Aspects of the concept of cyber-protected objects of a digital electrical network with elements of Zero Trust Architecture in Russia

Vladimir Karantaev[1,*], *and Vladislav* Karpenko[2]

[1]Moscow Power Engineering Institute, Center of National Technology Initiative,111250 Moscow, Russia
[2]Moscow Power Engineering Institute, Department of Relay Protection and automation of power systems,111250 Moscow, Russia

Abstract. Modern trends in the development of the electric power industry declare the widespread use of information and communication technologies and digital services to improve the operation of relay protection and automation (RPA) subsystems, Industrial Control Systems (ICS), commercial electricity metering systems, etc. However, it is associated with an increase in the number of cyber threats and risks of disrupting the stable functioning of electric power facilities due to destructive information influences. The report presents aspects of a holistic concept of building cyber-protected digital substations with elements of Zero Trust Architecture. Based on the results of the theoretical investigation the authors assume the possibility of technical testing of the proposed approaches to build a cyber-protected digital substation as a part of the emerging Research and Development (R&D) programs for the practical implementation of the zero-trust policy.

1 Introduction

The electric power industry of the Russian Federation is entering a new decade with the urgent tasks requiring the selection and adoption of optimal organizational and technical decisions in the process of modernization of electric power facilities which were set before it.

The tasks set for the industry are reflected in the number of strategic planning documents in the field of ensuring Russia's national security:

• The Doctrine of Energy Security of the Russian Federation approved by the Decree of the President of the Russian Federation on May 13, 2019 No. 216 [1];

• The Doctrine of information security of the Russian Federation approved by the Decree of the President of the Russian Federation dated December 05, 2016 No. 646 [2];

• Adopted in pursuance of doctrinal documents of regulatory legal acts including the Federal Law (FL) "On the Security of Critical Information Infrastructure of the Russian Federation" dated July 26, 2017 No. 187-FL [3].

Summarizing the provisions of the above documents, we can draw the following conclusions:

• In the Russian Federation, FL-187 becomes the main catalyst for accelerating the process of import substitution leading to the predominant use of microprocessors and microcontrollers as well as system and application software of domestic production in intelligent electronic devices installed at power facilities;

• The tasks were set to reduce the identified risks of energy and information security of the Russian Federation: modernization of the industry, overcoming the aging of fixed assets, development of domestic information and communication technologies (ICT), reducing the vulnerability of critical information infrastructure facilities (CIIF) of the fuel and energy complex ensuring the safe operation of CIIF.

2 Types of cyber threats to digital power facilities

In the context of this work it is important to focus on the transboundary threats to the energy security of the Russian Federation recorded in [1], the threats of computer attacks on CIIF operating in the fuel and energy complex of the Russian Federation (FEC RF) in companies of the electric power industry, in particular.

Over the past decade issues related to ensuring cybersecurity in the implementation of digital substation technologies have been raised in scientific discussions [4-6]. In the works attention is paid to the following aspects:

• Threats to the reliability of electric power systems and even threats to the energy security of Russia;

• The need to test the elements of a digital substation for resilience to cyberattacks;

• The need for certification of intelligent electronic devices (IED).

It was emphasized that in the implementation of any cyber threat in practice, functional failures of control systems of digital substations can lead to shutdown or damage to electric power equipment. As a result, there are general threats to reduce the reliability and disrupt

* Corresponding author: vladimir.karantaev@gmail.com

the stability of power systems which, in turn, is a threat to the energy security of entire regions [4]. The authors support these and several other statements about the need to improve the cybersecurity of digital substations (DS) and the technologies used in their construction.

In recent years analytical work has been carried out to consider the existing threats and risks of disruption to the functioning of digital power facilities as well as work to assess the possibility of unacceptable negative consequences. For example, in the initiative research work (R&D) implemented in 2019 by the ICS cybersecurity laboratory of Rostelecom Solar an assessment was made of some cyber-physical consequences, the occurrence of which is possible on the "digital facilities" of the electric power complex [7, 8] including the reason for the implementation of successful targeted computer attacks.

Within the framework of the national research-type table-top cyber exercises, which took place on December 23, 2019 at the Rostelecom Solar office, 5 reference scenarios for the disruption of functioning of electric power facilities of different voltage classes of 10/0.4 kV - 500 kV substations were considered. Techniques and tactics of offenders with different potentials from low to high were considered. The analysis of the proposed scenarios and the assessment of possible consequences force us to look for new approaches to the methodology for threat modelling (TM) to information security. There are assumptions that methodological approaches should be based on the assessment of consequences including cyber-physical consequences for a separate power facility, a group of facilities, or a part of the power system [9].

