Ensuring the security of cyber-physical systems in the energy sector in the context of the expansion of digital management services

Alexander Bugaev[1], Evgeny Grabchak[2], Vladimir Grigoriev[3] and Evgeny Loginov[4]

[1] Academician of the Russian Academy of Sciences, Moscow Institute of Physics and Technology (National Research University), 9, Institutskiy per., Dolgoprudny, Moscow Region, 141701, Russia
[2] Deputy Minister of Energy of the Russian Federation, Ministry of Energy of Russia, 42, Schepkina, Moscow, 107996, Russia
[3] MGIMO (University) of the Ministry of Foreign Affairs of Russia, 76, Vernadsky Ave., Moscow, 119454, Russia
[4] Situation and Analytical Center of the Ministry of Energy of Russia, 42, Schepkina, Moscow, 107996, Russia
loginovel@minenergo.gov.ru

Abstract. The article formulates approaches to the formation of an Integrated digital data management platform in the energy sector in the interests of ensuring the security of cyber-physical systems in the energy sector of Russia, as well as in other EAEU member states. The general goal of creating the proposed Integrated Digital Platform is to form a secure integrated information structure for intercorporate exchange of data and electronic documents in the organizational structure of energy entities of all forms of ownership and government bodies at various levels in Russia and in other EAEU member states. To study this problem, a systemic-structural approach was applied, adapted to the task of forming and using databases of individual energy entities within the digital model of the electric power industry. The proposed approaches to solving the problem of ensuring the security of cyber-physical systems in the energy sector have scientific novelty, since they are adapted to the conditions of expanding digital management services in relation to the distributed quasi-unified energy system of the EAEU. The necessity of creating an Integrated digital data management platform in the energy sector (systems) is substantiated, the purpose of the system, the goals and objectives of the system being created are formulated, the functional structure of the system is proposed, the subsystems of the digital platform being created are described, measures are developed to implement the proposed technical and organizational solutions. The article is aimed at leaders and specialists of government bodies and energy companies, it can be useful for scientists specializing in the study of problems in the field of energy and informatics, as well as graduate students and students.

Keywords: energy, security, information management system, digital platform

1 Introduction

By the end of 2021, it is planned to launch a single platform for the national data management system in Russia. The corresponding provision was approved by the Chairman of the Government of the Russian Federation M.V. Mishustin.

Based on this digitalization trend implemented by the Government of the Russian Federation, it is advisable to consider the possibility of forming an Integrated Digital Data Management Platform in the Energy Sector (hereinafter: the Integrated Digital Platform) in the interests of ensuring the security of cyber-physical systems in the energy sector of Russia, as well as in other EAEU member states.

2 Materials and methods

The problems of ensuring information security in the energy sector have been considered in the works of many domestic and foreign authors. The main approaches here are software methods widespread in Russia and abroad, focused on conventional information systems. Ensuring information security of automated and automatic control systems in our country is largely based on Soviet and post-Soviet technical solutions. The integration of technological control systems with public information and telecommunication networks in the Russian energy sector began to develop rapidly only a few years ago.

However, the problem of ensuring the security of cyber-physical systems in the energy sector in the context of the expansion of digital management services in relation to the distributed quasi-unified energy system of the EAEU has not yet been solved either theoretically or practically.

Taking into account the intensive processes of digitalization of the industry, this problem requires additional research.

To study this problem, it is advisable to apply a system-structural approach adapted to the task of forming and using databases of individual energy entities within the digital model of the electric power industry.

3 Purpose of the system

The general goal of creating the proposed Integrated Digital Platform is to form a secure integrated information structure for interoperate exchange of data and electronic documents in the organizational structure of energy entities of all forms of ownership and government bodies at various levels in Russia and in other EAEU member states.

Within the framework of the Integrated Digital Platform, the creation of an industry-specific computer cluster can also be implemented, if necessary. A computer clus-

ter is necessary to expand computing power in the interests of information and control systems based on existing computers of energy companies with state participation.

The integrated digital platform is designed to provide functional and general exchange, storage and processing of data and electronic documents within federal, regional and municipal authorities in Russia and in other EAEU member states and energy entities of all forms of ownership, as well as large and medium-sized enterprises energy consumers.

