# Assessment of risks due to cyberattacks on information and communication infrastructure of cyber-physical system in the electric power system control[1]

*Irina* Kolosok[1,2], *Liudmila* Gurina[1,*]

[1]Melentiev Energy Systems Institute SB RAS, Irkutsk, Russia
[2]Irkutsk National Research Technical University, Irkutsk, Irkutsk region, Russia

**Abstract.** The paper proposes an approach to risk assessment in the electric power system control to identify possible failures in the electric power system functioning caused by cyberattacks on SCADA systems and WAMS. There is a large number of information, hardware and software factors, which increase the automated dispatching control system vulnerability to cyberattacks. The study shows the influence of unforeseen cyber-incidents in the information and communication infrastructure on electric power systems through false control actions on their physical part. The effectiveness of the developed risk assessment approach is demonstrated by its performance under uncertainty.

## 1 Introduction

The digital transformation of the energy industry is aimed at creating an intelligent energy system (IES) with cyber-physical infrastructure based on digital (information) models [1]. The wide-scale use of information and communication technologies and the adoption of synchronized vector measurement technologies increase the controllability and observability of electric power systems (EPSs), thus providing their reliable and efficient operation [2,3]. Apart from the undoubted advantages of these changes, the number of cybersecurity vulnerabilities is increasing due to the growing scale and complexity of EPSs, the information interaction between the EPS information-communication and physical subsystems, the possibility of hidden threat occurrence when using hardware and software, and a great number of tools and devices for measuring, transmitting and processing information at all levels of hierarchy of the automated dispatching control systems of EPS. The integration of new information-communication technologies with the existing ones creates new cyber threats to the EPS control. Cyberattacks at the information and communication level can lead to control errors, power supply interruptions, delayed system restoration, and other adverse consequences. The need to provide and maintain reliable operation of the EPS requires an analysis and assessment of risks in the EPS control, which are created by possible cyberattacks on the measuring, information transmitting and processing devices, which constitute the SCADA systems and WAMS. Such cyberattacks can lead to generation of incorrect control actions and cause EPS malfunction.

In this regard, the paper proposes an algorithm for assessing risks in the EPS control due to cyberattacks on SCADA systems and WAMS, given the preservation of their cybersecurity properties. The development of the algorithm rested on the theory of fuzzy sets and probability theory.

The effectiveness of the approach developed for risk assessment is confirmed by its verification under the conditions of uncertainty caused by the lack of statistics on cyberattacks on SCADA systems and WAMS.

## 2 Cyber-physical electric power system and its cyber-vulnerability

The electric power system development based on the adoption of new information and communication technologies and digitalization of the electric power industry has led to the creation of a cyber-physical system that consists of information - communication and physical subsystems.

The efficiency of dispatching control of complex EPSs is provided by multiple-stream constantly updated and reliable data. The specific parameters and state variables of EPS are measured, processed, transmitted, analyzed and visualized by SCADA systems and WAMS, which are part of the information-communication system using modern technical means, which also produces, transmits and implements the necessary control actions.

[1] This study is supported by the Siberian Branch of the Russian Academy of Sciences (Project III.17.4.2) of the Federal Program of Scientific Research (№ AAAA-A17-117030310438-1).

[*] Corresponding author: gurina@isem.irk.ru

Even in the present-day power systems, the physical and information-communication subsystems become comparable in complexity and responsibility in terms of normal functioning of electric power systems and increasing requirements of consumers for the power supply reliability and the quality of electricity supplied to them (in the future power systems this trend will persist to an even greater extent). In the context of EPS digitalization, it is increasingly necessary to consider complex integrated cyber-physical electric power systems that are characterized by new properties and face exacerbating reliability problems [4].

The SCADA and WAMS data are used to perform the control and monitoring functions with the aid of hardware and software of their components [5].

The data acquisition system transfers the RTU and PMU measurements and the information about the positions of switching devices (switches, disconnectors) to the real-time data processing system. The transmission system provides data transfer to control centers, interaction, and coordination of actions between operators in various control centers. The information processing system, in addition to data processing, also performs the EPS state estimation, which should provide a reliable picture of the system state based on measurements, pseudo-measurements, and information on the network topology. The graphical interface displays the results of state estimation and analysis of unforeseen situations. It also shows alert messages and provides access to other information about the system in real time.

