scientific reports

OPEN

The functional safety assessment of cyber-physical system operation process described by Markov chain

Viacheslav Kovtun[1], Ivan Izonin[2]✉ & Michal Gregus[3]

The functional safety assessment is one of the primary tasks both at the design stage and at the stage of operation of critical infrastructure at all levels. The article's main contribution is the information technology of calculating the author's metrics of functional safety for estimating the instance of the model of the cyber-physical system operation. The calculation of metric criteria analytically summarizes the results of expert evaluation of the system in VPR-metrics and the results of statistical processing of information on the system's operation presented in the parametric space Markov model of this process. The advantages of the proposed approach are the following: the need to process orders of magnitude less empirical data to obtain objective estimates of the investigated system; taking into account the configuration scheme and architecture of the security subsystem of the investigated system when calculating the metric; completeness, compactness, and simplicity of interpretation of evaluation results; the ability to assess the achievability of the limit values of the metric criteria based on the model of operation of the investigated system. The paper demonstrates the application of the proposed technology to assess the functional safety of the model of a real cyber-physical system.

Assessing the functional safety of cyber-physical systems is undoubtedly relevant because new vulnerabilities are constantly identified[1–5]. Numerous facts of successful cyber attacks indicate a lack of security of cyber-physical systems of all levels and classes. The reasons for this (if there is a relevant and rationally designed tiered protection subsystem) are the emergence of new vulnerabilities and the negligence of privileged users. In addition, the cause of malfunctions is the failure to consider the specifics of the functioning of sensor networks (Industrial) Internet of Things.

The only adequate response to new vulnerabilities is periodically or continuously updating protection mechanisms. The latter option involves accumulating large data sets and high costs for their storage and analysis. However, this is not a problem regarding the functional security of the critical infrastructure. The Security Information and Event Management (SIEM) and User and Entity Behavior Analytics (UEBA) subsystems are responsible for storing and analyzing the results of the target cyber-physical system[6–11]. In the field of SIEM and UEBA already operates several commercial software products, including ArcSight ESM, QRadar SIEM, Splunk Enterprise Security, Micro Focus Security ArcSight UBA, Securonix UEBA, Splunk User Behavior Analysis. The practical experience of these solutions has revealed their imperfections in the analysis of causal relationships between the facts of failures and malfunctions and operative information about the operation of target systems.

Recognized information sources[12–14] such as the National Vulnerability Database (NVD), the Common Weakness Enumeration (CWE), the Common Attack Pattern Enumeration and Classification (CAPEC), MITER Att&ck, etc. are providers of benchmarks for known vulnerabilities. In addition to the essence of known vulnerabilities in these databases, there are metrics for ordering them by degree of danger. However, these metrics are reduced to a single indicator, the value of which can be objectively used only as an additional factor in expert analysis of the real cyber-physical system.

Ensuring the functional safety of cyber-physical systems is a complex problem. This thesis allows us to mention several methodologies related to our object of investigation. These are the following methodologies[15–19]:

- the integration of information;
- the security analysis;
- the analysis of security policies;
- the decisions support in the field of protection;

[1]Vinnytsia National Technical University, Vinnytsia 21000, Ukraine. [2]Lviv Polytechnic National University, Lviv 79013, Ukraine. [3]Comenius University in Bratislava, 820 05 Bratislava, Slovak Republic. ✉email: ivanizonin@gmail.com

- the automated control of the protection subsystem (including the based of Security Content Automation Protocol ones);
- the correlation analysis of events;
- the definition of security metrics.

Interestingly, apologists for expert methods of functional safety assessment[20,21] focus their efforts on developing methodologies to support decision-making and metrics in the field of investigation and summarize the results in the form of profile standards, such as ISO/IEC 61508, for example. Apologists of the methodology of automated control of the protection subsystem[15–17,19,22–24] define the core of such systems in the mathematical apparatus of probability theory and mathematical statistics, graph theory, and Petri nets, fuzzy logic, Markov chains, artificial intelligence and more. At the same time, the results obtained in this direction are of research interest because applying the obtained models and methods requires large amounts of empirical data and computing power.

The Markov process as a mathematical model for studying complex technical and information (cyber-physical) systems is well known[14,22–36]. Visibility, a high level of adequacy of the mathematical model and a deeply worked out mathematical apparatus of Markov processes make it possible to use it in such areas as control of operation processes, queuing systems, the operational reliability of these types of systems and their components. The main advantages of Markov processes are the ability to build predictively controlled models of the behaviour of a cyber-physical system or a group of its components in time based on statistical information or the results of operational observations. Most often, a Markov process is presented as a model with a probabilistic structure, which allows one to determine the probability of a cyber-physical system falling into one of the states of the process for a certain time or time interval.

One of the most effective ways to significantly reduce the cost of maintenance and repair of cyber-physical systems is the choice of the optimal strategy for their operation. When describing the model of the behaviour of a cyber-physical system using the analytical apparatus of the Markov process, it seems possible to link the probabilistic structure of the change in the state of the system with income or expenses that arise when the system passes from one state of the process to another (for example, the transition of a system from an unfunctional state to a functional one is accompanied by the cost of its repair). With this approach, labour costs for its maintenance are used as the main indicator for analyzing a system, and a model based on Markov processes allows us to estimate the total labour costs for maintaining a system for a certain period of operation, as well as to choose a control strategy in which the costs of operating the system under study will be optimal.

In addition, assessing the functional safety of the cyber-physical systems involves machine learning methods[25–27]. This trend is due to the need to automate the process of detecting in the logs with the results of the operation of the target system of features characteristic of known types of vulnerabilities. This task is semantically related to intelligent data analysis. However, the use of smart technologies in the field investigated in this article is risky because the first ones demonstrate high efficiency in processing the content of balanced and statistically representative data sets. Still, the content of real logs is far from these ideals. Also relevant is the question of the difference between qualitative metrics in intelligent data analysis (classification task in the field of pattern recognition theory) and the field of dependability theory.

Let's accumulate the mentioned information by defining the obligatory attributes of scientific investigation. Thus, the *object* of investigation is the operation process of the cyber-physical system. The *subject* of research is the mathematical apparatus of probability theory mathematical statistics, and the theory of Markov chains. This study *aims* to create information technology for assessing functional safety based on the Markov model of cyber-physical system operation. The *main contribution* of this paper are the following:

1. we have described the life cycle of the cyber-physical system in the context of determining its functional safety in the form of compact and informative metrics;
2. we have created the model of cyber-physical system operation using Markov chain, and have considered:
   - the situation of lack of the necessary mechanism in the protection subsystem (new vulnerability);
   - the situation when the protection subsystem neutralizes the failure caused by a known vulnerability in one cycle (normal operation of the protection subsystem);
   - the situation when the protection subsystem neutralizes the failure caused by a known vulnerability in more than one cycle (system in idle);
3. we have formalized the method of calculating the criteria of the created metric for an instance of the cyber-physical system operation model, taking into account information from etalon databases on known vulnerabilities and empirical information on the results of operation of the investigated system.