The considered Integrated Digital Platform should provide information support for the processes of reliable and safe power supply in the face of risks and threats of critical impacts of natural, man-made and special nature and other services (services) within the powers of federal, regional and municipal authorities in Russia and in other member states EAEU (included in the scope of the Integrated Digital Platform as it develops).

In the course of the development and implementation of the Integrated Digital Platform, the processes of secure interaction of information systems of federal, regional and municipal authorities in Russia and other EAEU member states and energy entities of all forms of ownership, as well as large and medium-sized enterprises-energy consumers, should be activated and coordinated.

4 Goals and objectives of the system being created

The goals of creating the Integrated Digital Platform are:

- Information support of federal, regional and municipal authorities in Russia and in other EAEU member states and energy entities of all forms of ownership in the field of ensuring reliable and safe energy supply in the face of risks and threats of critical impacts of a natural, man-made and special nature;
- Ensuring secure exchange of data and electronic documents of federal, regional and municipal authorities in Russia and in other EAEU member states and energy entities of all forms of ownership, as well as large and medium-sized enterprises-energy consumers in the implementation of energy supply processes to consumers in a distributed quasi-unified the EAEU energy system in the field of ensuring reliable and safe energy supply.

The tasks carried out within the framework of the Integrated Digital Platform include:

- Ensuring information interaction during the implementation of energy supply processes to consumers in the distributed quasi-unified energy system of the EAEU;
- Creation of common information resources and provision of access to them;
- Creation and maintenance on the basis of a unified system of classification and coding of a unified system of normative and reference information within the powers of federal, regional and municipal authorities in Russia and in other EAEU member states;

- Providing access to information and computing services that allow modeling and predicting the behavior of power systems and energy facilities under the influence of various factors;
- Ensuring access to information resources of energy companies in accordance with the powers of federal, regional and municipal authorities in Russia and in other EAEU member states;
- Creation and maintenance of the functioning of a common infrastructure for documenting information in electronic form;
- Providing federal, regional and municipal authorities in Russia and in other EAEU member states with information necessary for state control in the implementation of energy supply processes to consumers in the distributed quasi-unified EAEU energy system;
- Ensuring the protection of information during information interaction between federal, regional and municipal authorities in Russia and in other EAEU member states and energy entities of all forms of ownership, as well as large and medium-sized enterprises-energy consumers;
- Information support for the activities of federal, regional and municipal authorities in Russia and in other EAEU member states in difficult conditions, incl. in emergency situations.

5 Functional structure of the system

The integration segment of the Integrated Digital Platform is designed to support electronic data exchange between geographically distributed state information resources and information systems of federal, regional and municipal authorities in Russia and in other EAEU member states and energy entities of all forms of ownership, other possible participants, in the implementation of processes power supply to consumers in the distributed quasi-unified energy system of the EAEU, as well as to provide access by means of such information systems to common information resources and computing services.

The integration gateway of the Integrated Digital Platform provides electronic data exchange between information systems of federal, regional and municipal authorities and corporate segments of energy companies, as well as large and medium-sized enterprises-energy consumers by connecting their information systems to the integration segment.

It is proposed to combine the integration segment and corporate segments of energy companies with each other by secure data transmission channels connected to the integration gateway.

The integration gateway performs the following functions:

- Routing of electronic messages between the Integrated Digital Data Management Platform and information systems of federal, regional and municipal authorities in Russia and other EAEU member states, energy entities of all forms of ownership and energy companies, as well as large and medium-sized energy consumers;

- Guaranteed message delivery when interacting with integration gateways of other segments;
- Maintaining logs of operations performed by the integration gateway to ensure control of information interactions, handling emerging emergency situations and the possibility of analyzing ongoing interactions;
- Connection of information systems of federal, regional and municipal authorities in Russia and other EAEU member states and systems of interdepartmental information interaction with ensuring the conversion of protocols and formats of electronic messages (if necessary);
- Information interaction with integration gateways of other segments and information protection services.

6 Subsystems of the system being created

The information portal of the Integrated Digital Platform is designed to provide centralized access to information resources of the Integrated Digital Platform, as well as to generate, maintain and publish electronic documents and information used in the implementation of information interaction in the Integrated Digital Platform.

