scientific reports

Check for updates

OPEN

Reliability model of the security subsystem countering to the impact of typed cyber-physical attacks

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

The article's main contribution is the description of the process of the security subsystem countering the impact of typed cyber-physical attacks as a model of end states in continuous time. The input parameters of the model are the flow intensities of typed cyber-physical attacks, the flow intensities of possible cyber-immune reactions, and the set of probabilities of neutralization of cyber-physical attacks. The set of admissible states of the info-communication system is described taking into account possible variants of the development of the modeled process. The initial parameters of the model are the probabilities of the studied system in the appropriate states at a particular moment. The dynamics of the info-communication system's life cycle are embodied in the form of a matrix of transient probabilities. The mentioned matrix connects the initial parameters in the form of a system of Chapman's equations. The article presents a computationally efficient concept based on Gershgorin's theorems to solve such a system of equations with given initiating values. Based on the presented scientific results, the article proposes the concept of calculating the time to failure as an indicator of the reliability of the info-communication system operating under the probable impact of typical cyber-physical attacks. The adequacy of the model and concepts presented in the article is proved by comparing a statically representative amount of empirical and simulated data. We emphasize that the main contribution of the research is the description of the process of the security subsystem countering the impact of typed cyber-physical attacks as a model of end states in continuous time. Based on the created model, the concept of computationally efficient solution of Chapman's equation system based on Gershgorin's theorems and calculating time to failure as an indicator of the reliability of the info-communication system operating under the probable impact of typed cyber-physical attacks are formalized. These models and concepts are the highlights of the research.

A Cyber-Physical Attack (CPA) is an intentional or unintentional impact on the computing or communication infrastructure of the target system that causes a failure in the control of sensors or actuators. A CPA often exploits vulnerabilities in computing or communication components of relevant systems. For example, suppose an attacker manages to gain control over automated elements of municipal infrastructure, medical implants, and self-driving vehicles. In that case, he can cause damage to the physical dimension from the information dimension, endangering both material values and human lives. Today's society is so dependent on computer and network systems that CPAs are now considered a key threat to critical national infrastructures and a real threat to ordinary citizens[1–6].

The success of a CPA guarantees previous research aimed at identifying active vulnerabilities and relevant entry points into the target process. To assess the scale of the problem, we list only potential entry points[7–9]:

- radio communication between Remote Terminal Units (RTUs) / programmable logic controllers (PLCs) and sensors/actuators / Supervisory Control And Data Acquisition (SCADA) servers;
- control network formed by SCADA servers and operator workstations;

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

- communication gateway/channel between the control system and the corporate network (for example, the switching point between the primary and secondary archivers);
- corporate networks;
- Internet and corporate networks of partners;
- Wi-Fi network and related network equipment
- mobile and desktop service applications for the control of the appropriate process.

Paradoxically, although Cyber-Physical Systems' (CPS) system and application software is not intended for general use, there are no specialized "cyber-physical" security mechanisms. Universal tools are used[10–13]: authentication, access control, firewall, antivirus software, application/thread safelists, cryptography, and integrity control. In addition, this is even though the priority for CPSs is integrity and availability, rather than confidentiality (as for general-purpose computer systems). The latter fact necessitates a radically specific approach to forming security policy for CPSs. However, while teams of cyber-security experts are addressing this issue, the ***urgent task*** is to assess the reliability of existing CPSs, which is ensured by the ability of existing protection mechanisms to counter current types of CPAs.

Reliability theory[14–19] is a powerful, constantly evolving branch of theoretical science. The basic mathematical apparatus underlying it includes the provisions of probability theory and mathematical statistics, random process theory, queuing theory, mathematical logic, graph theory, optimization theory, and so on.

These methodologies form a toolkit for analyzing the performance of the studied information systems for a finite censored period. The analysis takes place in the context of determining:

1. The time between failures in the studied system;
2. The number of failures in the studied system for the censored period of its operation;
3. The reaction of the studied system to the provoked failures;
4. The response of the studied system to complex test effects.

Models[6–9] are focused on the description of the first performance indicator. They are based on the mathematical apparatus of time series analysis. Their purpose is to identify the parameters of the statistical distribution, which best describes the period between failures in the operation of the studied system. The adequacy of such models is determined by the representativeness of the data sample that characterizes the studied system's operation. When formalizing such models, only the fact of failure is taken into account without analyzing the causes of its occurrence and possible consequences.

Models[10–13] are focused on the description of the second performance indicator. It is assumed that a particular distribution law (most often Poisson's) with a continuous or discrete intensity function describes the stochastic parameter, which characterizes the number of time failures. The latter is determined by the results of static analysis of operational data. The disadvantages of this type of model are similar to those mentioned above.

Models[14–17] are focused on the description of the third performance indicator. The data for analysis in these models are:

- the number of failures in the studied system for the censored period, which was caused by unknown negative impacts;
- the number of failures in the operation of the studied system during the censored period, which was caused by negative impacts, and the mechanisms of counter-action which were embedded in the studied system at the stage of its design.

Data analysis is carried out by combinatorics and maximum likelihood methods. Such models are more informative but are still based on information, some of which were collected because of uncontrolled experiments.

Models[18–22] are focused on the description of the fourth performance indicator based solely on the results of controlled experiments. Considering that the causes of failures are usually interrelated, models of this type are based on the mathematical apparatus of Markov chains. It allows considered the multithreading in the operation of the studied system and the heterogeneity of the process of its recovery after a failure. Semi-Markov models more accurately describe the behavior of real information systems because the process of recovery of the first ones after failures can be characterized not only by the exponential distribution functions. The structural features of the studied system in this modeling approach can be considered in the graph of the flow of control, which brings the model closer to the described process. This qualitatively distinguishes the Markov approach from, for example, a nonparametric neural network[23,24], in which the structural features of the studied system are ignored.

A notable element of the methodological apparatus of the reliability theory, particularly info-communication systems, is the structural-logical method[20–23]. The method describes the studied system as a topology of interacting elements (devices, software services, operators), the set of which uniquely identifies the original studied object. Analytically, the relationships in the topology are characterized by the corresponding functions of the algebra of logic. The same functions in the transition to probabilistic or deterministic structural-logical models become the basis for formalizing the criteria for identifying the set of states of the studied system. Quantitative indicators of reliability based on the structural-logical model of the studied system are determined by replacing the minimum disjunctive normal form of logical functions with probabilistic or deterministic characteristics with a simultaneous transition from logical to arithmetic operations on them.

Graphical interpretation of structural-logical models is the corresponding schemes of functional integrity[22–25], depicted in the form of block diagrams, trees of faults or (and) events, the "bow-tie" techniques, and so on. An

algebra of groups of incompatible events in the paradigm of the general logical-probabilistic method[20,23,24,26] has been developed to remove the binary constraint (the stay of the model element in only one of two defined states), characteristic of structural-logical models. Note also that the fault tree analysis method is the basis for forming dynamic fault trees (have a wide range of logical operators) or generalized fault trees (possible further conversion to Bayesian networks, Petri nets, etc.) However, these add-ons are not used in practice due to their excessive complexity in implementing and interpreting the initial results. But, in the authors' opinion, the analysis of generalized fault trees seems promising due to the possibility of their direct integration with certain methods of machine learning.

However, the authors consider that the mathematical apparatus of Markov chains[23,24,27–31] is optimal for analyzing the reliability of CPSs taking into account their infrastructural and operational features[1–9]. Close analogs are the reliability models of information systems described in articles[24,27,29–31], formalized based on discrete Markov chains. These models represent the info-communication system as a system with failures and recoveries. The strength of the mentioned research is the mathematically correct stochastic characteristic of the states of the studied system and the analytically determined functional connection of the assessment of the reliability of the studied system with the relaxation time of the Markov chain. However, the apparent theoretical orientation of the scientific results presented in these articles is limited to their application. Also, the finite parametric space used in these investigations characterizes the studied processes in terms of probability theory and mathematical statistics rather than the theory of reliability. Finally, describing the studied process in discrete time presented in the mentioned articles introduces inaccuracy in assessing the reliability indicators.