Cyber incidents can occur in any of the described components of the information-communication infrastructure and cause a failure of control functions. In [6], the authors analyze and describe possible IES vulnerabilities.

The SCADA systems and WAMS are the most vulnerable to cyberattacks in the information-communication infrastructure. Since the control system affects the EPS through control actions or its output data, the consequences caused by cyber threat events in these systems pose the greatest danger to the EPS operation. This is because the control of EPS is based on the information from the SCADA systems and WAMS.

To reduce the dangerous consequences of cyberattacks for EPS, it is important to maintain the following cybersecurity properties of SCADA systems and WAMS [7]:

1. Timeliness of information. The SCADA systems and WAMS are rigid real-time systems [8, 9]. Transfer, receiving, and processing of data, as well as generation of control actions, are time-critical and must be done on time. This property means that any information should correspond to the current state of EPS.
2. Availability means that any component of the SCADA system and WAMS should be ready for use when needed.
3. Integrity requires that the data to be collected, transmitted, displayed, and stored in SCADA systems and WAMS be authentic and intact disregarding the unauthorized interference.
4. Cybersecurity is the ability of a system to constrain the local impact of cyberattacks, identify and delay the stream of corrupted data within the area vulnerable to cyberattack, without further transfer and use of these data in the control of a physical subsystem, in order not to cause emergencies leading to the development of system blackouts.
5. Confidentiality means that an unauthorized person should not have any access to the information related to a specific SCADA system and WAMS.

## 3 The effect of the information-communication infrastructure failures on the EPS operation

The reliable operation of EPS depends on the applied information and communication technologies in the automated control system. The power system itself becomes more vulnerable to information failures and cyber incidents in the information-communication infrastructure. Since the physical and information-communication systems are closely interconnected, the incompleteness and inaccuracy of information due to cyberattacks on SCADA systems and WAMS can lead to the generation and implementation of incorrect control actions and the development of emergencies in EPS. For example, false data injection attacks can lead to an incorrect EPS state estimation, which will negatively affect the correctness of control actions. Moreover, attackers, if not detected, can change the network topology and system state estimation. Table 1 shows the examples of possible malfunctions of the physical subsystem because of cyberattacks on the information-communication system, and their impact on the EPS control functions.

In order to prevent an EPS control failure, it is required to develop measures (techniques, tools, methods) to preserve the cyber-resilience properties of the system during cyberattacks. Solving this problem calls for an analysis and assessment of the factors influencing the control system, where the methods of risk theory are an important tool.

The assessment of risks during EPS control focuses on the information provided by SCADA systems and WAMS, given their cybersecurity properties.

## 4 An algorithm of risk assessment during EPS control based on the information factors

Threat and risk are the determining factors for cybersecurity. Threat is a potential cause that can lead to negative consequences for and damage to the system. Risk is the possibility of an undesirable outcome as a result of an incident, event or disturbance, as determined by its probability and the associated consequences. In fact, risk is a combination of the probability of threat event occurrence and its consequences (damage) with respect to a protected asset (resource). The consequences are determined by the level of effect [10, 11].

