Desalination and Water Treatment
www.deswater.com
doi: 10.5004/dwt.2022.28917

274 (2022) 1–6
October

Intelligent infrastructure (critical) of the water supply network for collective water supply systems – a case study

Piotr Małka[a,*], Krzysztof Gaska[b], Ewa Wysowska[c], Kazimierz Kudlik[d], Józef Ciuła[e]

[a]*AGH University of Science and Technology in Cracow, Poland, email: malka@agh.edu.pl, ORCID: 0000-0002-1377-6460*
[b]*Sądeckie Wodociągi Spółka z o.o. in Nowy Sącz, Silesian University of Technology in Gliwice, Poland, email: krzysztof.gaska@polsl.pl, ORCID: 0000-0002-9369-6144*
[c]*Sądeckie Wodociągi Spółka z o.o. in Nowy Sącz, AGH University of Science and Technology in Cracow, Poland, email: ewa.wysowska@swns.pl, ORCID: 0000-0002-9239-0477*
[d]*Sądeckie Wodociągi Spółka z o.o. in Nowy Sącz, Poland, email: kazimierz.kudlik@swns.pl, ORCID: 0000-0001-8107-1916*
[e]*State University of Applied Sciences in Nowy Sącz, Poland, email: jciula@pwsz-ns.edu.pl, ORCID: 0000-0002-9184-9282*

Received 21 April 2022; Accepted 29 August 2022

ABSTRACT

The article presents a method of solving a research and technological problem related to the optimization of data transmission and stabilization of interactions between the components of the information and communication technologies and hardware systems managing the process of predictive diagnostics of machines and devices as well as inferential control of actuators of the critical water supply network infrastructure. Building an intelligent infrastructure of the water production and distribution system requires the use of highly efficient IT systems that enable complex computational processes, including a dynamic hydraulic model of the network, as well as simulation of changes in process and technological parameters in real time. The conducted analyses have shown that the optimal approach is to combine virtual solutions with solutions based on physical workstations. An important consideration was to adjust system to the requirements of the Cybersecurity Act along with the selection of appropriate equipment enabling the implementation of procedures ensuring network security and safe access to the resources of the intelligent water supply system.

Keywords: Critical infrastructure; Cybersecurity of the ICT system; Intelligent water supply network

1. Introduction

Water intakes and elements of collective water distribution systems used by water supply companies are objects of the country's critical infrastructure [1]. They are critical elements for the security and functioning of society. The constantly changing environment, new threats and legal requirements, including the quality security of the services provided and cybersecurity, generate the need to implement modern and intelligent IT and network systems based on the best available techniques (BAT). Intelligent water supply infrastructure for collective water supply systems requires the use of such systems.

The currently operating water supply systems are not only technical facilities (intakes, water supply networks, water pumping stations), but in fact they are networks of field facilities (linear engineering facilities, hydrophore facilities, water intakes and water treatment plants) connected by extensive and complex industrial IT networks managing the indicated facilities and data exchange between them. Both the processes of water intake, water treatment and its distribution are currently based on IT systems for supervision

* Corresponding author.

Presented at the 2nd International Conference on Critical Infrastructure of Cities (CIC 2021), 6–8 October 2021, Rytro, Poland

and data acquisition of SCADA type. The operation of engineering facilities based on advanced IT and technological solutions increases their reliability and energy efficiency [2–4], while being an important element of the so-called Smart City.

Implementing the idea of the so-called smart cities resulting from the development of ICT (Information and Communication Technologies) brings with it challenges in the field of model solutions of the critical infrastructure [5]. One of the particularly important aspects of smart cities development is the maintenance of cyber security, especially of critical infrastructure facilities. The development of smart technologies in recent years has increased the frequency of cyber-physical attacks [6,7]. Network objects, including linear ones, multiply the need for control due to significant distances. Water supply network systems create industrial systems and, as confirmed by global data, they are one of the main targets of cyber-attacks [8,9]. They are particularly vulnerable to compromising their safety, while threatening the stability of the city as an organism.

