Adam Rosiński [1]
Wydział Transportu Politechniki Warszawskiej

Możliwości stosowania czujek magistralowych w bazach logistycznych

1. WPROWADZENIE

W transporcie, jako rozległym systemie, problem zapewnienia bezpieczeństwa wydaje się szczególnie ważny. Dotyczy to nie tylko obiektów ruchomych (np. pojazdy, samoloty, pociągi) z których korzystają osoby odbywające podróż, ale także obiektów stacjonarnych (np. dworce kolejowe, porty lotnicze, bazy logistyczne). Brak możliwości świadczenia usług przez przedsiębiorstwa, które wykorzystują te obiekty, może skutkować dezorganizacja transportu, a tym samym i gospodarki państwa na znacznym obszarze [1].

Elektroniczne systemy bezpieczeństwa mogą być zastosowane jako element składowy systemów telematyki transportu. Realizują one wówczas usługę zapewnienia bezpieczeństwa podróżowania, która jest jedną z usług realizowanych przez systemy telematyki transportu. Usługa ta jest realizowana m.in. poprzez systemy zainstalowane w obiektach stałych lotniska, dworcach kolejowych [8,9], bazach logistycznych [6], terminalach przeładunkowych, jak też poprzez systemy zainstalowane w obiektach ruchomych (np. pojazdach). Dzięki temu wzrasta poziom bezpieczeństwa zarówno podróżnych jak i przewożonych ładunków [7,10]. W artykule została przeprowadzona analiza elektronicznych systemów bezpieczeństwa ze szczególnym uwzględnieniem możliwości stosowania czujek magistralowych w bazach logistycznych.

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

- sygnalizacji włamania i napadu,
- sygnalizacji pożaru,
- kontroli dostępu,
- monitoringu wizyjnego,
- 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.

2. SYSTEMY SYGNALIZACJI WŁAMANIA I NAnapadu

System Sygnalizacji Włamania i Napadu (SSWiN) ma za zadanie wykryć i zasygnalizować stan zagrożenia mienia i osób. 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" [4], zawiera wykaz części składowych (elementów), które powinien zawierać SSWiN:

[1] adro@it.pw.edu.pl

- centralę alarmową,
- jedną lub więcej czujek,
- jeden lub więcej sygnalizatorów i/lub systemów transmisji alarmu,
- zasilacz podstawowy,
- zasilacz rezerwowy.

Centrala alarmowa stanowi „serce" systemu. Do niej przesyłane są informacje o stanie poszczególnych linii wejściowych (np. czujki), linii wyjściowych (np. obciążenia wyjść) czy dane wprowadzane przez użytkownika lub konserwatora (a wcześniej podczas instalacji systemu – instalatora). W zależności od typu centrali alarmowej informacje mogą być przesyłane bezpośrednio do płyty głównej centrali alarmowej lub też do modułów, realizujących określone funkcje (np. rozszerzeniowe wejść, rozszerzeniowe wyjść, interfejsy drukarek, itd.). Obecnie najczęściej informacje pomiędzy centralą alarmową a poszczególnymi modułami są przesyłane cyfrowo z zastosowaniem formatu transmisji RS-232 lub RS-485 lub innego (bardzo często opracowanego przez producenta) [3,5].

Centrale alarmowe stanowią wyspecjalizowane urządzenia, których zadaniem jest:

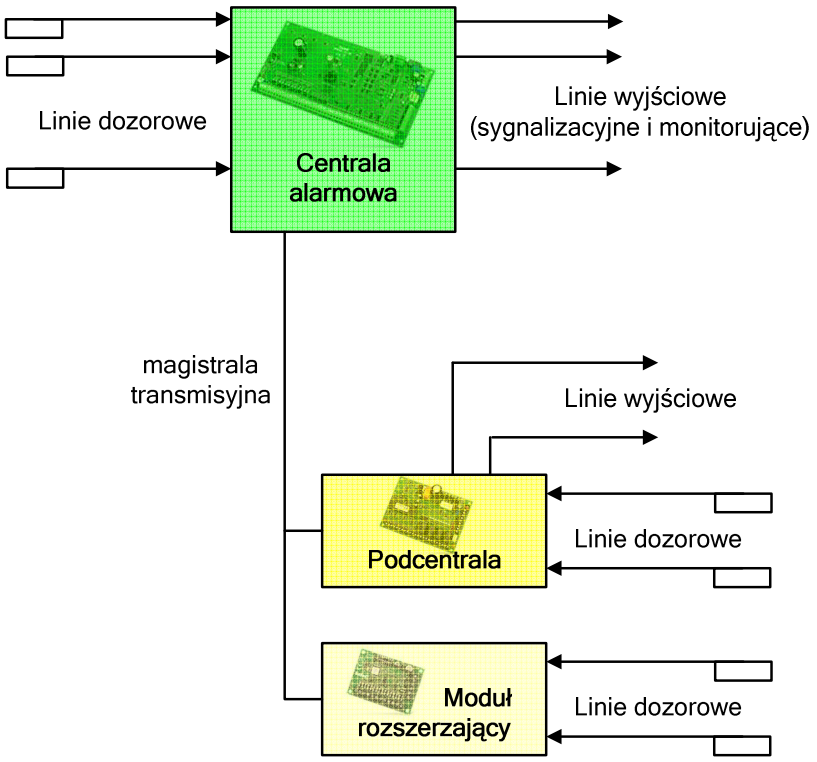
- odbieranie sygnałów informacyjnych (analogowych i/lub cyfrowych) od poszczególnych urządzeń,
- przetwarzania ich zgodnie z wcześniej zaprogramowanymi ustawieniami (instalatora i/lub producenta),
- sterowanie poprzez podanie odpowiednich sygnałów wyjściowych,
- obrazowanie zaistniałych zdarzeń na odpowiednich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

Norma PN-EN 50131-1:2009 „Systemy alarmowe - Systemy sygnalizacji włamania i napadu - Wymagania systemowe" określa stopień zabezpieczenia, którą powinny spełniać systemy sygnalizacji włamania. Są one następujące:

- 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 ogólno dostępne narzędzia i przenośne urządzenia, np. multimetr),
- stopień 3: Ryzyko średnie do wysokiego (zakłada się, że intruz zna biegle system alarmowy i 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 posiada zestaw dowolnego sprzętu, łącznie ze środkami do zastąpienia kluczowych elementów elektronicznego systemu alarmowego).

Po określeniu stopnia zabezpieczenia jaką system sygnalizacji włamania ma spełniać, dobiera się urządzenia, które spełniają założone wymagania. Oczywiście norma podaje jakie elementy muszą być zastosowane. Z tego też m.in. względu spotyka się różne rozwiązania konstrukcyjne central alarmowych i poszczególnych urządzeń wchodzących w skład systemu. Mogą one spełniać wymagania określonego stopnia zabezpieczenia, ale zarazem w zależności od producenta różnią się pomiędzy sobą.

Systemy sygnalizacji włamania i napadu posiadają określoną liczbę linii dozorowych wprowadzanych do centrali. Mają także możliwość współpracy z innymi centralami po łączach RS-232 lub RS-485, jak również możliwość współpracy z podcentralami lub modułami za pośrednictwem magistrali transmisyjnej. Na rys. 1 przedstawiono system sygnalizacji włamania i napadu w wersji mieszanej. Stosuje się go do obiektów, które wymagają dużej liczby linii dozorowych (przeważnie powyżej 16). Zwykle kilka linii dozorowych (od 4 do 16) wprowadza się wprost do listwy łączeniowej płyty głównej centrali alarmowej. Zazwyczaj te linie dozorowe nie są zbyt długie (od kilku do kilkudziesięciu metrów) i łączą czujki usytuowane blisko centrali alarmowej. Pozostałe dołączone są do modułów rozszerzeniowych wejściowych, przeważnie o 8 wejściach. Linie wyjściowe w tym systemie mogą być dołączone do wyjść płyty głównej lub do (najczęściej 4 wyjściowego) modułu rozszerzającego wyjścia. Jeśli jest to moduł podcentrali to posiada on zwykle do 8 wejść linii dozorowych i 8 wyjść.



