Jarosław Łukasiak, Adam Rosiński

Analiza niezawodnościowa wybranych struktur SSWiN

JEL: L94 DOI: 10.24136/atest.2018.446
Data zgłoszenia: 19.11.2018 Data akceptacji: 15.12.2018

Systemy Sygnalizacji Włamania i Napadu (SSWiN) wchodzą w skład elektronicznych systemów bezpieczeństwa. Są one obecnie instalowane w wielu obiektach, które można zaliczyć do obiektów o szczególnym znaczeniu. Różnorodność dostępnych central alarmowych i ich konfiguracji powoduje, że projektanci opracowują projekty SSWiN z zastosowaniem różnych struktur niezawodnościowych. W artykule zaprezentowano zagadnienia dotyczące analizy niezawodnościowej systemów sygnalizacji włamania i napadu.

Słowa kluczowe: niezawodność, eksploatacja, system sygnalizacji włamania i napadu, projektowanie.

Wstęp

W normie PN-EN 50131-1:2009 „Systemy alarmowe - Systemy sygnalizacji włamania i napadu - Wymagania systemowe" [15], która jest tożsama z normą europejską EN 50131-1:2006 „Alarm systems – Intrusion and hold-up systems – Part 1: System requirements", przedstawiony jest wykaz elementów składowych, które powinien zawierać System Sygnalizacji Włamania i Napadu (SSWiN). Należą do nich następujące urządzenia:

- centrala alarmowa,
- jedna lub więcej czujek,
- jeden lub więcej sygnalizatorów i/lub systemów transmisji alarmu,
- zasilacz podstawowy,
- zasilacz rezerwowy.

Wymienione urządzenia są wykorzystywane w projektach, aby SSWiN poprawnie funkcjonował i realizował cele, które mu wyznaczono. Oczywiście w celu prawidłowego zabezpieczenia obiektu, oprócz wspomnianego systemu należy także rozważyć instalację systemu kontroli dostępu [22] oraz systemu monitoringu wizyjnego [6].

Połączenia pomiędzy poszczególnymi urządzeniami SSWiN powinny spełniać określone wymagania zawarte zarówno w normach, jak i podane przez producenta [2]. Z tego też względu są produkowane różnego rodzaju systemy, które spełniają wymagania zawarte w normie PN-EN 50131-1:2009 „Systemy alarmowe - Systemy sygnalizacji włamania i napadu - Wymagania systemowe" odnośnie stopnia zabezpieczenia. Wyróżnia się następujące cztery poziomy [15]:

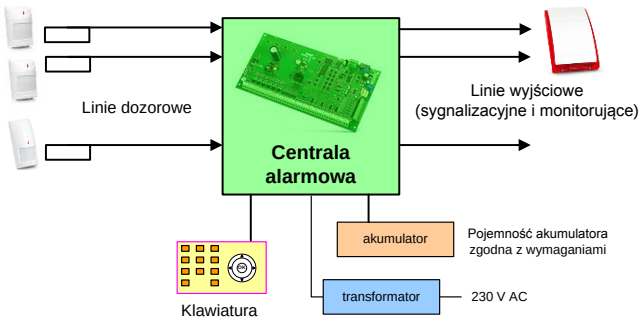
- stopień 1: Ryzyko małe (zakłada się, że intruz ma minimalną wiedzę na temat systemu alarmowego i posiada łatwo dostępne narzędzia w ograniczonym wyborze),
- stopień 2: Ryzyko małe do średniego (zakłada się, że intruz ma minimalną wiedzę na temat systemu alarmowego i posiada ogólnodostępne narzędzia i przenośne urządzenia, np. multimetr),
- stopień 3: Ryzyko średnie do wysokiego (zakłada się, że intruz zna biegle system alarmowy oraz posiada złożony zestaw zaawansowanych narzędzi i przenośnego sprzętu elektronicznego),
- stopień 4: Ryzyko wysokie (ma zastosowanie, gdy bezpieczeństwo ma priorytet nad wszystkimi innymi czynnikami. Zakłada się, że intruz posiada zdolności bądź środki by szczegółowo zaplanować włamanie i dysponuje zestawem dowolnego sprzętu, łącznie ze środkami do zastąpienia kluczowych elementów elektronicznego systemu alarmowego).

Po określeniu stopnia zabezpieczenia jaki system sygnalizacji włamania i napadu ma spełniać, projektant dobiera urządzenia, które spełniają założone wymagania.