So far, one of the first intelligent elements were teletechnical, energy and gas networks. The implementation of prediction systems in water systems is a great challenge due to many variables [10]. As indicated in the literature, the implementation of intelligent systems for collective water supply allows increasing the speed of decision-making, especially in emergency and extraordinary situations, which is critical from the point of view of the security and responsibility of the indicated supply networks [11]. As indicated by the results of scientific research and simulations [12,13] partial solutions based on models are more often suggested for implementation, in particular for monitoring elements of water supply networks and safety as well as reducing their energy consumption [14,15].

The indicated comprehensive system of intelligent water supply is implemented as part of the research and development project entitled Technologically advanced, intelligent infrastructure (critical) of the water supply network for collective water supply systems (POIR.04.01.04-00-0041/18) co-financed by the European Union from the European Regional Development Fund under the Intelligent Development Program 2014–2020. The project is carried out as part of the competition of the National Centre for Research and Development: "Application projects" by the Consortium of the Cracow University of Technology and the Sądeckie Wodociągi Sp. z o.o. in Poland. The research concerns the development and implementation of a mathematical model of an intelligent water supply network, through the implementation of control system models and the selection of appropriate algorithms for neural and genetic networks, to increase the reliability and safety of water preparation and distribution systems.

The implemented project is a response to new challenges in the field of continuous improvement of the reliability of the engineering system, including the reliability of water supply. Changing legal regulations, including those relating to the safety of the quantity and quality of water directed to recipients through collective supply systems [16], force the operators of these facilities to a new, even research and comprehensive approach to the management of the indicated infrastructure. The new EU Drinking Water Directive [17], currently being implemented, in addition to adding new parameters required for quality monitoring of drinking water, points to the need to improve access to water for all people, reduce water losses and facilitate access to water quality information and billing data. Research for the development of automation and computerization of water intake and distribution processes enable the increase in the optimization of these processes and constitute a response to the EU requirements.

A very important element that was focused on when building an IT system that supports the tasks performed under the project is to build a safe, secure and reliable IT/OT network. All tasks carried out under this project were correlated with the requirements of the Cybersecurity Act [18] and the current global guidelines in this aspect [19]. The speed of reaction in the event of cybersecurity incidents and the use of all possible elements of prevention and protection that can be implemented is one of the main aspects of control and security, as indicated by the Act on cybersecurity. The key issue is a properly developed communication system, especially in the event of a crisis. As emphasized by other authors, the assessment of the risk level and control of industrial systems is difficult; especially taking into account their territorial dispersion, frequently used worn-out water supply networks and problems with water pressure [8,13].

The solutions proposed by the authors are compatible with the results of the analysis of global researchers. As indicated, among others, by Won Lee et al. [20], intelligent water infrastructure solutions equipped with a two-way communication system play a key role in the provision of drinking water. Research conducted in the form of a case study by Ramos et al. [21] has demonstrated a number of benefits of implementing smart water networks in an urban structure. The authors emphasized in particular the increase in energy efficiency and savings in energy consumption because of reducing water losses, and thus reducing the CO_2 equivalent emitted to the environment. Gaska and Generowicz [22] also indicated the impact of the use of algorithmic models based on SCADA control systems in critical infrastructure facilities on their energy efficiency. The team led by Yasin et al. [23] likewise drew attention to the reduction of water losses and water wastage because of the use of extensive IT solutions. Vinod Kumar et al. [24] indicated that implementation of the so-called Smart Water Management allows to automatically solve problems and have real-time data. The research of strengths, weaknesses, opportunities, and threats (SWOT) carried out on the example of the Kozhikode Metropolitan Area (India) has just indicated the intelligent water supply system as a solution to the problems related to water supply to the metropolitan society.

The developing world, especially in the era of remote work and access to critical infrastructure resources, requires the use of solutions ensuring both the security and stability of operating systems and the security of process and project data protection, as well as the users with access to resources. The article presents a solution to the research and technological problem related to the optimization of data transmission and stabilization of interactions between the

components of the ICT system and hardware system managing the process of predictive diagnostics of machines and devices and inferential control of executive devices of the critical water supply network infrastructure, including in particular:

1. The results of the analysis and selection of IT systems supporting the processes implementing tasks related to the construction of intelligent water supply network infrastructure for:
   - industrial information systems
   - industrial network security systems
2. Results of selection along with technical verification of communication methods used for communication between individual elements of the system being built
3. Results of the selection of network and security system solutions along with verification at the test facility.

