W U T J o u r n a l o f T r a n s p o r t a t i o n E n g i n e e r i n g

P R A C E N A U K O W E - P O L I T E C H N I K A W A R S Z A W S K A . T R A N S P O R T

ISSN: 1230-9265 vol. **137**
DOI: 10.5604/01.3001.0054.3432 2023

Rationalization of the operation process of intrusion and hold-up alarm systems

Karolina Krzykowska-Piotrowska[1], **Adam Rosiński**[2,*], **Jacek Paś**[2]

[1] Warsaw University of Technology, Faculty of Transport
[2] Military Univerrity of Technology, Faculty of Electronics

Abstract: Intrusion and hold-up alarm systems (I&HAS) are part of electronic security systems. They are now installed in many facilities, including those classified as critical infrastructure. The variety of available alarm control panels and their configurations means that I&HAS are installed with the use of alarm control panels with various functional and diagnostic capabilities. In the process of operation of intrusion and hold-up alarm systems, maintenance actions are most often used when no damage has occurred. This is referred to as preventive maintenance. These activities are aimed at carrying out preventive maintenance that will reduce the likelihood of damage or deterioration of the system. An extension and also an evolution of preventive maintenance activities is the development of the eMaintenance concept. By implementing modern solutions in diagnosing intrusion and hold-up alarm systems and using advanced IT applications, it is possible to monitor them and manage the operational process in real-time with the possibility of observing the degradation of the I&HAS. This makes it possible to take action to prevent the transition to a state of partial fitness or unfitness. As a result of the analysis of the operation process of the intrusion and hold-up alarm systems, taking into account diagnostic information, a graph of relations occurring in the system was developed. Then, dependencies were determined to calculate the probabilities of the I&HAS being in a state of full ability, states of periodic service, states of partial ability, and a state of unfitness. The issues of modelling the operation process of intrusion and hold-up alarm systems presented by the authors make it possible to rationalize the intensity of periodic inspections. The result is an increase in the value of the readiness index of I&HAS, which is particularly important in the case of securing critical infrastructure facilities.

Keywords: intrusion and hold-up alarm systems, operation process, modelling

Article citation information:

Krzykowska-Piotrowska, K., Rosiński, A., Paś, J. (2023). Rationalization of the operation process of intrusion and hold-up alarm systems, WUT Journal of Transportation Engineering, 137, 103-113, ISSN: 1230-9265, DOI: 10.5604/01.3001.0054.3432

*Corresponding author
E-mail address: karolina.krzykowska@pw.edu.pl (K. Krzykowska-Piotrowska), adam.rosinski@wat.edu.pl (A. Rosiński), jacek.pas@wat.edu.pl (J. Paś)
ORCID iD: 0000-0002-1253-3125 (K.Krzykowska-Piotrowska), 0000-0002-1776-9540 (A.Rosiński), 0000-0001-8900-1445 (J.Paś)

Received 9 November 2023, Revised 4 December 2023, Accepted 11 December 2023, Available online 18 December 2023

1. Wprowadzenie

Systemy Sygnalizacji Włamania i Napadu (SSWiN) są elementem składowym elektronicznych systemów bezpieczeństwa. Instalowane są one w wielu obiektach transportowych, z których część jest zaliczana do infrastruktury krytycznej [17,18,19]. Duża różnorodność typów central alarmowych i ich konfiguracji skutkuje, iż SSWiN są projektowane z wykorzystaniem central alarmowych o różnych możliwościach funkcjonalnych i diagnostycznych.

Szczególne wymagania stawiane są rozwiązaniom z zakresu elektronicznych systemów bezpieczeństwa projektowanych i eksploatowanych w obiektach wojskowych. Systemy sygnalizacji włamania i napadu, by skutecznie chronić osoby i mienie przebywające w obiektach wojskowych powinny cechować się odpowiednimi wartościami wskaźników niezawodnościowo-eksploatacyjnych. O ile dla SSWiN stosowanych w obiektach cywilnych wymagania w zakresie eksploatacji są opisane w normach dość ogólnie, o tyle dla SSWiN stosowanych w obiektach wojskowych jest to precyzyjnie opisane w normach obronnych. Przykładem takiego opracowania jest Norma Obronna NO-04-A004-8:2016 Obiekty wojskowe, Systemy Alarmowe, Część 8: Eksploatacja [10].

W normie obronnej NO-04-A004-8:2016 Obiekty wojskowe, Systemy Alarmowe, Część 8: Eksploatacja zawarto zarówno wytyczne dotyczące wymaganych rozwiązań niezbędnych w SSWiN do ochrony obiektów wojskowych, jak również wymagania z obszaru procesu eksploatacji. Są one szczególnie istotne, gdyż działanie zgodnie z podanymi algorytmami i harmonogramami umożliwia wcześniejsze wykrycie stanów niezdatności, a tym samym zwiększenie wartości wskaźnika gotowości. Wpływa to bezpośrednio na potencjalny poziom bezpieczeństwa, jaki jest w zabezpieczanym obiekcie.

