Modelling smart city cyber-physical water supply systems: vulnerabilities, threats and risks

Nikolai Fomin[1], Roman Meshcheryakov[1]

[1] V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Moscow 117997, Russia
science-fomin@yandex.ru

Abstract. The article presents an approach to modeling the cyber-physical water supply system of a smart city. The shortcomings of control models are considered, and the list of vulnerabilities of the cyber-physical water supply system of a smart city based on scenario modeling is supplemented. The features of modeling the cyber-physical water supply system of a smart city were formed by a comprehensive threat analysis. The proposed approach makes it possible to generalize vulnerabilities, threats and create requirements for modeling scenarios of violation of the management of cyber-physical water supply systems in order to reduce potential risks. Based on a multi-criteria assessment, the optimal model for control the cyber-physical water supply system of a modern city was determined - a Digital water utility with a centralized data exchange system based on the state information system for water resources management. The results of the study were practically used in one of the largest water supply companies in Russia - the city of Saint Petersburg.

Keywords: Cyber-physical systems, Modeling of control systems, Smart city, Water supply systems, Modernization of control models, Cyber-physical water supply system of a smart city.

1 Introduction

In recent years, the threat to critical water infrastructure has increased, as evidenced by the growing number of reported attacks on these systems. Preventive security mechanisms are often insufficient to detect and neutralize the actions of attackers in order to limit the potential damage from successful attacks. Ensuring the security of the functioning of the smart city's enabling cyber-physical systems is a complex task [1]. The resilience of cyber-physical systems of a smart city to potential intrusions and cyber threats is particularly relevant due to the increase in the number of equipment connected to the systems. In addition to the quantitative increase in equipment, the complexity of building the architecture of cyber-physical systems of a smart city is also due to the disparity of the integrated subsystems, as well as the individual characteristics of the architectures themselves. The problem of safe functioning and resource management of modern cities is particularly relevant. Urbanization imposes certain requirements for improving resource management models [2]. By analyzing the existing trends in the functioning of cyber physical systems in modern cities, it is possible to identify a list of current vulnerabilities and threats and form an optimal management model.

2 Materials and Methods

Firstly, we will create a consolidated list of potential threats based on vulnerabilities for both digital and analog water utilities. Next, based on the hierarchy analysis method, we will conduct a multi-criteria assessment of possible alternatives to water management models in a modern city. To simplify the perception, we will divide the management alternatives into 4 categories, which will become the basis for choosing alternatives to management models based on the hierarchy analysis method.

3 Results

For ease of perception of the results obtained in the course of research, we group them into subsections:

- Assessment of control models of active water supply systems taking into account negative factors.
- Classification of potential vulnerabilities, threats and risks of functioning of cyber-physical water supply systems in a smart city
- Modeling of scenarios of water supply system control failure.

3.1 Assessment of control models of active water supply systems taking into account negative factors

Formulate the main terms used in the study.

A threat to the security of a cyber-physical system is a set of conditions and factors that create a potential or actual danger of violating the security of the functioning of a cyber-physical system.
Vulnerability of the cyber-physical system - a lack (weakness) of the infrastructure, software (software-technical), software-hardware levels, as well as the influence of the human factor on the functioning of the cyber-physical system as a whole, which can be used to implement security threats.
Security risk of a cyber-physical system is the product of the probability of a threat to the functioning of a cyber-physical system by the size (magnitude) of the potential consequences.

Cyber-physical attacks on water infrastructure have increased with the number of connected equipment and water automation-transforming into smart water management. Identifying and neutralizing potential vulnerabilities is an important process that allows you to safely and effectively use the benefits of digital equipment in the smart city water supply industry [3]. One way is to improve algorithms for detecting cyber-physical attacks in water network management [4]. Which uses data analysis from infrastructure equipment, model-based detection mechanisms, and rule checking (figure 1).

