Model for Assessing the Effectiveness of Information Security Systems of Interdependent Critical Infrastructures

Maksym Lutskyi[1], Viktoriia Sydorenko[1], Artem Polozhentsev[1], Nataliia Apenko[1], and Serhii Sydorenko[1]

[1]*National Aviation University, 1, Liubomyra Huzara ave. Kyiv, 03058, Ukraine*

Abstract

Today, critical infrastructure organization varies widely across countries, but important commonality is a close interconnection and significant interdependence on certain ICT. A state's national security and the quality of life of its citizens depend on the continued reliable operation of a complex, interdependent critical infrastructure, including transportation, electricity, oil, gas, telecommunications, and emergency services. A failure in one infrastructure can quickly and significantly affect another. Modern infrastructures are almost entirely dependent on ICT and often need to be interconnected through electronic communication channels to operate reliably. While these technologies offer tremendous efficiencies, they also create new vulnerabilities. Therefore, there is a need to develop new models and methods to ensure the stable operation of interdependent critical infrastructures. This paper proposes a model for assessing the effectiveness of information security systems, which, by representing interdependent critical infrastructures in the form of Markov and semi-Markov processes, introducing changes in the state space and transition matrix, allows optimizing costs and investments in the information security system while ensuring a given level of its security. In addition, an experimental study of the proposed model was conducted. The use of this model allows to comprehensively assess the main indicators of investment in ensuring the security of interdependent critical infrastructures of the state, considering budgetary constraints on the total costs incurred.

Keywords

Critical infrastructure, interdependent critical infrastructures, critical infrastructure objects, efficiency, performance assessment model, investment optimization, level of security.

1. Introduction

Today, critical infrastructure organization varies widely across countries, but important commonality is the close interconnection and significant interdependence on certain ICT. Infrastructure is defined as a network of interdependent systems and processes that interact to produce and distribute a continuous flow of goods and services necessary for community development. Critical infrastructures in different countries are highly integrated and interconnected, both physically and through a range of ICT. As a result, failures in one infrastructure can have a direct or indirect impact on other infrastructure assets, damaging the entire geographic region and having a significant impact on the economy of the country or even the global economy [1–2].

A state's national security and the quality of life of its citizens depend on the continued reliable operation of a complex, interdependent critical infrastructure, including transportation, electricity, oil, gas, telecommunications, and emergency services. A failure in one infrastructure can quickly and significantly affect another. Today critical infrastructure (Fig. 1) contains the following sectors (in the USA for example): Chemical Sector; Critical Manufacturing Sector; Commercial Facilities Sector; Communications; Dams Sector; Defense Industrial Base Sector; Emergency Services; Energy; Transportation etc.

CPITS 2023: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2023, Kyiv, Ukraine
EMAIL: m.lutskyi@gmail.com (M. Lutskyi); v.sydorenko@ukr.net (V. Sydorenko); artem.polozhencev@gmail.com (A. Polozhentsev); apenko_nata@ukr.net (N. Apenko); serh.sydorenko@gmail.com (S. Sydorenko)
ORCID: 0000-0003-1678-3196 (M. Lutskyi); 0000-0002-5910-0837 (V. Sydorenko); 0000-0003-0139-0752 (A. Polozhentsev); 0000-0001-6891-0869 (N. Apenko); 0000-0002-7170-123x (S. Sydorenko)

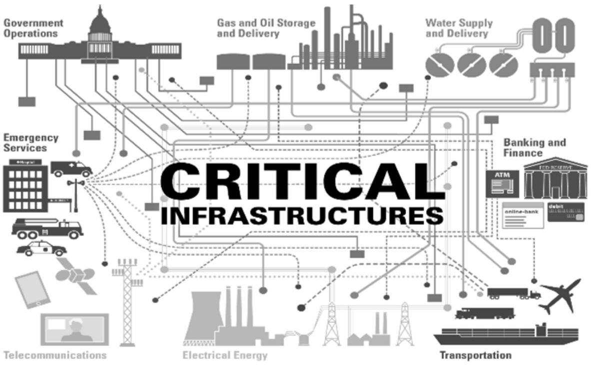


Figure 1: Critical infrastructures sectors (example)

Modern infrastructures are almost entirely dependent on ICT and the Internet and often need to be interconnected through electronic communication channels to operate reliably.