W celu racjonalizacji procesu eksploatacji systemów sygnalizacji włamania i napadu realizowane są działania z zakresu procedur diagnostyczno-obsługowych. Wymienione są cztery rodzaje przeglądów z podaniem zakresu czynności, jakie powinny być zrealizowane. Przeglądy te są przeprowadzane zgodnie z podanymi interwałami czasowymi. Należy jednak zauważyć, iż działania te przeprowadzane są w SSWiN, które znajdują się w różnych stanach technicznych. Wynika to z faktu, iż są one eksploatowane z różną intensywnością zależną od rodzaju chronionego obiektu [7,11,12]. Na wartości wskaźników niezawodnościowo-eksploatacyjnych wpływają również czynniki środowiskowe występujące w chronionym obiekcie [3,5,6,20]. Potrzebne jest więc dokonanie racjonalizacji procesu eksploatacji systemów sygnalizacji włamania i napadu, poprzez opracowanie modelu procesu eksploatacji uwzgledniającego informacje diagnostyczne, dzięki którym będzie można ulepszyć zakres działań przeprowadzanych w ramach przeglądów okresowych.

2. Systemy sygnalizacji włamania i napadu

W normie europejskiej EN 50131-1:2006 „Alarm systems – Intrusion and hold-up systems – Part 1: System requirements", która została przez Polski Komitet Normalizacyjny przyjęta jako Polska Norma PN-EN 50131-1:2009 „Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Wymagania systemowe", zamieszczono na początku wykaz definicji i skrótów, wśród których są m.in. następujące definicje [15]:

- system alarmowy (ang. *alarm system*) – instalacja elektryczna, która odpowiada na ręczne lub automatyczne wykrycie obecności zagrożenia,
- urządzenie sterujące i obrazujące (ang. *control and indicating equipment*) – urządzenie do odbierania, przetwarzania, sterowania, obrazowania oraz transmitowania dalej informacji.

Centrale alarmowe (określane w normie jako urządzenia sterujące i obrazujące) stanowią wyspecjalizowane płyty główne, których zadaniem jest [14]:

- odbieranie sygnałów informacyjnych (analogowych i/lub cyfrowych) od poszczególnych urządzeń,
- przetwarzanie ich zgodnie z wcześniej zaprogramowanymi ustawieniami (instalatora i/lub producenta),
- sterowanie poprzez podanie odpowiednich sygnałów wyjściowych,
- obrazowanie zaistniałych zdarzeń na odpowiednich urządzeniach wchodzących w skład systemu sygnalizacji włamania i napadu,
- transmisja informacji do innych systemów (np. alarmowego centrum odbiorczego (ang. *alarm receiving centre*, w skrócie ARC), a w obiektach wojskowych do Garnizonowego Centrum Monitorowania Alarmów GCMA).

Systemy sygnalizacji włamania i napadu aby móc skutecznie realizować wyznaczone zadania w zakresie ochrony obiektów zawiera następujące części składowe:

- centralę alarmową (a dokładniej jest to płyta główna),
- interfejsy człowiek – SSWiN,
- czujki,
- sygnalizatory i/lub systemy transmisji alarmu,
- układy zasilania (zasilanie podstawowe i rezerwowe).

Wśród wymienionych elementów składowych SSWiN nie znajduje się podsystem diagnostyczny. Stosowanie go jest jednak konieczne gdyż w normie PN-EN 50131-1:2009 zamieszczono informację, że system sygnalizacji włamania i napadu powinien zawierać środki umożliwiające wykrycie zagrożenia, sabotażu i rozpoznania uszkodzeń. Należą do nich m.in.:

- uszkodzenie zasilacza podstawowego,
- uszkodzenia zasilacza rezerwowego,
- uszkodzenie łączności (transmisji komunikatów i/lub sygnałów między elementami składowymi systemu alarmowego),
- uszkodzenie systemu (lub systemów) transmisji alarmu,
- uszkodzenie sygnalizatora (sygnalizatorów).

Powyższe niezdatności są wykrywane przez podsystem diagnostyczny, a następnie informacja ta jest przekazywana do uprawnionych osób (np. użytkownik, GCMA, ARC). W podanej normie wskazane jest także iż dopuszczalne jest by inne rodzaje uszkodzeń były rozpoznawane i obrazowane przez podsystem diagnostyczny. Nie może to jednak niekorzystnie wpływać na rozpoznawanie wymienionych uszkodzeń. Tym samym producenci wyposażają produkowane rozwiązania SSWiN w zaawansowane podsystemy diagnostyczne. Ich zastosowanie umożliwia wykrycie stanów częściowej zdatności czy też stanu niezdatności. Jest to możliwe, gdyż wykorzystywana jest informacja diagnostyczna. Wykorzystanie tej informacji pozwala także na przeprowadzanie racjonalizacji procesu

eksploatacji systemu sygnalizacji włamania i napadu. Rozważania z tego obszaru zamieszczono w niniejszym opracowaniu.

3. Racjonalizacja procesu eksploatacji systemów sygnalizacji włamania i napadu

W procesie eksploatacji systemów sygnalizacji włamania i napadu stosuje się najczęściej działania obsługowe podejmowane kiedy nie wystąpiło uszkodzenie. Jest to określane jako utrzymanie profilaktyczne (PM, ang. *preventive maintenance*). Działania te mają na celu przeprowadzanie obsług zapobiegawczych, które zmniejszą prawdopodobieństwo uszkodzenia lub pogorszania funkcjonowania systemu. W ramach tej strategii wyróżnia się następujące strategie [4,9,16,21]:

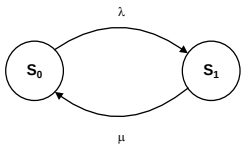
- obsługiwania okresowego,
- obsługiwania według stanu,
- mieszaną,
- według efektywności.

