UDC 004.492

Cyber Security Logical and Probabilistic Model of a Critical Infrastructure Facility in the Electric Energy Industry

Lesia Alekseichuk[1], Oleksii Novikov[1], Andrii Rodionov[1], Dmytro Yakobchuk[1]

[1] *National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», 37, Prosp. Beresteyskyi, Kyiv, 03056, Ukraine*

Abstract

In the work, a cyber security logical and probabilistic model of a critical infrastructure facility in the energy sector was developed and investigated. The cyber security logical and probabilistic model describes the development of adverse events that arise in the Industrial Control System of the electrical network from the realization of possible threats from cyberspace, such as attacks on the protection system through the corporate network, connection through a modem and wireless connection. The resulting model is based on sequentially developed structural, logical and probabilistic models.

The field of use of the developed model is automation systems for designing information protection systems or designing trajectories of attacks on these systems. The model was also applied to study the sensitivity of the probability of the development of adverse events to variations in the probability of realization of possible threats to the system.

Keywords: Critical infrastructure, Cyber security logical and probabilistic model, ICS, SCADA

Introduction

With the development of information and communication technologies, the number of threats and cyberattacks on critical infrastructure objects from cyberspace is increasing. In particular, in recent years, Ukraine has suffered and overcome the consequences of dozens of powerful cyber attacks. Among the most large-scale and well-known were - an attack against the information system "Vybory" during the presidential elections of Ukraine (May 2014), cyber attack of the BlackEnergy Trojan program on "Prykarpattia-oblenergo", "Chernivtsioblenergo" and "Kyivoblenergo" (December 2015), attack on "Ukrenergo" (December 2016), M.E.Doc backdoor attack (April 14, 2017), large-scale attack by the NotPetya worm (June 27, 2017) and others.

The intensity of cyberattacks on critical infrastructure facilities can be explained both by the motivation of attackers and by defects in the automated process control systems of Industrial Control System, systems of Supervisory Control and Data Acquisition of critical infrastructure and their components.

At the moment, a lot of attention is paid to issues of ensuring cyber security of critical infrastructure objects. The works [1] - [3] analyzed possible threats to critical infrastructure objects. The relevance and importance of cyber protection of these objects at the country level have been determined.

Threat modeling and risk analysis is an effective tool for designing, researching and monitoring the process of operating critical infrastructure facilities and has been studied by many scientists. In works [4], [5], the tasks of threat modeling, cyber security analysis and other aspects of the security of critical infrastructure objects are considered, taking into account feedback, cascading effects and relationships between objects. In works [6], [7] models of cyber security analysis of objects of critical infrastructure of the energy sector are proposed.

In [8], a logical and probabilistic method for assessing the security of structurally complex systems was proposed and developed. In works [9] - [14], the problems of further development and use of the logical and probability method in various fields were considered. In works [13], [14], the problems of modeling the development of adverse cyber security events were solved using the logical and probabilistic method.

Recently, the energy infrastructure has been a special object of attention of cyber-attackers. Taking into account the importance and relevance of cyber protection of the mentioned objects and the insufficient development of the problem, it is currently necessary to conduct further scientific research.

The aim of the research. The purpose of the work is the development and research of a cyber security logical and probabilistic model of a critical infrastructure object in the energy sector, subject to the realization of a set of possible threats from cyberspace.

Logical and probabilistic cyber security risk model of Industrial Control System. Consider the threats from cyberattacks on critical infrastructure facilities in the energy sector, which were identified in a report of the US Government Accountability Office (US GAO) at the request of the US Congress [3]. In the report states that the protection of objects of this class is an important and relevant component of US national security.

A typical structure of an electric network (Fig. 1) consists of three levels: generation and storage, transmission and distribution of electricity between consumers [3].

The basis of the first level contains power stations, renewable energy sources, energy storage equipment, step-up transformer substations. The second level consists of long-distance high-voltage power transmission lines. The third - step-down transformer substations, users, as well as low-voltage renewable sources of energy production and storage.

This network is managed by an Industrial Control System (ICS). The ICS includes a Supervisory Control and Data Acquisition (SCADA) together with a Distributed Control System (DCS) and a system of Programmable Logic Controller (PLC). In some cases, the functions of the ICS can be performed by the SCADA system.

