Methods for Analyzing and Increasing Cyber Resilience of Smart Energy System Facilities

I.S. Demidov*

Melentiev Energy Systems Institute of Siberian Branch of Russian Academy of Sciences, Irkutsk, Russia

Abstract — **Energy systems are currently undergoing digital transformation. The establishment and development of an intelligent energy system involves new information technologies for monitoring, controlling, measuring, and transmitting data to control and manage power flows. However, in addition to all the advantages to be gained using modern information technology, it becomes possible to carry out cyber-attacks on energy facilities. The purpose of this work is to review methods designed to analyze and enhance the cyber resilience of Smart energy system (SES) facilities. Various methods have been used to date, which, to one degree or another, can be used to achieve the above goal. The paper discusses in detail the methods, which can be utilized to:**

- **evaluate the risk of cyberattack;**
- **assess the consequences of cyberattacks;**
- **counteract cyberattacks;**
- **assess cyber situational awareness, and the ways to increase the cyber resilience of SES facilities.**

The paper also presents the problems facing information security and their causes, and proposes solutions to improve cyber security of electric power facilities.

Index Terms: **smart energy system, cyberattack, cybersecurity, resilience of energy system.**

* Corresponding author.
E-mail: demidov.is96@mail.ru

http://dx.doi.org/10.25729/esr.2023.03.0007

Received May 20, 2023. Revised September 13, 2023. Accepted September 20, 2023. Available online October 25, 2023.

I. Introduction

Smart energy system is an integration of classical technologies for energy generation, conversion, transmission and distribution, and modern information and communication computer technologies. Numerous operating parameters to be controlled and structure of the SES require the development and massive implementation of reliable, secure (protected from various kinds of interference), and high-speed information transmission systems. However, this creates conditions for accidental and uncontrolled impacts on the SES components and facilities. There is a possibility of cyber-attacks on energy facilities, and in this regard, the issue of cyber security is acute [1].

The concept of cybersecurity includes the prevention of damage, unauthorized use of information- communication networks and systems, and the information contained in them; the operation with guaranteed confidentiality, integrity, and availability of information, as well as its restoration and recovery of data communication networks in the event of a malicious attack or natural disaster. The main objective of the cybersecurity system in the electric power industry is to protect it against deliberate violations of information and technological security that can be launched by employees of the energy company, industrial spies, or other persons interested in hacking and penetrating the automated process control system (APCS) of the SES facility.

The advent of the first APCS at energy facilities brought about a pressing need to ensure cybersecurity. Cybersecurity threats at the information control system (ICS) level can be posed as weak points where system control can be accessed. The main types of information security threats in APCS are:

- Threats of unauthorized access to critical information by intruders – 57%;

- Threats of malware introduction into software and hardware components of automated process control systems – 36%;
- Threats of network attacks such as "denial of service" – 7% [2].

A “successful” cyber-attack allows attackers not only to obtain confidential data about the production process, but also to stop it. In this regard, the past few decades have seen actively conducted research on this topic. The study and analysis of the vulnerabilities of the ICS and its response to external influences, and the development of protection measures can significantly reduce and even prevent the risk of occurrence and development of the possible consequences. To this end, various methods for analyzing the cybersecurity of an energy facility are currently being developed [3–9], which are part of a more general method that considers the problem of cyber-physical stability of objects.

II. Methods for Analyzing the Cyber Resilience of SES Facilities

1.1 Methods for evaluating the risk of CAs

A cybersecurity system should be constructed so that it could be possible to take into account the implementation of cyber-attacks on the control systems of energy and industrial facilities from various sources, among which are the following [2]:

1. Internal (employees, suppliers, contractors);
2. External random (undirected);
3. External intentional (directed).

The main goals of cyber-attacks on the control systems of SES facilities are:

- to disrupt the production process by blocking or replacing information flows;
- to cause damage, blockage or shutdown of equipment, which may lead to a stoppage of production, a threat to human life or a negative impact on the environment;
- to use a disguise by sending erroneous information to operators, stimulating them to perform erroneous actions, which may be accompanied by negative consequences;
- to recommend to change the software configuration or equipment settings to disable SES components and systems;
- to transfer malware to the system (software designed to penetrate a computer without the informed consent of its owner);