Given the strengths and weaknesses of these analogs, we formulate the necessary attributes of our scientific research.

The ***research object*** is the process of the security subsystem of the info-communication system countering the impact of typed CPAs.

The ***research subject*** is the provisions of the theory of Markov processes, the theory of differential equations, the theory of probability and mathematical statistics, and the theory of experimental planning.

The ***aim*** of the research is the analytical formalization of estimating the reliability of the info-communication system on the model of the security subsystem, countering the impact of typed CPAs.

The ***objectives*** of the research are

1. The analytical formalization of the process of the security subsystem countering the impact of typed CPAs as a Markov chain in continuous time;
2. The analytical formalization of the computationally efficient concept of calculating the probabilities of realization of states in which the studied info-communication system can be at any moment;
3. The analytical formalization of the concept of calculating the time to failure as an indicator of the reliability of the info-communication system, operating under conditions of the probable impact of typified CPAs;
4. Proving the adequacy and demonstration of the functionality of the created mathematical apparatus.

The ***main contribution*** of the research is the description of the process of the security subsystem countering the impact of typed CPAs as a model of end states in continuous time. Based on the created model, the concept of computationally efficient solution of Chapman's equation system based on Gershgorin's theorems and calculating time to failure as an indicator of the reliability of the info-communication system operating under the probable impact of typed CPAs are formalized. These models and concepts are the ***highlights*** of the research.

Models and methods

Research statement and the proposed model. Consider the process of functioning of the info-communication system, which is potentially vulnerable to n CPAs. In general, the ability to counter CPAs is determined by the reliability of the target system, which is provided by the architecture and settings of its security subsystem. We formalize a mathematical model that allows us to quantify the process of the security subsystem confrontation to the impact of the typed CPAs.

Let the sequence of occurrence of an arbitrary i-th CPA be described by a Poisson flow of events with intensity λ_i. The oncoming Poisson flow of the cyber-immune reaction is characterized by the intensity μ_i and the probability of neutralization of the i-th CPA r_i. When $i \in \overline{1,n}$ the input parameters of the model are ordered in the form of:

- the set of intensities of CPAs $\Lambda = \{\overline{\lambda_1, \lambda_n}\}, \lambda_i \geq 0$;
- the set of intensities of cyber-immune reactions $\mathrm{M} = \{\overline{\mu_1, \mu_n}\}, \mu_i \geq 0$;
- the set of probabilities of neutralizing the corresponding CPAs $R = \{\overline{r_1, r_n}\}, 0 \leq r_i \leq 1$.

The functioning of the CPS in potentially aggressive conditions will be presented in terms of the finite state model. Let us denote by s_0 the serviceable state in which the system is, on which no CPA is carried out. The antagonist of the serviceable state will be the state of failure s_{n+1} in which the system is, on which the CPA was not successful. Intermediate between these polar states will be the states of confrontation s_i. The system is in a state of confrontation s_i when it is under the CPA of i-th type. The duration of the state of confrontation s_i is a stochastic quantity with a Poisson distribution with parameter μ_i. Depending on the result of the cyber-immune reaction, the system from the state of confrontation s_i either with the probability r_i transits to the serviceable state s_0 or with the probability $(1 - r_i)$ transits to the state of failure s_{n+1}. Assume that the model characterizes

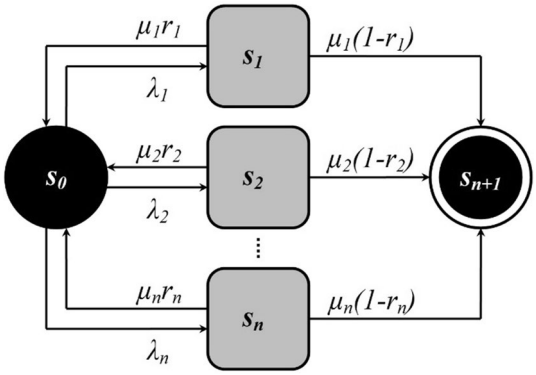

Figure 1. UML-state diagram of the model of the studied process.

the functioning of the security subsystem of the CPS of critical use, the transition of which into a state of failure marks the end of the life cycle (return to the serviceable state is impossible).

The described model of finite states is represented in graphical form by a UML state diagram (see Fig. 1).

The probability that the studied cyber*physical system at a time t is in the state s_i is denoted as $p_i(t)$, $i \in \overline{\{0, n+1\}}$. These probabilities can be determined in general by solving a system of ordinary differential equations known as Chapman's equations[32,33]. We specify the analytical form of these equations for the model of the studied process, presented graphically in Fig. 1. We obtain:

$$\begin{aligned} \frac{dp_0(t)}{dt} &= -\lambda_0 p_0(t) + \sum_{j=1}^{n} \mu_j r_j p_j(t), \\ \frac{dp_i(t)}{dt} &= \lambda_i p_0(t) - \mu_i p_i(t), \quad i = \overline{1, n}, \\ \frac{dp_{n+1}(t)}{dt} &= \sum_{j=1}^{n} \mu_j (1 - r_j) p_j(t), \end{aligned} \tag{1}$$

where $\lambda_0 = \sum_{i=1}^{n} \lambda_i$.

The probabilities $p_i(t)$ can be unambiguously determined based on the system of Eq. (1) only by setting their initiating values. Let

$$p_0(0) = 1, \quad p_j(0) = 0, \quad j = \overline{1, n+1}, \tag{2}$$

i.e. at the time, $t = 0$ the CPS is in a serviceable state.

For compactness, we present a system of Eq. (1) in matrix form:

$$\frac{d\mathrm{p}(t)}{dt} = \Pi \cdot \mathrm{p}(t), \tag{3}$$

where $\mathrm{p}(t) = \{p_0(t), p_1(t), \ldots, p_{n+1}(t)\}$ is the set of probabilities of realization of the corresponding state for the studied system, and Π is a square matrix of probabilities of transitions of dimension $(n+2) \times (n+2)$, the sum of the elements of each row of which is zero:

$$\Pi = \begin{pmatrix} -\lambda_0 & \lambda_1 & \lambda_2 & \ldots & \lambda_m & 0 \\ \mu_1 r_1 & -\mu_1 & 0 & \ldots & 0 & \mu_1(1-r_1) \\ \mu_2 r_2 & 0 & -\mu_2 & \ldots & 0 & \mu_2(1-r_2) \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ \mu_n r_n & 0 & 0 & \ldots & -\mu_n & \mu_n(1-r_n) \\ 0 & 0 & 0 & \ldots & 0 & 0 \end{pmatrix}. \tag{4}$$

Thus, we presented the process of the security subsystem confronting the typed CPAs in the form of a Markov chain in continuous time, which connects the set of input data $\langle \Lambda, \mathrm{M}, R \rangle$ with the system of Chapman's Eq. (1) using a matrix (4) taking into account the initiating values (2). The initial parameters of the model are the set of probabilities of realization of the corresponding states for the studied system in the form (3).

The concept of solving the Chapman equation system for the model of the studied process. In general, the solution of the system of Eq. (1), taking into account the initiating values (2), is relatively non-trivial. However, the description based on the proposed model of individual situations, typical for the life cycle of the CPS, may be the preamble, the existence of which will facilitate the further perception of readers of the material in this section.

Based on the model (1), we describe the CPS's situation in a serviceable state s_0. In this situation: $\lambda_i = 0 \forall i \in \{\overline{1,n}\}$. Under such conditions, the solution of the Cauchy problem for the system of Eq. (1) can be represented as $p_0(t) = 1$, $p_j(t) = 0$, $j = \overline{1,n+1}$. The resulting solution illustrates the obvious fact—if no CPA is carried out on the system, the last one is in the serviceable state.

