SAMPLE TRAINING MATERIAL

Water systems as cyber-physical entities

digital-water.city
digitalwater_eu

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

Table of content

1. Topic

The topic treated in this course module is on treating water systems as cyber-physical systems (CPS), with an introduction of the main risks associated with CPS.

Note: This module is inspired from contents in relevant NTNU courses and a book chapter on CPS [1].

2. Goals

- To explain, in very simple terms, why and how water systems can be considered CPS and further explain their layers (cyber and physical), as well as their interaction.
- To explain the **risks** associated with these systems. Emphasize on the links with STOP-IT tools.

3. Water systems as cyber-physical entities

Water systems generally include physical and cyber elements as part of their network. Physical elements include all assets of water collection, treatment and distribution needed to bring water in a safe and reliable way to customers, such as dams or reservoirs, spillways, water treatment plant buildings and technologies, aqueducts and tanks and, eventually, pipes that deliver water to end users. Cyber elements include, but are not limited to, all types of water quantity and quality sensors, the Supervisory Control and Data Acquisition (SCADA) system that monitors and controls processes, and networking elements to connect these elements (lines, LAN/WAN networks etc.). Both of these layers (i.e., the physical and the cyber) can be studied and designed separately in terms of functionality and risks; however, it is also important to consider these two layers as one interconnected (i.e., cyber-physical) entity for water, where cyber elements affect their physical counterparts and vice versa.

A system that integrates physical processes with computational engineering systems is termed a cyber-physical system (CPS). The cyber layer of this integration employs a networking, computing, and communication core of embedded computers and devices that monitors, controls and coordinates the physical processes. This synergy is accomplished via feedback loops, where the outcome of a physical process affects computation and vice versa [2]. While the term CPS was introduced in 2008 to describe “deeply embedded” systems that are fully integrated hybridizations of computational (logical) and physical actions [3], the concept and its application has started long before that, with the onset of automated control systems for physical processes and the handling of digital information by

mainframe computers. Contemporary CPSs are evolving, rapidly benefiting from the emergence of other related technologies in the informatics and computer science fields, such as IoT (internet of things), big data, cloud computing, novel sensor technology, and other advances in ICT like optical fiber wire connections and 5G cellular connectivity. Essentially all smart water systems can be considered CPS, as they rely heavily on the cyber layer and its interaction with the physical one.

A basic principle to understand the interaction between the cyber and physical layers in a CPS is the 'sensor-actuator' principle. According to this principle, what is commonly found in water systems is that cyber elements (sensors) gather information, in (near) real-time, about aspects of the water system. Operators then use this information, either by decision-making or through automation, to decide about the status and operation of physical elements, such as valves, gates, spillways etc. One can only then extrapolate that any compromise to a cyber element, such as a sensor, will have direct, physical impacts to the water system, as it will affect the operation of its assets.

Of course, a water CPS is not only contained to sensors and actuators. A plethora of basic elements for a CPS exist, such as:

- Conversion Units, such as Remote Terminal Units (RTU) and Programmable Logic Controllers (PLCs). These are connected to sensors and interpret the data collected, convert it to digital (if the sensor is analogue) and are able to command actuators using logical rules with the data collected. These units also send the data to the central SCADA unit.

- Master Units, the most important of which is the Supervisory Control and Data Acquisition (SCADA) unit. This is essentially the most prominent part of the cyber layer and the backbone of every CPS, as it serves as the central monitoring and control unit, gathering data from all distributed sub-units (RTUs/PLCs) and presenting an overview of the system status to the operators. The SCADA generally includes a database of all data collected (Historian), as well as a Human Machine Interface (HMI).

- Communication Networks and Protocols, which are the hardware that connects information across peripherals in the system (e.g., between a sensor, a PLC and an actuator), but also from distributed elements to the central SCADA unit. Communication networks include both wired (telephone lines, WAN circuits, fiber-optic cables) and wireless technologies (Wi-Fi, Bluetooth, radio, cellular, satellite), as well as the required protocols for device interaction (e.g., TCP/IP, Modbus).