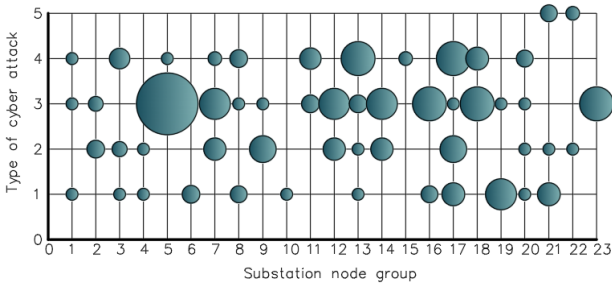


Fig. 1. Economic impact assessment diagram **[12].**

- to change the settings of security systems.

Examples [10, 11] provide several methods for analyzing possible cyber-attacks on SCADA systems. The paper [10] presents a method for measuring the risk of attacker’s manipulation of the system control process, the consequences of a violation of a controlled physical process, as well as the vulnerability of a SCADA system to malicious intrusion. This method involves applying Petri net’s state coverability analysis combined with the modeling process. These problems are solved by determining first the potential process failure conditions and examining the operational consequences of each process failure. Secondly, the SCADA failure modes that can cause corresponding process crash are found out for each identified process failure. Finally, we identify for each SCADA failure the network resources over which an adversary would need to exert control in order to induce the corresponding SCADA failure. Considering the initial state of a network attack, the method provides for the identification of network resources through which an attacker can potentially gain control. Thus, the risk is measured as a failure of process operational consequences function and propensity to induce process failure due to an attacker gaining control over the network resources during an attack.

In the paper [11], authors propose a mathematical model for determining the financial losses resulting from CAs on a computer-based information system used in industrial plants. The study suggests seven possible types of attacks (replay capture, spoofing, denial of service, etc.) and indicates six types of losses that an attack can cause (control loss, product loss, staff time loss, etc.) along with the probability of the type of loss for each type of CAs. The paper presents a formula for calculating the losses of each type. The cost of prevention, for example, is calculated as the product of the cost of upgrading the components that are resistant to a certain type of attack and the probability of loss of prevention for a given type of attack. Ultimately,

the total estimated loss of income from all types of CAs can be calculated using the model presented in the paper.

1.2. Methods for assessing CA consequences

Successful CAs can differ in their consequences and methods of action. The paper [12] presents a method for assessing the technological consequences of cyberattacks. This technique is designed to identify the nodes and objects of the energy system with the most severe economic consequences from cyber-attacks. In addition, this technique makes it possible to determine approaches to choosing the optimal architecture to build operational safety systems for energy facilities.

The method consists of the following steps:

1. Analysis of primary and secondary equipment;
2. Analysis of the CA types;
3. Calculation of cost indicators;
4. Construction of an evaluation diagram (Fig. 1).

To apply this method, it is necessary to understand which SES components are susceptible to CAs. The paper considers a 500/220/10 kV digital substation as an example. The following groups of nodes of this substation were identified separately for each voltage class:

1. Switching equipment;
2. Digital current and voltage transformers;
3. Converters of discrete signals;
4. Relay protection and automation equipment;
5. Bay controllers;
6. Process bus communication front-end equipment;
7. Measuring equipment;
8. Time server;
9. Station bus communication front-end equipment;
10. Telemetry controllers;
11. SCADA server;
12. Workstation (AWP);
13. Communications equipment.

This method also requires information about the types of possible CAs (for example, spoofing, DDoS attack, classical file virus infection, etc.) that can be applied to SES components.

The parameters determined for each group of nodes are:

1. Potential for a CAs;
2. Possible technological violations;
3. The timing of the CA consequences.

In addition, this method can be used to assess the cost of restoring components after CAs have happened. Calculation of the cost indicators of the CA consequences with this method takes into account the following:

1. Costs of emergency recovery work to repair failed equipment;
2. Shortfall in the compensation for electricity losses;
3. Additional costs of the electricity generation and transmission;
4. Economic damage due to false information transmitted to remote control.

