Technology of the Intelligent System Application for Cyber Threat Analysis at Energy Facilities

Daria A. Gaskova
Melentiev Energy Systems Institute of Siberian Branch of the Russian Academy of Sciences
Irkutsk, Russia
gaskovada@gmail.com

Aleksei G. Massel
Melentiev Energy Systems Institute of Siberian Branch of the Russian Academy of Sciences
Irkutsk, Russia
amassel@gmail.com

***Abstract*—The article discusses the methods of system analysis for research of cyber threats to energy facilities. This study proposes application of semantic methods to analyse the impact of cyber threats to energy facilities from the point of view of energy security. Such methods are used under conditions of lack or incompleteness of data on vulnerabilities in software and hardware equipment and on Cyber Security incidents in the energy sector. These methods are also employed in modelling the system behaviour that cannot be accurately forecasted or described formally. The article represents the technology of this Intelligent System application, comprising steps of cyber threats identification, scenarios modelling of extreme situations caused by the implementation of cyber threats, and risk assessment. The technology was developed to evaluate the number of critically vulnerable assets, explain the composition and the likelihood of implementing cyber threats that could cause extreme situations in the energy sector, and to assess risk from their implementation. The deployment of the proposed technology could simplify the process of analysing Cyber Security threats at energy facilities.**

Keywords—cyber threats; energy security; intelligent system; semantic modelling methods.

I. Introduction

The tendency of the digital transformation in the energy sector is currently observed in Russia. It is accompanied by the use of technologies such as Distributed Systems, Cloud Technologies, Big Data, Intelligent Technologies, and others. Ontological modelling and Blockchain technology are also promising technologies for the development of the urban energy system [1]. Up-to-date solutions for the technological process automation at energy facilities are becoming more complex and using modern digital technologies [2]. As a result, not only functionality, but also reliability and security of IT infrastructure is to be ensured at modern energy facilities [3,4]. Use of new technologies creates new Cyber Security risks. The threats list to energy security (ES) has been expanded by cyber threats within the context of technological innovations [5].

The analysis of cyber threats influence on the occurrence of the extreme situation in the energy sector is carried out within the scenario approach using the tool of Bayesian Belief Networks (BBN) [6] and expert system technology. The article describes the key points of the Intelligent System under development to support this analysis. BBN are involved within Semantic Modelling [7] and are applied in the research of Critical Infrastructures. The Intelligent System for analysing cyber threats to energy facilities is developing on the basis of the principles for the design Intelligent Instrumental Environment (IIE) [8] and it is aimed at solving one complicated formalized problem.

II. Cyber Threat Analysis at Energy Facilities

Modern sophisticated technological facilities include extensive physical infrastructure and are supported by information and communication technologies (ICT) [9]. Weaknesses and problems are found in areas of intersection of Information Security, Network Security, Internet Security, and Applications Security. Identifying and correcting them are often difficult tasks. The use of new ICT for industrial control systems and for energy facilities, in particular, creates new risks. The process of identifying, quantifying, analysing and evaluating risks, and their treatment should be an integral component of the overall management decision-making process. [10]. This process includes risk management containing the process of information systems security management. IT risk analysis is a key element in the process of information systems security management. In the context of IT systems security, the risk of IT systems is overall measure of probability and seriousness of situation, in which a given threat uses specific weakness, causing loss or damage of system assets, therefore indirect or direct loss for organization [11]. The issues of Cyber Security can be investigated using system risk analysis [12].

In this context, the authors understand cyber threat analysis at energy facilities as a part of the process of analysing IT risks that could be caused by such security threats realization to the extent that they could implement ES threat and give rise to extreme situations.

The following stages of the cyber threats analysis at energy facilities are highlighted:

1. *Iidentification of vulnerable assets* and cyber threats to energy facilities.

2. *Analysis of the causes and effects* of the energy security violation invoked by the cyber threats during modelling of extreme situations scenarios.
3. *Description and analysis of risks* from the cyber threats consequences using Bayesian probabilities.

To support these stages, Intelligent System is discussed in the next part of the article.

III. Intelligent System

Intelligent System [13] includes a set of three main components: 1) the production expert system for identifying the vulnerabilities of the information and communication system and the corresponding cyber threats; 2) the unit of BBN for probabilistic modelling of extreme situations at energy facilities caused by the implementation of cyber threats; 3) and the unit to assess risk from violation of cyber and energy security.