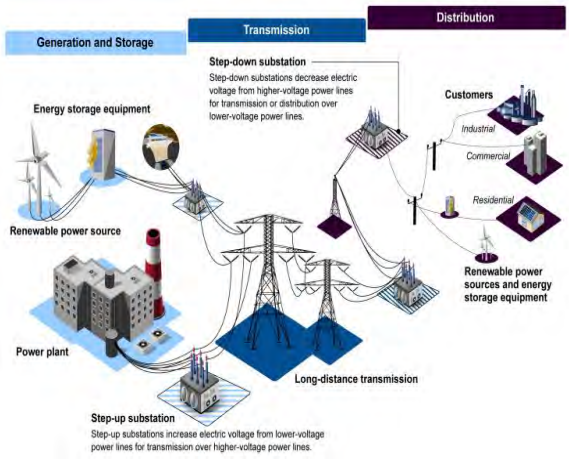

Figure 1: The electrical network structure [3]

Unfortunately, ICS systems have significant shortcomings in information security, which are implemented by Cyber Security Systems (CSS).

Due to the ubiquity of IP protocol and web technologies (WebSCADA), ICS inherent threats to conventional IT systems. In addition, the vast majority of DCS and PLC systems have imperfect or outdated information protection elements. In report [3], the main cyber threats to the energy network management system were identified (Fig. 2).

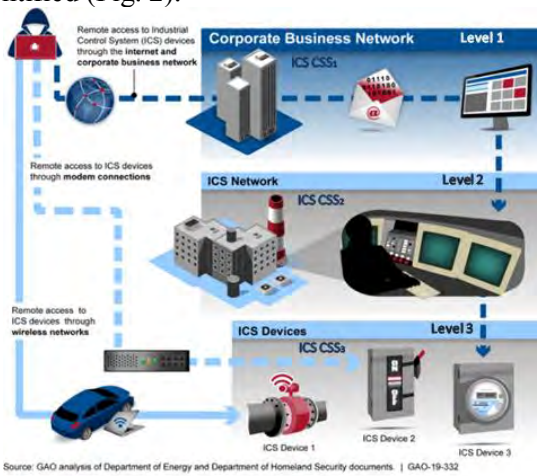

Figure 2: The main cyber threats to the energy network management system [3]

As defined in the report, the attacker has three possible scenarios for conducting a remote attack on the ICS: the first is via the Internet - access and the corporate business network, the second is a connection via a modem, and the third is via a wireless connection.

Unfavorable events that occur in the ICS of the electrical network from the realization of possible threats from cyberspace can be estimated using a logical and probability model [8].

According to the procedure for building logical and probabilistic models, we will form a structural, logical and probabilistic model of ICS security of the electric network.

Based on the functional scheme of conducting a remote attack on ICS control bodies (Fig. 2), the initiating events can be determined (Fig. 3): interception of control of ICS control bodies via the Internet - access through the corporate business network (event 1), over a modem connection (event 2) and over a wireless connection (event 3). Initiating conditions define the fact that the attacker has overcome the cyber protection systems of the corporate network (upper level) ICS CSS_1 (condition 4), distributed control system network cyber security systems (middle level) DCS ICS CSS_2 (condition 5) and programmable logic controller system cyber security systems (low level) PLC ICS CSS_3 (condition 6).

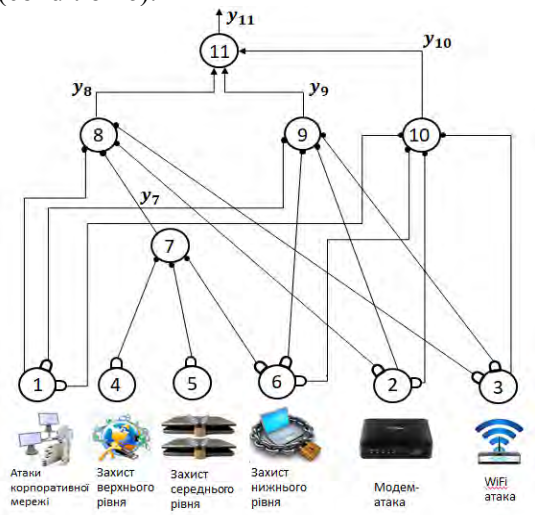

Figure 3: A direct structural diagram of the development of an adverse event

Fig. 3 shows the events that lead to the occurrence of an undesirable event - the compromise of the protection system of the control bodies of the lower-level PLC ICS CSS_3 automatic control system. An event will occur if at least one of the three triggering events 1-3 occurs.

At the first level, 6 functional vertices are depicted, which denote the initial elementary random events x_1 - x_6. The mentioned events occur with known probabilities of their occurrence P_j, $j=1,..,6$.