An overview of these elements can be seen in ***Figure 1***, where one may see a water distribution network with a single source, comprising pumps and valves in a city (lower part). There are sensors at key parts of the network, measuring operational attributes such as the water pressure and flow at given intervals. This information is then passed to RTUs, which act as peripheral information collection terminals that then send this information (through a wireless or wired manner) to the main SCADA unit. The SCADA unit forms the centre of operations, including all monitoring, analysis and customer service components. Finally, operator decisions travel the inverse way: from the SCADA unit back to the relevant PLCs that act as the convertors of digital information to physical actions through relevant switches. The result is a physical action in an actuator, for instance a change in pump settings or the closure of a valve. This flow of information towards the SCADA unit and back happens in (near) real-time, so a wealth of information is acquired during normal water system operations, aggregated within the SCADA unit and used to detect anomalies, assist operator decisions, improve customer service etc.

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

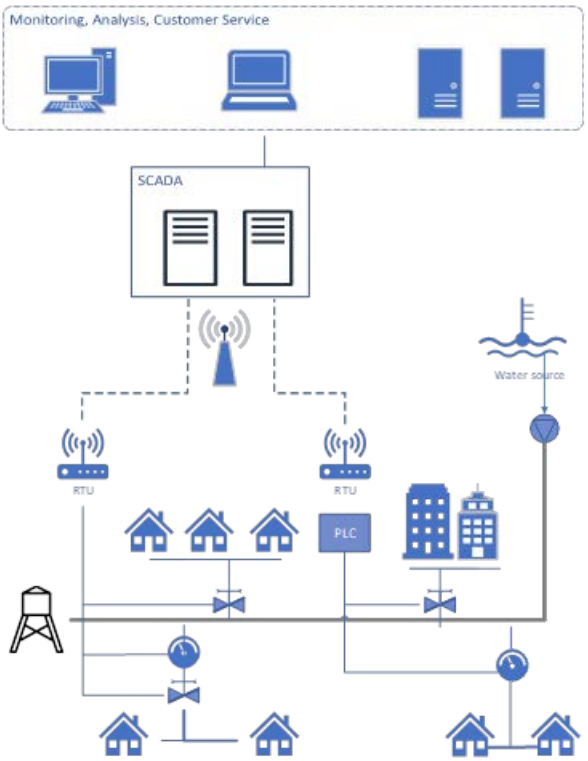

Figure 1: Overview of the interactions of cyber and physical elements in a CPS.

The various aforementioned elements in a CPS allow multiple possible attack routes of cyberattacks for adversaries. Physical attacks are the simplest form of CPS attacks, such as tampering with field devices or modifying and compromising wired connections (e.g., cable damage). Another common attack vector is the exploitation of backdoor (i.e., unauthorized hidden software or hardware mechanisms to circumvent security measures) or unintentional security holes in the network perimeter that allows some form of remote access or control. Finally, attack within the SCADA system may occur, for instance targeting the CPS database with methods like SQL injection, where malicious code is inserted in queries to manipulate data or even controls of the system. Finally, wireless networks have their own cybersecurity concerns, including eavesdropping on information from unsecured networks, compromise of remotely controlled, wireless sensors and actuators, and jamming signals.

The communication hijacking between such components (from a signal source to a destination) constitutes a wide class of attacks, called Man-in-the-middle, where the attacker may try to (a) interrupt a message so that data are not received at the destination, (b) intercept a message for information eavesdropping, (c) modify the data of a message, so that an altered version is received at the destination, or (d) by imposing the source, fabricate a bogus message, and send it to the destination. As this information is used for actions on the physical assets of the water system (e.g., through PLCs), this form of attacks is particularly severe for water systems. Cyberattacks on CPSs can be potentially even more hazardous when coupled with physical attacks (sabotage or other deliberate malicious actions) in a combined cyber-physical attack. For example, in a water CPS, adversaries may perform a terrorist attack such as contaminating a water source and simultaneously perform a cyberattack that manipulates input data from water quality sensors to magnify impact.

To summarize, attacks to water systems as CPS can have the following threats' nature:

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

- Cyber: Voluntary or not intent of individuals or groups to electronically corrupt or seize control of data or information essential to system operations.

- Physical: Water infrastructure is prone to any kind of physical threats either due to natural hazards (earthquakes, floods, etc.) or terrorist attacks or even due to an accident. The threat is a physical occurrence on the water supply system. By the physical type of threats, assets or technical devices of the water supply system will be damaged or manipulated. The physical threat may also destroy or damage sensors, data transmission lines or the process control/SCADA system in a way that the normal function is no longer possible.