In addition, the same technology that allows information to be transmitted around the world can be used to disrupt vital systems, including the flow of electricity or water and emergency services. And while these technologies provide significant efficiencies, they also create new vulnerabilities. These vulnerabilities point to an important scientific need to assess the effectiveness of the information security systems of interdependent critical infrastructures.

2. Analysis of modern approaches and problem statement

National and economic security depend on critical infrastructure and ICT, which are constantly supported. Special committees are created, and requirements are established for each sector of infrastructure to ensure their reliability and protection.

The activity of the mentioned committees is aimed at protecting the system against hostile penetration, or computer attacks, which can cause a failure in critical infrastructure.

According to [3, 4], critical infrastructures can be conditionally divided into the following two main categories:

1. Infrastructures whose activities are based exclusively on ICT refer to most financial infrastructures.
2. Infrastructures that operate through SCADA systems (Fig. 2). This is a special control and data collection system for critical infrastructure objects, such as electricity, water, gas, fuel, communications, transportation, etc. These systems use real-time information-providing sensors and allow for control and operational changes.

Another useful model for describing the behavior of critical infrastructure and the interdependence between them is the model of defining infrastructure systems as complex adaptive systems (CAS) [5].

These systems are complex because they are diverse and contain many interconnected components. They are adaptive, allowing components of the system to make the right decisions, and change in response to information from other components and external interventions.

A detailed analysis of existing methods for assessing the effectiveness of information security systems for critical infrastructure is presented below.

A process-statistical approach to performance evaluation is presented in papers [6–8]. As a result of this approach, it is possible to obtain a histogram of distribution and an integral percentage of the distribution of the total value of predicted losses. These values allow for the estimation of the probability of a specific value at any selected point or in each interval. This probability, with a specific value of predicted losses, can be considered as justification for the effectiveness of measures to increase the information security level with a guaranteed probability.

The effectiveness assessment optimization method described in [9] involves the creation of scenarios for the development of system risk in the form of a graph, which is a logical-probabilistic model that reflects the functioning of the system. This is a bipartite graph G (A, U), where the vertices in set A correspond to the hardware and software protection means, and the vertices in set U correspond to the respective information threats. Each element (vertex) in set A is characterized by its price and its effectiveness in neutralizing information threats. Each vertex in the set U is assigned a weight equal to its value, and each edge is assigned a weight r(i,j) = {1,0}. The last event determines the dangerous state of the system.

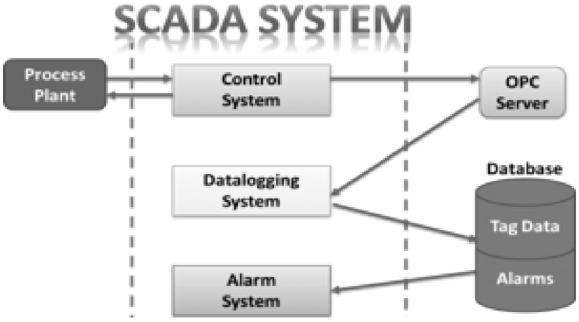


Figure 2: The scheme of SCADA system [14]

In the paper [10], the method of current and planned operating system protection measures for critical infrastructure functioning is presented, which describes the process of verifying the functionality and correctness of the operation of current systems. If it is assumed that an information protection means is functioning correctly, but this is not confirmed during business operations, then its functioning can become a source of possible vulnerability. The result of the method is a list of current and planned protective measures with information on their implementation status and use. The final determination of the risk is made by calculating the effectiveness indicator.

Based on the comparison of the results, it is concluded that if the risk is acceptable, the next step is to prepare documents for assessing the effectiveness of the information protection system. If the risk exceeds the acceptable level, it is necessary to adjust the protective measures and then repeat the procedure for calculating the potential security risk.

The model proposed in papers [11–12] for assessing the effectiveness of banking information resources is based on the calculation of a comprehensive investment efficiency indicator, which is allocated to ensuring their security and discounting future monetary inflows and outflows. The proposed approach, based on a comprehensive investment efficiency indicator, allows a new (emergent) and efficient approach to building effective security systems in terms of both security and cost-effectiveness [12].