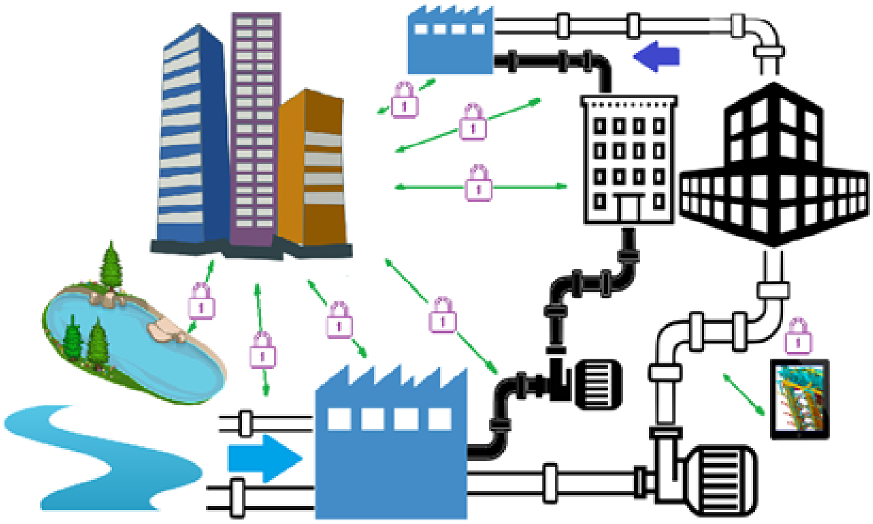

Fig. 1. Simulation of the functioning of the "digital water supply"

The digital water supply control model differs from the analog water supply control model. Digitalization of the industry has a positive impact on the level of development of water utilities, centralized data exchange via secure communication channels, and the ability to build both deterministic and stochastic models, which result in optimizing costs and improving the quality of services provided to consumers [5]. Often, the main problem of the transition to the management of a "digital water channel" is the lack of funding even to maintain the existence of an "analog water channel". The authors believe that this problem is a serious test and challenge for the modern world during the transition to digital format [6]. Smart city technology solutions must meet security requirements, including in the field of CPS water supply for Smart cities [7].

An important aspect is the procedure for detecting an attack on a cyber-physical water supply system. There are various mechanisms for integrated assessment of the state of systems, including the implementation of sustainable and safe remote monitoring. A set of measures to assess the state of the system at each time step contributes to the timely detection of certain attacks. The authors of [8] a numerically efficient algorithm for achieving stability and detecting attacks on remote monitoring systems has been developed. In [9] several traditional methods for detecting anomalies are considered and evaluated in the context of detecting attacks in water distribution systems. These algorithms were centrally trained across the feature space and compared with multi-stage detection methods that were developed to isolate both local and global anomalies. In addition, a new ensemble technique combining density-based and parametric algorithms was developed and tested in the applied environment. Traditional methods had comparable results with multi-stage systems, and when used in conjunction with a local anomaly detector, the effectiveness of these algorithms was significantly improved.

The infrastructure of water supply, distribution, and sanitation systems is socially significant. When modeling a water distribution system [10] a universal agent-based structure is used to evaluate the collective behavior of the control system during cyber-attacks launched against the implementation of this model. A real-time model of urban water cycle management is considered in [11], divided into water supply systems and urban drainage systems necessary for the functioning of urban society. Cyber-physical water supply system is presented as a technological complex for effective management of critical systems. Validation of the proposed approaches to managing the cyber-physical system was performed using virtual reality simulations based on MATLAB/SIMULINK and EPA-SWMM. Through modeling in these environments, a physical model of real objects and its digital counterpart (digital twin), water users and the environment were presented. The evaluation of information flows in the interaction of agents and management systems is carried out.

The work [12] is devoted to automatic detection of water losses in water distribution networks by dynamic analysis of time series associated with water consumption within the network, and the use of a classifier for wavelet detection of points of change to detect anomalies in the consumption structure. The wavelet point change method uses a continuous wavelet transform of time series (signals) to analyze how the frequency content of a signal changes over time. In the case of water distribution networks, the time series is associated with the streaming of water consumption data from automatic meter reading devices either at the level of individual consumers or at the level of the aggregated district area of the meter. The method of detecting wavelet points of change analyzes the provided time series to obtain its own knowledge about water consumption in normal conditions at the household level or throughout the territory, and then makes conclusions about water consumption in abnormal conditions.

