*Interdisciplinary Description of Complex Systems* 22(3), 291-300, 2025

# CYBERSECURITY IN SMART CITY ENERGY SYSTEMS

**Attila Dér***

Óbuda University, Doctoral School on Safety and Security Sciences
Budapest, Hungary

DOI: 10.7906/indecs.22.3.10
Regular article

*Received:* 20 February 2024.
*Accepted:* 1 November 2024.

## ABSTRACT

Recently, the number of cyber-attacks on critical organisational infrastructure has increased dramatically. These attacks have not spared the infrastructures of smart cities. It is no coincidence that the present research highlights the cyber defence of the smart cities' energy supply as the most vulnerable critical infrastructure. After all, it is easy to see that in such crowded smart grid systems, the adequate energy supply is vital. Therefore, one crucial goal for smart city management is to increasingly seek proactive measures to detect potential cyber-attacks before they occur, in order to protect against such attacks. As a consequence, it is worthwhile and useful to analyse and understand the attack patterns of the opponents. This article presents a colourful palette of defence solutions that build on or complement each other. The research will briefly cover the different defence models and techniques. Furthermore, their applicability and effectiveness in Smart Cities will also be discussed. Finally, the sustainability and future challenges of protecting energy supply systems will be examined and summarised by proposing modern and reliable protection for these systems.

## KEY WORDS

smart city, cybersecurity, critical infrastructure, energetic systems, energy supply systems

## CLASSIFICATION

ACM: 10003033.10003106.10003112

JEL: Q40

*Corresponding author, $\eta$: der.attila@uni-obuda.hu; -;
József körút 6., Budapest, 1088, Hungary

## INTRODUCTION

In most parts of the world today, an increasing proportion of the population lives in urban environments. This trend is set to continue in the future, as many countries already have specific strategic visions for building a sustainable and secure society with a smart economy, smart lifestyle and smart governance. There are many challenges to be faced in the modernisation of urbanisation, such as air pollution, traffic congestion, adequate living conditions, etc. With the development and spread of digital technology, a whole new range of possibilities has opened up to address these problems. With improved computer control and communication networks, the model of the smart city has also come to life. Smart cities now connect not only computers and data centres, but also devices that were previously not connected to the Internet. These include cars, traffic lights and smart meters, whose protection is of paramount importance. Obviously, these systems also need to run, so their power supply must be ensured. In these cities, as in simpler urban forms, power is supplied by industrial control systems Industrial Control Systems (ICS) and Supervisory control and data acquisition (SCADA). Since these control units in particular play a key role in energy supply, they can safely be called, together with their system components, critical elements in the operation of critical infrastructures.

Smart city energy systems, being interconnected and reliant on digital technologies, necessitate robust cybersecurity measures. Here are key considerations for securing smart city energy systems.

## NETWORK SECURITY

Implement strong encryption protocols to protect communication between devices and infrastructure components within the energy network.

Regularly update and patch software and firmware to address vulnerabilities and ensure the latest security features. It is basic rule that in energy supply centres, the administration part of the IT systems must be strictly separated from the operations management part. The most desirable solution would be to limit the communication between the most critical systems to a closed system and to segment them into separate sub-units, so that if one is attacked, the other units are still operational. Therefore, in practice, the interconnection would be provided by optical cables, with the network able to detect any disturbance if the set parameters of the light were changed. Obviously, in addition to physical prevention, a network monitoring system would also be in operation continuously, as the whole smart grid system is controlled by complex, adaptive and automated algorithms [1]. To mitigate cyber-attacks, a combination of different architectures such as Black Grid, Trusted SDN Controller, Unified Registration and Key Management Systems are possible.[2] In smart cities, Black Grids in which Grain128 or AES is used to encrypt payload and metadata (independently secured in the network) in an IoT protocol within Link layer communication can greatly reduce active and passive intrusions in energy networks [2, 3].