Table 1. System of logical equations development of an adverse event from implementation of possible threats

$y_1 = x_1$	$y_7 = \bar{y}_4\,\bar{y}_5\bar{y}_6$
$y_2 = x_2$	$y_8 = y_1\bar{y}_2\bar{y}_3y_7$
$y_3 = x_3$	$y_9 = \bar{y}_1y_2\bar{y}_3\bar{y}_6$
$y_4 = x_4$	$y_{10} = \bar{y}_1\bar{y}_2y_3\bar{y}_6$
$y_5 = x_5$	$y_{11} = y_8 \vee y_9 \vee y_{10}$
$y_6 = x_6$	

In the table 1 shows a system of logical equations under which an undesirable event will occur:

- the direct output function $y_{11} = y_8 \vee y_9 \vee y_{10}$ reflects the general conditions for the occurrence of an undesirable event, which includes the disjunction of three events, namely y_8 - the interception of control of the ICS control bodies by access through the corporate business network (event 1), y_9 – gaining access through a modem connection (event 2), y_{10} – gaining access through a wireless connection (event 3);

- the event of interception of the management of the ICS control bodies at the lower level by access through the corporate business network $y_8 = x_1\bar{x}_2\bar{x}_3y_7$ occurs on the condition that there is an attack x_1 on the corporate business network, there are no direct attacks x_2 and x_3 through modem and wireless connection and execution conditions $y_7 = \bar{x}_4\bar{x}_5\bar{x}_6$ of simultaneous conjunctive overcoming of three levels of cybernetic protection mechanisms x_4, x_5 and x_6;

- the event of interception of the management of the control bodies at the lower level by access through the modem connection $y_9 = \bar{x}_1x_2\bar{x}_3\bar{x}_6$ occurs under the condition of the presence of an attack x_2 via the modem connection, the absence of direct attacks x_1 and x_3 via the corporate business network, wireless connection uniting and overcoming the mechanism of cybernetic protection x_6;

- interception of lower-level controls by access via wireless connection $y_{10} = \bar{x}_1\bar{x}_2x_3\bar{x}_6$ occurs under the condition of presence of attack x_3 via wireless connection, absence of direct attacks x_1 and x_2 via corporate business network

and modem connection and overcoming the mechanism of cyber protection x_6.

By combining the logical conditions (Table 1) and solving the corresponding system of logical equations, we will obtain the conditions for the realization of an undesirable event - the compromise of the protection system of the control bodies of the automatic level control system PLC ICS CSS_3:

$$y_{11} = (x_1\bar{x}_2\bar{x}_3(\bar{x}_4\bar{x}_5\bar{x}_6)) \vee (\bar{x}_1x_2\bar{x}_3\bar{x}_6) \vee \vee(\bar{x}_1\bar{x}_2x_3\bar{x}_6) = (x_2\bar{x}_1\bar{x}_3\bar{x}_6) \vee (x_3\bar{x}_1\bar{x}_2\bar{x}_6) \vee \vee(x_1\bar{x}_2\bar{x}_3\bar{x}_4\bar{x}_5\bar{x}_6). \quad (1)$$

All members of the disjunction (1) are pairwise orthogonal, so we will obtain analytical indicators of probability estimation using the corresponding probability functions. In general, the procedure of orthogonalization of logical functions can be performed with the help of standard Python language libraries.

Using the theorems of multiplication of probabilistic dependent events and addition of probabilities of incompatible events, we will rewrite relation (1) in probabilistic form:

$$P_c = P_2Q_1Q_3Q_6 + P_3Q_1Q_2Q_6 + P_1Q_2Q_3Q_4Q_5Q_6 = = (P_2Q_1Q_3 + P_3Q_1Q_2 + P_1Q_2Q_3Q_4Q_5)Q_6 , \quad (2)$$

where P_c is the probability of an undesirable event, P_j, $j=1,..,6$ is the probability of the original elementary random events, Q_j, $j=1,..,6$ is the probability that the undesirable event will not occur.

Given that $Q_j = 1–P_j, j=1,..,6,$ we rewrite relation (2) in the form:

$$P_c = [P_2(1-P_1)(1-P_3) + P_3(1-P_1)(1-P_2) + +P_1(1-P_2)(1-P_3)(1-P_4)(1-P_5)](1-P_6). \quad (3)$$

Ratio (3) is a logical-probabilistic model of the probability of an undesirable cyber security event of a critical infrastructure object in the energy sector in the event of the realization of a set of possible threats from cyberspace.