A critical review of uncovered documented and malicious cybersecurity incidents in the water sector described in [13] also confirms the increased incidence of external interference. For each individual incident, the situation, response measures, remedial measures and lessons learned were compiled and described. The results of this review indicate an increase in the frequency, diversity and complexity of cyber threats in the water sector. While the emergence of new threats, such as ransomware or crypto jacking, has been detected, the recurrence of similar vulnerabilities and threats, such as insider threats, has also been evident, underscoring the need for an adaptive, cooperative, and comprehensive approach to water-based cyber defense.

3.2 Classification of potential vulnerabilities, threats and risks of functioning of cyber-physical water supply systems in a smart city

The described vulnerabilities and threats will be the basis for building new models for managing active water supply systems. It is important to note that managing these risks will increase the level of strategic security of cities in management. When assessing the vulnerabilities of digital water channels, the degree of threat impact on the stability of the water management system, we suggest dividing it into several contours: *a) Operation of IoT and IIoT terminal equipment; b) Integration of the cyber-physical system with smart city systems; c) Data centralization in the unified information system of the country.*

This paper does not address the third circuit issues - the possibility of centralizing the exchange of information from several smart cities. Such systems of combining information from several cities and regions represent a higher-level system. The requirements for such systems will be described by the authors in the following scientific papers. Such large-scale systems require additional analysis of vulnerabilities and threats [14], comparison of architecture options for building cyber-physical water supply systems in smart cities [15], and improvement of security [16].

Based on the results of current and previous studies, the authors concluded that it is necessary to group the problems of managing cyber-physical water supply systems into several areas (aspects):

- limited water resources;
- increased wear and tear of water supply systems;
- increase in the urban population;
- degradation of water sources;
- lack of backup water sources;
- non-compliance of equipment at water treatment plants with modern types of pollution - both chemical and biological: antibiotics, micro plastics, biologically active bacteria.

Next look at each of these aspects in more detail. The created classification (Table 1) is a basic one, compiled by an expert method based on the vulnerabilities, threats and risk levels identified in previous studies. When conducting a comprehensive assessment of the security status of cyber-physical water supply systems in a smart city, it is necessary to take into account the features of the system architecture, data exchange, and hardware used both for the operation of systems and for preventing potential management threats [17].

Table 1. Basic classification of potential vulnerabilities, threats and risks of functioning of cyber-physical water supply systems in a smart city.

Vulnerability	Threats	Risk level
Group 1 - Infrastructure level (water supply systems, equipment, water supply sources)		
Use of outdated technologies to detect the degree of water pollution	Chemical infestations Biological infections Increasing morbidity of the population The decline in the quality of water supplied	Medium
High level of water infrastructure wear and tear	Failure of water supply networks Losses during transport The decline in the quality of water supplied Increasing morbidity of the population Chemical infestations Biological infections	Medium

Lack of backup water supply sources	Emergency situation in a part of the city, district, and in the agglomeration as a whole The interruption in supply of water	Medium
Lack of fresh water storage facilities	Emergency situation in a part of the city, district, and in the agglomeration as a whole Water supply interruption (iodine deficiency) Poisoning of the population Failure of equipment and water treatment plants	Medium
Lack of network health monitoring systems	Losses during transport Chemical infestations Biological infections Unauthorized connections to the networks	High
Lack of main systems for monitoring the state of water supplied to the consumer	Losses during transport Chemical infestations Biological infections Unauthorized connections to the networks Poisoning of the population	High
Group 2 - Program level		
A program code of not declared possibilities of the software	Failure of systems and equipment Interception and corruption of data Remote monitoring and management of systems	Medium
Software injections	Failure of systems and equipment Interception and corruption of data Remote monitoring and management of systems	Medium
Accessibility from outside (a potential invasion of hackers)	Failure of systems and equipment Interception and corruption of data Remote monitoring and control of systems	Medium
Backdoors of imported software	Failure of systems and equipment Interception and corruption of data Remote monitoring and management of systems	High
Group 3 - Hardware level (digital equipment)		
Availability for connecting hardware	Failure of systems and equipment Interception and corruption of data Remote monitoring and control of systems	Medium
Ability to intercept the signal, suppression, distortion	Failure of systems and equipment Interception and corruption of data Remote monitoring and control of systems	High
Accessibility from outside (a potential invasion of hackers)	Failure of systems and equipment Interception and corruption of data Remote monitoring and control of systems	High
Backdoors of imported hardware	Failure of systems and equipment Interception and corruption of data Remote monitoring and control of systems	High

