Analysis of cyber vulnerabilities of the emergency control and relay protection to assess the reliability and survivability of electrical power systems in the era of total digitalization

Alexey Osak[1,*], *Daniil* Panasetsky [1], and *Elena* Buzina[1]

[1]ESI SB RAS, 664033 Lermontov str., 130, Irkutsk, Russia

Abstract. Cyber threats pose an increasing threat to energy objects. It is essential to ensure the cybersecurity of automatic control systems, such as relay protection devices (RP), devices of regime control (RC) and emergency control (EC), automated control systems. At the same time, the issues of cybersecurity include not only the problem of hacker attacks, but also the whole complex of problems relating to adequate functioning of cybernetic systems in the power industry. The authors consider two of the most acute aspects of cybersecurity in the energy systems of the future in the era of total digitalization: large-scale prepared cyber attacks on the electrical power systems (EPS) as a whole and large-scale cyber attacks on distribution networks with small-scale generation facilities and active consumers.

Introduction

Over the past decade, there have been active discussions on the topic of digital substations and the implementation of solutions for the power industry based on IEC 61850, and the process of introducing these technologies to power objects. In recent years, Russia has begun to open the active discussion about total digitalization and digital transformation of the power industry while also taking practical steps towards said digitalization [1-4]. In these conditions, the urgency of the problem of cybersecurity has significantly increased.

In addition to universal digitalization, the current trend in the modern electric power industry is active consumers, distributed low-power generation, including on renewable energy resources, and the emergence of new electric receivers, such as electric vehicles. All these trends lead to the fact that intelligent automatic control systems will appear in the distribution grid and small consumers [5], similar to those that are available or are being created within the main electric grids, large power plants and large industrial enterprises.

Against the background of rapidly changing external conditions, cyber threats pose an increasing threat to energy objects [6-8]. It is of great importance to ensure the cybersecurity of automatic control systems, such as relay protection devices, devices of regime and emergency control [9]. At the same time, the issues of cybersecurity include not only the problems of hacker attacks, but also the whole complex of problems of adequate functioning of cybernetic systems in the energy industry. It is important to pay attention to the influence of reliability and cybersecurity of digital subsystems on the overall reliability of power objects, EPS and their associations [10].

1. Reliability of digital control systems

Effective and adequate operational and emergency control is one of the factors determining the reliability of EPS. It is known that the operation of the EPS is possible only with appropriate continuous control, both over individual electrical installations and the EPS as a whole. Current trends lead to the fact that continuous automatic control is required not only for the system-forming electric grid and large-scale generation, but also distribution electric networks, distributed generation and active consumers should be involved and integrated in this automatic control.

Digital technologies allow you to create complex and flexible algorithms for operational dispatch and emergency control, covering many large and small power objects in the control loop. These capabilities of digital control systems, combined with a new generation of high -, medium-and low-voltage primary electrical equipment with high performance and monitoring and remote control capabilities, increase the overall reliability of the EPS.

At the same time, digital technologies and microprocessor technology are characterized by the possibility of a relatively simple change in functionality by reprogramming, which, when properly used, allows to improve technologies and control algorithms without replacing equipment, but also becomes the basis for new types of threats to the EPS – threats to cybersecurity. The versatility of communication networks and microprocessor devices allows them to solve any information problems, both useful and obviously malicious functions in the process of cyberattacks, which

* Corresponding author: osakalexey@mail.ru

could not be said about traditional devices, especially on an electromechanical basis. Therefore, block diagrams and the composition of software and hardware do not characterize the functionality of the control system (because similar software and hardware can create completely different control systems), especially in the process of a cyber attack, when the functionality of the devices may even change.

Cyberthreats [11] are executions not of the specified (required) functions, but of unintended functions, which can be interpreted as a partial or complete failure of the control system of the power object. Possible threats (disturbing factors) for electric power objects are named below [13-15]:

- internal threat:
  - undetected errors in algorithms and software, which result in information and control systems of the power object operating according to the wrong algorithm;
  - errors of operational personnel of the power object, which lead to incorrect changes in the mode of operation of the devices, to disabling the protection systems of external communication channels, to replacing the software with a non-project version, to infection with viruses, etc.
- external threat:
  - malicious software defects (Spyware) embedded in the software of microprocessor devices for the purpose of controlled system failure or unauthorized access to them;
  - cyberattacks from the outside, through external digital communication channels of the power object, by intercepting telemechanics and telecontrol channels, general corporate control channels or embedding malicious software code into control systems (virus infection).