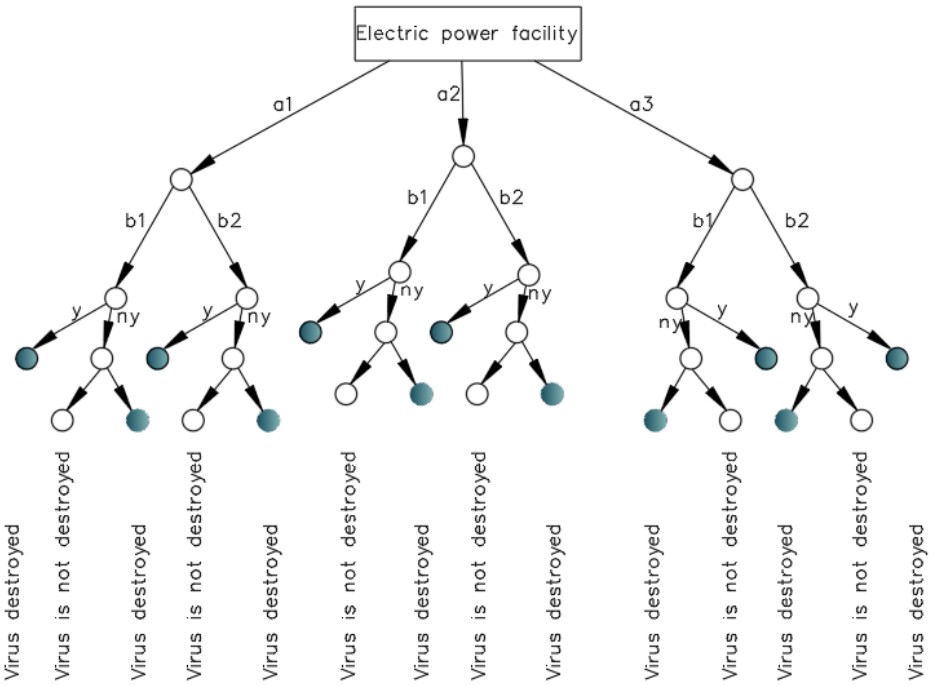


***Fig. 2. Tree of possible outcomes of a hacker attack* [1].**

Based on the data obtained above, a diagram (Fig. 1) is constructed to show the nodes of electric power facilities to encounter the most severe economic consequences of CAs.

1.3. Methods for counteracting CAs

The methods designed to simulate a CA on an energy facility are also common. The process of simulation involves development of various attack scenarios and assessment of the damage of their consequences.

The paper [1] describes the process of modeling the neutralization of hacker attacks by building a tree of possible outcomes (Fig. 2).

It is assumed that Party A (hacker) attacks the APCS system of an electric power facility by infecting it with a virus, and uses three options of viruses: a1, a2, a3. Party B organizes defense in two ways: b1, b2. Move 1: Party A chooses one of the attack options a1, a2, a3. Move 2: Party B chooses one of the options b1, b2 to protect the object. Move 3 (random): the information security system bj destroys (y) or does not destroy (ny) the virus ai. If the ai virus is neutralized, the game is over. If the ai virus has broken through to the APCS system, then the next move follows.

Each path from the initial vertex to the final vertex corresponds to one of the game variants. The number of possible game variants (games) is equal to the number of pendant vertices. As seen from Fig. 2, there are 18 possible games in the considered game. The marked 12 pendant vertices correspond to favorable outcomes of the game, when the protection of the electric power facility is effective.

This model can be used to simulate a cyber-attack on a designed or already built energy facility in order to find weaknesses in protection systems.

1.4. Methods for assessing cyber situational awareness

It is also important to emphasize that the vulnerabilities of energy facilities to CAs are currently being investigated within the framework of an approach called cyber situational awareness (CSA) [13–15]. CSA is a field of research related to the application of artificial intelligence methods in the field of cybersecurity, aimed at increasing awareness of possible situations of cybersecurity breaches and automatic detection of cyber threats. The paper [15] presents a method for analyzing CSA of an energy facility, which includes the following steps:

1. Analyze cyber threats of energy infrastructure;
2. Model scenarios of extreme situations in the energy sector caused by the implementation of cyber threats;
3. Assess the risks of violating the cybersecurity of the energy infrastructure.