Spośród wymienionych strategii w systemach sygnalizacji włamania i napadu zazwyczaj jest implementowania strategia obsługiwania okresowego, co jest zgodne z wytycznymi podanymi w normie obronnej NO-04-A004-8:2016 Obiekty wojskowe, Systemy Alarmowe, Część 8: Eksploatacja. W ramach tych działań przeprowadzane są czynności obsługowe, które zostały już wcześniej zaplanowane (dotyczy to zarówno ram czasowych, jak też i zakresu czynności). Terminy poszczególnych obsług okresowych są stałe i ustalone m.in. na podstawie wyników wieloletnich badań eksploatacyjnych SSWiN. Jak już wcześniej podano, działania realizowane w ramach tej strategii cechują się tym, że przeprowadza się je w SSWiN charakteryzującymi się różnymi bieżącymi stanami technicznymi. Tym samym wadą tej strategii jest konieczność realizacji wszystkich zaplanowanych obsług okresowych (niezależnie od stanu technicznego systemu sygnalizacji włamania i napadu przy świadomości różnej intensywności oddziaływania czynników środowiskowych).

Rozwinięciem a zarazem też ewolucją działań z zakresu utrzymania profilaktycznego jest opracowanie koncepcji eUtrzymania. Poprzez wdrażanie nowoczesnych rozwiązań w obszarze diagnozowania systemów sygnalizacji włamania i napadu oraz zastosowanie zaawansowanych aplikacji informatycznych możliwe jest ich monitorowane i zarządzanie procesem eksploatacyjnym w czasie rzeczywistym z możliwością obserwowania degradacji SSWiN. Umożliwia to podejmowanie działań zapobiegających przejściu do stanu częściowej zdatności czy niezdatności. W dalszej części niniejszego rozdziału przedstawiono autorski model procesu eksploatacji SSWiN uwzględniający informacje diagnostyczne. Celem przeprowadzonego modelowania procesu eksploatacji systemów sygnalizacji włamania i napadu jest racjonalizacja procesu obsługowego.

Podstawowy model procesu eksploatacji systemów (w tym systemów sygnalizacji włamania i napadu) nie zakłada dokonywania przeglądów okresowych. Naprawa realizowana jest wyłącznie gdy nastąpi jego uszkodzenie [1,2,13]. Takie zarządzanie procesem eksploatacyjnym nie jest stosowane w SSWiN, gdyż wówczas nie byłby zachowany odpowiedni poziom bezpieczeństwa jaki ma być zapewniony w chronionym obiekcie. Niemniej jednak w systemach, które nie pełnią istotnej roli w zapewnieniu

bezpieczeństwa ten model procesu eksploatacji jest stosowany. Jego graficzne zobrazowanie przedstawiono na rys. 1. Wyróżnione są dwa stany: stan użytkowania S_0, stan naprawy S_1.



Rys. 1. Relacje w systemie sygnalizacji włamania i napadu (źródło: opracowanie własne [5]). Oznaczenia na rys.: λ – intensywność uszkodzeń, μ – intensywność napraw.

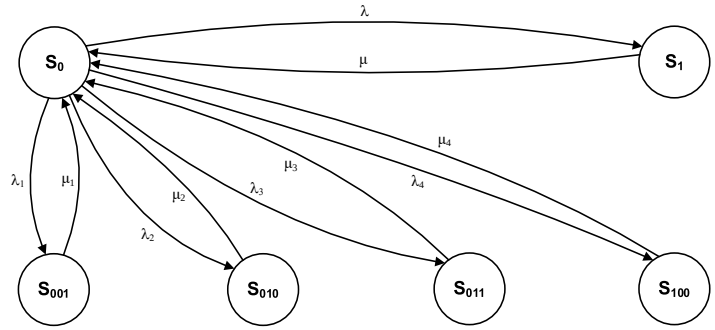
Przeprowadzając analizę matematyczną procesu eksploatacji SSWiN przedstawionego na rys. 1, można wyznaczyć zależności umożliwiające obliczenie wartości prawdopodobieństwa przebywania systemu w wyróżnionych stanach. Dysponując wartością intensywność uszkodzeń i intensywność napraw możliwe jest obliczenie wartości wskaźnika gotowości K_g według wzoru (1):

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

W systemach sygnalizacji włamania i napadu zainstalowanych w obiektach wojskowych proces eksploatacji jest przeprowadzany zgodnie z wytycznymi podanymi w normie obronnej NO-04-A004-8:2016 Obiekty wojskowe, Systemy Alarmowe, Część 8: Eksploatacja. Dla SSWiN wyróżniono cztery rodzaje przeglądów okresowych i są one oznaczane jako przegląd:

– codzienny (oznaczono jako stan S_{001}),
– miesięczny (oznaczono jako stan S_{010}),
– półroczny (oznaczono jako stan S_{011}),
– roczny (oznaczono jako stan S_{100}).