Systemy sygnalizacji włamania i napadu są to systemy, których celem jest wykrywanie zagrożeń występujących w chronionych obszarach. Funkcjonują one w zróżnicowanych warunkach eksploatacyjnych [12,13,18]. Ich poprawne działanie jest uzależnione m.in. od niezawodności poszczególnych części składowych tworzących system [5,11]. Dlatego niezbędne jest przeprowadzenie analizy struktur niezawodnościowych tych systemów, a następnie określenie ich wpływu na poziom niezawodności całego rozpatrywanego SSWiN. Przegląd literaturowy stanu zagadnienia pozwolił stwierdzić, iż obecne wytyczne z zakresu niezawodności i eksploatacji SSWiN są niewystarczające. Zarówno zalecenia zawarte w normach dostępnych w Polskim Komitecie Normalizacyjnym, oraz normach obronnych opracowanych przez Wojskowe Centrum Normalizacji, Jakości i Kodyfikacji, jak również w wytycznych producentów i przepisach branżowych, z zakresu niezawodności i obsługiwania nie wyczerpują w dostatecznym zakresie zagadnień eksploatacyjnych systemów SWiN. Nie uwzględniają one m.in. intensywności użytkowania poszczególnych elementów systemów co w konsekwencji powoduje, że nie ma możliwości uzyskania optymalnych wskaźników niezawodnościowo-eksploatacyjnych [4,9]. Dlatego też istnieje potrzeba przeprowadzenia analizy niezawodnościowej wybranych struktur SSWiN. Takie podejście przedstawiono w niniejszym artykule.

1.Przegląd wybranych struktur SSWiN

Jednym z najczęściej instalowanych w małych obiektach jest system sygnalizacji włamania i napadu o strukturze skupionej [19]. W takim systemie wszystkie linie dozorowe i linie wyjściowe są dołączone bezpośrednio do płyty głównej centrali alarmowej (rys. 1).



Rys. 1. System sygnalizacji włamania i napadu o strukturze skupionej [źródło: opracowanie własne]

Systemy sygnalizacji włamania i napadu o strukturze skupionej nie są instalowane w obiektach rozległych terytorialnie, ponieważ wymagało by to dużej liczby mediów transmisyjnych (w niniejszym artykule rozważane są tylko systemy przewodowe). Dlatego też w dużych obiektach stosuje się SSWiN o strukturze rozproszonej

[8,10,14]. W tego rodzaju rozwiązaniach tylko część linii dozorowych i wyjściowych wprowadzanych jest bezpośrednio do centrali alarmowej. Pozostałe linie wejściowe/wyjściowe są dołączone do SSWiN poprzez dodatkowe moduły rozszerzające. Moduły te są dołączone do centrali alarmowej poprzez magistrale transmisyjne [20,21].

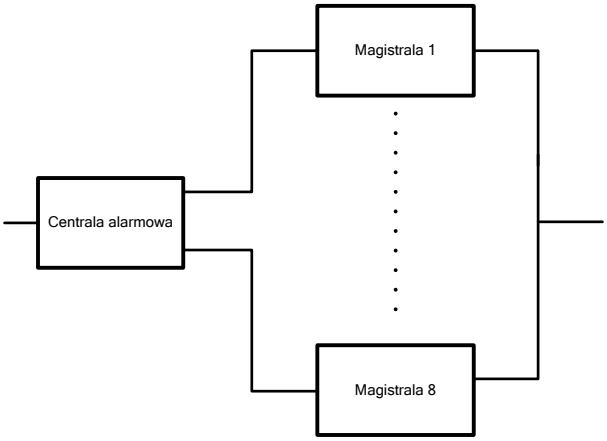
Na rys. 2 przedstawiono system sygnalizacji włamania i napadu o strukturze rozproszonej. Tego rodzaju SSWiN instaluje się w obiektach, które wymagają dużej liczby linii dozorowych (powyżej 16). Zwykle kilkanaście linii dozorowych (najczęściej do 16) wprowadza się bezpośrednio do listwy łączeniowej płyty głównej centrali alarmowej. Pozostałe linie dołączone są do modułów rozszerzeniowych wejściowych (przeważnie o 8 lub 16 wejściach). Linie wyjściowe w tym systemie mogą być dołączone bezpośrednio do wyjść płyty głównej lub do modułów rozszerzających wyjściowych.

Przedstawiony na rys. 2 SSWiN posiada 8 magistral transmisyjnych, do których można dołączać moduły zwiększające funkcjonalność systemu. Tego typu rozwiązania są stosowne m.in. w zabezpieczaniu obiektów specjalnych.