Models and methods

Research statement. Assume that the set of stable states of the investigated cyber-physical system in discrete time is defined as $S = \left\{S_j; j = \left\{0, i = \overline{1,n}, \overline{n+1,2n}\right\}\right\}$, where S_0 is the operational state and $S_{th} = \left\{S_i, i \in I = \overline{\{1,n\}}\right\} \in S$ is the set of intermediate inoperational states of the system response to i-th failure $i \in I$. From the $S_i \in S_{th}$-th state, the cyber-physical system can either (if the protection mechanisms neutralize the failure) return to the operational state S_0, or (otherwise) move to the corresponding final inoperational state $S_{2i} \in S_f = \left\{S_{2i}, i \in I = \overline{\{1,n\}}\right\} \in S$ (states of the set S_f differ in consequences from the implementation of the corresponding failures).

Suppose that at the initial moment $t = 0$ of the interval of censored observation, the investigated cyber-physical system is in the state S_0. Then:

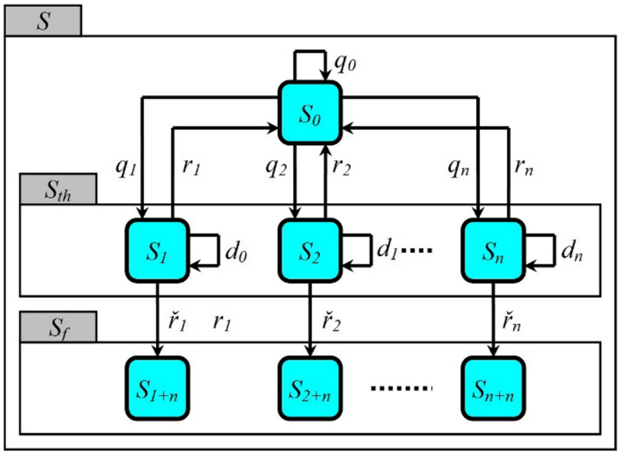

Figure 1. UML state diagrams of the model of the investigated cyber-physical system operation.

1. A cyber-physical system in state S_0 at a time $t > 0$ can at the time $t + 1$: (a) with probability q_i move to state $S_i \in S_{th}$ if the i-th failure is realized; (b) with probability $q_0 = 1 - \sum_{i=1}^{n} q_i$ will remain in state S_0.
2. A cyber-physical system in state $S_i \in S_{th}$ at a time $t > 0$ can at the time $t + 1$: (a) with probability r_i move to state S_0 (protection mechanisms have neutralized the failure); (b) with the probability d_i will remain in the state S_i (counteraction of protection mechanisms of failure proceeds); (c) with probability $\tilde{r}_i = 1 - r_i - d_i$ move to state $S_{2i} \in S_f$ (failure is not neutralized, so the system becomes inoperational).
3. The cyber-physical system in state $S_{2i} \in S_f$ at the time $t > 0$ will remain in this state throughout the censored observation interval.

These initial provisions indicate that the state of the investigated cyber-physical system at an arbitrary discrete moment of time is recognized only as the state in which it was at the previous moment of time. Thus, the semantic relationship between the states of the set S is determined by the provisions of the theory of Markov chains and can be clearly represented in the form of UML state diagram, visualized in Fig. 1.

The stochastic input parameters of the model of the investigated cyber-physical system operation are organized into such sets with power n as:

- set $Q = \left\{q_i; i = \overline{1, n}\right\}$, which characterizes the probabilities of the corresponding failures;
- set $R = \left\{r_i; i = \overline{1, n}\right\}$, which characterizes the probabilities of neutralization of the respective failures by protection mechanisms for one cycle Δt;
- the set $D = \left\{d_i; i = \overline{1, n}\right\}$ indicates the probabilities that protection mechanisms' counteraction to the respective failures will last more than one cycle Δt.

The values of the elements of these sets must correspond to the conditions:

$$\left(\sum_{i=1}^{n} q_i \leq 1\right) \& (d_i + r_i \leq 1) \forall i \in I. \tag{1}$$

In order to determine the Markov chain presented in Fig. 1, it is necessary to calculate the probabilities of all $i \in I$ of its states from the set S at time t:$\left\{p_i(t); i = \overline{0, 2n}\right\} = P(t)$. The classical formula can describe the process of this calculation in matrix form:

$$P(t) = P(0)\Pi^t. \tag{2}$$

For presented in Fig. 1 of the Markov chain, the matrix of transition probabilities Π mentioned in expression (2) is defined as

$$\Pi = \begin{pmatrix} q_0 & q_1 & q_2 & \dots & 0 & 0 & 0 & \dots & 0 \\ r_1 & d_1 & 0 & \dots & 0 & \breve{r}_1 & 0 & \dots & 0 \\ r_2 & 0 & d_2 & \dots & 0 & 0 & \breve{r}_2 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ r_n & 0 & 0 & \dots & d_n & 0 & 0 & \dots & \breve{r}_n \\ 0 & 0 & 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 1 \end{pmatrix}. \tag{3}$$

For real cyber-physical systems characterized by large values of n and t, the need to raise the matrix (3) to the power of t makes calculating the required values of the set $P(t)$ according to expression (2) computationally inefficient. But there are two exceptions:

1. If the protection mechanisms of the cyber-physical system do not function, i.e. $R = \{r_i = 0; i = \overline{1,n}\}$. In this case, the elements of the set P can be defined as

$$p_0(t) = q_0^t, t \geq 0, \tag{4}$$

$$p_i(t) = q_i\left(\frac{q_0^t - d_i^t}{q_0 - d_i}\right), \quad i = \overline{1,n}, \ t \geq 0, \tag{5}$$

$$p_{i+n}(t) = q_i\left(\frac{(1-q_0)(d_i^t - 1) - (q_0^t - 1)(1 - d_i)}{(q_0 - d_i)(1 - q_0)}\right). \tag{6}$$

2. If the protection mechanisms of the cyber-physical system have managed to neutralize the failure in one cycle Δt: $D = \{d_i = 0; i = \overline{1,n}\}$. In this case, the elements of the set P can be defined as:

$$p_0(t) = \frac{\gamma_+^{t+1} - \gamma_-^{t+1}}{w}, \quad t \geq 0, \tag{7}$$

$$p_i(t) = \frac{q_i\left(\gamma_+^t - \gamma_-^t\right)}{w}, \quad i = \overline{1,n}, \ t \geq 0, \tag{8}$$

$$p_{i+n}(t) = \frac{q_i(1 - r_i)}{w}\left(\frac{1 - \gamma_+^t}{1 - \gamma_+} - \frac{1 - \gamma_-^t}{1 - \gamma_-}\right), \tag{9}$$

where: $w = \sqrt{q_0 + 4\sum_{i=1}^{n} q_i r_i}$ is a controlled parameter that characterizes the generalized efficiency of the reaction of protection mechanisms and $\gamma_\pm = \frac{q_0 \pm w}{2}$.

For $r_i \to 0$ and $d_i \to 0$, expressions (4), (5), (6) and (7), (8), (9) coincide in pairs. For both described exceptions, the marginal relationship

$$\lim_{t\to\infty} p_0(t) = \lim_{t\to\infty} p_1(t) = \ldots = \lim_{t\to\infty} p_n(t) = 0, \tag{10}$$

holds, i.e., with a sufficiently large value of t, the values of the probabilities of the investigated system in the states of the combined set $S_0 \cup S_{th}$ are extremely small.