**Table 1.** Effects of cyberattacks on control functions and related consequences for EPS.

| **Threats** | **Information-communication system** | **Automated dispatching control system** | **Physical system** |
|---|---|---|---|
| False data injection | SCADA (RTU), WAMS (PMU, PDC), EMS, DMS, state estimation software. | Generation of incorrect control actions. Loss of frequency and voltage control. Loss of observability. Incorrect dispatching commands. False characteristics of failures will affect the distribution and transmission operations. | Stability loss. Short circuits (false line overload, sagging and overheating of wires).<br>Large fluctuations in the system dynamics:<br>- tripping of additional lines;<br>- shutdown of generators;<br>- load shedding. Blackout. |
| Time Synchronization Attacks (spoofing attacks, etc.) | WAMS (PMU, communication channels between PMU and PDC, GPS),<br>state estimation software. | False visualization of the current state, which leads to erroneous control and protection actions. Loss of frequency and voltage control. False information regarding the presence and location of a malfunction. A mismatch between the commands to switch off / operate smart devices. | Power outage, with a subsequent cascading chain of emergencies in the system. Loss of stability. |
| Denial of Service attacks (DoS jamming attacks, etc.) | SCADA (RTU), WAMS (PMU, PDC), EMS, DMS, state estimation software. | Delay in control. Generation of incorrect control actions. Loss of frequency and voltage control. Blocking of a control signal. Loss of observability. | Loss of stability. Increase in the system restoration time. Generation-load imbalance. Failure to disable/operate smart devices. |
| Replay, Distribution DoS attacks | SCADA (RTU), WAMS (PMU, PDC), state estimation software. | Control delay. Loss of observability. Violation of frequency and voltage control. | Loss of stability. |
| Coordinated Attacks | SCADA (RTU), WAMS (PMU), state estimation software. | All of the above. | Loss of stability. Cascade emergencies in the system. |
| Malicious software (Backdoor, Virus, worms, Trojan horse) | SCADA (HMI), WAMS. | Incorrect generation of control actions. Wrong operation of hardware and software. Loss of voltage and frequency control. | Unwanted tripping/operation of smart devices. Loss of stability. Voltage collapse. Blackout·. |

Information, software, and hardware, etc. can be considered as an asset. SCADA systems and WAMS are complex assets that include the above components. The possibility of vulnerability occurrence in the system assets is the main threat to cybersecurity.

The authors of [7] developed an algorithm for assessing the cybersecurity risks of information-communication infrastructure in the case of cyberattacks based on the theory of fuzzy sets. In this paper, the algorithm has been further developed and has undergone some changes in the semantic description of risk factors associated with the specific features of EPS control.

The risk assessment during the EPS control considers SCADA systems and WAMS as an asset. Loss of control is the damage caused by the cyber threat, which entails adverse consequences for the EPS operation.

The algorithm consists of two stages:

1. Assessment of risk during control for each cyber threat event;
2. Assessment of the resulting risk.

### 4.1 Risk assessment during control for each cyber threat event

The algorithm is based on the theory of fuzzy sets. To this end, input and output linguistic variables are defined.

The input linguistic variables are the intentions, capabilities, and purposes of an attacker; the vulnerability of the information-communication infrastructure; and the consequences determined by the level of impact on the information-communication infrastructure. The output linguistic variables (the probability of the threat initiation, the probability of a threat event, the probability of the threat event occurrence) are determined by the developed rules of the Mamdani Fuzzy Inference System (FIS), taking into account the recommendations [12].

A term set $\{VL, L, M, H, VH\}$ is defined (Table 2) and its semantic description is given for each risk factor [7]. A range of changes in the membership function in the segment $[0;1]$ is specified.

**Table 2.** A term set of risk factor.

| **Notation** | **Value** | **Range of membership function change** |
|---|---|---|
| $VL$ | Very low | $[0;0{,}4]$ |
| $L$ | Low | $[0{,}05;0{,}2]$ |
| $M$ | Moderate | $[0{,}21;0{,}79]$ |
| $H$ | High | $[0{,}8;0{,}95]$ |
| $CH$ | Critically high | $[0{,}96;1]$ |

Table 3 presents a semantic description of risk levels in EPS control.

**Table 3.** Risk levels.

| Level | Description |
|---|---|
| Very low risk | The threat event is expected to have a slight adverse effect on the EPS control. |
| Low risk | A threatening event may have a limited adverse effect on the EPS control; the consequences for functioning are local in nature. |
| Moderate risk | A hazardous event can have a serious adverse effect on the EPS control. |
| High risk | A threatening event can have a serious or catastrophic adverse effect on the EPS operation. |
| Critically high risk | A threat event can have numerous serious or catastrophic adverse effects on EPS operation. |

A hierarchical fuzzy system (Fig. 1) has been proposed for risk assessment during the EPS control, in which four systems of fuzzy logical inference $FIS1$, $FIS2$, $FIS3$, $FIS4$ are embedded. The factors such as the capabilities, intentions, and purposes of the attacker are used to assess the probability of threat initiation. Combinations of factors, such as the attacker capabilities and the information and communication infrastructure vulnerabilities, were used to assess the probability of a threat event as a result of adverse effect. Combination of these probabilities was used to determine the total probability of the threat event occurrence. The combinations of the probability of threats and the levels of impact (consequences) on SCADA systems and WAMS determine the risk estimate during the EPS control (Fig. 2).

