Water 4.0 in Hungary: Prospects and Cybersecurity Concerns

Tamás Szádeczky

Department of Instrumentation and Automation, Institute of Electronic and Communication Systems, Kandó Kálmán Faculty of Electrical Engineering, Óbuda University, Bécsi út 96/b, 1034 Budapest, Hungary
szadeczky.tamas@kvk.uni-obuda.hu

Budapest University of Technology and Economics, Faculty of Economic and Social Sciences, Department of Management and Business Economics, Műegyetem rkp. 3, 1111 Budapest, Hungary
szadeczky.tamas@gtk.bme.hu

Abstract: This paper discusses the increasing significance of smart water management, within the context of the fourth industrial revolution and the associated cybersecurity risks, particularly in Hungary and Central Europe. By examining the current state of smart water management and analyzing the various cybersecurity threats, this study seeks to raise awareness around the need for enhanced security measures, in this critical sector. The research methodology is primarily based on a through literature review and secondarily, on related data analysis. The paper identifies several cybersecurity challenges and potential solutions for smart water management and finally suggests future research directions, to ensure the safe and sustainable development of this critical infrastructure.

Keywords: Control system security; Critical infrastructure protection; Cybersecurity; Digital transformation; Water utility

1 Introduction

The role of IT in everyday life in the 21st Century is undeniable. Technology makes our lives more convenient and efficient, with less repetitive work. Machines can effectively automate processes. This technological shift leads to higher dependence on IT at the level of the individual, the organization and society. At the level of the individual, the vast majority of tasks now require the use of some kind of a computer. We can do our work from home, connected to the corporate network via a VPN or perhaps, on our tablet, while sitting on the plane. We post our queries to Google search and e-mail our business partners, preferably electronically signed and encrypted. We reach our remote loved ones via teleconferencing or chat

applications. We used these facilities in our daily work, during the peak virus season extensively.

When we think of an organization's dependence on IT, we can associate it with virtually any business record. For example, customer records are now kept in customer relationship management (CRM) systems. Accounting records are also stored on computers. While single-entry accounting, cash book, can still be done on paper, for double-entry accounting this now seems completely anachronistic. Above medium size, it is common for organizations to introduce an integrated ERP system, such as SAP or Microsoft Dynamics, which is used, not only for tracking costs, but also in the production process.

1.1 Industrial Revolutions

The term 'Industrial Revolution' is the best way to describe the automation of production and manufacturing. Such revolutions represented major advances in technology and significantly impacted both economy and society.

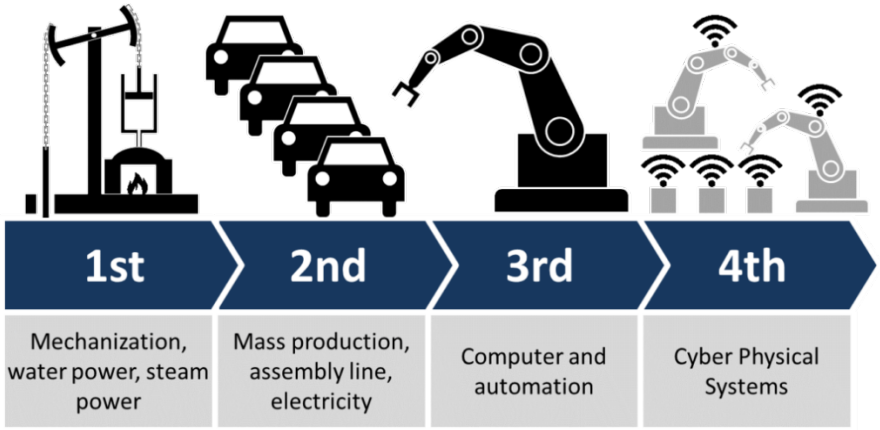

Figure 1
Industrial revolutions [1]

We count the first industrial revolution from the advent of the steam engine. This was strongly linked to the bourgeois revolution and led to the decline of the feudal system throughout Europe. At the technological level, it was characterized by the mechanization of the textile industry, steam-powered ships, steam railways, and the use of steam engines in manufacturing [2]. The second industrial revolution saw the emergence of mass production. One example of this was the Ford car company's mass production of motor vehicles. However, with the development of the iron and steel industry, the use of electricity, the invention of the combustion engine, the chemical industry, agricultural development, and the military industry also underwent significant technical developments. Economically, it was characterized

by the emergence of monopolies and, socially, by the emergence of a middle class and the differentiation of the working class. The third industrial revolution was the advent of computer technology and thus the automation of processes. This involved autonomous regulation and control and some form of centralized coordination, i.e., the industrial control systems (ICS). One of ICS's basic components is the programmable logic controller (PLC), which is in direct contact with sensors and actuators integrated into the process being controlled. These controllers can be interconnected over a suitable network, formerly RS-485, today Industrial Ethernet. Measurement data can be collected, for example, by a supervisory control and data acquisition (SCADA) system, or distributed control can be implemented by distributed control systems (DCS).