Within the framework of the methodology, the authors propose to apply semantic methods to analyze the impact of cyber threats on energy facilities in terms of energy security. The semantic methods show their high performance in the absence or incompleteness of data when modeling the behavior of systems that cannot be formally described or fairly accurately predicted. An approach to the analysis of CSA of energy objects is presented as a synthesis of cybersecurity and situational awareness studies, characterized by the use of semantic modeling.

III. Information Security Problems Facing Electric Power Facilities and Their Causes

Nowadays, the computing systems of power facilities have a high degree of integration and widely use digital communications based on open international standards, such as IEC 60870, IEC 61850, and IEC 61970. Increasing the connectivity and awareness of individual subsystems made it possible to significantly boost the capabilities of protection and control systems, to make them smarter and more efficient to use. Furthermore, the use of standardized approaches and tools has significantly reduced the cost of integration and ensured a higher degree of functional reliability.

Specialists of the Kaspersky Laboratory published a report on the information security problems at electric power facilities and their causes [16].

2.1 Open communications

Open and unsecured communication channels between the components of protection and control systems, as well as between power infrastructure facilities:

- Lack of authentication;
- Open standards and open data transfer;
- High detail of network communications;
- Communication with open networks.

2.2 Service personnel's lack of information security knowledge

A limited number of specialists maintain a large fleet of devices, which are situated at facilities that do not have permanent staff and are often distributed over a vast area. Moreover, these personnel often lack even basic knowledge in the field of information security:

- Privileged remote access from an untrusted network;
- Lack of password protection and user management policies;
- Outdated software;
- Service from unsafe workstations;
- Lack of regular control of hardware and software.

2.3 Information security requirements are not complied with

Devices, software, and systems based on them are developed and created without considering information security issues.

- Poor resistance to hacking;
- Incorrect or insufficient LAN security settings;
- Lack of protection of data transmitted through open channels;
- Lack of role-based access rights;
- Lack of solutions to control the launch of applications;
- Absence or insufficiency of tools for information security event registration.

2.4 Difficulties of contractor access control and differentiation

A common practice is to carry out certain types of maintenance by contractors. In this regard, the issue of providing temporary access to a limited amount of equipment without the possibility of influencing other parts of the system, as well as canceling such access upon completion of work, is essential.

2.5 Long service life of vulnerable components

The service life of devices and of control and protection systems is long (20–30 years). Thus, insecure systems that continue to be introduced at present will not be replaced until several decades later. A phased partial upgrade is extremely difficult, since secure solutions (for example, using encryption) are incompatible with conventional, vulnerable solutions. In view of the foregoing, there is obviously a systemic problem, which is as follows:

- Modern systems for protection and control of power system equipment are neither isolated from the outside world, nor are systems with a closed implementation;
- ACSs do not have sufficient built-in information security tools;
- Detection of illegitimate information impact, active or past, in the current context is organizationally and technically extremely difficult;
- If such an impact has been detected, it is not clear how to respond to it and what measures to take.

IV. Ways to Increase the Cyber Resilience of SES Facilities

In order to enhance the cyber resilience of SES facilities, it is necessary to eliminate the problems indicated in the second chapter. Cybersecurity is increased through such measures as fixing the vulnerability of access channels, introducing adequate information security procedures and processes, as well as using special technical solutions based on firewalls [1]. Since the functioning of SES facilities involves constant interaction of its constituent components, the effect of destabilizing factors that led to the failure of some components can have (and in most cases has) an impact on the performance indicators of components that are not directly affected by this effect. The flow diagrams of most of these objects are implemented with rather “rigid” structures, which allows external influences to spread (cascade development). Naturally, in this case, the reliability indices of both individual components and entire system are reduced, which can lead to a shutdown of the consumer's technological process or its transition to a partial operability mode. In accordance with the well-known approaches to improving the reliability of energy facilities and their components, it is not possible to duplicate all the components most vulnerable to the impact of destabilizing factors.

The paper [17] analyzes the ability of a digital substation (one of the key components of modern SES) to withstand cyber-attacks and restore its working state after their impact. The paper proposes the following steps to boost the resilience of such substations:

- Improve the quality of software for digital substation. In terms of authorization tools, access control, firewalls and other similar tools, various errors are found in the software every month, including those affecting its security. To increase security, it is necessary to guarantee the correctness of dedicated software for the digital substation.
- Provide functional decomposition and physical separation of information flows. Successful cyber-attack on certain digital substation nodes can disrupt many functions. This step would significantly reduce the damage from cyber-attacks.
- Enhance the quality of digital substation design. High-quality design of devices, modules, and programs, and then modeling of threats and attacks on these designed and upgraded devices, modules, and software will increase the cyber resilience of the digital substation.