2. Materials and methods

2.1. Analysis of industrial information systems

A working system of collective water supply, supplying over 100,000 recipients, was selected as a research facility on a technical (test) scale. It was required to isolate the infrastructure elements necessary for the implementation of research works and industrial systems in order to ensure uninterrupted and safe water distribution and monitoring. As part of the research, an analysis was carried out to enable the selection of an optimal database solution that will be used to record measurement and technological data. The adopted solutions will ultimately use an industrial Historian database. The collected data correspond to the time series with a given measurement interval [25]. These types of solutions are characterized by the optimization of the speed of operation and the reliability of data recording. The second element is compatibility with production solutions in a selected water supply company. The next stage of work related to the project was the appropriate design of communication between the individual components of the system being built. All its elements must be able to communicate in such a way to enable data exchange with both predictive packages, a mathematical model, a database, and other elements of the designed and built system. As a result of the simulations and analyses, the minimum requirements to be met by the constructed platform were developed:

a) Ensuring connection with other IT systems through standard mechanisms such as ODBC, Web Services, Oracle Gateway, DBLink, OPC UA, OLE DB, ADO, ADO.NET
b) Export and import (exchange) of data to/from systems in various formats, at least (txt, xls, csv)
c) On-line and off-line data exchange with any "server" and "file" databases using standard OPC, OPC UA, ODBC, OLE DB, ADO, ADO.NET drivers. Databases can be relational and non-relational (flat, object-oriented) (especially Oracle, MS-SGL, Access, DBF, Text, XML, Excel)
d) On-line data exchange through system mechanisms, interfaces or universal mechanisms (OPC, OPC UA, ODBC, OLE DB, ADO, ADO.NET.) with systems based on relational and object-oriented databases
e) Reading data from external SCADA systems through the OPC UA standard or through an indirect database (based on OPC)
f) Data exchange possible with the use of Web Services
g) The connection of the systems must take place through a SCADA type system (dedicated to the management of network and line facilities in particular), which will be built as part of the project and will ultimately be used for the exchange, archiving and processing of measurement data necessary for the implementation of the project. Subsequent works necessary to build an innovative system were related to the selection of an appropriate and efficient algorithm for data processing and analysis that would enable the installation, configuration and commissioning of measurement and computing systems. The conducted analyses showed that it is reasonable to use virtual operating systems on which components of the prediction system, programs such as Matlab, Databases, SCADA, Historian and various types of web services are installed. The advantage of the adopted solution is the possibility of quick reconfiguration of the systems built, taking into account research works and the use of efficient, fast and effective solutions. Another argument for this type of solution is the possibility of quick archiving and processing of both measurement data and the operating systems themselves. To display visualization screens, graphic terminals were used to connect a multi-monitor station to display synoptic visualization tables and screens of calculation stations of a hydraulic model and a predictive system.

2.2. Selection of industrial network security systems

The IT infrastructure requires the construction of an appropriate, efficient and secure IT/OT network. The changing geopolitical conditions and the requirements that are imposed on the systems currently being built using IT and OT networks force the use of appropriate hardware and software devices ensuring the security of the devices themselves, software, process data and know-how data that will be created during the project and during its implementation and operation period. An additional factor that forces the use of such solutions is the Act on the national cybersecurity system [16] introduced in Poland. In order to ensure an appropriate level of security, independent elements have been designed to properly secure access to resources from the external internet network and to separate the newly built system from the production system that performs the basic activities of the water supply company. One of the designed security elements will be used to exchange data with other distributed systems supplying data to perform the tasks of the prediction system and will make resources available only to users who have access through appropriately selected security and authentication tools and solutions. The designed security system will also be used to secure the network connection of the newly designed and built system with the existing master production system. The security system must meet several very important functionalities, such as:

a) Ensuring the possibility of building a minimum of 2 separate (physical or logical) system instances in the

scope of: Routing, Firewall, IPSec VPN, Antivirus, IPS, Application Control.

b) IPv4 and IPv6 support in terms of:
   - Firewall
   - Application layer protection
   - Dynamic routing protocols.

