Advances in Reliability, Safety and Security, Part 6 – Kołowrocki, Magryta-Mut (eds.)
© 2024 Polish Safety and Reliability Association, Gdynia, ISBN 978-83-68136-18-0 (printed), ISBN 978-83-68136-05-0 (electronic)

Advances in Reliability, Safety and Security

ESREL 2024
Monograph Book Series

Reliability And Operational Analysis Of Electronic Security Systems Operated Within State Critical Infrastructure Facilities

Jacek Paś, Jarosław Łukasiak, Michał Wiśnios, Adam Rosiński

Military University of Technology Faculty of Electronics, Warsaw, Poland

Abstract

The study addresses issues associated with the reliability and operational analysis of electronic security systems operated within state critical infrastructure facilities. They ensure security to facilities important to the continuity of state operations. For this reason, they should be characterized by a high readiness index, which would guarantee the proper implementation of assigned tasks. Satisfying this requirement is enabled through rationalising the operation process. The authors analysed the functioning of intrusion detection systems, and then, based on the guidelines related to the operation of alarm systems set out in a defence standard, they suggested modifying the operation process, taking into account four-type periodic inspections. Further research in this field will include financial expenditure assigned to specific types of periodic inspections.

Keywords: security system, reliability, operation, critical infrastructure

1. Introduction

All currently available electronic security systems (ESS) are employed to ensure technical safety of facilities within a vast area of state critical infrastructure (SCI) (Government Security Center, 2020; Fischer et al., 2019; Kierzkowski et al., 2021; Dziula et al., 2013). ESS monitoring security within a vast SCI area include (listed in order of operating priority) (Paś et al., 2018; Paś et al., 2022; Hulida et al., 2019; Zhao et al., 2022; Filizzola et al., 2016; Jakubowski et al., 2019):

- fire alarm system (FAS) integrated with an audio warning system (AWS);
- intrusion detection system (IDS);
- closed-circuit television (VSS);
- access control system (ACS);
- electromechanical, electronic and biometric entry, passage or exit systems and systems for monitoring the locking of used premises.

Solutions in the field of electronic security systems designed and operated within SCI are usually faced with particular requirements (Klimczak and Paś, 2020; Kornaszewski, 2019). For this reason, such systems should be characterized by appropriate values of reliability and operational indicators (Kołowrocki and Soszyńska-Budny, 2011). Requirements in this field applicable to IDS operated in civilian facilities are rather generally characterized in standard "PN-EN 50131-1:2009 – Alarm systems – Intrusion detection systems – Part 1: System requirements" (PN-EN 50131-1:2009). Whereas in the case of IDSs employed to secure state critical infrastructure facilities, it is preferable to apply more precise guidelines, set out in the Defence Standard "NO-04-A0004-8:2016 Military facilities, Alarm Systems, Part 8: Operation" (NO-04-A004-8:2016).

The Defence Standard "NO-04-A0004-8:2016 Military facilities, Alarm Systems, Part 8: Operation" present a general characteristic of electronic security systems and provides detailed requirements in terms of the operation process for, among others, intrusion detection, access control and VSS systems. Implementing the described operating procedures as per the specified algorithms and schedules enables diagnosing partial fitness states in advance. This leads to an increased readiness index value. It is beneficial for the security level provided within a protected state critical infrastructure facility.

Rationalising the intrusion detection system operation process requires implementing specific actions set out in diagnostic and maintenance procedures (Andrzejczak and Bukowski, 2021; Duer et al., 2016; Kozłowski et al., 2023; Kozłowski et al., 2020; Lewandowski et al., 2021; Młynarski et al., 2020; Oszczypała et al., 2022a; Oszczypała et al., 2022b; Drzazga et al., 2016). As already stated, they are described in the Defence Standard “NO-04-A0004-8:2016 Military facilities, Alarm Systems, Part 8: Operation”. The guidelines therein indicate the need to conduct periodic inspections at specified intervals. Four periodic inspection types have been distinguished, with the scope of specific actions provided for each of them. Despite the application of this approach within the IDS operation process, there are situations where such actions apply to IDS of various operational potential. This is a consequence of the varying operating intensity of IDS within different state critical infrastructure facilities. Thus, it seems justified to take actions targeting a change of the assumed four-type periodic inspections towards activities aimed at increasing the reliability and operational indicator values. Such deliberations have been presented in the following chapters of this paper. The conducted reliability and operational analyses are related to intrusion detection systems, since they are some of the most frequently employed electronic security systems. Their operating intensity is also quite variable depending on the nature of the protected state critical infrastructure facility. Therefore, the conducted rationalization of the operation process is characterized by a significant increase in the value of reliability and operational indicators. It will be possible to implemented the proposed activities related to operation system rationalization in relation to other electronic security systems, i.e., closed-circuit television or access control.

