Cyber-physical Hardening of the Digital Water Infrastructure

Umit Cali
Norwegian University of Science and Technology
Trondheim, Norway
umit.cali@ntnu.no

Ferhat Ozgur Catak
University of Stavanger
Stavanger, Norway
f.ozgur.catak@uis.no

Zsolt György Balogh
Corvinus University of Budapest
Budapest, Hungary
zsolt.balogh@uni-corvinus.hu

Rita Ugarelli
SINTEF Community
Oslo, Norway
Rita.Ugarelli@sintef.no

Martin Gilje Jaatun
SINTEF Digital
Trondheim, Norway
martin.g.jaatun@sintef.no
University of Stavanger
Stavanger, Norway
martin.g.jaatun@uis.no

ABSTRACT

Water supply and drainage systems, which are categorized as critical infrastructure, serve a crucial role in preserving societal health and well-being. Since climate change effects, harsher regulations, population changes, and aging infrastructure pose problems for these systems, the industry is experiencing a digital transition to meet these concerns. This article addresses Cyber-Physical-Social Systems (CPSS) and its application to water distribution networks, combining cyber, physical, and social components for adaptive, responsive, and intelligent management. This paper's primary contributions include a review of recent security problems in the water industry, which emphasizes the necessity for stronger security measures. The article also examines how water distribution networks, as CPSS, fit into the interrelated realms of physical infrastructure, digital components, and stakeholder involvement, necessitating an all-encompassing system design and management strategy. In addition, the article investigates various cyber-physical attack scenarios, risk management methodologies, and the crucial role of integrated knowledge in mitigating these risks. In the context of increasing digitalization, the paper emphasizes the significance of taking into account both water infrastructure regulations under social space, such as the Water Framework Directive 2000/60/EC (WFD), and cyberspace-related legal and legislative standards, such as the Network and Information Systems (NIS) Directive, the General Data Protection Regulation (GDPR) and Cybersecurity Act. By tackling these difficulties and concentrating on privacy concerns, water utilities may contribute to the overall security and resiliency of vital infrastructure while assuring compliance with applicable legislation.

EICC 2023, June 14–15, 2023, Stavanger, Norway

ACM ISBN 978-1-4503-9829-9/23/06.
https://doi.org/10.1145/3590777.3591408

CCS CONCEPTS

• **Computer systems organization** → **Sensors and actuators**; • **Security and privacy** → **Distributed systems security**; • **Applied computing** → *Computers in other domains*; • **Networks** → **Network reliability**.

KEYWORDS

critical infrastructure, water distribution networks, security

ACM Reference Format:
Umit Cali, Ferhat Ozgur Catak, Zsolt György Balogh, Rita Ugarelli, and Martin Gilje Jaatun. 2023. Cyber-physical Hardening of the Digital Water Infrastructure . In *European Interdisciplinary Cybersecurity Conference (EICC 2023), June 14–15, 2023, Stavanger, Norway*. ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3590777.3591408

1 INTRODUCTION

Water supply and drainage systems are classified as critical infrastructure. The service they provide is crucial for social health and wellbeing. The performance of these systems is challenged by multiple pressures: climate change impacts, stricter regulations (e.g., new EC water distribution and wastewater directives), demographic changes as well as the natural aging of their supporting infrastructures that can age back to even 100 years. The sector is currently under a process of digital transformation which provides the means to better monitor the system performance and simplify reliability studies and operation and maintenance scheduling. However, the digital transition should be properly planned and applied, not only in terms of technological maturity, but also in terms of organizational maturity and competence in facing new challenges. In fact, we talk about physical-cyber-social integrated systems that call for integrated assets, but also integrated expertise (e.g., hydraulic modeling and IT operation expertise should be integrated in new professional profiles). Integrated knowledge is also mandatory when looking at water system risk management. In systems that are more and more interconnected cyber attacks can impact the physical layer of the system and vice versa. Meaning safety and security should be aligned and combined in the water utilities risk management processes.

Beside the regulations that are directly related to the the water infrastructure such as Water Framework Directive 2000/60/EC (WFD), it is essential to consider the cyberspace related legal and legislative standards to investigate the cyber and physical aspects of the topic. The European Union (EU) has adopted a number of conventions, one of which is known as the Network and Information Systems (NIS) Directive, in order to ensure that vital services are protected from the threat of cyberattacks. The digital infrastructure of the water system is one example of this. The NIS directive's objective is to bring about, throughout the European Union, a level of security that is consistently high and uniformly high across all networks and information systems.

