Wybrane zagadnienia analizy niezawodnościowej rozproszonych systemów alarmowych

Mirosław Siergiejczyk, Adam Rosiński
Politechnika Warszawska, Wydział Transportu, Zakład Telekomunikacji w Transporcie, ul. Koszykowa 75, 00-662 Warszawa

Waldemar Szulc
Wyższa Szkoła Menedżerska w Warszawie, Wydział Menedżerski i Nauk Technicznych, ul. Kawęczyńska 36, 03-772 Warszawa

Streszczenie: Systemy sygnalizacji włamania i napadu wchodzą w skład elektronicznych systemów alarmowych. Są instalowane w wielu obiektach infrastruktury krytycznej państwa. Jedną z grup obiektów wymagających szczególnej ochrony są obiekty transportowe, zarówno stacjonarne jak i ruchome. Wytyczne zawarte w normie PN-EN 50131-1:2009 określają wymagania funkcjonalne. Do obowiązków producenta urządzeń i projektanta należy takie zaprojektowanie systemu alarmowego, by realizował cele, dla których został zainstalowany. Jednocześnie eksploatowany system powinien charakteryzować się wskaźnikami niezawodnościowo-eksploatacyjnymi o odpowiednich wartościach. W artykule przedstawiono rozważania z tego zakresu, przy czym szczególną uwagę zwrócono na prawdopodobieństwa przebywania systemu w wyróżnionych stanach.

Keywords: niezawodność, eksploatacja, system bezpieczeństwa, system sygnalizacji włamania i napadu, PN-EN 50131-1:2009, infrastruktura krytyczna

1. Wprowadzenie

Wymóg zapewnienia odpowiedniego poziomu bezpieczeństwa w obiektach publicznych jest bardzo istotny. Z tego względu Rządowe Centrum Bezpieczeństwa opracowało dokument *Narodowy Program Ochrony Infrastruktury Krytycznej* obowiązujący w Rzeczypospolitej Polskiej. Wymieniono w nim 11 systemów, które są zaliczane do infrastruktury krytycznej państwa [11]:
- zaopatrzenia w energię, surowce energetyczne i paliwa,
- łączności,
- sieci teleinformatycznych,
- finansowe,
- zaopatrzenia w żywność,
- zaopatrzenia w wodę,
- ochrony zdrowia,
- transportowe,
- ratownicze,
- zapewniające ciągłość działania administracji publicznej,
- produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

Autor korespondujący:
Adam Rosiński,adro@wt.pw.edu.pl

Artykuł recenzowany
nadesłany 11.08.2017 r., przyjęty do druku 22.09.2017 r.

Prawidłowe funkcjonowanie wymienionych systemów jest niezbędne dla zapewnienia ciągłości funkcjonowania struktur administracyjnych kraju. Takie podejście umożliwia zapewnienie określonego poziomu bezpieczeństwa obywateli. Wśród wymienionych systemów jednym z istotniejszych jest transport. W skład niego zaliczono [11]:
- transport kolejowy,
- transport samochodowy,
- transport lotniczy,
- transport rurociągowy,
- żeglugę śródlądową,
- żeglugę morską.

Aby zapewnić bezpieczeństwo osobom korzystającym ze środków transportowych i przewożonym towarom, wymaga się zagwarantowania odpowiedniego poziomu bezpieczeństwa obiektom transportowym. Z tego też względu stosuje się w transportowych obiektach (zarówno stacjonarnych [4, 16, 22] jak i ruchomych [5]) systemy ochrony elektronicznej. Zwiększają one poziom bezpieczeństwa w chronionych obszarach. W skład tych systemów zaliczamy:
- system sygnalizacji włamania i napadu (SSWiN),
- system sygnalizacji pożaru,
- system kontroli dostępu,
- system monitoringu wizyjnego,
- system ochrony terenów zewnętrznych.

Ochrona wynikająca z funkcjonowania tych systemów, dość często jest uzupełniana przez systemy:
- sygnalizacji stanu zdrowia lub zagrożenia osobistego,
- sygnalizacji zagrożeń środowiska,
- przeciwkradzieżowe,
- dźwiękowe systemy ostrzegawcze,
- zabezpieczenia samochodów przed włamaniem i uprowadzeniem.

