Kybernetika

Rasim Alguliyev; Ramiz Aliguliyev; Lyudmila Sukhostat

Method for quantitative risk assessment of cyber-physical systems based on vulnerability analysis

Kybernetika, Vol. 60 (2024), No. 6, 779–796

Persistent URL: `http://dml.cz/dmlcz/152859`

METHOD FOR QUANTITATIVE RISK ASSESSMENT OF CYBER-PHYSICAL SYSTEMS BASED ON VULNERABILITY ANALYSIS

Rasim Alguliyev, Ramiz Aliguliyev, and Lyudmila Sukhostat

Cyber-physical system protection against cyber-attacks is a serious problem that requires methods for assessing the cyber security risks. This paper proposes a quantitative metric to evaluate the risks of cyber-physical systems using the fuzzy Sugeno integral. The simulated attack graph, consisting of vulnerable system components, allows for obtaining various parameters for assessing the risks of attack paths characterizing the elements in the cyber and physical environment and are combined into a single quantitative assessment. Experiments are performed on a threat model using the example of a cyber-physical system for wind energy generation. The model integrates a cyber-physical network's topology and vulnerabilities, proving the proposed method's effectiveness in ensuring cyber resilience.

Keywords: cyber-physical system, risk assessment, attack graph, graph centrality measures, Sugeno λ-measure, fuzzy Sugeno integral, attack path

Classification: 68M15

1. INTRODUCTION

The connection between IT (Information Technology) and networks is essential when modeling the criticality of the cyber-physical system (CPS) nodes. Most existing works consider the criticality of a node in only one environment, i.e., either in an IT environment or an OT (Operational Technology) environment. In this case, the network is assumed to be homogeneous, in which all nodes work similarly and are configured with the same OS.

The use and benefits derived from the convergence of IT and OT are growing and allow for more efficient management and operation of CPS. OT consists of many sensors [29], actuators, programmable logic controllers (PLCs), or remote telemetry devices involved in the manufacturing process. They include human-machine interfaces (HMIs), alarm or notification systems, engineering workstations, etc. Existing IT systems and applications manage industrial automation and control functions throughout CPS [32]. The systems and functions at this level interact with the production area and exchange data with corporate systems and applications to perform a certain number and types of services. The severity of the node failure effect on CPS depends on the number of node

DOI: 10.14736/kyb-2024-6-0779

services and their diversity. It proves the need to measure the criticality of the system nodes.

Unlike existing approaches, this study aims to solve a specific problem of quantitative measurement of the cyber-physical security of CPS, taking into account the parameters that affect its physical and cyber layers.

Quantifying cyber security risks leads to identifying cyber vulnerabilities and will ensure that a mitigation plan is in place to prevent security threats [30].

For example, Ou and Singhal analyzed system risk in the context of a cyberattack using an attack graph without regard to node criticality [24]. Here, the criticality of a node indicates the maximum amount of damage inflicted on the system when an attacker compromises the node. The notion of node criticality was defined using a pattern of attacks on IT infrastructure based on pre-association and post-association with other nodes [2, 31]. Studies proved the influence of neighboring nodes of the attack graph on the criticality of the considered node.

This paper proposes a quantitative metric for assessing CPS risks based on measuring the vulnerabilities of attack graph nodes using a fuzzy Sugeno integral. The main contributions of this work are summarized as follows:

- A metric for assessing CPS risks using the fuzzy Sugeno integral, which is determined by combining indices from IT and OT, is proposed.
- Node risk assessment is based on calculating indices of closeness centrality, eigenvector centrality, Katz centrality, betweenness centrality, integrity score, availability score, and confidentiality score.
- An experimental evaluation of the proposed method is performed on a wind energy generation model that integrates the topology of the cyber-physical network and the vulnerabilities of the CPS components.

The remainder of the paper is organized as follows. Section 2 provides abbreviations, notations, and definitions used in the paper. Related works are discussed in Section 3. Section 4 presents the proposed approach. An example of critical cyber-physical infrastructure is given in Section 5. Section 6 provides experimental results and discussion. Section 7 presents the conclusion of this paper.

2. PRELIMINARIES

In this section, abbreviations, notations and definitions are presented that used in current paper to assist the reader.

2.1. Abbreviations

- IT: Information Technology;
- OT: Operational Technology;
- CPS: Cyber-Physical System;
- PLC: Programmable Logic Controller;

- HMI: human-machine interface;
- CVSS: Common Vulnerability Scoring System;
- SCADA: Supervisory Control and Data Acquisition;
- RTU: Remote Terminal Unit;
- CVE: Common Vulnerabilities and Exposures;
- DoS: Denial-of-Service.

2.2. Notations

- $G = (N, \varepsilon)$: a graph with a set of nodes (vertices) N and a set of edges ε;
- $N = \{1, \dots, n\}$: a set of nodes;
- n: a total number of nodes in a graph;
- $\varepsilon = \{(i, j) \mid i, j \in N\}$: a set of edges (i, j);
- (i, j): an edge between the nodes i and j;
- d_{ij}: a shortest distance from i to j;
- C_i^c: closeness centrality of the node i;
- E_i^c: eigenvector centrality of the node i;
- B_i^c: betweenness centrality of the node i;
- K_i^c: Katz centrality of the node i;
- $\mathbb{A} = \|a_{ij}\|_{i,j=1}^{n}$: an adjacency matrix of a graph G that is the $n \times n$ matrix such that a_{ij}=1 when the ith node is connected to the jth node, and a_{ij}=0 otherwise.
- δ_{max}: the largest eigenvalue of the adjacency matrix $\mathbb{A}$;
- σ_{ij}: a total number of shortest paths from the source node i to the destination node j;
- $\sigma_{ij,k}$: a total number of paths from i to j that pass through k.

2.3. Definitions

CPS systems have a diverse topological structure. Let's consider the following indices for assessing the criticality of attack graph nodes. These indices provide detailed information about the entire network.

Definition 1 (betweenness centrality). The betweenness centrality B_i^c of a node i is defined as follows [10]:

$$B_i^c = \sum_{\substack{k,j=1 \\ k \neq j \neq i}}^{n} \frac{\sigma_{kj,i}}{\sigma_{kj}}, \quad i = 1, \ldots, n. \tag{1}$$

The betweenness centrality measures the number of shortest paths passing through a particular graph vertex [10]. This graph-theoretic metric measures how often a node acts as a "bridge" on the shortest paths between two other nodes. Shortest paths refer to all shortest paths between every pair of vertices in a graph. If one vertex is part of the shortest paths, then it has high betweenness centrality. When translating the network into a graph-theoretic model, betweenness centrality of a node indicates the possibility of an attack passing through this node.

