ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 2013
Seria: TRANSPORT z. 81 Nr kol. 1896

Mirosław SIERGIEJCZYK, Adam ROSIŃSKI

DIAGNOSTYKA SYSTEMÓW BEZPIECZEŃSTWA STOSOWANYCH W TRANSPORCIE

Streszczenie. W transporcie, jako rozległym systemie, problem zapewnienia bezpieczeństwa publicznego jest zagadnieniem szczególnie istotnym [1]. Dotyczy ono nie tylko obiektów stacjonarnych (np. stacje kolejowe, porty lotnicze), ale także środków transportowych (pociągi, elektryczne zespoły trakcyjne, autobusy, metro) [14]. Dlatego też stosuje się różnego typu systemy bezpieczeństwa [9,11,12,13], w tym m.in. Systemy Sygnalizacji Włamania i Napadu (SSWiN). Przedstawiono stanowisko laboratoryjne, które pozwala na przeprowadzenie określonych czynności diagnostycznych SSWiN. Można to realizować zarówno lokalnie, z wykorzystaniem komputera z odpowiednim oprogramowaniem, który jest podłączony do systemu poprzez port RS-232 lub USB, bądź zdalnie, poprzez wykorzystanie określonych sieci telekomunikacyjnych (np. cyfrowa telefonia komórkowa GSM lub sieć komputerowa z protokołem TCP/IP).

Słowa kluczowe. Bezpieczeństwo, diagnostyka, systemy sygnalizacji.

DIAGNOSTIC OF SECURITY SYSTEMS USED IN TRANSPORT

Summary. In transport, as a large system, problem of public safety is an issue of particular importance. It applies not only to stationary objects (such as railway stations, airports), but also to the means of transport (trains, electric multiple units, buses, metro). Therefore, there are used various types of safety systems, including Intruder Alarms System (IAS). The paper presents the laboratory stand, which allows to perform specific diagnostics operations of IAS. This can be done either locally using a PC with the appropriate software, which is connected to the system via RS-232 or USB port, or remotely through the use of certain telecommunications networks (e.g. GSM digital mobile telephony or computer network with protocol TCP/IP).

Keywords. Safety, diagnosis, alarms system.

1. WPROWADZENIE

System pełnej sygnalizacji zagrożeń (tzw. ochrony elektronicznej) tworzy się z następujących systemów, wyróżnianych zależnie od wykrywanych zagrożeń [4] jako systemy:

- Sygnalizacji Włamania i Napadu (SSWiN),
- sygnalizacji pożaru,
- kontroli dostępu,

- monitoringu wizyjnego [3],
- ochrony terenów zewnętrznych.

Ochrona wynikająca z działania tych systemów może być uzupełniona przez systemy:
- sygnalizacji stanu zdrowia lub zagrożenia osobistego,
- sygnalizacji zagrożeń środowiska,
- przeciwkradzieżowe,
- dźwiękowe systemy ostrzegawcze,
- zabezpieczenia samochodów przed włamaniem i uprowadzeniem.

Istotnym elementem systemów alarmowych są systemy transmisji alarmu, stanowiące urządzenia albo sieci do przekazywania informacji o stanie jednego lub więcej systemów alarmowych do jednego lub kilku alarmowych centrów odbiorczych.

Norma europejska EN 50131-1:2006 „Alarm systems – Intrusion and hold-up systems – Part 1: System requirements", która ma jednocześnie status Polskiej Normy PN-EN 50131-1:2009 „Systemy alarmowe - Systemy sygnalizacji włamania i napadu - Wymagania systemowe" [6], zawiera wskazania dotyczące uszkodzeń systemu. Podaje ona definicje i skróty, m.in.:
- stan uszkodzenia: stan systemu alarmowego uniemożliwiający normalne działanie systemu alarmowego sygnalizacji włamania lub jego części,
- sygnał/komunikat uszkodzenia: informacja wytwarzana wskutek uszkodzenia.