Odpowiedni poziom bezpieczeństwa, jaki mają zapewnić obiektom transportowym systemy ochrony elektronicznej, zależy nie tylko od skuteczności zastosowanych poszczególnych systemów [18], ale także od prawidłowego ich zaprojektowania i uwzględnienia wytycznych zawartych w odpowiednich normach. Jednym z ważniejszych dokumentów jest norma PN-EN 50131-1:2009 *Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Część 1: Wymagania systemowe*. Zawiera one szczegółowe wytyczne dotyczące wymagań SSWiN. W dokumencie tym nie uwzględniono bezpośrednio wytycznych z zakresu niezawodności i eksploatacji, ale są one częściowo opisane przy poszczególnych aspektach projektowania (np. wymagania odnośnie zasilania podstawowego i rezerwowego).

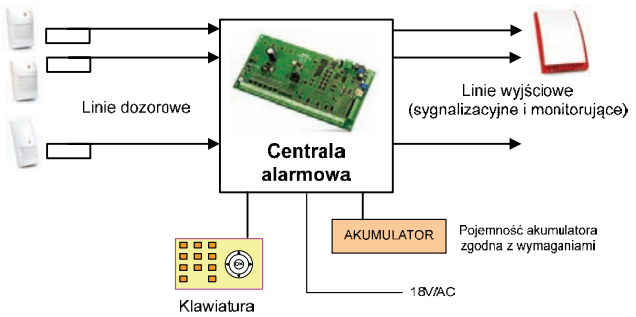
Systemy sygnalizacji włamania i napadu stosowane w obiektach infrastruktury krytycznej, a w szczególności w obiektach transportowych, powinny cechować się spełnieniem wielu specyficznych wymagań. Do najważniejszych z nich można zaliczyć m.in. dużą efektywność funkcjonowania i wykrycia zagrożeń (w szczególności związanych z aktami terrorystycznymi), miniaturyzację, odpowiednie wartości wskaźników niezawodnościowo-eksploatacyjnych [12, 15], możliwość diagnozowania podsystemów z uwzględnieniem jakości informacji [17], odporność na zakłócenia elektromagnetyczne [6, 13, 14] i wibracje [2]. Spełnienie tych oczekiwań wymaga opracowania wiarygodnych modeli niezawodnościowo-eksploatacyjnych tych systemów. Z tego względu w artykule zaprezentowano rozważania z tego obszaru.

2. Charakterystyka wybranych struktur SSWiN

Zaprojektowanie oraz realizacja systemu sygnalizacji włamania i napadu dla dużego i rozległego obiektu transportowego wymaga wiedzy technicznej oraz znacznego doświadczenia. Jednym z głównych kryteriów uwzględnianych na początku procesu projektowania SSWiN jest określenie stopnia zabezpieczenia, który ma wpływ na dobór struktur systemu i urządzeń. W normie PN-EN 50131-1:2009 (jest to wprowadzenie normy EN 50131-1:2006 *Alarm systems – Intrusion and hold-up systems – Part 1: System requirements* opracowanej przez European Committee for Electrotechnical Standardization CENELEC) wyróżniono następujące cztery stopnie zabezpieczenia [8]:

- stopień 1: Ryzyko małe (zakłada się, że intruz będzie miał niewielką wiedzę na temat systemu alarmowego i posiadał łatwo dostępne narzędzia w ograniczonym wyborze),
- stopień 2: Ryzyko małe do średniego (zakłada się, że intruz będzie miał niewielką wiedzę na temat systemu alarmowego i posiadał ogólnodostępne narzędzia i przenośne urządzenia, np. pomiarowe),
- stopień 3: Ryzyko średnie do wysokiego (zakłada się, że intruz będzie znał biegle system alarmowy i posiadał zestawy zaawansowanych narzędzi i przenośnego sprzętu elektronicznego),
- stopień 4: Ryzyko wysokie (ma zastosowanie, gdy bezpieczeństwo ma priorytet nad wszystkimi innymi czynnikami; zakłada się, że intruz będzie posiadał zdolności i/lub środki by szczegółowo zaplanować włamanie i posiadał zestaw dowolnego sprzętu, łącznie ze środkami do zastąpienia kluczowych elementów elektronicznego systemu alarmowego).