Definition 2 (closeness centrality). The closeness centrality C_i^c for a node i is calculated as follows [1]:

$$C_i^c = \frac{n-1}{\sum_{\substack{j=1 \\ j \neq i}}^{n} d_{ij}}, \quad i = 1, \ldots, n. \tag{2}$$

The closeness centrality measures how close a node (i.e. i) is to all other nodes by calculating the shortest path length from one node to other nodes in the network. Nodes with a high closeness centrality score have more influence over other nodes in the network.

Definition 3 (eigenvector centrality). The eigenvector centrality E_i^c for a node i is defined as follows [21]:

$$E_i^c = \frac{1}{\delta_{max}} \sum_{j=1}^{n} a_{ij} E_j^c, \quad i = 1, \ldots, n. \tag{3}$$

The eigenvector centrality shows the relationship between a graph's most "influential" vertex and neighboring vertices [21].

Definition 4 (Katz centrality). Katz centrality K_i^c of a node i is defined as [14]:

$$K_i^c = \sum_{q=1}^{\infty} \sum_{j=1}^{n} \beta^q \left(\mathbb{A}^q\right)_{ij}, \quad i = 1, \ldots, n, \tag{4}$$

where $\beta \in (0,1)$ is the attenuation coefficient, i.e., the share of remote vertices participation, and $\left(\mathbb{A}^q\right)_{ij}$ is the total number of q degree connections between the nodes i and j.

Katz centrality is a graph-theoretic parameter that gives importance to a node given the network structure and the node's position in the network. Katz centrality quantifies the number of nodes connected through this path, and the contribution of remote nodes is "penalized."

Definition 5 (fuzzy measure). Let $N = \{1, \ldots, n\}$ be a finite set and let $\mu : 2^N \to$ [0,1] be a function that $\mu(\varnothing) = 0$ and $\mu(N) = 1$ [13]. If for any A and B, such that $A \subseteq B \subseteq N$, it satisfies that $\mu(A) \leq \mu(B)$. Then the fuzzy set μ is called fuzzy measure.

Definition 6 (Sugeno λ-measure). Let $N = \{1, \ldots, n\}$ be a finite set and let $\lambda \in (-1, +\infty)$. The function $\mu : 2^N \to$ [0,1] is a Sugeno λ-measure if the followings properties hold [20]:

$$\mu(\varnothing) = 0, \tag{5}$$

$$\mu(N) = 1, \tag{6}$$

$$\mu(A) \leq \mu(B),\ \forall A, B \text{ such that } A \subseteq B \subseteq N, \tag{7}$$

$$\mu(A \cup B) = \mu(A) + \mu(B) + \lambda\mu(A)\mu(B),\ \forall A, B \subseteq N \text{ with } A \cap B = \varnothing, \tag{8}$$

where $\varnothing$ is the empty set.

Equation 5 and Equation 6 represents the measures of an empty set and a combination of the all sets, respectively. Equation 7 represents monotonicity property. Equation 8 represents the possible subsets and the combined subsets.

By the recurrent application of Equation 8, for each $A \subseteq N$ the value of $\mu(A)$ can be calculated as follows [20]:

$$\mu(A) = \left[\frac{\prod_{i \in A} \left(1 + \lambda\mu\left(\{i\}\right)\right)}{\lambda}\right]. \tag{9}$$

Using the constraint $\mu(N)$=1 (Equation 6) and applying Equation 9 the λ value can calculated by the Equation 10 [20, 22]:

$$\lambda + 1 = \prod_{i=1}^{n} \left(1 + \lambda\mu_i\right), \tag{10}$$

where $\mu_i = \mu\left(\{i\}\right)$.

Definition 7 (discrete Sugeno integral). Let μ be a fuzzy measure on N. The discrete Sugeno integral of function $\mathbb{x} = (x_1, x_2, \ldots, x_n) : [0,1]^n \to [0,1]$ with respect to μ is defined as [20]:

$$\begin{aligned} SI_\mu(x) &= \max_{1 \leq i \leq n} \left(\min\left(x_{\pi(i)}, \mu(\{\pi(1), \pi(2), \ldots, \pi(n)\})\right)\right) = \\ &= \max_{1 \leq i \leq n} \left\{\min\left\{x_{\pi(i)}, \mu(\{\pi(1)\})\right\}, \ldots, \min\left\{x_{\pi(n)}, \mu(\{\pi(1), \ldots, \pi(n)\})\right\}\right\}, \end{aligned} \tag{11}$$

where π is a permutation on N such that $x_{\pi(1)} \leq \cdots \leq x_{\pi(n)}$.

Main idea of the Sugeno integral based on weighted minimum and maximum, which allows to evaluate the importance of each model using fuzzy measures. The fuzzy Sugeno integral determines the highest level of similarity between the target and the predicted values.

3. RELATED WORKS

Currently, methods for analyzing and assessing CPS risks can be divided into qualitative [16, 34] and quantitative [17, 28] methods. The former are based on the expert's experience and reveal the nature of the risks. In this case, quantitative estimates calculate the magnitude of the risk. However, researchers favor quantitative risk analysis and assessment methods because they allow more precise optimization of security resources. Table 1 provides an analysis of modern methods for assessing CPS risks.

Summing up the above works, we propose a method based on the fuzzy Sugeno integral for assessing the risks of attack paths on CPS, taking into account the criticality of the attack graph nodes. CVSS (Common Vulnerability Scoring System) metrics indicate the vulnerabilities of the nodes in the considered graph.

4. PROPOSED APPROACH

This section describes the structure of the proposed risk assessment methodology: system modeling, system component criticality, and risk assessment.

The simulated attack graph aimed at CPS devices allows for obtaining various measurements to assess cyber risks. Various measurements from the cyber and physical environment are combined into a single quantitative assessment, which is used to diagnose the system's state.

The vulnerability values of the components in the cyber and physical CPS layers are used to calculate the system's risk based on the fuzzy Sugeno integral. Based on the obtained values, the most critical CPS nodes are selected, and possible attack paths are predicted.