The corresponding boundary relations for the states defined by expressions (6) and (9) from the set S_f are formalized as follows:

$$\lim_{t\to\infty} p_{i+n}(t) = \frac{q_i}{1 - q_0}, \quad i = \overline{1,n},$$

$$\lim_{t\to\infty} p_{i+n}(t) = \frac{q_i(1 - r_i)}{(1 - \gamma_+)(1 - \gamma_-)}, \quad i = \overline{1,n}.$$

It is seen that the limit values of the probabilities of realization of states from the set S_f are determined by the values of the initial parameters of the investigated system operation model, i.e., laid at the stage of its design.

Functional safety assessment technology based on the model of cyber-physical system operation. To determine the claimed technology, it is necessary to formalize the qualitative metrics and the concept of its calculation for an arbitrary instance of the model of cyber-physical system operation in the parametric space of the corresponding attribute of dependability, i.e. functional safety.

According to the material presented in "Research statement", it can be stated that the set of states of the model of the investigated cyber-physical systems operation S is a conglomerate of sets of states S_0, S_{th}, S_f:

$S = S_0 \cup S_{th} \cup S_f$, the probabilities of realization of which elements are formalized in the transition matrix (3). If we analyze the conglomerate of sets $S = S_0 \cup S_{th} \cup S_f$ from the standpoint of the structure shown in Fig. 1 of the graph, it can be stated that the states $S_i \in S_0 \cup S_{th}, i = \overline{0, n}$, are transient and the states $S_{i+n} \in S_f, i = \overline{1, n}$ are finite.

We define in the matrix of transient probabilities (3) fragments, which, respectively, characterize the transient and final states of the model of the investigated system operation:

$$Q(\Pi) = \begin{pmatrix} q_0 & q_1 & q_2 & \dots & 0 \\ r_1 & d_1 & 0 & \dots & 0 \\ r_2 & 0 & d_2 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ r_n & 0 & 0 & \dots & d_n \end{pmatrix}, \tag{11}$$

$$R(\Pi) = \begin{pmatrix} 0 & 0 & \dots & 0 \\ \breve{r}_1 & 0 & \dots & 0 \\ 0 & \breve{r}_2 & \dots & 0 \\ 0 & 0 & \dots & \breve{r}_n \end{pmatrix}. \tag{12}$$

Considering the content of matrices (11) and (12), we present a matrix of transition probabilities Π in block form:

$$\Pi = \begin{pmatrix} Q(\Pi) & R(\Pi) \\ 0 & I(\Pi) \end{pmatrix},$$

where $I(\Pi)$ is a unit matrix of dimension $n \times n$.

Considering the limit relations (10), for $t \to \infty$ we write: $Q^t(\Pi) \to 0$, where it is obvious that the absolute values of the eigenvalues of the matrix $Q(\Pi)$ are strictly less than one. This, in turn, means that the inverse form of the nondegenerate matrix $(I(\Pi) - Q(\Pi))$ can be represented as follows:

$$A = (Q(\Pi) - I(\Pi))^{-1} = I(\Pi) + Q(\Pi) + Q^2(\Pi) + \cdots \tag{13}$$

The element's value $a_{ij} \in A$ shows how many times the studied Markov process from the state S_j will reach the state S_i. We interpret this definition in the context of the task of finding the metrics of functional safety assessment based on the model of the cyber-physical system operation.

Let the process of the investigated cyber-physical system operation start from the state S_0. Then we estimate the time of the inoperation of this process to consider the stochastic value of the parameter T, which is equal to the number of transitions between states from the combined set $S_0 \cup S_{th}$ until the process enters one of the states from the set S_f. The mathematical expectation of the stochastic parameter T is determined by interpreting the contents of the matrix (13): $\tau = \sum_{j=1}^{n+1} a_{1j}$.

In the transition from the block representation of the matrix A to the form (11), the newly obtained expression can be redefined as follows:

$$\tau = \frac{\sum_{i=1}^{n} q_i \prod_{j=1}^{n} \left(1 - d_j\left(1 - \delta_{ij}\right)\right) + \prod_{j=1}^{n} \left(1 - d_j\right)}{\sum_{i=1}^{n} q_i \prod_{j=1}^{n} \left(1 - d_j - r_j\delta_{ij}\right)}, \tag{14}$$

where δ_{ij} is the corresponding Kronecker delta.

If the set of potential failures is a priori defined in the form Q, then the parameter τ can be expressed as some function in the form $\tau = f(Q, R, D)$, continuous in the domain of its arguments. The range of valid values of the parameter τ is defined as $[\tau_{\min}, \infty)$, where $\tau = f(Q, 0, 0)$ or $\tau_{\min} = 1 + \left(\sum_{i=1}^{n} q_i\right)^{-1}$.

As noted earlier, the probability of inoperation of the investigated cyber-physical system due to the implementation of the i-th failure despite the opposition of protective mechanisms is equal to $\breve{r}_i$. Let us estimate the losses from realizing such an event by a positive discrete value $u_i \in U = \left\{u_i; i = \overline{1, n}\right\}$. Let us summarize these values as the corresponding risk factor $f_i = \breve{r}_i u_i$. The mathematical expectation of such a stochastic quantity as a risk factor is defined as $\varphi = \sum_{i=1}^{n} \breve{r}_i u_i$.

We formalize the expression for calculating the parameter φ in terms of the Markov chain visualized in Fig. 1. Let's raise the matrix of transition probabilities Π presented in block form to the power t:

$$\Pi^t = \begin{pmatrix} Q^t(\Pi) & \varphi\left(\sum\limits_{k=0}^{t-1} Q^k \Pi\right) \\ 0 & I(\Pi) \end{pmatrix}. \tag{15}$$

The absolute values of the eigenvalues of the matrix $Q(\Pi)$ are strictly smaller than unity, so for $t \to \infty$ the following boundary relations are satisfied: $Q^t(\Pi) \to 0$, $\sum_{k=0}^{t} Q^k(\Pi) \to A$, where we have already mentioned the matrix in expression (13). We define the form of the matrix (15) for $t \to \infty$:

$$\lim_{t \to \infty} \Pi^t = \begin{pmatrix} 0 & \varphi A \\ 0 & I(\Pi) \end{pmatrix}.$$

Let the Markov model of the investigated system at time $t = 0$ be in the state S_0, then, at $t \to \infty$, we write:

$$\breve{r}_i = \lim_{t \to \infty} p_{i+n}(t) = \frac{q_i \prod_{j=1}^{n} \left(1 - d_j - r_j \delta_{ij}\right)}{\sum_{k=1}^{n} q_k \prod_{j=1}^{n} \left(1 - d_j - r_j \delta_{ij}\right)}, \quad i = \overline{1, n}. \tag{16}$$

Based on expression (16) for the parameter φ we write:

$$\varphi = \frac{\sum_{i=1}^{n} q_i u_i \prod_{j=1}^{n} \left(1 - d_j - r_j \delta_{ij}\right)}{\sum_{k=1}^{n} q_k \prod_{j=1}^{n} \left(1 - d_j - r_j \delta_{ij}\right)}. \tag{17}$$

Expressions (14) and (17) allow calculating the value of the required metric $\{\tau, \varphi\}$ (τ is the mathematical expectation of the time till the cyber-physical system inoperation, φ is the mathematical expectation of risk factor) for an instance of the Markov model of the operation of investigated cyber-physical system characterized by the content of the sets conglomerate $\{Q, D, R, U\}$. Also, an important parameter is the positive integer value of the duration of the cycle Δt, which means the minimum time interval after which the investigated system can change its state.