An antagonist is when the security subsystem lacks a specialized protective mechanism to counter a typified CPA. Let's assume that $r_i = 0 \forall i$. If no parameter μ_i coincides with λ_0, then we can analytically define the solutions of the corresponding first-order Kolmogorov Eq. (1), which describe the state graph shown in Fig. 1, in the form of such expressions:

$$\begin{aligned} p_0(t) &= \exp(-\lambda_0 t), \\ p_i(t) &= \frac{\lambda_i}{\lambda_0 - \mu_i}\left(\exp(-\mu_i t) - \exp(-\lambda_0 t)\right), \quad i = \overline{1,n}, \\ p_{n+1}(t) &= 1 - \exp(-\lambda_0 t) - \sum_{i=1}^{n} \frac{\lambda_i}{\lambda_0 - \mu_i}\left(\exp(-\mu_i t) - \exp(-\lambda_0 t)\right). \end{aligned}$$

The resulting expressions are formulated for the initial conditions defined in the form (2). From the obtained solution, it is seen that if the protective mechanism such as CPA does not match, the probability of the studied system in the serviceable state decreases exponentially, and the probability of its transition to the failure state s_{n+1}, on the contrary, increases towards one.

We now turn to solve the system of Eq. (1). Laplace transforms are usually used to solve the system of Chapman's equations with constant coefficients. We managed to propose a computationally efficient method based on the use of eigenvectors and eigenvalues of the transition probability matrix (4). Let's substantiate this thesis.

Prove that all real numbers of the matrix (4) belong to the interval $[-2\gamma, 0]$, where $\gamma = \max\{\mu_1, \mu_2, \ldots, \mu_n, \lambda_0\}$. The results presented in[34] confirm that the eigenvalues of the matrix of the form (4) belong to the set of real numbers. Our statement about the interval $[-2\gamma, 0]$ is based on Gershgorin's theorems[34,35]. Indeed, on their basis, it can be stated that all eigenvalues of the matrix (4) belong to the interval formed by combining the corresponding segments:

$$[-2\mu_1, 0] \cup [-2\mu_2, 0] \cup \ldots \cup [-2\mu_n, 0] \cup [-2\lambda_0, 0]. \tag{5}$$

From expression (5) it follows that each eigenvalue of the matrix (4) will belong to the segment $[-2\gamma, 0]$, where $\gamma = \max\{\mu_1, \mu_2, \ldots, \mu_n, \lambda_0\}$. Moreover, the matrix (4) always has a zero eigenvalue $\sigma_0 = 0$, because it has a zero string.

Based on expression (5), we define the spectrum of the matrix (4) as

$$spec(\Pi) = \{\sigma_0 = 0, -|\sigma_1|, -|\sigma_2|, \ldots, -|\sigma_{n+1}|\}, \tag{6}$$

where $\sigma_1, \sigma_2, \ldots, \sigma_{n+1}$ are negative real numbers. Next, we consider the spectrum (6) simple.

From the general theory of differential equations adapted to Chapman's system of equations, it is known that system (3) has $n+2$ linear independent solutions of the form

$$\mathrm{p}_0(t) = \mathrm{c}_0, \quad \mathrm{p}_1(t) = \mathrm{c}_1 \exp(\sigma_1 t), \quad \mathrm{p}_2(t) = \mathrm{c}_2 \exp(\sigma_2 t), \ldots, \mathrm{p}_{n+1}(t) = \mathrm{c}_{n+1} \exp(\sigma_{n+1} t),$$

where c_l is the left eigenvector of the matrix (4), which corresponds to the eigenvalue σ_l, $l = \overline{0,n+1}$.

Let's choose eigenvectors c_l so that the condition

$$\sum_{l=0}^{n+1} \mathrm{c}_l = \vec{\mathrm{e}} \tag{7}$$

is satisfied, where $\vec{\mathrm{e}}$ is the vector with $n+2$ elements of the form $(1, 0, \ldots, 0)$. Then the solution of the system of Chapman's equations of the form (1) with the initiating values (2) can be analytically expressed as

$$\begin{aligned} \mathrm{p}(t) = \sum_{l=0}^{n+1} \mathrm{c}_l \exp(\sigma_l t) &= \mathrm{c}_0 + \mathrm{c}_1 \exp(\sigma_1 t) \\ &+ \mathrm{c}_2 \exp(\sigma_2 t) + \cdots + \mathrm{c}_{n+1} \exp(\sigma_{n+1} t). \end{aligned} \tag{8}$$

Rewrite expression (8) as follows:

$$p_i(t) = \delta_{i,n+1} + \sum_{l=1}^{n+1} c_{l,i} \exp(\sigma_l t), \quad i = \overline{0,n+1}, \tag{9}$$

where δ is a Kronecker symbol, $c_{l,i}$ is the i-th element of the eigenvector c_l. Also, when formalizing expression (9), we took into account the fact that the eigenvector c_0 of length $n+2$, which corresponds to the eigenvalue $\sigma_0 = 0$, is defined as $(0, \ldots, 0, 1)$.

Initial values (2) can also be represented in terms of eigenvectors. Assuming $\mathrm{c}_l = (c_{l,i})$, we write:

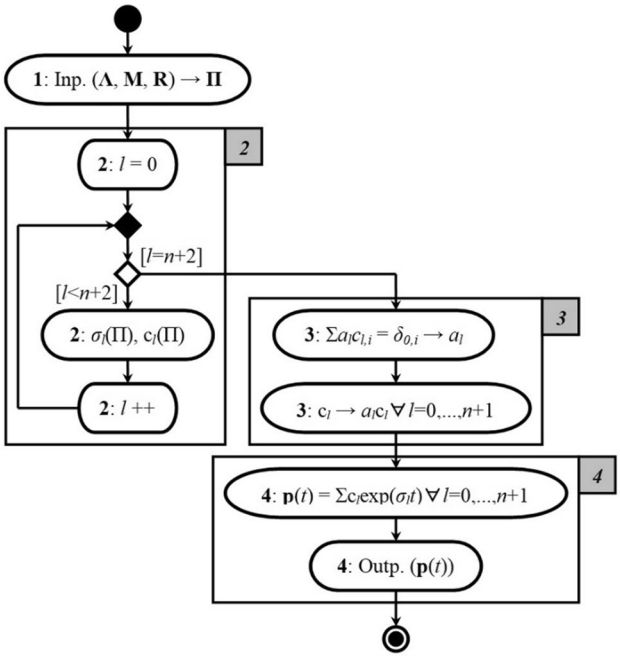

Figure 2. UML-activity diagram of the concept of solving the Chapman equation system for the model of the studied process.

$$\sum_{l=1}^{n+1} c_{l,i} = \delta_{0,i} - \delta_{n+1,i}, \quad i = \overline{0, n+1}. \tag{10}$$

The process of obtaining solutions of the Chapman ефіл of the form (1) with the initiating values (2) in the form of expression (9) can be easily generalized in the form of the UML-activity diagram presented in Fig. 2.

Let's comment on the stages presented in Fig. 2 computational process:

1. For the corresponding input parameters $\{\Lambda, M, R\}$ of the model (1), (2) we form a matrix of probabilities of transitions Π of the form (4);
2. We calculate the eigenvalues σ_l and the eigenvectors $c_l = (c_{l,i})$ of the matrix Π, $l = \overline{0, n+1}$;
3. Solve the system of linear homogeneous equations $\sum_{l=0}^{n+1} a_l c_{l,i} = \delta_{0,i}$ concerning the unknown a_l and replace $c_l \to a_l c_l \forall l = \overline{0, n+1}$;
4. According to expression (8) we obtain a formatted solution of the Cauchy problem for the system of Chapman's Eq. (1) with initiating values (2).

