Modeling scenarios of extreme situations in the energy sector caused by cyber threats

Daria A. Gaskova[1], *Aleksei G.* Massel[1]

[1]Melentiev Energy Systems Institute SB RAS, 664058, Irkutsk, Lermontova str., 130

Abstract. The paper considers the violation of cybersecurity as a possibility of a real impact (intentional or accidental) from cyberspace on the physical infrastructure of a digital energy facility. In energy security studies, such impacts are considered as extreme situations, including critical and emergency situations. A model of scenarios of extreme situations in the energy sector caused by cyber threats using Bayesian Belief Network and the stages of modeling are considered in more detail. The five main stages are i) modeling cyber threats vectors of intrusion and advance towards the target asset; ii) modeling an attack on a target system in the technological segment of the local area network; iii) modeling technogenic threats to energy security caused by cyber threats; iv) modeling consequences at the level of the facility system; v) modeling consequences at the level of the infrastructure. This approach allows one to build cause and effect relationships from vulnerabilities in the cyber environment to the consequences. Modeling stages are aimed at increasing the level of cyber situational awareness, which, in turn, related with energy security issues.

Keywords. cyber threats, cybersecurity, semantic modeling methods, Bayesian Belief Network.

1 Introduction

Since the beginning of 2021, the number of attacks on the industry has increased and remains at a consistently high level [1]. If earlier companies hid incidents related to cyberattacks, or simply could not establish the real reason for an incident, now such incidents and their consequences are openly publicized. Thuswise the consequences of the attack on the Colonial Pipeline were so significant that four American states (North Carolina, Virginia, Georgia, and Florida) declared a state of emergency [2]. Among the cyber threat trends for industrial enterprises in 2021, Kaspersky Lab ICS CERT notes [3] that although the number of attacked computers is decreasing, the number of serious incidents still far from becoming decrease.

In studies of energy security, threats are traditionally divided into strategic and tactical ones. Recently, cyber threats have been classified as strategic [4]. This is associated with the fact that in addition to various extreme situations, the current infrastructure of power systems is specifically vulnerable to cyberattacks and physical attacks that can cause small and large-scale power outages. This problem is partly related to the spread and usage of information and communication technologies in electrical networks [5], and digital transformation of the energy sector in general. Digital technologies developing and being implemented in the Russian energy sector include the Internet of Things (IoT), 3D modeling, modeling and forecasting based on Big Data, Neural Networks, Cloud Computing, Virtual and Augmented Reality, Machine Learning, computer simulation based on Digital Twins, smart sensors, production robotization, Additive Manufacturing. [6]. Digital energy facilities are distinguished by a high dependence of the physical infrastructure on the information and communication infrastructure. Hence extreme situations concern in the energy sector due to the cybersecurity violation at one or several digital energy facilities is raised. The paper considers the violation of cybersecurity as a possibility of a real impact (intentional or accidental) from cyberspace on the physical infrastructure of a digital energy facility. Such concerns are associated with several factors: i) an increase in the number of vulnerabilities of critical information infrastructure due to the large market of software products in which various vulnerabilities are present, software complexity, and the emergence of new weaknesses caused by their joint usage ii) cyber negligence associated with the transition period of digital transformation and changes in enterprises business models, the maintenance of which requires qualified specialists in the field of information technology; iii) cyberattacks, in particular advanced persistent threat; iv) the application of software products based on artificial intelligence that doesn't provide clear understanding of the forecasts for experts (the "black box" principle, malicious interference in algorithms and processes), etc.

Cyber situational awareness also plays an important role under these conditions. Cyber situational awareness includes awareness of any suspicious or interesting activity taking place in cyberspace, where cyberspace includes any activity related to a computer network [7]. Cyber situational awareness is viewed from both a technical and a cognitive perspective. In the first case, the automation of the analysis of security events and information management using monitoring systems and tools for analyzing the security of the cyber environment contains a number of flaws. Among these flaws are the following: [8, 9]:

- focused on specific detecting attacks;

• high growth rates in the volume of information available for monitoring, which can quickly exceed the capabilities to analyse and store information by these tools;

• labour intensity of analysis approaches due to large amounts of data;

• and as a consequence, a high susceptibility to errors.

