Development of a method for using AI systems for assessing cyber threats to electric power facilities

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, ICS, WAMS, etc. However, this 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 the results of the synthesis of a hybrid method for modeling cyber threats with possible cyber-physical consequences and the development of a demonstration prototype of an expert system that implements the method.

1 Introduction

The power industry in the world and particularly in Russia today is on the verge of large-scale modernization and technological changes. The issues of "digital transformation" are included in the agenda of all the largest industry conferences, forums, and round tables held over the past few years.

At conferences various aspects of the development of the electric power industry are discussed. In general, the discussions concern the choice of technological foundations for the future growth of this economic sphere. In fact, the choice has already been made in favor of the further development of the industry through digitalization, which implies the massive introduction of information and communication and other ready-made commercial technologies COTS (Commercial Off-The-Shelf - any hardware or software computer technologies from the open commercial market based on international standards, ready-made or adapted for use in special conditions) into the secondary subsystems of the objects of the electric power complex including the relay protection and automation subsystem.

The digitalization vector is driven largely by the International Electrotechnical Commission (IEC). In particular, by the technical committee No. 57 (TC 57) which develops standards of the IEC 61850, 60870-5, 61968, 61970, 62351, etc. series which are used in the digital transformation of the energy industry. The IEC TC 57 business plan [1] states that the further development of electric power systems is possible with the use of digital substations, distributed power supply systems, the implementation of demand response approaches, the development of the IIoT concept, the creation of load and generation management systems.

The practical implementation of IEC plans in Russia and the world has already begun. Examples of this are: a virtual power plant in Singapore [2]; demand management and distributed power supply systems in the USA, Australia, UK ([3], [4]); electricity trade taking into account the individual characteristics of consumers [5]; transfer of substations to telecontrol from remote centers [6]; introduction of digital substations of various voltage classes ([6], [7], [8]); introduction of digital electrical distribution networks [9].

With the expansion of digital technologies introduction, information and communication technologies at power facilities, the range of threats associated with the vulnerabilities of the technologies used are also expanding. The risks of disrupting the sustainable functioning of "digital objects" of the energy sector and their associations under the destructive influence of cyberattacks are growing.

The thesis put forward is not new, but the authors lay an emphasis on it. Despite the fact that the authors of numerous publications [10], [11], [12] addressed the problem of cyber threats to “digital power facilities”, many methodological and practical issues have not been resolved up to date.

Several technical reports and studies from the past decade have examined possible computer attacks targeting power control subsystems. For example, Technical Report [10] prepared by Sandia National Laboratories, New Mexico, USA, 2009 briefly highlights the possibility of attacks on the relay protection systems of power lines and generators as well as on ICS that were simulated in the laboratory. The report [11] was prepared in 2015 by the Center for Risk Studies, University of Cambridge, (Cambridge, UK). This paper describes the large-scale consequences of a cyberattack on the US electricity system and the economic losses

* Corresponding author: vladimir.karantaev@gmail.com

from business shutdowns. The report [12] contains a detailed analysis of relay protection systems and the distribution of the hazard level for each component of the relay protection and automatic control system and the consequences of the impact of cyberattacks on the functions of these systems.

Thus, one of the important unresolved issues for the power industry is ensuring the cybersecurity of relay protection and automation subsystems of digital substations. Since cyberattacks are destructive, they can provoke critical cyber-physical consequences. The solution to this issue begins with the development of a model of cyber threats, but problems arise with the existing methodological uncertainty. Therefore, the authors carried out the investigation that was aimed at developing a method for solving methodological issues in the analysis of cyber threats of the relay protection and automation subsystem of digital substations. The interim results of the investigation are presented in this article. The elaboration of the issue of modeling cyberattack scenarios remains outside the scope of this publication.

2 Problems of creating a cybersecurity threat model for electric power facilities

Despite the obvious need to solve the problems of ensuring cybersecurity, cyber resilience of electric power facilities from the practical point of view, this problem remains controversial.

