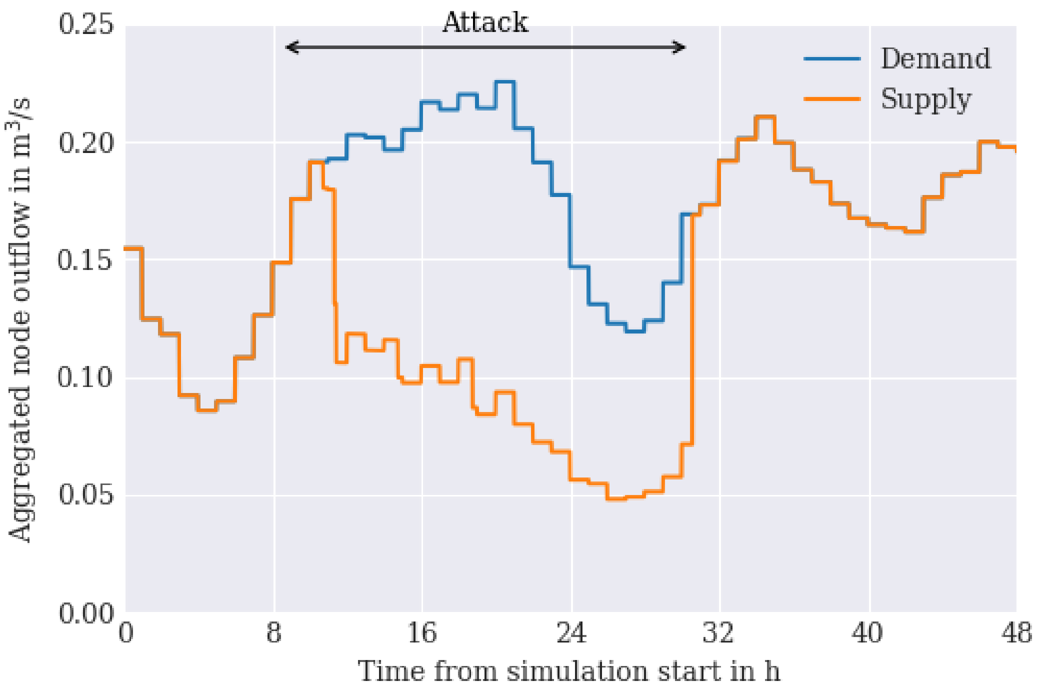
# Attack scenario #3

- **Type**: SCADA DoS Attack, Master-Slave protocol
- Attacker performs a DoS attack on the SCADA. PLCs have a Master-Slave SCADA communication protocol, so controls cannot be enabled and sensor readings are not registered. Timing is not perfect for the attacker.



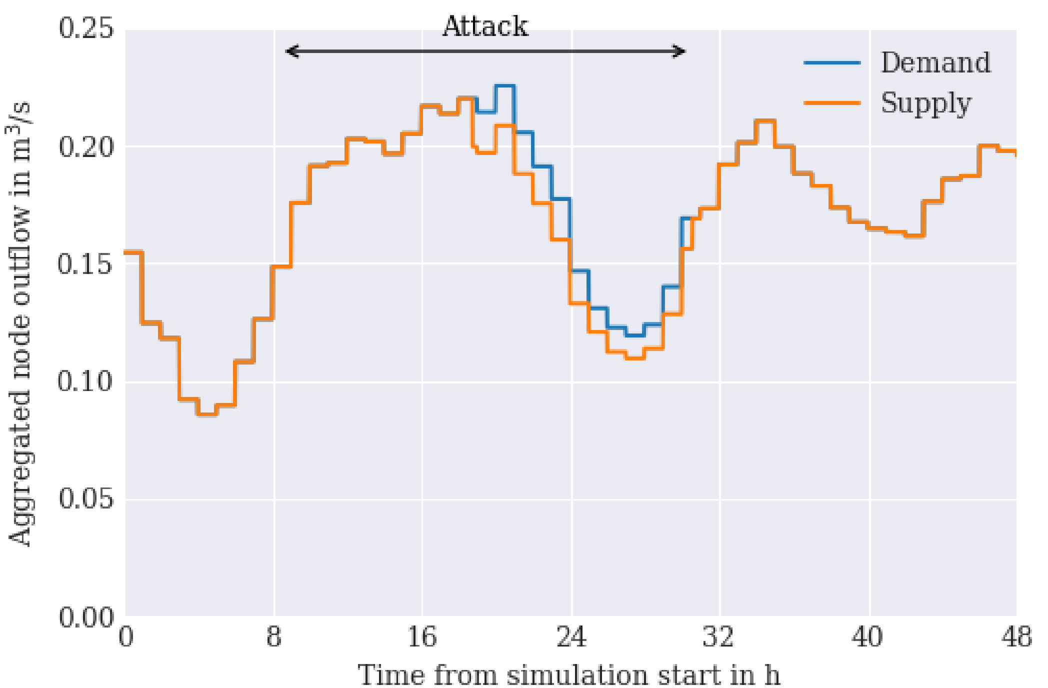
# Attack scenario #4

- **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.