The cognitive side of situational awareness concerns a person's ability to understand the consequences and draw conclusions to make informed decisions [7].

The authors propose to apply semantic modeling methods to analyze the impact of cyber threats on energy facilities from the standpoint of energy security. The semantic modeling methods offer efficiencies under in the absence or incompleteness of data in modeling the behavior of systems, that is not susceptible to formal description or sufficiently accurate prediction.

Probabilistic modeling based on Bayesian Belief Network is proposed as a tool for modeling extreme situations in the energy sector caused by cyber threats. The article then presents a model and the steps for this modeling.

2 Model of extreme situations scenario in the energy sector caused by cyber threats

The structure of the scenario of extreme situations in the energy sector caused by cyber threats includes the following types of concepts:

- **Vulnerability** (V) is a set of the detected critical vulnerabilities in the cyber environment of the facility in question.
- **Cyber threat** (T) is a set of cyber threats to cyber assets.
- **Technogenic threat** (W) stands for the set of technogenic threats to energy security caused by cyber threats T.
- **Consequence** (C) denotes a set of consequences from threats T и W.

The structure of the scenario also includes a classification of concepts by the types presented above and by the segments of the local area network under consideration. The segments are guest, corporate, demilitarized zones, and technological ones.

The model based on the Bayesian Belief Network is proposed in the form of an acyclic, directed, weighted graph G such that:

$$G = (N, U; q), \quad (1)$$

where N is a set of vertices of the graph, U is a set of graph arcs, q is the vertex function.

Each vertex N_i of the graph G associated with random variable X_i for which

$$X_i \in \{X^V \cup X^T \cup X^W \cup X^C\}, \quad (2)$$

where $i = \overline{1,n}$ and $n = |V| + |T| + |W| + |C|$, X^V is a set of random variables corresponding to V, X^T is a set of random variables corresponding to T, X^W stands for the set of random variables corresponding to W, X^C denotes a set of random variables corresponding to C.

Vertex function q defined as

$$q: N \to B, \quad (3)$$

where B_i is weight matrix for vertex N_i. For each vertex N_i, the elements of this matrix are the probabilities of the corresponding random variable X_i.

Furthermore $\mathcal{P} = \{P(X_i|pa(X_i)): X_i \in X\}$ is conditional probability distribution for each variable from X, where $pa(X_i)$ is a set of parents vertex of X_i. If $pa(X_i) = \emptyset$, than $\mathcal{P}(X_i)$ are the prior probabilities of X_i. The description of the constraints on the set of arcs is described for the modeling steps.

3 Modeling scenarios of extreme situations in the energy sector caused by cyber threats

The development of probabilistic model of the scenarios of extreme situations in the energy sector caused by cyber threats includes the following steps to use to describe it:

- Modeling cyber threats vectors of intrusion and advance towards the target asset.
- Modeling an attack on a target system in the technological segment of the local area network;
- Modeling technogenic threats to energy security caused by cyber threats.
- Modeling consequences at the level of the facility system.
- Modeling consequences at the level of the infrastructure.

3.1. Modeling cyber threats vectors of intrusion and advance towards the target asset

The construction of cause and effect relationships between vulnerabilities and threats as a part of the graph covers the assets of the guest, corporate, demilitarized zone segments of the local computer network under consideration. Such cause and effect relationships are defined by two types of arcs, which are (X^V, X^T) or (X^T, X^V).