Cybersecurity in the digital substation is a complex challenge that begins with analyzing cyber threats and ranking them according to the potential damage they cause. At the first stage of the investigation the goal was set to develop a hybrid method for modeling cyber threats for the electric power facility and digital substation which would take into account the following criteria:

- determination of the physical consequences of a successful cyberattack (accident);
- determination of cyber-physical consequences leading to accidents (impact);
- determination of the results of the implementation of cyber threats in the components of the relay protection and automation subsystem of the digital substation;
- cyber threats present in the components of the relay protection and automation subsystem of the digital substation;
- identification of weaknesses and vulnerabilities of the components of the relay protection and automation system of the digital substation;
- identification of the offender, tactics, and techniques used by him in carrying out a cyberattack.

An analysis of modern Russian and foreign methods, knowledge bases related to the modeling of cyber threats for compliance with the criteria was carried out:

- MITRE Matrix Enterprise ATT&CK and ICS ATT&CK;
- Cyber Kill Chain and ICS Cyber Kill Chain;
- STRIDE;
- Attack tree;
- Attack Library (MITRE CVE, CWE, CAPEC, OWASP);
- Drafts of the methodology of threat modelling of FSTEC of Russia 2015 and 2020.

The common point for all the considered methods is that none of them can be used without additional materials to satisfy the criteria formulated above. Therefore, during the investigation the authors decided to use a hybrid approach - to combine several methods using the advantages of each. Then, a set of methods that are the most suitable for solving the problem of synthesizing the hybrid approach for modeling cyber threats was identified.

The hybrid approach consists of the following methods:

- draft methodology of threat modelling of FSTEC of Russia 2020 as it has the most general approach and a set of stages;
- MITRE CVE and CWE libraries - sources of knowledge about vulnerabilities and software weaknesses;
- MITRE Matrix ICS ATT & CK - The source of knowledge about tactics and techniques used by cybersecurity offenders.

The approach proposed in this work can be illustrated by the structure in Fig 1.

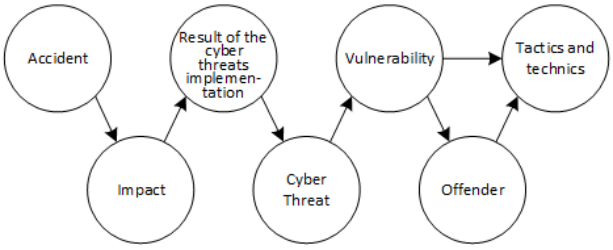

Fig. 1. The illustration of the way to simulate cybersecurity threats.

To test this method it was decided to develop a particular threat model for an imaginary digital substation of the 3rd architecture [13] with two RPA IEDs (RPA 500 kV transmission lines and RPA autotransformer 500/220/10 kV) and an automated workstation for an RPA engineer. Information flows and existing vulnerabilities of the considered components of the relay protection and automation system were analyzed and the threats that generate the identified vulnerabilities were validated.

A particular threat model was developed and during this work the following problems and additional opportunities were identified [14]:

- Combinatorics of variants of existing threats even in deterministic limited conditions is very large and requires a lot of efforts when developing manually;
- complicated combinatorics indicates that scaling up the results obtained is very difficult;
- a person who manually develops a threat model for an electric power facility in this way must have significant competencies in the areas of information security, electric power engineering, relay protection and automation;

• the method of threat modelling excluding the consideration of attacks can be used to analyze the current situation at a power facility if it is possible to instantly receive data on security events in the infrastructure of a technological facility.

Based on the experience gained in the development of a hybrid cyber threat model a hypothesis was put forward about the possibility of using artificial intelligence (AI) systems to automate the application of the proposed hybrid approach.

3 Comparison of ai approaches to create a cyber threat model

To solve the problem of modelling cyber threats and cybersecurity intruder of the digital substation, artificial intelligence systems based on the following approaches can be used:

• training of machine learning (ML) and neural networks (NN) models on labeled data;
• application of ML models for clustering;
• methods of "retraining" models of MO and NS;
• knowledge engineering methods.