The fourth industrial revolution, also referenced as Industry 4.0, or Industrial Internet of Things (IIoT), is currently underway. It is marked by the convergence of digital, physical, and biological systems, as well as the emergence of new technologies such as the Internet of Things (IoT), Artificial Intelligence (AI), robotics, and big data analytics [3]. This industrial revolution is based on these technologies but uses different, modern information technology principles and methods and is a data-driven and networked approach to manufacturing [4]. The IT tools of the 21st Century can collect and analyze previously unimaginable amounts of data, which is what data science or data science is all about. In addition, the massive use of the web developed in the 2000s – making the internet a ubiquitous and quasi-ubiquitous tool for all our lives – is also spilling over into manufacturing and process management. This will make manufacturing even more efficient. At any given moment we can optimize the process in real-time by analyzing millions of data sources, making more efficient use of human resources and becoming more effective at getting the job done. Whether this really is an industrial revolution, with economic and social impact, or just a passing fad that exists only on salespersons' desks can only be determined from a historical perspective. However, what is certain is that the use of IT or, more pejoratively, dependence on IT, is a seemingly unstoppable process.

However, some papers mention the existence of the fifth industrial revolution or Industry 5.0, which is a controversial topic and is not examined in this paper.

Smart water management, as a specialized application of Industry 4.0, involves using advanced digital technologies and data-driven approaches to optimize the planning, operation, and maintenance of water resources and infrastructure and improve the efficiency, sustainability, and resilience of water services and ecosystems. In recent years, smart water management has gained increasing attention and investment from more governments (mostly in well-developed states), utilities, industries, and some research institutions worldwide, driven by the growing challenges of water scarcity, pollution, climate change, and aging infrastructure, as well as the increasing expectations of consumers, regulators, and stakeholders for better quality, affordability, and accountability in water management [5].

However, the emergent reliance on those digital technologies, automation, and connectivity in smart water management also exposes the water sector to new cybersecurity threats, vulnerabilities, and risks, well known in IT security, which can have significant consequences for the safety, security, and reliability of critical water infrastructure and services, as well as for public health, the environment, and the economy. The increasing interdependence and complexity of water systems, combined with the rapid pace of technological innovation, deployment and the evolving nature of cyber threats, make it essential for researchers, practitioners, and policymakers to understand better, assess, and manage the emerging cybersecurity challenges and opportunities in intelligent water management.

1.2 Objectives, Research and Methodology

The paper aims to contribute to the growing body of knowledge and debate on cybersecurity and smart water management by examining the current state of smart water management in Hungary and Central Europe and by analyzing various cybersecurity threats, vulnerabilities, and risks in this critical sector. The paper also proposes a set of research questions and recommendations for future studies and actions to enhance the cybersecurity and resilience of smart water management in the region.

The research questions addressed in this study include:

- What are the drivers for digitalization in the water sector?
- What are the main cybersecurity vulnerabilities in the digitalization of water management in Hungary?
- What protection solutions are currently in place to address these vulnerabilities?
- What future research directions can be identified to strengthen the security of critical water infrastructure in Hungary?

The research methods involve a comprehensive literature review of academic articles, books, reports, and other publications related to the digitalization of water management, cybersecurity issues, and the Hungarian context.

The main objective of this paper is to investigate the cybersecurity issues arising from the digitalization of water management in Hungary and to provide insights and recommendations that may apply to other Central European countries facing similar challenges.

The remainder of the paper is organized as follows: Section 2 provides an overview of the digital transformation of water management, focusing on the key concepts and technologies associated with Water 4.0. Section 3 discusses the main cybersecurity issues and concerns in smart water management. Section 4 is about the known incidents in the field and possible countermeasures, based on the

literature research and analysis. In Section 4, the implications and recommendations are discussed, with a particular emphasis on the Hungarian context and the findings of the research. Finally, Section 5 offers conclusions and recommendations for future research.

2 Smart Water Management

When someone thinks of industry 4.0, they might first associate it with a Tesla factory or some space technology center. However, the fact is that the tools needed to make it happen become available to a wide range of people in the economy and society as their price has fallen dramatically. It is enough to think that millions of users have installed smart home solutions. For an investment of a few thousand dollars, we can automate and voice-control our family home with a dozen sensors and a cloud-based personal assistant. Furthermore, based on the concept of the Smart City, public services in the municipality can be optimized and used more efficiently. One such solution could be the introduction of smart parking, where sensors embedded in the curbside pass data on to the drivers' navigation system and allow them to see the available parking spaces closest to their destination via a mobile app and thus, minimize the time spent searching for a parking space.

2.1 Digitalization Drivers of Water Management

In recent years, more countries are heading towards smart water management, which countries face various water-related challenges and opportunities, such as water scarcity, pollution, climate change, aging infrastructure, and increasing demand for high-quality, affordable, and sustainable water services. The adoption and implementation of smart water management in the Central European region have been influenced and shaped by various factors, including national and international policies, regulations, and initiatives, as well as technological, organizational, and market developments and trends [5].

