Andrzej Tomczak
ID Electronics
ul. Przy Bażantarni 11; 02-793 Warszawa
tel.: 22 649 60 95, 22 649 60 94; faks: 22 649 61 00
ide@ide.com.pl www.ide.com.pl

inner range
Intelligent Security Solutions

CASE STUDY inteligentne rozwiązania systemów Inner Range „lekiem na całe zło"

To kolejny z serii kilku artykułów w formie tzw. analizy przypadku (case studies), skierowanych do projektantów, instalatorów i inwestorów systemów zabezpieczeń. Chcemy pokazać nie to, co producenci oferują w swoich katalogach, ale to, co faktycznie zostało wdrożone i sprawdzone w wielu już zrealizowanych instalacjach. Jako przykład wybraliśmy zintegrowane systemy zabezpieczeń firmy Inner Range, instalowane w Polsce już od ponad 10 lat.

Case sa Study

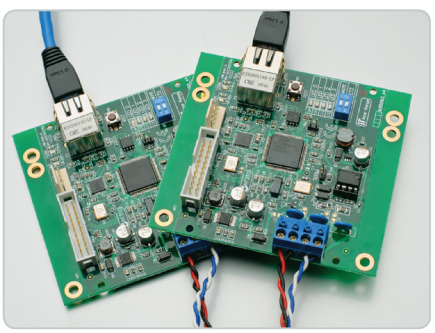
Cz. 5. Obiekty oddalone Komunikacja radiowa

Urządzenia firmy Inner Range pozwalają tworzyć zintegrowane systemy zabezpieczeń różnej wielkości – od małych instalacji wykorzystujących jedną centralę, po rozproszone, grupujące wiele central w duży system. Można je połączyć na wiele sposobów. W tej części cyklu *Case study* zostaną przedstawione systemy rozproszone o zasięgu lokalnym, wykorzystujące do komunikacji między sobą transmisję radiową.

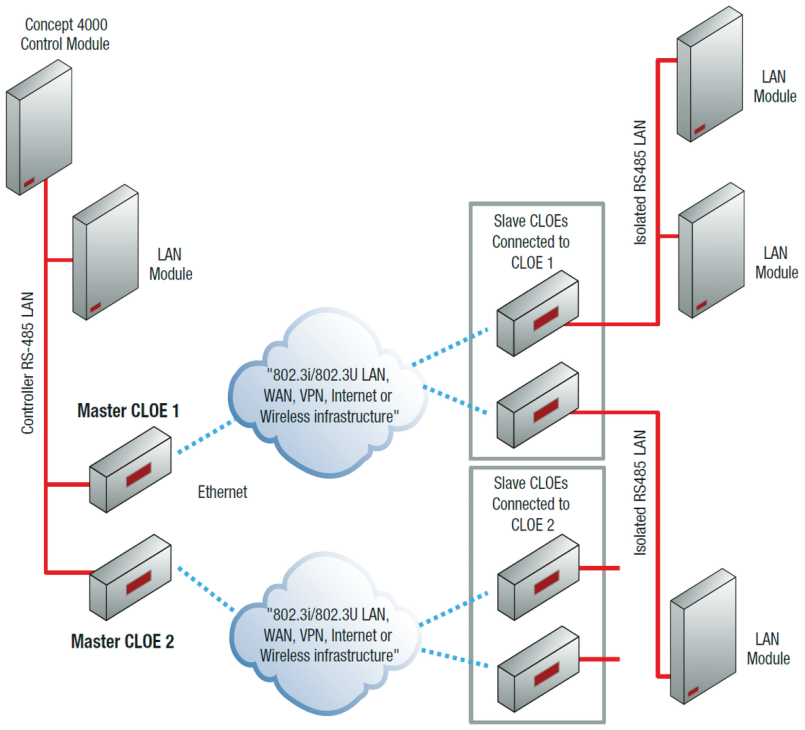
Zacznijmy od przypomnienia teorii dotyczącej transmisji sygnałów w systemach zabezpieczeń. Wymagają one zagwarantowania ciągłości i pewności transmitowania sygnałów wewnętrznych i komunikatów zewnętrznych, np. o wystąpieniu alarmu. Z tego powodu niektóre metody, takie jak transmisja radiowa czy transmisja w sieci Ethernet nie są dobrymi rozwiązaniami. Transmisja radiowa może zostać zakłócona, transmisja w sieci Ethernet natomiast jest niepewna. System zabezpieczeń funkcjonujący z wykorzystaniem sieci Ethernet (szczególnie współdzielonej) jest narażony na konflikt adresów IP, awarie, zaniki napięcia, ataki hakerskie czy nieprofesjonalne zarządzanie siecią. Jak wynika z tej wstępnej charakterystyki, obie metody transmisji nie są specjalnie zachęcające...

