

PRZEWODOWO CZY BEZPRZEWODOWO W SYSTEMACH ZABEZPIECZEŃ ELEKTRONICZNYCH?

Część 1. Linie dozorowe i detektory



Cezary Mecwaldowski

Odpowiedź na postawione w tytule pytanie wcale nie jest prosta. Niezależnie czy decyzję w tym zakresie ma podjąć projektant, instalator czy inwestor. Niezmiernie trudno odnaleźć rzetelne badania, które jednoznacznie wskazałyby prym jednego rozwiązania nad drugim. Najczęściej o zastosowaniu danego systemu decydują przyzwyczajenia lub przekonania projektanta, instalatora, inwestora. Czasami sytuacja sięga poziomu absurdu, gdy pojawia się konflikt pomiędzy uczestnikami procesu inwestycyjnego, wynikający z nieprecyzyjnych zapisów w specyfikacji technicznej. Debata dotyczy wówczas nie rzeczywistych korzyści lub wad danego rozwiązania, tylko argumentowania nieprecyzyjnych zapisów w specyfikacji lub zamówieniu. Tylko określenie jednoznacznych oczekiwań systemowych na etapie koncepcji, specyfikacji technicznej czy wyciecznych może zapobiec konfliktom pomiędzy uczestnikami inwestycji. Rzeczywistość pokazuje, że nie jest to takie proste i oczywiste.

Rozwiązania przewodowe i bezprzewodowe są powszechne w systemach alarmowych:

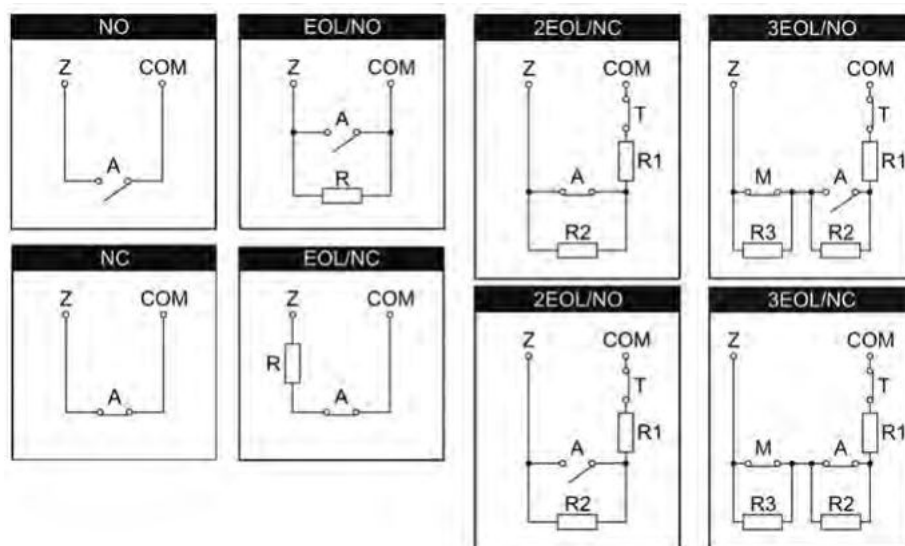
- Systemie Sygnalizacji Włamania i Napadu
- Systemie Kontroli Dostępu
- Systemie Dozoru Wizyjnego
- Systemie Sygnalizacji Pożarowej

a także wśród urządzeń i systemów klasyfikowanych szerzej, jako systemy zabezpieczeń elektronicznych. Stosowane technologie bezprzewodowe to: Wi-Fi, Bluetooth, BLE, LoRA, MESH, NFC, RFID, NB-IoT, SigFox, ZigBee, Z-Wave, zmienne dynamicznie kody czy szyfrowanie komunikacji w zakresie częstotliwości od 120 kHz do 10 GHz.

Dlaczego więc, tak trudno odszukać argumenty lub badania wskazujące na wyższość jednego rozwiązania nad drugim? Ponieważ do oceny należy wziąć pod uwagę wiele parametrów i zjawisk. Do każdego projektu należy wykonać złożoną, indywidualną analizę ryzyka. Zarówno rozwiązania przewodowe jak i bezprzewodowe posiadają cechy korzystne jak i niekorzystne, a korzyść bądź nie z danego zastosowania, będzie zależała od wielu czynników. W artykule zostaną poruszone wybrane zagadnienia, pozwalające przybliżyć czytelnikowi odpowiedź na postawione w tytule pytanie. Od dawna najwięcej kontrowersji budzi stosowanie bezprzewodowych elementów detekcyjnych i sygnalizacyjnych w systemach alarmowych¹, czy słusznie?

Występują przypadki, kiedy zastosowanie systemu bezprzewodowego ma wyłącznie

¹ C. Mecwaldowski, „Więzienie. Obiekt pod specjalnym nadzorem”, SEC&AS 5/2017



Rys. 1. Przykłady linii dozorowych w systemach alarmowych

Źródło: opracowano na podstawie: <https://bazawiedzyeltrox.pl/jakie-sa-typy-polaczen-linii-dozorowej/>.