- Cyber-Physical: The threat has a combined cyber-physical nature. It can generate in different ways, as for instance:
    - Combined cyber-physical threats: coordinated and long term attacks to the CI to reach and compromise the normal functioning.
    - Cyber threat to any of the physical component of the water infrastructure, e.g. monitoring devices (including e.g. IP cameras, networked sensors, AMR/AMI) that become more vulnerable to cyber attacks due to their higher automation/networking level
    - Physical threats to the "cyber" environment of the water utilities, e.g. Intrusion of attackers to the utilities control & operation centres (access to computers) or SCADA devices, etc.

4. EXAMPLE of relevant cyber attack

These attacks are becoming more and more frequent. There are examples of events in which attackers successfully deployed ransomware within a water utility's Supervisory Control and Data Acquisition (SCADA) system, forcing the facilities to switch to manual operation. Ransomware is most commonly deployed against information technology (IT) and business operations systems, but ransomware can also "infect connected OT systems, particularly if there is not adequate segmentation between IT and OT systems,"

Information about events is restricted, except for some very well-known ones as described in the following:

In February 2021, the City of Oldsmar, Florida, suffered an attack that could have compromised public health. A hacker breached the network of the city's drinking water treatment facility and manipulated the levels of chemicals used in the water purification process, attempting to increase the concentration of sodium hydroxide from its normal 100 parts-per-million (ppm) to 11,100 ppm.

Fortunately, an employee detected the hacker's movements in real time and stopped the chemicals from being released into the water supply.

The officials noted that it would have taken 24 to 36 hours for the chemicals to contaminate the water supply. The officials acknowledged, however, that the employee who witnessed the intrusion initially failed to report it, assuming it was another employee remotely accessing the network through an older program, rather than a hacker. The FBI cited poor cybersecurity, including weak passwords and outdated operating systems, as contributors to the hacker's success

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

A similar attack succeeded in 2019 in shutting down the treatment processes at a drinking water plant in Kansas. The Department of Justice accused a former employee of intentionally threatening public health and safety. Despite having resigned from the company two months earlier, the employee used his still-active remote-access credentials to interfere with the system.

5. Modeling approaches

Perceiving a water system as a CPS is no easy task, and needs the support of tools and models that help explore the effect of cyber-physical attacks on systems (and the cascade of effects between the two layers). Recent research has produced a variety of cyber-physical tools, which can be classified into two categories with regards to the representation of the cyber layer: (i) emulation/virtualization based and (ii) simulation based.

The first category (emulation/virtualization) formulates a detailed model of the cyber layer of the water CPS. This provides high fidelity in the explicit modeling of the behaviour of any real or virtual cyber component (from network cables to software protocols), using emulator platforms, discrete event simulators, virtualization machines, and software defined networks (SDNs). However, the implemented models tend to be domain-specific and applicable only to a specific CPS, with almost no chance of scalability or transferability to other systems. Moreover, monetary and time budget constraints increase with the scale of the systems and may be prohibitive for smaller utilities [4].

The second approach (simulation) represents both the cyber and physical layers with simulation models. As such, programming functions, routines, classes, and data structures represent elements and functionality of the cyber layer, modeling the information flow with feedback loops and interactions between the cyber and physical layers. This results in a lower fidelity process, since the focus is on the outcome of a cyber-operation or the state of a cyber-component, without the need for "bit-wise" modeling of interaction. Advantages compared to emulation/virtualization approaches include (a) "what-if' scenarios of cyber-physical attacks can be assessed without limitations, from the perspective of the water utility and by risk management officers untrained in ICT/IT fields and (b) the coupling with physical process simulators/models is much easier via the use of software wrappers, application programming interfaces, or dynamic link libraries. Simulation-based tools are also more generic and thus applicable to multiple water utilities, as long as their system can be converted to a network topology (with a physical and cyber layer) used by the model.

A simulation-based tool that is developed within STOP-IT is RISKNOUGHT (*Figure 2*), a holistic cyber-physical stress testing platform developed in Python [5]. The platform represents any water distribution system as a CPS, via automatically formulating a customizable SCADA model with enhanced control logic (e.g., users can add controls for water quality contamination response measures, controls based on data from the operational historian, etc.). An attack module is used to devise scenarios of complex cyber-physical attacks, as for example combinations of cyberattacks and backflow contaminant injection attacks. The latest version of RISKNOUGHT is interfaced with the water distribution model EPANET 2.2 to simulate the physical layer, and also leverages the WNTR water network resilience analysis Python package as a python interface [6].