Po przyjęciu przez projektanta określonego stopnia zabezpieczenia, jaki SSWiN ma spełniać, dobierane są urządzenia, które umożliwiają realizację przyjętych wymagń. Najważniejszym elementem systemu sygnalizacji włamania i napadu jest płyta główna centrali alarmowej. Ona decyduje o możliwościach funkcjonalnych całego projektowanego systemu. Obecnie jest to najczęściej mikroprocesorowa centrala alarmowa (CA). Do niej dołączone są poszczególne linie dozorowe, na których są umieszczone czujki wykrywające zagrożenia. Do CA dołączone są także linie wyjściowe, na których są umieszczone sygnalizatory i/lub systemy transmisji alarmu. Komunikacja między SSWiN a użytkowaniem (wcześniej instalatorem) odbywa się przez interfejsy człowiek-system (np. klawiatury, piloty bezprzewodowe, aplikacje zainstalowane w komputerze lub smartfonie). Takie rozwiązania SSWiN mają w małych obiektach strukturę skupioną, czyli wszystkie urządzenia końcowe są podłączone bezpośrednio do płyty głównej centrali alarmowej [18] (rys. 1).



Rys. 1. System sygnalizacji włamania i napadu o strukturze skupionej
Fig. 1. Compact Intrusion Alarm System

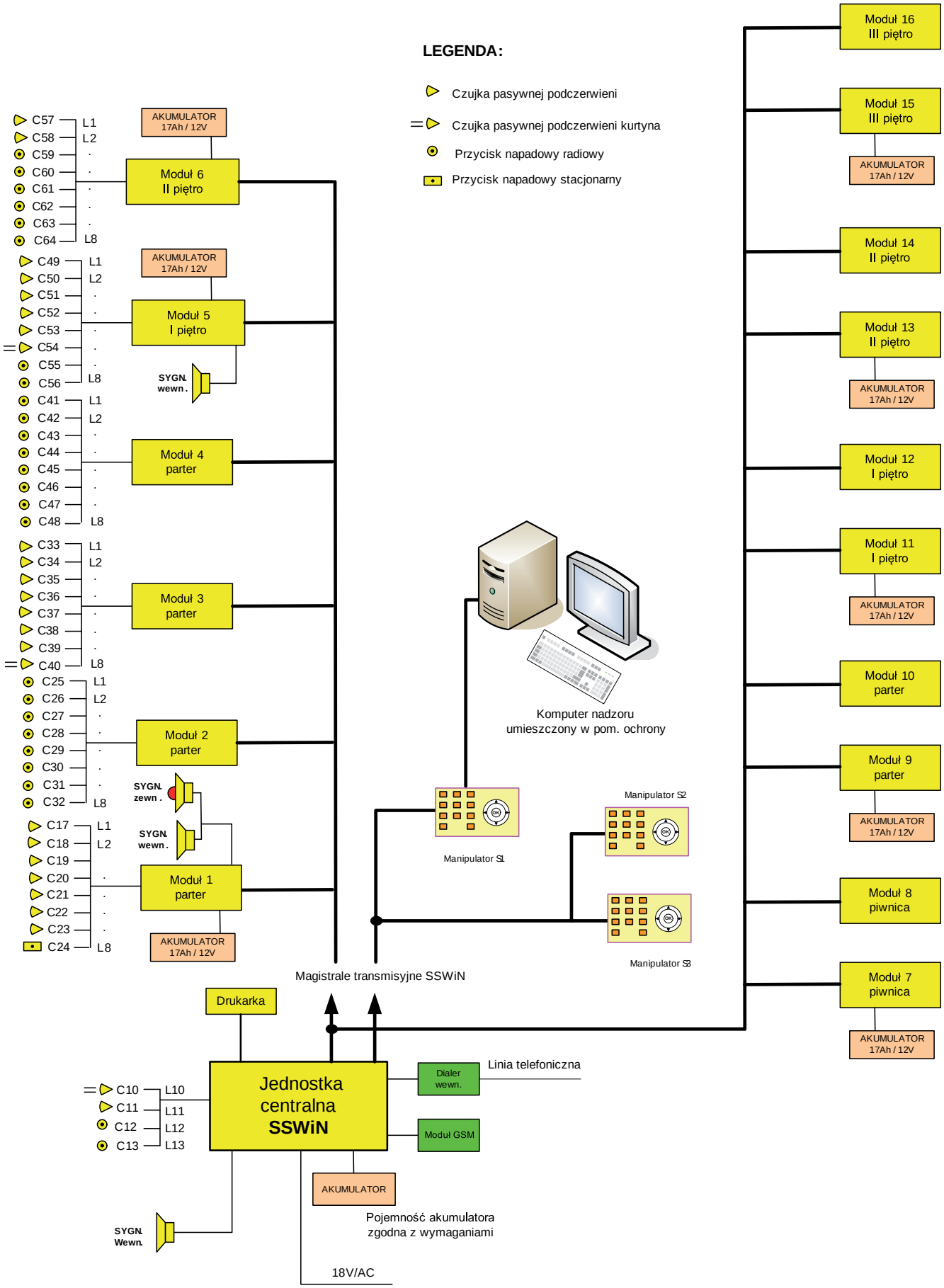
W obiektach transportowych system sygnalizacji włamania i napadu o strukturze skupionej nie jest popularny ze względu na fakt, iż liczba linii dozorowych nie przekracza najczęściej 16. Ponieważ obiekty transportowe charakteryzują się dużą rozległością terytorialną, to wymagają SSWiN o strukturze rozproszonej. W tego rodzaju systemach stosuje się cyfrowe magistrale transmisyjne, do których są podłączone moduły realizujące określone funkcje (np. rozszerzeniowe wejść, rozszerzeniowe wyjść, podcentrale, konwertery interfejsów). Obecnie dane między centralą alarmową a poszczególnymi modułami są najczęściej przesyłane z zastosowaniem zmodyfikowanego formatu transmisji RS-485 lub zbliżonego, który jest opracowany przez producenta.