Najistotniejszym elementem SSWiN przedstawionego na rys. 2 jest mikroprocesorowa centrala alarmowa. Jej właściwości decydują o możliwościach sprzętowych i programowych, a także o parametrach niezawodnościowych systemu. Zaprezentowany system ma możliwość dołączenia modułów do max. 8 magistral transmisyjnych. Przedstawiony SSWiN posiada otwartą architekturę sprzętową i programową. Umożliwia to rozbudowę systemu w przyszłości, adekwatnie do zmieniających się potrzeb użytkownika i funkcji chronionego obiektu, bez konieczności wymiany wszystkich urządzeń.

2.Analiza niezawodnościowa 8-magistralowego systemu sygnalizacji włamania i napadu

Analizując strukturę i funkcjonowanie [7,17] systemu sygnalizacji włamania i napadu przedstawionego na rys. 2, można stwierdzić iż ma on szeregowo-równoległą strukturę niezawodnościową [1,3]. Schemat tej struktury jest przedstawiony na rys. 3. Uszkodzenie centrali alarmowej skutkuje niezdatnością systemu. Uszkodzenie którejś z magistral transmisyjnych, skutkuje stanem niezdatności części systemu, a dokładniej modułów znajdujących się na danej magistrali [16].



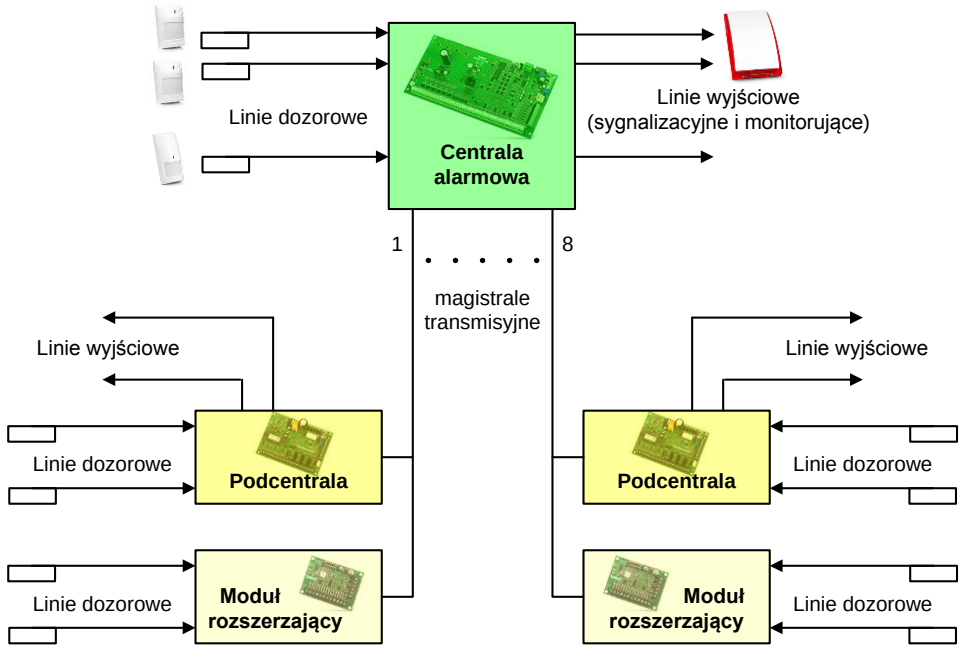
Rys. 3. Struktura niezawodnościowa SSWiN z ośmioma magistralami [źródło: opracowanie własne]

W celu przeprowadzenia obliczeń posłużono się autorskim (opracowanym przez jednego z autorów niniejszego artykułu) programem o nazwie ,,Wspomaganie Decyzji Niezawodnościowo-Eksploatacyjnych Transportowych Systemów Nadzoru" (rys. 4). Umożliwia on użytkownikom transportowych systemów nadzoru zarządzanie procesem eksploatacyjno-niezawodnościowym.