Furthermore, in addition to the cybersecurity aspects, the digital privacy and data protection matters shall be investigated. The GDPR applies to any firm that handles EU individuals' personal data, regardless of location. This means that water supply and drainage systems that deal with the personal information of EU citizens must follow GDPR. For example, if a water supply company gathers personal information from EU customers for billing or customer support, it would be a data controller under the GDPR and must get permission, verify data accuracy, and provide individuals with a chance to access and manage their data. The GDPR requires the corporation to take technological and organizational steps to protect personal data. The GDPR only covers personal data, which is any information about a living person. The GDPR applies exclusively to personal data handled by critical infrastructure systems like water supply and drainage systems.

The main contributions of this article as follows: We provide a brief survey of previous security incidents in the water sector as a motivation for the increased need for security in this domain. Furthermore, we demonstrate how water distribution networks fit into cyber-physical-social systems. We provide an example of a cyber-physical attack scenario, and explain how the related risks can be identified and handled. Finally, we delve into the privacy aspects that arise when water distribution networks transcend the cyber domain.

2 BACKGROUND

One of the earliest cases of cyber-physical security breach was the Maroochy Shire incident [20], where disgruntled former employee Vitek Boden abused credentials for wireless SCADA controllers, causing vast amounts of untreated sewage to be dumped in the environment, resulting in damages in the range of AUD 1 million. You could argue that this was more a case of poor configuration control than a cyber vulnerability (since Boden's credentials and access to equipment should have been revoked), but history does not stop here.

About a decade later, an image purporting to be a screenshot of a water treatment plant HMI was published on the text-sharing site Pastebin [7]. For people without local knowledge, it might have been a little confusing, since the image was headed "The city of South Houston Nevada water plant" - and Houston is surely in Texas, not in Nevada? A search with an online map tool quickly shows that the city of South Houston is indeed a suburb of the more famous city of Houston, a short 20-minute car ride away. Further searches reveal that the city of South Houston has a *street* named Nevada, where at the intersection of Beaumont St there appears to be a vacant lot. Switching to aerial photography it was possible to see something resembling a water tank, which was confirmed when switching to street view.

The technology enthusiast in question, simply referred to as "Pr0f", claimed to have accessed the HMI of several Siemens Simatic PLCs connected to the internet, due to the default password of "100" not having been changed. Ignoring for a moment the ridiculously short and simple default password, relying on an attacker not knowing the default password is the very worst form of security by obscurity. Used Siemens PLCs are abundantly available for purchase via online marketplaces, and even without buying your own PLC, default passwords tend to be shared widely in online forums.

Putting an industrial control system on the internet can seldom be done with impunity; there is even a specialized search engine (shodan.io) that can be used to find any "thing" on the internet. In February 2021, the threat to water infrastructures became real when an unauthorized person gained remote access to the water treatment plant in the town of Oldsmar, Florida [22], and managed to increase the amount of lye added to the drinking water to a potentially dangerous level. Monitoring at the water treatment plant did however detect the change immediately, and was able to reset the system to a safe state. In this case, the attack was made possible due to a remote desktop application (TeamViewer) being accessible from the open internet.

With a sufficiently motivated and technologically capable adversary, hardly any critical infrastructure is impervious to attack. This was evident in the attacks against the Ukrainian power grid in 2015 and 2016 [5], where a large number of people were left in the dark for several hours and more, and where restoration in many cases was only possible through manual intervention.

A number of recent European projects have addressed cyber-physical security of water infrastructures. The H2020 STOP-IT project [21] tackled cyber-physical security in water distribution networks on several levels, providing tools for managers, risk officers and process control managers and technical operators. The H2020 Digital Water City project [3] had a primary focus on safe urban water; particularly bathing in urban rivers and use of processed wastewater for agricultural irrigation.

3 CYBER PHYSICAL SOCIAL SYSTEM

Cyber-physical-social systems (CPSS) are a type of system that integrates cyber, physical, and social components to enable new functionalities and services. These systems are designed to be adaptive, responsive, and intelligent, allowing them to sense, learn, and interact with their environment and users. CPSS are characterized by their ability to collect, process, and analyze large amounts of data from different sources, including sensors, social media, and online platforms. They can also actuate physical processes, such as controlling traffic lights or adjusting the temperature in a building, based on the information they gather. CPSS has wide-ranging applications, from smart cities and transportation systems to healthcare and education, and is expected to play an increasingly important role in shaping our lives and society.

Figure 1 shows the overview of CPSS for a drinking water system. The CPSS comprises three interconnected components: Physical Space, Cyber Space, and Social Space. The Physical Space includes the physical infrastructure and assets of the water supply system. The Cyber Space includes the digital components, such as sensors and management systems, which are integrated into the water supply system architecture. The Social Space comprises the stakeholders who are engaged in the water supply system design, including end-users, regulators, policymakers, and other members of the community. The intersections between the three spaces show the interdependence and integration between them, highlighting the need for a comprehensive approach to the design, management, and security of digital water systems.