2.3. Analysis and optimization of data transmission methods and interactions between individual elements of the ICT system

The analyses of the systems used and designed in the area of the water supply company that require integration with the prediction system have shown that it is necessary to use various communication protocols. These protocols support data exchange between automation and control systems SCADA, PLC controllers, HMI operator panels, drives and converters used for control pumps and actuators as well as other programmable elements necessary for the implementation of the project. Standard protocols provided by equipment manufacturers were proposed for data exchange. In the opinion of the authors, such a solution will allow to maintain an appropriate level of security and reliability of the obtained data. Creating new dedicated communication protocols written for project needs may in the future cause a number of problems with their mutual compatibility and copyright. Therefore, it becomes justified to use solutions commercially available on the market within research and development projects. The main protocols planned to be used for data exchange with automation and control systems will be, among others, Modbus TCP, Modbus RTU, Ethernet/IP, GE Ethernet, GE SNP, ProfiBus and ProfiNet.

Another element for which it is necessary to properly select and configure communication protocols are systems supporting modeling and prediction as well as cooperating and supporting systems, which include geographic information system (GIS) and sales systems. In the case of a computing application (for modeling and prediction), a protocol based on OPC UA solutions will be used to exchange data between SCADA systems and the automation system. It is an open protocol that allows integration into a large number of different production systems. This protocol is object-oriented, which means that it can be used for many purposes in the process layer and provides support for advanced data structures and a flexible data model. Service-oriented OPC UA provides better support in the field of integration on various platforms, which in the case of the system being built is an important feature; enables better access, security and integrity of the transmitted process data. In the case of building a system under the project, the use of this solution guarantees the reliability and certainty of data exchange, enabling integration with other systems in the event of commercialization of the solution.

For other cooperating systems, it was proposed to use available solutions based on universal database protocols. On-line and off-line data exchange with both "server" and "file" databases will be performed using standard ODBC, OLE DB, ADO, ADO.NET drivers. In the case of using such protocols, it is necessary to prepare appropriate intermediate tables for data exchange with the SCADA and computing system. The tables have been designed in such a way as to minimize the amount of data flowing between individual system components and the load on the operating systems that support these databases.

2.4. Analysis and selection of operating system solutions

The research also included the preparation of the concept, design, implementation and possible configurations of test stands. The developed scheme assumes that the monitoring systems and executive control algorithms will be installed on computers equipped with virtualization mechanisms and supporting the work of industrial databases. In the case of such a solution, it is necessary to properly prepare and test the adopted assumptions, along with performance and hardware tests. The main element of the system necessary for proper operation is efficient and fast operation of databases, taking into account quick access to data and the possibility of reconfiguring tables used to read individual variables. A laboratory system consisting of servers connected with appropriate network connections and equipped with virtualization software based on the Microsoft Hyper-V solution was built for testing purposes. In the case of this solution, the standards adopted in the company were applied, so that the system is compatible with the existing solutions and gives the possibility of moving and migrating virtual machines to other servers used in the company in the future. The indicated solution will be used in emergency and crisis situations in order to obtain maximum reliability and continuity of the system being built. An important element included in the developed concept is to ensure appropriate redundant network connections using fiber optic links with appropriate network infrastructure devices: switches and routers. Fig. 1 is a schematic diagram of a conceptual test setup.

The analysis and verifications of the conceptual system have shown that one of the main sensitive elements for the SCADA and prediction system is the proper provision of network connections. Devices with a minimum bandwidth of 1 GB/s using fiber-optic connectivity and edge devices with a throughput of up to 700 Mbps should be used and applied. Another important element that should be taken into account when implementing a production system is the appropriate construction and optimization of tables and views used to exchange data between individual elements of the system being built.