The production expert system “Cyber” is based on an object-oriented approach. The knowledge model includes a systematized list of cyber threats to the information technology systems (ITS) and the physical equipment divided according to energy facilities classifications, ITS assets, their vulnerabilities, and their sources.

The unit “ThreatNet” for the formation of scenarios of extreme situations caused by the cyber threats implementation, is based on the BBN. The user solves problems of probabilistic forecasting the consequences for an energy facility from vulnerabilities and cyber and ES threats realization through direct derivation in BBN. Expectation estimates of a particular state in the model are based on Bayesian probabilities.

The unit of the risk assessment “RiskDiagram” includes classifying risk according to the “acceptable”, “average”, and “critical” scale, and displaying risks on the heat map and radar chart.

Intelligent System users are divided into three groups. The first group includes security engineers that are specialists in the field of Information Security or, in the absence of those, administrators of the local computer network. The second group includes knowledge engineers. Depending on the level of detail of the investigation they can be both experts in the field of energy security and operators/energy engineers at the facility. The third group of users includes Cyber Security and energy security risk analysts.

There are two options for using the Intelligent System:

- Cyber threats analysis of the existing information technology systems, including risk analysis for the energy facility.
- Cyber threats analysis in the selection of new IT solutions at the facility, including comparing scenarios of possible behavior of ITS and corresponding risks from the implementation of a particular solution.

IV. Technology of the Intelligent System application for cyber threat analysis at energy facilities

Figure 1 illustrate the main activities of the technology. The technology supports the following steps:

1. Cyber threats identification.
2. Modelling scenarios of extreme situations in the energy sector that may be caused by cyber threats.
3. Risk assessment of extreme situations.

Table 1 shows units of Intelligent System, user groups, and technology steps.

TABLE I. Technology and tools for analyzing cyber threats of energy facilities

Technology step	User groups	Units
Cyber threats identification	Security engineers	Expert system “Cyber”
Modelling scenarios	Energy knowledge engineers (experts)	“ThreatNet”
Risk assessment	Analysts	“RiskDiagram”

Cyber threats identification at energy facilities stage contains two preparatory activities. First, the survey of the information technology system. The description of the assets list in each subsystem of ITS is carried out during this activity. Information, software and hardware could be assets. Such list contains descriptions of the asset type, its place in the physical subsystem of an energy facility, and its significance. Secondly, the definition of a list of vulnerabilities in assets. Some vulnerabilities couldn't be promptly eliminated due to the lack of vendor updates or specifications of the technological process. Special scanners, databases, and guidelines can be used to determine vulnerabilities. The description of the vulnerabilities list usual is carried out by the metrics developed within the framework of The Common Vulnerability Scoring System (CVSS).

Potential cyber threats that use the detected asset vulnerabilities are proposed to be identified based on the attack vectors that are relevant to the energy facility. Two main attack vectors are identified in this study: 1) targeted attacks aimed at industrial equipment; 2) non-targeted attacks aimed at IT-infrastructure, which could adversely affect the normal functioning of industrial systems. The result of this technology step is a description of ITS assets, critical vulnerabilities, a list of cyber threats to an energy facility, and attack vectors for a specific power facility.

Modelling scenarios of extreme situations in the energy sector caused by cyber threats stage contains scenario formation and direct derivation in BBN. The scenario structure includes concept types and their interrelations and constitutes a graphical model, which is further analysed on the basis of energy security research methods [14].

The following types of concepts are highlighted:

- Factors affecting an extreme situation.
- ITS asset vulnerabilities.
- Threats to cyber and energy security.
- Consequences of an extreme situation in the energy sector.

Cyber threats are considered as initiating events for the ES threats, which could be software and hardware failures, equipment damage, and loss of communication. The main consequences of the ES threats could be loss of load, frequency, power, and disconnection of consumers.

As a result of the stage, a scenario of an extreme situation caused by cyber threats is formed, the BBN is completed, the probabilities of the consequences are determined.

Risk assessment stage should be carried out with determination of qualitative and quantitative risk parameters. Such parameters are determined by an expert. The use of a hybrid method of risk analysis allows us to do a more complete estimation likelihood and level of damage from an extreme situation.