In general, the number of fixed parameters for calculating the metric $\{\tau, \varphi\}$ is equal to $4n + 1$, where n is the number of potential categorized failures, which in modern cyberspace exceeds 1.5×10^5. However, this impressive number is an absolute one. More specifically, current failures for cyber-physical systems are justified and ranked according to the degree of danger in such open vulnerability assessment systems[14,28,29] as Damage, Reproducibility, Exploitability, Affected users, Discoverability (DREAD); Common Vulnerability Scoring System (CVSS); Vulnerability Priority Rating (VPR).

In the future, the authors will focus on the *VPR* system. Here is analytical information in favour of this choice. Not only publicly available technical data but also cyber intelligence is used to address vulnerabilities in the VPR system. Empirical studies[28,29] have shown that the upgrade of the information and communication system to address 400 critical vulnerabilities detected by VPR has shown the same effect on increasing functional safety as the upgrade of the base version of the same system to address 9000 critical vulnerabilities, detected using the CVSSv3 system. This result convincingly proves that the catalogue of vulnerabilities in the VPR system is organized more rationally than analogues.

Let the $M = \overline{1, m}$ vulnerabilities be identified in the investigated cyber-physical system at the pre-release testing stage[30–32]. Let $v_{\alpha,i}$ be the value of the base VPR metric for vulnerability α, which can lead to failure i (this cause-and-effect relationship we identify as $V_{\alpha,i}$), where $\alpha = \overline{1, m_i}$, $i = \overline{1, n}$, $\sum_{i=1}^{n} m_i = m$ (each vulnerability α can lead to only one failure i). It is possible to predict the existence of a certain functional relationship between the probability of i-th failure q_i and the value of the VPR-metric $v_{\alpha,i}$. Naturally, the more vulnerabilities that can cause the i-th failure, the greater the probability q_i against the background of analogues will be (remember that $\sum_{i=1}^{n} q_i = 1$). In the first approximation, we formalize this functional dependence as follows:

$$q_i = \alpha k_i, \quad i = \overline{1, n}, \tag{18}$$

where α is the positive weighting coefficient, and the parameter k_i is calculated by the expression

$$k_i = \frac{\sum_{\alpha=1}^{m_i} v_{\alpha,i}}{\sum_{j=1}^{n} \sum_{l=1}^{m_j} v_{jl}}. \tag{19}$$

Analysis of expression (19) allows us to state that the parameter k_i and available in the presented in Fig. 1 Markov chain[33,34], the probability of neutralization of the i-th failure $(1 - d_i)^{-1} r_i$ are also functionally related, which in the first approximation is described by the expression:

$$r_i = \beta (1 - d_i) k_i, \quad i = \overline{1, n} \tag{20}$$

where β is a positive weighting coefficient.

We connect the author's metric $\{\tau, \varphi\}$ with the VPR metric by summarizing expressions (14) and (18) and (17) and (20). In accordance:

$$\tau = \left(\frac{1}{\alpha} + \sum_{i=1}^{n} \frac{k_i}{1 - d_i} \right) \Bigg/ \left(1 - \beta \sum_{i=1}^{n} k_i^2 \right), \tag{21}$$

$$\varphi = \left(\sum_{i=1}^{n} u_i k_i (1 - \beta k_i) \right) \Bigg/ \left(1 - \beta \sum_{i=1}^{n} k_i^2 \right). \tag{22}$$

Expressions (21), (22) are formulated taking into account the rationing $\sum_{i=1}^{n} k_i = 1$. Note that in the expression (22) for the calculation of the mathematical expectation of the risk factor φ, the parameters α and $d_i \in D$ are absent.

The values of weighting coefficients α, β and parameters $d_i \in D$ are proposed to be determined by expert evaluation (at the design stage of the investigated cyber-physical system), or as a result of statistical analysis of the results of the censored period of its operation (for already accepted into operation cyber-physical system). Let's explore the latter option in more detail.

Let the content of the logs of the investigated cyber-physical system be sufficiently statically representative to calculate:

- the mathematical expectation of the number of cycles between failures $\langle T^* \rangle$;
- the mathematical expectation of the number of cycles required by the protective mechanisms to neutralize the i-th failure $\langle d_i^* \rangle$;
- share of successfully neutralized failures $\left(p_r^*\right)$.

In terms of presented in Fig. 1 the Markov chain, the estimation of these parameters can be indirectly calculated by the relevant expressions:

$$\langle T^* \rangle_{\approx} = \left(\sum_{i=1}^{n} q_i\right)^{-1}, \langle d_i^* \rangle_{\approx} = (1 - d_i)^{-1},$$

$$\left(p_r^*\right)_{\approx} = \sum_{i=1}^{n} \left(q_i r_i / (1 - d_i)\right) \Big/ \sum_{i=1}^{n} q_i. \tag{23}$$

Substituting expressions (23) into expressions (18), (20), we determine the estimates for the weighting coefficients α, β and parameters $d_i \in D$:

$$\alpha_{\approx} = 1/\langle T^* \rangle_{\approx}, \beta_{\approx} = \left(p_r^*\right) \Big/ \sum_{i=1}^{n} k_i^2, (d_i)_{\approx} = 1 - \frac{1}{\langle d_i^* \rangle},$$

based on which we analytically express the estimates for the metric $\{\tau, \varphi\}$:

$$\tau_{\approx} = \frac{\langle T^* \rangle_{\approx} + \sum_{i=1}^{n} \langle d_i^* \rangle_{\approx} k_i}{1 - \left(p_r^*\right)_{\approx}}, \tag{24}$$

$$\varphi_{\approx} = \frac{1}{1 - \left(p_r^*\right)_{\approx}} \left(\sum_{i=1}^{n} u_i k_i - \left(p_r^*\right)_{\approx} \frac{\sum_{i=1}^{n} u_i k_i^2}{\sum_{i=1}^{n} k_i^2}\right). \tag{25}$$

If inequality (26) holds, then expressions (25), (27) can be used to calculate the metric $\{\tau, \varphi\}$. Constraint

$$\left(p_r^*\right)_{\approx} \le \min_i \left\{ \sum_{j=1}^{n} k_j^2 \Big/ k_i \right\} \tag{26}$$

is formulated due to the extension to the parameters calculated by expression (23) the condition (1).

Finally, the values of the parameters $u_i \in U$, which characterize the losses associated with the inability of the protective mechanisms of the investigated instance (class) of cyber-physical systems to neutralize the i-th failure, should be assessed purely by an expert method[35–37].

Results

As an example, we use the technology presented in "Models and methods" to assess the functional safety of the model of a real cyber-physical system at the Situation Center of the Department of Information Technology (DIT) of Vinnytsia City Council (VCC) (Vinnytsia, Ukraine). This information and communication system was taken into operation in 2018 and is constantly evolving to improve the implemented services and add new ones. Currently, this information and communication system manages traffic lights on the roads of Vinnytsia. It supports the uninterrupted operation of the data center, which stores video streams from more than 1 k video cameras located in the city.