3.1 Physical Space

The CPSS is an innovative approach that integrates the water services industry's physical, digital, and social components for digital water systems. In the physical space, the water supply system architecture comprises a range of components, including the water source (groundwater, lakes, rivers, ...), reservoirs, gravity systems, water treatment plants (filtration, coagulation, disinfection, ...), pump stations, storage reservoirs, distribution networks, end-users, storage tanks, and potable water. The water supply system starts with sourcing water from lakes, rivers, or groundwater, which can then be transported to the reservoirs and stored for future use. Then, water is distributed to the water treatment plant, where filtration, coagulation, and disinfection processes remove impurities or contaminants. After treatment, the water can be pumped to the storage reservoir, and from there, it is distributed to end-users through a network of pipes. Residential, commercial, and industrial consumers are the end-users, and water metering devices can be installed to monitor water consumption and ensure accurate billing. The physical space of the CPSS also includes monitoring and managing the water supply system architecture using strategically placed sensors throughout the infrastructure to collect data on water pressure, flow rates, and quality. This data can be analyzed in real-time to identify potential issues or areas for optimization using intelligent management systems. Leveraging the CPSS approach, water utilities can improve the efficiency and effectiveness of the water supply system architecture. Real-time data analytics and predictive modelling help identify potential issues before they become more significant problems, minimizing water losses due to leaks or other issues and ensuring consistent water quality. In conclusion, the physical space of the CPSS for digital water systems is critical in delivering clean and safe water to end users. By incorporating advanced technologies and approaches, stakeholders across the industry can work together to optimize the physical space of the CPSS, improve water quality, conserve energy, and reduce water losses, ultimately benefiting society as a whole.

In addition to the components and infrastructure involved in the water supply system architecture, the physical space of the CPSS for digital water systems also includes the maintenance and repair of the infrastructure. This can involve regular maintenance activities such as pipe cleaning, valve replacement, pump maintenance, and emergency repairs in the event of a leak or other issue. With the help of advanced technologies such as remote monitoring, predictive maintenance, and automated repair systems, water utilities can minimize downtime and optimize the performance of their infrastructure. By proactively addressing issues and prioritizing maintenance tasks based on real-time data and analytics, water utilities can improve the reliability and resilience of their water supply systems, ultimately leading to better service for end-users.

3.2 Cyber Space

The cyber space is a critical aspect of the CPSS for digital water supply and drainage system, as it encompasses the digital components of the water supply system architecture. Sensors are considered to play important role in terms of digitization and positioned in both Cyber and Physical Spaces. This includes deploying a decentralized system of sensors, communication protocols, and intelligent management software to instantly collect, process, and disseminate information. The sensors in the CPSS measure various water-related metrics, such as pressure, quality, flow rate, purity, and temperature. This data is transmitted to smart management systems through wired and wireless communication protocols for analysis and optimization. The CPSS's intelligent management systems utilize advanced data analytics and machine learning algorithms to identify anomalies, recurring trends, and potential problems. The cyber space also enables remote monitoring and control technologies to adjust the water distribution infrastructure instantly in case of a breakdown, such as changing pump speeds, opening or shutting valves, or triggering emergency response procedures. Additionally, web-based portals or mobile apps can provide customers with real-time water use statistics, billing information, and other essential water supply system design details. By leveraging sensor technologies, communication protocols, and intelligent management systems, stakeholders can collaborate to enhance the performance of the water supply system design, improve water quality, and reduce water losses.

The cybersecurity and privacy of digital components such as sensors, communication protocols, and intelligent management systems are crucial for the CPSS framework in digital water systems. Protecting these components against cyber threats is vital as they become integral parts of the water supply system architecture. To prevent cybercrime like hacking and data leaks, the CPSS uses various technologies, processes, and rules, including firewalls, encryption, and intrusion detection systems. The CPSS places equal importance on cybersecurity and digital privacy, and sensitive user information is protected during the collection of water use data through secure communication methods, data retention policies, and anonymization techniques. Following best practices and standards is necessary for water utilities and other stakeholders to ensure the cybersecurity and digital privacy of the CPSS.