Remote control of equipment	Failure of systems and equipment Interception and corruption of data Remote monitoring and control of systems	Medium
Group 4 - Human factor (human influence on the system)		
Incorrect actions of the staff	Emergency situation in a part of the city, district, and in the agglomeration as a whole Water supply interruption (iodine deficiency) Poisoning of the population Failure of equipment and water treatment plants	High
Deliberate negative actions of personnel on the functioning of systems (sabotage)	Emergency situation in a part of the city, district, and in the agglomeration as a whole Water supply interruption (iodine deficiency) Poisoning of the population Failure of equipment and water treatment plants	Medium
Potential data leaks	The use of information for subversive purposes Remote monitoring and management of systems	Medium
Incorrect actions of the staff in case of an emergency (due to poor training)	Emergency situation in a part of the city, district, and in the agglomeration as a whole Water supply interruption (iodine deficiency) Poisoning of the population Failure of equipment and water treatment plants	High

3.3 Modeling of scenarios of water supply system control failure

Modeling the stability of the functioning of cyber-physical systems of smart cities is an important aspect of management [18]. It is necessary to determine the optimal management model based on a multi-criteria assessment of possible management alternatives [19]. When building models, both the digital water channel and the analog water channel will be analyzed. This type of organization management of cyber-physical water supply systems in smart cities is also possible, due to the lack of automated management and control systems. To complete the study, each group is divided into subgroups and represents management alternatives. The General structure of the hierarchy analysis method can include several hierarchical levels with their own criteria [20].

The method consists of a set of the following steps:

a) The first step is to structure the task as a hierarchical structure with several levels.
b) At the second stage, the goal, evaluation criteria, and possible alternatives are formed.
c) In the third stage, pairwise comparisons of elements of each level are performed.
d) The importance coefficients for each level's elements are calculated. This checks the consistency of judgments.
e) The combined weight coefficient is calculated and determined the best of the alternatives presented.

Problem statement: choose the optimal control model based on multi-criteria analysis using the analytic hierarchy process from the generated alternatives.

Goal: to identify which management model is more resilient to potential negative management threats.

Defining control alternatives:

a) A digital water utility with a centralized data exchange system based on the state water management information system (A1).
b) Digital water utility without a centralized data exchange system (A2).
c) Analog water utility with improved (updated) infrastructure (A3).
d) Analog water utility without infrastructure upgrade (A4).

Assessment criteria:

a) Ability to detect chemical contamination at both water treatment plants and water supply networks (C1).
b) Ability to detect biological contamination both at water treatment plants and water supply networks (C2).
c) Operational control of potential unauthorized connections to networks and identification of water resources losses (C3).
d) Ensuring water quality control at the consumer (C4).
e) Stability of control systems to cyber-attacks (C5).
f) System management level (C6).
g) Centralization of data on water production and consumption (C7).

The described hierarchical model consisting of 7 criteria and 4 alternatives can be presented visually (Fig. 2).