## ACCESS CONTROL

Enforce strict access controls, limiting system access only to authorized personnel. Multi-factor authentication enhances security by requiring multiple forms of verification.

It collects information from smart grid consumers' habits, meter data and other sensor parameters to ensure that the smart city's energy supply is reliable, economical and efficient. Since most of the information is quite sensitive and not public, appropriate registration, login and authentication protocols have been developed to protect against unauthorized or malicious attackers. One such module is Collaborative Mutual Authentication (CMA), which uses an

MGA-RF-based machine learning algorithm. Based on studies conducted, this blockchain-based mechanism seems to be very promising in terms of filtering out unauthenticated requests and ensuring reliable data communication [4]. Furthermore, data integration and consistency in the cloud can be securely addressed by an algorithm that performs blockchain-based data storage verification [5]. Of course, the privacy protection mentioned in the previous point – via black networks – identity management and authentication can be extended to this access control part, together with SDN and Unified Registry [6].

## ANOMALY DETECTION

Employ AI-driven anomaly detection systems to identify unusual patterns or behaviours in the energy network, indicating potential cybersecurity threats.

Traditional Intrusion Detection Systems (IDS) have had to be equipped with artificial intelligence to detect increasingly sophisticated attack techniques. This system based on Machine Learning (ML) and feature selection technique can use four types of Machine Learning techniques, which are Decision Tree (DT), K-Nearest Neighbours (KNN), Support Vector Machine (SVM) and Random Forest (RF). As shown in Figure 1, recent research has shown that among the above methods, Random Forest has the most satisfactory performance and accuracy [7]. Distributed Denial of Service (DDoS) and "plain" Denial of Service (DoS) attacks are of great importance in the energy supply of smart cities. As a consequence, it is advisable to prevent attack techniques that operate by overloading the network, for which the best detection method is the NSL-KDD dataset. This technique is a combination of Convolutional Neural Network CNN and Long Short Term Memory Neural Network (LSTM) models [8].

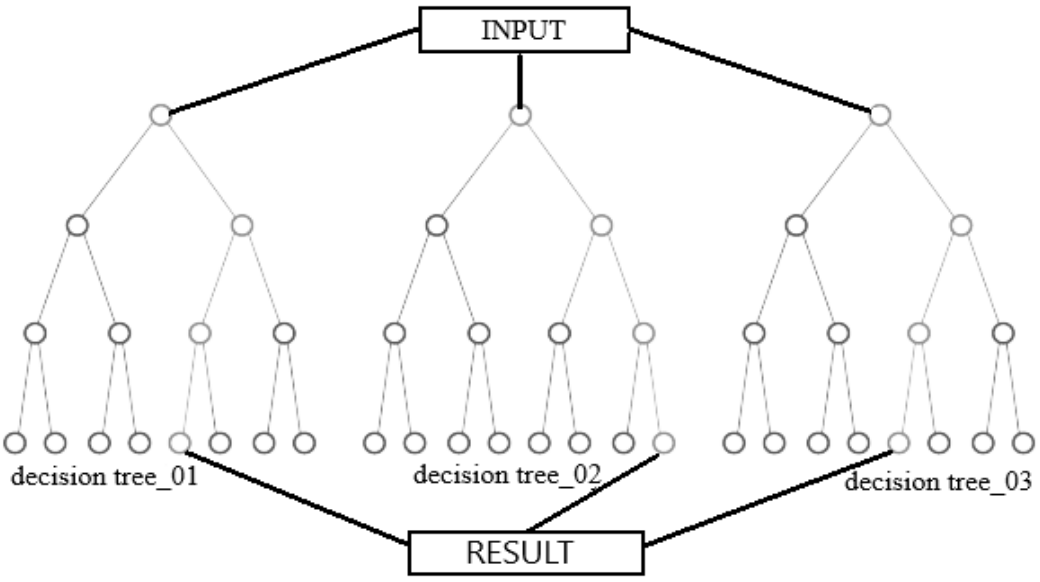


**Figure 1.** How Random Forest (RF) works.

## INCIDENT RESPONSE PLANNING

Develop and regularly update an incident response plan to ensure a swift and effective response to cybersecurity incidents, minimizing potential damage and downtime.