Podane definicje określają stan systemu, w którym to SSWiN nie w pełnym zakresie spełnia stawiane mu wymagania dotyczące zapewnienia ochrony osób i mienia. Taki stan jest niedopuszczalny z punktu widzenia użytkownika systemu, ale nie jest możliwe całkowite wyeliminowanie go spośród stanów eksploatacyjnych, które mogą wystąpić w rzeczywistych warunkach pracy. Poprzez informacje otrzymywane z podsystemów diagnostycznych możliwe jest jednak szybkie zareagowanie na powstałą sytuację i podjęcie odpowiednich działań zmierzających do usunięcia uszkodzenia i jednocześnie przywrócenia stanu zdatności systemu. Jednocześnie osoba dokonująca naprawy ma ułatwione zadanie w poszukiwaniu miejsca uszkodzenia, a także uzyskuje w pewnym stopniu (zależnie od zastosowanego podsystemu diagnostycznego) wiedzę dotyczącą rodzaju i zakresu uszkodzenia.

2. PODSYSTEMY DIAGNOSTYCZNE W SSWIN

Koncepcja zastosowania podsystemów diagnostycznych w Systemach Sygnalizacji Włamania i Napadu wymaga od projektanta uwzględnienia następujących kwestii z zakresu funkcjonowania układów diagnostycznych i charakteru ich pracy [10]:
- czy będą mierzone wielkości ciągłe czy dyskretne (a może oba rodzaje),
- jak będzie dokonywana akwizycja mierzonych wartości [5],
- czy będzie zastosowany układ decyzyjny ułatwiający wnioskowanie diagnostyczne,
- jak będą prezentowane wyniki pomiarów.

Można tak zaprojektować podsystem diagnostyczny, aby realizował wiele więcej funkcji niż te, które wymieniono. Istotnym kryterium są tu koszty przyjętego rozwiązania. Zaletą podsystemów rozbudowanych jest to, iż znacznie obniżają one koszty eksploatacji poprzez [10]:

- zmniejszenie kosztów związanych z diagnostyką systemów (np. możliwe jest zdalne wykonanie tej czynności poprzez wykorzystanie sieci WAN 1, LAN 2, GSM 3 czy telefonicznej [7]),
- zmniejszenie czasów przeglądów okresowych dzięki zautomatyzowaniu procesu diagnostycznego,
- zwiększenie liczby informacji diagnostycznych, a tym samym zwiększenie zakresu badań diagnostycznych i wiarygodności postawionych hipotez,
- zmniejszenie liczby personelu diagnostycznego (jeśli zastosowano zdalną diagnostykę),
- dostarczenie informacji o rodzaju uszkodzenia, a tym samym szybsze określenie jego miejsca (szczególnie istotne w przypadku SSWiN o strukturze rozproszonej).

Na rys. 1 przedstawiono schemat Systemu Sygnalizacji Włamania i Napadu o strukturze mieszanej [8], który został zaprojektowany i zrealizowany z wykorzystaniem mikroprocesorowej centrali alarmowej INTEGRA. Składa się on m.in. z:

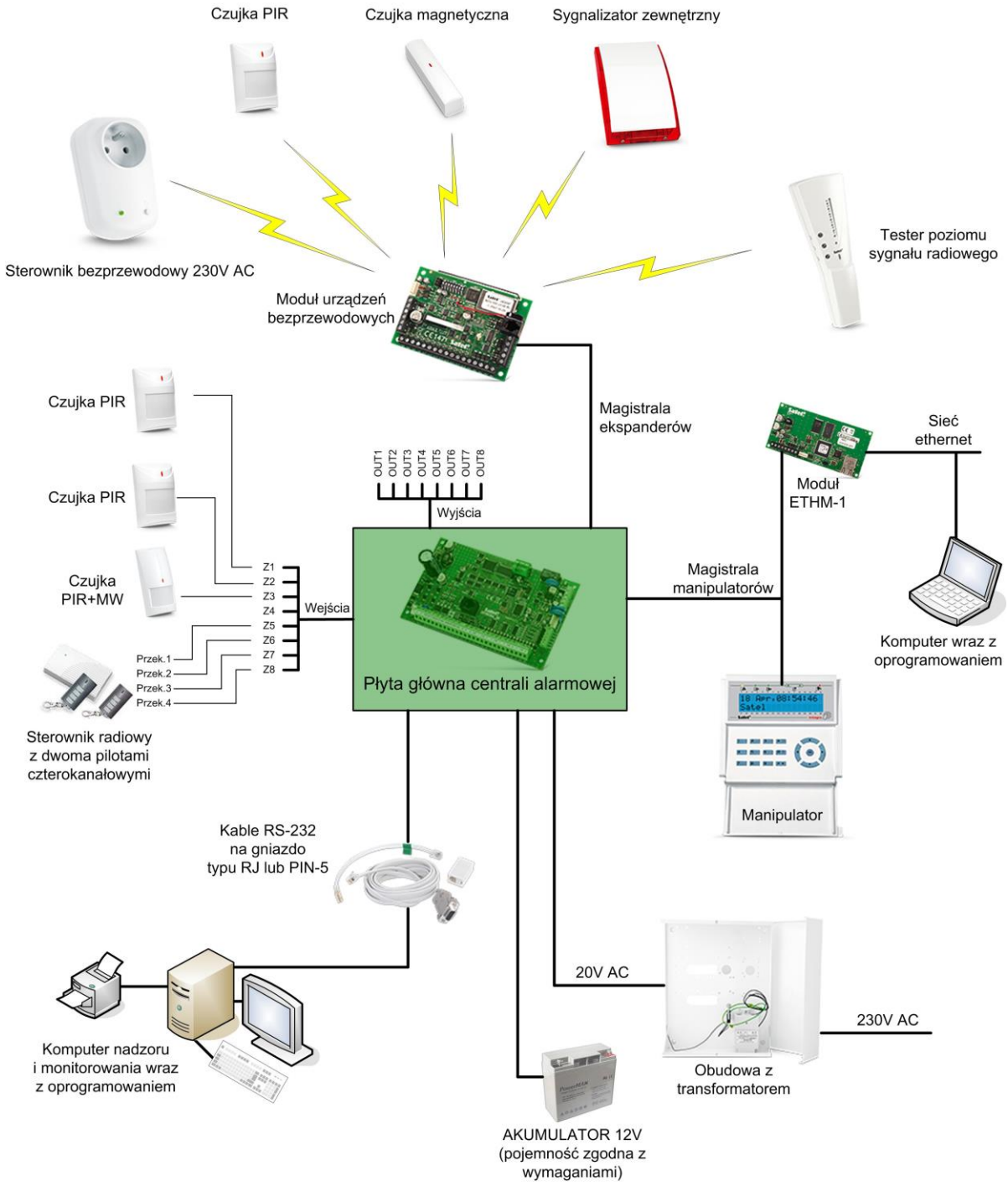
- płyty głównej centrali alarmowej,
- manipulatora,
- modułu ethernetowego,
- modułu urządzeń bezprzewodowych.

W skład wchodzą także urządzenia przewodowe (np. czujki PIR, PIR+MW) oraz bezprzewodowe (np. sterownik bezprzewodowy 230V AC, czujka magnetyczna). Jest to system, który jest wykorzystywany w ćwiczeniu laboratoryjnym z zakresu programowania i diagnostyki SSWiN.

Przedstawione stanowisko umożliwia przeprowadzenie diagnostyki systemu:

- lokalnie, m.in. poprzez:
  - wykorzystanie manipulatora,
  - wykorzystanie programu DLOADX (połączonego z SSWiN poprzez port RS-232 lub USB w nowszych typach central) obrazującego:
    - listę zdarzeń,
    - stan systemu – manipulator, strefy, wejścia, wyjścia, zasilanie modułów,
    - poziom sygnału radiowego odbieranego przez moduł urządzeń bezprzewodowych z testera poziomu sygnału radiowego,
  - wykorzystanie testera poziomu sygnału radiowego i pomiar poziomu sygnału radiowego odbieranego przez tester z modułu urządzeń bezprzewodowych,
- zdalnie, m.in. poprzez:
  - wykorzystanie programu GUARDX (połączonego z SSWiN poprzez sieć LAN/WAN (łączność TCP/IP) za pośrednictwem modułu ETHM-1 podłączonego do centrali INTEGRA), który obrazuje:
    - stan chroniony obiektu na monitorze komputera,
    - informacje o sytuacjach alarmowych,
    - pamięć zdarzeń centrali alarmowej.
  - wykorzystanie wirtualnego manipulatora LCD, uruchomionego w przeglądarce stron WWW za pomocą aplikacji JAVA, poprzez sieć LAN/WAN (łączność TCP/IP), za pośrednictwem modułu ETHM-1 podłączonego do centrali INTEGRA.