Collected of confidential information in the system is open only to authorized employees of the Vinnytsia City Council, the National Police of Ukraine, the Security Service of Ukraine, etc. In order for these privileged persons to have prompt access to the relevant information, a local network was created consisting of data center servers, communication equipment, workstations, and software. In normal operation, this LAN is not isolated from the WWW. However, the processing, storage, and audit of confidential information are carried out by a specialized relational database management system, access to which is organized through a specialized web interface. Data, databases and management system, web interface—all these components are located on dedicated servers.

We imitate a situation where attackers exert a deliberate influence on the information and communication system of the Situation Center, which threatens the functional safety of the latter. Attackers seek information about network architecture, workstations, servers, operating systems, user accounts and more. Analysis of this information can identify hardware and software vulnerabilities, some of which may not fall within the scope of the protection subsystem.

In the realities of modern cyberspace, exploits are often created based on data collected as a result of:

- In_1 (Apache): analysis of internal and outgoing network traffic, the mechanism for supporting remote access;
- In_2: buffer overflow;
- In_3: SQL injection.

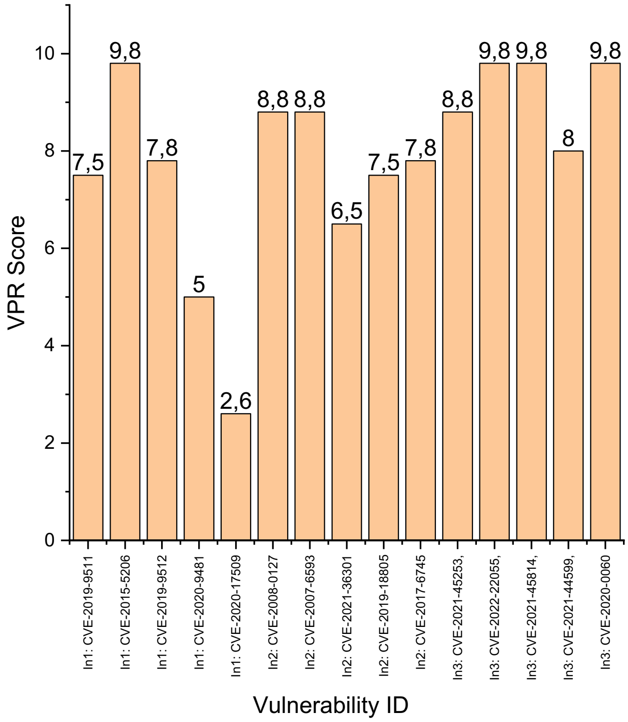

Figure 2. Values of VPR metrics for vulnerabilities mentioned in sets In_1–In_3.

The analysis of the logs of the information and communication system of the Situation Center revealed the following categorized vulnerabilities[38–40]:

- In_1: (a) CVE-2019-9511, (b) CVE-2015-5206, (c) CVE-2019-9512, (d) CVE-2020-9481, (e) CVE-2020-17509;
- In_2: (a) CVE-2008-0127, (b) CVE-2007-6593, (c) CVE-2021-36301, (d) CVE-2019-18805, (e) CVE-2017–6745;
- In_3: (a) CVE-2021-45253, (b) CVE-2022-22055, (c) CVE-2021-45814, (e) CVE-2021-44599, (e) CVE-2020-0060.

A full description of these vulnerabilities can be found at https://www.cvedetails.com/. Note that at the request of VCC administration, the sets In_1–In_3 do not contain a complete list of vulnerabilities identified in the investigated system. However, these data are sufficient to demonstrate the functionality of the technology presented in "Models and methods". The values of the VPR metric for the vulnerabilities listed in the sets In_1 –In_3 are clearly presented in Fig. 2.

Using the presented in Fig. 2 data $v_{i,\alpha}$, $i=\overline{1,3}$, $\alpha=\overline{1,5}$, by expression (19) we calculate the values of the coefficients k_i: $K=\{0.3331, 0.3910, 0.2764\}$. For further calculations, it is necessary to determine the duration of the cycle Δt. Analysis of the logs of the investigated system allows us to establish it as equal to the day: 24 [h]. Based on the known description of the identified vulnerabilities, the involved experts estimated the average duration of the impact of each i-th type of vulnerabilities, $i=\overline{1,3}$, on the investigated system as follows: $\langle D^*\rangle_\approx=\{96, 24, 60\}$ [h], and the estimated loss u_i from their implementation as follows: $U=\{0.2, 0.2, 0.6\}$ [c.u.] We substitute the obtained values into expressions (24), (25) and get object-oriented expressions for estimating the criteria of the author's metric $\{\tau, \varphi\}$:

$$\tau_\approx=\frac{2.4151+\langle T^*\rangle_\approx}{1-\left(p_r^*\right)_\approx}, \tag{27}$$

$$\varphi_\approx=\frac{0.3562-0.3795\left(p_r^*\right)_\approx}{1-\left(p_r^*\right)_\approx}. \tag{28}$$

Now we define the object-oriented condition (26) for the application of estimates (27): $\left(p_r^*\right)_\approx<\max\left(p_r^*\right)=0.8702$.

By changing the parameter's value $\left(p_r^*\right)_\approx$ at a fixed value of the parameter $\langle T^*\rangle_\approx=const$, we calculate the dependence of $\tau_\approx=f\left(\left(p_r^*\right)_\approx, \langle T^*\rangle_\approx\right)$ for the investigated system using expression (27) and present the results in Fig. 3.

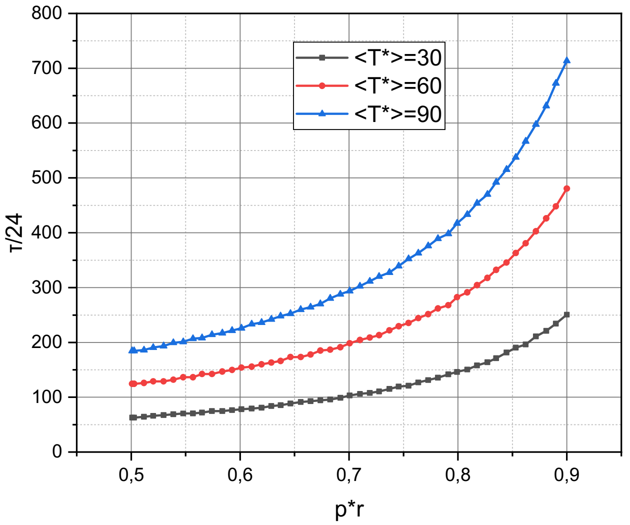

Figure 3. Calculated dependences $\tau_{\approx} = f\left(\left(p_r^*\right)_{\approx}, \langle T\rangle_{\approx} = \{30, 40, 60\}\right)$.