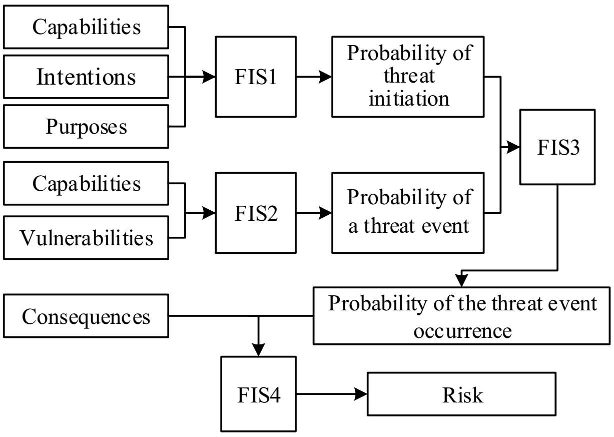
Capabilities
Intentions
Purposes
FIS1
Probability of threat initiation
Capabilities
Vulnerabilities
FIS2
Probability of a threat event
FIS3
Consequences
Probability of the threat event occurrence
FIS4
Risk

**Fig. 1.** Hierarchical fuzzy system of risk assessment during EPS control.

A matrix has been obtained to assess risk during EPS control (Fig. 2).

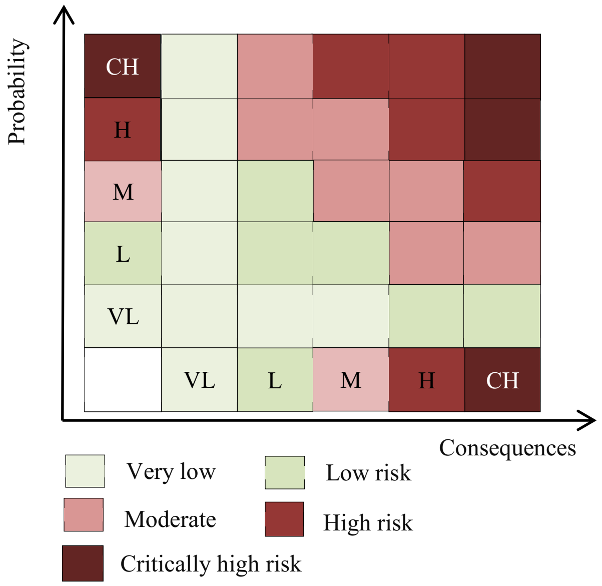

**Fig. 2.** Matrix of risk assessment during EPS control.

## 4.2 Assessment of a resulting risk

An error in the EPS control can be caused by several cyberattacks. Events of $i$-x cyber-threats ($i = \overline{1,n}$) are joint independent events (they may appear simultaneously and the probability of one threat event occurrence does not change depending on the other threat event occurrence [13]). In this case, the resulting risk estimate during control $R_c$ at $n$ cyberattacks is calculated according to:

$$\begin{aligned} R_c &= R_{c1} + R_{c2} + \ldots + R_{cn} - R_{c1}R_{c2} - \ldots - \\ &- R_{n-1}R_n + R_{c1}R_{c2}R_{c3} + \ldots + R_{cn-2}R_{cn-1}R_{cn} - \\ &- \ldots + (-1)^{n-1} R_{c1}R_{c2}..R_{c3}\ldots \quad , \end{aligned} \tag{1}$$

where risk under the $i$-th cyberattack $R_{ci}$ is calculated according to the method presented in the previous section (Figs.1,2).

The obtained cyberattack-related risk assessments can be useful in choosing the models and methods of processing SCADA and WAMS data streams in real time, which could provide the necessary completeness and reliability of the information [14, 15] used for EPS control.

## 5 Case study

To assess the risk during EPS control, we considered a jamming attack (a type of DOS attack) and a spoofing attack (a type of time synchronization attack) [16] on WAMS.

Table 4 shows the values of the input linguistic variables for each cyberattack.