In Table 1, the results of the analysis of methods for evaluating the effectiveness of the functioning of information security systems are summarized according to the following criteria (proposed by authors and based on modern approaches in this field):

1. Clarity of formalization (clarity and comprehensibility of mathematical calculations).
2. Ease of implementation (absence of overly complex procedures).
3. Flexibility and universality (ability to change parameters and apply them in different areas).
4. Objectivity (ability to be independently evaluated).

Table 1
The analysis of methods for assessing the effectiveness of information security systems

Approach	1	2	3	4
Process-statistical Method for Performance Evaluation	+	-	+	+
Effectiveness Assessment Optimization Method	-	+	+	-
Method of current and planned operating system protection measures	-	-	-	+
The model for assessing the effectiveness of banking information resources	+	+	-	+

Therefore, from Table 1, it can be seen that the most appropriate model for all parameters is the model for evaluating the effectiveness of banking information resources, which calculates efficiency, takes into account changes in security investments over time, but is oriented (in most cases) only to banking security and safety.

The objective of this paper is to develop and study a model for assessing the effectiveness of information security systems in interdependent critical infrastructures. To achieve this goal, the following tasks must be addressed:

1. To analyze existing approaches to assessing the effectiveness of information security systems to determine their advantages and disadvantages.
2. To develop a model for assessing the effectiveness of information security systems in interdependent critical infrastructures to enable the comprehensive determination of key investment indicators in information security systems and the provision of a specified level of security.
3. To conduct experimental research on the developed model for assessing the effectiveness of information security systems to verify its effectiveness.

3. Model for Assessing the Effectiveness of Information Security Systems of Interdependent Critical Infrastructures

The model for assessing the effectiveness of information security systems of interdependent critical infrastructures (for example, transport [15–19]) consists of four stages, namely:

1. Identification of the connections

2. Identification of the links
3. Calculation of the system efficiency and performance
4. Investments optimization [1–2]

Let's consider them in more detail below.

Stage 1: Identification of connections

To represent the system of associated critical infrastructures, graphical theory should be used, where the nodes of the graph represent critical infrastructure objects and the arcs represent infrastructure components or connections between them. It should be noted that graph arcs can change and even be uncertain. In addition, certain capabilities of one component or subsystem may be related to the performance of several other components or subsystems, and the failure of a particular link may cause the same or more serious difficulties.

For example, a critical infrastructure supply network contains separate suppliers labeled S1 and S2. The critical infrastructure entering the distribution network from supplier S1 enters through node DS1. Similarly, critical infrastructure that enters the distribution network from supplier S2 enters through node DS2. There are four different requirements for the critical infrastructure served by this network, two of which will be labeled as E1 and E2. By dividing the generation facilities into two nodes and a connecting arc (e.g., E1 and G1), a "node failure" (partial or total loss of a generator) can be represented as a loss of capacity on the connecting arc. The critical infrastructure demand values (during each period) are determined at nodes D1, D2, L1, and L2. The numbers next to the connections in the network represent the nominal capacity of these connections.

Stage 2: Identification of the links

The SCADA equipment monitors, controls, and regulates the transport of the critical infrastructure objects at the connections a → b, b → c, c → d, and d → e. Let's assume that SCADA has two main subsystems. One subsystem supports the a → b and b → c links and the other supports the c → d and d → e connections. Changes in bandwidth over time may include random failures (which reduce arc power) or repairs of indefinite duration (which restore performance). To determine the communication states corresponding to different performance levels, we use Markov and semi-Markov processes [13] to represent state transitions in time.

The state of each of the two SCADA subsystems is represented by a binary random variable, where "0" indicates a reduced state (partial loss of functionality) and "1" indicates full functionality. Since links a → b and b → c are controlled by the same SCADA subsystem, changes in their performance determined by the state of the SCADA system occur together, creating a correlation between them. The same applies to the c → d and d → e links. Since the capabilities of the a → b, b → c, c → d, and d → e link systems depend on the state of the SCADA system, the definition of states depends on the state of the corresponding SCADA subsystem.

Stage 3: Calculation of the system efficiency and performance

Assessing the probability distribution of critical infrastructure objects supplied at D1 and D2, L1 and L2 is critical to understanding the quality of service that can be provided to customers. Understanding the "recovery time" provides insight into the reliability of the system.