Przykład symulacyjny

Obliczenia przeprowadzono dla następujących wartości wejściowych:

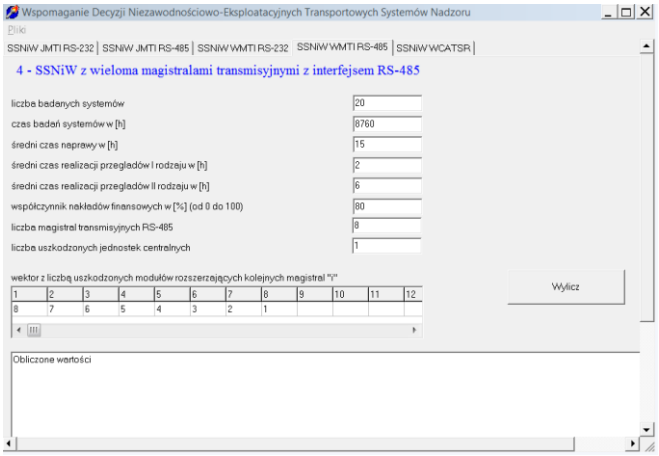
- Czas obserwacji systemu – 1 rok = 8760 godz.,
- Liczba badanych systemów: 20 (o strukturze takiej jak przedstawiona na rys. 2),
- Podczas obserwacji stwierdzono, że uszkodzeniu uległy:
- centrala - 1 szt.,
- moduły rozszerzające magistrali 1 - 8 szt.,
- moduły rozszerzające magistrali 2 - 7 szt.,
- moduły rozszerzające magistrali 3 - 6 szt.,
- moduły rozszerzające magistrali 4 - 5 szt.,



Rys. 2. System sygnalizacji włamania i napadu o strukturze rozproszonej 8-magistralowej [źródło: opracowanie własne]

– moduły rozszerzające magistrali 5 - 4 szt.,
– moduły rozszerzające magistrali 6 - 3 szt.,
– moduły rozszerzające magistrali 7 - 2 szt.,
– moduły rozszerzające magistrali 8 - 1 szt.

Ponieważ stosowane są urządzenia elektroniczne, to założono wykładniczy rozkład czasu zdatności.



Rys. 4. Widok okna programu ,,Wspomaganie Decyzji Niezawodnościowo-Eksploatacyjnych Transportowych Systemów Nadzoru" [źródło: opracowanie własne]

Otrzymano następujące wartości prawdopodobieństw przebywania systemu w:

– stanie pełnej zdatności R0: 0,57
– stanie zagrożenia bezpieczeństwa QZB1: 0,31115
– stanie zagrożenia bezpieczeństwa QZB2: 0,07022
– stanie zagrożenia bezpieczeństwa QZB3: 0,00869
– stanie zagrożenia bezpieczeństwa Q_{ZB4}: 0,00064
– stanie zagrożenia bezpieczeństwa QZB5: 0,00003
– stanie zagrożenia bezpieczeństwa Q_{ZB6}: 0,0000008
– stanie zagrożenia bezpieczeństwa Q_{ZB7}: 0,00000001
– stanie zawodności bezpieczeństwa Q_B: 0,0392

Powyższe wartości zostały obliczone z wykorzystaniem autorskiego programu komputerowego ,,Wspomaganie Decyzji Niezawodnościowo-Eksploatacyjnych Transportowych Systemów Nadzoru". Zostały one także zobrazowane w programie (rys. 5).