Water utilities should also do frequent risk assessments to detect possible vulnerabilities in the digital components of the water supply system architecture and then take the necessary security steps to mitigate such weaknesses. With regular penetration testing, vulnerability scanning, and other security checks, holes and threats may be found. Furthermore, the CPSS for digital water systems must include protections for both cyberspace and digital privacy. Water utilities and other stakeholders may safeguard end-user privacy and reduce the risk of cyber attacks by adopting suitable security

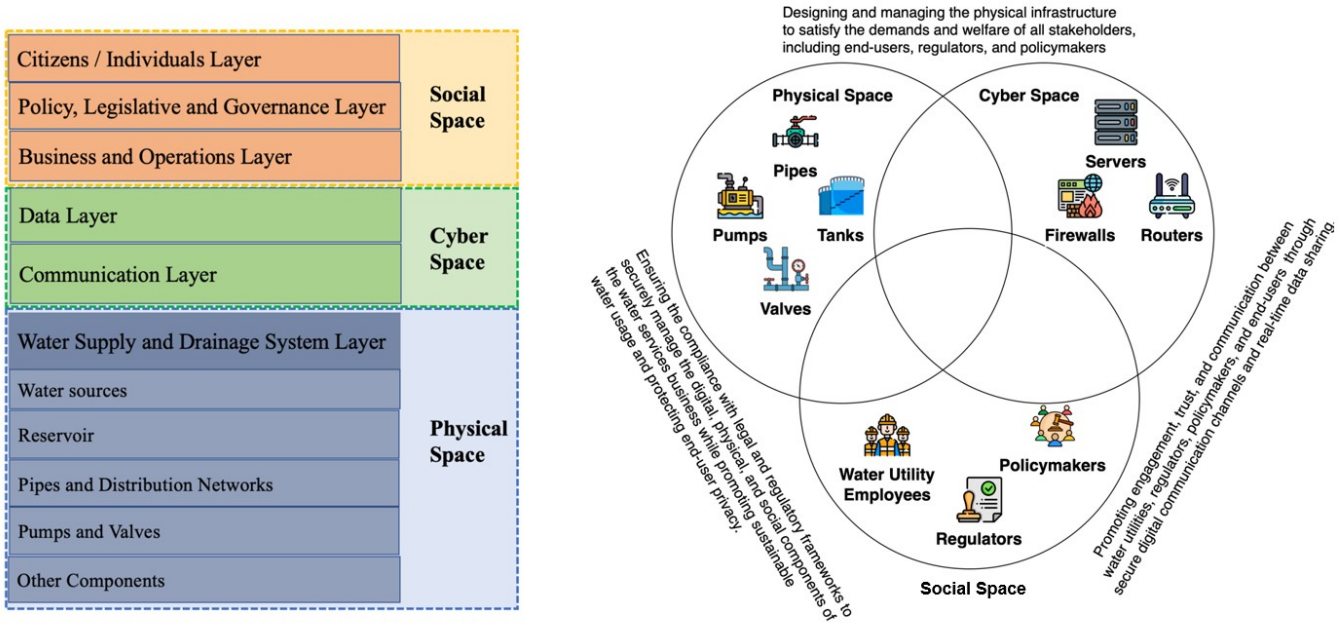

Figure 1: Cyber Physical Social System (CPSS) for Digital Water Systems.

measures and best practices to maintain the integrity, availability, and confidentiality of the digital components of the water supply system architecture.

3.3 Social Space

In the CPSS for digital digital water supply and drainage system, the social space comprises the stakeholders who are engaged in the water supply system management, including water operators, consumers /individuals, regulators, policymakers, and other members of the community. The social space is essential for designing and managing the water supply system architecture to satisfy all stakeholders by considering the public policy, legislative, and judicial aspects. The CPSS social space improves water utility-end-user communication and engagement. Water utilities may provide real-time data on water use, quality, and other parameters to end-users through web-based portals and mobile apps. This may promote water utility-end-user openness, trust, and engagement. The CPSS social environment may also help regulators, legislators, and water utilities work together. These stakeholders may help build and manage the water supply system architecture to suit all stakeholders' demands. This might involve implementing water management best practices and sustainable water usage rules. CPSS social space may also address water management-related social and environmental challenges. This includes water conservation, alternate water sources, and water loss reduction measures. These programs may encourage sustainable water usage and solve social and environmental water management issues by incorporating the community. In the CPSS for digital water systems, it is necessary to examine the legal and regulatory considerations connected to the digital, physical, and social components of the water services business. The water services industry's digital, physical, and social components must be managed securely and compliantly in accordance with legal and regulatory requirements like NIS 2 and GDPR. EU Law NIS 2 protects important infrastructure and services, including digital water systems. NIS 2 mandates that water utilities and other stakeholders secure the digital components of the water supply system architecture against cyberattacks. Incident response strategies, risk management frameworks, and security and data protection requirements are examples. The digital water system, CPSS, must also address GDPR. GDPR regulates data collection, storage, and processing, including water use and consumption statistics. Protecting end-user privacy and ethically managing personal data requires GDPR compliance. National data protection and cybersecurity regulations must also be examined. These standards may include criteria for managing and storing personal data and protecting the digital components of the water supply system design against cyberattacks. Water utilities and other stakeholders must adopt policies and processes for managing and preserving the digital, physical, and social components of the water services business to comply with these legal and regulatory criteria. These may include security measures, incident response strategies, and data protection and cybersecurity requirements.As summarized, the CPSS for digital water systems must comply with legal and regulatory frameworks to securely handle the digital, physical, and social components of the water services business.