The result of user interaction with the risk assessment unit can be used to plan technological regimes of the system in extreme situations, to improve the software and hardware complex used, to develop and introduce new models and algorithms for automated control tasks, and to prepare guidance materials. Since the result of working with the unit is a list of risks of extreme situations at a facility, such information, in case of the electric power industry, could be useful to energy sales companies, which ensure minimizing business risk, including extreme situations.

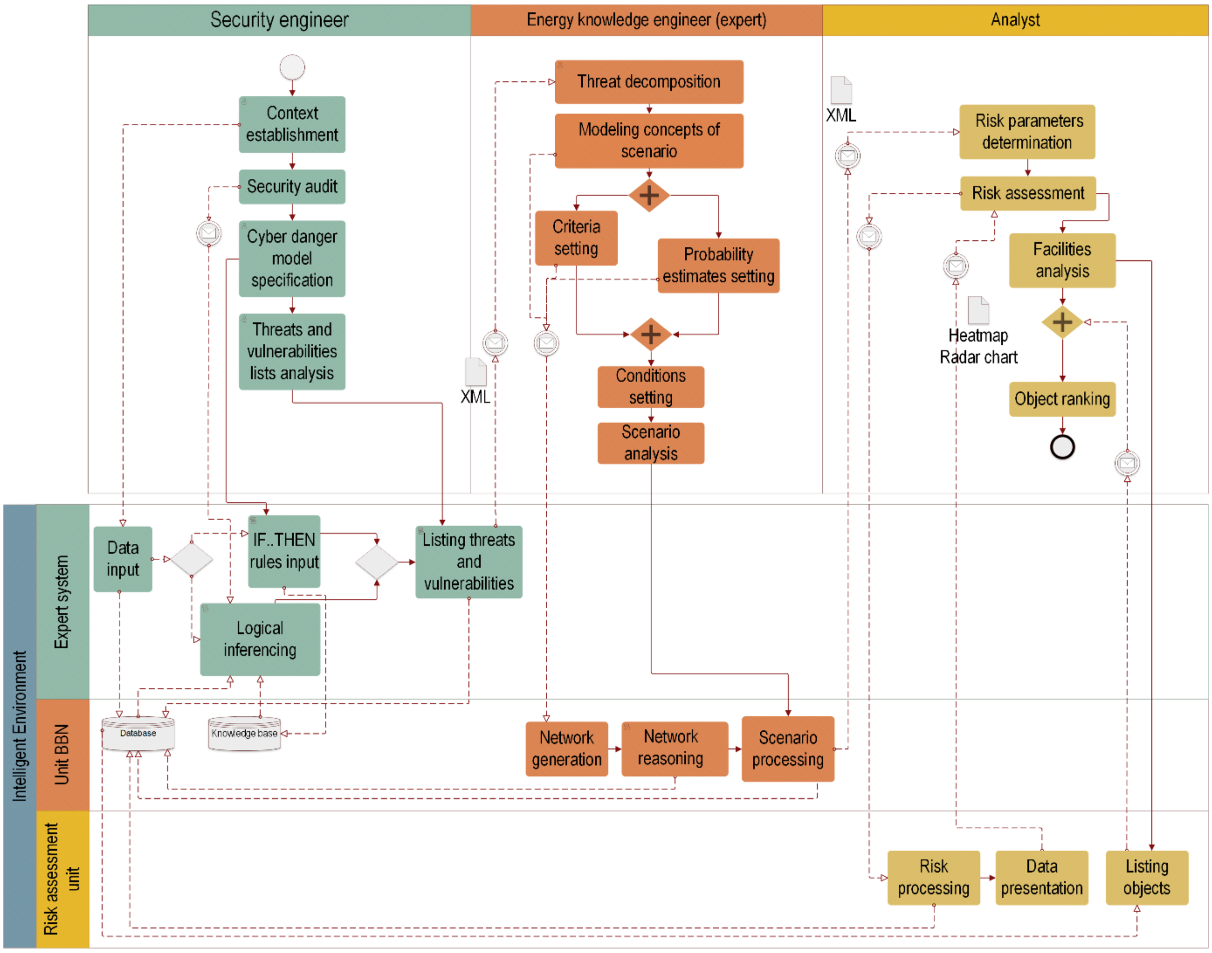

Fig. 1. Technology of the Intelligent System application for cyber threat analysis at energy facilities in bpmn 2.0 notation.