Przedstawiony na rys. 2 schemat systemu sygnalizacji włamania i napadu w wersji rozproszonej, jest stosowany najczęściej do obiektów transportowych, które wymagają dużej liczby linii dozorowych (przeważnie powyżej 32). Zazwyczaj kilka linii dozorowych (4–16) doprowadza się bezpośrednio do listwy łączeniowej płyty głównej centrali alarmowej. Są na nich umieszczone czujki usytuowane najbliżej centrali alarmowej. Pozostałe czujki są dołączone do modułów rozszerzeniowych wejściowych (przeważnie 8-wejściowych).

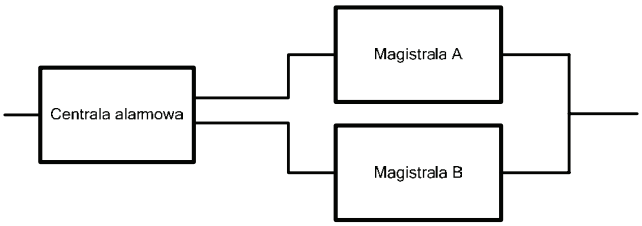
Duża różnorodność central alarmowych i ich konfiguracji powoduje, iż projektanci realizują SSWiN z zastosowaniem różnych struktur niezawodnościowych (szeregowe, szeregowo-równoległe, równoległe) [1, 21]. Konieczna jest analiza porównawcza tego typu rozwiązań, która umożliwi stosowanie racjonalnych wariantów dla założonych kryteriów wyboru.

3. Analiza niezawodnościowa SSWiN w wersji rozproszonej

Analizując strukturę i funkcjonowanie systemu sygnalizacji włamania i napadu (rys. 2) można stwierdzić, iż ma on strukturę niezawodnościową typu szeregowo-równoległego [3, 7, 10] (rys. 3). Uszkodzenie centrali alarmowej skutkuje niezdatnością systemu. Uszkodzenie jednej z magistral transmisyjnych skutkuje stanem niezdatności części systemu, a dokładniej modułów znajdujących się na danej magistrali.

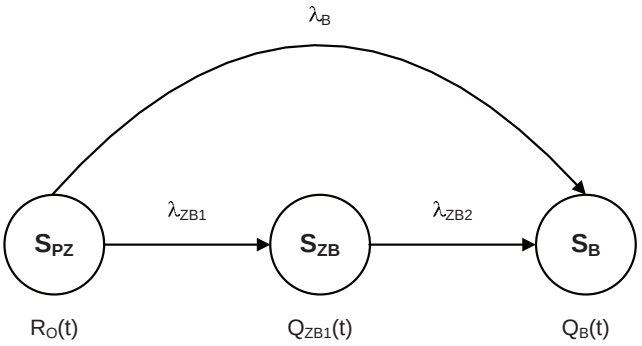


Rys. 2. System sygnalizacji włamania i napadu o strukturze rozproszonej
Fig. 2. Distributed Intrusion Alarm System



Rys. 3. Struktura niezawodnościowa SSWiN z dwoma magistralami transmisyjnymi
Fig. 3. Reliability structure of SSWiN with two transmission lines

W wyniku analizy rzeczywistych systemów sygnalizacji włamania i napadu i ich struktury niezawodnościowej (rys. 3), autorzy zaproponowali graf relacji zachodzących w rozproszonym systemie alarmowym. Relacje zachodzące w systemie dla rzeczywistego obiektu zostały przedstawione na rys. 4.