Despite the importance of the aspect of protection from external threats, it is not the only one, just as the general concept of the term security is not limited to the state of protection against external threats only. An equally important aspect is to ensure protection against internal threats, which include flaws and errors in the software. By considering only external threats, one overlooks the shortcomings of the design and development of modern automatic and automated control systems. In previous works of the authors [16], an integrated approach was considered for qualitative analysis of the structure of RP, EC, and RC systems from the perspective of cybersecurity.

Most publications and regulatory documents dealing with cybersecurity of electric power objects focus on unauthorized, deliberate and malicious actions of certain individuals who seek to gain access to information, resources and means of the attacked party through cyberspace. No matter how the software and hardware that perform application and communication functions at power facilities are improved in resistance to cyberattacks, and no matter what additional special technical means are used to protect against cyberattacks, all this does not solve the problem of the human factor [12]. The problems of the human factor will be most acute when automating power distribution grids, at small distributed generation objects, and when integrating active consumers into the general control loop of the EPS regimes.

In recent years, the Russian Federation has adopted a number of laws and regulations in the field of cybersecurity, including those affecting the cybersecurity of critical information infrastructure, which can include automatic and automated control systems in the electric power industry. The relevant competent state organizations are working to solve the existing problems, including certification of hardware and software for protecting information from unauthorized access. But all this does not negate the problem of the human factor, which is aggravated by insufficient staff qualifications and staff turnover at a number of energy enterprises. Therefore, even the most stringent technical, organizational and administrative measures will not completely solve the problem of the human factor. This aspect is discussed in more detail later in the article.

2. The problem of targeted external cyberattacks

In the future, in the era of total digitalization, the situation may be aggravated by the fact that cyberattacks or other negative ways of affecting the digital infrastructure of critical infrastructure objects and systems, which include the power systems, will become elements of geopolitical and military confrontation [16], which is already publicly spoken about by senior officials of various countries of the world.

When targeted external cyberattacks are launched by foreign countries or large corporations, significant resources, both financial and human, are allocated to their implementation. The qualification of attacking hackers can be significantly higher than the qualification of most specialists in the power industry. If a cyberattack is blocked by technical means, it is possible to bribe, blackmail or deceive specialists at power objects, specialists of engineering companies or enterprises producing technical means for the power industry. In the context of the comprehensive use of smartphones, smart gadgets, social networks and other tools of digital communications, the task of bribery, blackmail or deception of specialists is greatly simplified if it is done by representatives of the special services of foreign countries. For these purposes, they have access to fairly complete information about the specialist, his family, interests, Hobbies, friends and so on. Contacts and information about close family members are available, including their current location, audio, photos, and videos. And here it is important to note that we are talking about the impact of foreign intelligence services on ordinary professionals, not on intelligence officers. Ordinary employees do not give the legally and morally binding oath at the workplace, do not have special training, etc. So if not this, so another specialist, if not this, so another object will succumb to bribery, blackmail or deception, respectively, open access, disable protection, etc. Therefore, the probability of a

successful attack of this sort is almost 100%. In this case, the preparatory stage will be invisible from the side of the energy object itself, i.e. the attack is likely to be unexpected.

These are typical problems of any defence, because the attacking side can concentrate all efforts on one area, attract the best specialists, allocate large funds for the attack. And not knowing place and time attacks, protection and defence will have provide on all objects and systems, that causes dispersion forces and funds, and as a consequence, natural lack of these forces and funds, in camping on champion personnel in place full-scale attacks.

Therefore, it can be concluded that if the hostile impact on the digital component of critical infrastructure facilities and systems become elements of geopolitical and military confrontation, then all echelons of cyber defence will be overcome in the point of a full-scale complex attack. The exception here can be only a few objects, which even in normal conditions apply super-strength in the field of cybersecurity.