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

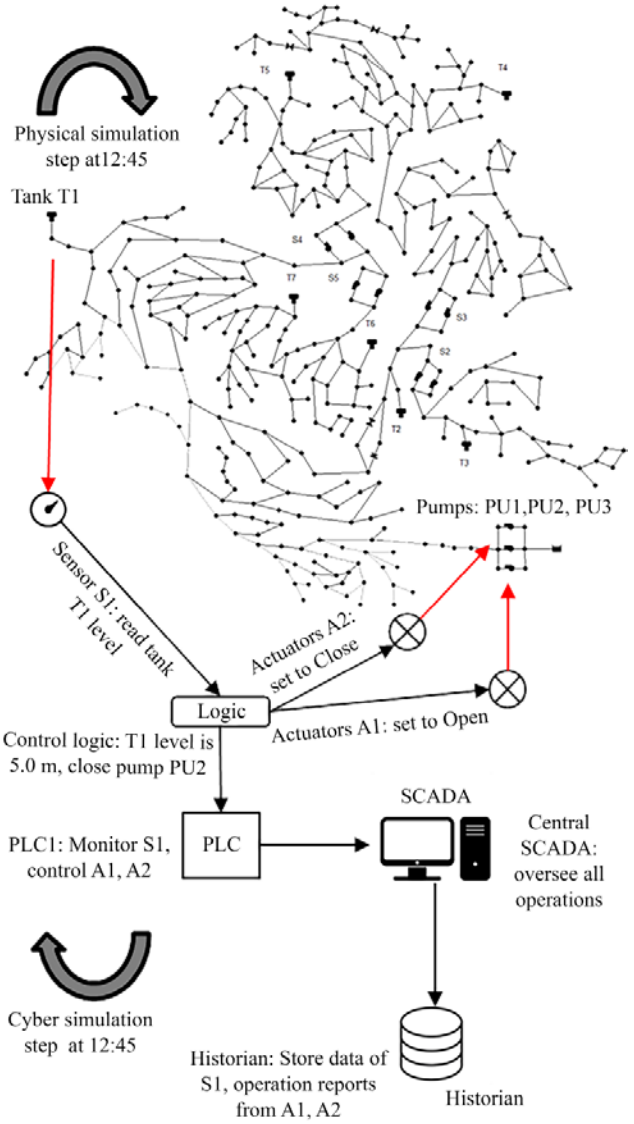

Figure 2: Example of the RISKNOUGHT, simulation-based tool for CPS and the different elements modeled with it.

digital-water.city
digitalwater_eu

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

6. Evaluation questions

1.) A contemporary water system includes:

☐	A: Physical elements, such as pipes and valves.
☐	B: Cyber elements, such as SCADA units and digital sensors.
☒	C: Both physical and cyber elements.
☐	D: Neither physical nor cyber elements.

Note: C is correct

2.) The concept of Cyber-Physical Systems (CPS) in water means that one has to look at a water system as a:

☐	A: Set of two connected layers, physical and cyber, where the cyber layer interacts with the physical layer.
☒	B: Set of two connected layers, physical and cyber, where both layers interact and exchange information with each other.
☐	C: Set of two connected layers, physical and cyber, where the physical layer interacts with the cyber layer.
☐	D: Set of multiple connected layers, including physical and digital ones but also human capital and financial ones.

Note: B is correct

3.) The most important cyber element in a water CPS is:

☐	A: A sensor that measures a critical aspect of the network operation (e.g. flow in a District Meter Area).
☐	B: A PLC, because it converts digital information, through logic rules, to physical actions.
☒	C: The SCADA unit, as it aggregates information from all sources and is a fundamental tool of the system operators.
☐	D: The Historian database because it includes a thorough history of network operations and data.

Note: C is correct

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

4.) The sensor-actuator principle in CPS means that:

☒	A: Information from cyber elements (from sensors) affects physical actions (through actuators).
☐	B: Information from physical elements (from actuators) affects cyber actions (sensors).
☐	C: There are both sensors and actuators in all water systems everywhere.
☐	D: There are either sensors or actuators in all water systems everywhere.