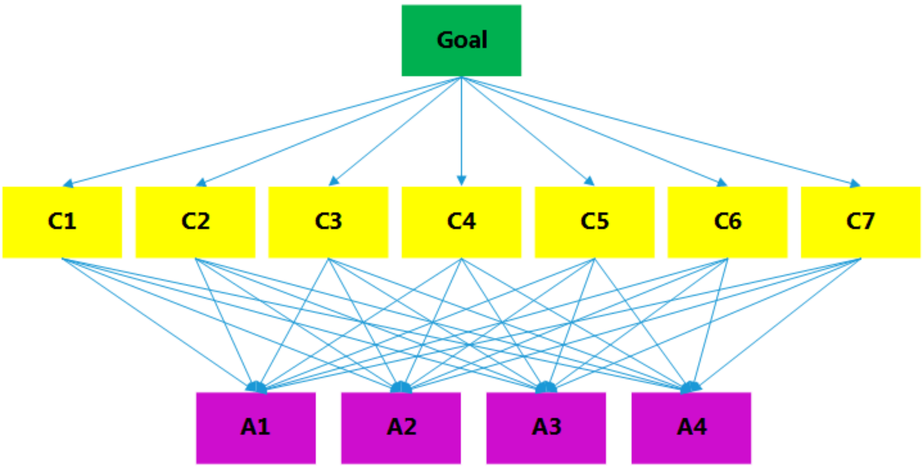

Fig. 2. The design of the model hierarchy

The matrix of paired comparisons represents the second level of the hierarchy. For pairwise comparisons, we use a scale of relative importance from 1 to 9. for Example, criterion C5 is significantly more important than criterion C2, so the number 3 is entered in the corresponding cell; 1/3 is automatically entered in a cell that is symmetrical relative to the diagonal, which corresponds to the opposite comparison. The basis for calculating the relative importance of criteria is an expert assessment. The expert assessment of the criteria is based on a survey of 5 groups of people with different profiles: specialists in the field of water supply; specialists in the field of cyber security; specialists in the field of Economics; civil servants; residents of several cities of different gender and age. The resulting values are rounded and shown in Table 2.

Table 2. The matrix of comparing the criteria.

Criteria	C1	C2	C3	C4	C5	C6	C7	Eigen-vector	The vector of priorities
C1	1	1	3	2	4	4	3	2.25	0.27
C2	1	1	2	2	3	4	3	2.03	0.24
C3	0.33	0.5	1	1	1	3	3	1.06	0.13
C4	0.5	0.5	1.0	1	3	3	2	1.24	0.15
C5	0.25	0.33	1.0	0.33	1	1	2	0.66	0.08
C6	0.25	0.25	0.33	0.33	1	1	2	0.54	0.06
C7	0.33	0.33	0.5	0.5	0.5	0.5	1	0.64	0.08

After that, priority vectors were calculated, which are also shown in Table 2, the maximum eigenvalue λmax, the consistency index, and the consistency ratio. The maximum eigenvalue λmax is calculated using the matrix of paired comparisons as follows: stack each column of judgment, then the sum of the first multiplied by the value of the first components of the normalized vector of priorities, the sum of the second column on the second component, etc. then the resulting numbers are added together. The consistency index (CI) is determined using the following formula (1), where *n* is the number of elements to compare (the size of the matrix).

$$CI = (\lambda_{max} - n) / (n - 1) \tag{1}$$

Calculating the average value of the consistency index for the resulting matrix. Dividing the *CI* by the number corresponding to random consistency (RC), we get the consistency ratio (*CR*). For a matrix of size n = 7, random consistency *RC* = 1.32. Calculate the consistency ratio using the following formula (2):

$$CR= CI / RC \tag{2}$$

The consistency ratio of the resulting *CR* matrix = 0.09. The consistency level is considered acceptable when the *CR* is ≤ 0.1. if the consistency level exceeds 0.1, then a review of the judgments is necessary. This is not required in the current case.

After performing the calculations of the second level, we proceed to the third - a pairwise comparison of alternatives with each of the criteria [21]. We get seven matrices of judgments with dimension 7 × 4, since there are seven criteria at the second level and four control alternatives. The resulting matrices allow us to calculate the coefficients of importance of the corresponding elements of the hierarchical level. This was computed eigenvector matrix, and then normalized. As a result, the following priority vectors for each criterion were obtained, shown in Table 3.

Table 3. Priority vector for level 3.