4 ATTACK AND COUNTERMEASURES IN THE CYBER-PHYSICAL SPACE

4.1 Cyber Physical Attack Scenario

Systems being more interconnected as C-P systems also calls for an integrated risk management covering both the cyber and the physical part in order to intercept and being prepared for integrated hazards and cascading effects. As an example, consider a water distribution system supplying water to a city (see Figure 2). The network is composed of different districts (District Metered Areas - DMA) and the water is supplied by a system of several tanks. This fictional network is known as "C-town" in the literature, where all LoRa sensors are connected with wireless technology to gateways with the IoT LoRaWAN protocol. The network is composed of 5 District Metered Areas (DMAs), 443 pipes, 399 nodes, 4 Pressure Release Valves (PRVs), one Check Valve and one Temperature Control Valve (TCV). The water is pumped through pumping station S1 to tanks T1 and T2, and water supply to T2 is controlled by TCV. Pumping stations S2 and S3 draw water to tanks T3 and T4, while stations S4 and S5 pump supply from T1 to T5, T6 and T7.

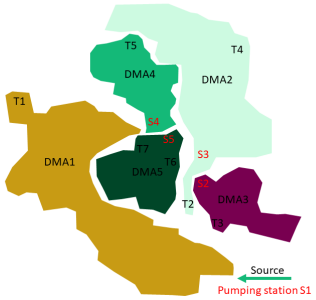

Figure 2: High-level overview of the c-town water network

Customers report of loss of water pressure in the district 2 (DMA2) which is served by T2. Its automated refill protocol is known. When the tank sensor leads low stages, the supplying valve (TVC) opens – filling the tank. When the tank stage is high enough (>5.5 m) then the PLC controlling the valve, orders it to close. What can have possibly happened?

Possible causes include:

(1) Use Case 1: Physical attack on water pipeline: a critical pipe feeding DMA2 is broken, either as physical attack or simply due to structural failure. In this case, depending on the level of redundancy of the network, the reduced water supply will be detected quite easily, either as a drop of pressure monitored in the system, or as customers complain.
(2) Use case 2: Cyber attack on pump from reservoir to balancing tank, cutting off flow of water

4.2 Possible Countermeasures

In the general case, there are a number of possible physical countermeasures:

(1) Real time pressure monitoring – this requires reliable water pressure measuring sensors placed at strategic points in the water network
(2) Identify pipes at higher hydraulic criticality (i.e., pipes that created major impact in terms of unsupplied water, if they fail) and increase redundancy of the system, e.g., creating bypass pipes
(3) Protect the site: To build a fence around the Tank 2, where the Level Sensor is installed, would be helpful in mitigating the risk in terms of reducing the probabilities of an intrusion.
(4) Binary contacts: To install binary contacts at the entrances of the building would help significantly in the detection of physical intrusion at the Tank 2. It would be helpful in mitigating the risk in terms of reducing the consequences because the amount of time to act against the attack would be reduced.

On the real time dimension, a physical attack can be compounded by compromising of sensors that should alert the water operator. Incidents should be detected and countermeasures should be instigated before the customers themselves have to notify the operator. The sensors themselves can have different levels of security, as explained by Bour et al. [2]. Using Bour's checklist [1], IoT sensor developers can raise the bar significantly, avoiding many of the entry-level attacks on the sensors.

Modern water distribution networks are controlled by SCADA systems that effectively are industrial computer networks, and as such they can benefit from many network security devices that traditionally have only been used in IT networks. One example is the Security Information and Event Management (SIEM) application described by Gonzales et al. [6].

Effective countermeasures are dependent on risk identification (as otherwise it is impossible to determine what should be protected against), and for this purpose Ostfeld et al. [12] document a Risk Identification Database that can be tailored to a specific case, and used to enumerate relevant risk. Handling of these risks is facilitated by a companion Risk Remediation Measures Database [10] that offers a generic starting point (but which also should be customized to the case at hand).

On the preparedness dimension, it is possible to increase the ability to respond to attack events, through scenario-based stress-testing of the network. Example of stress-testing modelling solutions is the RAET framework [9] developed in the STOP-IT project. RAET supports the stress–testing of the integrated cyber-physical system against single and complex scenarios of attack compromising both water quality and quantity. It can model purely physical attacks (e.g., contaminant injection), cyber-attacks (e.g., false-positive contamination event by sensor manipulation) or combined cyber-physical attacks (e.g., contaminant injection and sensor manipulation). For simulated events, the user can select and test possible risk reduction measures, and assess its effectiveness in reducing either the probability or the consequence.