The statistics subsystem is designed to collect, store, process and accumulate data from energy companies, as well as large and medium-sized enterprises that consume energy.

The information and analytical subsystem is designed to provide access for employees of federal, regional and municipal authorities in Russia and in other EAEU member states to information resources of the Integrated Digital Platform using a web interface in order to generate analytical reporting forms and ad hoc requests, as well as for analytical processing data loaded from various sources, including those generated within the statistics subsystem of the Integrated Digital Platform.

The modeling subsystem is intended for modeling the processes of functioning and development of an industrial technological complex under the influence of various factors, modeling the behavior of the electric power system taking into account various criteria and restrictions at various time intervals, modeling events that affect the stability of the power system, and others.

The project and program management subsystem is designed to support the development of measures to prevent or minimize the shortage of fuel and energy resources among consumers, as well as to record and monitor the implementation of decisions of federal, regional and municipal authorities in Russia and other EAEU member states, and other projects , programs and action plans.

The subsystem for maintaining reference information, registers and registers is designed to maintain databases containing reference information, classifiers and other information used in the implementation of energy supply processes to consumers in the distributed quasi-unified energy system of the EAEU. It can also be used to provide reference information by means of the Integrated Digital Platform, as well as to make such information available to interested structural units of federal, regional and municipal authorities in Russia and other EAEU member states and energy entities of

all forms of ownership, and also large and medium-sized enterprises-energy consumers by means of the information portal of the Integrated Digital Platform.

The monitoring and control subsystem is designed to obtain information about the state and operability of the functional and supporting subsystems of the Integrated Digital Platform, as well as to automate the control tasks of the Integrated Digital Platform during its operation.

The information security subsystem is designed to ensure confidentiality, integrity and availability of data during their processing and storage in the integration segment, as well as during their transmission through communication channels when interacting with corporate segments.

The information security subsystem is proposed to be built with an orientation both to conventional information systems and to automated and automatic control systems.

7 Structuring the creation of the system

It seems expedient to structure projects for ensuring the security of cyber-physical systems when creating an Integrated Digital Platform in the Energy Industry in accordance with the following principles:

- Technological solutions that meet the needs in the component base of the electric power industry in the short, medium and long term;
- Technological solutions that make it possible to produce competitive domestic equipment to meet demand when creating an Integrated Digital Platform, taking into account the phased decommissioning of foreign equipment in the medium and long term;
- Innovative solutions that provide a technological breakthrough in the long term when creating an Integrated Digital Platform.

To create an Integrated Digital Platform, it is necessary to develop and structure the following materials:

- Analysis of possible forms of building the infrastructure of the Integrated Digital Platform for the purpose of network integration of databases of individual energy entities within the digital model of the electric power industry, including:

  - A general description of possible forms of digital platforms and means and systems for ensuring information security and an analysis of their compliance with the tasks of the industry Integrated Digital Platform, for the purpose of forming and using databases of individual energy entities within the digital model of the electric power industry;
  - Analysis of technological trends in the use of information security tools and systems;
  - A list of possible reasons that impede the implementation and use of distributed databases of individual energy entities within the digital model of the electric power industry;

– A description of the general recommended architecture of the Integrated Digital Platform used to create and use databases of individual energy entities within the digital model of the electric power industry, requirements for components and modules, methods and mechanisms of interaction between modules, as well as with external automated systems, including:

- List and general description of the basic functions of the Integrated Digital Platform;
- Conceptual requirements for the architecture of the Integrated Digital Platform;
- Requirements for the elements of the information and telecommunications infrastructure and databases of individual energy entities, including in terms of scalability, fault tolerance, dynamic load redistribution and interaction with the DBMS and taking into account the import substitution program in the energy industry;
- Description of conceptual approaches and requirements for the means of organizing data storage, providing access to them;
- Comparative analysis of various types of means and systems for ensuring information security and their suitability for use as databases of individual energy entities within the digital model of the electric power industry;
- Methods of ensuring scalability, fault tolerance, dynamic redistribution of loads, as well as interaction of the modules of the Integrated Digital Platform;
- Standard requirements for methods and procedures to ensure the preservation of data integrity;
- Description of the basic principles and interfaces of interaction with external information systems;