3. Results and discussion

As part of the research, a system ensuring network traffic safety using UTM and firewall solutions was developed. Such a solution will allow for full control of network traffic and control over the users connecting to the system and the data that is sent within the individual components of the system being built and the data downloaded and sent to the external systems of the water supply company infrastructure. A system consisting of a UTM system and a firewall, which will control two-way traffic, has also been designed. UTM, together with the firewall, will be responsible for communication with external systems located outside the infrastructure of the water supply company and will provide access for users using the intelligent infrastructure system by properly securing data transmission

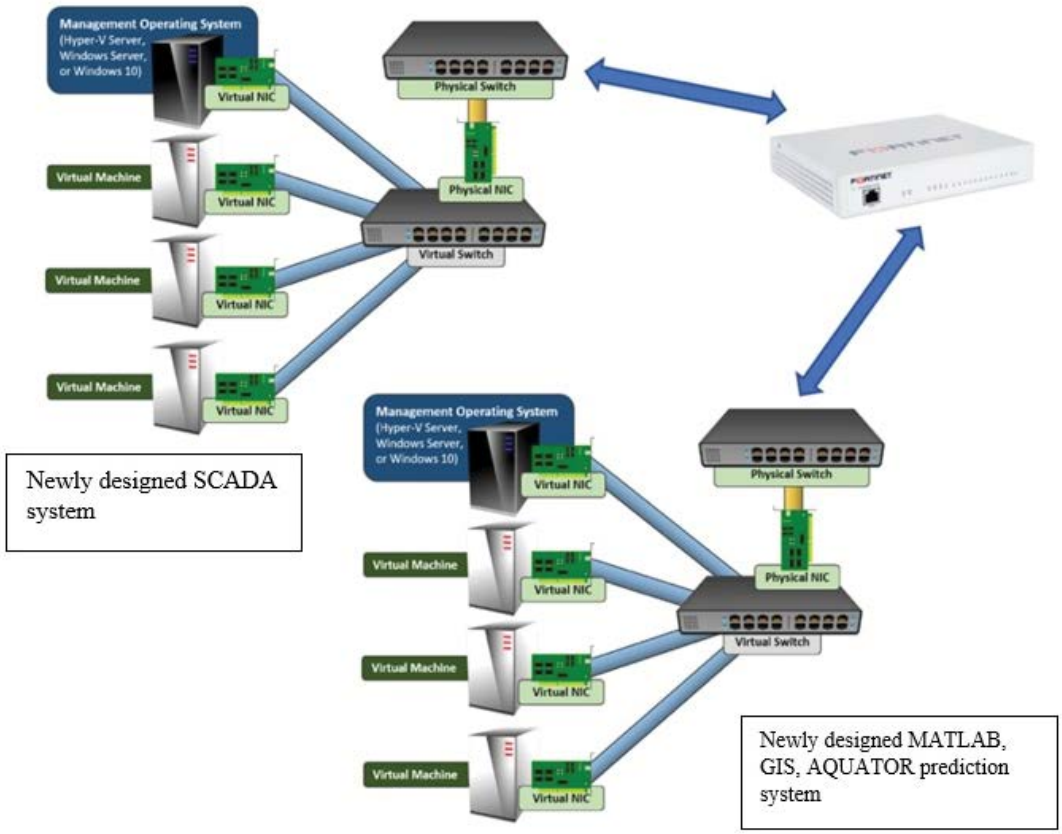

Fig. 1. Diagram of the test system for the verification of the system platform – own study.

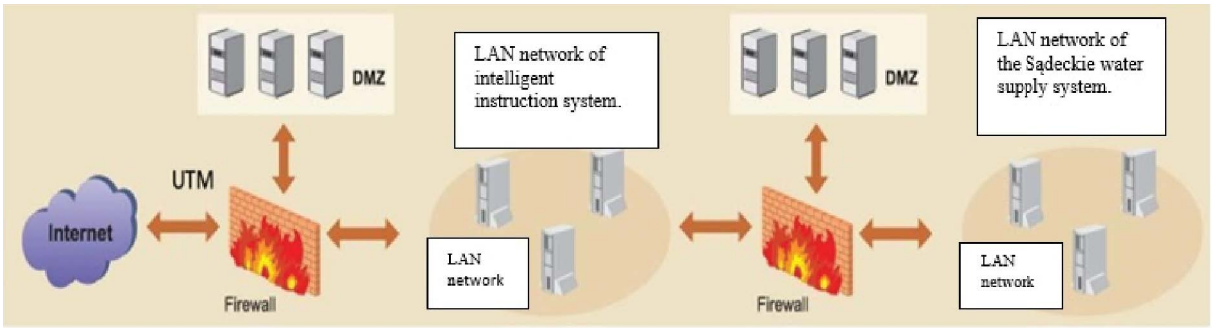

Fig. 2. Diagram of the network security system and cybersecurity of the system being built – own study.