Rys. 1. System sygnalizacji włamania i napadu
Źródło: opracowanie własne.

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 50131-1:2007 „Systemy alarmowe - Systemy sygnalizacji włamania i napadu - Wymagania systemowe", zawiera wykaz definicji i skrótów, które następnie są stosowane w kolejnych rozdziałach tej normy. Wśród nich jest m.in. definicja:

– łączność (ang. *communication*) – transmisja komunikatów i/lub sygnałów między elementami składowymi systemu sygnalizacji włamania i napadu.

W zależności od przyjętych założeń podczas projektowania systemu sygnalizacji włamania i rozwiązań konstrukcyjnych producenta stosowanych urządzeń istnieją różne możliwości połączenia czujek z płytą główną (lub modułami) centrali alarmowej. Można wyróżnić następujący podział czujek ze względu na komunikację z centralą alarmową lub modułem:

– analogowe:
  - NC[2] (normalnie zwarte),
  - NO[3] (normalnie otwarte),
  - EOL[4]/NC (parametryczne NC),
  - EOL/NO (parametryczne NO),
  - 2EOL/NC (dwuparametryczne NC),
  - 2EOL/NO (dwuparametryczne NO),
– cyfrowe:
  - adresowalne,
  - magistralowe.

Linie zwykłe można podzielić na: linie dozorowe typu otwartego, które współpracują z czujką wyposażoną w zestyki tzw. normalnie otwarte NO (ang. *normal open*) i linie typu zamkniętego, które współpracują z czujką wyposażoną w zestyki tzw. normalnie zamknięte NC (ang. *normal closed*). Kryterium

[2] NC – normalnie zamknięte (ang. *normal closed*)
[3] NO – normalnie otwarte (ang. *normal open*)
[4] EOL – typ linii alarmowej (ang. *end-of-line*)

alarmu to zwarcie lub rozwarcie linii. Linie typu otwartego są rzadko stosowane ze względu na niemożność odróżnienia przerw w linii od stanu czuwania. Znacznie częściej stosowane są linie typu zamkniętego (NC). Podstawową wadą tych linii jest brak sygnalizacji zwarcia linii tak istotny w przypadku, gdy na danej linii pracuje kilka czujek i zwarcie w linii może wyeliminować określoną część czujek systemu. Należy jednak pamiętać o liczbie czujek na jednej linii dozorowej w aspekcie klas systemów alarmowych. Wadę tę można jednak wyeliminować stosując linie parametryczne z grupy linii konwencjonalnych.

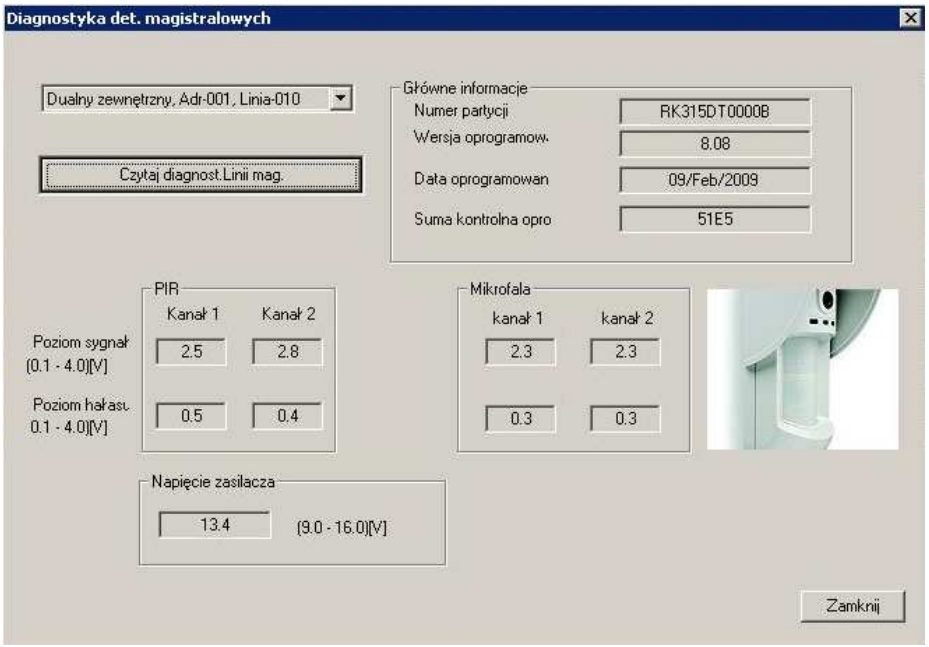
Linia dozorowa parametryczna jest linią, która jest zakończona rezystorem charakterystycznym. Zadaniem rezystora R_{CH} jest ustalenie wartości prądu płynącego w linii dozorowej w stanie dozorowania. Zmian tego prądu może być spowodowana przejściem czujki w stan alarmu a więc np. na skutek pojawienia się intruza w chronionym obiekcie co powoduje zmianę wartości napięcia na wejściu centrali alarmowej. Zmianę tę wykrywają obwody wejściowe centrali i odpowiednio ja interpretują. Rezystancja charakterystyczna linii dozorowej R_{CH} (a więc wartość tego rezystora) jest określana indywidualnie dla danego typu central przez producenta. Może ona być złożona z kilku rezystorów instalowanych w czujkach dołączonych do linii dozorowej.