Accordingly, we are no longer talking about repelling an attack on a typical power object, we are talking about minimizing the consequences and damage after a successful cyber attack. In this case, the magnitude of the expected damage in comparison with the cost of a massive cyber attack will be the criterion of whether or not a particular critical infrastructure will be attacked. Accordingly, measures to reduce possible damage will be an effective means of preventing cyberattacks [17].

As a result of a cyberattack of this kind, for one reason, you can get the following negative consequences:

- Simultaneous failure of a large number of digital devices RP, RC and EC of one manufacturer at one power object or a group of power objects located in the same information space that has a physical connection to the Internet or public access channels. However, logical defenses such as firewalls or routing can be disabled as part of this attack.
- Simultaneous failure of a large number of intra-and inter-site digital networks (channels) located in the same information space that has a physical connection to the Internet or public access channels.
- Simultaneous access to a large number of digital devices RP, RC and EC of one manufacturer at one power object or a group of power objects located in the same information space that has a physical connection to the Internet or public access channels. Use this access to change the settings and algorithms of operation or for remote control, including to create an emergency situation.

It is important to note that the principles of short-range and long-range redundancy in relay protection, as well as the principles of several echelons of emergency control do not imply simultaneous and mass failure of a large number of protections and automatics. Accordingly, there may be unrecoverable short circuit, operation of the equipment in overload mode and other emergencies that can lead to damage to the primary equipment.

Another dangerous consequence of a cyberattack of this kind is the long recovery time of the EPS. Given the complete dependence of all spheres of public life and the economy on the availability of electricity, the disruption of electricity supply to a large number of consumers at the same time with a long recovery time is already catastrophic.

Thus, universalism of digital solutions, unification of digital interfaces, hardware platforms, operating systems, availability of centralized administration tools, common information space at the physical level – significantly increase the likelihood of large-scale cyberattacks, as they increase the potential damage from a successful cyberattack [12, 16]. The heterogeneity of solutions, their incompatibility, lack of integration into a single information space – reduce the likelihood of large-scale cyberattacks, because the potential damage from a successful cyber attack is limited due to the limited number of devices and systems that can be subjected to this kind of attack.

Therefore, when building automatic control systems in the power industry in the era of total digitalization, it is necessary to adhere to the layered principle, where the systems of the last tier must be either isolated or minimally integrated into digital control systems. If an expensive cyber attack, requiring the participation of unique specialists-hackers, can not lead to significant damage, and will not lead to a significant increase in the recovery time of EPS after an accident caused by a cyber attack, then the feasibility of such an attack becomes far from obvious in a geopolitical or military confrontation.

Another possible solution to the problem is to install fixed functionality equipment (with fixed logic) on power objects to restrict access and interaction with external networks, the settings and operating modes of which cannot be changed by the power object staff without the use of specialized equipment. Accordingly, if you need to change the settings, such equipment is sent to the manufacturer (or to a specialized service center), where all changes are made in the factory using special devices. This approach somewhat complicates the operation, but it encourages better performance of work, and also significantly limits the influence of the human factor of the operating personnel of power objects in the event of a targeted cyber attack. This approach will be most appropriate for use in medium-capacity generating facilities, especially in distribution grids, small-scale generation objects, and active consumers, where there are problems with staff qualifications and staff turnover.

3. Cybersecurity challenges in the electric power industry of the future

In modern conditions, there is a mass construction of small power plants based on renewable energy sources, the installation of power storage devices is gaining momentum, consumers electrical installations are being modified (they are becoming adaptive and intelligent), and electric vehicles are being mass-produced.

Low-power gas generation (gas turbine power plants, gas-piston power plants) has problems with stability during emergency disturbances in the grid [5, 18], inverter generation has problems with overload capacity and in terms of switching from parallel operation to autonomous mode and back, and generation on renewable sources has problems with instability of energy resources. Small utility and household active consumers are not involved in operational dispatch control and the prospect of their involvement in the future is unlikely, so the nature and schedule of loads of active consumers with an autonomous control system is poorly predictable.