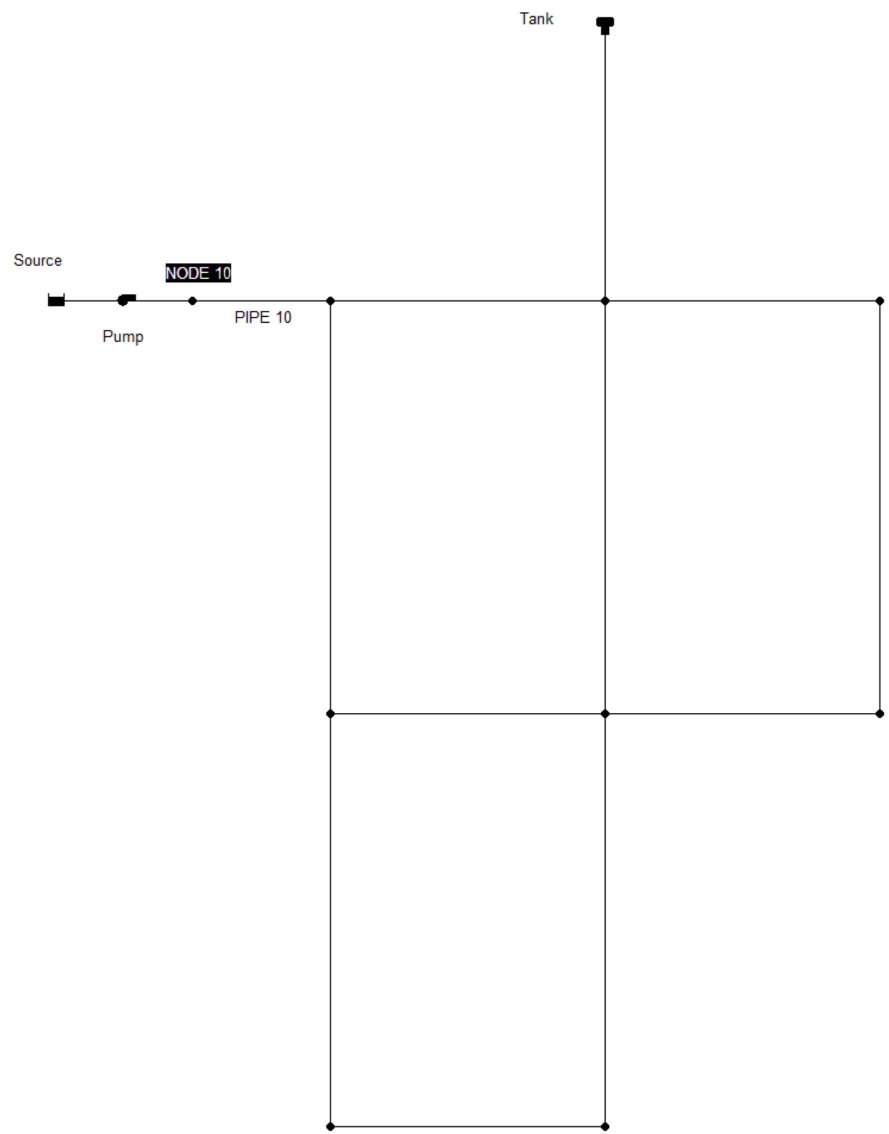
# Attack scenario #5

- **Type**: SCADA DoS Attack, Autonomous PLCs, insider knowledge
- Same as scenario #4, but the protocol is not Master-Slave for all PLCs. Some can operate autonomously in case connection to SCADA is lost (semi-distributed control protocol).



