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

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

inner range
Intelligent Security Solutions

Cz. 4. Obiekty oddalone Systemy rozproszone

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 oferują producenci w swoich katalogach, ale to co faktycznie zostało przez firmę ID Electronics (IDE) wdrożone i sprawdzone w wielu wykonanych już instalacjach. Jako przykład wybraliśmy zintegrowane systemy zabezpieczeń firmy Inner Range, instalowane w Polsce już od ponad 10 lat.

Urządzenia firmy **Inner Range** pozwalają tworzyć zintegrowane systemy zabezpieczeń różnej wielkości – od małych instalacji z jedną centralą, po rozproszone, grupujące wiele central w jeden duży system. Urządzenia mogą być łączone na kilka sposobów. W tym odcinku Case study zajmiemy sie systemami rozproszonymi o zasięgu lokalnym i globalnym, wykorzystującymi do komunikacji między sobą porty Ethernet, w które są wyposażone centrale i niektóre moduły systemów **Concept 4000** oraz **Integriti** firmy Inner Range. Do tworzenia tego typu systemów wykorzystuje się przede wszystkim sieci typu LAN i WAN.

TROCHĘ TEORII DOTYCZĄCEJ TRANSMISJI SYGNAŁÓW W SYSTEMACH ALARMOWYCH

Systemy alarmowe wymagają zagwarantowania ciągłości i pewności transmitowania sygnałów wewnętrznych i komunikatów zewnętrznych, np. o wystąpieniu alarmu. Z tego powodu transmisja w sieci Ethernet nie jest dobrym rozwiązaniem. Połączenia przewodami miedzianymi są ograniczone do ok. 100 m. Transmisja na większe odległości wymaga dodatkowych urządzeń aktywnych, np. switchy czy routerów sieciowych.

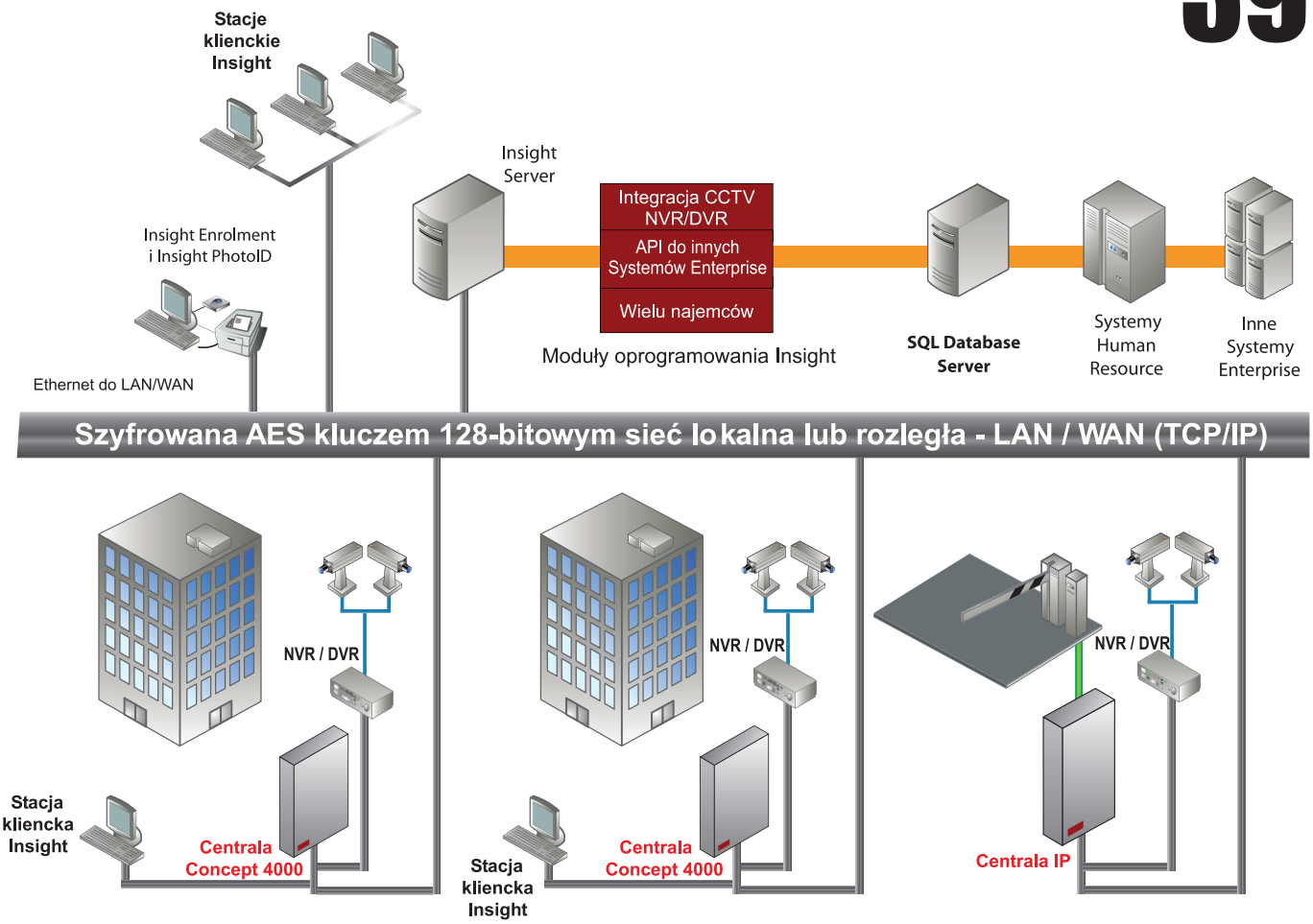
Wiążą się z tym problemy, które najlepiej zrozumieć na przykładzie. Wyobraźmy sobie, że system sygnalizacji włamania i napadu opiera sie na modułach (podcentralkach, ekspanderach, koncentratorach, modułach adresowych) komunikujących się po TCP/IP. Sygnał jest transmitowany w sieci LAN poprzez zewnętrzne urządzenia aktywne. Gdy zostanie wyłączone np. zasilanie któregokolwiek z sieciowych urządzeń aktywnych, system przestanie prawidłowo działać, a sygnał alarmu może nie zostać przesłany! Wniosek – urządzenia aktywne muszą działać tak samo sprawnie jak wszystkie pozostałe elementy systemu alarmowego, czyli muszą być wyposażone w awaryjne zasilanie na wypadek zaniku napięcia 230 VAC.