For water utilities, this may sound utopistic for those who are aware of the current technical and funding situation in Central Europe. Even according to the government, the waterworks infrastructure in Hungary is in a highly depreciated state. According to a presentation by the Deputy Secretary of State for Sustainable Development at the Ministry of Innovation and Technology, Hungary [6], 30% of domestic drinking water pipelines are classified as at-risk and 56% as predominantly at-risk, while 3% of wastewater pipelines are classified as at-risk and 4% as predominantly at-risk. During the research, it was not possible to collect precise information on the degree of automation. In a case study analysis, which was done in the example of the Hungarian city of Baja, no central process control was available at the water supply of a 40000 inhabitant supply area, around the city of Baja. The government

modernized this town's infrastructure in 2012 from an EU fund, which cost 15 million euros, but still, no remote monitoring and intervention capability was built. The only way of monitoring, is that the local control equipment (PLC) sends fault reports to the operators via text messages in all water utilities. If necessary, troubleshooting is carried out with the involvement of the electrician-engineer, technologist or branch manager. Fault rectification is reported to the dispatching service, where the matter is dealt with without any process automation. Due to the deficient level of automation, in fact, the solutions are stuck at the technology level of the 90s and therefore, a significant part of the operators, also think that the issue of Water 4.0 is very far from Hungarian practice. However, incorporating the available extremely low-cost technology makes it possible to achieve much more efficient operating parameters with a low investment volume. Depending on the current IT and plant management infrastructure of a given company, this technology, or elements of it, may become part of daily practice. We should certainly expect technological developments in this direction in the coming years [7].

Despite the progress and potential of smart water management, there are still various barriers and challenges to its broader adoption and impact, such as the lack of awareness, knowledge, and skills about smart water technologies and benefits among decision-makers, stakeholders, and users; the high costs, risks, and uncertainties of investing in smart water projects and assets; the limited availability and accessibility of data, information, and tools for water management decision-making and performance evaluation; the fragmentation, heterogeneity, and compatibility of water governance and management structures, processes, and systems; and the need for more vital collaboration, coordination, and communication between various actors and sectors involved in smart water management.

2.2 Practical Advantages of Water 4.0

In 1994, VITUKI carried out a world survey on how computer technology is used in water and sewerage utilities in different countries [8]. The main areas identified were geographic information system (GIS) applications, process management of operations, water tariff billing and the implementation of expert systems. Even today a small Hungarian water utility is often lagging behind the French practice described two and a half decades ago. However, such development is often not an organic market development but a government decision. For example, in terms of spatial information technology, the process of electronic utility registration and reconciliation is well known in the industry. The authority builds its database by requesting data in electronic form, which significantly simplifies the process of utility planning and operation. Nevertheless, beyond this, given the correct data (e.g., from the smart meters below), web-based knowledge base systems can be built to facilitate the task of civil engineers in the construction of waterworks infrastructure [9].

The complexity of water and wastewater treatment plant management processes requires the use of many sensors and actuators. Digitalization can be used in the following processes:

1) Quantification and optimization of raw water intake
2) Energy efficiency in pump operation
3) Monitoring of reservoir water quality
4) Quantification of water to be treated and analysis of its quality
5) Optimization of the water treatment process (chemical, chlorine gas usealumina dosing).
6) It could be possible to determine the optimum pumping capacity at the point of delivery to the network, monitoring of the pressure of the water delivered to the network
7) Detection of pipe bursts and leaks
8) Real-time assessment of consumer demand
9) Pressure boosting in tower blocks
10) Protection of waterworks infrastructure

Despite having numerous data sources, there are many elements of the hydraulic network which cannot be measured. For those, we might implement virtual sensors to form a real-time dynamic hydraulic model for water loss reduction [10].

The operator can optimize the operation of pumps in pressurized sewerage systems, assess odor effects at sewage treatment plants, and optimize sewage treatment process flow. The utility could optimize the operation of wastewater treatment plants, streamline the sludge treatment process, increase the energy efficiency of biogas use, and measure the quality of treated wastewater before discharge to the intake [11]. Also, sludge storage can be optimized, and in the case of combined sewer systems, any bypassing processes can be scheduled. These processes can be combined with precision irrigation systems [12] to achieve a more efficient and optimally distributed load on the aquifer or water base.

The lowest-hanging fruit of digitalization is the use of smart meters, for which numerous technologies are available in the European market today. The smart water meter can be installed in the maintenance hole or basement, which can communicate with the water utility's systems from a place previously inaccessible by any other radio means, at low speed but with high reliability, using NB-IoT technology provided by the telecommunications operator [13]. Smart meters allow real-time analysis of water consumption patterns and on-demand adjustment of water treatment and supply technology to meet actual demand [14], making the water billing process more efficient than traditional solutions, as the bill can always be based on actual consumption data. The supplier can impose water consumption restrictions on the customer without on-site intervention. Data can be accessed directly from the

operational process in a billing system integrated with the ERP system. Postage costs and bill issuing logistics are minimized by issuing paperless but authentic bills sent in electronically signed PDFs.

The industry calls these solutions Water 4.0, Digital Water, Smart Water, and Internet of Water (IoW). The aforementioned solutions will undoubtedly reform municipal water management's entire infrastructure and operation and support more economically efficient operation of water utilities, customer satisfaction, environmental protection, process optimization, predictable maintenance and regulatory compliance. From a financial point of view, these solutions are characterized by lower operating costs (OPEX), better return on investment and higher revenues, while also increasing the company's economic value. Furthermore, in terms of operational security, higher levels of availability and more predictable human resource management can be achieved.

3 Security Considerations

To gain a deeper understanding of the cybersecurity challenges and opportunities in smart water management, this study did a literature review and secondary data analysis, focusing on academic articles, reports, and case studies related to cybersecurity incidents, trends, and measures in the water sector, both globally and in Hungary and Central Europe. The main findings and insights from this analysis are summarized below.