2. Electronic security systems

The ESS most frequently employed within vast SCI areas include IDS with a diverse technical structure – from the simplest, focused ones, to complex scattered or mixed systems (Paś, 2015; Caban and Walkowiak, 2019; Bednarek et al., 2019). Fig. 1 shows and IDS classified as a so-called scattered system. Such solutions are characterized by the application of transmission buses that enable expanding the alarm control unit motherboard with modules enhancing system functionality (e.g., input expansion module, output expansion module, addressable device modules, etc.) or bus detectors. Therefore, they are employed to protect large-sized and territorially extensive facilities.

Each of the distinguished (in Fig. 1) IDSs has a separate AS control unit with hooked-up alarm lines or buses SL1,…,SLn; to $SL1_{11n}$,…,$SL1_{11nn}$. These lines contain detectors with sensors that respond to various physical phenomena characteristic of unauthorized intrusion into a protected area, e.g., human movements or presence in a room (other temperature than the general environment), etc. The number of detectors within lines and buses vary depending on the number of monitored rooms, and their area expressed in (m^2). All ESSs are powered, which is shown in a simplified way in Fig. 1 – PS. The power supply for an entire IDS within an SCI area is always an AS. Due to the potential unfitness of industrial power lines supplying a SCI area, there is always a so-called backup power supply organized for ESS, most usually in the form of a battery bank or power generators. All alarm control units, from AS1,.... to ASn operate in a redundant system for reasons associated with the reliability of the control “ring” using internal telecom buses ICB. All information exchanged between AS1 and ASn are encrypted, and only a certified service team located in a specific building within the SCI, and available 24/7, is authorized to control and modify the configuration. Immediately upon detecting an unfitness, the service team takes corrective actions using an on-site spare parts warehouse located at the supervision site. All information on the functioning of security systems – e.g., monitoring, damage or alarm status, is sent to a superior unit supervising the entire operation process. For example, a fire alarm signal is sent to the State Fire Service (PSP), the Police or other law enforcement units, which has been simplified in Fig. 1 (room arrangement within facility No. 1). All information on the technical condition of operated ESSs is also sent to an Alarm Receiving Centre (ARC). Two independent sources with signal encryption are always applied to transmit information on ESS technical conditions. These most often include hard-wired (leased telephone line) and wireless sources employing specific connections at the SCI (dedicated transmitter and receiver with antennas). In addition, perimeter security or CCTV can be used in the case of remote SCI facilities, as shown in Fig. 1 (Paś et al., 2021). Such a solution always extends the time to take specific actions available to security guards at a SCI facility.