Tym samym graf relacji w systemie sygnalizacji włamania i napadu przedstawiony na rys. 1. ulegnie zmianie, gdyż będą dodane cztery kolejne stany odpowiadające poszczególnym rodzajom przeglądów jakie zostały wymienione powyżej. W sposób graficzny to podejście zastosowane w procesie eksploatacyjnym można zobrazować grafem relacji przedstawionym na rys. 2.



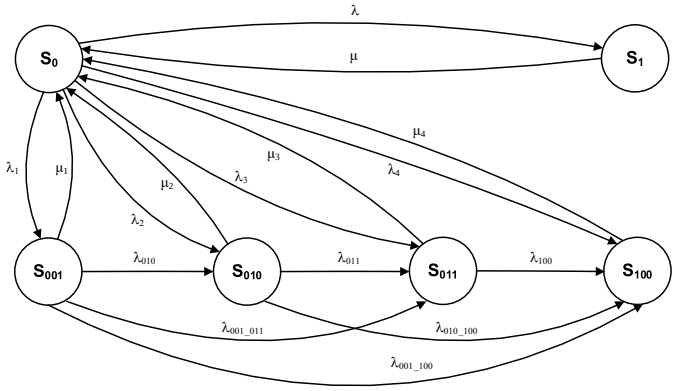
Rys. 2. Graf przejść między stanem użytkowania S_0, naprawy S_1, przeglądu codziennego S_{001}, przeglądu miesięcznego S_{010}, przeglądu półrocznego S_{011} i przeglądu rocznego S_{100} systemu sygnalizacji włamania i napadu (źródło: opracowanie własne [5]). Oznaczenia na rys. 2: λ – intensywność uszkodzeń, μ – intensywność napraw, λ_1 –

intensywność przeglądów codziennych, μ_1 – intensywność obsługiwania eksploatacyjnego codziennego, λ_2 – intensywność przeglądów miesięcznych, μ_2 – intensywność obsługiwania eksploatacyjnego miesięcznego, λ_3 – intensywność przeglądów półrocznych, μ_3 – intensywność obsługiwania eksploatacyjnego półrocznego, λ_4 – intensywność przeglądów rocznych, μ_4 – intensywność obsługiwania eksploatacyjnego rocznego.

Znając wartości intensywności przejść pomiędzy wyróżnionymi stanami przedstawionymi na rys. 2, możliwe jest obliczenie wartości wskaźnika gotowości K_{g1} według wzoru (2):

$$K_{g1} = \frac{\mu \cdot \mu_1 \cdot \mu_2 \cdot \mu_3 \cdot \mu_4}{\mu \cdot \mu_1 \cdot \mu_2 \cdot \mu_3 \cdot \mu_4 + \lambda \cdot \mu_1 \cdot \mu_2 \cdot \mu_3 \cdot \mu_4 + \lambda_1 \cdot \mu \cdot \mu_2 \cdot \mu_3 \cdot \mu_4 + \\ + \lambda_2 \cdot \mu \cdot \mu_1 \cdot \mu_3 \cdot \mu_4 + \lambda_3 \cdot \mu \cdot \mu_1 \cdot \mu_2 \cdot \mu_4 + \lambda_4 \cdot \mu \cdot \mu_1 \cdot \mu_2 \cdot \mu_3} \quad (2)$$

Przeprowadzenie racjonalizacji procesu eksploatacji systemów sygnalizacji włamania i napadu wymaga uwzględnienia nie tylko rzeczywistych warunków środowiskowych występujących w chronionym obiekcie, ale także zmiany w zakresie dopuszczalnych przejść pomiędzy wyróżnionymi stanami. Jedną z istotniejszych zmian jest możliwość rozszerzenia zakresu czynności obsługowych, które to są możliwe dzięki wykorzystaniu informacji diagnostycznych z podsystemu diagnostycznego SSWiN. Tym samym graf relacji w systemie sygnalizacji włamania i napadu przedstawiony na rys. 2. ulegnie zmianie, gdyż będą dodane dodatkowe przejścia pomiędzy stanami oznaczającymi przeglądy okresowe. Zastosowanie dodatkowych przejść pomiędzy wyróżnionymi stanami przeglądów okresowych umożliwi racjonalne dostosowanie obsług okresowych w poszczególnych SSWiN [8]. W sposób graficzny to podejście zastosowane w procesie eksploatacyjnym można zobrazować grafem relacji przedstawionym na rys. 3.



Rys. 3. Graf przejść między stanem użytkowania S_0, naprawy S_1, przeglądu codziennego S_{001}, przeglądu miesięcznego S_{010}, przeglądu półrocznego S_{011} i przeglądu rocznego S_{100} systemu sygnalizacji włamania i napadu z uwzględnieniem przejść pomiędzy stanami przeglądów (źródło: opracowanie własne [8]). Oznaczenia na rys. 3: λ_{010} , λ_{011} , λ_{100} , λ_{001_011} , λ_{010_100} , λ_{001_100} – intensywność przejść pomiędzy stanami oznaczającymi przeglądy okresowe