Digitalization has many positive benefits for individuals, organizations, and society, that we perceive day to day. However, we must not forget the dangers of being vulnerable to technology. In particular, the loss of IT applications and services, the automation of processes, and the difficulties arising from the complexity of systems must be taken into account.

3.1 Cybersecurity Threats

The new cybersecurity threats, vulnerabilities, and risks can significantly affect the safety, security, and reliability of critical water infrastructure and services and public health, the environment, and the economy. Some of the top cybersecurity challenges and threats in smart water management are shown below.

3.1.1 Cyber-Physical Attacks

These are attacks that target physical components and automation processes of water systems, such as pumps, valves, treatment plants, and distribution networks, through the manipulation or disruption of their digital control systems, such as supervisory

control and data acquisition (SCADA) systems, distributed control systems (DCS), programmable logic controllers (PLCs), and remote terminal units (RTUs) [15]. Cyber-physical attacks may cause physical damage, malfunction, or failure of water infrastructure, leading to water service interruptions, contamination, leakage, or flooding, with potentially severe consequences for public health, the environment, and the economy.

3.1.2 Data Breaches

Data breaches are unauthorized access, disclosure, or theft of sensitive or confidential data, such as personal or business-related information, financial transactions, or operational data, stored or transmitted in water management systems, such as customer billing systems, asset management systems, or monitoring and control systems [15]. Data breaches can result in privacy violations, legal consequences, identity theft, financial fraud, or industrial espionage, undermining the trust, reputation and compliance of water utilities and authorities.

3.1.3 Denial of Service (DoS) Attacks

These attacks aim to disrupt, overwhelm, or minimize the availability, performance, or functionality of water management systems, networks, or services, by flooding them with excessive data, requests, or traffic or exploiting their vulnerabilities and weaknesses or design flaws [15]. DoS attacks can cause temporary or permanent loss of access, control, or communication in water management and increase the workload, costs, and delays of system recovery and restoration.

As in the 2003 blackout mentioned in section 3.2, Cybersecurity incidents and trends in the water sector, water utility services can easily be lost in the event of the failure of some other critical infrastructure element. For example, without electricity, the pumps do not operate; therefore, drinking water will not be available. Nevertheless, even the loss of internet service could also be a problem for water utilities with a loss of communication, remote controls and a lack of data acquisition. The cause of these problems can be traced back to system unreliability and natural phenomena, but, most typically, human beings pose the greatest threat. This person could be an external attacker who wants to disrupt the industrial control systems through cybercrime or cyberwarfare. Industrial automation and control systems are also targets of military cyber operations, for example, with Advanced Persistent Threats (APT) [16].

3.1.4 Insider Threats

These are cybersecurity risks that originate from within the organization, such as employees, contractors, or partners, who have legitimate access and knowledge of water management systems, policies, or procedures, but who intentionally or unintentionally (e.g., error) misuse, abuse, or compromise them due to negligence, greed, revenge, or other motives [15]. Insider threats can be challenging to detect,

prevent, and respond to. They often involve exploiting trust, authority, or familiarity and can bypass or circumvent security controls and measures.

Internal staff also poses a threat by negligence or malicious acts. This includes using default passwords in ICS systems, which seems to be a trivial mistake, but still happens frequently because of the fictitious detachment of ICS systems from the Internet.

It is, therefore of paramount importance to support the digitization process with appropriate cybersecurity research and the resulting implementation of necessary information security control measures. IT-related areas need to employ staff with a higher level of cybersecurity expertise, which is generally not available in water and sewerage utilities.

3.1.5 Supply Chain Risks

These are cybersecurity risks that arise from the interdependencies and relationships between different actors and components in the supply chain of water management systems. These actors can be the vendors, suppliers, integrators, operators, and maintainers, who provide, produce, assemble, install, maintain, or update hardware, software, firmware, or services, which may contain vulnerabilities, defects, or backdoors, or which may be subject to tampering, sabotage, or counterfeit [15]. As process operation is highly dependent on the functionality of sensors, actuators, and the control system, the likelihood of downtime due to technical reasons is higher than in traditional systems [17]. The Internet of Things (IoT), the cloud computing infrastructure, and data processing are also major risk-increasing factors [18], which can only be effectively mitigated by a complex, interconnected control system [19]. Moreover, the failure of one system element can easily lead to a complete service outage. Supply chain risks can compromise the security, quality, and reliability of water management systems and create opportunities for attackers to exploit or manipulate these systems through various entry points, stages, or channels.

3.2 Cybersecurity Incidents and Trends in the Water Sector

Several high-profile cybersecurity incidents have been reported in the water sector in recent years, demonstrating the vulnerability and impact of water systems to cyber threats and attacks. An early example is the blackout that affected the northeastern United States and central Canada in August 2003 [20]. The world's second-largest blackout affected 55 million people and meant an almost total blackout for two days and abnormal service levels for two weeks. The exciting thing for us is that the incident started with a software failure at a service provider and the failure in an otherwise redundant system spread to other systems and took out the connected systems as well. For example, in 2016, a water treatment plant in the United States was compromised by a cyber-physical attack, which manipulated the levels of

disinfection chemicals used in the water treatment process, potentially endangering public health and safety [15]. According to the Israeli government, Palestinian hackers attempted to cause the mass chlorine poisoning at an Israeli water plant by switching the chlorine distribution system in April 2020, but the attack was hindered. The Palestinian side denied the accusation [21]. Other sources claim that the Safety Instrumented System (SIS), which is operated alongside the control system, averted the attack. Incidentally, SIS is also a control system design requirement.