To sum up, cyber security countermeasures include:

(1) Use the IoT Securiity Checklist to maximise security of IoT devices [1]
(2) Deploy a SIEM [6] to monitor the water network for cuyber threats

(3) Use the RIDB [12] and RRMD [10] databases to support cyber risk management
(4) Perform stress-testing modeling [9] that takes cyber risks into acoount

5 PRIVACY AND CYBERSECURITY CYBERLAW ASPECTS

In particular when it comes to the introduction of smart water meters [18], there have been some concern with respect to privacy of individuals, with many similar aspects as privacy of smart electricity meters [8].

Smart water meters can help to detect leaks in the distribution network (when the sum consumption in an area is significant less that the volume measured centrally), but also have higher privacy concerns as noted above.

Beyond the technological, economic and social ecosystem it is the regulation which grants the proper functional framework for elements of vital infrastructure. The water supply system is obviously one of the most sensitive components of these, and the regulatory authorities of the European Union are more than aware of this paramount importance. The functionality and safety of the water resources and the supply network – namely the pipelines, water treatments and pumps – greatly depends on the automatic, computerized controlling system.

The "larger systems are vulnerable as well" – observes Bruce Schneier, a prominent expert and author in cybersecurity.[19] He also warns about the physical effects of the information systems, stipulating that as they "affect the world directly and physically, the risks increase dramatically as they come under computer control "[19] . All these observations are obviously meet the water supply systems which are extensive and greatly ubiquitous. As these system components are exposed to cyber-attacks, there is a vital need to ensure their continued, reliable and secure operation through legal regulation, too. Beyond the technical data, these systems also contain and process a plethora of personal data, so the business continuity and integrity shall not be enough. The security regime must also protect the personal data, too. To summarize these expectations, we can see the classical core concept of the cybersecurity management, that is the so-called CIA triad.

The CIA triad is the complex doctrine of Confidentiality, Integrity and Availability, destined to protect the functionality, operability and reliability of an information system. Functionality of the system is based on the readiness and accessibility of transaction data – irrespective whether these data are referred to technological processes, economic operations or informational privacy.[4]

- The Confidentiality generally means the protection of informational privacy. Concerning the water supply systems, we must consider the protection of personal data both for clients and the staff members, employee of the service provider.
- Integrity in this respect encompass the consistency, accuracy and trustworthiness of the technical and transaction data contained in the control and management system. A duly designed system shall prevent any unauthorized person in alteration or deletion of data either within the system and/or in course of data transfer.
- As to the Availability, under these attributes the system will keep the data consistently and readily accessible for authorized persons. These criteria also involve the permanent functionality of the control system and the services.

5.1 The scope of the relevant European regulatory framework

The cybersecurity regime of water supply fits flawless to the relevant regulatory framework of the European Union. The most important elements of the current regime are as follows:

- The GDPR [14]
- the NIS Directive (2016/1148/EU) [13]
- the Cybersecurity Act (Regulation 2019/881/EU).[15]

The confidentiality criteria of the CIA triad is treated in the framework of GDPR, while the two other purposes are regulated by the NIS directive and the Cybersecurity Act.

All these statutes are destined for general purpose, not specially for the water supply system, which should be seen as just one of the affected activities and businesses. The drinking water supply and distribution system is subsumed under the scope of cybersecurity regulation by the provisions of the NIS directive as the directive identified these systems as one of the essential services. Considering the provisions of Article 4 (4) on "operators of essential services" and the Annex II. thereof we shall conclude that the security regime of these systems should be regulated by the NIS directive and related laws. The Article 2 excludes the option of regulation on data protection referring the Directive 95/46 as relevant law in this respect. Importantly, the prior data protection regulation has been replaced by the General Data Protection Regulation (GDPR), which now controls relevant data processing issues. Thus, the GDPR is an integral part of the legislative framework for protecting the security of water supply systems.

The operators of such systems are due to work under special security provisions. The scope of the directive covers only the water suppliers for whom distribution of water for human consumption is the general activity. Namely for instance the traders of bottled water – trafficking this among other products in a supermarket – are not affected by these provisions of NIS directive. The regulatory environment is constantly evolving, differentiating, and trying to keep pace with the challenges posed by the digital environment. We are therefore witnessing relatively rapid generational changes in this area. New directives and regulations are replacing legislation made out just a few years ago. At the same time, new institutions and organisations are being created.