Method of calculating indicators of reliability of the studied system taking into account the specifics of the process of its exploitation. Stochastic modeling is an effective tool that complements the process of rigorous analytical evaluation of the pool of quantitative characteristics (indicators) of reliability of the studied system, which, in the event of potential CPAs, is provided by the security subsystem.

Perhaps the most important and easy to interpret is such a reliability indicator as a time to failure (*TTF*). In the context of the mathematical model formulated in section "Research statement and the proposed model", we define this indicator as the amount of time $T \in [0, \infty)$ from the start of exploitation of the studied system ($t = 0$, the system is in the serviceable state s_0) to the moment $t = T$ its transition to the state of failure s_{n+1} due to the successful CPA of any type.

We formally analyze the process of estimation of this indicator based on the Markov model of the security subsystem confrontation to the impact of typed CPAs. The indicator T is a continuous stochastic quantity. Define for a random stochastic quantity T the function and the density of the distribution as $F_T(t)$ and $f_T(t)$, respectively. The value of the function $F_T(t)$ at time t characterizes the probability that the value T will be less than or equal to t: $F_T(t) = P(T \le t)$, or (equivalently)—the probability that the studied system at a time t is in a state of failure s_{n+1}: $F_T(T) = p_{n+1}(t)$.

Since the function $F_T(t)$ is differentiated, equality $f_T(t) = F'_T(t)$ holds. Therefore, we can write $f_T(t) = p'_{n+1}(t)$. Considering expression (9), the last expression for $f_T(t)$ can be rewritten as

$$f_T(T) = \sum_{l=1}^{n+1} c_{l,n} \sigma_l \exp(\sigma_l t). \tag{11}$$

If we take into account expression (11) in condition (10), we obtain the rationing condition:

$$\int_0^\infty f_T(t)dt = \sum_{l=1}^{n+1} c_{l,n+1}\sigma_l \int_0^\infty \exp(\sigma_l t)dt$$
$$= \sum_{l=1}^{n+1} c_{l,n+1}\sigma_l \frac{1}{\sigma_l} = \sum_{l=1}^{n+1} c_{l,n+1} = 1.$$

We present the process of calculating the k-first moments of the stochastic quantity T in terms of eigenvalues and eigenvectors of the matrix of transition probabilities (4). Interpret expressions (9) and (11) in the context of the definition of k-first moment:

$$\mu_k[T] = \int_0^\infty t^k f_T(t)dt = \sum_{l=1}^{n+1} c_{l,n+1}\sigma_l \int_0^\infty t^k \exp(\sigma_l t)dt, \tag{12}$$

where $c_{l,n+1}$ is the $(n+1)$-th element of the eigenvector c_l of the matrix Π, equivalent to the eigenvalue σ_l.

Since $\sigma_l < 0 \forall l = \overline{1, n+1}$ the integrals in the right part of the expression (12) coincide:

$$\int_0^\infty t^k \exp(\sigma_l t)dt = \frac{k!}{|\sigma_l|^{k+1}}. \tag{13}$$

Substitute expression (13) into expression (12). The result is:

$$\mu_k[T] = -\sum_{l=1}^{n+1} \frac{c_{l,n+1}}{|\sigma_l|^k}, \tag{14}$$

In particular, based on expression (14), we define the mathematical expectation of the stochastic quantity T (or the time to the failure of the studied system) as

$$\tau = \mu_1[T] = \sum_{l=1}^{n+1} \frac{c_{l,n+1}}{\sigma_l}. \tag{15}$$

Undoubtedly, the time to the failure of the studied system is a fundamental indicator of its reliability, provided by the security subsystem. Assessing the value of this indicator at the design stage of the latter will allow us to plan the number of funds for cyber-security measures adequately.

Using expression (15), we describe a fundamentally critical situation for the security subsystem when the latter lacks a protective mechanism to neutralize a certain CPA (equivalent situation—the security subsystem is disabled/absent).

In this situation, we have $r_i = 0 \forall i \in \{\overline{1, n}\}$. Accordingly, the eigenvalues of the matrix Π will be equal to $\sigma_0 = 0, \sigma_1 = -\mu_1, \ldots, \sigma_n = -\mu_n, \sigma_{n+1} = -\lambda_0$. Determine the analytically corresponding eigenvectors c_l, $l = \overline{0, n+1}$, that satisfy condition (7):

$$\mathrm{c}_0 = (0, 0, \ldots, 0, 1),$$
$$\mathrm{c}_1 = \left(0, \frac{\lambda_1}{\lambda_0 - \mu_1}, 0, \ldots, 0, -\frac{\lambda_1}{\lambda_0 - \mu_1}\right),$$
$$\mathrm{c}_2 = \left(0, 0, \frac{\lambda_2}{\lambda_0 - \mu_2}, 0, \ldots, 0, -\frac{\lambda_2}{\lambda_0 - \mu_2}\right),$$
$$\ldots$$
$$\mathrm{c}_n = \left(0, \ldots, 0, \frac{\lambda_n}{\lambda_0 - \mu_n}, -\frac{\lambda_n}{\lambda_0 - \mu_n}\right),$$
$$\mathrm{c}_{n+1} = \left(1, -\frac{\lambda_1}{\lambda_0 - \mu_1}, -\frac{\lambda_2}{\lambda_0 - \mu_2}, \ldots, -\frac{\lambda_n}{\lambda_0 - \mu_n}, -1 + \sum_{j=1}^{n} \frac{\lambda_j}{\lambda_0 - \mu_j}\right).$$

The defined set $\{\Sigma = (\sigma_0, \sigma_1, \ldots, \sigma_{n+1}), \mathrm{C} = (\mathrm{c}_0, \mathrm{c}_1, \ldots, \mathrm{c}_{n+1})\}$ allows us to formulate the desired expression for calculating the indicator τ based on expression (15):

$$\tau = \mu_1[T] = \frac{1}{\lambda_0}\left(1 + \sum_{i=1}^{n} \frac{\lambda_i}{\mu_i}\right). \tag{16}$$

Assume that $n = 1$. Then, based on expression (16), we obtain $\tau = \lambda_1^{-1} + \mu_1^{-1}$, i.e., the average time to failure of the studied system τ is formed by the sum of the average time to CPA λ_1^{-1} and the average time of its implementation μ_1^{-1}.

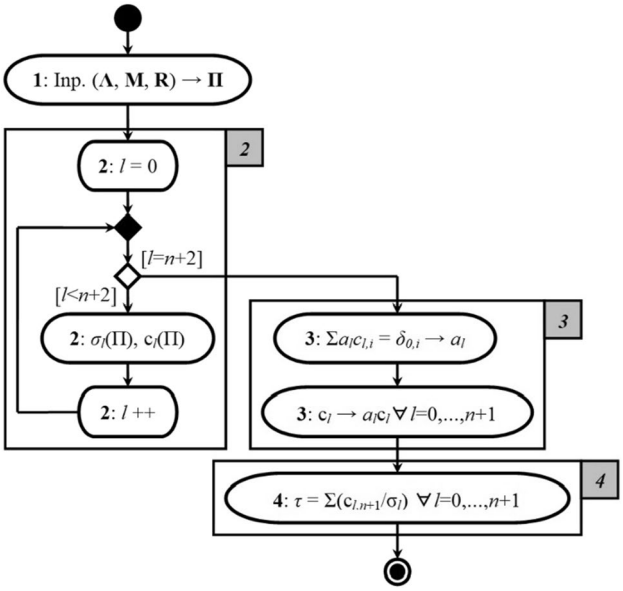

Figure 3. UML-activity diagram of the concept of calculating the time to failure of the studied system.

We summarize the proposed concept of calculating the time to failure as an indicator of the reliability of the studied system in the form of a UML-activity diagram, presented in Fig. 3.

