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

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 propose a methodical approach to the analysis of the structure of automatic means of regime and emergency control in terms of their impact on the reliability and survivability of power systems (EPS), taking into account the known threats to cybersecurity.

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, these discussions take place against the background of the process of introducing these technologies to power objects. Participating in these discussions, the authors repeatedly noted the presence of the problem of cybersecurity in the mass introduction of digital substation technologies. 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.

Against the background of rapidly changing external conditions, cyber threats pose an increasing threat to energy objects [5]. It is of great importance to ensure the cybersecurity of automatic control systems, such as relay protection devices, devices of regime and emergency control, automated control systems [6]. 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 power 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 [7].

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.

On the one hand, digital technologies make it possible to create complex and flexible algorithms for operational-dispatch and emergency control, which, combined with a new generation of primary equipment with high performance and monitoring and control capabilities, increases the overall reliability of the EPS. On the other hand, 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 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.

The subject of cybersecurity has become extremely popular in recent years, but in most publications and regulations on cybersecurity of power objects, the emphasis is on unauthorized, intentional and malicious actions of certain persons who seek to gain access to information, resources and means of the attacked party through cyberspace. No matter how the software and

* Corresponding author: osakalexey@mail.ru

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 [9].

While the aspect of protection against external threats is important, 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.

Cyberthreats [10] 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 [11]:

- 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).

A comprehensive approach for common analysis of the structure of RP, RC and EC systems from the perspective of cybersecurity is proposed.

2. Approach for general assessment of reliability of modern RP, RC and EC systems from the cybersecurity perspective

The assessment of reliability of any system is connected with an assessment of probability and scales of consequences of failures of elements of system. The following types of failures can be distinguished for automatic control systems in the electric power industry (RP, RC and EC) [12]:

- the failure of the hardware of the computing system;
- interface and I/O failures;
- errors in the applied algorithms;
- bugs in the software;
- errors in settings.

Considering the reliability of modern automatic control systems, it can be noted that the hardware of the microprocessor computer system has a high internal reliability. The failures encountered in practice are mainly due to a complete failure of functioning, and not to errors in logical or arithmetic calculations. Accordingly, the required reliability of the microprocessor system is provided by duplication of devices.

Failures of interface and I/O include failures of any adjacent connections: circuits and I/O modules of analog and discrete signals, external digital communications. On objects with classical DC operational circuits, analog current circuits and voltage circuits, all the problems of cable connections are manifested. Unlike electromechanical devices, microprocessor terminals and controllers require intermediate circuit interface modules. The application of IEC 61850 has its own problems of digital communications, which are potentially vulnerable to cyber attacks from the outside.

Errors in applied algorithms can be divided into two groups:

- Errors in logic;
- Errors in principle decisions when some state-mode situations, certain emergencies or equipment failures are not taken into account.

Software errors can be divided into two groups:

- Errors (bugs) made in both system and application software.
- Errors resulting from inconsistencies between designed algorithms and real software. Quite often, designed algorithms are schematic drawings made in a universal graphics editor such as Autocad or Visio. This schematic drawing is agreed and approved at the stage of design or working documentation, but it is not a program code in itself. And the problem here is that the software of the terminals RP, RC and EC in the source code is not sent and, accordingly, is not checked by either the customer or other matching organizations. The quality of this software depends on the personal qualities of programmers and the quality of the organization of internal processes of software development and testing within the manufacturer. This is all opaque, and accordingly, the actual quality of the software is quite random and unpredictable.

Errors in settings can be divided into two groups:

- Errors in settings, from incorrect recording of parameters in paper forms to incorrect setting of parameters in terminals. To exclude this factor rechecks and tests are necessary, but the human factor can lead to the omission of these errors.
- Errors caused by misunderstandings between manufacturers, designers, operating organizations, no matter how improved standards and requirements

are, there is always the influence of the human factor.

Modern computers and controllers, as well as their programming tools, contain hundreds of thousands or even millions of lines of program code and a corresponding number of machine code commands. And these lines actually contain errors (bugs), which is confirmed by systematic software updates of household and corporate devices. The problem is compounded by the fact that public devices are more widespread, which due to the mass leads to the detection of more errors, and industrial software has a small number of installation, which greatly increases the risk of undetected errors.