Though the NIS directive is still in effect, the new replacement directive is already promulgated. The NIS2 directive was enacted by the European Parliament and the Council in December 2022, and entered into force 16 January 2023. This is the sunrise period of the NIS2, which should be applicable for the member states after 21 months of national implementation from 17 October 2024. The affected trades are identified as Essential services and Important services. Essential services are

- Energy supply (Gas/Oil/Electricity; District heating; Hydrogen)
- Transport
- Banking

- Financial market
- Health
- Drinking water supply
- Waste water treatment
- Digital infrastructure
- Public administration
- Space technology

Other Important services are enlisted as follows:

- Postal and courier services
- Waste management
- Chemicals (Manufacture; Production; Distribution)
- Manufacturing of
  - Medical devices
  - Computer, electronic and optical products
  - Electrical equipment
  - Machinery
  - Motor vehicles, trailers, semi-trailers
- Digital providers
  - Online market places
  - Online search engines
  - Social networking platforms

This timeframe is quite tight considering the volume and dimensions of the task. 27 member states and plenty of operators in 15pivotal trades are about the be prepared for a more robust and resilient cybersecurity regime [17].

The NIS stipulated the installation of a European-wide notification and response system equally robust in every member states. This expectation is not fulfilled appropriately, yet. NIS2 is scheduled to eliminate these inadequacies of the current regime, and to implement new measurements in cybersecurity, like reinforcing the reporting obligations and enhancing collaboration among service operators and the competent authorities.

NIS2 expects organizations to comply with a new set of expectations including risk assessment and information security policies, business continuity and incident management, supply chain security [11]. Extensive use of cryptography and data encryption is a necessary part of this scenario. Blockchain-based resources obviously also can find the place in this ecosystem[16].

5.2 Compliance and Certification

The Cybersecurity Act of the EU foresighted the implementation a continental, pan-European cybersecurity certification system. This can make visible and conceivable the compliance to the cybersecurity criteria and can enhance the security awareness among the users of IT services. The program coordinator agency is the ENISA, which is expected to accomplish the preparatory work by the year 2023.

The European cybersecurity certification scheme is about to be a comprehensive regime of technical cybersecurity requirements, industrial standards and evaluation procedures, equally accepted and implemented in every EU member states. Applicant may gain a European cybersecurity certificate endorsing that the relevant IT product, process or service has been certified by a competent authority under the provisions of cybersecurity requirements [15]. The granted certificates will be disclosed on a dedicated portal of the ENISA.

The cybersecurity scheme shall grant certification on three levels as:

- basic
- substantial
- high

The elements of essential services shall be expected to be certified on “high” level, and obviously this goes for the drinking water supply and distribution systems.

6 CONCLUSION

In conclusion, the growing interconnection of water supply and drainage systems as cyber-physical-social systems (CPSS) needs an all-encompassing and unified approach to risk management, digital privacy, and cybersecurity. This article has offered an overview of the challenges and possibilities posed by the digital transformation of the water industry, including the need to handle cybersecurity, digital privacy, and the integration of cyber, physical, and social components.

A hypothetical cyber-physical attack scenario on a water distribution network has been explored, highlighting the necessity of detecting and managing risks in both cyber and physical worlds. Real-time pressure monitoring, boosting redundancy, safeguarding physical installations, and installing improved security measures for sensors and SCADA systems are potential measures. Furthermore, using resources such as risk identification databases and risk mitigation measures databases may facilitate the customization of risk management techniques for particular circumstances.

In addition to the technical issues, it is essential to take into account the privacy and cybersecurity cyberlaw aspects that regulate the correct functioning framework of vital infrastructure, such as water supply systems. The legislative framework in the European Union consists of the GDPR, the NIS Directive, and the Cybersecurity Act, which jointly safeguard the confidentiality, integrity, and availability of information systems. The next NIS2 Directive intends to significantly improve the security regime for critical services, such as water distribution networks.

Compliance and certification, as envisioned by the Cybersecurity Act, are essential for improving security awareness and ensuring that IT systems, processes, and services fulfill severe cybersecurity criteria. The deployment of smart water meters intensifies privacy problems, highlighting the necessity for effective privacy protection measures in the water industry’s digital transformation. Moreover, the lessons learned and experiences obtained from other critical infrastructure domains, such as power systems, can be used to water infrastructure use cases.

Ultimately, the successful transition to digitally enhanced water distribution networks as CPSS will necessitate a holistic approach that incorporates technological advancements, regulatory compliance, and stakeholder participation in order to maintain and enhance the essential services provided by water supply and drainage systems. In order to secure the cyber-physical security, resilience, and compliance of water critical infrastructure in the face of new threats, this will need not just solving the difficulties of digital transformation but also navigating the expanding regulatory framework.