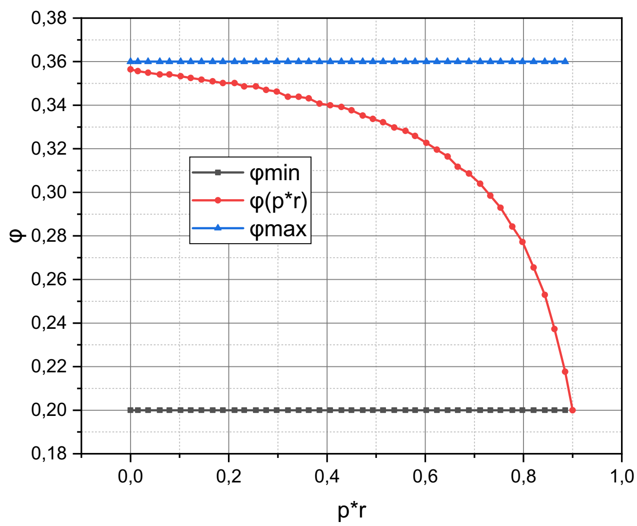

Figure 4. The calculated dependence $\varphi_{\approx} = f\left(\left(p_r^*\right)_{\approx}\right)$ in the confidence interval $[\varphi_{\min} = 0.2, \varphi_{\max} = 0.36]$.

The dependence $\tau_{\approx} = f\left(\left(p_r^*\right)_{\approx}, \langle T^*\rangle_{\approx}\right)$ is chosen not by chance because it has an application, which is to determine the minimum threshold value $\left(p_r^*\right)_{\approx}$, at which the value of the criterion τ will not be less than the specified value τ_0. For the investigated information and communication system, this definition is embodied in the expression

$$\left(p_r^*\right) \geq 1 - \left(2.4152 + \left\langle T^*\right\rangle_{\approx}\right)\tau_0^{-1}. \tag{29}$$

By changing the parameter's value $\left(p_r^*\right)_{\approx}$, we calculate the dependence of $\varphi_{\approx} = f\left(\left(p_r^*\right)_{\approx}\right)$ for the investigated system using expressions (28) and present the results in Fig. 4.

As we noted in the formalization of expression (17), the change in the parameter $\langle T\rangle$ does not affect the value of the criterion φ. The dependence $\varphi_{\approx} = f\left(\left(p_r^*\right)_{\approx}\right)$ also has an application, which is to determine the minimum threshold value $\left(p_r^*\right)_{\approx}$, at which the value of the criterion φ will not be less than the specified value of φ_0. For the investigated information and communication system, this definition is embodied in the expression

$$\left(p_r^*\right) \geq (\varphi - 0.3562)/(\varphi_0 - 0.3795). \tag{30}$$

Thus, as an experiment, we investigated the model of operation of the cyber-physical system of the Situation Center of DIT of VCC in the metrics of functional safety, formalized in "Models and methods".

Discussion

Let's start the discussion of the results presented in "Results" with a brief excursion into their theoretical background. Thus, we calculated the estimates of the metric $\{\tau, \varphi\}$ (τ is the mathematical expectation of the time till the cyber-physical system inoperation, φ is the mathematical expectation of risk factor that describes the losses from the probable fact of implementation of the failure despite the operation of protection mechanisms that cause inoperation) for the cyber-physical system of the Situation Center of DIT of VCC. It is characterized by the content of the conglomerate of sets $\{Q, D, R, U\}$ and the value of the duration of the cycle Δt (the minimum time interval after which the investigated system can change its state).

The availability of a statistically representative amount of information on the operation of the investigated system allowed experts to classify potential failures in the VPR metric. These circumstances allowed us to move from the direct calculation of the criteria of the metric $\{\tau, \varphi\}$ by expressions (21), (22) to the calculation of estimates of these criteria $\{\tau_{\approx}, \varphi_{\approx}\}$ by expressions (24), (25). To calculate the estimates $\{\tau_{\approx}, \varphi_{\approx}\}$ for the investigated system by expressions (23), the elements of the sets:—$\langle T^* \rangle$ (mathematical expectations of the number of cycles between the respective failures), $\langle D^* \rangle$ (mathematical expectations of the number of cycles required by protection mechanisms to neutralize the corresponding failures), $\left(p_r^*\right)$ (share of successfully neutralized failures); were previously calculated for the investigated system by expressions (23).

The presented in Fig. 2 information shows that defined in the VPR-metrics of the risk assessment of the identified threats to the investigated system differ significantly in terms of the values of this general characteristic and the mechanisms for implementing the relevant failures. Direct analysis of this information without the mathematical apparatus presented in "Models and methods" does not allow to establish a functional relationship between the information in Fig. 2 and the values of the indicators of the functional safety attribute. Thus, the relevance of our research was reaffirmed.

The presented in Fig. 3 information shows that the increase in the values of both parameter $\langle T^* \rangle_{\approx}$ and parameter $\left(p_r^*\right)_{\approx}$ positively affect the value of the criterion $\tau_{\approx}$, which characterizes the assessment of the mathematical expectation of the time till the investigated cyber-physical system inoperation. Obviously, the greater the parameter value $\langle T^* \rangle_{\approx}$, the greater the interval between failures, i.e., the intensity of the negative impact on the investigated system decreases. At the same time, the growth of the parameter $\left(p_r^*\right)_{\approx}$ indicates an increase in the share of successfully neutralized failures, i.e., positively characterizes the configuration scheme and architecture of the protection subsystem of the investigated system.

The condition (29) defined for the investigated system also positively affects the practical orientation of the criterion τ. With its help, for example, it is easy to see that for the value of the criterion τ for the investigated system to be greater than $\tau_0 = 200 \times 24$ [h], it is necessary that the inequality $\left(p_r^*\right)_{\approx} \geq 0.9879 - 0.005 \langle T^* \rangle_{\approx}$ be satisfied, i.e., at $\langle T^* \rangle_{\approx} = 30 \times 24$ [h] we has $\left(p_r^*\right)_{\approx} \geq 0.8379$ and at $\langle T^* \rangle_{\approx} = 60 \times 24$ [h] we have $\left(p_r^*\right)_{\approx} \geq 0.6879$. But unfortunately, the parameter $\left(p_r^*\right)_{\approx}$ is a general qualitative characteristic of the protection subsystem. In this research, we do not give recommendations on how to organize this subsystem and do not assess whether the calculated value $\left(p_r^*\right)_{\approx}$ is achievable in principle.

The presented in Fig. 4 information shows that the risk factor acquires its maximum value $\varphi_{\approx} = 0.3562$ at $\left(p_r^*\right)_{\approx} = 0$, i.e. if the protection subsystem functions perfectly or negative effects on the investigated system are completely absent (relatively close to reality example of such a situation is the operation of the investigated system isolated from the global network) then the risk factor acquires the minimum value of $\varphi_{\approx} = 0.2$ for the investigated system at $\left(p_r^*\right)_{\approx} = 0.8702$.

The result proves the obvious fact that even an ideal protection subsystem is not a basis for claiming that the target system is guaranteed against inoperation. Thus, the antagonism of the "second law of thermodynamics vs. perpetuum mobile" also works for cyber-physical systems. Another advantage of Fig. 4 is clear—the more convex the curve $\varphi_{\approx} = f\left(\left(p_r^*\right)_{\approx}\right)$, the more efficient the protection subsystem.

So, we have described two functional security metrics based on the Markov model for the operation of a cyber-physical system. We have also shown that using the general VPR vulnerability system, the parameters of this model can be effectively estimated based on a small amount of empirical data, which is an undeniable advantage compared to, for example, the expert assessment method. Of course, the model we have considered has several assumptions related, in particular, to the impossibility of the simultaneous occurrence of several failures, as well as their independence from each other. Our further work will be aimed at weakening these assumptions and obtaining a more complex and generalized model, the dynamics of which will be as close as possible to the behaviour of real systems.