Alternatives/ criteria	C1	C2	C3	C4	C5	C6	C7
A1	0.47	0.47	0.54	0.53	0.56	0.54	0.55
A2	0.28	0.28	0.26	0.27	0.26	0.26	0.27
A3	0.16	0.16	0.12	0.14	0.12	0.12	0.13
A4	0.1	0.1	0.07	0.06	0.07	0.07	0.06

The maximum eigenvalue λ_{max} the consistency index, and the consistency ratio were also calculated to detect inconsistency of the obtained level 3 matrices. For a matrix of size n = 4, random consistency RC = 0.9. the consistency Ratio for level 3 pair comparison matrices was: according to the criterion C1 = 0.01; C2 = 0.01; C3 = 0.04; C4 = 0.07; C5 = 0.04; C6 = 0.04; C7 = 0.05. The resulting OS values correspond to the OS condition ≤ 0.1, and therefore no revision is required to improve consistency.

The best alternative is determined using the formula (3), where V_i is the quality weight of the i – th alternative; w_i the weight of the i-th criterion; V_i is the importance of the j-th alternative according to the i-th criterion.

$$V = \sum_{i=1}^{n} w_i V_i \tag{3}$$

For each control method, we determine the weight coefficient and get the following values (table 4).

Table 4. Calculated values of the weighting factors of the alternatives.

Alternatives	Weighting factor
A1	0.5
A2	0.27
A3	0.14
A4	0.08

The above calculations allow us to determine the weight coefficient of each control alternative according to the specified criteria and identify the optimal control model from them. In this case, the best indicator is the A1 control model based on digital control with a centralized data exchange system, the weight coefficient of which is = 0.5. The presented calculations became the basis for the practical implementation of the modernization of the management model in one of the largest cities in Russia - the city of Saint Petersburg. The population of the city is more than 5 million people.

4 Discussion

The results of the study suggest that modeling the functioning of cyber-physical systems of smart cities is important. Cases of external intrusions aimed at destabilizing the functioning of systems have become more frequent. The authors ' basic classification of potential vulnerabilities and threats to the functioning of cyber-physical water supply systems in smart cities allows us to summarize potential incidents.

Based on a multi-criteria assessment of possible alternatives for managing the cyber-physical water supply system of a modern city, the optimal management model was chosen - a Digital water utility with a centralized data exchange system based on the state information system for water resources management. Secure centralization of information makes it possible to increase the level of strategic security of cities and countries in General. The authors will design architectures for building a centralized system at the state level in the following studies. Features of the projected cyber-physical systems and existing cyber-physical water supply systems of cities will be taken into account.

5 Conclusion

The article presents an approach to modeling the cyber-physical water supply system of a Smart city. The shortcomings of management models are considered, and the list of vulnerabilities of the cyber-physical water supply system of a Smart city based on scenario modeling is supplemented. Thanks to a comprehensive threat analysis, the features of modeling the cyber-physical water supply system of a smart city were formed. The proposed approach makes it possible to generalize vulnerabilities, threats and create requirements for modeling scenarios of violation of the management of cyber-physical water supply systems in order to reduce potential risks. New models for managing active cyber-physical water supply systems in a smart city allow you to increase the level of management, reduce potential negative factors in providing water supply to the city, and can be applied by different cities. Based on a multi-criteria assessment, the optimal model for managing the cyber-physical water supply system of a modern city was determined - a Digital water utility with a centralized data exchange system based on the state information system for water resources management.

Data centralization in the unified information system of the country from several smart cities is not considered in this paper. Such systems of combining information from several cities and regions represent a higher-level system. The requirements for such systems will be described by the authors in the following scientific papers. Such large-scale systems require additional analysis of vulnerabilities and threats, and comparison of architecture options for building cyber-physical water supply systems in smart cities.

Acknowledgments

The reported study was partially funded by ICS RAS according to the state project.