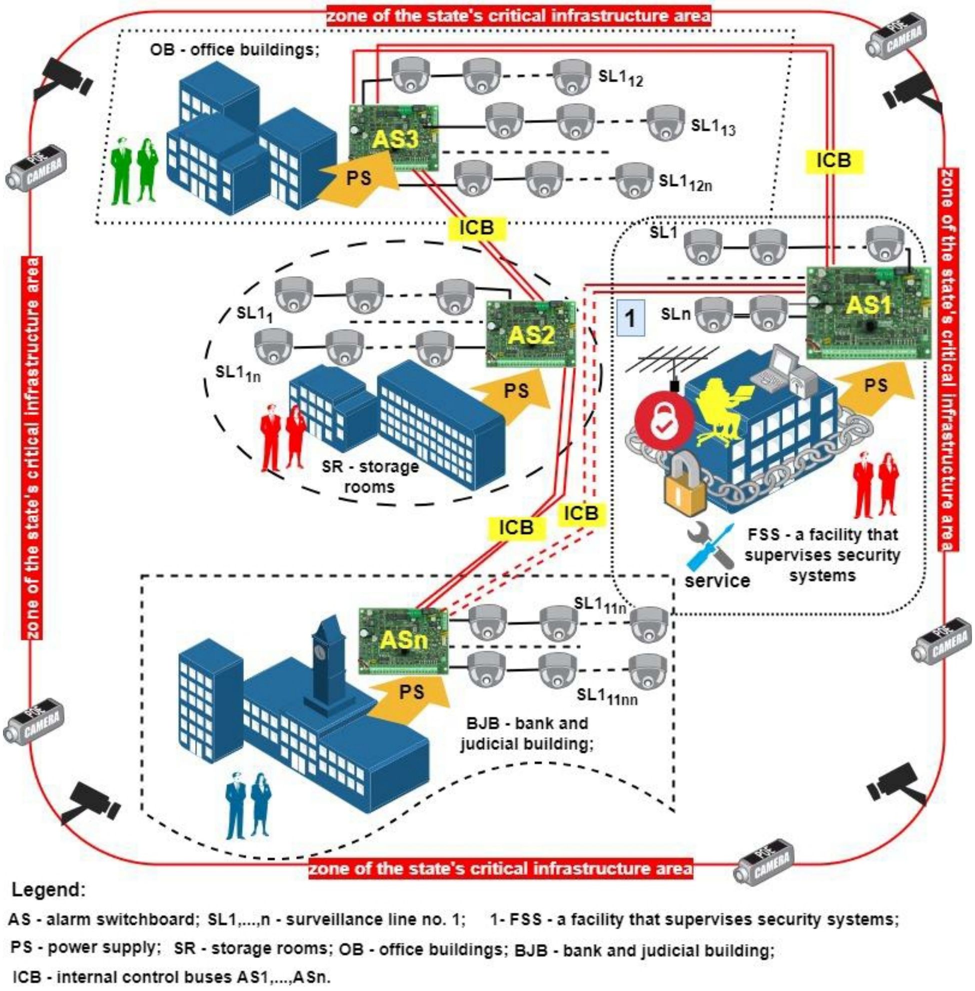
zone of the state's critical infrastructure area
OB - office buildings;
SL1$_{12}$
SL1$_{13}$
SL1$_{12n}$
AS3
PS
ICB
ICB
SL1
SL1$_1$
SL1$_{1n}$
AS2
PS
SR - storage rooms
1
SLn
AS1
PS
ICB
ICB
FSS - a facility that supervises security systems
service
SL1$_{11n}$
SL1$_{11nn}$
ASn
PS
BJB - bank and judicial building;
CAMERA
Legend:
AS - alarm switchboard; SL1,...,n - surveillance line no. 1; 1- FSS - a facility that supervises security systems;
PS - power supply; SR - storage rooms; OB - office buildings; BJB - bank and judicial building;
ICB - internal control buses AS1,...,ASn.

Fig. 1. Scattered IDS monitoring a vast area classified as the so-called SCI.

Solutions in the field of electronic security systems designed and operated within SCI are faced with particular requirements. Intrusion detection systems should be characterized by appropriate reliability and operating indicator values to effectively protect people and property in military facilities.

3. Rationalising an IDS operation process, taking periodic inspections into account

The guidelines in the Defence Standard "NO-04-A0004-8:2016 Military facilities, Alarm Systems, Part 8: Operation" indicate the application of an operational strategy according to periodic maintenance. Four types of periodic inspection are adopted for implementation. The standard stipulates their specific scopes of activity to be conducted in relation to an intrusion detection system (NO-04-A004-8:2016). The intervals related to each of the four periodic inspection types are also adopted as fixed. Therefore, these inspections apply to IDSs exhibiting various current technical condition (Będkowski and Dąbrowski, 2006). Thus, the idea to rationalize the operation procedure previously employed as per the defence standard above is reasonable.

The basic intrusion detection system operation process includes the potential absence of periodic inspections (usually in relation to IDSs operated in private facilities, which lack persons responsible for supervising technical systems). In such a case, two states are distinguished, namely, operational state S_0 and repair state S_1 (Dąbrowski et al., 2014; Dyduch et al., 2011; Łukasiak et al., 2022). The transition from the operational state to the repair state is effected upon an IDS failure (Paś and Buchla, 2019a, 2019b). A reverse transition takes place when actions are taken to restore IDS fitness. Such an operational procedure should not be implemented in relation to intrusion detection systems protecting state critical infrastructure facilities.

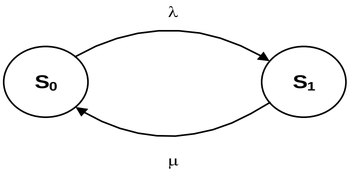

Fig. 2. Relationships within an intrusion detection system (source: own study (Łukasiak et al., 2022)). Designations in the Fig.: λ – failure intensity, μ – repair intensity.