Both expert knowledge and projects aimed at researching cyber situational awareness, for example, the matrix of adversary tactics and techniques MITRE ATT&CK [10] are capable of being to structure fragmented knowledge about the possible behavior of an attacker. Positive Technologies in their research [11] presented heat maps, which reflect the most frequently used attack techniques on energy companies, based on the MITRE ATT&CK matrix. The consideration of the Internet of Things in Industrial Control System (ICS) security studies is often limited to remote terminal units (RTUs), programmable logic controllers (PLCs), intelligent electronic devices (IEDs), etc. Despite that position modeling at this stage can be extended by

considering the vulnerabilities of IoT devices that can be attacked in guest or corporate segments.

3.2. Modeling an attack on a target system in the technological segment of the local area network

At this stage, possible ways of disrupting the functioning of the target system in the cyber environment are formed. Michael J. Assante and Robert M. Lee in theis study [12] adapted the Cyber Kill Chain model for Industrial Control Systems, where they presented three categories of common methods for achieving functional impact on ICS. They are i) loss, ii) denial and iii) manipulation. They include a loss of view, denial of view, manipulation of view, denial of control, loss of control, manipulation of control, activation of safety, denial of safety, manipulation of safety and manipulation of sensors and instruments [12]. In [5] identifies seven groups of cyberattacks, depending on the ultimate goal of the attacker: i) bad measurement injection (Man-in-the-middle attack), ii) bad command injection (manipulating command signals), iii) control center impersonation attack, iv) communication delay attack, v) unresponsive command attack, vi) disabled RTU (denial of services attack), and vii) coordinated cyber-attack. Research [13] notes that data integrity attacks on control signals show a higher attack severity than on the measurement signals.

3.3. Modeling technogenic threats to energy security caused by cyber threats

At this stage of the formation of a part of the graph, connections between the attack on the target asset of the cyber environment and the functioning of the units of the energy facility are established. Connections are defined by arcs of the type (X^T, X^W) or (X^W, X^W).

Failures, explosions, and fires are classified as technogenic threats to energy security according to [14]. Such events can affect the uninterrupted reliable operation of energy facilities. Such events are different for facilities of different energy systems, an example of energy systems ontology is presented, for example, in [15].

In the electric power industry for generating facilities, such events include load growth on current transmission system, voltage instability, issues of management of active and reactive power resources, unnecessary load shedding, loss of visibility and power outages.

3.4. Modeling consequences at the level of the facility system

The stage is associated with the establishment of links between the events of the occurrence of technogenic threats caused by cyber threats and the possible consequences for the facility under consideration. Such consequences are characterized by damages. Links are defined by arcs of the type (X^W, X^C).

As an example, for a power generating facility, there are three technogenic threats: i) disconnection of generating capacities from the power grid; ii) failure of generating capacities; iii) launch of unplanned additional generation of electricity in the the power grid. Then it is possible to single out such consequences as downtime of production, undersupply of products, socio-economic and environmental consequences.

3.5. Modeling consequences at the level of the infrastructure

At this stage, cascading accidents can be considered. In [5] definition of a cascade failure is given as an uncontrolled sequential loss of system elements caused by an incident anywhere. The main problems emerging in this phase include transmission line overloads, voltage collapse, frequency oscillation, dynamic instability, and inappropriate under frequency load shedding [5]. In addition, due to the close dependence of critical infrastructure facilities, the failure of an energy facility may affect related critical infrastructure of a different type (for example, healthcare, chemical industry, transport highway, etc.). Such accidents are not predictable and are classified as rare high impact events. And while it is difficult to determine precise estimates of the probabilities of such events, it is noted that information from subject matter experts, including the use of Bayesian statistical methods, can help determine interval estimates [5].

Conclusions

This article describes the process of modeling scenarios of extreme situations in the energy sector caused by cyber threats, based on the use of a cyber threats scenario model using the Bayesian Belief Network. The modeling process includes five stages: i) modeling cyber threats vectors of intrusion and advance towards the target asset; ii) modeling an attack on a target system in the technological segment of the local area network; iii) modeling technogenic threats to energy security caused by cyber threats; iv) modeling consequences at the level of the facility system; v) modeling consequences at the level of the infrastructure.