Without involving this small generation and active consumers in unified systems for controlling normal and emergency regimes of the EPS, both the overall system reliability of the EPS and the reliability of power supply to specific consumers will decrease [19].

As soon as the involvement of low-power power objects in a unified centralized or decentralized control system of EPS regimes begins, the whole range of cybersecurity problems immediately arises. Large energy companies are able to attract qualified and highly paid information security specialists, but even so, they still have problems with the human factor. And small-capacity electric power objects have and will have problems with personnel, and even more so in the field of cybersecurity.

Control systems for small generation and active consumers in the same energy district will probably be of the same type, with identical settings. Therefore, a successful cyberattack will not lead to the failure of a single electrical installation, which is not particularly critical, but to a mass failure across the entire energy district or the entire power system.

The problem is compounded by the fact that cybersecurity issues will be at the intersection of various enterprises and individuals (power grid and generating companies, Telecom operators and active consumers). All this will inevitably affect both the quality of the initial study of information security issues, and the efficiency of solving emerging issues. In any case, it will not be possible to achieve the indicators for the speed and quality of implementation of emergency measures that are available in the system-forming electric grids and at large power plants.

As noted above, the potential damage from a cyber attack determines the probability of organizing prepared cyber attacks, involving highly qualified hackers. Therefore, reducing potential damage is an effective way to reduce the risk of a cyber attack itself. The main way to reduce damage is to increase the speed of elimination of a possible accident caused by a cyber attack. Due to the lack of the required specialists, in the event of a successful cyber attack, it is unlikely that it will be possible to quickly restore the operability of control systems dispersed over many small objects in the distribution grids.

Therefore, when creating power systems of the future, involving low-power power objects in a unified centralized or decentralized control system of the EES regimes, it is necessary to initially work out ways to easily and quickly mode changes:

- active consumers to passive ones, by excluding of intelligent systems from the control cycle;
- low-power generation in local control mode, for example, with the function of maintaining the voltage level on the generator buses without issuing power to the external electrical grid (covering only its own load);
- local devices of regimes and emergency control in the distribution electric grid for autonomous control algorithms based on local parameters of the regimes.

In this case, if there is a real cyberattack that will lead to the failure of a unified centralized or decentralized control system of the EPS regimes or the mass failure of grass-roots control systems at low-power power objects, then each such power object can independently, by performing simple operations, switch to an autonomous control mode, and thereby quickly restore its power supply, ensure the operation of the distribution electric grid, even if not in the optimal, but quite acceptable regime.

Conclusion

The paper shows that cyber threats in the power industry should be understood not only as cyber attacks in the form of hacker activities, but also the whole complex of possible failures of the cybernetic control system, without which the power system is unable to function.

Situations with potentially possible cyber attacks initiated by foreign States or large corporations within the framework of a geopolitical confrontation are considered.

Possible new problems for the electric power industry of the future and features of ensuring cybersecurity in the conditions of involving low-power power objects in a unified centralized or decentralized control system of the regimes of electric power systems are considered separately.

The work was carried out within the project III.17.4.2 (No. AAAA-A17-117030310438-1) of the fundamental research program of the Siberian Branch of the Russian Academy of Sciences.

References

1. A.L. Teksler, “Power industry digitalization: from process automation to the digital transformation of the industry”, Energy Policy. № 5. 2018. p. 3-6. (in Russian)
2. D.V. Holkin, I.S. Chausov, “Digital transition in Russian power engineering: in search of meaning”, Energy Policy. № 5. 2018. p. 7-16. (in Russian)
3. Report “Digital Transition in the Electric Power Industry of Russia”, Ed. V.N. Knyaginin, D.V. Holkin. CSR, 2017. URL: https://www.csr.ru/wp-content/uploads/2017/09/Doklad_energetika-Web.pdf (in Russian)