A relationship that enables calculating the probability of an IDS remaining in the operational state can be provided for the relationship graph illustrated in Fig. 1. Then, knowing the failure and repair intensity values, the K_g readiness index value is determined through relationship (1):

$$K_g = \frac{\mu}{\mu + \lambda} \tag{1}$$

The Defence Standard "NO-04-A0004-8:2016 Military facilities, Alarm Systems, Part 8: Operation" stipulates that intrusion detection systems protecting state critical infrastructure facilities should follow an operational strategy taking into account four inspection types:

- daily (designated as state S_{001});
- monthly (designated as state S_{010});
- semi-annual (designated as state S_{011});
- annual (designated as state S_{100});

Therefore, the relationship graph in Fig. 1 should be expanded with fourth further states corresponding to the four types of periodic inspections. A graphical illustration of an updated IDS relationship graph is shown in Fig. 2. The transition from the operational state S_0 to the states standing for individual periodic inspection types is implemented in accordance with the following relationships:

- λ_1 - daily inspection intensity;
- λ_2 - monthly inspection intensity;
- λ_3 - semi-annual inspection intensity;
- λ_4 - annual inspection intensity;

The activities related to a given periodic inspection is characterized by the following intensities:

- μ_1 – daily inspection maintenance intensity;
- μ_2 – monthly inspection maintenance intensity;
- μ_3 – semi-annual inspection maintenance intensity;
- μ_4 – annual inspection maintenance intensity;

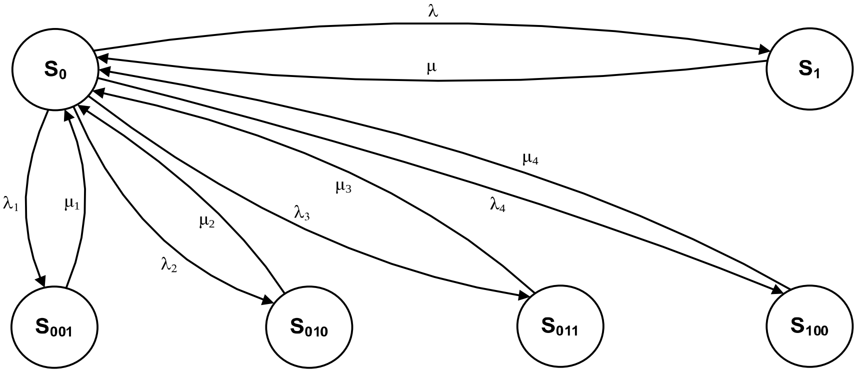

Fig. 3. Relationships within an intrusion detection system, taking into account the daily inspection S_{001}, monthly inspection S_{010}, semi-annual inspection S_{011} and annual inspection S_{100} (source: own study (Łukasiak et al., 2022)).

A relationship that enables calculating the probability of an IDS remaining in the operational state can be provided for the relationship graph illustrated in Fig. 3. Then, knowing the failure and repair intensities, and the intensities characterizing four individual periodic inspection types, the K_{g1} readiness indicator value is determined through relationship (2):

$$K_{g1}=\frac{\mu\cdot\mu_1\cdot\mu_2\cdot\mu_3\cdot\mu_4}{\begin{array}{l}\mu\cdot\mu_1\cdot\mu_2\cdot\mu_3\cdot\mu_4+\lambda\cdot\mu_1\cdot\mu_2\cdot\mu_3\cdot\mu_4+\lambda_1\cdot\mu\cdot\mu_2\cdot\mu_3\cdot\mu_4+\\+\lambda_2\cdot\mu\cdot\mu_1\cdot\mu_3\cdot\mu_4+\lambda_3\cdot\mu\cdot\mu_1\cdot\mu_2\cdot\mu_4+\lambda_4\cdot\mu\cdot\mu_1\cdot\mu_2\cdot\mu_3\end{array}} \qquad (2)$$

The rationalization of an intrusion detection system operation process will take into account the varying IDS operating potential (Grabski, 2015; Nowakowski and Siergiejczyk, 2022; Stawowy, 2019; Werbińska-Wojciechowska, 2019). This enables expanding the scope of maintenance activities for daily, monthly and semi-annual inspections. Therefore, the relationship graph shown in Fig. 3 will take the form as in Fig. 4. The application of additional states meaning further activities that are extra in relation to a given periodic inspection types will enable adapting periodic maintenance to individual IDSs operated with different intensity.