The first step in an incident management plan is to develop a smart city energy security policy. Following a risk assessment, the sensitive elements that provide the energy supply will be identified, and a Computer Security Incident Response Team (CSIRT) will be established to professionally oversee the cyber protection of these assets.

The second step is to identify any deviations from normal operation in the smart city's power-related IT systems. Identified deviations need to be classified according to their severity and type, and then properly documented. The third step would be to isolate the computer networks of industrial control units.

The fourth step is to eliminate malware from the systems concerned. Take improvement measures to avoid detected incidents.

Step five should be to carry out the recovery of the live system and prepare a case study. Further analysis should be performed before the incident is closed, and then a post-mortem analysis of the incident should be conducted [9].

There are several types of security plans. One of the divisions shows how to effectively design a system by identifying roles and responsibilities. The clear assignment of responsibilities is important for accountability and building subsequent solution models. The next strategic step is to document the network architecture, which maps the precise containment of sensitive data and the detection of errors in system operation. Continuous monitoring and Risk Management of Smart city network systems will also contribute greatly to the elimination of system vulnerabilities. In the next step, the study mentions the early deployment of defence in depth and the layered architecture of cyber security. Furthermore, cybersecurity requirements, programs and the corrective actions to be taken in case of security problems should be defined. It is important that these guidelines include rules and procedural protocols tailored to users and those with administrative rights. The next section deals with the issue of configuration management of power system hardware and software, which is an essential prerequisite for system security, especially in the area of control and data acquisition systems. The self-testing of SCADA systems provides an excellent opportunity to identify faults, and thus increase the efficiency of repairs. This could include the continuous performance of various vulnerability tests or the auditing of networks according to standards. The aim of this research is not to describe these methods and guidelines in detail, so only the main steps will be outlined, such as mapping the models used for disaster recovery; agreeing on the expectations of the people managing the power systems in relation to the cyber defence action plan, and finally the standardised management of sensitive information of SCADA systems [10]. Finally, cybersecurity must be addressed from the design phase of smart grid systems to their decommissioning. In this way, a complete life cycle can be documented, which will provide the right support for management in future new concepts [11].

## ENDPOINT SECURITY

Secure all endpoints, including smart meters and IoT devices, with up-to-date security protocols to prevent unauthorized access or manipulation.

As a consequence, there is a strong focus on endpoint encryption and the control of services used by IoT smart devices. It is essential to use strong passwords, and to change or disable them regularly for endpoints where the use of passwords is relevant. Support end-to-end security with integrated endpoint control, policy enforcement, central management and monitoring. It is also important to note that virus signatures or service patch databases should be continuously updated to maintain adequate protection capabilities. This is where network access control (NAC) plays a major role, helping to secure network endpoints before network access is granted.

It is important to mention Wireless Sensor Networks (WSN), where various biometric authentication methods are used to identify people from fingerprints, faces, etc. Here too, the protection is based on Machine Learning [12]. For IoT devices such as Advanced Measurement Infrastructure (AMI) and Smart Meters (SM), instead of traditional routing algorithms such as

LEACH, Directed Diffusion and PEGASIS, a system called ActiveTrust has been proposed for WSNs [13].

With this algorithm, the security of the data path can be improved as it actively creates newer and newer paths, thus avoiding black holes [14].

It is also important to mention the possibility of using Microsoft Azure IoT in smart city buildings, as two strong authentication methods are used in this cloud architecture. One is to establish the connection using an SAS token with a symmetric key, and the other is based on TLS, which can handle X.509 certificate-based authentication [15].

## DATA ENCRYPTION

Encrypt sensitive data both in transit and at rest to safeguard against interception or unauthorized access.