Let's comment on the stages presented in Fig. 3 computational process:

1. For the corresponding input parameters $\{\Lambda, \mathrm{M}, R\}$ of the model (1), (2) we form a matrix of probabilities of transitions Π of the form (4);
2. We calculate the eigenvalues σ_l and the eigenvectors $\mathrm{c}_l = \left(c_{l,i}\right)$ of the matrix Π, $l = \overline{0, n+1}$;
3. Solve the system of linear homogeneous equations $\sum_{l=0}^{n+1} a_l c_{l,i} = \delta_{0,i}$ concerning the unknown a_l and replace $c_l \to a_l c_l \forall l = \overline{0, n+1}$;
4. According to expression (15), we calculate the time to failure of the studied system τ.

Experiments

As an example, we use the mathematical apparatus presented in section "Models and methods" to evaluate the reliability indicator of the real CPS of the Situation Center of the Information Technology Department of Vinnytsia City Council (Vinnytsia, Ukraine) (hereinafter—SC system). This info-communication system was put into operation in 2018 and is constantly evolving to improve the implemented services and add new ones. Currently, the SC system manages traffic lights on the roads of Vinnytsia. It maintains the uninterrupted exploitation of the data centre, which stores video streams from more than 1 k video cameras located in the city. Thus, the SC system is, by definition, cyber-physical.

The information collected in the SC system is confidential and available only to authorized employees of the Vinnytsia City Council, the National Police of Ukraine, the Security Service of Ukraine, etc. For these privileged persons to have quick access to the relevant information, a local network was created consisting of data centre servers, communication equipment, workstations, and software (i.e. SCADA). In normal exploitation, this LAN is not isolated from the Internet. 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, management systems, web interface—all these components are located on dedicated servers.

We describe the situation when attackers carry out a CPA on the SC system. Attackers seek information about network architecture, workstations, servers, operating systems, user accounts, etc. Analysis of this information can potentially identify hardware and software vulnerabilities, some of which may not fall within the scope of control of the protective mechanisms of the security subsystem. In the realities of modern cyberspace, exploits are often created based on data collected as a result of:λ_1 (Apache): analysis of internal and outgoing network traffic, remote access support mechanism; λ_2: buffer overflow; λ_3: SQL injection. Analysis of the logs of the SC system revealed the following categorized vulnerabilities: λ_1: (a) CVE-2019-9511, (b) CVE-2015-5206, (c) CVE-2019-9512, (d) CVE-2020-9481, (e) CVE-2020-17509; λ_2: (a) CVE-2008-0127, (b) CVE-2007-6593, (c) CVE-2021-36301, (d) CVE-2019-18805, (e) CVE-2017-6745; λ_3: (a) CVE-2021-45253, (b) CVE-2022-22055, (c) CVE-2021-45814, (d) 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 the Vinnytsia City Council administration, further in the set $\Lambda = \{\lambda_1, \lambda_2, \lambda_3\}$ is not taken into account the entire list of vulnerabilities identified as a result of the analysis of logs of the SC system. However, these data are sufficient to demonstrate the functionality and prove the adequacy of the mathematical apparatus presented in section "Models and methods".

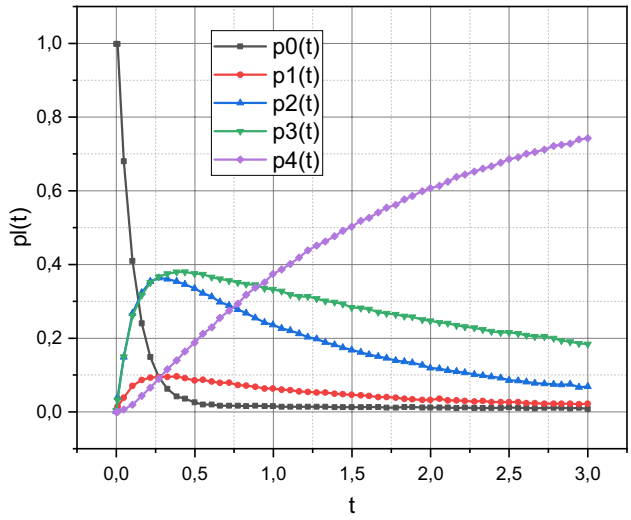

Figure 4. Dependences $p_l(t), l = \overline{0,4}$, at $t \in [0,3]$, calculated for the SC system using the concept presented in section "The concept of solving the Chapman equation system for the model of the studied process".

Analysis of the logs of the SC system for the period from 01.09.2021 to 16.09.2021 (15 full days) in the context of detecting cases of CPAs described in the set Λ, allowed us to determine the following input data for modeling:

$$\begin{aligned} &n = 3, \quad \Lambda = (4.27, 3.96, 1.12), \\ &\mathrm{M} = (0.91, 0.41, 0.94), \quad R = (0.09, 0.39, 0.0.37). \end{aligned} \tag{17}$$

Accordingly, the matrix Π will look like this:

$$\Pi = \begin{pmatrix} -9.381 & 4.27 & 3.96 & 1.12 & 0 \\ 0.093 & -0.91 & 0 & 0 & 0.827 \\ 0.169 & 0 & -0.41 & 0 & 0.251 \\ 0.362 & 0 & 0 & -0.94 & 0.588 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

The spectrum (6) for this matrix will look like

$$spec(\Pi) = \{0, -9.5461, -0.9373, -0.8528, -0.3334\}.$$

Applying the condition of normalization (7) of the form $\sum_{l=0}^{4} c_l = (1,0,0,0,0)$ to the eigenvectors $\mathrm{c_l}, l = \overline{0,4}$, of the matrix Π we obtain:

$$\begin{aligned} \mathrm{c}_0 &= (0,0,0,0,1); \\ \mathrm{c}_1 &= (0.982, -0.487, -0.427, -0.129, 0.062); \\ \mathrm{c}_2 &= (0.001, -0.064, -0.002, 0.023, 0.042); \\ \mathrm{c}_3 &= (0.007, 0.472, -0.068, 0.086, -0.497); \\ \mathrm{c}_4 &= (0.011, 0.079, 0.497, 0.020, -0.606). \end{aligned}$$

According to expression (8) we obtain a formatted solution of the Cauchy problem for the above system of Chapman's equations and initiating values:

$$\begin{aligned} p_0(t) &= 0.982e^{-9.546t} + 0.001e^{-0.937t} + 0.007e^{-0.853t} + 0.011e^{-0.334t} \\ p_1(t) &= -0.487e^{-9.456t} - 0.064e^{-0.937t} + 0.472e^{-0.853t} + 0.079e^{-0.334t} \\ p_2(t) &= -0.427e^{-9.456t} - 0.002e^{-0.937t} - 0.068e^{-0.853t} + 0.497e^{-0.334t} \\ p_3(t) &= -0.129e^{-9.456t} + 0.023e^{-0.937t} + 0.086e^{-0.853t} + 0.020e^{-0.334t} \\ p_4(t) &= 1 + 0.062e^{-9.456t} + 0.042e^{-0.937t} - 0.497e^{-0.853t} + 0.606e^{-0.334t} \end{aligned}$$

Below, in Fig. 4, the dependences of the probabilities $p_0(t) \div p_4(t)$ at $t \in [0,3]$ are visualized.

Now calculate the value of the time to failure s for the SC system. Since we have already given the results of the calculation of eigenvalues and eigenvectors of the matrix Π, which represents the model of the operation of the SC system, we can immediately apply the concept described in section "Method of calculating indicators of reliability of the studied system taking into account the specifics of the process of its exploitation", summarized by expression (15):

$$\tau = \frac{0.062}{-9.546} + \frac{0.042}{-0.937} + \frac{-0.497}{-0.853} + \frac{-0.606}{-0.334} = 2.350.$$

Assuming that all elements of the set R are zero (protective mechanisms are completely helpless against the types of CPAs carried out on the SC system), then using expression (16) we can estimate the value of time to failure for the SC system:

$$\tau_{\min} \equiv \tau|_{R=0} = 1.737.$$

As expected, $\tau > \tau_{\min}$. The use of existing protective mechanisms (the effectiveness of which to counteract CPAs generalized by the set Λ is represented by the values of the elements of the set R) allows extending the time to failure for the SC system by 35% relative to the estimated value of $\tau_{\min}$.