$R_O(t)$ – funkcja prawdopodobieństwa przebywania systemu w stanie pełnej zdatności S_{PZ}
$Q_{ZB}(t)$ – funkcja prawdopodobieństwa przebywania systemu w stanie zagrożenia bezpieczeństwa S_{ZB}
$Q_B(t)$ – funkcja prawdopodobieństwa przebywania systemu w stanie zawodności bezpieczeństwa S_B
λ_B – intensywność przejścia centrali alarmowej
λ_{ZB1}, λ_{ZB2} – intensywność przejść magistrali (odpowiednio A i B)

Rys. 4. Relacje zachodzące w SSWiN
Fig. 4. Relations in SSWiN

Stosując przekształcenia matematyczne [9] otrzymuje się zależności, które umożliwiają wyznaczenie wartości prawdopodobieństw przebywania rozważanego systemu sygnalizacji włamania i napadu w wyróżnionych stanach:
– stan pełnej zdatności S_{PZ}

$$R_0(t) = e^{-(\lambda_B+\lambda_{ZB1})\cdot t} \tag{1}$$

– stan zagrożenia bezpieczeństwa S_{ZB}

$$Q_{ZB1}(t) = \lambda_{ZB1} \cdot \left[\frac{e^{-(\lambda_B+\lambda_{ZB1})\cdot t} - e^{-\lambda_{ZB2}\cdot t}}{\lambda_{ZB2} - \lambda_B - \lambda_{ZB1}}\right] \tag{2}$$

– stan zawodności bezpieczeństwa S_B

$$Q_B(t) = \frac{\lambda_B}{\lambda_B + \lambda_{ZB1}} \cdot \left[1 - e^{-(\lambda_B+\lambda_{ZB1})\cdot t}\right] + \lambda_{ZB1} \cdot \lambda_{ZB2} \cdot \cdot \left[\frac{e^{-(\lambda_B+\lambda_{ZB1})\cdot t}}{(\lambda_B+\lambda_{ZB1})(\lambda_B+\lambda_{ZB1}-\lambda_{ZB2})} - \frac{e^{-\lambda_{ZB2}\cdot t}}{(\lambda_B+\lambda_{ZB1}-\lambda_{ZB2})\lambda_{ZB2}} + \frac{1}{(\lambda_B+\lambda_{ZB1})\lambda_{ZB2}}\right] \tag{3}$$

Przykład

Korzystając z zależności (1–3) dokonano symulacji obliczeniowej dla następujących wartości wejściowych:
– czas obserwacji systemu – 1 rok = 8760 godz.,
– liczba badanych systemów: 100 (o strukturze z rys. 3),
– podczas obserwacji stwierdzono, że uszkodzeniu uległy:
  – centrala – 1 szt.,
  – moduły rozszerzające magistrali A – 3 szt.,
  – moduły rozszerzające magistrali B – 2 szt.

Ponieważ stosowane są urządzenia elektroniczne [19, 20], to założono wykładniczy rozkład czasu zdatności.

Otrzymano następujące wartości prawdopodobieństw przebywania systemu w:
– stanie pełnej zdatności R_O: 0,9603
– stanie zagrożenia bezpieczeństwa Q_{ZB1}: 0,02955
– stanie zawodności bezpieczeństwa Q_B: 0,01015

Powyższe wartości zostały obliczone na podstawie równań (1–3) z wykorzystaniem autorskiego programu komputerowego *Wspomaganie Decyzji Niezawodnościowo-Eksploatacyjnych Transportowych Systemów Nadzoru*.