Podobnie krytyczna sytuacja nastąpi, gdy ktoś np. wyjmie wtyczkę sieci Ethernet z gniazda krosownicy czy urządzenia aktywnego. Może wtedy dojść do omyłkowego lub celowego rozłączenia komunikacji systemu alarmowego. W związku z tym urządzenia aktywne i krosownice muszą być zabezpieczone przed dostępem osób niepowołanych, a obudowy przed sabotażem, z odpowiednią sygnalizacją w systemie alarmowym.

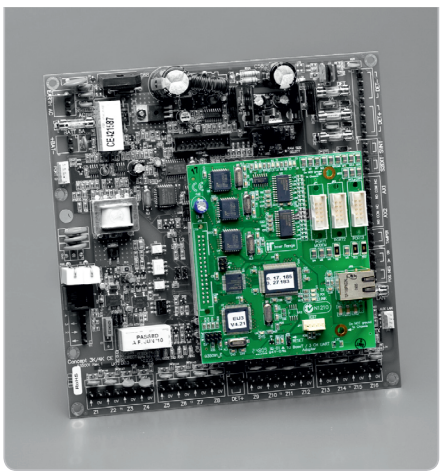
Można sobie wyobrazić, jak kłopotliwe i praktycznie nierealne finansowo jest uzyskanie certyfikatu na stopień zabezpieczenia zgodnie z normami PN-EN 50131 dla każdego zestawu urządzeń SSWiN z urządzeniami aktywnymi sieci i szafami, czyli praktycznie dla każdej lokalizacji systemu! **Certyfikacji należałoby poddać urządzenia SSWiN, włącznie z konkretnymi urządzeniami aktywnymi sieci Ethernet, wyposażonymi w odpowiednie zasilanie awaryjne, o napięciu bezpiecznym (w przypadku napięć typu SELV jest to napięcie stałe poniżej 60 VDC lub napięcie przemienne poniżej 25 VAC), w obudowach (szafach), które zostaną w danym obiekcie zastosowane.** I oczywiście pod warunkiem że sieć taka będzie wydzielona fizycznie i logicznie od innych sieci.

W przypadku współdzielenia sieci, infrastruktury szaf, krosownic i urządzeń aktywnych szanse na uzyskanie takiego certyfikatu są równe 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.