At this stage, secure communication, strong user authentication, permission (access), logging and reporting should be thought out. Consideration of the most likely attack scenarios requires the identification of vulnerabilities in network services and applications, as well as the assessment of the degree of resilience of network components and possible damage. When modeling attacks on link layer protocols, the cyber resilience of the network at the link layer level should be checked. It is crucial to involve top cybersecurity experts when developing and testing equipment and software for the digital substation. Ensuring cyber resilience of the digital substation in the face of cyber threats, should involve, at least, the following steps:

- Carrying out dynamic analysis of network and application traffic of the TCP/IP protocol stack, and using intrusion detection and prevention systems, since well-known anti-virus programs and firewalls are effective only for protecting obvious network access points.
- Providing correct configuration of firewalls, especially those enabling access to global networks. This can be achieved by organizing inter-network separation using simplex channels instead of duplex ones, with appropriate communication protocols, converting digital information to analog signals, and then analog signals back to digital information.
- Performing regular technological testing to identify existing vulnerabilities in IT infrastructure components for the corporate network perimeter (external test) and for internal resources (internal test).
- Checking the stability of routing, etc.
- Using High Availability Seamless Redundancy and Parallel Redundancy Protocol, the latest additions to the IEC 62439 standard for high availability industrial Ethernet networks. Designed for mission-critical and time-sensitive applications such as substation automation and traffic control, HSR and PRP provide guaranteed behavior in harsh environments and increased network reliability.
- Ensuring remote configuration/parameterization, monitoring, remote SCADA communication, remote diagnostics and firmware updates are becoming important requirements for intelligent electronic devices (IEDs). The security of the communication line is an imperative condition for remote firmware updating.
- Providing network segmentation and protection of remote communication channels by creating encrypted tunnels to prevent an intruder from having full access to device settings.

V. Conclusion

The creation and development of a smart energy system involves the introduction of new computer technologies for controlling, measuring, and transmitting data for monitoring and managing operation of the system. However, in addition to all the advantages gained through these implementations, the vulnerability of energy facilities to cyberattacks increases. Therefore, apart from the conventional challenges of enhancing the efficiency of electricity production, conversion, transmission, and distribution; and improving reliability, security, and resilience of smart energy systems, it is also crucial for them to address the concerns regarding their cybersecurity. This paper presents a review of modern methods for analyzing the cyber resilience of SES facilities and the methods to improve it.

VI. Acknowledgement

The study was carried out within the framework of the State assignment project (No. FWEU-2021-0001) of the program of fundamental research of the Russian Federation for 2021–2030 (Reg. No. AAAA-F21-121012190027-4).

References

[1] B. V. Papkov, P. V. Ilyushin, A. L. Kulikov, *Reliability and efficiency of modern power supply: monograph*. Nizhny Novgorod, Russia: Scientific Publishing Center "XXI century," 2021, 160 p. (In Russian)

[2] B. V. Papkov, A. L. Kulikov, V. L. Osokin, *Cyber threats and cyberattacks in the electric power industry: textbook*. Nizhny Novgorod, Russia: Nizhny Novgorod Institute of Management (Branch of RANEPA), 2017, 80 p. (In Russian)

[3] N. I. Voropai, I. N. Kolosok, E. S. Korkina, “Estimation of the stability of the software-computer complex for assessing the state in the conditions of cyberattacks,” in *Methodological problems of reliability study of large energy systems*, vol. 69, book 2, Irkutsk, Russia, 2018, pp. 9–18. (In Russian)

[4] I. Kolosok, E. Korkina, L. Gurina, “Vulnerability analysis of the state estimation problem under cyberattacks on WAMS,” in *Proc. Intern. Conf. on Problems of Critical Infrastructures*: *Joint 6th Conference of International Institute for Critical Infrastructures and 6th International Conference on Liberalization and Modernization of Power Systems*, Saint Petersburg, Russia, 2015, pp. 73–84.