– Requirements for the elements of information and telecommunications infrastructure in order to form and use distributed databases of individual energy entities, including, in terms of scalability, fault tolerance, dynamic load redistribution and interaction with the DBMS:

- List of basic functions of the Integrated Digital Platform and requirements for them;
- Recommendations on methods of ensuring scalability and fault tolerance of solutions used for the formation and use of databases of individual energy entities within the digital model of the electric power industry;
- A list of the main vulnerabilities of digital platforms created in order to form databases of individual energy entities within the digital model of the electric power industry and recommendations on protection methods, including recommendations on the choice of methods and means of encryption and cryptography;
- Recommendations on typical methods of reaction to emerging collisions;
- A typical list of application software modules of the Integrated Digital Platform, including definitions of the basic requirements for them, as well as the definition of principles of interaction with external automated systems;
- Principles of scaling the infrastructure of digital platforms, taking into account the principles of territorial distribution of storage and data management systems;

— Recommendations on the use of distributed databases of individual energy entities within the digital model of the electric power industry, including:

- Recommended structure of distributed databases of individual energy entities, rules for interaction between GCD and data exchange;
- Recommended technologies for ensuring data integrity and consistency, including protocols for reaching consensus and validating and verifying changes;
- Recommendations on ensuring the logging of changes made with preservation from previous versions, as well as data on the date, reason, justifying documents and other information on all changes made;
- Recommended distribution of roles in the distributed database system of individual energy entities in order to form and use a digital network model, recommended cryptographic methods and tools;
- A list of recommended changes to be made to the existing regulatory and legal framework;

— An action plan ("road map") for the phased deployment of digital platforms, the introduction of means of receiving, transferring, verifying and protecting primary data in order to form databases of individual energy entities within the digital model of the electric power industry.

In order to comprehensively assess the technical and economic efficiency of projects to ensure the security of cyber-physical systems based on the formation of an Integrated Digital Platform in the energy sector, it is necessary to implement the following measures:

— To conduct a technical and economic analysis of the scientific, technical and human potential available in the Russian Federation for each of the submitted projects, as well as collect information on the technological equipment of the project participants;
— To develop a methodology and analyze the priority and criticality of the proposed technological solutions and projects for the industry;
— To analyze the amount of equipment planned for production by industrial partners, with details on the estimated volume of sales to energy companies;
— To reveal the technical and economic parameters of the competitiveness of equipment intended for mass production, including a comparative analysis of foreign analogues;
— To formulate indicators of economic efficiency of innovative projects, including NPV, IRR, discounted payback period for each of the submitted projects;
— To analyze the existing technological and production capacities of domestic enterprises for replicating the results obtained in the implementation of each of the presented projects, as well as proposals for the creation of new information capacities.

8 Conclusion

On the basis of the Integrated Digital Platform in the energy sector, an organizational and information base can be created to reduce the risks that threaten the security of cyber-physical systems in the energy sector in the context of the expansion of digital management services. Thus, an information environment will be created, including databases and computing services for the accumulation of information, its analysis, forecasting and planning of work and development of infrastructure facilities and systems in the energy sector, including in conditions of possible network attacks, taking into account various factors affecting the operation of industry equipment and the resulting threats to the security of cyber-physical systems.

9 Acknowledgments

The article was prepared with the financial support of the Russian Foundation for Basic Research (project No. 19-010-00956 A "Strategy for the implementation of elements of the digital economy in Russia to optimize the interaction of aggregated groups of economic agents based on the development of logistics of digital assets and intelligent mobility").