Risk value can be static [33], dynamic [9], and cascading [4, 12]. When an adversary does not exploit CPS vulnerabilities, the risk score is called the static risk value R_0. The R_0 value shows how easy it is to cope with the vulnerabilities of the CPS distribution network. The dynamic risk value R $(R > R_0)$ indicates that an attacker exploited some system vulnerabilities. The risk assessment cycle is completed and compared with the static risk value R_0. If $R > R_0$, the risk has arisen, and emergency measures are immediately taken to eliminate the risk. Furthermore, the next assessment is carried out at a certain interval if there is no risk.

4.1. CPS risk assessment based on criticality indices

To ensure the cyber-resilience of the CPS based on the attack graph, it is necessary to determine the criticality of its nodes. Risk assessment indices make it possible to measure how vulnerable a system is to cyberattacks and to determine the location of CPS components relative to each other.

The considered indices cover the following two main areas: (1) OT and (2) IT. The considered environments are (1) physical and (2) cyber.

IT and OT indicators predict the state of CPS when an undesirable event occurs. For example, to analyze the wind power system's state for failures, the operator must first know parameters such as the cut-in speed, the rated speed, the cut-off speed, and the nominal power at each system node [5].

References	Proposed approach	Main contribution	Limitations	Case study	Method type
Salayma (2024) [27]	An approach to enable representing and maintaining attack paths through the system	Optimized treatment of graphs	Application of dynamic network scenarios	Healthcare system	quantitative risk assessment
Liu et al. (2023) [18]	A method for the dynamic security risk assessment of industrial control systems	A risk calculation method that considers the exploit success rate, threat value, device importance, attack data, and industrial protocol characteristics.	Zero-day attacks are not analysed.	Tennessee Eastman process control system	quantitative risk assessment
Nourian and Madnick (2018) [23]	System theoretic framework for attack modeling and threat assessment in CPS	Causal Analysis based on STAMP is used for the analysis of Stuxnet to address security risks	Zero-day attacks are not analysed.	Uranium enrichment infrastructure	quantitative risk assessment, qualitative risk assessment
Zhang et al. (2018) [34]	A fuzzy probability Bayesian network approach for dynamic Risk Assessment	Fuzzy probabilities replace the crisp probabilities required in a standard Bayesian network model.	Computational complexity	Chemical reactor control system	qualitative risk assessment
Li et al. (2018) [16]	Asset-based dynamic assessment of cyberattacks	The total impact is quantified from various possible consequences.	Execution time depends on the length of predicted time and the system size.	Chemical control system	qualitative risk assessment
Lyu et al. (2020) [19]	Bayesian Network Based C2P Risk Assessment	Quantification of the cyber threat impact on physical process safety.	Does not suit dynamic risk assessment.	Double-tank water system	quantitative risk assessment
Semertzis et al. (2022) [28]	Quantitative risk assessment using attack graphs	The digital twin simulates power system cascading failures caused by cyberattacks.	Focus on computer networks, indirectly considering OT through critical assets.	IEEE 39-bus system	quantitative risk assessment
Leao et al. (2023) [15]	Augmented digital twin for cyberattacks identification	Integrates IT and OT, providing an analysis of possible threats.	Computational complexity	IEEE 123-bus system	quantitative risk assessment
Beyza and Yusta (2021) [3]	Integrated risk assessment for robustness evaluation and resilience optimization	The satisfied demand index is measured to quantify the power supply within the infrastructure.	Operational or dynamic limitations were not considered.	IEEE 118-bus system	quantitative risk assessment
Cheng et al. (2021) [7]	Random multi-hazard resilience modeling of CPS	Proves that the shape of the resilience curve depends on the convexity of system hazard function and availability.	Computational complexity	IEEE 9-bus system	quantitative risk assessment
Chen et al. (2020) [6]	Risk assessment considering the characteristics of attack behaviors	The utility value and utility attenuation model are adopted to describe different attacks and characteristics of candidate targets.	Coordinated cyberattacks and cascading outages were not considered	IEEE RTS79 system	quantitative risk assessment
Liu et al. (2021) [17]	A method to identify critical assets based on their connection	The method assesses risks based on critical assets.	The attack scenarios focus on the physical level, assuming an attacker has already compromised the system using the threat model.	IEEE 12-bus system	quantitative risk assessment

Tab. 1. Overview of state-of-the-art risk assessment methods in CPS.

The failure of individual CPS components can cause uncontrolled deviations of various parameters due to cyberattacks by intruders, which can ultimately lead to the collapse of the system [25, 26].

Figure 1 shows an example of a CPS scheme consisting of 17 nodes: 7 cyber nodes and 10 physical nodes. In this example, the complex system includes two layers, namely IT and OT, and their interaction. The figure shows the links between cyber and physical components. The red arrows represent an attack path that an intruder can take from the input node to the target node of the attack. The path starts from the cyber node of the system to the target node of the physical layer.

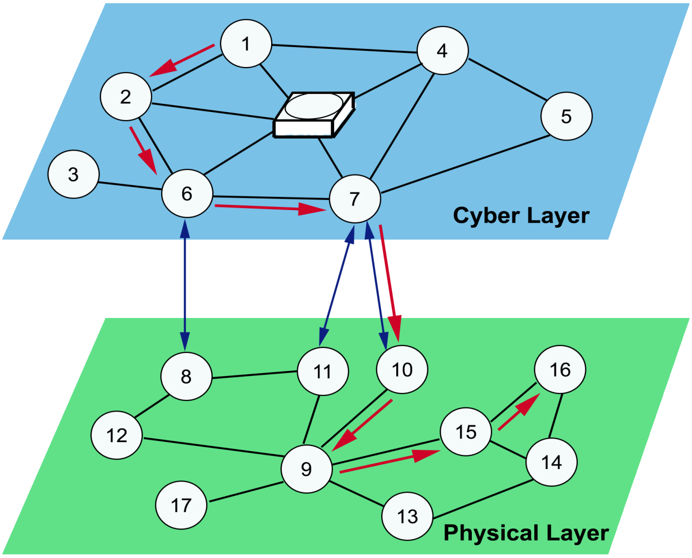

Fig. 1. Attack-path prediction demonstration diagram.

CVSS is used as a scoring system that quantifies the cyber risk of vulnerabilities that present in a system [8]. The attack graph G makes it possible to link different vulnerabilities. It identifies potential threats to CPS nodes based on vulnerability information to represent attack paths in the system. In fact, CVSS estimates the complexity of implementing a cyber-attack, taking into account vulnerabilities for each device that exists in a particular CPS node.