System controllers and power centre staff often use external devices, removable media and web applications in their daily work. Unfortunately, this data is not only used within a protected system, but also on external IoT devices. Sensitive data is usually copied to removable storage devices or uploaded to the cloud. Thus, these facts should be taken into account when encrypting data. The network monitoring capability of data loss prevention ensures electronic correspondence for all users using the energy solver's IT network, web-based information transfer, file sending and uploading, and FTP traffic, based on a set of rules, and it also detects and prevents the leakage of information to be protected from the Company's closed IT system. A DLP system provides an indication of the shipments identified by the rules system, and also creates a log entry containing the sender's and recipient's e-mail address and other descriptive data and data duration of the shipment, supplemented by the sender's AD system data stored in the system. The log entries shall be stored by the DLP system for the time necessary to manage the incident, but not longer than one year. The network module of the DLP system also provides the possibility to quarantine and block the shipment if necessary.

It is also important to mention in this chapter the possibility of using the latest cryptographic algorithms, such as homomorphic cryptography, where the actual operations and results of the computations are also encrypted. This procedure has a good chance of protecting the private information contained in sensitive data [16].

## SECURITY AUDITS AND TESTING

Conduct regular security audits and penetration testing to identify vulnerabilities in the energy system's cybersecurity infrastructure and address them promptly.

The conventional (fossil fuel-rich) network of smart cities is predicted to be completely replaced by Distributed Energy Resources (DER) and Renewable Energy Systems (RESS), which will greatly contribute to the reliability, automatic detection and immediate response of smart grid energy services [17, 18]. As a consequence, an important aspect is auditing, where mandatory audits are independent audits conducted annually, and internal audits semi-annually. Audits should cover the central resources and applications running in the Data Centre, the computer network, and the physical and personnel environment. Security audits should also take into account IT security audits, where the analysis of the protection capability is key. Of course, risk analysis should not be omitted as a factor mentioned earlier. Finally, the current status of the power system in terms of IT security and certification must be systematically assessed on the basis of the relevant standards and tests, so that it can provide the responsible management officials with objective information on the state of IT security, the security requirements adopted by the organisation, and the possible security incidents [19].

## COLLABORATION WITH CYBERSECURITY EXPERTS

Engage with cybersecurity experts to continuously assess and enhance the resilience of the energy system against evolving cyber threats. Smart cities have a vital need for professionals who can provide a high level of energy security. Think of the damage that would be caused if there was no power for just one hour, or if a hacker attacked traffic lights. Thus, the advice or hiring of these cybersecurity experts is essential to enable the responsible management groups to plan, maintain and continuously improve the cybersecurity protection of smart grid systems with the appropriate expertise [15, 20].

## SECURE COMMUNICATION PROTOCOLS

Use secure communication protocols for data exchange, ensuring the confidentiality and integrity of information transmitted across the energy network. At the time when there was a direct link between the IT network and the operational technology (OT) network, there was no need for network protection. However, when the Internet connection was introduced and the closed IT network was removed, communication protocols started to have security problems. Unfortunately, data exchanges on energy networks also suffer from this problem. In addition, because the system is time-critical, the use of stateful packet inspection and simple firewalls should be severely limited. There are recommendations for special open source or paid firewalls for SCADA networks. However, it is important to consider the use of these for compatibility and security standards. The majority of suspicious IP addresses do not use any position camouflage, making them relatively easy to filter out within the communication protocol. The database of this technique is the premium geolocation service, which increases and accelerates smart grid transmission performance [21-23].

## REGULATORY COMPLIANCE

Adhere to relevant cybersecurity regulations and standards to ensure compliance and maintain a strong security posture. In energy supply systems, attention must be paid to information security from the ground up. There are binding legal regulations and highly recommended national and international standards, recommendations and concepts. For security concepts, in addition to the above, a risk assessment and its evaluation supports the so-called pyramid approach, where security components build on each other [24]. This is the reason why the ISA112 standards committee has launched an initiative to develop a new SCADA system-specific standard, which plans to develop a complete set of standards from 2016 to 2027. What is also worth mentioning is the IEC 62443 standard in combination with the NIS2 directive for critical infrastructure control [25].