Zdj. 1. Przykład detektorów przewodowych instalowanych na ogrodzeniu
 Źródło: materiały własne.

ekonomiczny wymiar, kiedy koszty instalacji okablowania są nie do zaakceptowania lub systemem ma zostać zabezpieczony obiekt, w którym okablowania wykonać po prostu nie można np. obiekt muzealny. Poza powyższymi przypadkami, projektant, instalator lub inwestor staje przed wyborem rozwiązania. W części pierwszej artykułu, analizie poddane zostaną kwestie komunikacji przewodowej i bezprzewodowej w zakresie linii dozorowych.

Linie dozorowe central alarmowych można podzielić na:

- konwencjonalne, zwykłe;
- konwencjonalne, parametryczne;
- adresowalne, otwarte;
- adresowalne, zamknięte;
- radiowe, nieadresowane;
- radiowe, adresowane.

W przewodowej, konwencjonalnej, zwykłej linii dozorowej centrala alarmowa odczytuje tylko dwa stany: linia normalnie otwarta NO (rozwarta) lub normalnie zamknięta NC (zwarła). W takiej linii można instalować więcej niż jeden element detekcyjny równoległe lub szeregowo. Brak jest wtedy identyfikacji poszczególnych elementów. Takie stany NO/NC oferują także moduły odbiornika radiolinii i prostych pilotów napadowych, podłączane do konwencjonalnych linii dozorowych centrali alarmowej.

W zależności od stopnia systemu alarmowego, w konwencjonalnej, parametrycznej linii dozorowej systemu alarmowego występują, następujące stany:

- dozór;
- alarm;
- maskowanie;
- sabotaż;
- usterka.

Powyższe stany w jednej linii dozorowej można uzyskać stosując parametryzację linii rezystorami – instalowanymi przy detektorze, urządzeniu. Występują linie EOL (End Of Line), 2EOL i 3EOL, które różnią się konfiguracją – połączeniami rezystorów parametryzujących

linię i liczbą uzyskiwanych stanów, odpowiednio: 1 rezystor, 2 rezystory i 3 rezystory (rys. 1). Wartości rezystorów zależą od przyjętego rozwiązania przez danego producenta systemu. Alarm oznacza sygnał z detektora o wykryciu intruza lub zjawiska fizycznego. Sabotaż linii traktowany jest jako działanie celowe, mające wpływ na działanie systemu np. próba podmiany, „zablokowania” detektora lub jego odłączenia bez wygenerowania alarmu. W praktyce ogranicza się do pomiaru rezystancji linii i w związku z tym może także wynikać z błędów instalacyjnych (luzy na złączach, złamanie przewodów) lub eksploatacyjnych (korozja). Usterka to zwarcie (rezystancja bliska 0 Ohm lub rozwarcie linii dozorowej (rezystancja bardzo wysoka „nieskończoność”).

W liniach dozorowych adresowalnych, otwartych detektory łączone równoległe posiadają swój unikatowy adres pozwalający identyfikować je w centrali alarmowej (precyzyjnie identyfikować miejsce wystąpienia zdarzenia). W liniach adresowalnych, zamkniętych tzw. pętlowych detektory również łączone są równoległe, posiadają swój unikatowy adres pozwalający identyfikować je w centrali alarmowej (precyzyjnie identyfikować miejsce wystąpienia zdarzenia). Ponadto, połączenie w pętli z wbudowanymi izolatorami zwarcie pozwala, w razie uszkodzenia elementów automatycznie odciąć część pętli z uszkodzonymi detektorami, pozostawiając pozostałe elementy pracujące prawidłowo. Stany detektora w systemach adresowalnych przesyłane są cyfrowo do centrali alarmowej lub modułu linii dozorowych.

Linie dozorowe radiowe, nieadresowane pozwalają na komunikację 1 do 1. Jeżeli w tym samym kanale radiowym pracuje więcej urządzeń, centrala odbierze sygnał o zdarzeniu, ale nie ma identyfikacji detektora (podobnie jak w przewodowych liniach konwencjonalnych). Identyfikacja detektora występuje w liniach dozorowych radiowych (zdj. 2), adresowanych, tożsamo do przewodowych (zdj.1). Identyfikowany w systemie jest każdy detektor, a informacja o stanie detektora wysyłana



Zdj. 2. Przykład detektorów bezprzewodowych instalowanych na ogrodzeniu
 Źródło: materiały własne.



Zdj. 3. Przykład dodatkowych zabezpieczeń przepięciowych do elementów systemów przewodowych

Źródło: materiały własne.

jest w postaci cyfrowej do modułu/centrali. Najbardziej zaawansowanymi systemami radiowymi są systemy typu MESH, gdzie każdy element systemu (detektor, moduł) przesyła sygnał odebrany od innego elementu systemu, który nie dotarł bezpośrednio do centrali.