Thus, the concepts proposed in sections "The concept of solving the Chapman equation system for the model of the studied process" and "Method of calculating indicators of reliability of the studied system taking into account the specifics of the process of its exploitation", based on the model presented in section "Research statement and the proposed model", allow to visually, quantitatively, and computationally effectively characterize the reliability of a real CPS, considering the development of the process of the security subsystem countering to the impact of typed CPAs.

However, we still do not pay enough attention to the issue of proving the adequacy of the mathematical model of the security subsystem, countering the impact of typed CPAs presented in section "Research statement and the proposed model". Let's fix this shortcoming.

We will compare the obtained empirical results for the SC system with simulation modeling results. To implement the simulation model, a specialized software MathWorks MATLAB was chosen. The rationale for this choice is that the toolbox functions of this software platform have been tested worldwide, and their adequacy has been empirically proven. Mainly using the Hidden Markov Model Toolbox, we created the following custom functions:

- *MyErlang*(k, λ) is a function that simulates a stochastic quantity with Erlang distribution of the k-th order with a positive parameter λ;
- *MyState*$(X, \Lambda, \mathrm{M}, R, k)$ is a function for realizing the transition of the Markov chain in continuous time to the next state from the current X, which is characterized by a set $\langle \Lambda, \mathrm{M}, R \rangle$, where $\Lambda = \{\overline{\lambda_1, \lambda_n}\}$ is the set of CPAs flow intensities, $\lambda_i \geq 0$; $\mathrm{M} = \{\overline{\mu_1, \mu_n}\}$ is the set of cyber-immune response flow intensities $\mu_i \geq 0$; $R = \{\overline{r_1, r_n}\}$ is the set of CPA neutralization probabilities, $0 \leq r_i \leq 1$;
- *MyTTF*$(\Lambda, \mathrm{M}, R, k)$ is a function for the implementation of a parameterized instance of a Markov chain in continuous time and the recognition for it of the time to failure through the consistent application of the concepts presented in sections "The concept of solving the Chapman equation system for the model of the studied process" and "Method of calculating indicators of reliability of the studied system taking into account the specifics of the process of its exploitation".

Let us focus on the description of the function *MyState*. For a Markov chain, the state X is determined by a pair of parameters (t, m), where t is the time of transition of the system to the state X; $m \in \{\overline{0, n+1}\}$ is the identifier of the state X. The function *MyState* implements the transition of the system from the current state $X = (t, m)$ to the new state $X' = (t', m')$: $X \to X'$. The values of the parameters t' m' are determined depending on the value of the parameter m. If:

- $m = 0$ (the system is in the serviceable state s_0), the function *MyState* generates a set of stochastic quantities $\mathrm{T} = \{\tau_i\}, i = \overline{1, n}$, distributed according to the Poisson distribution law with parameters λ_i, respectively. Let $\tau_j = \min\{\overline{\tau_1, \tau_n}\}$ be for $j \in \{\overline{1, n}\}$, then take $t' = t + \tau_j$ and $m' = m + j$, i.e. $X' = (t + \tau_j, j)$;
- $m \in \{\overline{1, n}\}$ (the system is in a state of counter-action to the m-th CPA s_m), the function *MyState* generates a stochastic quantity τ, distributed according to the Poisson distribution law with the parameter μ_m. We accept $t' = t + \tau$. Using the standard MATLAB function *rand*, we obtain a stochastic number x evenly distributed over the interval $[0, 1]$. If the inequality $r_m > x$ holds, then we accept $m' = 0$, otherwise we accept $m' = n + 1$;
- $m = n + 1$ (the system is in a state of failure s_{n+1}), then the function *MyState* takes $t' = t$ and $m' = m$. Accordingly, $X' = X = (t, m = n + 1)$.

Operating according to the algorithm just described, the function *MyState* allows for a Markov chain in continuous time to implement a sequence of states of the form $X_0 = (t_0 = 0, m_0 = 0) \to X_1 = (t_1, m_1) \to \ldots \to X_M = (t_M, M = n + 1)$. Starting from the state X_0, each implementation is generated by the function *MyTTF*. Transitions $X \to X'$ occur until the implementation goes to the state X_M, $M \in \mathbb{N}$. It is t_M the value returned by the function *MyTTF*. It is the required time to failure of the system due to a successful CPA.

We compare the data calculated using the sequential application of the concepts presented in sections "The concept of solving the Chapman equation system for the model of the studied process" and "Method of calculating indicators of reliability of the studied system taking into account the specifics of the process of its exploitation" on time to failure of the SC system with the results of simulation modeling of the values of this reliability indicator obtained using the author's functions.

We obtained the last values by running the function *MyTTF* with input parameters $\langle \Lambda, \mathrm{M}, R \rangle$ similar to (17). As a result, we obtained a set of 10^3 simulated values of the time to failure for the SC system, which was visualized

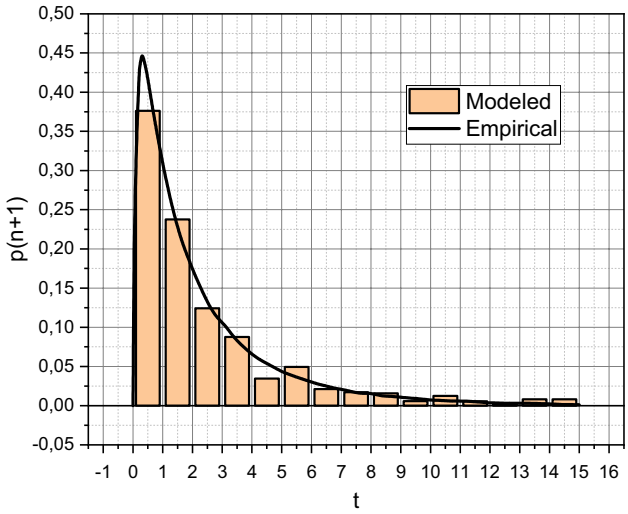

Figure 5. Proving the adequacy of the mathematical apparatus proposed in section "Models and methods".

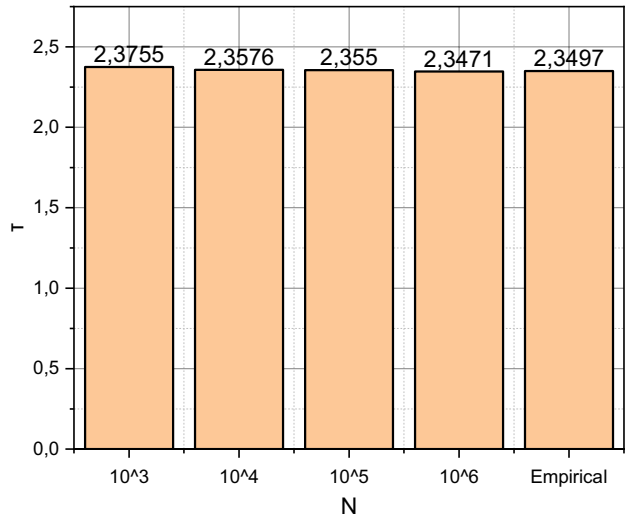

Figure 6. Precise comparison of empirical and simulated estimates of time to failure for the SC system.

in the form of a histogram in Fig. 5. For clarity of comparison, we differentiated the empirically calculated function $p_4(t)$ for the SC system (see the analytical expression before Fig. 4), obtaining an empirical function of the probability density $f_T(T)$ of the form $f_T(t) = -0.587e^{-9.546t} - 0.040e^{-0.937t} + 0.424e^{-0.853t} + 0.202e^{-0.334t}$ The obtained curve $f_T(T)$ is also visualized in Fig. 5.