## EMPLOYEE TRAINING

Train personnel on cybersecurity best practices and create awareness about potential threats, emphasizing the importance of adhering to security protocols. The importance of cybersecurity should be stressed to children from an early age. Unfortunately, the human factor is far from sufficient for the various types of intelligent protection in industrial applications, so it is advisable to improve the education of employees in this area and to involve psychologists. It is recommended to fill in a validated behavioural-cognitive Internet security questionnaire for staff and to introduce personalised training based on its evaluation [26].

## CONTINUOUS MONITORING

Employ continuous monitoring systems to detect and respond to cybersecurity threats in real-time, reducing the risk of prolonged security breaches. The Security Operations Center (SOC),

which monitors devices around the clock and centralizes the security monitoring and control of devices, plays a key role in managing these threats. In addition to the SOC, which performs monitoring and control, there must also be an incident management capability that can physically implement the relevant actions. A dedicated computer emergency response team is called a Computer Emergency Response Team (CERT) or Computer Security Incident Response Team (CSIRT) [27, 28].

## CONCLUSION

By incorporating these cybersecurity measures, smart cities can better protect their energy systems, ensuring the reliability, integrity, and security of critical infrastructure components essential for the functioning of a modern urban environment. From the above points, it has become clear that Smart Grids are a digital, two-way energy management system that is highly sensitive and vulnerable but can recover by using the appropriate protection models. Furthermore, it can provide a reliable and economical supply for smart cities by relying on adaptive and adaptable predictions from its wider environment [13].

The future direction for the development of smart city wireless networks is determined by the fact that 5G will be gradually replaced by 6G, which is expected to be 10 times more efficient and capable of handling close to 100 million devices. This will meet the growing needs in the energy sector and related automated processes or IoT services and applications. 6G is also expected to provide a solution to adequately protect the predicted seemingly unmanageable amount of data [29].

Several possible innovative and alternative systems, techniques and methods to reduce and prevent cyber-attacks have been presented. In conclusion, in smart cities, blockchain-based security mechanisms can be implemented in energy supply systems as well as in the rest of the grid. It is the latest and most secure technology compared to other existing security solutions [13]. This study has confirmed that Internet access from the power system should not be possible in any way, and that the most critical smart grid components should be connected with fibre optic cables. Furthermore, the segmentation of systems and the strict regulation of the handling of sensitive data and data carriers will also need to be ensured in the near future to provide a secure and reliable power system for the growing number of smart cities [30].

## ACKNOWLEDGMENT

Project no. 2024-2.1.2-EKÖP-KDP has been implemented with the support provided by the ministry of culture and innovation of Hungary from the national research, development and innovation fund, financed under the 2024-2.1.2-EKÖP-KDP funding scheme.

## REFERENCES

[1] Hudasi, L. and Ady, L.: *Artificial Intelligence Usage Opportunities in Smart City Data Management.*
Interdisciplinary Description of Complex Systems **18**(3), 382-388, 2020,
http://dx.doi.org/10.7906/indecs.18.3.8,

[2] Chakrabarty, S. and Engels, D.W.: *A secure IoT architecture for Smart Cities.*
13th IEEE Annual Consumer Communications & Networking Conference. IEEE, Las Vegas, 2016,
http://dx.doi.org/10.1109/CCNC.2016.7444889,

[3] Villar Miguelez, C.; Monzon Baeza, V.; Parada, R. and Monzo, C.: *Guidelines for Renewal and Securitization of a Critical Infrastructure Based on IoT Networks.*
Smart Cities **6**(2), 728-743, 2023,
http://dx.doi.org/10.3390/smartcities6020035,

[4] Khadidos, A.O., et al: *An Intelligent Security Framework Based on Collaborative Mutual Authentication Model for Smart City Networks.*
IEEE Access **10**, 85289-85304, 2022,
http://dx.doi.org/10.1109/ACCESS.2022.3197672,