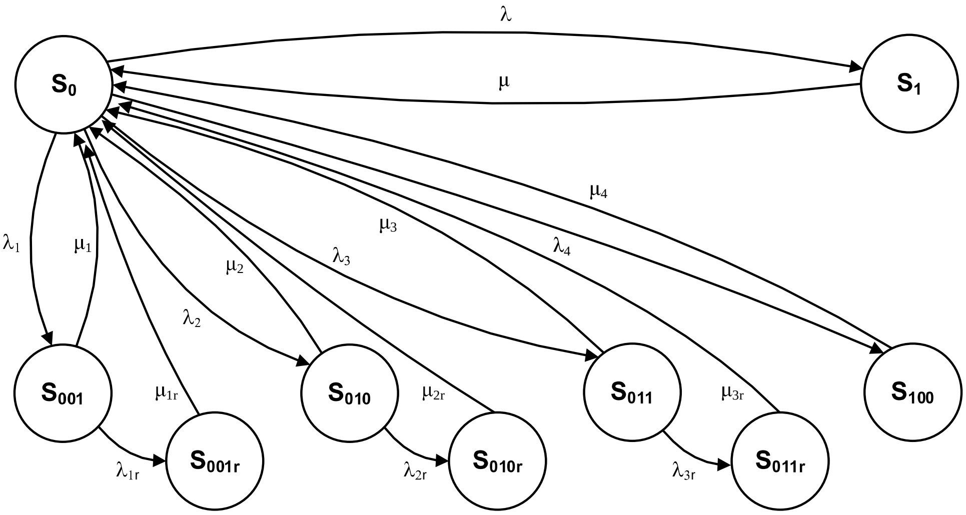

Fig. 4. Relationships within an intrusion detection system, taking into account the daily inspection S_{001}, monthly inspection S_{010}, semi-annual inspection S_{011}, annual inspection S_{100}, extended daily inspection S_{001r}, extended monthly inspection S_{010r}, extended semi-annual inspection S_{011r} (source: own study).

Designations in Fig. 4 are as follows:

- λ_{1r} - intensity of additional activities relative to daily inspections;
- λ_{2r} - intensity of additional activities relative to monthly inspections;
- λ_{3r} - intensity of additional activities relative to semi-annual inspections;
- μ_{1r} - operational maintenance intensity of additional activities relative to daily inspections;
- μ_{2r} - operational maintenance intensity of additional activities relative to monthly inspections;
- μ_{3r} - operational maintenance intensity of additional activities relative to semi-annual inspections;

For the purposes of determining the probabilities of an intrusion detection system (Fig. 4) remaining in individual, distinguished states, the transition graph was described by the following equations:

$$\begin{array}{l}
-\lambda\cdot P_0+\mu\cdot P_1-\lambda_1\cdot P_0+\mu_1\cdot P_{001}+\mu_{1r}\cdot P_{001r}-\lambda_2\cdot P_0+\mu_2\cdot P_{010}+\mu_{2r}\cdot P_{010r}-\\
-\lambda_3\cdot P_0+\mu_3\cdot P_{011}+\mu_{3r}\cdot P_{011r}-\lambda_4\cdot P_0+\mu_4\cdot P_{100}=0\\
\lambda\cdot P_0-\mu\cdot P_1=0\\
\lambda_1\cdot P_0-\mu_1\cdot P_{001}-\lambda_{1r}\cdot P_{001}=0\\
\lambda_{1r}\cdot P_{001}-\mu_{1r}\cdot P_{001r}=0\\
\lambda_2\cdot P_0-\mu_2\cdot P_{010}-\lambda_{2r}\cdot P_{010}=0\\
\lambda_{2r}\cdot P_{010}-\mu_{2r}\cdot P_{010r}=0\\
\lambda_3\cdot P_0-\mu_3\cdot P_{011}-\lambda_{3r}\cdot P_{011}=0\\
\lambda_{3r}\cdot P_{011}-\mu_{3r}\cdot P_{011r}=0\\
\lambda_4\cdot P_0-\mu_4\cdot P_{100}=0
\end{array}\tag{3}$$

The solution to the system of equations (3) are relationships that determine the probability of an intrusion detection system in question remaining in individual, distinguished states. These relationships enable rationalising an IDS operation process, taking periodic inspections into account.