Examples of the use of the logical and probability model. The main purpose of the logical and probability model (3) is to use it in automation systems for designing information protection systems or designing attack trajectories for these systems. At the same time, this model can directly be the basis for studying some properties of the system under consideration.

Let's consider several examples of the use of the logical and probability model (3) of the development of an adverse cyber security event from the realization of possible threats. The problem statements of such studies to determine the properties of reliability or safety of complex systems were formulated in the paper [8].

We will determine the probability of the development of an adverse cyber security event from variations in the probability of the implementation of initial threats to the ICS system. For this, by the method of expert evaluations, we determine the probabilities P_j, $j=1,..,6$ of the realization of the original elementary random events (threats) x_j, $j=1,..,6$ (Table 2).

Table 2. Probabilities P_j, $j=1,..,6$ of initial elementary random events

Probabilities of realization of initial elementary random events	P_j, $j=1,..,6$	Value
System attack through the corporate network	P_1	0.5
System attack through modem connection	P_2	0.6
System attack via Wi-Fi connection	P_3	0.8
Overcoming the top-level corporate network security system	P_4	0.7
Overcoming the security system of the corporate network of the middle level	P_5	0.1
Overcoming the lower-level corporate network security system	P_6	0.9

Substituting the values of the probabilities $P_j, j=1,..,6$ into the ratio (3), we get P_c = 0.027 - the probability of the development of an adverse event from the realization of possible threats to the ICS system.

The second example of the use of the logical and probability model (3) is the determination of the sensitivity of the system to a positive change in its elements. To do this, we successively differentiate relation (3) with respect to $P_j, j=1,..,6$ and obtain:

$$\partial P_c/\partial P_1 = -P_2(1-P_3)(1-P_6) - P_3(1-P_2)(1 - -P_6) + (1-P_2)(1-P_3)(1-P_4)(1-P_5)(1-P_6);$$
$$\partial P_c/\partial P_2 = (1-P_1)(1-P_3)(1-P_6) - P_3(1 - -P_1)(1-P_6) - P_1(1-P_3)(1-P_4)(1-P_5)(1-P_6);$$
$$\partial P_c/\partial P_3 = -P_2(1-P_1)(1-P_6) + +(1-P_1)(1 - -P_2)(1-P_6) - P_1(1-P_2)(1-P_4)(1-P_5)(1 - -P_6);$$
$$\partial P_c/\partial P_4 = -P_1(1-P_2)(1-P_3)(1-P_5)(1-P_6);$$
$$\partial P_c/\partial P_5 = -P_1(1-P_2)(1-P_3)(1-P_4)(1-P_6);$$
$$\partial P_c/\partial P_6 = -P_2(1-P_1)(1-P_3) - P_3(1-P_1)(1 - -P_2) - P_1(1-P_2)(1-P_3)(1-P_4)(1-P_5). \quad (4)$$

Substitute the probabilities P_j, $j=1,..,6$ (Table 2) into the system of equations (4). The results are presented in Table 3.

Table 3. System sensitivity $\partial P_c/\partial P_j$, $j=1,..,6$ to changes in parameters P_j, $j=1,..,6$

System sensitivity	System sensitivity, $\partial P_c/\partial P_j$, $j=1,..,6$	Value
The sensitivity of the system to an attack through the corporate network	$\partial P_c/\partial P_1$	-0.04
Susceptibility of the system to an attack through a modem connection	$\partial P_c/\partial P_2$	-0.03
Susceptibility of the system to an attack through a Wi-Fi connection	$\partial P_c/\partial P_3$	-0.01
The sensitivity of the system to overcoming the protection system of the corporate network of the upper level	$\partial P_c/\partial P_4$	-0.04
The sensitivity of the system to overcoming the protection system of the corporate network of a medium level	$\partial P_c/\partial P_5$	-0.09
The sensitivity of the system to overcoming the protection system of the corporate network of the lower level	$\partial P_c/\partial P_6$	-0.02

Conclusions

A cyber security logical and probabilistic model of a critical infrastructure facility in the energy sector has been developed and researched. The logical and probabilistic model describes the development of adverse events that occur in the ICS of the electrical network during the action of various threats from cyberspace. Threats include attacks on cyber protection systems through corporate networks, modem connections, and wireless connections. To create the final model, structural, cyber security logical and probabilistic models were developed sequentially.