[5] Vivekanandan, M.; Premkamal, P.K.; Johnpaul, C.I. and Ebinazer, S.E.: *Blockchain based Secure Data Storage Verification Algorithm for Smart City Environment.*
4th International Conference on Innovative Trends in Information Technology. IEEE, Kottayam, 2023,
http://dx.doi.org/10.1109/ICITIIT57246.2023.10068638,

[6] Lv, Z.; Hu, B. and Lv, H.: *Infrastructure Monitoring and Operation for Smart Cities Based on IoT System.*
IEEE Transactions on Industrial Informatics **16**(3), 1957-1962, 2019,
http://dx.doi.org/10.1109/TII.2019.2913535,

[7] Avci, I. and Koca, M.: *Cybersecurity Attack Detection Model, Using Machine Learning Techniques*.
Acta Polytechnica Hungarica **20**(7), 29-44, 2023,
http://dx.doi.org/10.12700/APH.20.7.2023.7.2,

[8] Ahmed Issa, A.S. and Albayrak, Z.: *DDoS Attack Intrusion Detection System Based on Hybridization of CNN and LSTM*.
Acta Polytechnica Hungarica **20**(7), 105-123, 2023,
http://dx.doi.org/10.12700/APH.20.2.2023.2.6,

[9] Barthélemy, J.; Verstaevel, N.; Forehead, H. and Perez, P.: *Edge-Computing Video Analytics for Real-Time Traffic Monitoring in a Smart City.*
Sensors **19**(9), 1-23, 2019,
http://dx.doi.org/10.3390/s19092048,

[10] Ruiz Salvador, L.C.; Phuoc Dai, N.H. and Rajnai, Z.: *SCADA Systems: Security Concerns and Countermeasures.*
IEEE 21st World Symposium on Applied Machine Intelligence and Informatics. IEEE, Herlany, 2023,
http://dx.doi.org/10.1109/SAMI58000.2023.10044495,

[11] Tokody, D.; Albini, A.; Ady, L.; Rajnai, Z. and Pongrácz, F.: *Safety and Security through the Design of Autonomous Intelligent Vehicle Systems and Intelligent Infrastructure in the Smart City*.
Interdisciplinary Description of Complex Systems **16**(3-A), 384-396, 2018,
http://dx.doi.org/10.7906/indecs.16.3.11,

[12] Houichi, M.; Jaidi, F. and Bouhoula, A.: *Analysis of Smart Cities Security: Challenges and Advancements.*
15th International Conference on Security of Information and Networks. IEEE, Sousse, 2022,
http://dx.doi.org/10.1109/SIN56466.2022.9970494,

[13] Nafrees, A.C.M.; Sujah, A.M.A. and Mansoor, C.: *Smart Cities: Emerging technologies and Potential solutions to the Cyber security threads.*
5th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques. IEEE, Mysuru, 2022,
http://dx.doi.org/10.1109/ICEECCOT52851.2021.9707994,

[14] Ekler, P.; Levendovszky, J. and Pasztor, D.: *Energy Aware IoT Routing Algorithms in Smart City Environment.*
IEEE Access **10**, 87733-87744, 2022,
http://dx.doi.org/10.1109/ACCESS.2022.3199757,

[15] Sándor, B. and Rajnai, Z.: *Cyber Security Analysis of Smart Buildings from a Cyber Security Architecture Point of View.*
Interdisciplinary Description of Complex Systems **21**(2), 141-147, 2023,
http://dx.doi.org/10.7906/indecs.21.2.2,

[16] Mugarza, I.; Amurrio, A.; Azketa, E. and Jacob, E.: *Dynamic Software Updates to Enhance Security and Privacy in High Availability Energy Management Applications in Smart Cities.*
IEEE Access **7**, 42269-42279, 2019,
http://dx.doi.org/10.1109/ACCESS.2019.2905925,