Let's consider the problem of an infinite horizontal generalized network flow with a set of nodes *N* and a set of arcs *A*. Let $c_t(i,j)$ be the arc capacity $(i,j) \in A$ in period *t*.

Let $C_t = (c_t(i,j)) \in E$ and $C = \{C_t\} \in E^\infty$ where *E* is the state space for the capacity on all links in period *t*. Let's consider *C* as a semi-Markov process with a probability measure $\mu(C,\theta)$.

Let *D* be the demand for each node in each period. Let f be the performance indicator defined on E^∞. In the interim analysis, f is the distribution of the time to "recover". In the steady state analysis, f is the probability distribution for the product delivered to each demand node. It is possible to estimate the probability distribution and the recovery time using the model. The procedure for creating an observation from this distribution is as follows:

1. Let *I* = 1, then for each connection it should be assumed that the capacitance has just reached the lowest possible state.
2. Given the capacity of each link, determine the demand satisfied at each location by solving the generalized flow problem, assuming that all demands are equally important.
3. Let *I* = *i* + 1.

4. When all the demands are satisfied, the flow stops, and the value will reflect the number of periods needed to recover.
5. Recover each link state based on the associated stochastic process and continue with Step 2.

Since some stochastic processes have a transition probability that is quite small and quite long, many replications are likely to be needed. To overcome this problem, important samples can be used. The basic idea behind using importance sampling is to select alternative transition matrices and residence time distributions that are more computationally efficient but to "adjust" the results using the relative probability of observing the initial parameters.

Stage 4: Investments optimization

Investment opportunities that may have an impact on efficiency can be represented in Markov models as changes in transition matrices. After all, the transition matrix for a communication channel in a network has an overall effect on the performance of the system, and this effect can be estimated by Markov models.

That is, if C is a Markov or semi-Markov process that depends on some parameter θ, it has a probability measure $\mu(C,\theta)$, that determines the probabilities of the system being in different states. If the system has a performance measure $g(C)$, the simulation model can be seen as an estimate of the expected performance for a given θ, as follows:

$$f(\theta) = E_\theta\left[g(C)\right] = \int g(C)\mu(dC,\theta).$$

To assess the effectiveness, the following expression should be used:

$$a(\theta) = \sum g(C)\pi(C,\theta),$$

where $g(C)$ is the probability that all requirements will be met, $\pi(C,\theta)$ is the probability of a steady state at θ.

Therefore, the process is as follows:

Step 1: It is necessary to compute 1000 sample paths of the system, each with 1000 periods, using transition matrices for each link that are similar to those of the basic configuration of the system, but that allows a more "efficient modeling". Let θ be the stochastic processes chosen for each link. Then, it is necessary to calculate the probability that all requirements are satisfied θ and let this value be P^*.

Step 2: Identify the links that have enough funds to make the next additional investments. If there are no links, then stop the analysis.

Step 3: For each of the links identified in Step 2, calculate separately the probability that all requirements can be met if additional investment is made in the link. Each calculation requires an "adjustment" of the 1000 sample routes identified in Step 1, based on an "importance function" for the links.

Step 4: Make an additional investment in the link that gives the largest increase in the probability that all requirements can be met, if this increase is positive. If the improvement is positive, update P, reduce the budget available for these investments, update the stochastic process set on the links O, and proceed to Step 2; otherwise stop.

The proposed model for assessing the effectiveness of information security systems, which, by representing interdependent critical infrastructures in the form of Markov and semi-Markov processes, introducing changes in the state space and transition matrix, allows for optimization the costs and investments in the information security system while ensuring a given level of its security.

4. Experimental study of the model

Stage 1: Identification of connections

For the experimental study of the proposed model, the following example of two interdependent critical infrastructures which are a gas distribution network, and an electricity generation/distribution network is considered [1–2]. The gas distribution network is supported by dispatch control and a data collection system.

The combined gas and electricity network is shown in Fig. 3. It contains two separate suppliers, labelled S1 and S2. Gas entering the distribution network from supplier S1 is delivered through node DS1.