The organizational and technical measures taken to ensure the safety of the CIIF functioning of the electric power industry subjects (ICS, RPA, etc.) should reflect the adopted and implemented security policy (information security) of the company, the formed threat model (assessment of consequences, hybrid threat model) including threats to information security assessing the potential and motivation of the offender.

Considering the non-triviality of the task of developing a practically applicable TM, knowledge-based systems can become a tool for implementation. For example, knowledge-based systems can vary: decision support systems or expert systems with the "core of knowledge" which is based on ontology of cyber threats (nowadays ontology is being developed).

3 Relevance of the application of new security models

On the basis of the mentioned above the authors consider it an important practical and research task to discuss and determine the directions for the development of security models and implemented security mechanisms for information and control systems of newly created and undergoing deep modernization of electric power facilities of the digital electrical network.

The decisions made will directly concern the requirements for the developed IEDs for digital substations, for the issues of the practical implementation of DS software and hardware complexes and for the operation of power facilities.

In the emerging situation of increasing requirements for ensuring the safe operation of the CIIF and the growing risks of targeted computer attacks, “zero trust” approach deserves attention.

The model of "zero trust" provides a set of concepts and ideas designed to reduce the uncertainty while making accurate decisions about on-demand access in information systems and services in the network considered as compromised [10].

According to the authors, at the current level of the development, the concept of "zero trust" is a reflection of the accepted abstract-level threat model, the main provisions of which are:

• Within any logical perimeter, a computer, technological telecommunications network (environment) is untrusted by default [10].

This thesis actually captures:

• relevance of the presence of a malicious insider in any information, information control, automated, automatic system;

• acceptance of a potentially possible compromise of infrastructure and overcoming the "protection perimeter" "fixing" intruders within the "trusted" security perimeter and the development of a computer attack.

In fact, acceptance by default, the possibility of implementing certain stages of the computer attack, which are fixed in the Kill Chain framework, and implementing in practice the techniques and tactics, which are presented in the MITRE matrix.

The authors note that the specified level of the intruder's model for digital relay protection and automation systems is fixed in the document of Rosseti holding [11] in section 6.2. “Possible threats to information security”. In the document [11] it is proposed that the sources of threats to the security of relay protection devices can be as follows: intelligence services of foreign states, terrorist organizations, representatives of competing firms and organizations. The accepted rules in the information security industry indicate that these types of attackers have the potential to carry out the attacks outlined above.

On fig. 1 the main possible vectors of a computer attack on secondary systems of digital substation are shown.

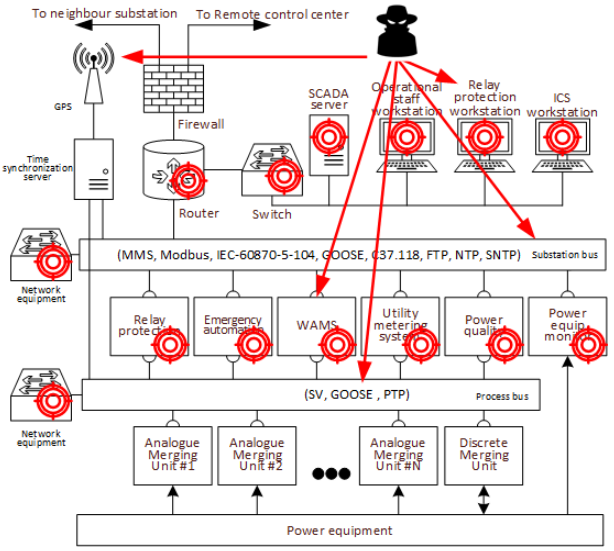

Fig. 1. Possible vectors of a computer attack on digital substation.

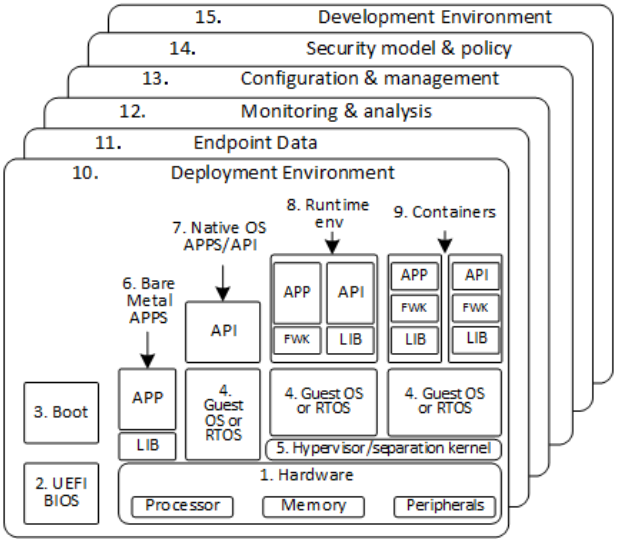

Fig. 2. The threats and vulnerabilities of modern IoT devices.