References

1. Habibzadeh, Hadi, et al. "A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities." Sustainable Cities and Society 50 (2019): 101660.
2. Vasel-Be-Hagh, Ahmad, and David SK Ting, eds. Environmental Management of Air, Water, Agriculture, and Energy. CRC Press, 2020.
3. Yang, Longzhi, Noe Elisa, and Neil Eliot. "Privacy and security aspects of E-government in smart cities." Smart cities cybersecurity and privacy. Elsevier, 2019. 89-102.
4. Taormina, R., Galelli, S., Tippenhauer, N. O., Salomons, E., Ostfeld, A., Eliades, D. G., et al. (2018). Battle of the Attack Detection Algorithms: Disclosing Cyber Attacks on Water Distribution Networks (Article). Journal of Water Resources Planning and Management, 144(8), 11. doi:10.1061/(asce)wr.1943-5452.0000969.
5. Alilou, Hossein, et al. "A cost-effective and efficient framework to determine water quality monitoring network locations." Science of the total environment 624 (2018): 283-293.
6. Shao, Qigan, et al. "Developing a sustainable urban-environmental quality evaluation system in China based on a hybrid model." International journal of environmental research and public health 16.8 (2019): 1434.
7. Camara, Moriken, et al. "Economic and efficiency based optimisation of water quality monitoring network for land use impact assessment." Science of The Total Environment (2020): 139800.
8. Ge, X. H., Han, Q. L., Zhang, X. M., Ding, D. R., & Yang, F. W. (2020). Resilient and secure remote monitoring for a class of cyber-physical systems against attacks (Article). Information Sciences, 512, 1592-1605. doi:10.1016/j.ins.2019.10.057.
9. Ramotsoela, D. T., Hancke, G. P., & Abu-Mahfouz, A. M. (2019). Attack detection in water distribution systems using machine learning (Article). Human-Centric Computing and Information Sciences, 9, 22. doi:10.1186/s13673-019-0175-8.
10. Mishra, V. K., Palleti, V. R., & Mathur, A. (2019). A modeling framework for critical infrastructure and its application in detecting cyber-attacks on a water distribution system (Article). International Journal of Critical Infrastructure Protection, 26, 19. doi:10.1016/j.ijcip.2019.05.001.
11. Sun, C. C., Puig, V., & Cembrano, G. (2020). Real-Time Control of Urban Water Cycle under Cyber-Physical Systems Framework (Article). Water, 12(2), 17. doi:10.3390/w12020406.
12. Christodoulou, S. E., Kourti, E., & Agathokleous, A. (2017). Waterloss Detection in Water Distribution Networks using Wavelet Change-Point Detection (Article). Water Resources Management, 31(3), 979-994. doi:10.1007/s11269-016-1558-5.
13. Hassanzadeh, A., Rasekh, A., Galelli, S., Aghashahi, M., Taormina, R., Ostfeld, A., et al. (2020). A Review of Cybersecurity Incidents in the Water Sector (Review). Journal of Environmental Engineering, 146(5), 13. doi:10.1061/(asce)ee.1943-7870.0001686.
14. Chow, Richard. "The last mile for IoT privacy." IEEE Security & Privacy 15.6 (2017): 73-76.

15. Kim, Hyunbum, and Jalel Ben-Othman. "Toward Integrated Virtual Emotion System with AI Applicability for Secure CPS-Enabled Smart Cities: AI-Based Research Challenges and Security Issues." IEEE Network 34.3 (2020): 30-36.
16. Zhao, Lei, et al. "Optimal edge resource allocation in IoT-based smart cities." IEEE Network 33.2 (2019): 30-35.
17. Chatterjee, Sheshadri, et al. "Prevention of cybercrimes in smart cities of India: from a citizen’s perspective." Information Technology & People (2019).
18. Jan, Sivan, Asaf Cohen, and Gideon Oron. "Multi-objective optimization for solving water shortage issues in arid zones via the analytic hierarchy process (AHP): the Israeli case." DESALINATION AND WATER TREATMENT 188 (2020): 10-19.
19. Carli, Raffaele, Mariagrazia Dotoli, and Roberta Pellegrino. "Multi-criteria decision-making for sustainable metropolitan cities assessment." Journal of environmental management 226 (2018): 46-61.
20. Saaty, Thomas L., and Pierfrancesco De Paola. "Rethinking design and urban planning for the cities of the future." Buildings 7.3 (2017): 76.
21. Saaty, Thomas. "Decision-making. Analytic hierarchy process.” – M.: Radio and Svyaz. p.278 (1993).