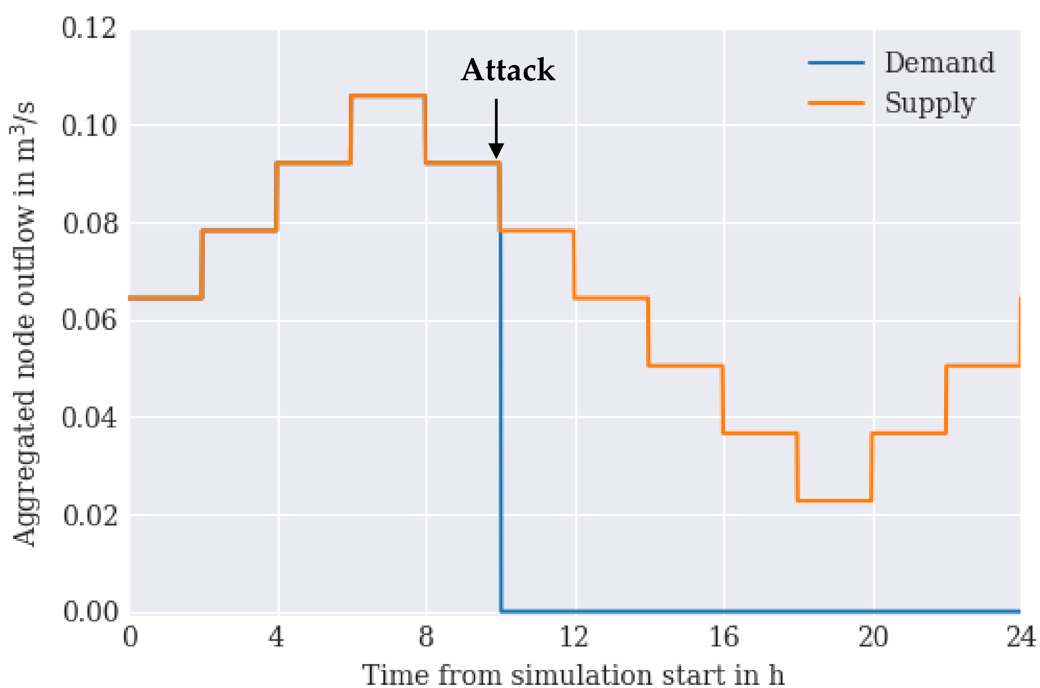
# Benchmark network: Net 1+

- Simple network model for *quality* stress-testing: one source, one tank, one pump, 8 demand nodes
- Augmented SCADA controls with actions on the event of contaminant detection
- Single quality sensor at NODE 10
- If an anomaly is detected, PIPE 10 is isolated and the Tank valve is closed



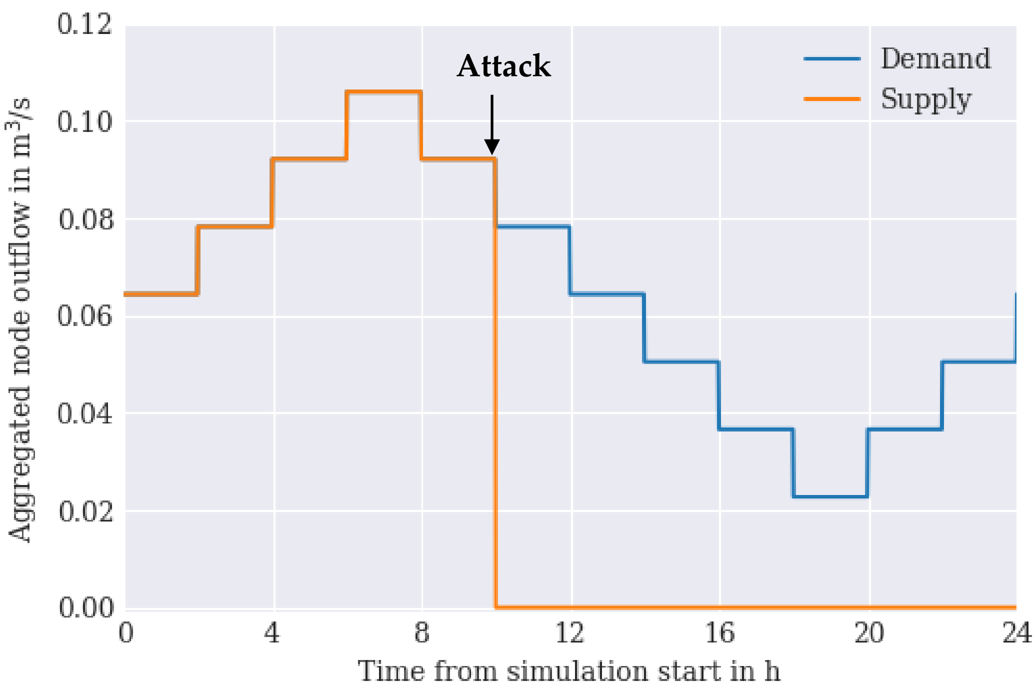
# Attack scenario #6

- **Type**: Contaminant injection, attack on quality sensor
- Attacker contaminates the water distribution system and at the same time hacks the connection between the sole quality sensor of the network. The quality sensor reports “normal” readings.



# Attack scenario #7

- **Type**: Manipulation of quality sensor
- Attacker exploits vulnerabilities and manipulates the readings of the sole quality sensor in the network in order to fake a severe contamination event, leading to the closing of the main distribution pipes.



# 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 risk reduction measures
- Bridge the gap between *precise emulation* of SCADA systems and *simple simulation* of control logic rules of hydraulic operations
- Support for extensive water quality modelling with the EPANET-MSX extension

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

# 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.

# 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.

# Thank you for your attention