From those presented in Fig. 5 results, it is obvious that the mathematical apparatus offered in section "Models and methods" is adequate. To further confirm this fact, we obtain estimates of the time to failure of the SC system by consistently generalizing the $N = \left(10^3, 10^4, 10^5, 10^6\right)$ results of statistical tests (starts of the author's function *MyTTF*). The obtained estimates are presented in the form of a diagram in Fig. 6.

Figure 6 shows that $10^5 < N < 10^6$ empirical and simulated estimates of the SC system's time to failure (reliability indicator) coincide with the fourth decimal place.

Discussion

The "cornerstone" of any research that results in a mathematical apparatus is to prove its adequacy. That is why we will start the discussion by analyzing the information presented in Figs. 5 and 6. In the first of them, we can compare the probability density functions of time to failure of the info-communication system of the Situational Center of the Department of Information Technology of Vinnytsia City Council (Vinnytsia, Ukraine), the results of exploitation of which were summarized as data in a set (17). Empirical values were calculated by sequential application of the concepts presented in sections "The concept of solving the Chapman equation system for the model of the studied process" and "Method of calculating indicators of reliability of the studied system taking into account the specifics of the process of its exploitation", which allowed to obtain the shown in Fig. 5 smooth

curve of the transition of the SC system to the state of failure. Showed in Fig. 5 histogram presents the simulation modeling process and summarizes the 10^3 results of controlled experiments with an author's functions *MyTTF*, *MyState* і *MyErlang* implemented based on a priori adequate Hidden Markov Model Toolbox. It should be noted that the empirical and simulated results of estimation of the time to failure for the SC system coincide throughout the time interval of the analysis (for 15 full days). And this is even though the data visualized is characterized by significant nonlinearity, which persists throughout the censored interval of observations. Slight fluctuations of the simulated value relative to the empirical one in the general trend indicate a lack of accuracy in simulation modeling. This thesis is fully confirmed by the research results presented in Fig. 6. It is seen that $10^5 < N < 10^6$ empirical and simulated estimates of the time to failure of the SC system coincide with the fourth decimal place. Thus, the adequacy of the mathematical apparatus proposed in the article is proved strictly following the provisions of the theory of experimental planning and mathematical statistics.

Now, starting from the research objectives, we need to demonstrate the functionality of the proposed mathematical apparatus because the question of assessing the reliability of automated systems has been studied for many decades. At once, we will note such advantages of the offered approach as simplicity and intelligibility. The analysis of the target info-communication system logs to detect the facts of exploitation of known vulnerabilities can be performed automatically. The mathematical apparatus proposed in the article allows evaluating the efficiency of the security subsystem in the form of a single indicator of reliability—time to failure, based on generalized sets of exploitation data in the form of a tuple $\langle \Lambda, \mathrm{M}, R \rangle$. Moreover, the proposed mathematical apparatus allows us to create a system-oriented reference point—to calculate the time to failure of the target system for a certain intensity of current CPAs when the security subsystem is disabled. A simple comparison of these two values indicates the effectiveness of the security subsystem. In particular, the increase in the time to failure for the SC system to activate the security subsystem in the context of current CPAs of type $\lambda_1 \div \lambda_3$ was only 35%, prompting Vinnytsia City Council's guidance to allocate funds to purchase appropriate protective mechanisms.

Finally, we turn to the one shown in Fig. 4 empirical information. Note that $\sum_{i=0}^{4} p_i(t) = 1 \forall t \in [0, 3]$ is an indirect confirmation of the adequacy of the created mathematical apparatus. As we noted in section "Models and methods", the effectiveness of the security subsystem in counteracting typified CPAs increases with an increasing degree of convergence of the symmetric elements of the sets Λ M. Accordingly, in descending order of the probability of neutralization by the security subsystem, the types of CPAs should be arranged as follows: $\lambda_3, \lambda_2, \lambda_1$. In Fig. 4 we see that in descending order of absolute values, the curves $p_i(t), i = \overline{1,3}$, are arranged in the following order: $p_3(t), p_2(t), p_1(t)$. Accordingly, experimental data confirmed the theoretical reasoning. Also, a significant discrepancy between the values of the sets Λ M causes a relatively small calculated value $\tau = 2.350$ for the security subsystem of the SC system.

Conclusions

The article's main contribution is the description of the process of the security subsystem countering the impact of typed CPAs as a model of end states in continuous time. The input parameters of the model are the flow intensities of typed CPAs, the flow intensities of possible cyber-immune reactions, and the set of probabilities of neutralization of CPAs. The set of admissible states of the info-communication system is described taking into account possible variants of development of the modelled process. The initial parameters of the model are the probabilities of the studied system in the appropriate states at a certain moment. The dynamics of the life cycle of the info-communication system is embodied in the form of a matrix of transient probabilities. The mentioned matrix connects the initial parameters in the form of a system of Chapman's equations. The article presents a computationally efficient concept based on Gershgorin's theorems to solve such a system of equations with given initiating values. Based on the presented scientific results, the article proposes the concept of calculating the time to failure as an indicator of the reliability of the info-communication system operating under the probable impact of typical CPAs. The adequacy of the model and concepts presented in the article is proved by comparing a statically representative amount of empirical and simulated data. The application of the presented mathematical apparatus to analyze operational information of the Situational Center of the Information Technology Department of Vinnytsia City Council (Vinnytsia, Ukraine) showed the next. The security subsystem involved in the current CPAs prolongs the time to failure by 35% compared to the variant of operation of the mentioned info-communication system with an inactivated security subsystem.

Note that when formalizing the Markov model of the process of the security subsystem of the info-communication system confronting the impact of typed CPAs, it was considered that the latter ones are 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

Most data is contained within the article. All the data is available on request due to restrictions e.g., privacy or ethics.

Received: 5 April 2022; Accepted: 22 July 2022
Published online: 27 July 2022

References

1. Jena, P. K., Ghosh, S., Koley, E., Mohanta, D. K. & Kamwa, I. Design of AC state estimation based CPA for disrupting electricity market operation under limited sensor information. *Electr. Power Syst. Res.* **205**, 107732. https://doi.org/10.1016/j.epsr.2021.107732 (2022).