Recent examples in the Russia-Ukraine armed conflict showed us multiple examples. During the conflict, many hacker groups have been attacking ICS/SCADA systems on both sides, as shown in Figures 2 and 3. Water utilities are attractive targets, as despite being critical infrastructure, the level of security protection is usually lower than electricity provision.

These incidents show the need for increased vigilance, preparedness, and resilience in the water sector against cybersecurity threats and risks.

The literature review and secondary data analysis revealed several emerging cybersecurity trends in the water sector, such as the growing number of reported cyber incidents, the increasing sophistication and complexity of cyber threats (like usage APTs), the expanding attack surface and vectors due to the proliferation of IoT devices, the evolving regulatory and compliance landscape, and the rising awareness and investment in cybersecurity measures and best practices. These trends indicate that cybersecurity is becoming a critical concern and priority for water utilities, authorities, and stakeholders, as well as for researchers, developers, and providers of smart water technologies and solutions.

Figure 2
Unverifiable information of a successful attack against a water supply SCADA system on 2022-03-07 reported by CyberThreat.Report [22]

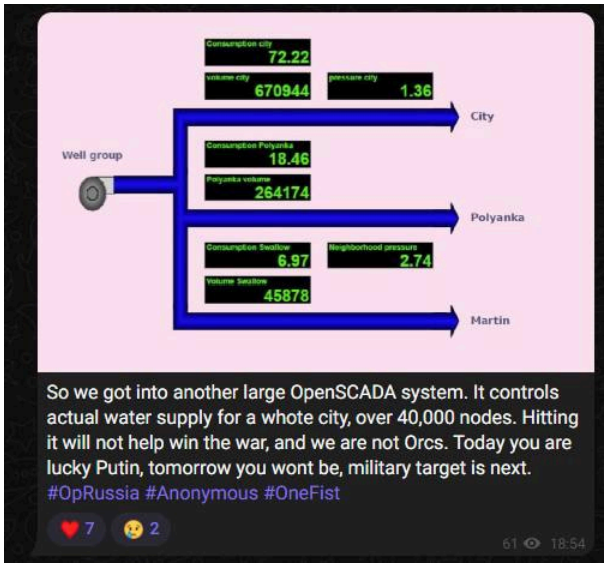

Figure 3
Unverifiable information of a successful attack against a water supply SCADA system on 2022-06-02 reported by CyberThreat.Report [22]

3.3 Cybersecurity Measures in the Water Sector

The research identified several cybersecurity measures and best practices that have been proposed or implemented in the water sector to address and mitigate information security risks and vulnerabilities. These measures include risk assessments, audits, and certifications, which help to identify, evaluate, and prioritize cybersecurity risks and controls; security policies, procedures, and guidelines, which define and communicate cybersecurity roles, responsibilities, and expectations; security training, education, and awareness training, which develop and maintain cybersecurity skills, knowledge, and culture; technical controls, such as firewalls, antivirus, encryption, and access controls, which protect and monitor information systems and networks; and incident response, recovery, and continuity plans, which prepare and guide organizations in handling and recovering from cybersecurity incidents [15]. In order to minimize the risk of cyber-physical attacks, we shall determine the critical objects, to strengthen their protection [23]. Most of the risks and countermeasures in computer networks and systems apply to industrial control systems, but they are biased. Access control, i.e., the restriction of access to authorized subjects, is basic in IT security, but it is more problematic in ICS. The reason of this is the lack of access control capabilities in many ICS devices. Against the insider threats, the solution could be a well-designed access control strategy [24]. The updates patching software flaws in ICS are rare and irregular in contrast to IT systems. Traditionally in ICS, functional safety is a priority over any other aspects. Patching of a running well-configured

industrial control system is apparently a risk from the aspect of functional safety, just like in IT systems. Although, in the IT systems there is a well-designed patch control process with central management (e.g., Windows Server Update Services, WSUS), rollback functions, test systems and patch piloting groups. Even software development and operation practices, like Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), Enhanced Mitigation Experience Toolkit (EMET), and Control Flow Enforcement (CFE) might be applied to minimize the risk of exploiting software vulnerabilities. [25] In the ICS systems, those methods and tools do not exist. Furthermore, in time-critical applications, neither a reboot is allowed. Network-based protection is by default based on air gaps, thus physical disconnection of networks. Historically there was no direct connection between the IT network and the operation technology (OT) network, which handles the ICT systems. Therefore, the network protection was unnecessary. The network-related problems arise when a previously air-gapped network is not just IT-network, but Internet-connected, because of industry 4.0 features [26]. Also, IT network security technologies might be only partly usable on the OT network. As functions are mostly time-critical, there is no delay allowed, so stateful packet inspection or application-level firewalls might not be used. Intrusion Prevention Systems (IPS) might disrupt regular communication when dropping packets, so they might be used with special caution.