ACKNOWLEDGMENTS

To be added after review

REFERENCES

[1] Guillaume Bour. 2022. IoT SECURITY CHECKLIST. https://www.sintef.no/contentassets/8fa5c7e3a81749b8952979000ee34c31/iot-security-checklist-v1.1.0.pdf

[2] Guillaume Bour, Camillo Bosco, Rita Ugarelli, and Martin Gilje Jaatun. 2023. Water-Tight IoT – Just Add Security. *Journal of Cybersecurity and Privacy* 3, 1 (2023), 76–94. https://doi.org/10.3390/jcp3010006

[3] Nicolas Caradot. 2022. Digital Water City project. https://zenodo.org/communities/dwc/about/ H2020 - 820954.

[4] Wesley Chai. 2023. *What is the CIA triad (confidentiality, integrity and availability)?* TechTarget. https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA

[5] Dragos. 2017. *CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations.* Technical Report. Dragos Inc.

[6] Gustavo González-Granadillo, Susana González-Zarzosa, and Rodrigo Diaz. 2021. Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures. *Sensors* 21, 14 (2021), 4759.

[7] Matt Liebowitz. 2011. Hacker says he breached Texas water plant network. *NBC News* (2011). https://www.nbcnews.com/id/wbna45394132

[8] Maria Bartnes Line, Inger Anne Tøndel, and Martin Gilje Jaatun. 2011. Cyber security challenges in Smart Grids. In *Innovative Smart Grid Technologies (ISGT Europe), 2011 2nd IEEE PES International Conference and Exhibition on.* IEEE. https://doi.org/10.1109/ISGTEurope.2011.6162695

[9] C. Makropolous, G. Moraitis, D. Nikolopoulos, G. Karavokiros, A. Lykou, I. Tsoukalas, M. Morley, M. Castro Gama, E. Okstad, and J. Vatn. 2019. STOP-IT D4.2: Risk Analysis and Evaluation Toolkit (RAET). https://stop-it-project.eu/download/risk-analysis-and-evaluation-toolkit/

[10] H.J. Mälzer, F. Vollmer, and A. Corchero. 2019. STOP-IT D4.3 Risk Remediation Measures Database (RRMD). https://doi.org/10.5281/zenodo.3947951

[11] Marina Nonkovic. 2023. *NIS2 Directive comes into force to create a common level of cybersecurity.* https://www.burges-salmon.com/news-and-insight/legal-updates/data-protection/nis2-directive-comes-into-force-to-create-a-common-level-of-cybersecurity

[12] A. Ostfeld, E. Salomons, P. Smeets, C. Makropolous, E. Bonet, J. Meseguer, H.-J. Mälzer, F. Vollmer, and R. Ugarelli. 2018. STOP-IT D3.2 Risk Identification Database (RIDB). https://stop-it-project.eu/download/ridb-supporting-document-d3-2/

[13] European Parliament and Council of the European Union. 2016. Directive 2016/1148/EU of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive). Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L1148

[14] European Parliament and Council of the European Union. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation; GDPR). Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

[15] European Parliament and Council of the European Union. 2019. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0881

[16] European Parliament and Council of the European Union. 2022. Directive 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Official Journal of the European Union. *URLoftheofficialpublication*

[17] European Parliament and Council of the European Union. 2022. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. Official Journal of the European Union. *URLoftheofficialpublication*

[18] Elad Salomons, Lina Sela, and Mashor Housh. 2020. Hedging for Privacy in Smart Water Meters. *Water Resources Research* 56, 9 (2020), e2020WR027917. https://doi.org/10.1029/2020WR027917 arXiv:https://agupubs.onlinelibrary.wiley.com/doi/pdf/10.1029/2020WR027917 e2020WR027917 2020WR027917.

[19] Bruce Schneier. 2018. *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World.* W. W. Norton & Company. https://www.schneier.com/books/click-here/

[20] Jill Slay and Michael Miller. 2007. Lessons learned from the Maroochy water breach. In *International conference on critical infrastructure protection.* Springer, 73–82.

[21] R Ugarelli, J Koti, E Bonet, C Makropoulos, J Caubet, S Camarinopoulos, M Bimpas, M Ahmadi, L Zimmermann, and MG Jaatun. 2019. STOP-IT-Strategic, Tactical, Operational Protection of water Infrastructure against cyber-physical Threats. *Physical and Cyber Safety in Critical Water Infrastructure* 56 (2019), 130.

[22] Amir Vera, Jamiel Lynch, and Christina Carrega. 2021. Someone tried to poison a Florida city by hacking into the water treatment system, sheriff says. *CNN News* (2021). https://edition.cnn.com/2021/02/08/us/oldsmar-florida-hack-water-poison