Training of ML and NN models on the labeled data is a popular method in the world for solving applied problems for prediction (regression), classification and ranking. The task of developing a cybersecurity threat model belongs to the tasks of classification. Therefore, we will describe the task that the AI system must solve:

$$X - a\ set\ of\ objects\ (samples)\ (descriptions\ of\ cyber\ threats\ by\ selected\ metrics); \quad (1)$$

$$Y - a\ set\ of\ responses\ (label)\ (a\ type\ of\ cyber\ threat); \quad (2)$$

$$X \to Y - unknown\ dependence\ (target\ function); \quad (3)$$

$$Given: \{x_1, x_2, \ldots, x_n\} \in X - training\ sample; \quad (4)$$

$$y_i = y(x_i),\ i = 1,2 \ldots n - known\ answers; \quad (5)$$

$$Search: a: X \to Y - algorithm,\ decision\ function\ that\ approximates\ y\ on\ the\ entire\ set X. Vector(f_1(x), \ldots f_l(x)) - - attribute\ description\ of\ an\ object x. \quad (6)$$

Feature-attributes matrix (features data):

$$F = ||f_i(x_i)||_{n \times l} = \begin{pmatrix} f_1(x_1) & \ldots & f_l(x_1) \\ \ldots & \ldots & \ldots \\ f_1(x_n) & \ldots & f_l(x_n) \end{pmatrix} \quad (7)$$

$$A = \{a(x) = g(x,\theta)\ |\theta \in \theta\} - predictive\ model,\ whereg: X \times \theta \to Y - fixed\ function. \theta - set\ of\ valid\ parameter \theta values\ (required\ vector\ of\ parameters). \quad (8)$$

$$For\ example,\ if\ we\ take\ a\ linear\ model\ with\ a\ vector\ of\ parameters \theta = (\theta_1, \ldots, \theta_n), \theta = \ddot{Y}^n \quad (9)$$

Then for the classification into at least two classes *(Y={-1;+1}),* it will look like this:

$$g(x,\theta) = sign \sum_{j=1}^{l} (\theta_j f_j(x)) \quad (10)$$

At this stage difficulties arise with applying this approach:

• there is no labeled dataset with an indicative description of cybersecurity threats for the RPA subsystem of the digital substation where the model could be trained (at least in open sources);
• there are more than two threat classes and they can overlap; accordingly, the complexity of the model greatly increases;
• the choice of ML models to achieve the set goal is a non-trivial task.

Similar problems with clustering methods and retraining of ML models. Firstly, it is necessary to perform separative clustering, but there is no data set. Then, an additional problem arises with the fact that there are no models specially trained for the classification of the cyber threats to the RPA subsystem of the digital substation.

Knowledge engineering approaches to solving this problem do not have such problems, namely, knowledge-based systems (expert systems (ES)). Expert systems allow to accumulate and consolidate the knowledge of experts about a certain subject area and build logical chains and receive answers when forming queries. ES are of different architectures whence two large groups divided as far as possible to take into account the time factor are distinguished:

• static (the conditions of the problem do not change in the course of its solution);
• dynamic (the conditions of the problem can change in the course of its solution).

Dynamic ES can be used to solve the problems of increasing situational awareness in terms of information security events for dispatchers of power facilities when implementing the method proposed in this work. For this, it is necessary that security sensors and event correlation systems must be installed at the facility. The ES has the functionality of processing these events in real-time, therefore, it is possible to draw a conclusion on their basis, for example, when infrastructure object is compromised and what consequences might happen afterwards.

Static expert systems can be used for modelling cyber threats at the design stages of electric power facilities and to update the threat model when it is necessary. As a part of the investigation in this work a demo prototype of a static expert system that implements a hybrid threat modelling approach proposed earlier with the knowledge base established on a semantic network (ontology) was developed.

The general architecture of such a system and sources of the knowledge for it are shown in Fig. 2.

Table 1. A part of the cyber threat model.