3. CZUJKI MAGISTRALOWE

Osobna grupą czujek są czujki cyfrowe, tj. takie w których transmisja pomiędzy nimi a centralą alarmową (lub modułami) odbywa się z zastosowaniem transmisji cyfrowej. Ich zaletą jest możliwość transmisji dwukierunkowej, dzięki czemu mogą być to elementy programowalne. Pozwala to zatem je konfigurować zdalnie z użyciem komputera i odpowiedniego oprogramowania. Możliwe jest też przeprowadzenie diagnostyki.

Podczas zdalnej konfiguracji czujek magistralowych możliwa jest regulacja zasięgu mikrofal, regulacja czułości detektorów toru podczerwieni i mikrofali. Można także włączać i wyłączać funkcje antymaskingu oraz diody elektroluminescencyjne (ang. *Light Emitting Diode*, w skrócie LED) służące do zobrazowania stanu pracy.

Na rys. 2 przedstawiono widok okna pozwalającego na przeprowadzenie zdalnej diagnostyki czujki magistralowej. Podana jest m.in. rzeczywista wartość napięcia zasilania oraz poziomy sygnałów dla obu detektorów (tj. pasywnej podczerwieni PIR i mikrofali). Można stwierdzić, iż poziom sygnału szumów (ewentualnie celowo wprowadzanych zakłóceń – np. podczas sabotażu czujki) jest wyraźnie mniejszy od poziomu sygnału detekcji intruza.



Rys. 2. Diagnostyka czujki magistralowej

Źródło: opracowanie własne.

Dzięki wymienionym zaletom czujki magistralowe znajdują zastosowanie w obiektach magazynowych. Przykład czujki sufitowej przedstawiono na rys. 3 [2].

Rys. 3. Przykład zastosowania czujki magistralowej sufitowej w magazynie
Źródło: materiały otrzymane od firmy RISCO.

4. PODSUMOWANIE

Przedstawione rozwiązanie w postaci czujek magistralowych, które mogą być zastosowane w Systemach Sygnalizacji Włamania i Napadu, doskonale znajduje zastosowanie w bazach logistycznych i magazynach wysokiego składowania. Możliwość zdalnej konfiguracji czujki (np. włączanie i wyłączanie poszczególnych detektorów, zmian ich czułości), a także przeprowadzania diagnostyki (np. poziomy sygnałów i szumów dla poszczególnych detektorów) pozwala na montaż jej na dużej wysokości, bez konieczności późniejszego „dostawania się" do niej. Korzystnym rozwiązaniem jest też zastosowanie do łączności pomiędzy czujkami a centrala magistrali transmisyjnej wykorzystującej transmisje cyfrową. Pozwala to na zaprojektowanie okablowania, gdzie na jednej linii (4-żyłowej) można zainstalować do 16 (w niektórych rozwiązaniach firmowych do 32) czujek. Przedstawione rozwiązanie w postaci czujek magistralowych ma także wady. Do nich należy zaliczyć konieczność stosowania centrali alarmowej i czujek jednego producenta (brak kompatybilności pomiędzy urządzeniami różnych producentów) oraz dość znaczną cenę w porównaniu do czujek tradycyjnych, które wykorzystują łączność analogową. Niemniej należy sądzić, iż w obiektach o dużej powierzchni i znacznych wysokościach pomieszczeń będą one coraz częściej stosowane.