4 Discussion: Implications and Recommendations

Based on the findings and insights from the literature review and secondary data analysis, as well as the context and conditions of Hungary and Central Europe, the following implications and recommendations can be derived for enhancing the cybersecurity and resilience of smart water management on the national level, or even in the region:

4.1 Strategies, Policies, Governance and Cooperation

Governments and authorities in Hungary and Central Europe should develop and implement comprehensive, coherent, and coordinated cybersecurity strategies and policies (or apply the current ones to the water sector), which address the specific risks, challenges, and opportunities of smart water management, and which are aligned with and supported by international, national, and sectoral cybersecurity frameworks, standards, and guidelines.

Some components of municipal water management are de facto critical infrastructures in Hungary, as specified in Act CLXVI of 2012 on the Identification, Designation and Protection of Critical Systems and Facilities [27] and in Government Decree 541/2013 (XII. 30.) on the Critical Water Management System Elements and Water Facilities

in Hungary [28]. Therefore, water supply is in the public interest, and wastewater collection and treatment, as a public health issue, shall also be continuously provided.

Freshwater is a strategic issue, and in many geographical regions (e.g., Israel, Tibet, Kashmir, Nile Valley), the use of limited freshwater resources is currently causing armed conflicts [29]. With water scarcity, the country is highly vulnerable to upstream countries if it does not have adequate storage capacity. This is a current problem in most of the Central European countries, mainly for social reasons, i.e., land use. Storage is important from both an economic (protection costs, utilization) and a strategic (indirect security risks) point of view [30].

Water utilities, authorities, and stakeholders in Hungary and Central Europe should establish and strengthen their cybersecurity governance and capacity by assigning clear organizational roles, responsibilities, and resources for cybersecurity management, integrating cybersecurity considerations into their organizational culture, processes, and systems, and by engaging in continuous learning, improvement, and innovation in cybersecurity practices and technologies [15].

Governments, utilities, industries, and research institutions in Hungary and Central Europe should promote and facilitate cybersecurity collaboration and information sharing in the water sector through various mechanisms and platforms, such as partnerships, networks, conferences, workshops, and publications, which enable the exchange of knowledge, experience, and intelligence about cybersecurity threats, vulnerabilities, incidents, and countermeasures, as well as the identification and dissemination of best practices and lessons learned in cybersecurity management and research [31].

Professional processes were initiated to increase legislative control concerning the electricity supply and distribution infrastructure, partly because of previous incidents and partly because of the higher level of IT exposure. This legislation started a decade ago in the United States, but just in recent years in Europe. However, as it is coupled with legislative intent, we can expect an increased resilience of the sector to cyberattacks [32].

As this is no longer the sole problem of countries, the European Union and NATO are dealing with this problem with different approaches. NATO addresses the strategic aspect and urges the preparation of member states for cyber operations as a distinct dimension of warfare [33]The EU deals more with the operative direction: in the Cybersecurity Act [34], one exact application is the information security-related certification of ICS components, as written in the Recommendations for the Implementation of the Industrial Automation & Control Systems Components Cybersecurity Certification Scheme (ICCS) by the European Commission, Joint Research Centre [35].

Since the digitalization described above is still in its infancy in Central Europe, it is advisable to use a Western European model for studies in this direction. A good example can be the German market, which also has many small public utilities.

German regulators are already addressing the cyber security of water utilities, with the KRITIS strategy and the resulting legislation setting out cyber security responsibilities for the entire German critical infrastructure [36].

In Hungary, a pioneering initiative is the SeConSys, a group of professionals and regulators working together on the cyber security of critical energy infrastructure. The Cybersecurity Handbook on Industrial Control Systems for Electricity [37], produced within this framework, is a missing piece of work that provides guidance for developing protection at the regulatory, design, and operational levels. In addition, case studies can be found in the Hungarian academic literature on the design of adequate cyber protection in the power sector [38].

4.2 Research, Development, and Innovation

Governments, public utilities, industries, and research institutions in Hungary and Central Europe should encourage and support cybersecurity research, development, and innovation in the water sector by funding (or applying to) multidisciplinary and collaborative research projects, programs, and centers, which focus on the design, evaluation, and deployment of secure, resilient, and trustworthy smart water technologies, systems, and services, as well as on the development and application of advanced cybersecurity methods, tools, and techniques, such as risk assessment, threat modeling, vulnerability analysis, intrusion detection, and incident response [15].

Although lagging behind, the maturity of water utilities' management and IT systems and the resulting cybersecurity risks will follow the same path as that of the electricity sector. The advance of digitalization in this area is inevitable, which also involves the emergence of new types of risks. Furthermore, the current unstable geopolitical situation makes critical infrastructure protection even more important. In order to prepare operators, legislators, and regulators for the challenges involved, it is essential to set up European professional and scientific initiatives to research the issue extensively.

University research has also started in this area. For example, the CYBERWATER NATO Advanced Research Workshop conducted research under the leadership of Harsha Ratnaweera, professor at the Norwegian University of Life Sciences [39].

Conclusions

This paper analyzed the increasing importance of smart water management, within the context of the fourth industrial revolution and its associated cybersecurity risks, particularly in Hungary and Central Europe. By examining the current state of smart water management and analyzing various cybersecurity threats, vulnerabilities, and risks in this critical sector, the study has sought to raise awareness about the need for enhanced security measures and practices in smart water management, as well as to provide a basis and course for future research.

The research was limited to the literature and the sources listed in the references. Even the application example, was based on one water utility, for which, the author had operational details. A broader research with more utilities (including large ones) could strengthen the findings.