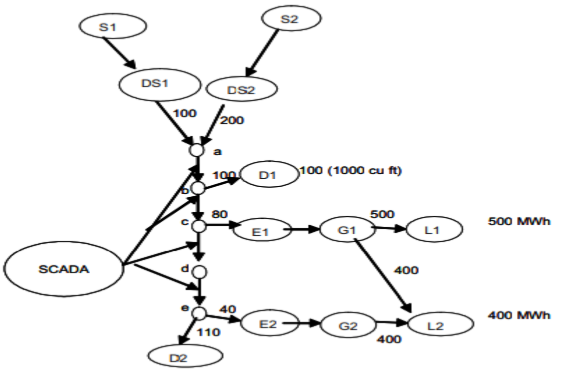


Figure 3: Representation of the network of interdependent critical infrastructures

Similarly, gas entering the distribution network from supplier S2 enters through node DS2. There are four different gas consumers served by this network, two of which are power stations (E1 and E2). Each power plant can supply the electrical load on L2, but only one of the generators can supply the electrical load on L1. By dividing the generating units into two nodes and one interconnecting line (e.g. E1 and G1), it is possible to represent a "node failure" (partial or total loss of a generator) as a loss of capacity on the interconnecting line.

The gas and electricity demand values (during each period) are recorded at nodes D1, D2, L1, and L2. The numbers next to the network connections represent the nominal capacity of these connections.

Stage 2: Identification of the links

The SCADA system [20–23] consists of two main sub-systems. One subsystem supports the connections a → b and b → c and the other—c → d and d → e. Fig. 1 shows the possibilities of establishing connections that are considered to be deterministic. In addition, stochastic processes have been identified for those connections that are considered to have an uncertain capacity. For example, the S1 → DS1 link can have a capacity of 90, 95, 100, or 105. It is assumed that the capacity evolution of gas transmission pipelines is a semi-Markov process, while other links are characterized by Markov processes. Observations of these distributions are rounded to determine the number of periods in which the process is carried out.

The state of each of the two SCADA subsystems is represented by a binary random variable, where 0 indicates a reduced state (partial loss of functionality) and 1 indicates full functionality. Thus, if the part of the SCADA system supporting a → b and b → c connections is in a reduced state, then the maximum state of the tank with the a → b connection is 250 instead of 300.

Stage 3: Calculation of the system efficiency and performance

Assessing the probability of gas supply to D1 and D2 and electricity supply to L1 and L2 is essential to understand the quality of service offered to customers. And indicator f contains four possible distributions.

Fig. 3 shows the distribution of the probability of temporary restoration based on 1000 replications. The average recovery time is 10.6 periods, but there is about a 5% chance that it will take 20 or more periods, and in one experiment it took 36 periods to recover the system. The structure of the analysis makes it relatively easy to determine the conditions that led to each recovery time observation. Such information is likely to be particularly valuable to policymakers seeking to improve system efficiency.