4.2. CPS risk assessment based on fuzzy Sugeno integral

Combining the CPS risk assessment criteria values is performed using fuzzy integrals, which are determined concerning fuzzy measures. It is assumed that the values of the fuzzy measure and all input parameters vary within a unit interval.

This study uses a metric based on the fuzzy Sugeno integral to assess the risk of attack paths. The risk of each attack graph's node is calculated as follows:

$$Risk_i = Probability_i \times ImpactSI_i, \quad i = 1, \ldots, n, \tag{12}$$

where $Probability_i$ is the access probability to node i, which shows the number of attack paths and is calculated as follows:

$$Probability_i = 1 - \prod_{j=1}^{n} (1 - P_j), \quad i = 1, \ldots, n, \tag{13}$$

where P_j is an attack probability to node j.

Here P_i is calculated as

$$P_i = AV_i \times AC_i \times UI_i \times PR_i, \quad i = 1, \ldots, n, \tag{14}$$

where AV_i is an attack vector, AC_i is an attack complexity, UI_i is the user interaction, PR_i is a privilege required.

The risk exposure using the fuzzy Sugeno integral (SI) is calculated using the indices B_i^c, C_i^c, E_i^c and K_i^c, as well as integrity (I_i), availability (A_i) and confidentiality (C_i) scores, derived from CVSS v3.1, as follows:

$$ImpactSI_i = SI(B_i^c, C_i^c, E_i^c, K_i^c, I_i, A_i, C_i), \quad i = 1, \ldots, n. \tag{15}$$

Nodes with high $ImpactSI$ values are considered more vulnerable in terms of CPS cybersecurity (see below Algorithm).

```
Algorithm: Risk Assessment of CPS
Input: Attack graph $G$
Output: Risk value $R$
Step 1: For node $i$, get information about vulnerability $v$ from the vulnerability database.
Step 2: Calculate centrality measures using Equations 1 - 4 and security metrics.
Step 3: Taking into account the values obtained using Equations 1 - 4, calculate the risk of node $i$ using Equation 12 in case of successful vulnerability exploitation.
Step 4: Repeat steps 1-3 and calculate the risk of the considered node $i$ for different vulnerabilities.
Step 5: Calculate the risk of a CPS system.
```

A metric based on several indices characterizes each node of the system better. Unlike a single index, it is more informative

Below we consider an example for cyber risk assessment based on the fuzzy Sugeno integral. Once the required coefficients are calculated, they are combined using multi-criteria decision analysis. The fuzzy Sugeno integral is used to assess the risk of attack paths to ensure the cyber resilience of CPS.

For example, the indices used as input $ImpactSI_i$ to the node i might be: $x_{1,i} = I_i$, $x_{2,i} = A_i$, $x_{3,i} = C_i$, $x_{4,i} = B_i^c$, $x_{5,i} = C_i^c$, $x_{6,i} = E_i^c$, and $x_{7,i} = K_i^c$. Each of these indices is assigned an appropriate "expert" weight: μ_1, μ_2, μ_3, μ_4, μ_5, μ_6 and

μ_7. Hereafter, for the sake of simplicity, the second index i of the variables x has been omitted.

Suppose the importance of each input index is expressed through fuzzy densities $\mu_1 = \mu(x_1)$=0.95, $\mu_2 = \mu(x_2)$=0.27, $\mu_3 = \mu(x_3)$=0.25, $\mu_4 = \mu(x_4)$=0.38, $\mu_5 = \mu(x_5)$=0.28, $\mu_6 = \mu(x_6)$=0.19, and $\mu_7 = \mu(x_7)$=0.12.

The numerical value of the parameter λ can be calculated as a solution of the following equation:

$$1 + \lambda = (1 + \lambda\mu_1)(1 + \lambda\mu_2)(1 + \lambda\mu_3)(1 + \lambda\mu_4)(1 + \lambda\mu_5)(1 + \lambda\mu_6)(1 + \lambda\mu_7). \qquad (16)$$

As a result, a solution $\lambda = -0.9893$ was obtained. And fuzzy Sugeno measures also include $\mu(x_1, x_2) = 0.9662, \dots, \mu(x_3, x_4) = 0.5360, \dots, \mu(x_6, x_7) = 0.2874, \dots, \mu(x_1, x_2, x_3) = 0.9772, \dots, \mu(x_1, x_4, x_5) = 0.9834, \dots, \mu(x_3, x_4, x_5, x_6) = 0.7320, \dots, \mu(x_1, x_2, x_3, x_4, x_5, x_6, x_7) = 1$. Further, the obtained values are fuzzified based on the Gaussian membership function. In this case, the Sugeno fuzzy integral is equal to 0.9382.

A variable R_0 is introduced, which is a threshold value at which the CPS node with *Risk* higher this threshold is considered "unstable." In practice, this value should be determined by experienced experts. If the node is "unstable," emergency measures are immediately taken to eliminate the risk. If *Risk* is below R_0, then the node is considered "stable," and there is no risk. In this case, the following risk assessment can be performed after a certain interval.

The final solution *Risk* makes the system more cyber-resilient in terms of cyber-physical security. Figure 2 shows the general scheme of the proposed approach for assessing CPS risks to achieve the system's cyber-resilient operation.

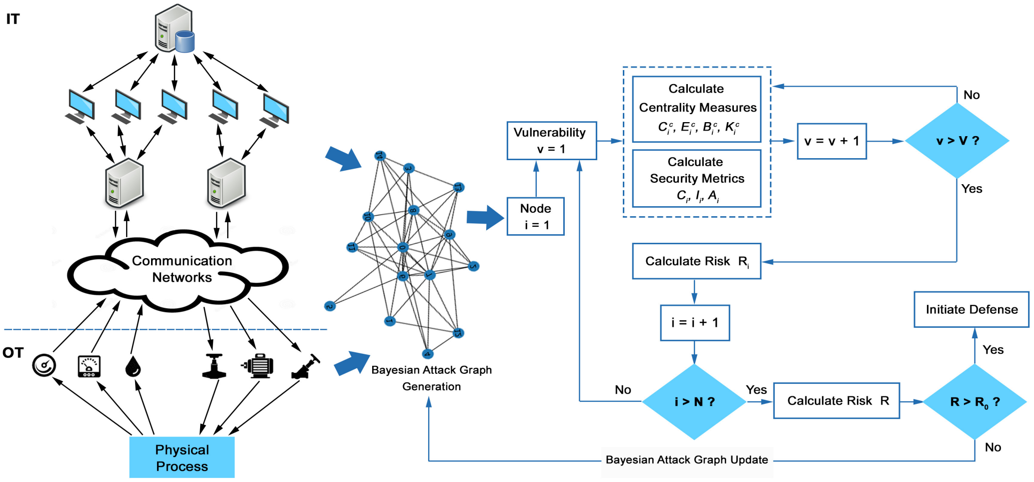

Fig. 2. General framework of the proposed CPS risk assessment approach.