W celu wyznaczenia prawdopodobieństw przebywania systemu sygnalizacji włamania i napadu w poszczególnych wyróżnionych stanach należy graf przejść przedstawiony na rys. 3 opisać następującymi równaniami:

$$
\begin{aligned}
&-\lambda \cdot P_0 + \mu \cdot P_1 - \lambda_1 \cdot P_0 + \mu_1 \cdot P_{001} - \lambda_2 \cdot P_0 + \mu_2 \cdot P_{010} - \lambda_3 \cdot P_0 + \\
&+\mu_3 \cdot P_{011} - \lambda_4 \cdot P_0 + \mu_4 \cdot P_{100} = 0 \\
&\lambda \cdot P_0 - \mu \cdot P_1 = 0 \\
&\lambda_1 \cdot P_0 - \mu_1 \cdot P_{001} - \lambda_{010} \cdot P_{001} - \lambda_{001\_011} \cdot P_{001} - \lambda_{001\_100} \cdot P_{001} = 0 \\
&\lambda_2 \cdot P_0 - \mu_2 \cdot P_{010} + \lambda_{010} \cdot P_{001} - \lambda_{011} \cdot P_{010} - \lambda_{010\_100} \cdot P_{010} = 0 \\
&\lambda_3 \cdot P_0 - \mu_3 \cdot P_{011} + \lambda_{011} \cdot P_{010} - \lambda_{100} \cdot P_{011} + \lambda_{001\_011} \cdot P_{001} = 0 \\
&\lambda_4 \cdot P_0 - \mu_4 \cdot P_{100} + \lambda_{100} \cdot P_{011} + \lambda_{001\_100} \cdot P_{001} + \lambda_{010\_100} \cdot P_{010} = 0
\end{aligned} \tag{3}
$$

Rozwiązanie układu równań (3) umożliwia wyznaczenie zależności, które mogą zostać wykorzystane w celu obliczenia wartości prawdopodobieństw przebywania SSWiN w wyróżnionych stanach. Zależności te mogą być wykorzystane do zarządzania procesem eksploatacji systemu sygnalizacji włamania i napadu.

Dalsza racjonalizacja procesu eksploatacji systemu sygnalizacji włamania i napadu wymaga wprowadzenia stanu diagnozowania oznaczonego jako S_D. W stanie tym, na podstawie informacji diagnostycznych otrzymywanych z podsystemu diagnostycznego SSWiN, podejmowana jest decyzja o rozszerzeniu zakresu przeglądów okresowych. W sposób graficzny to podejście zastosowane w procesie eksploatacyjnym można zobrazować grafem relacji przedstawionym na rys. 4.

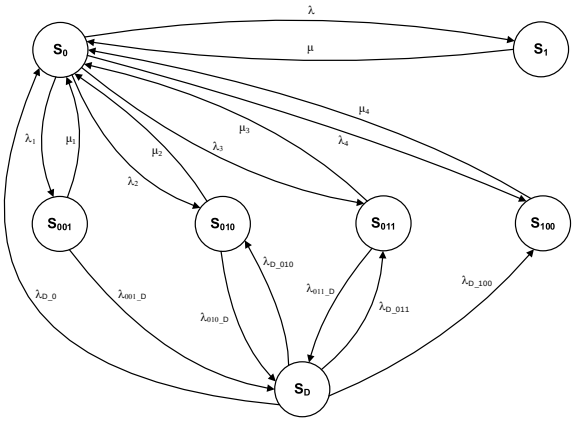
W celu wyznaczenia prawdopodobieństw przebywania systemu sygnalizacji włamania i napadu w poszczególnych wyróżnionych stanach należy graf przejść przedstawiony na rys. 4 opisać następującymi równaniami:

$$
\begin{aligned}
&-\lambda \cdot P_0 + \mu \cdot P_1 - \lambda_1 \cdot P_0 + \mu_1 \cdot P_{001} - \lambda_2 \cdot P_0 + \mu_2 \cdot P_{010} - \lambda_3 \cdot P_0 + \\
&+\mu_3 \cdot P_{011} - \lambda_4 \cdot P_0 + \mu_4 \cdot P_{100} + \lambda_{D\_0} \cdot P_D = 0 \\
&\lambda \cdot P_0 - \mu \cdot P_1 = 0 \\
&\lambda_1 \cdot P_0 - \mu_1 \cdot P_{001} - \lambda_{001\_D} \cdot P_{001} = 0 \\
&\lambda_2 \cdot P_0 - \mu_2 \cdot P_{010} - \lambda_{010\_D} \cdot P_{010} + \lambda_{D\_010} \cdot P_D = 0 \\
&\lambda_3 \cdot P_0 - \mu_3 \cdot P_{011} - \lambda_{011\_D} \cdot P_{011} + \lambda_{D\_011} \cdot P_D = 0 \\
&\lambda_4 \cdot P_0 - \mu_4 \cdot P_{100} + \lambda_{D\_100} \cdot P_D = 0 \\
&-\lambda_{D\_0} \cdot P_D + \lambda_{001\_D} \cdot P_{001} + \lambda_{010\_D} \cdot P_{010} - \lambda_{D\_010} \cdot P_D + \\
&+\lambda_{011\_D} \cdot P_{011} - \lambda_{D\_011} \cdot P_D - \lambda_{D\_100} \cdot P_D = 0
\end{aligned} \tag{4}
$$

Analogicznie jak we wcześniej rozważanych modelach procesu eksploatacji SSWiN, rozwiązanie układu równań (4) umożliwia wyznaczenie zależności, które mogą zostać wykorzystane w celu obliczenie wartości prawdopodobieństw przebywania systemu w wyróżnionych stanach. Zależności te mogą być wykorzystane do racjonalizacji procesem eksploatacji systemu sygnalizacji włamania i napadu.