4. Podsumowanie i wnioski

W artykule zaprezentowano zagadnienia dotyczące analizy niezawodnościowej systemów sygnalizacji włamania i napadu. Scharakteryzowano SSWiN o strukturze skupionej i rozproszonej, przy czym uwzględniono zarówno wymagania zawarte w normie PN-EN 50131-1:2009, jak i doświadczenia autorów związane z projektowaniem i eksploatacją systemów alarmowych. Szczególną uwagę zwrócono na system o strukturze rozproszonej z dwoma magistralami transmisyjnymi. Tego typu rozwiązanie jest bardzo często stosowane w zabezpieczeniu rozproszonych obiektów transportowych. Przeprowadzone rozważania niezawodnościowe pozwoliły na otrzymanie zależności umożliwiających wyznaczenie wartości prawdopodobieństw przebywania rozważanego SSWiN odpowiednio w stanach: pełnej zdatności, zagrożenia bezpieczeństwa i zawodności bezpieczeństwa. Praktyczne zastosowanie otrzymanych rozwiązań umożliwia porównanie systemów już na etapie projektowania i wybór określonego (przy przyjętych kryteriach wyboru). W dalszych rozważaniach planuje się uwzględnienie czynności obsługowych przywracających zdatność systemu.

Bibliografia

1. Będkowski L., Dąbrowski T., *Podstawy eksploatacji*, cz. II *Podstawy niezawodności eksploatacyjnej*. Wojskowa Akademia Techniczna, Warszawa 2006.
2. Burdzik R., Konieczny Ł., *Research on structure, propagation and exposure to general vibration in passenger car for different damping parameters*. "Journal of Vibroengineering", Vol. 15, Iss. 4, 2013, 1680–1688.
3. Dyduch J., Paś J., Rosiński A., *Podstawy eksploatacji transportowych systemów elektronicznych*. Wydawnictwo Politechniki Radomskiej, Radom 2011.
4. Kierzkowski A., Kisiel T., *Airport security screeners reliability analysis*. [in:] "Proceedings of the IEEE International Conference on Industrial Engineering and Engineering Management IEEM 2015", Singapore 2015, 1158–1163, DOI: 10.1109/IEEM.2015.7385830.
5. Łubkowski P, Laskowski D., *Selected issues of reliable identification of object in transport systems using video monitoring services*. [in:] „Communication in Computer

and Information Science", editor: J. Mikulski, Springer, 2015, Vol. 471, 59–68, DOI: 10.1007/978-3-662-45317-9_7.
6. Paś J., Siergiejczyk M., *Interference impact on the electronic safety system with a parallel structure*. "Diagnostyka", Vol. 17, No. 1, 2016, 49–55.
7. Paś J., *Eksploatacja elektronicznych systemów transportowych*. Uniwersytet Technologiczno-Humanistyczny, Radom 2015.
8. PN-EN 50131-1:2009 – Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Część 1: Wymagania systemowe.
9. Rosiński A., *Metoda wyboru strategii eksploatacji w transportowych systemach nadzoru*. Rozprawa doktorska, Politechnika Warszawska, Warszawa 2006.
10. Rosiński A., *Modelowanie procesu eksploatacji systemów telematyki transportu*. Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2015.
11. Rządowe Centrum Bezpieczeństwa, *Narodowy program ochrony infrastruktury krytycznej*. Załącznik 1: Charakterystyka systemów infrastruktury krytycznej, Warszawa 2013.
12. Siergiejczyk M., Krzykowska K., Rosiński A., *Reliability assessment of integrated airport surface surveillance system*. [in:] „Proceedings of the Tenth International Conference on Dependability and Complex Systems DepCoS-RELCOMEX", „Advances in intelligent systems and computing", Vol. 365. Springer 2015, 435–443, DOI: 10.1007/978-3-319-19216-1_41.
13. Siergiejczyk M., Paś J., Rosiński A., *Issue of reliability–exploitation evaluation of electronic transport systems used in the railway environment with consideration of electromagnetic interference*. "IET Intelligent Transport Systems", Vol. 10, Iss. 9, 2016, 587–593, DOI: 10.1049/iet-its.2015.0183.
14. Siergiejczyk M., Rosiński A., *Reliability analysis of electronic protection systems using optical links*. [in:] Zamojski W., Kacprzyk J., Mazurkiewicz J., Sugier J., Walkowiak T. (eds), „Dependable Computer Systems", „Advances in intelligent and soft computing", Vol. 97. Springer-Verlag, Berlin Heidelberg 2011, DOI: 10.1007/978-3-642-21393-9_15.
15. Siergiejczyk M., Rosiński A., Krzykowska K., *Reliability assessment of supporting satellite system EGNOS*. [in:] Zamojski W., Mazurkiewicz J., Sugier J., Walkowiak T., Kacprzyk J. (eds), "New results in dependability and computer systems", „Advances in intelligent and soft computing", Vol. 224. Springer, 2013. 353–364, DOI: 10.1007/978-3-319-00945-2_32.
16. Skorupski J., Uchroński P., *A fuzzy reasoning system for evaluating the efficiency of cabin luggage screening at airports*. "Transportation Research Part C – Emerging Technologies", Vol. 54, 2015, 157–175, DOI: 10.1016/j.trc.2015.03.017.
17. Stawowy M., Dziula P., *Comparison of uncertainty multilayer models of impact of teleinformation devices reliability on information quality*. [in:] "Proceedings of the European Safety and Reliability Conference ESREL 2015", Podofillini L., Sudret B., Stojadinovic B., Zio E., Kröger W. (eds), CRC Press/Balkema, 2015, 2685–2691, DOI: 10.1201/b19094-351.
18. Szulc W., Rosiński A., *Systemy sygnalizacji włamania. Część 1 – Konfiguracje central alarmowych*. Zabezpieczenia, Nr 2(66)/2009, wyd. AAT, Warszawa 2009.
19. Szulc W., Rosiński A., *Wybrane zagadnienia z elektroniki cyfrowej dla informatyków* (część II – cyfrowa). Wydawnictwo Wyższej Szkoły Menedżerskiej w Warszawie, Warszawa 2012.
20. Szulc W., Rosiński A., *Wybrane zagadnienia z miernictwa i elektroniki dla informatyków* (część I – analogowa). Oficyna Wydawnicza WSM, Warszawa 2012.
21. Szulc W., *Struktura niezawodnościowo-eksploatacyjna elektronicznego systemu bezpieczeństwa*. „Pomiary Automatyka Robotyka", R. 19, Nr 1, 2015, 65-70, DOI: 10.14313/PAR_215/65.
22. Wiśnios M., Dąbrowski T., Bednarek M., *Metoda zwiększania poziomu bezpieczeństwa zapewnianego przez system biometrycznej kontroli dostępu*. „Przegląd Elektrotechniczny", R. 91, Nr 10, 2015, 229–232.