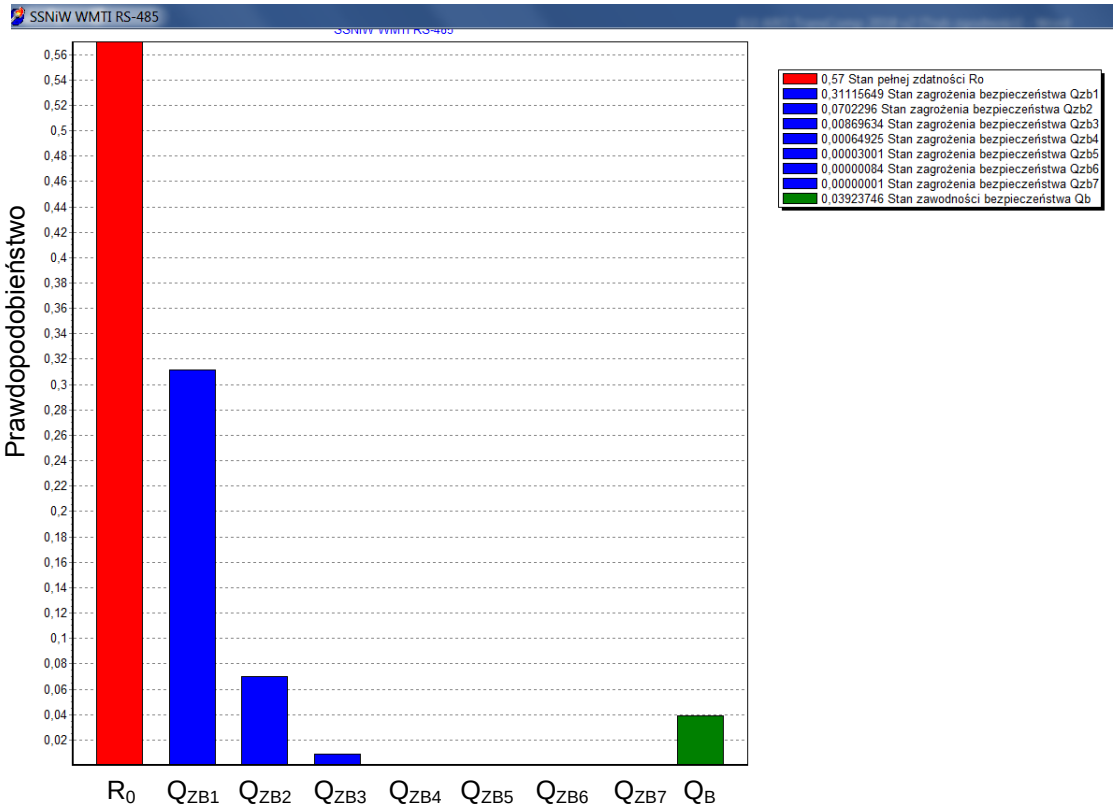
Analizując otrzymane wartości prawdopodobieństw przebywania systemu sygnalizacji włamania i napadu w wyróżnionych stanach można uznać, iż wartość R_0=0,57 jest niewystarczająca dla obiektów specjalnych. Jednakże należy także w rozważaniach uwzględniać wartości dla stanów Q_{ZB1} , Q_{ZB2} , Q_{ZB3} , Q_{ZB4} , Q_{ZB5} , Q_{ZB6} , Q_{ZB7} i Q_B wówczas można przyjąć, że:

$$R_{0(całk)} = R_0+Q_{ZB1}+Q_{ZB2}+Q_{ZB3}+Q_{ZB4}+Q_{ZB5}+Q_{ZB6}+Q_{ZB7}=0,96076254$$

Otrzymana wartość $R_{0(całk)}$ jest znacząco większa od R_0 i można uznać ją za wartość uwzględnianą podczas rozważań z punktu widzenia całego SSWiN.

Podsumowanie

W artykule zaprezentowano zagadnienia dotyczące analizy niezawodnościowej systemów sygnalizacji włamania i napadu o strukturze rozproszonej. Dokonano przeglądu stosowanych struktur SSWiN, zaś następnie poddano szczegółowej analizie system o strukturze rozproszonej z ośmioma magistralami transmisyjnymi. Tego typu rozwiązania są szczególnie korzystne w zastosowaniach dla rozległych obiektów o charakterze specjalnym. Przeprowadzone rozważania niezawodnościowe umożliwiły obliczenie wartości prawdopodobieństw przebywania rozważanego systemu sygnalizacji włamania i napadu w odpowiednich stanach: pełnej zdatności, zagrożenia bezpieczeństwa i zawodności bezpieczeństwa. Zapro-



Rys. 5. Graficzne przedstawienie prawdopodobieństw przebywania SSWiN w stanach R_O, Q_{ZB1} , Q_{ZB2} , Q_{ZB3} , Q_{ZB4} , Q_{ZB5} , Q_{ZB6} , Q_{ZB7} i Q_B [źródło: opracowanie własne]

ponowane podejście w analizie SSWiN może zostać zastosowane do oceny i porównań różnego rodzaju rozwiązań.

Bibliografia:

1. Będkowski L., Dąbrowski T., Podstawy eksploatacji, cz. II Podstawy niezawodności eksploatacyjnej, Wojskowa Aka-demia Techniczna, Warszawa 2006.
2. Dabrowski T., Bednarek M., Fokow K., Wisnios M., The method of threshold-comparative diagnosing insensitive on disturbances of diagnostic signals, "Przeglad Elektrotechniczny - Electrical Review", 88(11A), 2012, pp. 93-97.
3. Dąbrowski T., Paś J., Olchowik W., Rosiński A., Wiśnios M., Podstawy eksploatacji systemów. Laboratorium, Wojskowa Akademia Techniczna, Warszawa 2014.
4. Dyduch J., Paś J., Rosiński A., Podstawy eksploatacji transportowych systemów elektronicznych, Wydawnictwo Politechniki Radomskiej, Radom 2011.
5. 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, pp. 1158-1163.
6. 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, vol. 471. Springer, Berlin Hedelberg 2015, pp. 59-68.
7. Łukasiak J., Rosiński A., Analysis of exploitation process in the aspect of readiness of electronic protection systems, "Diagnostyka", 2017, vol. 18, no. 4, pp. 37-42.
8. Łukasiak J., Rosiński A., Graphic keypad in intrusion and hold-up alarm systems, "Biuletyn Wojskowej Akademii Technicznej", 2017, vol. LXVI, nr 4, Warszawa 2017, pp. 215-224, DOI: 10.5604/01.3001.0010.8363.
9. Paś J., Eksploatacja elektronicznych systemów transportowych, Uniwersytet Technologiczno - Humanistyczny, Radom 2015.
10. Paś J., Rosiński A., Wiśnios M., Berczyński R., Stanowisko badawczo-dydaktyczne Systemu Sygnalizacji Włamania i Napadu, „Logistyka", nr 6/2014, wyd. Instytut Logistyki i Magazynowania, Poznań 2014.
11. Paś J., Rosiński A., Wiśnios M., Majda-Zdancewicz E., Łukasiak J., Elektroniczne systemy bezpieczeństwa. Wprowadzenie do laboratorium, Wojskowa Akademia Techniczna, Warszawa 2018.
12. Paś J., Rosiński A., Selected issues regarding the reliability-operational assessment of electronic transport systems with regard to electromagnetic interference, "Eksploatacja i Niezawodnosc – Maintenance and Reliability", 2017, 19(3), pp. 375–381, DOI: 10.17531/ein.2017.3.8.
13. Paś J., Shock a disposable time in electronic security systems, „Journal of KONBiN", 2016, nr 2(38).
14. Paś J., Siergiejczyk M., Interference impact on the electronic safety system with a parallel structure, „Diagnostyka", 2016, vol. 17, no. 1.
15. PN-EN 50131-1:2009 - Systemy alarmowe - Systemy sygnalizacji włamania i napadu - Część 1: Wymagania systemowe.
16. Rosiński A., Modelowanie procesu eksploatacji systemów telematyki transportu, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2015.
17. Siergiejczyk M., Krzykowska K., Rosiński A., Reliability-exploitation analysis of electronic power systems used for airport security, in: „Safety and Reliability – Theory and Applications", editors: M. Čepin & R. Briš, CRC Press Taylor & Francis Group, London 2017, pp. 649-654.
18. 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", 2016, vol. 10, issue 9, pp. 587–593.
19. Szulc W., Rosiński A., Systemy sygnalizacji włamania. Część 1 – Konfiguracje central alarmowych, "Zabezpieczenia", nr 2(66)/2009, wyd. AAT, Warszawa 2009.
20. Szulc W., Rosiński A., Wybrane zagadnienia z elektroniki cyfrowej dla informatyków (część II – cyfrowa), Wydawnictwo Wyższej Szkoły Menedżerskiej w Warszawie, Warszawa 2012.
21. Szulc W., Rosiński A., Wybrane zagadnienia z miernictwa i elektroniki dla informatyków (część I – analogowa), Oficyna Wydawnicza WSM, Warszawa 2012.
22. Wiśnios M., Dąbrowski T., Bednarek M., Metoda zwiększania poziomu bezpieczeństwa zapewnianego przez system biometrycznej kontroli dostępu, „Przegląd Elektrotechniczny", 2015, nr 10, str. 229-232.

Reliability analysis of selected I&HAS structures

Intrusion and hold-up alarm systems (I&HAS for short) can be classified as belonging to the group of electronic security systems. They are currently installed in many special-purpose objects. The variety of available control panels and their many possible configurations causes designers to develop I&HAS projects that take into account various reliability structures. The article presents issues that concern the reliability analysis of intrusion and hold-up alarm systems.

Keywords: reliability, exploitation, intrusion and hold-up systems, projects.

Autorzy:

mgr inż. **Jarosław Łukasiak** – Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego, Wydział Elektroniki, Instytut Systemów Elektronicznych, Zakład Eksploatacji Systemów Elektronicznych, 00-908 Warszawa, ul. Gen. Witolda Urbanowicza 2, jaroslaw.lukasiak@wat.edu.pl

dr hab. inż. **Adam Rosiński** – Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego, Wydział Elektroniki, Instytut Systemów Elektronicznych, Zakład Eksploatacji Systemów Elektronicznych, 00-908 Warszawa, ul. Gen. Witolda Urbanowicza 2, adam.rosinski@wat.edu.pl