Finally, it should be noted that the technology of functional safety assessment based on the Markov model of cyber-physical system operation proposed in the article is based on generally accepted, valid, updated VPR-metrics and proved to be an adequate mathematical apparatus of Markov chains. These facts, and the rigor and reversibility of the analytical transformations made in the formalization of the metric $\{\tau, \varphi\}$ substantiate the adequacy of the mathematical apparatus presented in the article.

Conclusions

The assessment of functional safety is one of the primary tasks both at the design stage and at the stage of operation of critical infrastructure at all levels. The article's main contribution is the information technology of calculating the author's metrics of functional safety for estimating the instance of the model of the cyber-physical system operation. The calculation of metric criteria (mathematical expectation of cyber-physical system operation to failure and risk factor) analytically summarizes the results of expert evaluation of the system in VPR-metrics and the results of statistical processing of information on the system's operation presented in the parametric space Markov model of this process. The advantage of the author's approach over analogues is:

- the need to process orders of magnitude less empirical data to obtain objective estimates of the investigated system;
- taking into account the configuration scheme and architecture of the security subsystem of the investigated system when calculating the metric;
- completeness, compactness, and simplicity of interpretation of evaluation results;
- the ability to assess the achievability of the limit values of the metric criteria based on the model of operation of the investigated system.

As an example, the article demonstrates the author's technology to assess the functional safety of the model of a real cyber-physical system of the Situation Center of the Department of Information Technology of Vinnytsia City Council (Vinnytsia, Ukraine).

However, in formalizing the Markov model of cyber-physical system operation, attackers believed that vulnerabilities used to lead to failures or inoperation were independent. The probable situation of simultaneous exploitation of one vulnerability by more than one attacker was also not considered. Considering these circumstances in the mathematical apparatus presented in the article is the direction of further research.

Data availability

The datasets for the analyzed during the current study are available in CVE Details: the ultimate security vulnerability data source repository: https://www.cvedetails.com/. All data on the link is in the public domain. In our study, we used data on such vulnerabilities as: CVE-2019-9511, CVE-2015-5206, CVE-2019-9512, CVE-2020-9481, CVE-2020-17509, CVE-2008-0127, CVE-2007-6593, CVE-2021-36301, CVE-2019-18805, CVE-2017-6745, CVE-2021-45253, CVE-2022-22055, CVE-2021-45814, CVE-2021-44599, CVE-2020-0060.

Received: 8 February 2022; Accepted: 20 April 2022
Published online: 30 April 2022

References

1. Kochanthara, S. *et al.* A functional safety assessment method for Cooperative Automotive Architecture. *J. Syst. Softw.* **179**, 110991. https://doi.org/10.1016/j.jss.2021.110991 (2021).
2. Babeshko, E., Illiashenko, O., Kharchenko, V. & Ruchkov, E. Safety and reliability assessment of NPP instrumentation and control systems considering different communication architectures. *Nucl. Radiat. Saf.* **2**(86), 38–43. https://doi.org/10.32918/nrs.2020.2(86).05 (2020).
3. Kharchenko, V., Ponochovnyi, Y., Waleed, A.-K.A., Boyarchuk, A. & Brezhniev, I. The availability models of two-zone physical security system considering cyber attacks. *Theory Appl. Dependable Comput. Syst.* https://doi.org/10.1007/978-3-030-48256-5_32 (2020).
4. Śliwiński, M., Piesik, E. & Piesik, J. Integrated functional safety and cyber security analysis. *IFAC-PapersOnLine* **51**(24), 1263–1270. https://doi.org/10.1016/j.ifacol.2018.09.572 (2018).
5. Hoffman, L. J. & Chu, B. C. When is seeking safety functional? Taking a pragmatic approach to distinguishing coping from safety. *Cogn. Behav. Pract.* **26**(1), 176–185. https://doi.org/10.1016/j.cbpra.2018.11.002 (2019).
6. Menges, F. *et al.* Towards GDPR-compliant data processing in modern SIEM systems. *Comput. Secur.* **103**, 102165. https://doi.org/10.1016/j.cose.2020.102165 (2021).
7. Radoglou-Grammatikis, P. *et al.* Spear siem: A security information and event management system for the smart grid. *Comput. Netw.* **193**, 108008. https://doi.org/10.1016/j.comnet.2021.108008 (2021).
8. Bryant, B. D. & Saiedian, H. Improving siem alert metadata aggregation with a novel kill-chain based classification model. *Comput. Secur.* **94**, 101817. https://doi.org/10.1016/j.cose.2020.101817 (2020).
9. Eswaran, S., Srinivasan, A. & Honnavalli, P. A threshold-based, real-time analysis in early detection of endpoint anomalies using SIEM expertise. *Netw. Secur.* **2021**(4), 7–16. https://doi.org/10.1016/s1353-4858(21)00039-8 (2021).
10. Martín, A. G., Beltrán, M., Fernández-Isabel, A. & Martín de Diego, I. An approach to detect user behaviour anomalies within identity federations. *Comput. Secur.* **108**, 102356. https://doi.org/10.1016/j.cose.2021.102356 (2021).
11. Maher, D. Can artificial intelligence help in the war on cybercrime?. *Comput. Fraud Secur.* **2017**(8), 7–9. https://doi.org/10.1016/s1361-3723(17)30069-6 (2017).
12. Hariyanti, E., Djunaidy, A. & Siahaan, D. Information security vulnerability prediction based on business process model using machine learning approach. *Comput. Secur.* **110**, 102422. https://doi.org/10.1016/j.cose.2021.102422 (2021).
13. Santos, J. C. S., Tarrit, K., Sejfia, A., Mirakhorli, M. & Galster, M. An empirical study of tactical vulnerabilities. *J. Syst. Softw.* **149**, 263–284. https://doi.org/10.1016/j.jss.2018.10.030 (2019).
14. Ruohonen, J. A look at the time delays in CVSS vulnerability scoring. *Appl. Comput. Inform.* **15**(2), 129–135. https://doi.org/10.1016/j.aci.2017.12.002 (2019).
15. Alanen, J. *et al.* Hybrid ontology for safety, security, and dependability risk assessments and security threat analysis (STA) method for Industrial Control Systems. *Reliab. Eng. Syst. Saf.* **220**, 108270. https://doi.org/10.1016/j.ress.2021.108270 (2022).
16. Blanc, S., Bonastre, A. & Gil, P. J. Dependability assessment of by-wire control systems using fault injection. *J. Syst. Archit.* **55**(2), 102–113. https://doi.org/10.1016/j.sysarc.2008.09.003 (2009).
17. Chemweno, P., Pintelon, L., Muchiri, P. N. & Van Horenbeek, A. Risk assessment methodologies in maintenance decision making: A review of dependability modelling approaches. *Reliab. Eng. Syst. Saf.* **173**, 64–77. https://doi.org/10.1016/j.ress.2018.01.011 (2018).
18. Kroculick, J. & Hood, C. A dependability assessment process for ensuring consistent provisioning of network recovery. *Proc. Comput. Sci.* **8**, 177–183. https://doi.org/10.1016/j.procs.2012.01.036 (2012).
19. Sun, D., Rauchhaupt, L. & Jumar, U. Multi-task learning for dependability assessment of industrial wireless communication systems. *IFAC-PapersOnLine* **54**(4), 165–170. https://doi.org/10.1016/j.ifacol.2021.10.028 (2021).
20. Faller, R. Project experience with IEC 61508 and its consequences. *Saf. Sci.* **42**(5), 405–422. https://doi.org/10.1016/j.ssci.2003.09.008 (2004).
21. Auzinger, W., Obelovska, K., Dronyuk, I., Pelekh, K. & Stolyarchuk, R. A continuous model for states in&CSMA/CA-based wireless local networks derived from state transition&diagrams. *Proc. Int. Conf. Data Sci. Appl.* https://doi.org/10.1007/978-981-16-5348-3_45 (2021).