5. CASE STUDY

For example, we consider wind energy generation to be one of the critical infrastructure sectors (Figure 3). Wind turbines are widely used in various facilities: enterprises, households, private houses, etc. Wind flows rotate the wind turbine's blades, setting it in motion [11]. The stronger the wind, the more energy is generated. This rotation starts the turbine, which also begins to rotate. Wind turbines are devices that convert wind energy into electrical energy. Energy is transmitted along the rotor shaft, which is connected to a gearbox that drives an electric generator.

The turbine consists of a cooling system, a condition monitoring system, and a weather vane. These serve as input data for the controller, which determines the position of the blades and rotor. The battery management system monitors and controls multiple battery packs and ensures grid stabilization.

Process parameter values obtained during monitoring are stored in the data historian. The HMI provides the interaction of process operators with the control system. Engineering workstations contain software development tools, with the help of which an expert can make changes and additions to the system configuration via a corporate network or the Internet. Connection via RTU (remote terminal unit) links the wind park to the central SCADA (supervisory control and data acquisition) system.

Let's assume that an attacker exploited the vulnerabilities of CPS components and performed the following cyberattack scenarios (Figure 3):

- Manipulation and Denial of Control. An attacker capable of interacting with the SCADA server can exploit the CVE-2019-14925 vulnerability to manipulate system configurations, files, or critical values related to wind park operations. The vulnerability could result in unauthorized access to confidential data, including usernames, passwords, and other sensitive information. An adversary could also abuse the fact that connections are unauthenticated (CVE-2021-27395), allowing unauthorized data manipulation and issuing commands to the RTU. This could stop logical tasks from running and disrupt communication between SCADA and RTU. This would prevent operators from monitoring the compressor stations.

- Loss of Control. To compromise credentials and gain access to the wind park network, the adversary exploits the CVE-2019-9013, CVE-2022-1159, and CVE-2021-22797 vulnerabilities to gain code execution on RTU. This will enable the transition to control of individual turbines. The attacker can penetrate the internal network of the control system using the CVE-2018-5452 vulnerability to manipulate the system configuration, operational settings, and controller firmware. This can lead to the disabling of the overspeed protection function built into the RTU and disconnecting the load to cause a turbine shutdown. Using CVE-2020-7566, the adversary can compromise the data and turn off the health monitoring systems that would provide early warning of danger. Additionally, they can target the PLC and use CVE-2020-6992 to compromise credentials and obtain execution code on the PLC. With this, an attacker can affect battery management functions, leading to system downtime and potentially destabilizing CPS.

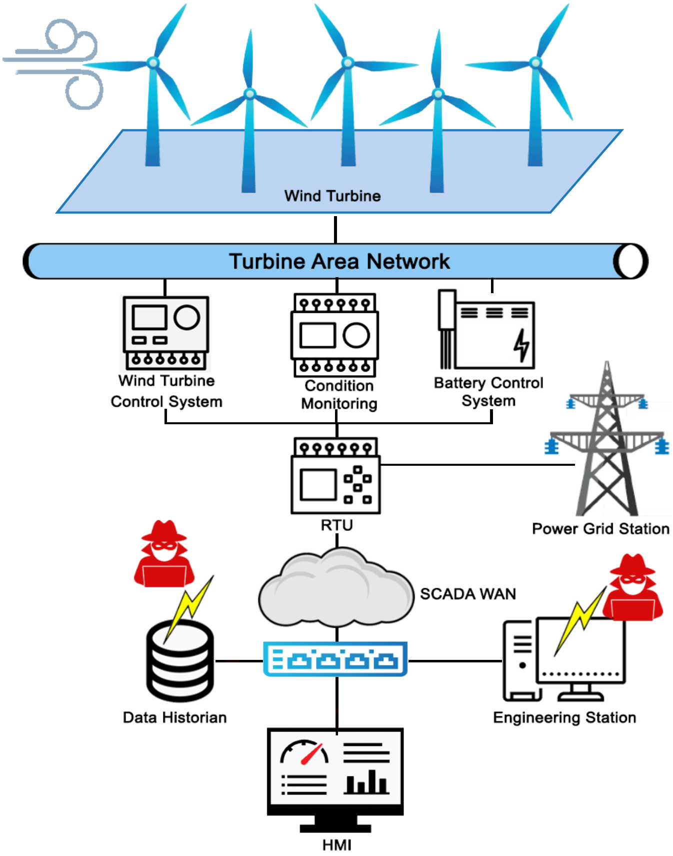

Fig. 3. Examples of attack scenarios on CPS.

6. EXPERIMENTAL RESULTS AND DISCUSSION

The results of the proposed approach assessment based on creating an attack graph using a predefined CPS vulnerability model are presented. An attacker is a host where an intruder is located in an external network environment. The considered CPS model consists of two layers and 17 nodes. The attacker's ultimate goal is to compromise the PLC and RTU nodes. A denial-of-service (DoS) attack was considered as a threat.

CPS risk assessment is performed in Python 3.7.12 using various libraries, including the NetworkX module. All experiments are run on an Intel Xeon(R) processor X5670 @ 2.93GHz*24 with 24GB of RAM.