Streszczenie

W artykule zaprezentowano zagadnienia związane z Systemami Sygnalizacji Włamania i Napadu, które są stosowane w wielu obiektach transportowych, w tym m.in. w bazach logistycznych. Przedstawiono system oraz urządzenia wchodzące w jego skład. Zaprezentowano też nowe rozwiązanie w postaci czujek magistralowych. Mogą być one doskonale zastosowane w magazynach wysokiego składowania, dzięki możliwości zdalnej konfiguracji i diagnostyki. Zastosowanie tego typu rozwiązań zwiększa poziom bezpieczeństwa baz logistycznych.

Słowa kluczowe: bezpieczeństwo, baza logistyczna, czujka magistralowa.

Possibility of using field bus detectors in logistics bases

Abstract

The paper presents problems connected with the Intruder and Hold-up Alarms Systems, which are used in many transport objects, including the logistics bases. The system and devices included in it are presented. The paper proposes a new solution in the form of field bus detectors. They can be perfectly applied in magazines of high stories, thanks the possibility of remote configuration and diagnostics. Application of these solutions improve the security of logistics bases.

Key words: security, logistic base, field bus detector.

LITERATURA

[1] Hołyst B.: Terroryzm. Tom 1 i 2. Wydawnictwa Prawnicze LexisNexis, Warszawa 2011.
[2] Instrukcje techniczne urządzeń i systemów firmy RISCO.
[3] Mikulik J. (praca pod red. E. Niezabitowskiej): Budynek inteligentny. T. 2, Podstawowe systemy bezpieczeństwa w budynkach inteligentnych. Wydawnictwo Politechniki Śląskiej, Gliwice 2005.
[4] Norma PN-EN 50131-1:2009: Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Wymagania systemowe.
[5] Rosiński A.: Kierunki rozwoju Systemów Sygnalizacji Włamania i Napadu. XI ogólnopolskie seminarium „Problemy techniczno-prawne utrzymania obiektów budowlanych na terenach zamkniętych i obszarach kolejowych", Główny Urząd Nadzoru Budowlanego, Warszawa 2010.
[6] Rosiński A.: Rozproszone systemy sygnalizacji włamania i napadu w bazach logistycznych. VII Konferencja Naukowo-Techniczna LOGITRANS 2010, Szczyrk 2010.
[7] Rosiński A.: Systemy bezpieczeństwa – przeciwdziałanie atakom terrorystycznym. Międzynarodowa Konferencja „Wojna z terroryzmem w XXI wieku", Warszawa 2009.
[8] Rosiński A.: Systemy monitoringu wizyjnego obiektów zlokalizowanych na obszarach kolejowych. X ogólnopolskie seminarium „Problemy techniczno-prawne utrzymania obiektów budowlanych na terenach zamkniętych i obszarach kolejowych", Główny Urząd Nadzoru Budowlanego, Warszawa 2009.
[9] Siergiejczyk M., Gago S.: Koncepcja systemu monitorowania i nadzoru w węźle kolejowym. VI Międzynarodowa Konferencja Naukowo-Techniczna LOGITRANS 2009, Szczyrk 2009.
[10] Siergiejczyk M., Rosiński A.: Wykorzystanie wybranych elementów telematyki transportu w zapewnieniu bezpieczeństwa publicznego. IV Międzynarodowa Konferencja Naukowa „Bezpieczeństwo Publiczne BP'11", Poznań 2011.