The authors, aided by mathematical software, determined a relationship that enables calculating the probabilities for an IDS remaining in the operational and repair states. They are expressed through relationships (4) and (5).

$$P_0=\frac{-\mu\cdot\left(-\lambda_{1r}-\mu_1\right)\cdot\mu_{1r}\cdot\left(-\lambda_{2r}-\mu_2\right)\cdot\mu_{2r}\cdot\left(-\lambda_{3r}-\mu_3\right)\cdot\mu_{3r}\cdot\mu_4}{\begin{array}{l}\lambda_1\cdot\mu\cdot\left(-\lambda_{2r}-\mu_2\right)\cdot\left(-\lambda_{3r}-\mu_3\right)\cdot\left(\lambda_{1r}\cdot\mu_{2r}\cdot\mu_{3r}\cdot\mu_4+\mu_{1r}\cdot\mu_{2r}\cdot\mu_{3r}\cdot\mu_4\right)+\\
+\left(-\lambda_{1r}-\mu_1\right)\cdot\left(\begin{array}{l}\lambda_2\cdot\mu\cdot\mu_{1r}\cdot\left(-\lambda_{3r}-\mu_3\right)\cdot\left(\lambda_{2r}\cdot\mu_{3r}\cdot\mu_4-\mu_{2r}\cdot\mu_{3r}\cdot\mu_4\right)+\\
+\left(-\lambda_{2r}-\mu_2\right)\cdot\left(\begin{array}{l}\lambda_3\cdot\mu\cdot\mu_{1r}\cdot\mu_{2r}\cdot\left(\lambda_{3r}\cdot\mu_4+\mu_{3r}\cdot\mu_4\right)+\\
+\left(-\lambda_{3r}-\mu_3\right)\cdot\left(\begin{array}{l}\mu\cdot\mu_{1r}\cdot\mu_{2r}\cdot\mu_{3r}\cdot\left(-\lambda_4-\mu_4\right)-\\
-\lambda\cdot\mu_{1r}\cdot\mu_{2r}\cdot\mu_{3r}\cdot\mu_4\end{array}\right)\end{array}\right)\end{array}\right)\end{array}}\tag{4}$$

$$P_1=\frac{-\lambda\cdot\left(-\lambda_{1r}-\mu_1\right)\cdot\mu_{1r}\cdot\left(-\lambda_{2r}-\mu_2\right)\cdot\mu_{2r}\cdot\left(-\lambda_{3r}-\mu_3\right)\cdot\mu_{3r}\cdot\mu_4}{\begin{array}{l}\lambda_1\cdot\mu\cdot\left(-\lambda_{2r}-\mu_2\right)\cdot\left(-\lambda_{3r}-\mu_3\right)\cdot\left(\lambda_{1r}\cdot\mu_{2r}\cdot\mu_{3r}\cdot\mu_4+\mu_{1r}\cdot\mu_{2r}\cdot\mu_{3r}\cdot\mu_4\right)+\\
+\left(-\lambda_{1r}-\mu_1\right)\cdot\left(\begin{array}{l}\lambda_2\cdot\mu\cdot\mu_{1r}\cdot\left(-\lambda_{3r}-\mu_3\right)\cdot\left(\lambda_{2r}\cdot\mu_{3r}\cdot\mu_4-\mu_{2r}\cdot\mu_{3r}\cdot\mu_4\right)+\\
+\left(-\lambda_{2r}-\mu_2\right)\cdot\left(\begin{array}{l}\lambda_3\cdot\mu\cdot\mu_{1r}\cdot\mu_{2r}\cdot\left(\lambda_{3r}\cdot\mu_4+\mu_{3r}\cdot\mu_4\right)+\\
+\left(-\lambda_{3r}-\mu_3\right)\cdot\left(\begin{array}{l}\mu\cdot\mu_{1r}\cdot\mu_{2r}\cdot\mu_{3r}\cdot\left(-\lambda_4-\mu_4\right)-\\
-\lambda\cdot\mu_{1r}\cdot\mu_{2r}\cdot\mu_{3r}\cdot\mu_4\end{array}\right)\end{array}\right)\end{array}\right)\end{array}}\tag{5}$$

Relationships (5) and (6) enable rationalising the intrusion detection system operation process, taking into account the four-type periodic inspections, standard and those with an extended scope of activities.

4. Conclusions and summary

The study discusses issues associated with analysing and rationalising the process of operating electronic security systems, focusing on intrusion detection systems. Based on the guidelines regarding maintenance activities set out in the Defence Standard "NO-04-A0004-8:2016 Military facilities, Alarm Systems, Part 8: Operation", the authors analysed the current state of the IDS operation process. Next, they suggested a rationalisation of the intrusion detection system operation process, taking into account the four-type periodic inspections, standard and those with an extended scope of activities.