Future research directions in cybersecurity and smart water management may include the following:

- Conducting empirical and comparative studies on the effectiveness and efficiency of different cybersecurity measures, practices, and technologies in the water sector.
- Exploring the ethical, legal, and social implications and challenges of cybersecurity and privacy in smart water management, such as, data ownership, consent and accountability.

By addressing these and other research questions and gaps, the academic and professional communities can contribute to the advancement of knowledge and practice, in cybersecurity and smart water management. This will help to ensure that the benefits and opportunities of digital transformation and innovation, in the water supply sector, are realized and sustained, without compromising the security, resilience and trust of critical water infrastructure/services, in Hungary, Central Europe and beyond.

Acknowledgement

The author would like to thank the two anonymous reviewers for their valuable feedback and suggestions, which helped to improve and extend the paper.

The research was supported by the Hungarian Academy of Sciences Bolyai János Research Scholarship (Grant No. BO/00372/22/9).

This research was supported by the ERDF project “CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence” (No. CZ.02.1.01 / 0.0 / 0.0 / 16_019 / 0000822).

References

[1] C. Roser, “AllAboutLean.com,” 2021. https://www.allaboutlean.com/industry-4-0/industry-4-0-2/ (accessed May 06, 2023).

[2] D. Wienecke-Janz, *Die Chronik der Deutschen (The Chronicle of the Germans)*. Gütersloh-Munich: Chronik Verlag, 2007.

[3] K. Schwab, *The Fourth Industrial Revolution*. Crown Business, 2017.

[4] H. Lasi, P. Fettke, H.-G. Kemper, T. Feld, and M. Hoffmann, “Industry 4.0,” *Business & Information Systems Engineering*, Vol. 6, No. 4, pp. 239–242, 2014, doi: 10.1007/s12599-014-0334-4.

[5] A. D. Gupta, P. Pandey, A. Feijóo, Z. M. Yaseen, and N. D. Bokde, "Smart Water Technology for Efficient Water Resource Management: A Review," *Energies (Basel)*, Vol. 13, No. 23, p. 6268, Nov. 2020, doi: 10.3390/en13236268.

[6] M. Makai, "Wastewater sector issues after the KEHOP, before the end of the derogation. Strengthening higher education in water management in the framework of smart specialisation," Decentralized Wastewater Treatment Conference at National University of Public Service, Faculty of Water Sciences, Baja, Mar. 21, 2019.

[7] S. R. Krishnan *et al.*, "Smart Water Resource Management Using Artificial Intelligence—A Review," *Sustainability*, Vol. 14, No. 20, p. 13384, Oct. 2022, doi: 10.3390/su142013384.

[8] J. Deri, *Computerised technologies for water and sewerage plants (in Hungarian: Számítógépesített technológiák víz- és csatornaműveknél)*. Budapest: Vituki Innosystem, 1994.

[9] R. A. Stewart, R. Willis, D. Giurco, K. Panuwatwanich, and G. Capati, "Web-based knowledge management system: linking smart metering to the future of urban water planning," *Australian Planner*, Vol. 47, No. 2, pp. 66–74, Jun. 2010, doi: 10.1080/07293681003767769.

[10] M. S. Osman, A. M. Abu-Mahfouz, and P. R. Page, "A Survey on Data Imputation Techniques: Water Distribution System as a Use Case," *IEEE Access*, Vol. 6, pp. 63279–63291, 2018, doi: 10.1109/ACCESS.2018.2877269.

[11] M. Patziger, *Efficient operation of medium and small wastewater treatment plants (in Hungarian: Közepes és kis szennyvíztisztító telepek hatékony üzemeltetése)*. Budapest: Hungarian Water Utility Association, 2018.

[12] S. Takács, T. Bíró, L. Helyes, and Z. Pék, "Variable rate precision irrigation technology for deficit irrigation of processing tomato," Vol. 68, pp. 234–244, 2019, doi: 10.1002/ird.2299.

[13] S. Alvisi *et al.*, "Wireless Middleware Solutions for Smart Water Metering," *Sensors*, Vol. 19, No. 8, p. 1853, Apr. 2019, doi: 10.3390/s19081853.

[14] S. D. B. Moraes, C. Langhi, and M. Crivelaro, "How an existing telecommunications network can support the deployment of smart meters in a water utility?," *Independent Journal of Management & Production*, Vol. 6, No. 4, 2015, doi: 10.14807/ijmp.v6i4.351.

[15] Y. Cherdantseva *et al.*, "A review of cyber security risk assessment methods for SCADA systems," *Comput Secur*, Vol. 56, pp. 1–27, Feb. 2016, doi: 10.1016/J.COSE.2015.09.009.

[16] W. Steingartner and D. Galinec, "Cyber Threats and Cyber Deception in Hybrid Warfare," *Acta Polytechnica Hungarica*, Vol. 18, No. 3, pp. 25–45, 2021, doi: 10.12700/APH.18.3.2021.3.2.

[17] M. Moy de Vitry, M. Y. Schneider, O. Wani, L. Manny, J. P. Leitão, and S. Eggimann, "Smart urban water systems: what could possibly go wrong?," *Environmental Research Letters*, Vol. 14, No. 8, p. 081001, Aug. 2019, doi: 10.1088/1748-9326/ab3761.