For each node i of the system, the values of indices B_i^c, C_i^c, E_i^c, and K_i^c, as well as integrity (I_i), availability (A_i), and confidentiality (C_i), obtained based on CVSS v3.1, were calculated. This made it possible to identify the critical nodes of the system. The indices were assigned "expert" weights. The higher the weight, the higher the

Node	Vulnerability	Base	Impact	Exploitability	Access	C	I	A	UI	PR	AC
	CVE-ID	Score	Score		Vector						
1	CVE-2021-41773	7.5	3.6	3.9	0.85	0.56	0	0	0.85	0.85	0.77
2	CVE-2022-22720	9.8	5.9	3.9	0.85	0.56	0.56	0.56	0.85	0.85	0.77
3	CVE-2022-30522	7.5	3.6	3.9	0.85	0	0	0.56	0.85	0.85	0.77
4	CVE-2014-7844	7.8	5.9	1.8	0.55	0.56	0.56	0.56	0.85	0.85	0.77
5	CVE-2019-9557	6.1	2.7	2.8	0.85	0.22	0.22	0	0.62	0.85	0.77
6	CVE-2020-2512	5.9	3.6	2.2	0.85	0	0	0.56	0.85	0.85	0.44
7	CVE-2020-24673	9.8	5.9	3.9	0.85	0.56	0.56	0.56	0.85	0.85	0.77
8	CVE-2020-6992	6.7	5.9	0.8	0.55	0.56	0.56	0.56	0.85	0.27	0.77
9	CVE-2021-27395	8.1	5.2	2.8	0.85	0	0.56	0.56	0.85	0.62	0.77
10	CVE-2020-3960	8.4	5.8	2.0	0.55	0.56	0	0.56	0.85	0.62	0.77
11	CVE-2021-22797	7.8	5.9	1.8	0.55	0.56	0.56	0.56	0.62	0.85	0.77
12	CVE-2019-14925	6.5	3.6	2.8	0.85	0.56	0	0	0.85	0.62	0.77
13	CVE-2019-9013	8.8	5.9	2.8	0.62	0.56	0.56	0.56	0.85	0.85	0.77
14	CVE-2022-1159	7.2	5.9	1.2	0.85	0.56	0.56	0.56	0.85	0.27	0.77
15	CVE-2020-7566	7.3	5.2	2.1	0.62	0.56	0.56	0	0.62	0.85	0.77
16	CVE-2018-5452	7.5	3.6	3.9	0.85	0	0	0.56	0.85	0.85	0.77
17	CVE-2023-0286	7.4	5.2	2.2	0.85	0.56	0	0.56	0.85	0.85	0.44

Tab. 2. Vulnerability information (CVSS v3.1).

"informativeness" of the index.

Information about the considered vulnerabilities, including base score, impact score, exploitability, access vector, I, A, C, UI, PR, and AC, is shown in Table 2.

Table 3 shows the index values for all 17 nodes of the considered CPS. These values allow the evaluation system device criticality based on the impact and probability values.

The proposed approach was chosen to assess the severity of the vulnerability according to the criteria:

$$R = \begin{cases} critical, & v \in [5, 10] \\ high, & v \in [3, 5) \\ medium, & v \in [2, 3) \\ low, & v \in [0, 2). \end{cases} \tag{17}$$

We consider various attack paths aimed at possible graph nodes to change their states. For brevity, three targets of attacks in the simulated network are considered: nodes 17, 16, and 12. Tables 4, 5, and 6 show the extracted attack paths and severity of vulnerabilities that can lead to unwanted events.

So, there are five possible attack paths to nodes 17 and 12 (Tables 4 and 6). According to Table 5, the largest attack step was determined to be six steps for node 16. We got five attack paths for each of the considered nodes.

The highest risk was obtained for the P3 attack path and amounted to 3.1896 (Table 5). Thus, the most likely attack path is to use nodes X_1, X_2, X_7, X_{10}, and then attack X_8 and X_{15}, and finally attack the final node X_{16} in P3. Therefore, the vulnerabilities of the considered nodes are the most important objects of CPS, on which it is necessary to focus the attention of experts.

Figure 4 shows the P and $ImpactSI$ values of each attack path on the system. Comparing these scores makes identifying the most likely attack paths that could lead to undesirable events easier. The P values for the attack path targeting end nodes 17 and

Node	B_i^c	C_i^c	E_i^c	K_i^c
1	0.0125	0.1667	0.0777	0.2411
2	0.0422	0.1667	0.0777	0.2411
3	0.0125	0.1250	0.0530	0.2193
4	0.0125	0.1000	0.0362	0.2172
5	0.0042	0.1667	0.0777	0.2411
6	0.0453	0.3125	0.2199	0.3112
7	0.2060	0.3214	0.3169	0.3182
8	0.0190	0.2045	0.1500	0.2264
9	0.2500	0.2500	0.3650	0.2429
10	0.0943	0.2188	0.2162	0.2271
11	0.1390	0.2667	0.3186	0.2497
12	0.0000	0.2101	0.2490	0.2195
13	0.0229	0.2101	0.2490	0.2195
14	0.0042	0.2156	0.3398	0.2391
15	0.0688	0.2101	0.2490	0.2195
16	0.0000	0.2402	0.4018	0.2411
17	0.0000	0.2101	0.2490	0.2195

Tab. 3. Criticality assessment indices of CPS nodes.

Path	Attack path description	Probability	Path risk	Vulnerability severity
P1	$X_1 \to X_2 \to X_7 \to X_{10} \to X_8 \to X_{17}$	0.8968	3.1415	High
P2	$X_1 \to X_6 \to X_7 \to X_{10} \to X_8 \to X_{17}$	0.8571	2.3053	Medium
P3	$X_1 \to X_2 \to X_7 \to X_{11} \to X_8 \to X_{17}$	0.7318	2.4721	Medium
P4	$X_1 \to X_6 \to X_7 \to X_{11} \to X_8 \to X_{17}$	0.8571	2.1983	Medium
P5	$X_1 \to X_6 \to X_9 \to X_{11} \to X_8 \to X_{17}$	0.7553	1.9372	Low

Tab. 4. Risk assessment of attack paths to Node #17.

Path	Attack path description	Probability	Path risk	Vulnerability severity
P1	$X_1 \to X_6 \to X_7 \to X_{10} \to X_8 \to X_{15} \to X_{16}$	0.9228	2.3662	Medium
P2	$X_1 \to X_2 \to X_7 \to X_{11} \to X_8 \to X_{15} \to X_{16}$	0.9149	2.9764	High
P3	$X_1 \to X_2 \to X_7 \to X_{10} \to X_8 \to X_{15} \to X_{16}$	0.9442	3.1896	High
P4	$X_1 \to X_6 \to X_7 \to X_{11} \to X_8 \to X_{15} \to X_{16}$	0.9228	2.2515	Medium
P5	$X_1 \to X_6 \to X_9 \to X_{11} \to X_8 \to X_{15} \to X_{16}$	0.8677	2.1171	Medium

Tab. 5. Risk assessment of attack paths to Node #16.