They also determined relationships that enable calculating the probability of an IDS remaining in a state of operation and a state of repair, allowing for the correct selection of the intensities of individual periodic inspection types and the expansion of individual inspection types with additional activities related to a given type. The practical application of the described relationships enables rationalizing the IDS operation process.

As part of further research on the issue in question, the authors plan to include financial expenditure allocated to specific periodic inspection types and their expansion with additional activities. Such an analysis will enable verifying the developed rationalisation for the operation of IDS in actual facilities, taking the economic factor into account.

Acknowledgements

This work was co-financed by the Military University of Technology under research project UGB ISE 2024.

References

Andrzejczak, K., Bukowski, L. 2021. A method for estimating the probability distribution of the lifetime for new technical equipment based on expert judgement. Eksploatacja i Niezawodność – Maintenance and Reliability, 23, 757–769.

Bednarek, M., Dąbrowski, T., Olchowik, W. 2019. Selected practical aspects of communication diagnosis in the industrial network. J. Konbin, 49, 383–404.

Będkowski, L., Dąbrowski, T. 2006. Podstawy eksploatacji, cz. II Podstawy niezawodności eksploatacyjnej *[Fundamentals of operation. Part 2: Operational reliability basics]*. Military University of Technology, Warsaw.

Caban, D., Walkowiak, T. 2019. Dependability analysis of hierarchically composed system-of-systems. In Thirteenth International Conference on Dependability and Complex Systems DepCoS-RELCOMEX; Springer: Cham, Switzerland. pp. 113–120.

Dąbrowski, T., Paś, J., Olchowik, W., Rosiński, A., Wiśnios, M. 2014. Podstawy eksploatacji systemów: Laboratorium *[System operation fundamentals: Laboratory]*. Military University of Technology, Warsaw.

Defence Standard NO-04-A0004-8:2016 – Military facilities – Alarm Systems – Part 8: Operation.

Drzazga, M., Kołowrocki, K., Soszyńska-Budny, J. Methodology for oil pipeline critical infrastructures safety and resilience to climate change analysis. J. Pol. Saf. Reliab. Assoc. Summer Safety. Reliab. Semin. 2016, 7, 173–178.

Duer, S., Duer, R., Mazuru, S. 2016. Determination of the expert knowledge base on the basis of a functional and diagnostic analysis of a technical object. Nonconv. Technol. Rev., 20, 23–29.

Dyduch, J., Paś/ J., Rosiński/ A. 2011. Podstawy eksploatacji transportowych systemów elektronicznych *[Fundamentals of operating electronic transport systems]*. Wydawnictwo Politechniki Radomskiej, Radom.

Dziula, P., Kołowrocki, K., Soszyńska-Budny, J. Maritime Transportation System Safety-Modeling and Identification. TransNav Int. J. Mar. Navig. Saf. Transp. 2013, 7, 169–175.

Filizzola, C., Corrado, R., Marchese, F., Mazzeo, G., Paciello, R., Pergola, N., Tramutoli, V. Rst-fires an exportable algorithm for early fire detection and monitoring: Description implementation and field validation in the case of the msg-seviri sensor. Remote Sens. Environ. 2016, 186, 196–216.

Fischer, R.J., Halibozek, E.P., Walters, D.C. 2019. Introduction to Security. Butterworth-Heinemann.

Government Security Center. 2020. National Critical Infrastructure Protection Programme in Poland.

Grabski, F. 2015. Semi-Markov Processes: Applications in System Reliability and Maintenance. Elsevier, Amsterdam.

Hulida, E.; Pasnak, I.; Koval, O.; Tryhuba, A. Determination of the Critical Time of Fire in the Building and Ensure Successful Evacuation of People. Period. Polytech. Civ. Eng. 2019, 63, 308–316.

Jakubowski, J., Solarczyk, M., Wisnios, M. 2019. Smoke detection in a digital image with the use of convolutional network. XII Conference On Reconnaissance And Electronic Warfare Systems, vol. 11055, DOI: 10.1117/12.2524560.

Kierzkowski, A., Kisiel, T., Uchroński, P. 2021. Simulation Model of Airport Security Lanes with Power Consumption Estimation, Energies, 14, 6725.

Klimczak, T., Paś, J. 2020. Basics of Exploitation of Fire Alarm Systems in Transport Facilities. Military University of Technology, Warsaw.

Kołowrocki, K., Soszyńska-Budny, J. 2011. Reliability and Safety of Complex Technical Systems and Processes: Modeling—Identification—Prediction—Optimization. Springer, London.