№	Accident	Impact	Results of the cyber threats implementation	Cyber threat	Vulnerability	Offender
1	Switch off T-Line	Excessive operation	Firmware tampering	Data tampering	CVE-2019-10930	Engineer
2	Switch off T-Line	Excessive operation	Firmware tampering.	Data tampering	CVE-2019-10930	Hacker
3	Switch off T-Line	Exces-sive opera-tion	Firmware tampering.	Improper access	CVE-2019-10930	Engineer
4	Switch off T-Line	Exces-sive opera-tion	Firmware tampering.	Improper access	CVE-2019-10930	Hacker
5	Switch off T-Line	Excessive operation	Config. Tampering	Data tampering	CVE-2019-10930	Engineer
6	Switch off T-Line	Excessive operation	Config. Tampering	Data tampering	CVE-2019-10930	Hacker
7	Switch off T-Line	Excessive operation	Config. Tampe-ring	Improper access	CVE-2019-10930	Engineer
8	Switch off T-Line	Exces-sive opera-tion	Config. Tampe-ring	Improper access	CVE-2019-10930	Hacker
9	Switch off T-Line	Excessive opera-tion	Malicious software exe.	Data tampering	CVE-2019-10930	Engineer
10	Switch off T-Line	Excessive opera-tion	Malicious software exe.	Data tampering	CVE-2019-10930	Hacker

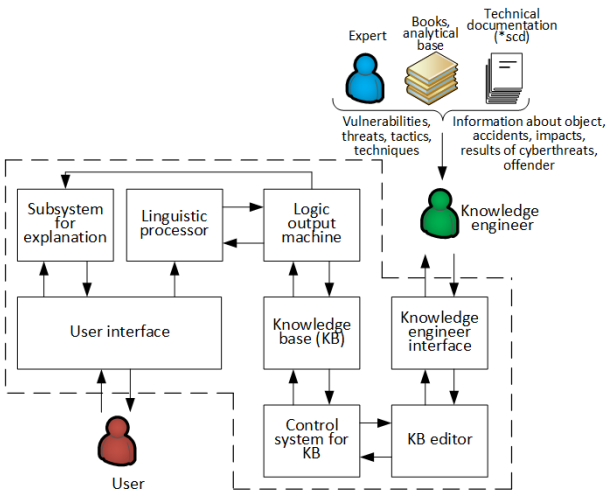

Fig. 2. The general architecture of the static expert system for threat modelling.

The knowledge base in the current experiment included all the data from the analysis of an imaginary digital substation, for which a particular threat model was formed. Disconnections and damage to power equipment were considered as physical consequences while violations of the basic properties of the relay protection and automation subsystem (sensitivity, selectivity, speed-of-reaction, reliability) were considered as influences. The illustration of the knowledge base that was obtained during the experiment is shown in Fig. 3.

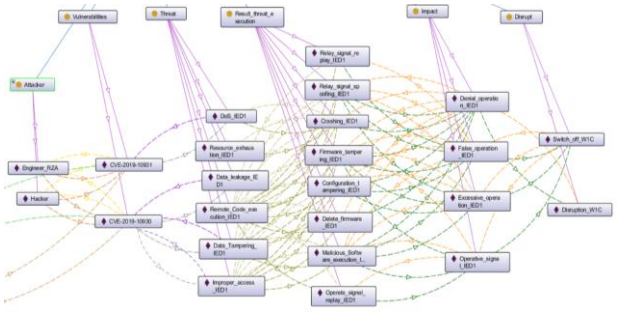

Fig. 3. Knowledge base illustration.

By means of the developed prototype of the expert system the obtained knowledge base was processed and, thus, a private model of threats for an imaginary digital substation was formed in an automated mode.

A part of the threat model is shown in Table 1.

This threat model contains a description of several possible cybersecurity threats in accordance with the approach proposed in the investigation. The results of the model development using ES and manually coincided completely. Thus, the hypothesis about the possibility of using ES for the development of cyber threat model is confirmed. It should be noted that based on the results of the simulation it was found that the same physical consequences can be caused by the implementation of different cyber threats. At the same time not in every case there is a violation of the basic properties of the relay protection system mentioned above. This allows us to put forward a hypothesis that for the stable functioning of the relay protection and automation subsystem of an energy facility it is not enough to provide only its basic properties and it is necessary to additionally ensure the property of the cybersecurity.