The relevance of choosing an adequate security policy increases with the accumulation of practical experience in the implementation of projects for the organization of remote technological and dispatch control of power facilities of voltage classes 110 kV - 500 kV, for the implementation of which distributed control systems are used, consisting of products from a number of manufacturers using heterogeneous data transmission channels.

One of the lingering problems of Russian and international vendors is the lack of complex regulatory and technical requirements formed within national boundaries that impose requirements for the implementation of safety functions in IEDs, software and hardware complexes and distributed systems in general.

The sources [12, 13] describe the threats and vulnerabilities of IoT (Internet of things) devices which can be largely correlated with the threats and vulnerabilities of modern IEDs. See fig. 2.

- (1) Hardware Threats;
- (2)(3) Threats for process of the first boot;
- (4)(5) Threats for operating system;
- (6)(7)(8)(9) Threats for application software;
- (10) Threats for installation (deployment) process;
- (11) Threats of access to endpoint data;
- (12) Threats for monitoring and analysis;
- (13) Threats for configuration and management;
- (14) Threats of policies and security models;
- (15) Threats of development process.

4 Selected issues of practical implementation of zero trust architecture

The authors suggest the following practical steps to support the policy of "zero trust" that could be practically implemented.

The following mechanisms should be implemented at the level of applications and services:

- Identification, authentication, authorization of the following user roles: relay protection engineer, operating personnel, contractors;
- Identification, authentication devices in network: IED, Programming logic controller (PLC) etc.;
- Providing cryptographic protection of network traffic; (reports [14, 15] are devoted to particular issues of cryptographic methods of protection in RPA system of the digital substation);
- Collection and analysis of log files including security logs from the IED of all technological subsystems of the digital substation.

In software and hardware complexes IEDs can be used, which are implemented on a Russian microprocessor basis under the control of an operating system developed with taking into account a set of requirements for its reliable and safe operation. Conceptual issues of creating protected IEDs were covered in one of the reports at the conference of “ICS CIIF 2020” [12]. The use of modern microprocessors and real-time operating systems should allow the development of advanced protection scenarios based on built-in security mechanisms. This approach is the global trend in the development of embedded systems.

Operation systems (OS) with a monolithic kernel (based on the Linux kernel) and security extensions (Security Extensions) as well as OS based on a microkernel architecture using the MILS (Multiple Independent Levels of Security) concept (VxWorks, Pike OS, Kaspersky OS, etc.) can be used to develop IEDs in a protected design. In general, it is necessary to

use an OS that can provide guarantees for the safe operation of devices under their control.

The use of embedded operating systems with the implementation of security functions should be facilitated by the protection profiles issued by Federal Service of Technic and Export Control (FSTEC) of Russia on the operating system including real-time operating systems [16] and embedded operating systems.

The implementation of these functions is possible in newly designed IEDs with close interaction between the group of vendors of information security tools (IST) and IEDs that is the way to creating an IED in a secure design (practical implementation of the principle of secure by design).

The authors propose to consider the possibility of using the standards of the IEC 62351 and IEC 62443-4-2, IEC 62443-4-1 series in the formation of requirements for newly created IEDs and technical specifications for newly created digital substations.

IEC 62351-14, Power systems management and associated information exchange - Data and communications security - Part 14: Cyber security event logging [17] is a standard that describes the format of collected security logs. IEC 62351-8, Power systems management and associated information exchange - Data and communications security - Part 8: Role-based access control [18] is a standard that describes the implementation of a role-based access control model.

The issues of using security operation centers (SOC) in companies of the power grid complex with the integration of security events from the level of technological systems were covered in 2018 in the report [19] at the international conference "Opportunities and challenges in Digital Transformation". At present the use of SOC for monitoring and detecting computer attacks aimed at automated control systems for power facilities has received a certain practical implementation in the Russian Federation. The effectiveness of SOC use is limited by the current level of development of built-in security mechanisms in the IED. The development of the necessary functionality in the implementation of the concept of a protected digital substation will increase the level of maturity of the implemented software and hardware-software solutions.