Kornaszewski, M. 2019. Modelling of exploitation process of the railway traffic control device. WUT J. Transp. Eng., 124, 53–63.

Kozłowski, E., Borucka, A., Oleszczuk, P., Jałowiec, T. 2023. Evaluation of the maintenance system readiness using the semi-Markov model taking into account hidden factors. Eksploatacja i Niezawodność – Maintenance and Reliability, 25 (4).

Kozłowski, E., Borucka, A., Świderski, A. 2020. Application of the logistic regression for determining transition probability matrix of operating states in the transport systems. Eksploatacja i Niezawodność – Maintenance and Reliability, 22, 192–200.

Lewandowski, J., Młynarski, S., Pilch, R., Smolnik, M., Szybka, J., Wiązania, G. 2021. An evaluation method of preventive renewal strategies of railway vehicles selected parts. Eksploatacja i Niezawodnosc – Maintenance and Reliability, 23 (4).

Łukasiak, J., Rosiński, A., Wiśnios, M. 2022. Problematyka racjonalizacji procesu eksploatacji systemów sygnalizacji włamania i napadu *[Rationalising the operation process of intrusion detection systems]*, in: Ciszewski, T., Wojciechowski, J. (ed.), Współczesne wyzwania transportu i elektrotechniki *[Contemporary challenges for transport and electrical engineering]*. Kazimierz Pulaski University of Technology and Humianities in Radom.

Łukasiak, J., Rosiński, A., Wiśnios, M. 2022. The Issue of Evaluating the Effectiveness of Miniature Safety Fuses as Anti-Damage Systems. Energies, 15, 11, 4013.

Młynarski, S., Pilch, R., Smolnik, M., Szybka, J., Wiązania, G. 2020. A model of an adaptive strategy of preventive maintenance of complex technical objects. Eksploatacja i Niezawodność – Maintenance and Reliability, 22, 35–41.

Nowakowski, T., Siergiejczyk, M. (ed.). 2022. Inżynieria niezawodności - teoria i praktyka. 50 lat Zimowych Szkół Niezawodności *[Reliability engineering – theory and practice. 50 years of Winter Schools of Reliability]*. Oficyna Wydawnicza Politechniki Warszawskiej, Warsaw.

Oszczypała, M., Ziółkowski, J., Małachowski, J. 2022. Analysis of Light Utility Vehicle Readiness in Military Transportation Systems Using Markov and Semi-Markov Processes. Energies, 15, 5062.

Oszczypała, M., Ziółkowski, J., Małachowski, J. 2022. Reliability Analysis of Military Vehicles Based on Censored Failures Data. Appl. Sci., 12, 2622.

Paś, J. 2015. Operation of Electronic Transportation Systems. Publishing House University of Technology and Humanities, Radom.

Paś, J., Buchla, S. 2019. Analysis of the Electronic Device Exploitation Process - Research Results, Journal of KONBiN, 49.

Paś, J., Buchla, S. 2019. Exploitation of Electronic Devices - Selected Issues, Journal of KONBiN, 49.

Paś, J., Rosiński, A., Białek, K. 2021. A reliability-operational analysis of a track-side CCTV cabinet taking into account interference. Bull. Pol. Acad. Sci. Tech. Sci., 69, e136747.

Paś, J., Rosiński, A., Wiśnios, M., Majda-Zdancewicz, E., Łukasiak, J. 2018. Elektroniczne systemy bezpieczeństwa. Wprowadzenie do laboratorium. Military University of Technology, Warsaw.

Paś, J., Rosiński, A., Wiśnios, M., Stawowy, M. 2022. Assessing the Operation System of Fire Alarm Systems for Detection Line and Circuit Devices with Various Damage Intensities. *Energies*, 15, 9, 3066.

PN-EN 50131-1:2009 - Alarm systems - Intrusion detection systems - Part 1: System requirements.

Stawowy, M. 2019. Metoda wielowarstwowego modelowania niepewności w szacowaniu jakości informacji systemów teleinformatycznych w transporcie *[Multi-layer uncertainty modelling method in estimating information quality within ICT systems in transport]*. Oficyna Wydawnicza Politechniki Warszawskiej, Warsaw.

Werbińska-Wojciechowska, S. 2019. Technical system maintenance: delay-time-based modelling. Springer.

Zhao, H., Schwabe, A., Schläfli, F., Thrash, T., Aguilar, L., Dubey, R.K., Karjalainen, J.; Hölscher, C., Helbing, D., Schinazi, V.R. Fire evacuation support