4 Conclusions

The main findings of the investigation are:

• Formed hypothesis about the insufficiency of providing the basic properties of the relay protection system for its stable functioning;

• A method for modelling cybersecurity threats based on the draft methodology for threat modelling of the FSTEC of Russia 2020 taking into account the industry specifics of the electric power industry;

• Demonstrated the possibility of using engineering approaches knowledge to simulate cybersecurity threats to the RPA subsystem of the digital substation;

• A demo prototype of the expert system has been developed taking into account possible combinatorics in deterministic conditions;

The results of the investigation have the ability to scale with further development by developing reference threat models for each type of component of the relay protection system. Further work is planned to create a working prototype of the expert system and its approbation on real objects (within the framework of R&D).

References

1. Strategic Buisiness Plan: official edition: approved by IEC Technical Committee, Power systems management and associated information exchange, 57 (29 November 2019)
2. V. Sidorovich, First Virtual Power Plant Created in Singapore [Electronic resource] (14.10.2019) Available at: https://medium.com/internet-of-energy/vpp-416fa87671f5 (accessed: 02.03.2020)
3. I. Chausov, Decentralization of system reliability [Electronic resource] (23.01.2020) Available at: https://medium.com/internet-of-energy/https-medium-com-p-89bf0a444f2a-89bf0a444f2a (accessed: 02.03.2020)
4. V. Sidorovich, Regional grids buy flexibility services from energy consumers [Electronic resource] (27.11.2019) Available at: https://medium.com/internet-of-energy/northern-powergrid-1d82c816c6aa (accessed: 02.03.2020)
5. I. Chausov, Hyper-personalization – a new word in the electricity trade [Electronic resource] (05.02.2020) Available at: https://medium.com/internet-of-energy/ed04c55a46ae (accessed: 02.03.2020)
6. Integrated annual report 2018: FGC UPS of Russia [Electronic resource] Available at: http://www.fsk-ees.ru/upload/docs/GO%20FSK%20EES%202018.pdf (accessed: 02.07.2019)
7. I. Leontev, A. Gurev, D. Nesveyanov, Features of the design of the relay protection system for new construction and reconstruction of the digital substation: presentation [Electronic resource], RMC «EKRA» Available at: http://digitalsubstation.com/wp-content/uploads/2019/08/Osobennosti-proektirovaniya-sistem-RZA-TSPS.pdf (accessed: 02.08.2019)
8. D. Gvozdev, M. Gribkov, Experience in the implementation of digital substations in the company “Rosseti Moscow Region”: scientific and technical journal “Electric Power, Transmission and distribution”, founder and publisher “Kabel”, Moscow, 4 (55), 42-46 (2019) ISSN: 2218-3116
9. E. Poviraev, Concept of the “Digital RES” project, Implementation experience: Yantarenergo: presentation [Electronic resource], NTI Energynet Available at: https://digitalsubstation.com/wp-content/uploads/2017/11/Tavrida-Elektrik-EnergyNet-TSPS-Kontseptsiya-TSRES.pdf (accessed: 02.08.2019)
10. E. Stamp Jason, A. Laviolette Randall, R. Phillips Laurence, et all, Impacts Analysis for Cyber Attack on Electric Power Systems: technical report (Albuquerque, New Mexico: Sandia National Laboratories, 2009)
11. Business Blackout, The insurance implications of a cyberattack on the US power grid: emerging risk report (Lloyd's and the University of Cambridge Centre for Risk Studies – Cambridge, 2015)
12. A. Motorin, V. Kharlamov, Variants of possible vectors of impact on relay protection equipment in real operating conditions: collection of reports of conference «Relay protection and automation of power systems 2017» S.-Petersburg, 896-899 (25-28 April 2017)
13. V. Kirilenkov, S. Vergazov, Technical solutions for relay protection and automation offered by Rosseti as part of the creation of Digital Substations: presentation [Electronic resource], Rosseti, Moscow (2018) Available at: http://digitalsubstation.com/wp-content/uploads/2018/04/3.-Rosseti.pdf (accessed: 30.03.2020)
14. V. Karantaev, An example of an IS expert system based on an ontological model: online-report of conference “EnergyNet Con”: YouTube video [Electronic resource], NRU MPEI, Moscow (2020) Available at: https://www.youtube.com/watch?v=MEWS9lVEGWA (accessed: 20.12.2020)