12 are highlighted in magenta and cyan, respectively. Whereas the *ImpactSI* values for the nodes of the attack path to nodes 17 and 12 are indicated in red and blue, respectively.

The advantage of the proposed method is more clearly proved by using several indices in assessing the CPS components' risks. Therefore, we considered the three most critical nodes of the system. Using the fuzzy Sugeno integral made it possible to most accurately identify the risk of an attack path based on probability and impact aimed at the most vulnerable components of CPS. It will help decision-makers allocate resources to restrict access to particular system components that adversaries can use to attack critical infrastructure.

Path	Attack path description	Probability	Path risk	Vulnerability severity
P1	$X_1 \to X_2 \to X_7 \to X_{10} \to X_8 \to X_{12}$	0.9084	2.3299	Medium
P2	$X_1 \to X_6 \to X_7 \to X_{10} \to X_8 \to X_{12}$	0.8725	1.5228	Low
P3	$X_1 \to X_2 \to X_7 \to X_{11} \to X_8 \to X_{12}$	0.9084	2.2164	Medium
P4	$X_1 \to X_6 \to X_7 \to X_{11} \to X_8 \to X_{12}$	0.8725	1.4192	Low
P5	$X_1 \to X_6 \to X_9 \to X_{11} \to X_8 \to X_{12}$	0.7804	1.2694	Low

Tab. 6. Risk assessment of attack paths to Node #12.

Thus, a quantitative metric for assessing the CPS cyber risk based on the fuzzy Sugeno integral is proposed to solve the problems of ensuring the cyber resilience of the system.

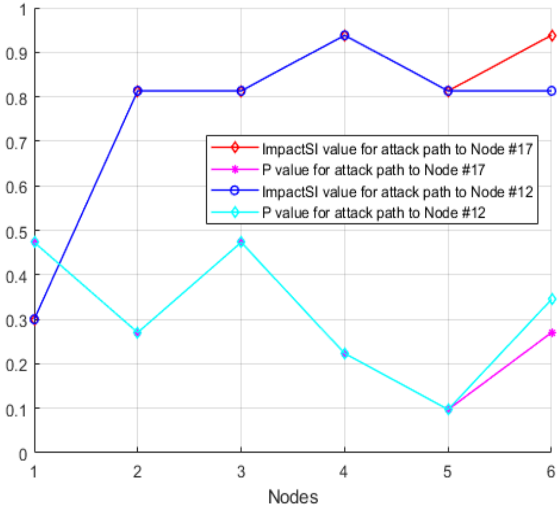

Fig. 4. Distribution of *ImpactSI* and *P* values on the attack paths.

It is intended to include various types of critical indices that affect the cyber resilience and operation of CPS while providing a quantitative assessment of the cyber and physical state of the system. This metric considers the vulnerabilities in IT and OT devices deployed in the physical and cyber layers of the CPS. Experimental results based on a DoS attack showed the effectiveness of risk assessment in the nodes of the considered system.

7. CONCLUSIONS

This paper analyses the attacking paths to the CPS, considering the criticality of its components based on graph theory. It gives informed control over cyber resilience, helps identify threats based on vulnerabilities, and mitigates risk by keeping the system up and running in the event of a cyberattack.

The paper proposes a method for quantitative risk assessment of CPS attack paths using a metric based on the fuzzy Sugeno integral. Closeness centrality, eigenvector centrality, betweenness centrality, Katz centrality, integrity, availability, and confidentiality, leading to cyberattacks on the CPS systems, were considered as IT and OT vulnerability assessment indices. The proposed metric considers the relationship between vulnerabilities and the impact of cyberattacks on the physical layer. A threat model using the example of a CPS for wind energy generation was used. The proposed method allows for determining the possible risk of the system and detection of the ultimate goal on the attack path, which will allow the expert to make the final decision more effectively.

ACKNOWLEDGEMENTS

This work was supported by the Science Foundation of the State Oil Company of Azerbaijan Republic (SOCAR) (Contract No. 01LR-EF/2024).

The authors would like to thank the editor and anonymous reviewers for their helpful comments and feedback, which greatly strengthened the overall manuscript.

(Received October 6, 2024)

REFERENCES

[1] A. Akbarzadeh and S. Katsikas: Identifying critical components in large scale cyber physical systems. In: IEEE/ACM 42nd International Conference on Software Engineering Workshops (ICSEW), IEEE 2020, pp. 230–236. DOI:10.1145/3387940.3391473

[2] M. Alhomidi and M. Reed: Attack graph-based risk assessment and optimization approach. Int. J. Netw. Secur. Appl. *6* (2014), 3, 31–43. DOI:10.5121/ijnsa.2014.6303

[3] J. Beyza and J. M. Yusta: Integrated risk assessment for robustness evaluation and resilience optimisation of power systems after cascading failures. Energies *14* (2021), 7, 1–18. DOI:10.3390/en14072028

[4] M. Z. A. Bhuiyan, G. J. Anders, J. Philhower, and S. Du: Review of static risk-based security assessment in power system. IET Cyper-Phys. Syst.: Theory Appl. *4* (2019), 3, 233–239. DOI:10.1049/iet-cps.2018.5080

[5] A. Chermitti, M. Bencherif, Z. Nakoul, N. Bibitriki, and B. Benyoucef: Assessment parameters and matching between the sites and wind turbines. Physics Procedia *55* (2014), 192–198. DOI:10.1016/j.phpro.2014.07.028

[6] B. Chen, Z. Yang, Y. Zhang, Y. Chen, and J. Zhao: Risk assessment of cyber-attacks on power grids considering the characteristics of attack behaviors. IEEE Access *8* (2020), 8, 148331–148344. DOI:10.1109/ACCESS.2020.3014785

[7] Y. Cheng, E. Elsayed, and X. Chen: Random multi hazard resilience modeling of engineered systems and critical infrastructure. Reliab. Eng. Syst. Safe. *209* (2021), 1–13. DOI:10.1016/j.ress.2021.107453

[8] CVSS: Common Vulnerability Scoring System version 3.1, 2020. https://www.first.org/cvss/v3-1/cvss-v31-specification r1.pdf

[9] D. Z. Fang, A. K. David, C. Kai, and C. Yunli: Improved hybrid approach to transient stability assessment. IEE Proc., Gener. Transm. Distrib. *152* (2005), 2, 201–207. DOI:10.1049/ip-gtd:20041223

[10] L. C. Freeman: A set of measures of centrality based on betweenness. Sociometry *40* (1977), 35–41. DOI:10.2307/3033543