Note: A is correct

5.) A simulation-based CPS tool is:

☐	A: High-fidelity, as there is explicit modeling of the (bit-wise) behavior of any real or virtual cyber component (from network cables to software protocols).
☒	B: Low-fidelity, as the focus is on the overall outcome of a cyber-operation or the state of a cyber-component, without the need for lower-level, "bit-wise" modeling of element interactions.
☐	C: Either high-fidelity or low-fidelity, depending on the simulation used.
☐	D: Non-fidelity, as it does not combine the physical and cyber layers.

Note: B is correct

6.) An example of an attack in a CPS is:

☐	A: An eavesdropping attack, compromising information between a sensor and a PLC.
☐	B: An SQL injection attack in the SCADA database
☐	C: A physical attack to a wired connection within the water system.
☐	D: A malware installed in the SCADA unit using a security loophole.
☐	E: Answers (A), (B) and (D).
☒	F: Answers (A), (B), (C) and (D).
☐	G: Answers (A) and (D).

Note: F is correct

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

7.) An example of an attack in a CPS according to the sensor-actuator principle is:

☐	A: An SQL injection attack in the SCADA database.
☐	B: A physical attack damaging a fiber optic cable connection within the water system.
☐	C: A malicious change in the logic rules of a PLC, so that a valve of a network does not close at regular sensor reading thresholds.
☐	D: A compromise of the communication system between the sensor and the PLC, so that bogus (fake, synthetic) signals are read by the PLC instead of real information coming from the sensor.
☐	E: Answers (A), (C) and (D).
☒	F: Answers (C) and (D).
☐	G: Answers (A), (B), (C) and (D).

Note: F is correct

8.) What are the main categories of CPS modeling tools and their main characteristics?

……
……
……

Note: emulation-based vs. simulation-based, mention of fidelity aspects

9.) Describe two basic elements in a water CPS and mention if they are (primarily) cyber or physical.

……
……
……

Note: Based on the text mention, including extra elements (SCADA, communication protocols etc.)

7. More information

Five more training modules are described in DWC Deliverable 4.8:

- Information Systems for water
- Communication technologies for water
- Risk Management for Cyber-physical Security
- IoT Security for water systems
- Organizational Resilience Training

D4.8 will be available at https://www.digital-water.city/resources/ in early 2023!

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

8. References

[1] Dionysios Nikolopoulos, Georgios Moraitis, and Christos Makropoulos: "Chapter 7, Strategic and Tactical Cyber-Physical Security for Critical Water Infrastructures", in Soldatos, Praça, Jovanović (eds.) (2021), "*Cyber-Physical Threat Intelligence for Critical Infrastructures Security: Securing Critical Infrastructures in Air Transport, Water, Gas, Healthcare, Finance and Industry*", Boston-Delft: now publishers, http://dx.doi.org/10.1561/9781680838237].

[2] John Soldatos (ed.), Isabel Praça (ed.), Aleksandar Jovanović (ed.) (2021), "Cyber-Physical Threat Intelligence for Critical Infrastructures Security: Securing Critical Infrastructures in Air Transport, Water, Gas, Healthcare, Finance and Industry", Boston-Delft: now publishers, http://dx.doi.org/10.1561/9781680838237

[3] Gill, H. A Continuing Vision: Cyber-physical Systems. In Proceedings of the HCSS National Workshop on New Research Directions for High Confidence Transportation CPS: Automotive, Aviation, and Rail; Washington, DC, USA, 2008; pp. 1–28.

[4] Nikolopoulos, D.; Makropoulos, C.; Kalogeras, D.; Monokrousou, K.; Tsoukalas, I. Developing a Stress-Testing Platform for Cyber-Physical Water Infrastructure. In Proceedings of the 2018 International Workshop on Cyber-physical Systems for Smart Water Networks (CySWater); IEEE, 2018; pp. 9–11

[5] Nikolopoulos, D.; Moraitis, G.; Bouziotas, D.; Lykou, A.; Karavokiros,G.; Makropoulos, C. Cyber-Physical Stress-Testing Platform for Water Distribution Networks. J. Environ. Eng. 2020, 146, 04020061, doi: 10.1061/(ASCE)EE.1943-7870.0001722

[6] Klise, K.A.; Bynum, M.; Moriarty, D.; Murray, R. A software framework for assessing the resilience of drinking water systems to disasters with an example earthquake case study. Environ. Model. Softw. 2017, 95, 420–431, doi: 10.1016/j.envsoft.2017.06.022

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.

Digital Water .City

Leading urban water management to its digital future

digital-water.city
digitalwater_eu

digital-water.city has received funding from the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 820954.