[1] WAN – rozległa sieć komputerowa, ang. *Wide Area Network*.
[2] LAN – lokalna sieć komputerowa, ang. *Local Area Network*.
[3] GSM – system mobilnej telefonii komórkowej, ang. *Global System for Mobile Communications.*



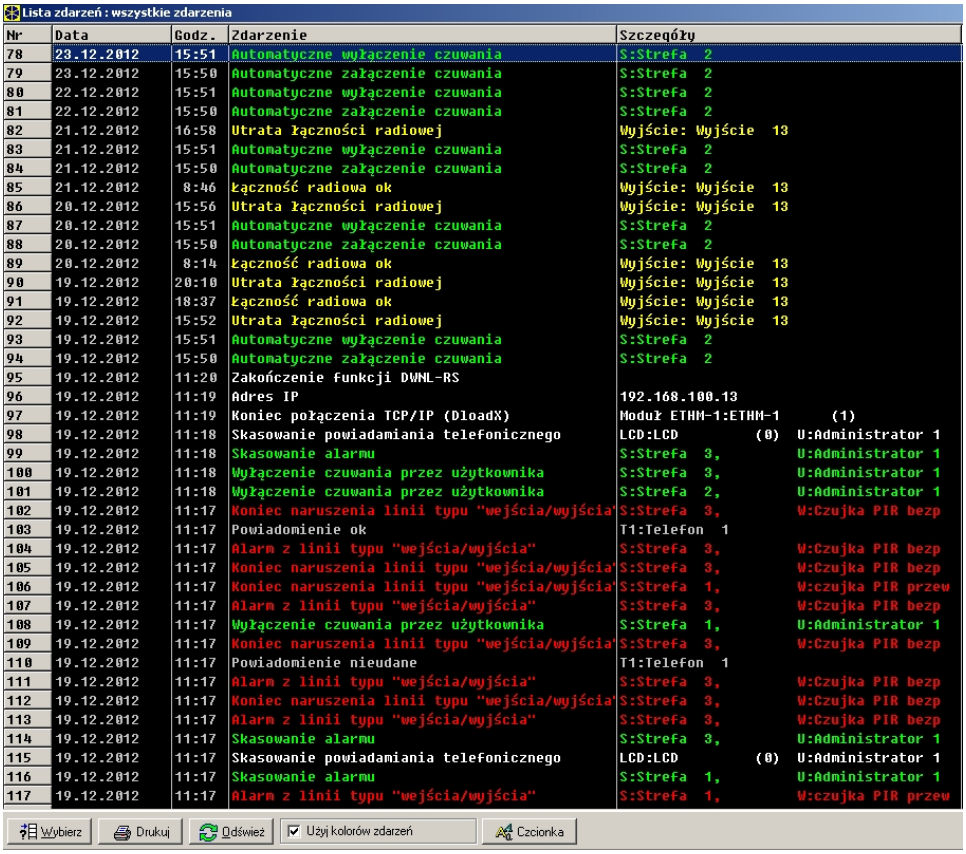
Rys. 1. System Sygnalizacji Włamania i Napadu o strukturze mieszanej
Fig. 1. The Intrusion Alarms System with the mixed structure

Podsystem diagnostyczny w rozpatrywanym SSWiN umożliwia wykrycie m.in. następujących stanów niezdatności [2]:

- awaria (sygnalizacja wykrycia stanu uszkodzenia),
- brak zasilania podstawowego płyty głównej centrali alarmowej,
- awaria akumulatora płyty głównej centrali alarmowej,
- brak akumulatora płyty głównej centrali alarmowej,
- brak zasilania podstawowego modułu [n], gdzie n – numer modułu,

- awaria akumulatora modułu [n], gdzie n – numer modułu,
- brak akumulatora modułu [n], gdzie n – numer modułu,
- awaria zasilania manipulatorów,
- awaria szyny manipulatorów,
- awaria wyjścia [n], gdzie n – numer wyjścia centrali alarmowej,
- awaria z wejścia [n], gdzie n – numer wejścia,
- awaria baterii w urządzeniu bezprzewodowym [n], gdzie n – numer urządzenia bezprzewodowego,
- awaria baterii pilotów,
- awaria zegara,
- awaria linii telefonicznej analogowej,
- awaria monitoringu TCP/IP,
- inne zależne od systemu.