Załóżmy, że system sygnalizacji włamania i napadu opiera się na modułach (podcentralkach, ekspanderach, koncentratorach, modułach adresowych) komunikujących się drogą radiową czy po TCP/IP. Sygnał jest transmitowany za pomocą fal radiowych lub w sieci LAN poprzez zewnętrzne urządzenia aktywne. Jeśli np. transmisja radiowa zostanie zakłócona lub wyłączone zasilanie któregokolwiek z urządzeń aktywnych sieci, system przestanie poprawnie działać! Sygnał alarmu nie zostanie przetransmitowany! Nie można więc w 100% ufać transmisji radiowej czy transmisji w sieci Ethernet. Należy pamiętać, że w przypadku sieci Ethernet urządzenia aktywne muszą działać tak samo sprawnie jak pozostałe elementy systemu alarmowego, czyli muszą być wyposażone w awaryjne zasilanie na wypadek zaniku napięcia sieci. Równie krytyczna sytuacja nastąpi, gdy ktoś np. wyjmie wtyczkę sieci z gniazda krosownicy czy też urządzenia aktywnego – może przecież dojść do omyłkowego lub celowego rozłączenia komunikacji systemu zabezpieczeń. W związku z tym urządzenia aktywne i krosownice muszą być zabezpieczone przed dostępem osób niepowołanych, a obudowy zabezpieczone przed sabotażem, z odpowiednią sygnalizacją w systemie alarmowym.

Można też sobie wyobrazić, jak kłopotliwe i praktycznie nierealne finansowo jest uzyskiwanie certyfikatu na stopień zabezpieczenia zgodnie z normami PN-EN 50131 dla każdego zestawu urządzeń SSWiN z urządzeniami aktywnymi sieci i szafami, czyli praktycznie dla każdej lokalizacji systemu! Należałoby poddać certyfikacji urządzenia systemu sygnalizacji włamania i napadu łącznie z konkretnymi urządzeniami aktywnymi sieci Ethernet, wyposażonymi w odpowiednie zasilanie awaryjne (dające napięcie bezpieczne – w przypadku napięć typu SELV jest to napięcie stałe mniejsze niż 60 VDC lub napięcie przemienne mniejsze niż 25 VAC), w obudowach (szafach), które zostaną w danym obiekcie zastosowane, pod warunkiem że sieć taka zostanie wydzielona fizycznie i logicznie z innych sieci. W przypadku współdzielenia sieci, infrastruktury szaf, krosownic i urządzeń aktywnych szanse na uzyskanie takiego certyfikatu są bliskie zeru! Rozwiązaniem byłoby wyposażenie każdego modułu komunikującego się po TCP/IP w oddzielny nadajnik transmisji alarmów i (lub) wyjście na sygnalizatory alarmowe, czyli przyjęcie, że każdy moduł wyposażony w TCP/IP jest oddzielną centralą alarmową. Wówczas do każdego modułu TCP/IP trzeba by również doprowadzić oddzielne łącze do stacji monitorowania alarmów.