**Table 4.** Input linguistic variables.

| | **Jamming-attack** | **Spoofing-attack** |
|---|---|---|
| **Capabilities** | 0.75 | 0.97 |
| **Intentions** | 0.76 | 0.92 |
| **Purposes** | 0.6 | 0.7 |
| **Vulnerabilities** | 0.85 | 0.92 |
| **Effects** | 0.92 | 0.93 |

The values of the output linguistic variables are obtained according to the rules of fuzzy inference of systems $FIS1$, $FIS2$, $FIS3$, $FIS4$ (Table 5).

**Table 5.** Input linguistic variables.

| | **Jamming-attack** | **Spoofing-attack** |
|---|---|---|
| **Probability of threat initiation** | 0.63 | 0.81 |
| **Probability of threat event** | 0.76 | 0.81 |
| **Probability of threat event occurrence** | 0.69 | 0.75 |
| **Risk (see Fig. 3)** | 0.67 – the moderate level | 0.72 – the moderate level |

The resulting risk estimate $R_c = 0.91$, obtained according to (1), indicates a high level of risk and allows us to draw the conclusions (which are confirmed by the calculations) that successful joint jamming and spoofing attacks can cause far greater damage to the power system and cause more serious consequences for its operation (Table 1) than each of the cyberattacks individually.

## Conclusion

The proposed algorithm for risk assessment during EPS control in case of cyberattacks makes it possible to assess the consequences for the EPS functioning. It can also be useful to conduct further studies aimed at improving the quality of the information data streams required for monitoring and control, and to develop measures to enhance the cybersecurity of the entire EPS infrastructure.

## References

1. N.Voropai, M. Gubko, S. Kovalev, L. Massel, D. Novikov, A. Raikov, S. Senderov, V. Stennikov, Control Sciences, **1**, 2-14, (2019). doi: 10.25728/pu.2019.1.1
2. Remote control at substations: 330 kV Gubkin substation and 500 kV Shchelokov substation. Available at: http://digitalsubstation.com/blog/2018/06/27/teleupravlenie-na-podstantsiyah-ps-330-kv-gubkin-i-ps-500-kv-shhyolokov/
3. A. Zhukov, D. Dubinin, Releyshchik, **3**, 22-29, (2013)
4. N. Voropai, I. Kolosok, E. Korkina, A. Osak, Energy Policy, **5**, 53-61, (2018)
5. Yu. Ivanov, A. Cherepov, D. Dubinin, E. Satsuk, Energetik, **3**, 8-12, (2016)
6. B. Papkov, *Methodological problems in the reliability study of large energy systems. Research and provision of the reliability of energy systems,* **68**, 441–451, (2017)
7. I. Kolosok, L. Gurina, Information and Mathematical Technologies in Science and Management, **2 (14)**, 40-51, (2019). DOI: 10.25729/2413-0133-2019-2-04
8. B. Ayuev, P. Erokhin, Yu. Kulikov, *Technologies for controlling the operating conditions of energy systems of the 21st century: Collected papers of All-Russian Scientific and practical. conf.,* 83-92 (Novosibirsk: Publishing House of NSTU, 2006).
9. STO 59012820.35.240.50.004-2011. Dispatching control systems in the electric power industry. System of Supervisory Control And Data Acquisition (SCADA) in dispatching control. Available at: https://www.so-ups.ru
10. B. Papkov, A. Kulikov, *Cyber-threats and cyberattacks in the electric power industry*, (Nizhny Novgorod: NRU RANEPA, 2017)
11. A. Dorofeev, A. Markov, Voprosy Kiberbezopasnosti, **1(2)**, 67-73, (2014)
12. National Institute of Standards and Technology NIST Special Publication 800-30 rev. 1 (Sep. 2012), Guide for Conducting Risk Assessments. Available at: National Institute of Standards and Technology
13. E. Wentzel. *Probability Theory: Textbook for universities,* (5th ed. M.: Higher School, 1998)
14. I. Kolosok, L. Gurina, Voprosy Kiberbezopasnosti, **3 (27)**, 63-69, (2018) . doi: 1021681 / 2311-3456-2018-3-63-6915
15. I. Kolosok, L. Gurina, *2018 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM)*, (Moscow, Russia, 2018). doi: 10.1109/ICIEAM.2018.8728768
16. K. Gai, M. Qiu, Z. Ming, H. Zhao, L. Qiu, IEEE Transactions on Smart Grid, **8 (5)**, 2431-2439, (2017). doi: 10.1109/TSG.2017.2664043