[5] J. Yu, A. Mao, Z. Guo, “Vulnerability assessment of cyber security in power industry,” in *Proc. Power systems conference and exposition (PSCE)*, IEEE, 2006, pp. 2200–2205.

[6] D. Gertman, R. Folkers, J. Roberts, “Scenario-based approach to risk analysis in support of cyber security,” in *Proc. 5th International Topical Meeting on Nuclear Plant Instrumentation Controls, and Human Machine Interface Technology*, Albuquerque, NM, USA, 2006.

[7] J. Song, J. Lee, C. Lee, K. Kwon, D. Lee, “A cyber security risk assessment for the design of I&C Systems in nuclear power plants,” *Nucl. Eng. Technol*., vol. 44, no. 8, pp. 919–928, 2012.

[8] J. D. Markovic-Petrovic, M. D. Stojanovic, “An improved risk assessment method for SCADA information security,” *Elektronika ir Elektrotechnika*, vol. 20, no. 7, pp. 69–72, 2014.

[9] Ming-Chang Lee, “Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method,” *International Journal of Computer Science & Information Technology (IJCSIT)*, vol. 6, no. 1, pp. 29–45, 2014. DOI: 10.5121/ijcsit.2014.6103.

[10] M. H. Henry, R. M. Layer, K. Z. Snow, D. R. Zaret, “Evaluating the risk of CAs on SCADA systems via Petri net analysis with application to hazardous liquid loading operations,” in *Proc. IEEE Conference on Technologies for Homeland Security, HST '09*, IEEE, 2009, pp. 607–614.

[11] S. Patel, J. Zaveri, “A risk-assessment model for CAs on information systems,” *Journal of Computers*, vol. 5, no. 3, pp. 352–359, 2010.

[12] A. Voloshin, N. Lebedeva, “Transition from the coordinate system "integrity, confidentiality, availability" to the coordinate system "underdelivery, recovery time, damage",” presented at *International Conference and Exhibition “Protection and Automation for Electric Power Systems*, Moscow, Russia, Sep. 29 – Oct. 1, 2021.

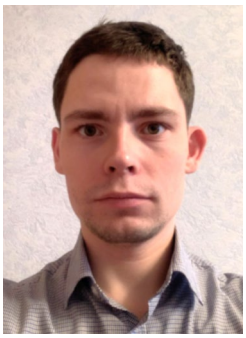
[13] U. Frank, J. Brynielsson, “Cyber Situational Awareness – A systematic review of literature,” *Computers & Security*, vol. 46, pp. 18–31, 2014. DOI: 10.1016/j.cose.2014.06.008.

[14] Y. Cheng, J. Deng, J. Li, S. A. DeLoach, A. Singhal, X. Ou, “Metrics of Security,” in *Cyber Defense and Situational Awareness. Advances in Information Security*, vol. 62, A. Kott, C. Wang, R. Erbacher, Eds. Springer, Cham, 2014. DOI: 10.1007/978-3-319-11391-3_13.

[15] D. A. Gaskova, A. G. Massel, “The Method of Cyber Awareness Analysis of an Energy Facility,” *Vestnik NSU. Series: Information Technologies*, vol. 19, no. 2. pp. 17–28, 2021. DOI: 10.25205/1818-7900-2021-19-2-17-28. (In Russian)

[16] Cyber security of electric power infrastructure. [Online] Available: https://ics.kaspersky.ru/media/KICS-for-Energy-WhitePaper-RU.pdf. Accessed on Aug. 05, 2022. (In Russian)

[17] N. I. Voropai, I. N. Kolosok, E. S. Korkina, “An increase in cyber resilience of digital substation,” *Relay Protection and Automation*, no. 1(34), pp. 78–83, 2019. (In Russian)



Ivan Demidov received Bachelor’s degree (2018) and Master’s degree (2020) in Electrical Power and Electrical Engineering from Irkutsk National Research State Technical University. Currently, he is a postgraduate student at the Melentiev Energy Systems Institute of the Siberian Branch of the Russian Academy of Sciences. I. Demidov also holds the position of a leading engineer of the Power Supply and Automation Department at JSC SibVAMI (UC RUSAL).