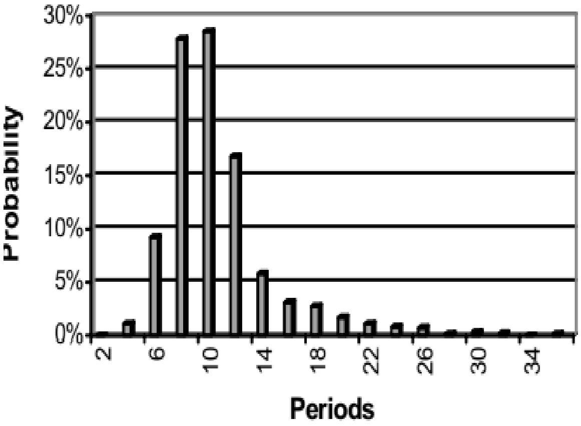


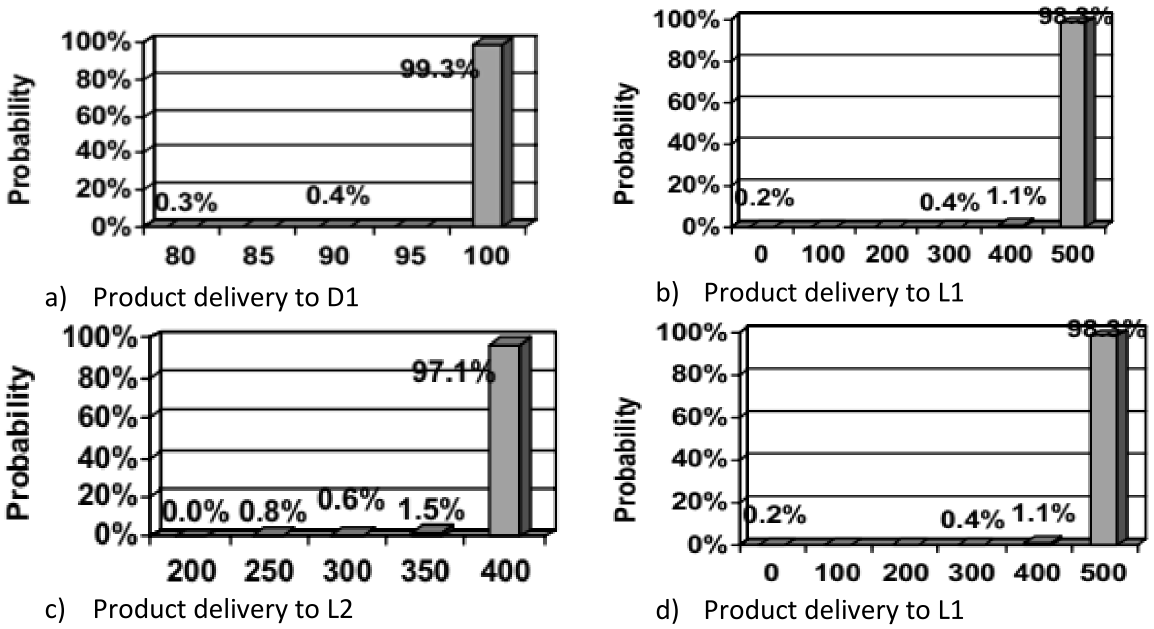
Figure 4: Time to restore the operation of the interdependent critical infrastructure systems

Then, using the algorithm described in Step 3, the stationary probability distribution for the product delivered to each demand location was estimated. Fig. 4 illustrates the probability distribution for the products delivered to each demand node based on 1000 replications of the stationary sampling scheme.

In addition, Fig. 5 shows the probability distribution for the products delivered to each demand node (if the storage tank is not available), based on 1000 replications of the steady-state sample. The proportion of periods in which demand is met by different "load nodes" of the system varies from about 94% to 99%. In general, it is more difficult to meet demand at D2 than at D1 because of the uncertainty associated with the b → c, c → d, and d → e connections.

Stage 4: Investments optimization

Investment opportunities that can improve efficiency are represented in the Markov models as changes in the transition matrices. For example, the reliability of a particular piece of equipment can be improved, and this improvement can be represented as a reduction in the probability of fault injection in the Markov model by capacity. This alternative transition matrix for the network link and the overall impact on system performance can be evaluated using simulation. Replacing the old transition matrix also has a cost associated with its improvement. Thus, the investment optimization task is to determine which investments (changes in specific transition matrices) should be made to maximize system performance, given the budget constraints on the total cost incurred.



a) Product delivery to D1

b) Product delivery to L1

c) Product delivery to L2

d) Product delivery to L1

Figure 5: Probabilities of product delivery distribution in stable operation

5. Results and discussion

Let us consider in detail what investments can be made to improve the reliability of gas supply from suppliers, SCADA system, gas pipelines, and generators. Let's assume that for $100 thousand invested in the connection, the lowest state of the tank is removed and the possibility of transition to this state is added to those for the next lower state. For each successive state removed, the cost is $150, $200, $250, $300, $350, and $400 thousand, respectively. Link investments must be made properly. For example, securing at least 100,000 cubic feet of gas from Supplier 1 requires an investment of $250,000. The goal of cost optimization is to find a tradeoff that satisfies the condition of maximizing the steady-state probability that all requirements will be met.

The proposed order of investments is to ensure the reliability of gas supplies from supplier 2 first, then to invest in gas pipelines c → d and d → e, and then in power generation lines E1 → G1 and E2 → G2.

The most significant improvement in overall system reliability is the increased reliability of gas supply from supplier 2. Without this supply, further "downstream" capacity increases are ineffective. Further investments in gas pipelines and power generation may slightly improve system reliability, but the optimization points to gas supply as the most important investment area.

This example is both simple and complex enough to illustrate processes in much larger, complex real-world networks [24–30].

As the experiment has shown, the usage of the proposed model allows a comprehensive assessment of the main indicators of investment in the security of the state's interdependent critical infrastructure [24, 31–34], considering budgetary constraints on the total cost incurred.