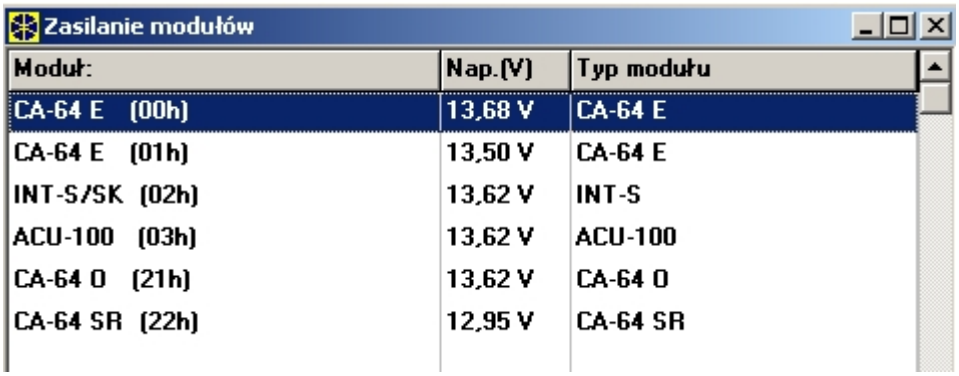
Przykładowe stany niezdatności zostały ukazane na rys. 2. W tym celu zastosowano oprogramowanie służące do programowania i obsługi central alarmowych.



Rys. 2. Widok okna „Lista zdarzeń” programu DLOADX, służącego do programowania i obsługi serwisowej central alarmowych

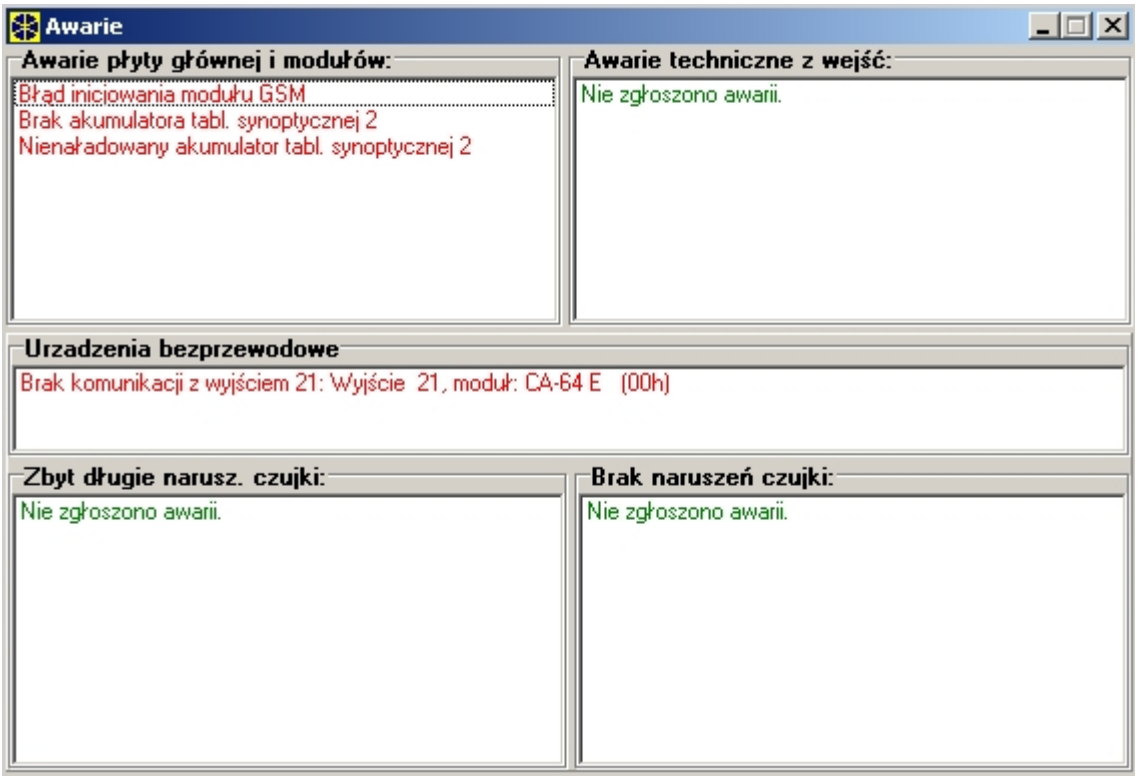
Fig. 2. The view of the "Event List" of program DLOADX used for programming and service alarm control panels

Na rys. 3 zaprezentowano wartości napięć na poszczególnych modułach wchodzących w skład systemu skonfigurowanego i wykonanego podczas zajęć laboratoryjnych przez studentów.