References

1. Antonov, S.G., Antsiferov, I.I., Klimov, S.M.: Methodology for instrumental and computational assessment of the sustainability of critical information infrastructure objects under information and technical influences. Nadezhnost, 20, 4, 35-41 (2020).
2. Bulatov, L.I., Salikhov, A.O., Mishin, K.N.: Analysis of the state of information security of enterprises in the fuel and energy sector. Methods of protection against cyberattacks on key information infrastructure. Internauka, 45-1(127) 21-26 (2019).
3. Voropay, N.I., Massel, L.V., Kolosok, I.N., Massel, A.G.: IT infrastructure for building intelligent management systems for the development and functioning of energy systems based on digital twins and digital images. Izvestia of the Russian Academy of Sciences. Energy, 1, 3-13 (2021).
4. Gaskova, D.A.: Method for determining the level of cyber-situational awareness of energy objects. Information and Mathematical Technologies in Science and Management, 4 (20), 64-74 (2020).
5. Gvozdev, D.B.: Increasing information security of automated dispatch control systems in electric power systems. Bulletin of the Moscow Power Engineering Institute, 3, 27-36 (2019).
6. Grachkov, I.A.: Information security of APCS: possible attack vectors and protection methods. Security of information technologies, 25, 1, 90-98 (2018).
7. Karagodin, V.V., Rybakov, D.V., Ryzhiy, N.V.: Justification of the directions of improving the power supply systems of ground complexes taking into account information security. Power supply, 1, 32-40 (2020).
8. Karantaev V.G.: Cybersecurity Issues in the Changing Electricity Industry. Relayshchik, 1 (33), 48-51 (2019).

9. Kolosok, I.N., Gurina, L.A.: Cybersecurity risk assessment of the information and communication infrastructure of the intelligent energy system. Information and Mathematical Technologies in Science and Management, 2 (14), 40-51 (2019).
10. Smirnova, E.V.: Features of information security in the electric power industry. Refrigeration equipment and technology, 53, 3, 39-44 (2017).
11. Strebkova, T.V., Tuchina, D.S., Zvada, P.A.: Conducting a practical cyberattack on the data transmission channel of a digital substation. Bulletin of the North Caucasus Federal University, 3 (72), 22-27 (2019).
12. Bojko, P.A.: Convergent use of neural network information technologies for monitoring and evaluating the performance of digital control operators of situational centers at critical infrastructure facilities. IOP Conference Series: Materials Science and Engineering. III International Scientific and Practical Conference on Innovations in Engineering and Technology, 012044 (2020).
13. Bortalevich, V.Y.: Intelligent monitoring, modeling and regulation information traffic to specify the trajectories of the behavior of organizational agents in the context of receipt of difficult-interpreted information. IOP Conference Series: Materials Science and Engineering, 012015 (2019).
14. Grabchak, E.P.: Ensuring observability and controllability of complex technical systems in difficult and irregular situations when commands with a large distortion component are received. Lecture Notes in Electrical Engineering, 729 LNEE, 624-631 (2021).
15. Grigoriev, V.V. The use of electronic semantization of the cognitive activity manifestations with the aim of detection of intentions of the group of people leading to the destabilization of the digital super system. IOP Conference Series: Materials Science and Engineering. 1st International Conference on Innovative Informational and Engineering Technologies, IIET, 012002 (2020).
16. Shkuta, A.A.: The use of artificial intelligence's elements to block the manifestations of individuals' behavioral activity going beyond the quasi-stable states. IOP Conference Series: Materials Science and Engineering, 012028 (2019).
17. Stennikov, V.A.: Application of digital technologies for expansion planning of integrated energy systems. E3S Web of Conferences. Ser. "ENERGY-21 - Sustainable Development and Smart Management" 02003 (2020).
18. Voropai, N., Kurbatsky, V., Tomin, N., Efimov, D., Kolosok, I.: Intelligent control and protection of power systems in the russian cities. SMARTGREENS 2019 - Proceedings of the 8th International Conference on Smart Cities and Green ICT Systems, 8, 19-29 (2019).
19. Voropai, N., Serdyukova, E., Gerasimov, D., Suslov, K.: Development of a simulation model of an integrated multi-energy system based on the energy hub concept. E3S Web of Conferences. 2020 Rudenko International Conference on Methodological Problems in Reliability Study of Large Energy Systems, RSES, Kazan, 01028 (2020).
20. Wang, H., Liu, Y., Cao, G., Zhou, B., Voropai, N., Barakhtenko, E., Jia, Y.: Advanced adaptive frequency support scheme for dfig under cyber uncertainty. Renewable Energy, 161, 98-109 (2020).