Selected Issues of Reliability Analysis of Distributed Alarm Systems

Abstract: Intruder Alarm Systems are part of electronic alarm systems. They are currently installed in many important state infrastructure facilities. One such group of objects requiring special protection are transport objects, both stationary and mobile. The guidelines included in the standard PN-EN 50131-1: 2009 "Alarm systems – Intruder alarm systems – System requirements" define the functional requirements. As far as the device manufacturer and designer are concerned, the alarm system should be designed to meet the objectives for which it was installed. At the same time the exploited system should have appropriate values of reliability and operational indicators. This article is a review of the distributed alarm systems, with particular attention paid to the probability of staying in particular states.

Keywords: reliability, exploitation, security systems, intrusion and hold-up systems, PN-EN 50131-1:2009, critical infrastructure

prof. nzw. dr hab. inż. Mirosław Siergiejczyk
msi@wt.pw.edu.pl

Zainteresowania naukowe obejmują m.in. problemy architektury i usług systemów i sieci telekomunikacyjnych ze szczególnym uwzględnieniem możliwości ich wykorzystania w transporcie, niezawodności i eksploatacji systemów i sieci teleinformatycznych, modelowanie, projektowanie i organizacja sieci i systemów teleinformatycznych w transporcie.

doc. dr inż. Waldemar Szulc
waldemar.szulc@mac.edu.pl

Zainteresowania naukowe obejmują elektronikę analogową i cyfrową oraz elektroniczne systemy bezpieczeństwa obiektów. Jest autorem lub współautorem ponad 10 patentów oraz autorem lub współautorem 52 wdrożeń urządzeń elektronicznych. W dorobku naukowym posiada ponad 150 publikacji. Jest autorem lub współautorem wielu unikalnych rozwiązań z dziedziny bezpieczeństwa obiektów o charakterze specjalnym.

prof. nzw. dr hab. inż. Adam Rosiński
adro@wt.pw.edu.pl

Zainteresowania naukowe obejmują analizę niezawodnościowo-eksploatacyjną systemów telematyki transportu, inteligentnych systemów transportowych oraz elektronicznych systemów bezpieczeństwa (m.in. systemy sygnalizacji włamania i napadu, systemy monitoringu wizyjnego, systemy kontroli dostępu). W dorobku naukowym posiada kilkadziesiąt publikacji naukowych.