W systemach bezprzewodowych występują tożsame stany: dozór, alarm, maskowanie, sabotaż, usterka. Alarm oznacza przestanie sygnałem radiowym informacji o detekcji intruza lub zjawiska fizycznego. Sabotaż występuje przy problemach komunikacyjnych, zakłócenia sygnału radiowego. Usterka to brak nawiązania połączenia radiowego z detektorem lub modułem. Powyższe wskazuje na tożsame funkcjonalnie działanie systemu przewodowego i bezprzewodowego. W zależności od stopnia systemu alarmowego wymagane jest, aby urządzenie bezprzewodowe miało nadzorowany stan baterii. Taka informacja jest przesyłana radiowo do centrali systemu. Detektory, moduły bezprzewodowe posiadają również czujniki sabotażu obudowy (Tamper), maskowania i inne, tak jak urządzenia przewodowe.

Przypadkowe, niedookreślone zapisy w specyfikacji technicznej lub wytycznych o tym, że detektory podłączone są do centrali systemu alarmowego przez linie dozоровe przewodowe, mogą utrudniać zastosowanie systemów, w których detektory bezprzewodowe (lub przewodowe) podłączone są do systemu alarmowego przewodowo do linii dozоровych, ale przez moduł odbiornika cyfrowego. Takie specyfikacje techniczne/wytyczne nie powinny bez uzasadnienia, ograniczać możliwości zastosowania szeregu nowoczesnych technologii.

Przy wyborze systemu bezprzewodowego do ochrony obiektu, należy dokonać pomiarów zasięgu łączności radiowej w obiekcie. Zarówno w budynku – grubości i konstrukcje ścian, stropów oraz na zewnątrz – metalowe wygradzenia, siatki i inne przeszkody lub źródła zakłóceń. Producenci do tego celu udostępniają dedykowane urządzenia w postaci nadajnika i odbiornika. Nadajnik przykłada się w miejscu przyszłościowej lokalizacji detektora a odbiornik w miejscu

centrali/modułu. Pozwala to dokonać ewentualnej korekty lokalizacji urządzeń i zapobiega problemom komunikacyjnym po zainstalowaniu systemu. Do zalet systemu bezprzewodowego należy zaliczyć możliwość szybkiej reorganizacji w ochronie obiektu, zmiany lokalizacji detektorów i urządzeń wykonawczych, bez potrzeby demontażu i instalacji okablowania. Odporność systemu bezprzewodowego na przepięcia i pobliskie wyładowania atmosferyczne jest większa (system przewodowy wymaga stosowania dedykowanych zabezpieczeń (zdj. 3) oraz uzemień wyrównawczych). Technologicznie sprawność urządzeń radiowych rośnie z roku na rok. Czas pracy urządzeń na jednej baterii sięga 8–10 lat, a temperatura pracy w zakresie od – 25°C do 60°C.

Komunikacja radiowa jest szyfrowana i nadzorowana. Co prawda może zostać zakłócona, podobnie jak uszkodzona może być instalacja przewodowa. System z komunikacją radiową informuje o stanach komunikacji, co stanowi tożsamą informację jak przy uszkodzeniach instalacji przewodowej. W systemach radiowych również należy stosować zasadę zasięgu komunikacji w strefie chronionej detektorami tożsamo, jak prowadzenie okablowania w strefie chronionej. Szczególnym miejscem jest granica obszaru chronionego, strefa perymetryczna np. ogrodzenie, gdzie zarówno systemy kablowe jak i bezprzewodowe są „potencjalnie dostępne” dla intruza lub wandal². Kwestia podatności systemowej drogi komunikacyjnej na zagrożenie jest względna, zależna od stopnia wiedzy, umiejętności i wyposażenia intruza w odpowiednie narzędzia. Dokonanie sabotażu, uszkodzenia jest możliwe w systemach przewodowych jak i bezprzewodowych. Współcześnie przy dostępie intruza do wyspecjalizowanych narzędzi, a także dronów latających, jeżdżących, krocących, pełzających, pływających systemy przewodowe oraz bezprzewodowe narażone są podobnie³. Sabotaż czy uszkodzenie w systemie radiowym i przewodowym ma tożsamy skutek i powinno uruchamiać dedykowaną procedurę ochronną. To nie przewodowe czy bezprzewodowe rozwiązanie decyduje o bezpieczeństwie obiektu a wiedza i umiejętności projektanta. Projekt bezwzględnie powinien być poprzedzony rzetelną analizą ryzyka. ■

mjr mgr inż. Cezary Mecwaldowski

Komendant Centralnego Ośrodka Szkolenia Służby Więziennej w Kulach. Wykładowca Ośrodka Szkolenia Polskiej Izby Systemów Alarmowych. Ekspert think tanku Obserwatorium Bezpieczeństwa.pl

² C. Mecwaldowski, „Zabezpieczenia w ochronie obwodowej” w publikacji „Zabezpieczenia techniczne w bezpieczeństwie antyterrorystycznym budynków użyteczności publicznej” pod red. mjr rez. dr inż. Jarosława Stelmacha 2020 [dostęp: https://www.researchgate.net/publication/363056541_Zabezpieczenia_techiczne_w_bezpieczenstwie_antyterrorystycznym_budynkow_uzytecznosci_publicznej]

³ C. Mecwaldowski, „Drony i zakłady karne”, SEC&AS 1/2018