V. CONCLUSION

The article describes the technology aimed at identifying energy facilities most susceptible to Cyber Security risk, the level of such risk and determining their critical consequences. This technology is supported by the Intelligent System, which development is based on the systems analysis and semantic modelling methods. The Technology of the Intelligent System application combines the efforts of experts in various object domains and serves to conduct the full risk assessment of cyber threats to energy facilities.

In comparison with traditional approaches to ensuring Information Security, the proposed technology is aimed at identifying vulnerabilities and cyber threats, the implementation of which could cause a disruption in the functioning of an energy facility (seen as an extreme situation). Also, the proposed technology supports the probabilistic assessment of extreme situations in the energy sector caused by cyber threats.

Designing Intelligent System based on the principles of IIE allows to complement it with units that implement other semantic modelling methods. For example, there are Dynamic Cognitive Map methods for analysing cyber threats. Additional methods will allow to make a comprehensive assessment of the ES in the energy sector. At the same time, the stages of technology do not require significant changes since it is based on the general principles of system analysis.

ACKNOWLEDGMENT

This work was performed within the framework of project according to state assignment MESI SB RAS №AAAA-A17-117030310444-2. The study of separated aspects was supported by RFBR grants № 19-07-00351, № 19-57-04003, № 18-07-00714, № 18-37-00271, № 18-57-81001, № 17-07-01341.

REFERENCES

[1] Zhang C., Romagnoli A., Zhou L., and Kraft M. (2017) “From Numerical Model to Computational Intelligence: The Digital Transition of Urban Energy System.” Energy Procedia 143: 884–890.

[2] Irmak E., and Erkek I. (2018) “An overview of cyber-attack vectors on SCADA systems.” 6th International Symposium on Digital Forensic and Security (ISDFS), 2018. doi:10.1109/isdfs.2018.8355379

[3] Zio E. (2016) “Challenges in the vulnerability and risk analysis of Critical Infrastructures.” Reliability Engineering & System Safety 152: 137–150. doi:10.1016/j.ress.2016.02.009

[4] Aven T. (2016) “Risk assessment and risk management: Review of recent advances on their foundation.” European Journal of Operational Research 253 (1): 1–13. doi:10.1016/j.ejor.2015.12.023

[5] Massel L.V., Voropai N.I., Senderov S.M., Massel A.G. (2016) “Cyber Danger as one of the strategic threats to Russia’s Energy Security.” Cybersecurity issues 4 (17): 2-10 (in Russian).

[6] Massel L.V., Pyatkova E.V. (2012) “Application of Bayesian Networks for the intelligent support of Energy Security problem researches.” Proceedings of Irkutsk State Technical University 2: 8-13 (in Russian).

[7] Massel L.V., Massel A.G. (2013) “Semantic technologies based on the integration of Ontological, Cognitive and Event modeling.” Proceedings of III International Science and Technology Conference “OSTIS-2013” Minsk; 247-250 (in Russian).

[8] Massel L.V., Massel A.G. (2012) “Intelligent computing in researches of energy sector development directions”, Bulletin of Tomsk Polytechnic University, 321(5): 135-140

[9] Sridhar S., Hanh A., Govindarasu M. (2012) “Cyber-physical system security for the electric power grid.” Proc. IEEE 100 (1): 210-224.

[10] Yacov Y. Haimes. (2008) “Systems-based risk analysis”. In: “Global Catastrpphic Risks” Nick Bostrom, Milan M. Cirkovic (ed), Oxford; 146-163.

[11] Rot A. (2008) “IT Risk Assessment: Quantitative and Qualitative Approach.”, Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA

[12] Aven T. (2011) “Quantitative Risk Assessment: The Scientific Platform.” Cambridge: Cambridge University Press. doi:10.1017/CBO9780511974120

[13] Massel A.G., Gaskova D.A. (2018) “Methods and approaches to cybersecurity ensuring for enterprises of digital energy industry.”, Energy Policy 5: 62-72 (in Russian)..

[14] Pyatkova E.V. (2013) “Methods of Energy Security threats modelling with Bayesian Belief Networks.” Modern Technologies.