Spośród prawdopodobieństw przebywania systemu w wyróżnionych stanach, jednym z istotniejszych jest zależność umożliwiająca obliczenie wartości prawdopodobieństwa przebywania SSWiN w stanie użytkowania. W wyniku przeprowadzonych obliczeń, z wykorzystaniem programu Mathematica, wyrażona jest ona następująca zależnością (5). Wykorzystując zależność (5) można przeprowadzić racjonalizację procesu eksploatacji systemu sygnalizacji włamania i napadu.

$$
\begin{aligned}
P_0 = \frac{}{}
&-\left(-\lambda_{001\_D}-\mu_1\right)\cdot\left(\begin{array}{l}-\mu^2\cdot\left(-\lambda_{010\_D}-\mu_2\right)\cdot\mu_3\cdot{\mu_4}^2\cdot\left(\lambda_{D\_010}\cdot\mu\right)\cdot\\ \left(-\lambda_{011\_D}-\mu_3\right)\cdot\mu_4+\left(-\lambda_{010\_D}-\mu_2\right)\cdot\left(\begin{array}{l}\mu\cdot\left(-\lambda_{011\_D}-\mu_3\right)\cdot\\ \left(-\lambda_{D\_100}-\mu_4\right)+\\ +\lambda_{D\_011}\cdot\mu\cdot\mu_4\end{array}\right)\end{array}\right)-\\
&-\mu\cdot\left(-\lambda_{010\_D}-\mu_2\right)\cdot\left(-\lambda_{011\_D}-\mu_3\right)\cdot\mu_4\cdot\\
&\cdot\left(\begin{array}{l}-\lambda_{D\_010}\cdot\left(\mu^2\cdot\mu_2\cdot{\mu_4}^2-\mu^2\cdot\mu_3\cdot{\mu_4}^2\right)+\left(-\lambda_{010\_D}-\mu_2\right)\cdot\\ \cdot\left(\begin{array}{l}\mu^2\cdot\mu_3\cdot\left(-\lambda_{D\_100}-\mu_4\right)\cdot\mu_4-\\ -\mu^2\cdot\mu_4\cdot\left(-\lambda_{D\_0}\cdot\mu_4-\lambda_{D\_100}\cdot\mu_4\right)\end{array}\right)\end{array}\right)\\
&-\lambda_1\cdot\left(-\left(-\lambda_{010\_D}-\mu_2\right)\cdot\left(\begin{array}{l}\mu^2\cdot\mu_1\cdot{\mu_4}^2-\\ -\mu^2\cdot\mu_3\cdot{\mu_4}^2\end{array}\right)\right)\cdot\left(\begin{array}{l}\lambda_{D\_010}\cdot\mu\cdot\left(-\lambda_{011\_D}-\mu_3\right)\cdot\mu_4+\\ +\left(-\lambda_{010\_D}-\mu_2\right)\cdot\left(\begin{array}{l}\mu\cdot\left(-\lambda_{011\_D}-\mu_3\right)\cdot\\ \cdot\left(-\lambda_{D\_100}-\mu_4\right)+\\ +\lambda_{D\_011}\cdot\mu\cdot\mu_4\end{array}\right)\end{array}\right)-\\
&-\mu\cdot\left(-\lambda_{010\_D}-\mu_2\right)\cdot\left(-\lambda_{011\_D}-\mu_3\right)\cdot\mu_4\cdot\left(\begin{array}{l}\\ -\lambda_{D\_010}\cdot\left(\mu^2\cdot\mu_2\cdot{\mu_4}^2-\mu^2\cdot\mu_3\cdot{\mu_4}^2\right)+\\ +\left(-\lambda_{010\_D}-\mu_2\right)\cdot\\ \cdot\left(\begin{array}{l}\mu^2\cdot\mu_3\cdot\left(-\lambda_{D\_100}-\mu_4\right)\cdot\mu_4-\\ -\mu^2\cdot\mu_4\cdot\left(-\lambda_{D\_0}\cdot\mu_4-\lambda_{D\_100}\cdot\mu_4\right)\end{array}\right)\end{array}\right)+\\
&+\left(-\lambda_{001\_D}-\mu_1\right)\cdot\left(\lambda_2\cdot\mu\cdot\left(-\lambda_{011\_D}-\mu_3\right)\cdot\mu_4+\left(-\lambda_{010\_D}-\mu_2\right)\cdot\left(\begin{array}{l}\lambda_3\cdot\mu\cdot\mu_4-\left(-\lambda_{011\_D}-\mu_3\right)\cdot\\ \cdot\left(-\mu\cdot\left(-\lambda_4-\mu_4\right)+\lambda\cdot\mu_4\right)\end{array}\right)\right)\cdot\\
&\cdot\left(\begin{array}{l}\lambda_{010\_D}\cdot\left(\mu^2\cdot\mu_2\cdot{\mu_4}^2-\mu^2\cdot\mu_3\cdot{\mu_4}^2\right)+\\ +\left(-\lambda_{010\_D}-\mu_2\right)\cdot\left(\begin{array}{l}\mu^2\cdot\mu_3\cdot\left(-\lambda_{D\_100}-\mu_4\right)\cdot\mu_4-\\ -\mu^2\cdot\mu_4\cdot\left(-\lambda_{D\_0}\cdot\mu_4-\lambda_{D\_100}\cdot\mu_4\right)\end{array}\right)-\\ -\left(\lambda_{010\_D}\cdot\mu\cdot\left(-\lambda_{011\_D}-\mu_3\right)\cdot\mu_4+\left(-\lambda_{010\_D}-\mu_2\right)\cdot\left(\begin{array}{l}\mu\cdot\left(-\lambda_{011\_D}-\mu_3\right)\cdot\left(-\lambda_{D\_100}-\mu_4\right)+\\ +\lambda_{D\_011}\cdot\mu\cdot\mu_4\end{array}\right)\right)\cdot\\ \cdot\lambda_2\cdot\left(\mu^2\cdot\mu_2\cdot{\mu_4}^2-\mu^2\cdot\mu_3\cdot{\mu_4}^2\right)+\left(-\lambda_{010\_D}-\mu_2\right)\cdot\left(\begin{array}{l}\mu\cdot\mu_3\cdot\mu_4\cdot\left(-\mu\cdot\left(-\lambda_4-\mu_4\right)+\lambda\cdot\mu_4\right)+\\ +\mu\cdot\mu_4\cdot\left(\begin{array}{l}\lambda\cdot\mu\cdot\mu_4-\mu\cdot\\ \cdot\left(-\left(\left(\begin{array}{l}-\lambda-\lambda_1-\lambda_2-\\ -\lambda_3-\lambda_4\end{array}\right)\cdot\mu_4\right)-\right.\\ \left.-\lambda_4\cdot\mu_4\right)\end{array}\right)\end{array}\right)\end{array}\right)
\end{aligned}
\tag{5}
$$