The main area of use of the logical and probability model is systems for automating the design of information protection systems or designing the trajectories of attacks on these systems. The model was also applied to study such properties of the system as the sensitivity of the probability of the development of adverse events to the variation of the probabilities of the realization of possible threats to the system.

References

[1] Konstantin M. Zuev, Michael Beer, Reliability of Critical Infrastructure Networks: Challenges. Access mode: http://www.researchgate.net/publication/312043117

[2] US GAO Report «Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems » GAO-04-628T, March 30, 2004. Access mode: https://www.gao.gov/products/gao-04-628t, 25 p.

[3] US GAO Report «Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid» GAO-19-332, August 26, 2019. Access mode: https://www.gao.gov/products/gao-19-332, 94p.

[4] Dinesh Kumar Saini. Cyber Defense: Mathematical Modeling and Simulation. International Journal of Applied Physics and Mathematics, Vol. 2, No. 5, September 2012, p. 312-315. Access mode: https://www.researchgate.net/publication/272892530_Cyber_Defense_Mathematical_Modeling_and_Simulation

[5] Juan Fernando Balarezo, Song Wang, Karina Gomez Chavez, Akram Al-Hourani, Sithamparanathan Kandeepan A survey on DoS/DDoS attacks mathematical modelling for traditional, SDN and virtual networks. Engineering Science and Technology, an International Journal, Vol. 31, July 2022, 15 p. Access mode: https://www.researchgate.net/publication/355579987_A_survey_on_DoSDDoS_attacks_mathematical_modelling_for_traditional_SDN_and_virtual_networks

[6] Saeed Ahmadian, Xiao Tang, Heidar A. Malki, Zhu Han, Modelling Cyber Attacks on Electricity Market Using Mathematical Programming With Equilibrium Constraints. IEEE Access, vol. 7, 2019. Access mode: https://ieeexplore.ieee.org/document/8651454

[7] Rajaa Vikhram Yohanandhan, Rajvikram Madurai Elavarasan, Premkumar Manoharan, Lucian Mihet-Popa, Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis With Cyber Security Applications. IEEE Access, vol. 8, 2020. Access mode: https://www.researchgate.net/publication/343666012_Cyber-Physical_Power_System_CPPS_A_Review on_Modeling_Simulation and_Analysis_With_Cyber_Security_Applications

[8] Ryabinin I.A. Logical and Probabilistic Calculus: A Tool for Studying the Reliability and Safety of Structurally Complex Systems. Automation and Remote Control vol. 64, 2003, P. 1177–1185. Access mode: https://link.springer.com/article/10.1023/A:1024798521540#article-info

[9] Alexeev V. Logical and probabilistic analysis of the reliability of the metallurgical complex electric supply. International Journal of Risk Assessment and Management, January 2018, 21(1/2):42. Access mode:https://www.researchgate.net/publication/323409400_Logical_and_probabilistic_analysis_of_the_reliability_of_the_metallurgical_complex_electric_supply

[10] V.V. Gorshkov, Logical probabilistic method for calculation of the survivability of complex systems. Cybernetics, vol. 18, 1982, p. 122–126. Access mode: https://link.springer.com/article/10.1007/BF01078059#citeas

[11] Zavgorodnii V., Zavgorodnya A., Maiko V., Malikov V., Zhuk D. Methods And Models For Assessment Of Reliability Of Structural-Complex Systems. World Science, No 11(39), 2018. Access mode: https://rsglobal.pl/index.php/ws/article/view/1364

[12] A.Musaev, I.Gladkov Current Status and Directions of a General Logic-probabilistic Method of System Analysis. SPIIRAS Proceedings 1(12):75, p. 75-96. Access mode: https://www.researchgate.net/publication/305293530 Current_Status_and_Directions_of a General Logic probabilistic Method of System Analysis

[13] Novikov O.M., Timoshenko A.O. Pobudova logiko-jmovirnisnoyi modeli zahishenoyi komp'yuternoyi sistemi //Pravove, normativne ta metrologichne zabezpechennya sistemi zahistu informaciyi v Ukrayini. - 2001. - Vip. 3. - S. 101-105.

[14] Hnigicheva O.M., Novikov O.M., Timoshenko A.O. Modelyuvannya bezpeki skladnih informacijno-komunikacijnih sistem z vikoristannyam logiko-jmovirnisnogo metodu //Naukovi visti NTUU «KPI». - 2010. - Vip.6. - S. 70-81. Access mode: https://ela.kpi.ua/handle/123456789/36294