4. The concept of "Digital transformation 2030", PJSC "ROSSETI", Moscow. 2018. 31p. URL: https://www.rosseti.ru/investment/Kontseptsiya_Tsifrovaya_transformatsiya_2030.pdf (in Russian)
5. Ilyushin P.V., Kulikov A.L. "Automatic control of normal and emergency modes of power districts with distributed generation", Nizhny Novgorod: The Russian Presidental Academy of National Economy and Public Administration; 2019, 364 p. (In Russian)
6. Massel' L.V., Voropay N.I., Senderov S.M., Massel' A.G., "Cyber Danger as One of the Strategic Threats to Russia"s Energy Security" Cybersecurity issues, 2016, №4 (17), p. 2-10. DOI: 10.21681/2311-3456-2016-4-2-10. (in Russian)
7. Papkov B. V., Kulikov A. L., Osokin V. L. "Cyber threats and attacks in electric power industry", N.Novgorod, NIU RANKhiGS, 2017, 80 p. (in Russian)
8. Papkov B.V., Kulikov A.L., Osokin V.L. "The problems of cybersecurity of the electrical engineering", The library of an electrical engineer. Appendix to the magazine "Energetik", Moscow: Energoprogress Publ., 2017, lssue 9 (225), 96 p. (In Russian).
9. Kulikov A. L., Osokin V. L., Papkov B. V., Shilova T. V. "The extension of the concept «reliability» in modern electric power industry", Bulletin NGIEI. 2018. № 3 (82). p. 88–98. (in Russian)
10. A.B. Osak, A.I. Shalaginov, D.A. Panasetsky, E.Ya. Buzina, "The impact of cybersecurity of power objectson the reliability of the EPS", Methodic problems of studies of reliability of large power systems, Eds. N.I. Voropai, Yu.Ya. Chukreev, Syktyvkar: LLC "Komi Republican Printing House", 2016, p. 377-385. (in Russian)
11. A.S. Alpeev, "Terminology of security: cybersecurity, information security", Cybersecurity issues, 2014, №5(8), p. 39-42. (in Russian)
12. A.B. Osak, A.I. Shalaginov, D.A. Panasetsky, E.Ya. Buzina, "Human factor in ensuring cybersecurity of power objects", Book of reports of international conference "Modern tendencies of System Development of Relay Protection and Automation of Power System", Sochi. 1-5 June 2015. (in Russian)
13. A.P. Doukhvalov, "Cyber attacks on critical facilities – the probable cause of the accident", Cybersecurity issues, №3(4), 2014, p. 50-53. (in Russian)
14. Voropaj N.I., Kolosok I.N., Korkina E.S., Osak A.B. "Cyberthreats and cybersecurity in electric power systems", in Proceedings of the All-Russian Sicence and Technology al conference "Power Engineering through the Eyes of Youth", Irkutsk, Russia, September 16–20, 2019, Vol.1. Pp. 32-37. (in Russian)
15. A.B. Osak, A.I. Shalaginov, D.A. Panasetsky, E.Ya. Buzina, " Reliability of emergency control and relay protection from the position of cybersecurity", Methodic problems of studies of reliability of large power systems, Eds. N.I. Voropai, ESI SB RASm 2018, Vol.2. p. 99-108. (in Russian)
16. Osak A., Panasetsky D., Buzina E. "Analysis of the emergency control and relay protection structures approached from the point of view of EPS reliability and survivability by taking into account cybersecurity threats", E3S Web Conf. Volume 139. 2019. Article Number 01029. DOI: 10.1051/e3sconf/201913901029.
17. A.B. Osak, A.I. Shalaginov, D.A. Panasetsky, E.Ya. Buzina, "Cybersecurity of power objects as a factor of EPS reliability", Methodic problems of studies of reliability of large power systems, Eds. N.I. Voropai, M.A. Korotkevich, A.A. Mikhalevich. – Minsk: Belarusian National Technical University, 2015, p. 258-264. (in Russian).
18. Ilyushin P.V. "Features of emergency control organization in networks with modern generating units". Proceedings of Irkutsk State Technical University. 2018, vol. 22, no. 5, pp. 134–151. DOI: 10.21285/1814-3520-2018-5-134-151. (In Russian).
19. Ilyushin P. V. "Prospects of using and problems of integrating distributed energy sources in grids", Moscow, Energoprogress Publ., 2020. 116p. (in Russian)