2. Qin, B., Liu, D. & Chen, G. Formal modeling and analysis of cyber-physical cross-space attacks in power grid. *Int. J. Electr. Power Energy Syst.* **141**, 107790. https://doi.org/10.1016/j.ijepes.2021.107790 (2022).
3. Wu, S. *et al.* An integrated data-driven scheme for the defense of typical cyber–physical attacks. *Reliab. Eng. Syst. Saf.* **220**, 108257. https://doi.org/10.1016/j.ress.2021.108257 (2022).
4. Cui, H. Handoff control strategy of cyber physical systems under dynamic data attack. *Comput. Commun.* **178**, 183–190. https://doi.org/10.1016/j.comcom.2021.07.026 (2021).
5. Cao, G., Gu, W., Lou, G., Sheng, W. & Liu, K. Distributed synchronous detection for false data injection attack in cyber-physical microgrids. *Int. J. Electr. Power Energy Syst.* **137**, 107788. https://doi.org/10.1016/j.ijepes.2021.107788 (2022).
6. Tahoun, A. H. & Arafa, M. Secure control design for nonlinear cyber–physical systems under DoS, replay, and deception cyber-attacks with multiple transmission channels. *ISA Trans.* https://doi.org/10.1016/j.isatra.2021.11.033 (2021).
7. Stellios, I., Kotzanikolaou, P. & Grigoriadis, C. Assessing IoT enabled CPA paths against critical systems. *Comput. Secur.* **107**, 102316. https://doi.org/10.1016/j.cose.2021.102316 (2021).
8. Jena, P. K., Ghosh, S. & Koley, E. Design of a coordinated CPA in IoT based smart grid under limited intruder accessibility. *Int. J. Crit. Infrastruct. Prot.* **35**, 100484. https://doi.org/10.1016/j.ijcip.2021.100484 (2021).
9. Li, L. *et al.* Cyber attack estimation and detection for cyber-physical power systems. *Appl. Math. Comput.* **400**, 126056. https://doi.org/10.1016/j.amc.2021.126056 (2021).
10. Snehi, M. & Bhandari, A. Vulnerability retrospection of security solutions for software-defined cyber-physical system against DDoS and IoT-DDoS attacks. *Comput. Sci. Rev.* **40**, 100371. https://doi.org/10.1016/j.cosrev.2021.100371 (2021).
11. Ding, D., Han, Q.-L., Xiang, Y., Ge, X. & Zhang, X.-M. A survey on security control and attack detection for industrial CPSs. *Neurocomputing* **275**, 1674–1683. https://doi.org/10.1016/j.neucom.2017.10.009 (2018).
12. Lima, P. M., Carvalho, L. K. & Moreira, M. V. Detectable and undetectable network attack security of CPSs. *IFAC-PapersOnLine* **51**(7), 179–185. https://doi.org/10.1016/j.ifacol.2018.06.298 (2018).
13. Barrère, M., Hankin, C., Nicolaou, N., Eliades, D. G. & Parisini, T. Measuring cyber-physical security in industrial control systems via minimum-effort attack strategies. *J. Inf. Secur. Appl.* **52**, 102471. https://doi.org/10.1016/j.jisa.2020.102471 (2020).
14. Liu, Y., Deng, L., Gao, N. & Sun, X. A reliability assessment method of cyber physical distribution system. *Energy Procedia* **158**, 2915–2921. https://doi.org/10.1016/j.egypro.2019.01.951 (2019).
15. Friederich, J. & Lazarova-Molnar, S. Towards data-driven reliability modeling for cyber-physical production systems. *Procedia Comput. Sci.* **184**, 589–596. https://doi.org/10.1016/j.procs.2021.03.073 (2021).
16. Zeng, G., Yu, T., Wang, Z. & Lin, D. Analytical reliability assessment of cyber-physical distribution system with distributed feeder automation. *Electr. Power Syst. Res.* **208**, 107864. https://doi.org/10.1016/j.epsr.2022.107864 (2022).
17. Wang, D. Data reliability challenge of cyber-physical systems. In *Cyber-Physical Systems* 91–101 (Elsevier, 2017). https://doi.org/10.1016/B978-0-12-803801-7.00006-7.
18. Hazra, A., Dasgupta, P. & Chakrabarti, P. P. Formal assessment of reliability specifications in embedded CPSs. *J. Appl. Log.* **18**, 71–104. https://doi.org/10.1016/j.jal.2016.09.001 (2016).
19. Liu, J. *et al.* Reliability assessment of cyber physical distribution system. *Energy Procedia* **142**, 2021–2026. https://doi.org/10.1016/j.egypro.2017.12.405 (2017).
20. Yang, Y., Wang, S., Wen, M. & Xu, W. Reliability modeling and evaluation of CPS (CPS) considering communication failures. *J. Frankl. Inst.* **358**(1), 1–16. https://doi.org/10.1016/j.jfranklin.2018.09.025 (2021).
21. Yuan, H., Li, G., Bie, Z. & Arif, M. Distribution system reliability assessment considering cyber-physical integration. *Energy Procedia* **158**, 2655–2662. https://doi.org/10.1016/j.egypro.2019.02.018 (2019).
22. Li, S., Cui, T. & Alam, M. Reliability analysis of the internet of things using space fault network. *Alex. Eng. J.* **60**(1), 1259–1270. https://doi.org/10.1016/j.aej.2020.10.049 (2021).
23. Yazdani, A., Shahidzadeh, M.-S. & Takada, T. Bayesian networks for disaggregation of structural reliability. *Struct. Saf.* **82**, 101892. https://doi.org/10.1016/j.strusafe.2019.101892 (2020).
24. Guo, Y. *et al.* A discrete-time Bayesian network approach for reliability analysis of dynamic systems with common cause failures. *Reliab. Eng. Syst. Saf.* **216**, 108028. https://doi.org/10.1016/j.ress.2021.108028 (2021).
25. Bhattacharya, B. A reliability based measure of structural robustness for coherent systems. *Struct. Saf.* **89**, 102050. https://doi.org/10.1016/j.strusafe.2020.102050 (2021).
26. Auzinger, W., Obelovska, K. & Stolyarchuk, R. A revised Gomory–Hu algorithm taking account of physical unavailability of network channels. In *Computer Networks* (eds Gaj, P. *et al.*) 3–13 (Springer, 2020). https://doi.org/10.1007/978-3-030-50719-0_1.
27. Fedevych, O., Dronyuk, I. & Lizanets, D. Researching measured and modeled traffic with self-similar properties for ateb-modeling method improvement. In *Computer Networks* (eds Gaj, P. *et al.*) 13–25 (Springer, 2018). https://doi.org/10.1007/978-3-319-92459-5_2.
28. Demydov, I., Dronyuk, I., Fedevych, O. & Romanchuk, V. Traffic fluctuations optimization for telecommunication SDP segment based on forecasting using ateb-functions. In *Data-Centric Business and Applications: Evolvements in Business Information Processing and Management—Volume 1* (eds Kryvinska, N. & Greguš, M.) 71–88 (Springer, 2019). https://doi.org/10.1007/978-3-319-94117-2_4.
29. O. Tymchenko, O. O. Tymchenko, B. Havrysh, O. Khamula, O. Sosnovska & S. Vasiuta. Efficient calculation methods of subtraction signals convolution. In *2019 IEEE 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM)* (IEEE, 2019). https://doi.org/10.1109/cadsm.2019.8779250.
30. Kovtun, V., Izonin, I. & Gregus, M. Mathematical models of the information interaction process in 5G-IoT ecosystem: Different functional scenarios. *ICT Express* https://doi.org/10.1016/j.icte.2021.11.008 (2021).
31. Kovtun, V., Izonin, I. & Gregus, M. Formalization of the metric of parameters for quality evaluation of the subject-system interaction session in the 5G-IoT ecosystem. *Alex. Eng. J.* **61**(10), 7941–7952. https://doi.org/10.1016/j.aej.2022.01.054 (2022).
32. Kamal, Md. S. *et al.* Hidden Markov model and Chapman Kolmogrov for protein structures prediction from images. *Comput. Biol. Chem.* **68**, 231–244. https://doi.org/10.1016/j.compbiolchem.2017.04.003 (2017).
33. Iwankiewicz, R. Integro-differential Chapman–Kolmogorov equation for continuous-jump Markov processes and its use in problems of multi-component renewal impulse process excitations. *Probab. Eng. Mech.* **26**(1), 16–25. https://doi.org/10.1016/j.probengmech.2010.06.002 (2011).
34. Stanković, L. On the sparsity bound for the existence of a unique solution in compressive sensing by the Gershgorin theorem. *Signal Process.* **190**, 108316. https://doi.org/10.1016/j.sigpro.2021.108316 (2022).
35. Zeng, Z., Zhao, J., Liu, Z., Mao, L. & Qu, K. Stability assessment for multiple grid-connected converters based on impedance-ratio matrix and Gershgorin's theorem. *Int. J. Electr. Power Energy Syst.* **138**, 107869. https://doi.org/10.1016/j.ijepes.2021.107869 (2022).

Acknowledgements

The authors would like to thank anonymous reviewers who helped present the research results 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. The Department of Computer Control Systems, Vinnytsia National Technical University, Vinnytsia, Ukraine, the Department of Artificial Intelligence,

Lviv Polytechnic National University, Ukraine, and the Faculty of Management, Comenius University in Bratislava, Slovakia, has supported this work.

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. All authors reviewed and approved the manuscript.

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.