Rys. 4. Graf przejść między stanem użytkowania S_0, naprawy S_1, przeglądu codziennego S_{001}, przeglądu miesięcznego S_{010}, przeglądu półrocznego S_{011} i przeglądu rocznego S_{100} systemu sygnalizacji włamania i napadu z uwzględnieniem przejść pomiędzy stanami przeglądów a stanem diagnozowania (źródło: opracowanie własne). Oznaczenia na rys. 4: λ_{001_D} , λ_{010_D} , λ_{011_D} , λ_{D_010} , λ_{D_011} , λ_{D_100} , λ_{D_0} – intensywność przejść pomiędzy stanami przeglądów okresowych a stanem diagnozowania oraz stanem diagnozowania i stanem użytkowania

4. Wnioski i podsumowanie

W opracowaniu przestawiono problematykę zarządzania procesem eksploatacji systemów sygnalizacji włamania i napadu, jako systemu wchodzącego w skład elektronicznych systemów bezpieczeństwa. Stosowanie tych systemów jest konieczne, by zapewnić odpowiedni poziom bezpieczeństwa w chronionych obiektach transportowych (zwłaszcza tych zaliczanych do infrastruktury krytycznej).

W wyniku przeprowadzonej analizy procesu eksploatacji systemu sygnalizacji włamania i napadu z uwzględnieniem informacji diagnostycznych opracowano graf relacji zachodzących w systemie. Następnie wyznaczono układ równań umożliwiający obliczanie wartości prawdopodobieństw przebywania SSWiN w stanie pełnej zdatności, stanach obsług okresowych, stanach częściowej zdatności i stanie niezdatności. Umożliwia to m.in. racjonalizację intensywności realizacji przeglądów okresowych.

Przedstawione przez autorów zagadnienia modelowania procesu eksploatacji systemów sygnalizacji włamania i napadu z wykorzystaniem informacji diagnostycznych otrzymywanych z podsystemu diagnostycznego umożliwiają racjonalizację intensywności realizacji przeglądów okresowych. Efektem tego będzie zwiększenie wartości wskaźnika gotowości SSWiN, co jest szczególnie istotne w przypadku zabezpieczania obiektów transportowych. Zasadne jest także zastosowanie przedstawionych rozważań z obszaru racjonalizacji procesu eksploatacji także do innych urządzeń i systemów (w szczególności elektronicznych w których dostępne są informacje diagnostyczne).

Bibliografia

1. Będkowski, L., Dąbrowski, T. (2006). Podstawy eksploatacji, cz. II Podstawy niezawodności eksploatacyjnej, Wojskowa Akademia Techniczna.