Semantic modeling methods make it possible to formalize disparate information and knowledge of experts. However, they require much labor contribution to search and structure knowledge. The article presents the use of only one semantic model, though the approach proposed by the authors includes the use of ontological models and the technology of expert systems to reduce the labor contribution of an expert and an analyst in formalizing, structuring and further searching for information necessary for modeling.

This approach allows one to build cause and effect relationships from vulnerabilities in the cyber environment to the consequences at the system level of the facility and, some possible consequences at the infrastructure level, and to carry out a probabilistic assessment even taking into account the incompleteness of information about the probabilities.

This work was executed within the framework of project on state task MESI SB RAS FWEU-2021-0007 № AAAA-A21-121012090007-7. The studying of separated

aspects was supported by RFBR grants No 19-07-00351, No 20-010-00204, No 19-57-04003.

References

1. "Positive Research 2021", Analytical articles by Positive Technologies. Available at https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/positive-research-2021-rus.pdf (in Russian).
2. "Dark Chronicles: what the attack on the Colonial Pipeline led to", Report of Kaspersky Lab ICS CERT. Available at https://ics-cert.kaspersky.ru/reports/2021/05/21/darkchronicles-the-consequences-of-the-colonial-pipeline-attack/ (in Russian).
3. "Cyber Threats to Industrial Enterprises in 2021", Report of Kaspersky Lab ICS CERT. Available at https://ics-cert.kaspersky.ru/reports/2020/12/02/ics-threat-predictions-for-2021/ (in Russian).
4. L.V. Massel, N.I. Voropay, S.M. Senderov, A.G. Massel, Cybersecurity issues. **4**(17) (2016) Pp. 2-10. DOI: 10.21681/2311-3456- 2019-2-42-49 (in Russian).
5. A. Gholami, T. Shekari, M.H. Amirioun, F. Aminifar, M.H. Amini, A. Sargolzaei, IEEE Access. **6** (2018) Pp. 32035–32053. DOI:10.1109/ACCESS.2018.2845378.
6. "Energy Strategy of the Russian Federation until 2035", decree of the Russian Federation Government no.1523-p dated 09.06.2020 Available at http://government.ru/docs/all/128340/ (in Russian).
7. U. Frank, J. Brynielsson, Computer Security. **46**, 18-31 (2014), Stockholm, Sweden. DOI: 10.1016/j.cose.2014.06.008.
8. Y. Cheng, J. Deng, J. Li, S.A. DeLoach, A. Singhal, X. Ou, (2014) in Cyber Defense and Situational Awareness. Advances in Information Security. Vol 62 (2014). DOI: 10.1007/978-3-319-11391-3_13.
9. E. D. Knapp, J. T. Langill, in Industrial Network Security. Pp. 351-386. DOI:10.1016/b978-0-12-420114-9.00012-5.
10. MITRE ATT&CK. knowledge base of adversary tactics and techniques. Available at https://attack.mitre.org/
11. "APT attacks on the Russian fuel and energy complex: an overview of tactics and techniques", Analytical articles by Positive Technologies. Available at https://www.ptsecurity.com/ru-ru/research/analytics/apt-attacks-energy-2019/
12. M. J. Assante, R.M. Lee "The Industrial Control System Cyber Kill Chain". Available at https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-systemcyber-kill-chain-36297.
13. V. K. Singh, M. Govindarasu and R. Nuqui, 2021 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT). Pp. 1-5 (2021). DOI: 10.1109/ISGT49243.2021.9372232.
14. N.I. Pyatkova, V.I. Rabchuk, S.M. Senderov, M.B. Cheltsov, "Energy Security in Russia: Problems and Solutions". (2011) Novosibirsk: SB RAS, 211 p. (in Russian).
15. L.V. Massel, 3rd Russian-Pacific Conference on Computer Technology and Applications (RPC). (2018) P.p. 1-5. DOI:10.1109/rpc.2018.8482138.