The draft standard IEC 61850-8-1 [20] contains a description of the possibility of using secure profiles MMS, GOOSE, SV protocols creating the prerequisites for the implementation of the provisions of the standards developed by WG 15 TC 57 IEC: IEC 62351 [21, 22]. Development and implementation of secure profiles will allow to solve the problem of traffic protection, identification and authentication of subjects and objects of access, devices in the network (IED, PLC, etc.). See fig. 3

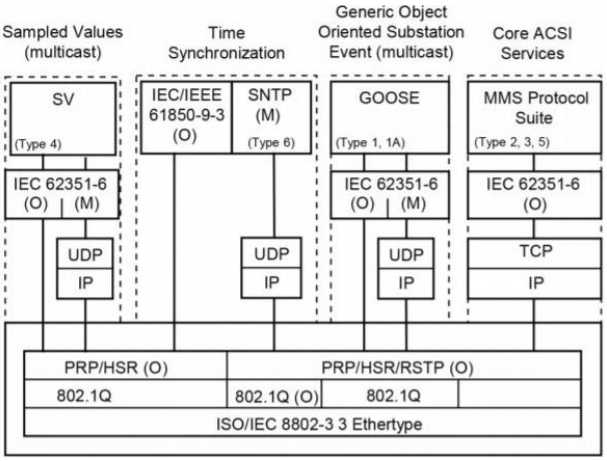

Fig. 3. Overview of functionality and profiles.

Part 8 of the IEC 62351 series of standards [18] is devoted to solving the problem of identification, authentication, and authorization of users (relay protection engineer, operating personnel, contractors) which implies the implementation of a role-based access control model. From the practical point of view, one can implement a policy for different groups of access subjects by using:

- **LDAP** catalogue for workstations and servers;
- **RADIUS**-server for all network equipment which are used on digital substation;
- **LDAP** catalogue and **RADIUS**-server for IEDs, merging units etc.

LDAP catalogue, **RADIUS**-server can be implemented using a secure operating system, for example, Linux which has the potential for development in the Russian Federation on the basis of domestic microprocessors. The authors addressed this topic in the article in the journal Relayshchik [23]. The authors also note that operator access to an automated control system or individual IEDs should be provided with the least privileges necessary to perform his professional duties.

In the current regulatory and technical requirements of Federal Grid Company of United Power System (FGC UPS) of Russia [24] individual elements of the security system are proposed. The introduction of them should increase the security of the LAN of digital substation. However, these requirements were formed only for digital substations of FGC UPS. In fact, these requirements cannot be considered integral for newly designed digital substations.

5 Conclusions

The paper presents aspects of building a cyber-protected DS with elements of Zero Trust Architecture concept. Based on the results of the analytical investigation the authors propose to consider:

- The possibility of technical testing of the proposed approaches to building a cyber-protected digital substation in new R&D programs for the practical implementation of "zero trust" policy;
- The feasibility of harmonizing standards IEC 62351 and IEC 62443 in the Russian Federation;

• The possibility of adapting the current requirements for the creation, operation, distribution of cryptographic protection tools used in ICS, RPA, WAMS and other technological systems.