2. Dyduch. J., Paś. J., Rosiński. A. (2011). Podstawy eksploatacji transportowych systemów elektronicznych, Wydawnictwo Politechniki Radomskiej.
3. Fischer, R.J., Halibozek, E.P., Walters, D.C. (2019). Introduction to Security, Butterworth-Heinemann.
4. Grabski, F. (2015). Semi-Markov Processes: Applications in System Reliability and Maintenance, Elsevier.
5. Nowakowski, T., Siergiejczyk, M. (red.). (2022). Inżynieria niezawodności - teoria i praktyka. 50 lat Zimowych Szkół Niezawodności, Oficyna Wydawnicza Politechniki Warszawskiej.
6. Kierzkowski, A., Kisiel, T., Uchroński, P. (2021). Simulation Model of Airport Security Lanes with Power Consumption Estimation, Energies, 14, 6725.
7. Klimczak, T., Paś, J. (2018). Podstawy eksploatacji systemów sygnalizacji pożarowej w obiektach transportowych, Wojskowa Akademia Techniczna.
8. Łukasiak, J., Rosiński, A., Wiśnios, M. (2022). Problematyka racjonalizacji procesu eksploatacji systemów sygnalizacji włamania i napadu, w: Ciszewski, T., Wojciechowski, J. (red.), Współczesne wyzwania transportu i elektrotechniki, Uniwersytet Technologiczno-Humanistyczny im. Kazimierza Pułaskiego w Radomiu.
9. Młyńczak, M., Nowakowski, T., Werbińska-Wojciechowska, S. (2014). Klasyfikacja modeli utrzymania systemów technicznych, w: Siergiejczyk, M. (red.), Problemy utrzymania systemów technicznych, Oficyna Wydawnicza Politechniki Warszawskiej.
10. Norma Obronna NO-04-A004-8:2016. Obiekty wojskowe, Systemy Alarmowe, Część: 8 Eksploatacja.
11. Paś, J., Buchla, S. (2019). Analysis of the Electronic Device Exploitation Process - Research Results, Journal of KONBiN, 49.
12. Paś, J., Buchla, S. (2019). Exploitation of Electronic Devices - Selected Issues, Journal of KONBiN, 49.
13. Paś, J. (2023). Eksploatacja elektronicznych systemów bezpieczeństwa, Wojskowa Akademia Techniczna, Warszawa.
14. Paś, J., Rosiński, A., Wiśnios, M., Majda-Zdancewicz, E., Łukasiak, J. (2018). Elektroniczne systemy bezpieczeństwa. Wprowadzenie do laboratorium, Wojskowa Akademia Techniczna.
15. PN-EN 50131-1:2009 - Systemy alarmowe - Systemy sygnalizacji włamania i napadu - Część 1: Wymagania systemowe.
16. Rosiński, A. (2015). Modelowanie procesu eksploatacji systemów telematyki transportu, Oficyna Wydawnicza Politechniki Warszawskiej.
17. Rządowe Centrum Bezpieczeństwa. (2020). Narodowy program ochrony infrastruktury krytycznej – tekst jednolity.
18. Rządowe Centrum Bezpieczeństwa. (2020). Narodowy program ochrony infrastruktury krytycznej. Załącznik 1: Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje.
19. Siergiejczyk, M., Krzykowska, K., Rosiński, A. (2017). Reliability-exploitation analysis of electronic power systems used for airport security, w: Čepin, M., Briš, R. (red.), Safety and Reliability – Theory and Applications, CRC Press Taylor & Francis Group.
20. Stawowy, M. (2019). Metoda wielowarstwowego modelowania niepewności w szacowaniu jakości informacji systemów teleinformatycznych w transporcie, Oficyna Wydawnicza Politechniki Warszawskiej.
21. Werbińska-Wojciechowska, S. (2019). Technical system maintenance: delay-time-based modelling, Springer.

Racjonalizacja procesu eksploatacji systemów sygnalizacji włamania i napadu

Streszczenie: Systemy Sygnalizacji Włamania i Napadu (SSWiN) wchodzą w skład elektronicznych systemów bezpieczeństwa. Są one obecnie instalowane w wielu obiektach, w tym także tych zaliczanych do infrastruktury krytycznej. Różnorodność dostępnych central alarmowych i ich konfiguracji powoduje, że instalowane są SSWiN z zastosowaniem central alarmowych o różnych możliwościach funkcjonalnych i diagnostycznych. W procesie eksploatacji systemów sygnalizacji włamania i napadu stosuje się najczęściej działania obsługowe podejmowane kiedy nie wystąpiło uszkodzenie. Jest to określane jako utrzymanie profilaktyczne. Działania te mają na celu przeprowadzanie obsług zapobiegawczych, które zmniejszą prawdopodobieństwo uszkodzenia lub pogorszania funkcjonowania systemu. Rozwinięciem a zarazem też ewolucją działań z zakresu utrzymania profilaktycznego jest opracowanie koncepcji eUtrzymania. Poprzez wdrażanie nowoczesnych rozwiązań w obszarze diagnozowania systemów sygnalizacji włamania i napadu oraz zastosowanie zaawansowanych aplikacji informatycznych możliwe jest ich monitorowane i zarządzanie procesem eksploatacyjnym w czasie rzeczywistym z możliwością obserwowania degradacji SSWiN. Umożliwia to podejmowanie działań zapobiegających przejściu do stanu częściowej zdatności czy niezdatności. W wyniku przeprowadzonej analizy procesu eksploatacji systemu sygnalizacji włamania i napadu z uwzględnieniem informacji diagnostycznych opracowano graf relacji zachodzących w systemie. Następnie wyznaczono zależności umożliwiające obliczanie wartości prawdopodobieństw przebywania SSWiN w stanie pełnej zdatności, stanach obsług okresowych, stanach częściowej zdatności i stanie niezdatności. Przedstawione przez autorów zagadnienia modelowania procesu eksploatacji systemów sygnalizacji włamania i napadu umożliwiają racjonalizację intensywności realizacji przeglądów okresowych. Efektem tego jest zwiększenie wartości wskaźnika gotowości SSWiN, co jest szczególnie istotne w przypadku zabezpieczania obiektów infrastruktury krytycznej.
Słowa kluczowe: system sygnalizacji włamania i napadu, eksploatacja, modelowanie