[11] FVL: Forescout Vedere Labs. OT: ICEFALL: The legacy of "insecure by design" and its implications for certifications and risk management, 2022. https://www.forescout.com/resources/ot-icefall-report/

[12] P. Henneaux, P. E. Labeau, J. C. Maun, and L. Haarla: A two-level probabilistic risk assessment of cascading outages. IEEE Trans. Power Syst. *31* (2015), 2393–2403. DOI:10.1109/TPWRS.2015.2439214

[13] N. Kartli, E. Bostanci, and M.S. Guzel: Heuristic algorithm for an optimal solution of fully fuzzy transportation problem. Computing *106* (2024), 3195-3227. DOI:10.1007/s00607-024-01319-5

[14] L. Katz: A new status index derived from sociometric data analysis. Psychometrika *18* (1953), 39-43. DOI:10.1007/BF02289026

[15] B. P. Leao, J. Vempati, S. Bhela, T. Ahlgrim, and D. Arnold: Augmented digital twin for identification of most critical cyberattacks in industrial systems. (2023). In: arXiv preprint: 2306.04821

[16] X. Li, C. Zhou, Y. C. Tian, N. Xiong, and Y. Qin: Asset-based dynamic impact assessment of cyberattacks for risk analysis in industrial control systems. IEEE Trans. Ind. Inf. *14* (2018), 608–618. DOI:10.1109/TII.2017.2740571

[17] C. Liu, Y. Alrowaili, N. Saxena, and C. Konstantinou: Cyber risks to critical smart grid assets of industrial control systems. Energies *14* (2021), 1–19. DOI:10.3390/en14175501

[18] K. Liu, Y. Xie, S. Xie, and L. Sun: SEAG: A novel dynamic security risk assessment method for industrial control systems with consideration of social engineering. J. Process Control *132* (2023), 1–10. DOI:10.1016/j.jprocont.2023.103131

[19] X. Lyu, Y. Ding, and S. H. Yang: Bayesian network based C2P risk assessment for cyber-physical systems. IEEE Access *8* (2020), 88506–88517. DOI:10.1109/ACCESS.2020.2993614

[20] G.E. Martínez, C.I. Gonzalez, O. Mendoza, and P. Melin: General type-2 fuzzy Sugeno integral for edge detection. J. Imaging *5* (2019), 8, 1-20. DOI:10.3390/jimaging5080071

[21] O. Mason and M. Verwoerd: Graph theory and networks in biology. IET Syst. Boil. *1* (2007), 89–119. DOI:10.1049/iet-syb:20060038

[22] T. Murofushi and M. Sugeno: A theory of fuzzy measures. Representation, the Choquet integral and null sets. J. Math. Anal. Appl. *159* (1991), 2, 532–549. DOI:10.1016/0022-247X(91)90213-J

[23] A. Nourian and S. Madnick: A systems theoretic approach to the security threats in cyber physical systems applied to Stuxnet. IEEE Trans. Dependable Secur. Comput. *15* (2018), 1, 2–13. DOI:10.1109/TDSC.2015.2509994

[24] X. Ou and A. Singhal: Quantitative Security Risk Assessment of Enterprise Networks. Springer, 2011.

[25] Z. Qu, W. Sun, J. Dong, J. Zhao, and Y. Li: Electric power cyber-physical systems vulnerability assessment under cyber-attack. Front. Energy Res. *10* (2023), 1–12. DOI:10.3389/fenrg.2022.1002373

[26] I. Rahman and J. Mohamad-Saleh: Hybrid bio-Inspired computational intelligence techniques for solving power system optimization problems: A comprehensive survey. Appl. Soft Comput. *69* (2018), 72-130. DOI:10.1016/j.asoc.2018.04.051

[27] M. Salayma: Threat modelling in Internet of Things (IoT) environments using dynamic attack graphs. Front. Internet of Things *3* (2024), 1-25. DOI:10.3389/friot.2024.1306465

[28] I. Semertzis, V. S. Rajkumar, A. Ştefanov, F. Fransen, and P. Palensky: Quantitative risk assessment of cyber-attacks on cyber-physical systems using attack graphs. In: 10th IEEE Workshop on Modelling and Simulation of Cyber-Physical Energy Systems (MSCPES), IEEE 2022, pp. 1–6.

[29] Y. Shen and L. Lin: Adaptive output feedback stabilization for nonlinear systems with unknown polynomial-of-output growth rate and sensor uncertainty. Kybernetika *58* (2022), 4, 637–660. DOI:10.14736/kyb-2022-4-0637

[30] R. Shikhaliyev: Cybersecurity risks management of industrial control systems: A review. Probl. Inf. Technol. *15* (2024), 1, 37–43. DOI:10.25045/jpit.v15.i1.05

[31] C. Suh-Lee and J. Jo: Quantifying security risk by measuring network risk conditions. In: IEEE/ACIS 14thInternational Conference on Computer and Information Science (ICIS), IEEE 2015, pp. 9–14.

[32] Z. Wang, C. Zhai, H. Zhang, G. Xiao, G. Chen, and Y. Xu: Coordination control and analysis of TCSC devices to protect electrical power systems against disruptive disturbances. Kybernetika *58* (2022), 2, 218–236. DOI:10.14736/kyb-2022-2-0218

[33] F. Xiao and J. D. McCalley: Power system risk assessment and control in a multobjective framework. IEEE Trans. Power Syst. *24* (2009), 1, 78–85. DOI:10.1109/TPWRS.2008.2004823

[34] Q. Zhang, C. Zhou, Y. C. Tian, N. Xiong, Y. Qin, and B. Hu: A fuzzy probability Bayesian network approach for dynamic cybersecurity risk assessment in industrial control systems. IEEE Trans. Ind. Inf. *14* (2018), 6, 2497–2506. DOI:10.1109/TII.2017.2768998

Rasim Alguliyev, Institute of Information Technology, AZ1141, B. Vahabzade Street, 9A, Baku. Azerbaijan.
e-mail: r.alguliev@gmail.com

Ramiz Aliguliyev, Institute of Information Technology, AZ1141, B. Vahabzade Street, 9A, Baku. Azerbaijan.
e-mail: r.aliguliyev@gmail.com

Lyudmila Sukhostat, Institute of Information Technology, AZ1141, B. Vahabzade Street, 9A, Baku. Azerbaijan.
e-mail: lsuhostat@hotmail.com