with an encrypted VPN protocol. The second firewall will support and ensure data security between the newly built network infrastructure and the existing network used by the water supply company. This solution will ensure control over the flow of data between systems and ensure the security of the most important system, which is the company's production system. Fig. 2 shows a conceptual design of a network security system.

The implemented solution based on UTM, through the mechanisms embedded in it, will enable full control against virus threats, malware, spoofing, modification of source codes and any system vulnerabilities and errors. The conducted analyzes and tests have shown that the solutions proposed under the research project are best suited to the system that allows for individual adjustment of the system to the conditions required by the intelligent water supply system under construction, enabling full control over the users.

4. Conclusions

The conducted research and analyses related to the preparation, design and target implementation of the IT system necessary to build an intelligent water supply network

were mainly focused on the selection of an appropriate system to support the infrastructure under construction. The authors presented the methodology of selecting, verifying and testing systems and solutions necessary to build modern and intelligent systems supporting critical infrastructure. The most important issues of selecting system and technical solutions were identified and include:

a) The main and most important feature of such infrastructure is safety, reliability, integrity and universality of the solutions applied
b) Elements securing the access to resources from the external internet network and separating the newly built system from the production system performing the basic activity of the water supply company
c) The need to ensure that all components of the system have the ability to communicate and exchange data with both production system components and the prediction system and other database components through standard mechanisms
d) The need to use various communication protocols.

The authors emphasize that the results of the analyses presented in this publication constitute a proposal for the selection of hardware and IT solutions for industrial systems of the critical water supply infrastructure. This problem requires constant updating and scientific filling of the gap for the constantly changing and emerging cyber threats of the indicated systems. This is of particular importance for the functioning of smaller and large agglomerations and entire societies.

Acknowledgements

The article was presented during the II International Scientific and Technical Conference "Critical Infrastructure of Cities" on October 6–8, 2021 in Rytro, Poland.

Conflict of interest

The authors declare no conflict of interest.