22. Trunov, A., Kazan, P., Alieksieiev, V., Korolova, O., Sliusarenko, O., & Dronyuk, I. Functioning model of the ground robotic complex. In *2021 IEEE 16th International Conference on Computer Sciences and Information Technologies (CSIT)*. (2021). https://doi.org/10.1109/csit52700.2021.9648595.
23. Auzinger, W., Obelovska, K. & Stolyarchuk, R. A revised Gomory-Hu algorithm taking account of physical unavailability of network channels. In *Computer Networks. CN 2020. Communications in Computer and Information Science* Vol. 1231 (eds Gaj, P. *et al.*) (Springer, 2020). https://doi.org/10.1007/978-3-030-50719-0_1.
24. Obelovska, K., Panova, O. & Karovič, V. Performance analysis of wireless local area network for a high-/low-priority traffic ratio at different numbers of access categories. *Symmetry* **13**(4), 693. https://doi.org/10.3390/sym13040693 (2021).
25. Singh, R. *et al.* Highway 4.0: Digitalization of highways for vulnerable road safety development with intelligent IOT sensors and machine learning. *Saf. Sci.* **143**, 105407. https://doi.org/10.1016/j.ssci.2021.105407 (2021).
26. Stock, D., Schel, D. & Bauernhansl, T. Middleware-based cyber-physical production system modeling for operators. *Proc. Manuf.* **42**, 111–118. https://doi.org/10.1016/j.promfg.2020.02.031 (2020).
27. Yang, J., Xue, Y., Dai, X., Lu, H. & Yang, M. An intelligent operational supervision system for operability and reliability analysis of operators manual actions in Task Implementation. *Process Saf. Environ. Prot.* **158**, 340–359. https://doi.org/10.1016/j.psep.2021.12.023 (2022).
28. Ascione, F., De Masi, R. F., Mastellone, M. & Vanoli, G. P. Building rating systems: A novel review about capabilities, current limits and open issues. *Sustain. Cities Soc.* **76**, 103498. https://doi.org/10.1016/j.scs.2021.103498 (2022).
29. Razavi, S. D., Kapiriri, L., Wilson, M. & Abelson, J. Applying priority-setting frameworks: A review of public and vulnerable populations' participation in health-system priority setting. *Health Policy* **124**(2), 133–142. https://doi.org/10.1016/j.healthpol.2019.12.005 (2020).
30. Fataliyev, T. K. & Mehdiyev, S. A. Integration of cyber-physical systems in escience environment: State-of-the-art, problems and effective solutions. *Int. J. Mod. Educ. Comput. Sci. IJMECS.* **11**(9), 35–43 (2019).
31. Fataliyev, T. K. & Mehdiyev, S. A. Analysis and new approaches to the solution of problems of operation of oil and gas complex as cyberphysical system. *Int. J. Inf. Technol. Comput. Sci. IJITCS.* **10**(11), 67–76. https://doi.org/10.5815/ijitcs.2018.11.07 (2018).
32. Abdus, S. & Nabil, I. A regression based sensor data prediction technique to analyze data trustworthiness in cyber-physical system. *Int. J. Inf. Eng. Electron. Bus. IJIEEB.* **10**(3), 15–22. https://doi.org/10.5815/ijieeb.2018.03.03 (2018).
33. Hitigala Kaluarachchilage, P. K., Attanayake, C., Rajasooriya, S. & Tsokos, C. P. An Analytical approach to assess and compare the vulnerability risk of operating systems. *Int. J. Comput. Netw. Inf. Secur. IJCNIS.* **12**(2), 1–10. https://doi.org/10.5815/ijcnis.2020.02.01 (2020).
34. Burkhardt, J. Bayesian parameter inference of explosive yields using markov chain Monte Carlo techniques. *Int. J. Math. Sci. Comput. IJMSC.* **6**(2), 1–17. https://doi.org/10.5815/ijmsc.2020.02.01 (2020).
35. Das, S., Roy, K. & Saha, C. K. Establishment of automated technique of FHR baseline and variability detection using CTG: Statistical comparison with expert's analysis. *Int. J. Inf. Eng. Electron. Bus. IJIEEB.* **11**(1), 27–35. https://doi.org/10.5815/ijieeb.2019.01.04 (2019).
36. Anley, M. B. & Tesema, T. B. A collaborative approach to build a KBS for crop selection: Combining experts knowledge and machine learning knowledge discovery. *Int. J. Inf. Eng. Electron. Bus. IJIEEB.* **11**(3), 8–15. https://doi.org/10.5815/ijieeb.2019.03.02 (2019).
37. Alguliyev, R. M., Nabibayova, G. C. & Abdullayeva, S. R. Evaluation of websites by many criteria using the algorithm for pairwise comparison of alternatives. *Int. J. Intell. Syst. Appl. IJISA.* **12**(6), 64–74. https://doi.org/10.5815/ijisa.2020.06.05 (2020).
38. Zagane, M. & Abdi, M. K. Evaluating and comparing size, complexity and coupling metrics as web applications vulnerabilities predictors. *Int. J. Inf. Technol. Comput. Sci. IJITCS.* **11**(7), 35–42. https://doi.org/10.5815/ijitcs.2019.07.05 (2019).
39. Ndichu, S., McOyowo, S., Okoyo, H. & Wekesa, C. A domains approach to remote access logical vulnerabilities classification. *Int. J. Comput. Netw. Inf. Secur. IJCNIS.* **11**(11), 36–45. https://doi.org/10.5815/ijcnis.2019.11.05 (2019).
40. Baako, I. & Umar, S. An integrated vulnerability assessment of electronic commerce websites. *Int. J. Inf. Eng. Electron. Bus. IJIEEB.* **12**(5), 24–32. https://doi.org/10.5815/ijieeb.2020.05.03 (2020).

Acknowledgements
The authors would like to thank the reviewers for the correct and concise recommendations that help present the materials better. We would also like to thank the Armed Forces of Ukraine for providing security to perform this work. This work has become possible only because of the resilience and courage of the Ukrainian Army.

Author contributions
V.K.: Concept, design, analysis, writing—review and editing. I.I.: Concept, design, analysis, writing—review and editing. M.G.: Concept, design, analysis, writing—review and editing.

Funding
The National Research Foundation of Ukraine funded this research under the project "Neural network models, methods and tools for high-speed IoT data processing in information systems of the critical application".

Competing interests
The authors declare no competing interests.

Additional information
Correspondence and requests for materials should be addressed to I.I.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.