6. Conclusions

The paper analyzes existing approaches to assessing the effectiveness of interdependent critical infrastructures and identifies their main advantages and disadvantages. It is found that the model for assessing the effectiveness of banking information resources has the greatest advantages, which calculates efficiency and takes into account changes in security investments over time, but mostly focuses only on banking security and security of information resources.

A model for assessing the effectiveness of information security systems has been developed, which, by representing interdependent critical infrastructures in the form of Markov and semi-Markov processes, introducing changes in the state space and transition matrix, allows optimizing costs and investments in the information security system while ensuring a given (required) level of its security.

In addition, the paper conducts an experimental study of the mentioned model, which confirms its effectiveness in the comprehensive assessment of the main indicators of investment in ensuring the security of interdependent critical infrastructure of the state, considering budgetary constraints on the total cost incurred.

7. References

[1] L. Nozick, et al., Assessing the Performance of Interdependent Infrastructures and Optimizing Investment, 37th Hawaii International Conference on Systems Sciences, 2004.

[2] N. Xu, et al., Optimizing Investment for Recovery in Interdependent Infrastructure, 40th Annual Hawaii International Conference on System Sciences (HICSS'07), Waikoloa, HI, USA, 2007, 112–112. doi: 10.1109/HICSS.2007.413

[3] S. Boyer, SCADA Supervisory Control and Data Acquisition, USA: ISA—International Society of Automation, 179, 2010.

[4] H. Abbas, A. Mohamed, Review in the Design of Web-Based SCADA Systems Based on OPC DA Protocol, Int. J. Comput. Netws. 2(6) (2011) 266–277.

[5] S. Rinaldi, J. Peerenboom, T. Kelly, Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies, IEEE Control Systs. Magazine, 21(6) (2001) 11–25. doi:10.1109/37.969131

[6] D. Mussington, Concepts for Enhancing Critical Infrastructure Protection: Relating Y2K to CIP Research and Development, RAND: Sci. Technol. Inst. Santa Monica, 2002.

[7] F. Petit, K. Wallace, J. Phillips, An Approach to Critical Infrastructure Resilience, The CIP Report, Center for Infrastructure Protection and Homeland Security, George Mason University School of Law, January, 12(7), 2014, 17–20.

[8] J. Phillips, et al., A Framework for Assessing Infrastructure Risk, M4-I Resilience Evaluation Approaches for the Analysis of Complex Systems, Risk Analysis: Advancing Analysis, Society for Risk Analysis, 2012.

[9] G. Gürkan, Y. Ozge, S. Robinson, Sample Path Optimization in Simulation, Winter Simulation Conference, 1994, 247–254.

[10] H. Abbas, A. Mohamed, Review in the Design of Web-Based SCADA Systems Based on OPC DA Protocol, Int. J. Comput. Netws. 2(6) (2011) 266–277.

[11] S. Yevseyev, O. Korol, Complex Indicator of Investments Efficiency in Bank Information Security Based on a Synergistic Threat Model, VI International Scientific Conference “Information, Communication, Society 2017”, Slavske, Ukraine, 2017, 18–19.

[12] S. Yevseyev, Methodology for Building a Security System for Banking Information Resources, [Qualifying Scientific Work in Manuscript]. National Aviation University, Kyiv, 2018.

[13] N. Limnios, G. Oprisan, Semi-Markov processes and reliability, Birkhäuser, 2001.

[14] SCADA Projects and System. URL: https://www.ssla.co.uk/scada-projects/

[15] O. Okoro, et al., Optimization of Maintenance Task Interval of Aircraft Systems, Int. J. Comput. Netw. Inf. Secur. 14(2) (2022) 77–89. doi: 10.5815/ijcnis.2022.02.07.

[16] J. Al-Azzeh, et al., A Method of Accuracy Increment Using Segmented Regression, Algorithms, 15(10) (2022) 1–24. doi: 10.3390/a15100378

[17] M. TajDini, V. Sokolov, P. Skladannyi, Performing Sniffing and Spoofing Attack Against ADS-B and Mode S using Software Define Radio, IEEE International Conf. on Information and Telecommunication Technologies and Radio Electronics, 2021. doi: 10.1109/ukrmico52950.2021.9716665

[18] S. Gnatyuk, Critical Aviation Information Systems Cybersecurity, Meeting Security Challenges Through Data Analytics and Decision Support, IOS Press Ebooks, 47(3) (2016) 308–316. doi: 10.3233/978-1-61499-716-0-308

[19] R. Odarchenko, et al., Improved Method of Routing in UAV Network, 2015 IEEE 3rd International Conference on Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD), Kyiv, Ukraine, October 2015, 294-297.