[17] Himdi, T.; Ishaque, M. and Ikram, M.J.: *Cyber Security Challenges in Distributed Energy Resources for Smart Cities.*
9th International Conference on Computing for Sustainable Global Development. IEEE, New Delhi, 2022,
http://dx.doi.org/10.23919/INDIACom54597.2022.9763107,

[18] Rele, M. and Patil, D.: *Enhancing Safety and Security in Renewable Energy Systems within Smart Cities.*
12th International Conference on Renewable Energy Research and Applications. IEEE, Oshawa, 2023,
http://dx.doi.org/10.1109/ICRERA59003.2023.10269395,

[19] Muha, L. and Krasznay, Cs.: *Managing the security of electronic information systems.* In Hungarian.
Nemzeti Közszolgálati Egyetem, Budapest, 2014,

[20] Demertzi, V.; Demertzis, S. and Demertzis, K.: *An Overview of Cyber Threats, Attacks and Countermeasures on the Primary Domains of Smart Cities.*
Applied Sciences **13**(2), No. 790, 2023,
http://dx.doi.org/10.3390/app13020790,

[21] Altaleb, H. and Rajnai, Z.: *Malware Attacks on SCADA Systems: Assessing Risks and Strengthening Cybersecurity Measures.*
IEEE 21st Jubilee International Symposium on Intelligent Systems and Informatics. IEEE, Pula, 2024,
http://dx.doi.org/10.1109/SISY60376.2023.10417951,

[22] Čergeť, M. and Hudec, J.: *Cyber-Security Threats Origins and their Analysis.*
Acta Polytechnica Hungarica **20**(9), 23-41, 2023,
http://dx.doi.org/10.12700/APH.20.9.2023.9.2,

[23] Szádeczky, T.: *Water 4.0 in Hungary: Prospects and Cybersecurity Concerns.*
Acta Polytechnica Hungarica **20**(7), 211-230, 2023,
http://dx.doi.org/10.12700/APH.20.7.2023.7.12,

[24] Pető, R. and Tokody, D.: *Building and Operating a Smart City.*
Interdisciplinary Description of Complex Systems **17**(3-A), 476-484, 2019,
http://dx.doi.org/10.7906/indecs.17.3.6,

[25] Hankó, V.: *Cybersecurity of SCADA Systems from Critical Infrastructure Aspect*. In Hungarian.
Hadmérnök **18**(3), 145-160, 2023,
http://dx.doi.org/10.32567/hm.2023.3.10,

[26] Solic, K.; Velki, T.; Fosic, I. and Vukovic, M.: *Study on Information Security Awareness using the Behavioral-Cognitive Internet Security Questionnaire.*
Acta Polytechnica Hungarica **21**(4), 49-68, 2024,
http://dx.doi.org/10.12700/APH.21.4.2024.4.3,

[27] Kralovánszky, K.: *A villamosenergia-rendszer kiber- és nemzetbiztonsági kockázatai.*
Nemzetbiztonsági Szemle **7**(3), 40-57, 2019,
http://dx.doi.org/10.32561/nsz.2019.3.4,

[28] Ferencz, K.; Domokos, J. and Kovács, L.: *Cloud Integration of Industrial IoT Systems. Architecture, Security Aspects and Sample Implementations.*
Acta Polytechnica Hungarica **21**(4), 7-28, 2024,
http://dx.doi.org/10.12700/APH.21.4.2024.4.1,

[29] Cheng, Z.; Sivaparthipan, C.B. and Muthu, B.: *IoT based smart and intelligent smart city energy optimization*.
Sustainable Energy Technologies and Assessments **49**, No. 101724, 2022,
http://dx.doi.org/10.1016/j.seta.2021.101724,

[30] Répás, S. and Rajnai, Z.: *The Role of Virtual Power Plants in Energy Supply and their Cybersecurity Issues*. In Hungarian.
6. Báthory-Brassai Konferencia. Obuda University, Budapest, 2015.