Rys. 3. Zdalny pomiar napięć na poszczególnych modułach SSWiN
Fig. 3. Remote measurement of voltages for individual modules IAS

Na rys. 4 zaprezentowano widok okna programu, w którym ukazane są stany niezdatności SSWiN.



Rys. 4. Widok okna programu z informacjami dotyczącymi stanów niezdatności SSWiN
Fig. 4. View of program window with information on incapacity states of IAS

3. WNIOSKI

Stosowanie zaawansowanych podsystemów diagnostycznych w Systemach Sygnalizacji Włamania i Napadu jest obecnie bardzo rozpowszechnione wśród projektantów i producentów tych urządzeń. Poprzez takie rozwiązania oraz zastosowanie różnorodnych standardów transmisyjnych (przewodowych i bezprzewodowych) możliwy jest zdalny pomiar wielu wielkości ciągłych i dyskretnych występujących w systemie przy stosunkowo niskich kosztach takiego SSWiN.

Analizując stosowane rozwiązania można stwierdzić, iż ich dalszy rozwój zmierza do wykorzystania coraz większej liczby monitorowanych parametrów diagnostycznych

z uwzględnieniem możliwości ich zobrazowania poprzez sieć telekomunikacyjną. Pozwala to na przeprowadzanie zdalnej diagnostyki, a jednocześnie też zmniejsza koszty związane z przeglądami okresowymi poprzez wykonanie części czynności obsługowych „zdalnie".

Bibliografia

1. Hołyst B.: Terroryzm. Tom 1 i 2. Wydawnictwa Prawnicze LexisNexis, Warszawa 2011.
2. Instrukcje serwisowe i użytkowników systemów SATEL.
3. Kałużny P.: Telewizyjne systemy dozorowe. WKiŁ, Warszawa 2008.
4. Mikulik J., Niezabitowska E.: Budynek inteligentny. T. 2. Podstawowe systemy bezpieczeństwa w budynkach inteligentnych. Wydawnictwo Politechniki Śląskiej, Gliwice 2005.
5. Nawrocki W.: Komputerowe systemy pomiarowe. WKiŁ, Warszawa 2006.
6. Norma PN-EN 50131-1:2009: Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Wymagania systemowe.
7. Vademecum teleinformatyka. Część 1, 2, 3. Wydawnictwo IDG, Warszawa 1998, 1999, 2002.
8. Rosiński A.: Rozproszone systemy sygnalizacji włamania i napadu w bazach logistycznych. VII Konferencja Naukowo-Techniczna LOGITRANS 2010, Szczyrk 2010.
9. Rosiński A.: Systemy bezpieczeństwa – przeciwdziałanie atakom terrorystycznym. Międzynarodowa Konferencja „Wojna z terroryzmem w XXI wieku". Warszawa 2009.
10. Rosiński A.: Diagnostyka elektronicznych systemów bezpieczeństwa. Biuletyn Wojskowej Akademii Technicznej, Warszawa, nr 4(660)/2010, s. 99-109.
11. Siergiejczyk M., Gago S.: Koncepcja systemu monitorowania i nadzoru w węźle kolejowym. VI Międzynarodowa Konferencja Naukowo-Techniczna LOGITRANS 2009, Szczyrk 2009.
12. Siergiejczyk M., Rosiński A.: Reliability analysis of electronic protection systems using optical links. Konferencja „Dependability and Computer Systems DepCoS - RELCOMEX 2011", Pałac Brunów 2011.
13. Siergiejczyk M., Rosiński A.: Wykorzystanie wybranych elementów telematyki transportu w zapewnieniu bezpieczeństwa publicznego. IV Międzynarodowa Konferencja Naukowa „Bezpieczeństwo Publiczne BP'11", Poznań 2011.
14. Wawrzyński W.: Telematyka transportu - zakres pojęciowy i obszar zastosowań. Przegląd Komunikacyjny, nr 11, Warszawa 1997.