References

[1] National Critical Infrastructure Protection Program, 2020, Consolidated Text. Available at: https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej (Access 23/10/2021) (in Polish).
[2] P. Małka, T. Uhl, J. Kłapyta, R. Langer, Integrated energy efficiency system as an important element increasing the reliability of water supply and sewage systems, Gas Water Sanit. Technol., 4 (2017) 154–156 (in Polish).
[3] P. Małka, Cybersecurity of Industrial Systems OT Operating in Municipal Infrastructure, Critical Infrastructure of Cities: Safe Functioning of Municipal Infrastructure: Water Supply, Sewage, Energy, ICT: International Scientific and Technical Conference, October 24–26, 2018, Nowy Sącz - Rytro, Nowy Sącz: "Sądeckie Wodociągi" Spółka z o. o., 2018, p. 19 (in Polish).
[4] K. Gaska, A. Generowicz, M. Lobur, N. Jaworski, J. Ciuła, M. Vovk, Advanced algorithmic model for poly-optimization of biomass fuel production from separate combustible fractions of municipal wastes as a progress in improving energy efficiency of waste utilization, E3S Web Conf., 122 (2019) 01004, doi: 10.1051/e3sconf/201912201004.
[5] R. Brodziak, A. Urbaniak, Management and monitoring of the water supply system in a smart city, Gas Water Sanit. Technol., 5 (2019) 165–171 (in Polish).
[6] D. Chen, P. Wawrzyński, L. Zhihan, Cyber security in smart cities: a review of deep learning-based applications and case studies, Sustainable Cities Soc., 66 (2021) 102655, doi: 10.1016/j.scs.2020.102655.
[7] A. Hassanzadeh, A. Rasekh, S. Galelli, M. Aghashahi, R. Taormina, A. Ostfeld, M. Katherine Banks, A review of cybersecurity incidents in the water sector, J. Environ. Eng., 146 (2020) 1–44.
[8] G. Falco, C. Caldera, H. Shrobe, IIoT cybersecurity risk modeling for SCADA systems, IEEE Internet Things J., 5 (2018) 4486–4495.
[9] J. Ciuła, Modeling the migration of anthropogenic pollution from active municipal landfill in groundwaters, Archit. Civ. Eng. Environ., 14 (2019) 81–90.
[10] M. Załęska-Orłowska, N. Wronowski, Intelligent network management system in Żywiec, Direction Wod-Kan, 2 (2018) 24–28 (in Polish).
[11] J. Bylka, Wyzwania dla inteligentnych sieci wodociągowych, Kierunek Wod-Kan. T. 2 Challenges for smart water networks, Direction Wod-Kan, 2 (2017) 32–34 (in Polish).
[12] R. Padulano, G. Del Giudice, A mixed strategy based on self-organizing map for water demand pattern profiling of large-size smart water grid data, Water Resour. Manage., 32 (2018) 3671–3685.
[13] C. Giudicianni, M. Herrera, A. di Nardo, A. Carravetta, H.M. Ramos, L. Adeyeye, Zero-net energy management for the monitoring and control of dynamically-partitioned smart water systems, J. Cleaner Prod., 252 (2020) 119745, doi: 10.1016/j.jclepro.2019.119745.
[14] R. Wyczółkowski, Intelligent water network monitoring system, Oper. Reliability, 1 (2008) 33–36 (in Polish).
[15] G. Tzagkarakis, P. Charalampidis, S. Roubakis, A. Makrogiannakis, P. Tsakalides, Quantifying the computational efficiency of compressive sensing in smart water network infrastructures, Sensors, 20 (2020) 3299, doi: 10.3390/s20113299.
[16] E. Wysowska, A. Kicińska, Assessment of health risks with water consumption in terms of content of selected organic xenobiotics, Desal. Water Treat., 234 (2021) 1–14.
[17] Directive (EU) 2020/2184 of the European Parliament and of the Council of 16 December 2020 on the Quality of Water Intended for Human Consumption.
[18] The Act of 5 July 2018 on the National Cybersecurity System, Journal of Laws 2018 Item 1560 (Accessed on October 23, 2021) (in Polish).
[19] Cybersecurity A.D. 2018 Strategy, Policy, Recommendations – Cybersecurity in the Policy Perspective, NASK Publishing House.
[20] S. Won Lee, S. Sarp, D. Jin Jeon, J. Ha Kim, Smart water grid: the future water management platform, Desal. Water Treat., 55 (2015) 339–346.
[21] H.M. Ramos, A. McNabola, P. Amparo López-Jiménez, M. Pérez-Sánchez, Smart water management towards future water sustainable networks, Water, 12 (2020) 58, doi: 10.3390/w12010058.
[22] K. Gaska, A. Generowicz, SMART computational solutions for the optimization of selected technology processes as an innovation and progress in improving energy efficiency of smart cities—a case study, Energies, 13 (2020) 3338, doi: 10.3390/en13133338.
[23] M.H. Yasin, S.R.M. Zeebaree, M.A.M. Sadeeq, A.Y. Ameen, I.M. Ibrahim, R.R. Zebari, R.K. Ibrahim, A.B. Sallow, IoT and ICT based smart water management, monitoring and controlling system: a review, Asian J. Res. Comput. Sci., 8 (2021) 42–56.
[24] T.M. Vinod Kumar, C. Mohammed Firoz, P. Bimal, P.S. Harikumar, P. Sankaran, Smart Water Management for Smart Kozhikode Metropolitan Area, T. Vinod Kumar, Ed., Smart Environment for Smart Cities, Advances in 21st Century Human Settlements, Springer, Singapore, 2020. Available at: https://doi.org/10.1007/978-981-13-6822-6_7
[25] W. Cieżak, J. Łomotowski, Z. Siwoń, P. Linczar, J. Cieżak, Neural models in the analysis and forecasting of water partition, Instal, 7 (2011) 61–63 (in Polish).