Rys. 1. CLOE – moduły do „rozciągania" magistrali LAN za pomocą sieci Ethernet TCP/IP



Rys. 2. Schemat przedłużania magistrali centrali Concept 4000 przy użyciu modułów CLOE

Rys. 3. Strategie wykorzystania komunikacji radiowej w obiektach kampusu Lithgow High School w Australii

Jeżeli natomiast tak niepewne transmisje, jak transmisja radiowa czy transmisja w sieci Ethernet, wykorzystamy w systemach kontroli dostępu, sytuacja wygląda dużo lepiej. Wystarczy, aby zastosowany system był wyposażony w tzw. inteligencję rozproszoną (każda centralka ma własną pamięć programu, uprawnień użytkowników i pamięć zdarzeń), wówczas praktycznie nie ma przeszkód, by komunikacja przebiegała łączem radiowym czy w sieci Ethernet. Z kolei jeżeli system nie jest wyposażony w inteligencję rozproszoną, problemy komunikacyjne mogą powodować blokowanie przejść!

Systemy Concept 4000 i Integriti firmy Inner Range rozwiązują powyższe dylematy w sposób wzorcowy. Otóż urządzenia związane z centralą sygnalizacji włamania i napadu oraz kontroli dostępu komunikują się za pomocą wewnętrznych magistral opartych na przemysłowym standardzie transmisji danych, odpornym na zakłócenia zewnętrzne, pozwalającym ciągnąć ponadkilometrowe magistrale wykonane z przewodów miedzianych.

W port TCP/IP są wyposażone tylko te urządzenia systemu firmy Inner Range, które nie są wrażliwe na zakłócenia transmisji danych wysyłanych w sieci Ethernet. Zakłócenia działania tej sieci nie mają wówczas bezpośredniego wpływu na bezpieczeństwo obiektów ani na pracę systemu kontroli dostępu – brak transmisji w sieci Ethernet nie ma wpływu na poprawne wysłanie komunikatu o alarmie do stacji monitorowania z systemu alarmowego SWiN czy też otwarcie drzwi osobie uprawnionej przez system kontroli dostępu.

Magistrala wewnętrzna może być przedłużana za pomocą urządzeń sieci Ethernet, z użyciem modułów CLOE *(Concept LAN Over Ethernet)* pokazanych na *rys. 1.* Realizują one przedłużenia mostowe magistrali z wykorzystaniem sieci Ethernet TCP/IP. Jeżeli po drugiej stronie „mostu" zostaną zainstalowane urządzenia „inteligentne", system kontroli dostępu będzie działał bez zakłóceń. Takimi inteligentnymi modułami kontroli dostępu są np. inteligentny kontroler dwóch przejść i inteligentny kontroler czterech przejść.

Analizując za i przeciw przy realizowaniu systemu kontroli dostępu w kampusie szkoły **Lithgow High School** w miejscowości Lithgow (Australia, Nowa Południowa Walia), ustalono, że ze względów bezpieczeństwa i przyszłej, jak najmniej zakłóconej sprawności systemu należy rozproszone obiekty kampusu połączyć ze sobą drogą radiową. Układanie nowych kabli pomiędzy budynkami nie wchodziło w grę ze względu na wysokie koszty.

Rys. 4. Montaż jednej z anten w kampusie Lithgow High School

Australijska firma **Central Security Distribution** (CSD) wdrożyła rozproszony system kontroli dostępu oparty na radiolinii firmy UbiQUiTi oraz modułach CLOE, służących do „rozciągania" magistrali LAN za pomocą sieci Ethernet TCP/IP. Schemat podłączenia modułów CLOE pokazano na *rys. 2.* Do wyjść Ethernet modułów CLOE podłączono nadajniki i odbiorniki urządzeń radiowych firmy UbiQUiTi. Wykorzystano dwie strategie połączeń, pokazane na *rys. 3.*

Firma CSD wykonała połączenia radiowe pomiędzy budynkami kampusu w ciągu trzech dni. Rozwiązanie to znacząco obniżyło koszty systemu oraz skróciło proces wykonywania całej instalacji do kilkunastu dni. Na *rys. 4* pokazano montaż jednej z anten w kampusie.

Po raz kolejny urządzenia Concept firmy Inner Range potwierdziły ogromną elastyczność, pozwalając zrealizować oparty na nich bezprzewodowy rozproszony system kontroli dostępu. Rozwiązanie z komunikacją radiową okazało się bardzo udane, a do tego na tyle tanie, że na jego instalację mogła sobie pozwolić placówka edukacyjna, która nawet w Australii nie należy do grupy tych najbardziej „bogatych".