[18] R. O. Andrade, S. G. Yoo, L. Tello-Oquendo, and I. Ortiz-Garcés, "A Comprehensive Study of the IoT Cybersecurity in Smart Cities," *IEEE Access*, Vol. 8, pp. 228922–228941, 2020, doi: 10.1109/ACCESS.2020.3046442.

[19] A. Toth, "Cloud of Things Security Challenges and Solutions; Cloud of Things Security Challenges and Solutions," in *Communication and Information Technologies (KIT)*, Vysoke Tatry, Slovakia, 2021, pp. 1–6. doi: 10.1109/KIT52904.2021.9583760.

[20] M. Tabibzadeh and S. Mirzaei, "A system-oriented framework for risk and resiliency analysis of power blackouts," in *Proceedings of the 2016 Industrial and Systems Engineering Research Conference, ISERC 2016*, 2020, pp. 582–587.

[21] "Iranian Cyberattack Aimed to Raise Chlorine Level in Israeli Water, Report Says," *Haaretz*, Jun. 01, 2020. Accessed: Jun. 04, 2022. [Online]. Available: https://www.haaretz.com/israel-news/iranian-cyberattack-aimed-to-raise-chlorine-level-in-israeli-water-report-says-1.8886235

[22] CyEx Kft, "Cyberthreat.Report closed Facebook group," Mar. 07, 2022. https://www.facebook.com/groups/469363908185824 (accessed May 08, 2023).

[23] A. Massel and D. Gaskova, "Identification of Critical Objects in Reliance on Cyber Threats in the Energy Sector," *Acta Polytechnica Hungarica*, Vol. 17, No. 8, pp. 61–73, 2020, doi: 10.12700/APH.17.8.2020.8.5.

[24] B. Leander, A. Čaušević, H. Hansson, and T. Lindström, "Toward an Ideal Access Control Strategy for Industry 4.0 Manufacturing Systems," *IEEE Access*, Vol. 9, pp. 114037–114050, 2021, doi: 10.1109/ACCESS.2021.3104649.

[25] L. Erdődi and A. Jøsang, "Exploitation vs. Prevention: The ongoing saga of software vulnerabilities," *Acta Polytechnica Hungarica*, Vol. 17, No. 7, pp. 199–218, 2020, doi: 10.12700/APH.17.7.2020.7.11.

[26] E. D. Knapp and J. T. Langill, *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. Waltham, MA: Syngress, 2015.

[27] Hungarian Parliament, *Act on Identification, Designation and Protection of Critical Systems and Facilities*. 2012. Accessed: May 08, 2023. [Online]. Available: https://njt.hu/eli/TV/2012/166

[28] Hungarian Government, *Government Decree 541/2013 (XII. 30.) on the Critical Water Management System Elements and Water Facilities*. Hungary, 2013.

[29] J. Padányi, "Water conflicts," *Military Science*, Vol. 25, No. e, pp. 272–284, 2015.

[30] K. Ligetvári, "Water security problems in hungary in comparison with EU and world tendencies," *Military Science*, Vol. 23, No. 1, pp. 4–13, 2013.

[31] Z. Bederna and Z. Rajnai, "Analysis of the cybersecurity ecosystem in the European Union," *International Cybersecurity Law Review*, Vol. 3, No. 1, pp. 35–49, Jun. 2022, doi: 10.1365/s43439-022-00048-9.

[32] E. D. Knapp and R. Samani, *Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure*. Waltham, MA: Syngress, 2013.

[33] P. Bányász, C. Krasznay, and A. Tóth, "NATO's cybersecurity politics (in Hungarian: A NATO kibervédelmi szakpolitikája)," in *Today's NATO: Status and roles of the alliance (in Hungarian: A mai NATO: A szövetség helyzete és feladatai)*, Z. Szenes, Ed., Budapest: HM Zrínyi, 2021, pp. 130–149.

[34] European Parliament and the Council, *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)*. European Union, 2019. Accessed: May 08, 2023. [Online]. Available: http://data.europa.eu/eli/reg/2019/881/oj

[35] P. ; Theron *et al.*, "Recommendations for the Implementation of the Industrial Automation & Control Systems Components Cybersecurity Certification Scheme (ICCS)," Ispra, 2020. Accessed: Oct. 01, 2022. [Online]. Available: https://ec.europa.eu/jrc

[36] J. Fettig and M. Oldenburg, "Overview: Preparedness in the Water Supply and the Sanitation and Sewerage Sectors in Germany and Europe," in *Physical and Cyber Safety in Critical Water Infrastructure*, H. Ratnaweera and O. A. Pivovarov, Eds., Amsterdam: IOS Press, 2019.

[37] I. Angyal *et al.*, *Cybersecurity handbook on industrial control systems for electricity service provision*, 2nd ed. Budapest: National Cyber Defense

Institute of the National Security Service, 2021. [Online]. Available: https://m2.mtmt.hu/api/publication/32462794

[38] C. Krasznay and M. Danyek, "Protecting the National Electricity System in the Cyberspace – A Case Study," in *Information- and cybersecurity*, B. Török, Ed., Budapest: Ludovika Egyetemi Kiadó, 2020, pp. 149–163.

[39] NATO, "NATO Newsroom," 2018. https://www.nato.int/cps/en/natohq/news_157806.htm (accessed May 06, 2023).