Considering the finished product as a "black box", by conducting external tests, even theoretically it is impossible to detect all possible errors. In practice, in accordance with the current standards, a very limited number of test experiments is required, which amounts to tens or hundreds, which is several orders of magnitude less than the number of lines of program code, which, in fact, is checked by testing the "black box".

External "black box" tests are not enough to get a reliable hardware and software product. Modern programming methodologies indicate that for the development of correctly working (error-free) software it is necessary to use a whole range of organizational, methodological and technical means, starting with the selection of personnel and improvement of their skills. Testing should be performed starting with an automatic or automated check of the operability of each program procedure (function), even if it contains only a few lines of code. But all this significantly increases the initial cost of the software product. And at the level of competitive procedures for the purchase of equipment, where the price criterion is decisive, the excess cost will not contribute to the choice in favour of the quality software product.

It is important to note that in modern conditions, organizational and managerial forms of limited liability are widely used, starting with the fact that these are all joint-stock companies and limited liability companies (the situation is identical in all countries of the world). The liability of specialists is limited by labour legislation. All this is subject to financial and time constraints. The result of all this is the fact that absolutely error-free software simply does not exist, if we talk about products that solve complex problems.

Summarizing the above, it can be noted that any microprocessor-based automatic control device can operate incorrectly, both in terms of failure, and in terms of false or excessive operation. The complexity of the structure of modern devises and systems, and the growth of the number of modern devices of RP, RC and EC, leads to the fact that many failures are difficult to predict.

It is proposed to consider the failures of automatic control systems of different types in the design and planning of power systems. At a minimum, it is necessary to take into account the possibility of false operation of any device in the form of issuing the largest or most adverse control action. Any terminal RP or EC due to a certain failure can simultaneously issue all connected control actions, even if their combination is not provided by the application algorithm, because such a failure may be caused by an error in the software. In this regard, it is proposed to systematize and expand the types of failures of RP, RC and EC devices that need to be worked out when designing and planning the development of power systems.

A clear illustration of the problem of cybersecurity in the presence of internal threats is the accident in the United Power System of Russia in 27.06.2017 [12], where there were only two initiating failures: the first, a false issue of the maximum load shedding stage, the second – an error in accounting for the power direction sign. During this accident there was no short circuit or damage to the primary power equipment, but the volume of disconnected generation was about 7 GW, disconnected load about 4 GW. According to the results of the investigation of this accident, changes were made to the algorithms of the EC of the 500 kV transmission of Bratsk – Irkutsk in order to detect and prevent a false operation. It is important to note that the problem of false alarm was not raised when performing design on this complex Automatic Stability Control System, including not raised by the operating organizations and branches of JSC "SO UPS". In the future, it is necessary to take into account the experience of this accident (and others like it), and to raise these issues and find solutions to prevent false alarms and minimize the potential volumes of falsely issued excessive operation for load shutdown, generation and change of the state of network elements early at the design stage.

It is possible to improve business processes in companies developing hardware and software, you can take into account the experience and reputation of manufacturers and engineering companies. But as soon as cybersecurity issues move into the sphere of geopolitical rivalries, these methods of improving quality will not be enough.

3. 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, 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 [8].

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. Accordingly, 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.

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.

The main types of failures of automatic control systems in the electric industry (RP, RC, EC) are analyzed and recommendations on the account of these

failures in the design and planning of power systems development are given. Situations with potentially possible cyberattacks initiated by foreign countries or large corporations in the framework of geopolitical confrontation 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. 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)
6. 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)
7. 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)
8. 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)
9. 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)
10. A.S. Alpeev, “Terminology of security: cybersecurity, information security”, Cybersecurity issues, 2014, №5(8), p. 39-42. (in Russian)
11. A.P. Doukhvalov, “Cyber attacks on critical facilities – the probable cause of the accident”, Cybersecurity issues, №3(4), 2014, p. 50-53. (in Russian)
12. 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)