References

1. Russian Federation, Presidential Decree, On approval of the Energy Security Doctrine of the Russian Federation [Electronic resource], 216 (13 May 2019) Available at: https://www.garant.ru/products/ipo/prime/doc/72140884/ (accessed: 09.07.2020)
2. Russian Federation, Presidential Decree, On approval of the Information Security Doctrine of the Russian Federation [Electronic resource], 646 (5 December 2016) Available at: https://www.garant.ru/products/ipo/prime/doc/71456224/ (accessed: 09.07.2020)
3. Russian Federation, Laws, On the security of the critical information infrastructure of the Russian Federation [Electronic resource], adopted by the State Duma on 12 July 2017, 187 (19 July 2017) Available at: https://base.garant.ru/71730198/ (accessed: 09.07.2020)
4. A. Osak, D. Panasetskiy, E. Buzina, Reliability and safety aspects of digital substation design: presentation, scientific and technical conference "Modern trends in the development of relay protection systems and automation of power systems", 3-7 July 2013, Ekaterinburg (2013)
5. G. Nudelman, Cybersecurity requirements for relay protection and automation systems using IEC 61850: Collection of reports XXI conference "Relay protection and automation of power systems", 29-31 May 2012, Moscow, 18-23 (2012) ISBN: 978-5-9903581-2-6
6. B. Papkov, A. Kulikov, V. Osokin, Electricity Cybersecurity Issues: scientific and technical journal "Energetic": founder and publisher "Energoprogress", Moscow, 9 (225), 96 (2017) ISSN: 0013-7278
7. V. Karantaev, V. Karpenko, Analysis of operational disruptions to power facilities due to cyberattacks: journal Connect, WIT: founder and publisher PH "Connect", Moscow, 1-2, 11-12 (2020)
8. V. Karpenko, V. Karantaev, O. Arhangelskiy, et all, Analysis of the consequences of the impact of cyberattacks on relay protection systems and emergency control systems for substations of high voltage classes: journal "Releyschik", founder and publisher PH "All Electrotechnic", Moscow, 2 (36), 32-34 (2020)
9. V. Karantaev, A. Kuznetsov, O. Arhangelskiy, et all, Experience in conducting cyber exercises to analyze operational disruptions to power facilities as a result of cyberattacks: journal "Releyschik", founder and publisher PH "All Electrotechnic", Moscow, 1 (35), 58-60 (2020)
10. SP 800-207, Zero Trust Architecture: analytical report NIST [Electronic resource] Available at: https://csrc.nist.gov/publications/detail/sp/800-207/final (accessed: 05.09.2020)
11. The concept of development of relay protection and automation of the power grid complex [Electronic resource], Appendix 1 to minutes of the Management Board of "Rosseti", 356pr (22 June 2015) Available at: https://www.rosseti.ru/investment/science/tech/doc/vipiska_prilogenie.pdf (accessed: 03.07.2020)
12. S. Paryev, Issues of development of cyber-protected PLC: presentation [Electronic resource], the 8th soecial conference "Information security of ICS CIIF", Moscow (4-5 March 2020)
13. Industrial Internet of Things Volume G4: Security Framework: analytical report Industrial Interner Consortium [Electronic resource] Available at: https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf (accessed: 03.07.2020)
14. V. Karantaev, Ensuring information security of modern relay protection systems: presentation, the 4th cpecial conference "Safety of critical objects of the fuel and energy complex", Moscow (31 May 2016)
15. V. Karantaev, Particular issues of the implementation of cryptographic information protection means for the subsystem of relay protection and automation: collection of reports of the conference "Relay protection and automation of power systems 2017", St. Petersburg, 935-940 (25-28 April 2017)
16. Methodical document, Protection profile of operating systems type "b" of the fourth protection class: protection profile [Electronic resource], FSTEC of Russia: publisher FSTEC of Russia, Moscow, (2020) Available at: https://fstec.ru/component/attachments/download/1578 (accessed: 30.03.2020)
17. IEC 62351-14, Draft for public comment, Power systems management and associated information exchange – Data and communications security – Part 14: Cyber security event logging: international standard: official edition: introduced for the first time: date of introduction 08.11.2019, Developed by IEC Technical Committee, Power systems management and associated information exchange, TC 57 IEC (2020)
18. IEC 62351-8, Power systems management and associated information exchange – Data and communications security – Part 8: Role-based access control for power system management: international standard: official edition: introduced for the first time: date of introduction 28.04.2020, Developed by IEC Technical Committee, Power systems management and associated information exchange, TC 57 IEC (2020)
19. V. Karantaev, Managed Detection and Response (MDR) Delivery Models for Industrial Control

Systems (ICS): presentation, 6th international conference dedicated to industrial cybersecurity "Opportunities and challenges in Digital Transformation", Sochi (19-21 August 2018)

20. IEC 61850-8-1: 2011+AMD1: 2020 CSV Consolidated version, Communication networks and systems for power utility automation - Part 8-1: Specific communication service mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3: international standard: official edition: introduced for the first time: date of introduction 21.02.2020, Developed by IEC Technical Committee, Power systems management and associated information exchange, TC 57 IEC (2020)
21. IEC 62351-6, Power systems management and associated information exchange – Data and communications security – Part 6: Security for IEC 61850: international standard: official edition: introduced for the first time: date of introduction 20.10.2020, Developed by IEC Technical Committee, Power systems management and associated information exchange, TC 57 IEC (2020)
22. IEC 62351-9, Power systems management and associated information exchange – Data and communications security – Part 9: Data and communications security key management for power system equipment: international standard: official edition: introduced for the first time: date of introduction 18.05.2017, Developed by IEC Technical Committee, Power systems management and associated information exchange, TC 57 IEC (2017)
23. V. Karantaev, V. Karpenko, Particular issues of the implementation of a cyber-protected digital substation: journal "Releyschik", founder and publisher PH "All Electrotechnic", Moscow, 2 (34), 38-42 (2019)
24. STO 56947007-29.240.10.302-2020, Typical technical requirements for the organization and performance of technological LANs in the ICS of the UPS substations: approved and put into effect by Order of «FGC UPS», 68, introduced for the first time: date of introduction 26.02.2020, developed by «Intelligent Grids» – Moscow: «FGC UPS» (2019)