[20] M. Fall, et al., Enhancing SCADA System Security, 2020 IEEE 63rd International Midwest Symposium on Circuits and Systems (MWSCAS), Springfield, MA, USA, 2020, 830–833. doi: 10.1109/MWSCAS48704.2020.9184532

[21] O. Ivanchenko, et al., Dependability Assessment for SCADA System Considering Usage of Cloud Resources, 2020 IEEE 11th International Conference on Dependable Systems, Services and

Technologies (DESSERT), Kyiv, Ukraine, 2020, 13–17. doi: 10.1109/DESSERT50317.2020.9125052

[22] A. Khadra, R. Rammal, SCADA System for Solar Backup Power System Automation, 2022 International Conference on Smart Systems and Power Management (IC2SPM), Beirut, Lebanon, 2022, 75–79. doi: 10.1109/IC2SPM56638.2022.9988760

[23] Y. Chen, et al., Work-in-Progress: Reliability Evaluation of Power SCADA System with Three-Layer IDS, International Conference on Compilers, Architecture, and Synthesis for Embedded Systems, Shanghai, China, 2022, 1–2. doi: 10.1109/CASES55004.2022.00007.

[24] Yu. Danik, R. Hryschuk, S. Gnatyuk, Synergistic Effects of Information and Cybernetic Interaction in Civil Aviation, Aviation, 20(3) (2016) 137–144.

[25] V. Sydorenko, Experimental FMECA-Based Assessing of the Critical Information Infrastructure Importance in Aviation, CEUR Workshop Proc. 2732 (2020) 136–156.

[26] V. Grechaninov, et al., Formation of Dependability and Cyber Protection Model in Information Systems of Situational Center, in: Workshop on Emerging Technology Trends on the Smart Industry and the Internet of Things, vol. 3149 (2022) 107–117.

[27] M. TajDini, V. Sokolov, V. Buriachok, Men-in-the-Middle Attack Simulation on Low Energy Wireless Devices using Software Define Radio, in: 8th International Conference on "Mathematics. Information Technologies. Education": Modern Machine Learning Technologies and Data Science, vol. 2386 (2019) 287–296

[28] P. Anakhov, et al., Evaluation Method of the Physical Compatibility of Equipment in a Hybrid Information Transmission Network, Journal of Theoretical and Applied Information Technology 100(22) (2022) 6635–6644.

[29] V. Grechaninov, et al., Decentralized Access Demarcation System Construction in Situational Center Network, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3188, no. 2 (2022) 197–206.

[30] O. Potii, Y. Tsyplinsky, Methods of Classification and Assessment of Critical Information Infrastructure Objects, 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 2020, 389–393. doi: 10.1109/ dessert50317.2020.9125028

[31] F. Adochiei et al., Intelligent System for Automatic Assessment and Interpretation of Disguised Behaviour for Critical Infrastructure Personnel, 2022 E-Health and Bioengineering Conference (EHB), Iasi, Romania, 2022, 01–04. doi: 10.1109/EHB55594.2022.9991710

[32] V. Rosato et al., The European Infrastructure Simulation and Analysis Centre (EISAC) initiative and its technological assets, 2020 43rd International Convention on Information, Communication and Electronic Technology (MIPRO), Opatija, Croatia, 2020, 1848–1851. doi: 10.23919/MIPRO48935.2020.9245340

[33] G.L. Pahuja, Component Importance Measures based Risk and Reliability Analysis of Vehicular Ad Hoc Networks, Int. J. Comput. Netw. Inf. Secur. 10(10) (2018) 38–45. doi:10.5815/ijcnis.2018.10.05

[34] X. Zhang, E. Izquierdo, K. Chandramouli, Critical Infrastructure Security Using Computer Vision Technologies, Secur. Technols. Social Implic. (2023) 149–180. doi: 10.1002/9781119834175.ch6