Podobnie rzecz ma się w przypadku systemów kontroli dostępu (KD). **Jeżeli są to systemy**



Rys. 1. Schemat podłączania systemu Concept 4000 do sieci Ethernet



Rys. 2. Moduł Ethernet UART zainstalowany na płycie centrali Concept 4000

KD o „inteligencji rozproszonej", w których każda centralka ma własną pamięć programu, uprawnień użytkowników i pamięć zdarzeń, wówczas może komunikować się po TCP/IP. W każdej innej sytuacji problemy z komunikacją w sieci Ethernet mogą spowodować np. opóźnienia w otwieraniu lub wręcz zablokowanie przejść! Sposób podejścia do tych problemów przez producentów świadczy o jakości i niezawodności systemów.

Systemy Concept 4000 oraz Integriti firmy Inner Range rozwiązują dylematy transmisji w sieci Ethernet w sposób wzorcowy. Otóż urządzenia związane z centralami SWiN czy KD komunikują się za pomocą wewnętrznych magistral opartymi na przemysłowym standardzie transmisji danych, bardzo odpornym na zakłócenia zewnętrzne, pozwalającym wykorzystać ponadkilometrowe magistrale z przewodów miedzianych. Natomiast urządzenia systemu wyposażone w „inteligencję rozproszoną" mogą się komunikować za pomocą sieci Ethernet.

Przykładową konfigurację do transmisji po TCP/IP pokazano na *rys. 1.* Zakłócenia działania tej sieci nie mają wówczas bezpośredniego wpływu na bezpieczeństwo obiektów ani poprawność pracy systemu KD. Problemy z transmisją w sieci Ethernet nie mają wpływu na wysyłanie komunikatu o alarmie do stacji monitorowania czy włączenie sygnalizacji lokalnej ani na otwieranie przejść kontrolowanych uprawnionym osobom i pojazdom.

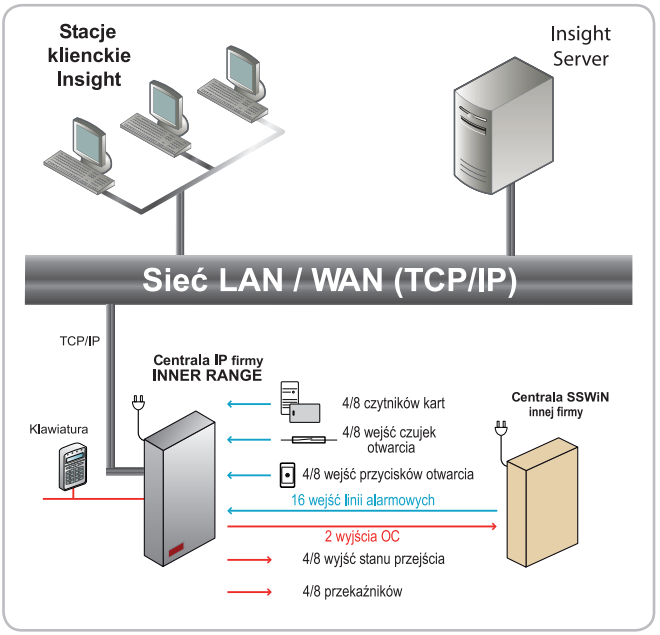
Komunikacja po TCP/IP jest możliwa dzięki zastosowaniu w urządzeniu modułu o nazwie **Ethernet UART** *(rys. 2),* który obsługuje jednocześnie maks. cztery połączenia. Operator używający oprogramowania **Insight Professional** może bez problemów komunikować się z centralą, która równolegle wymienia dane np. z systemem automatyki budynku, stacją monitorowania alarmów, interfejsami do sterowania windami czy urządzeniami GSM.

SYSTEM ROZPROSZONY OBSŁUGUJĄCY PONAD 250 ODDZIAŁÓW JEDNEGO Z BANKÓW

Atuty systemu Concept 4000 zostały wykorzystane przy tworzeniu zabezpieczeń jednego z banków działających na rynku polskim. W związku z dostosowywaniem zabezpieczeń oddziałów do wymogów rozporządzenie Ministra SWiA z 7.09.2010 r. *w sprawie szczegółowych zasad i wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne,* podjęto decyzję o wymianie systemów w części placówek bankowych (ok. 260 obiektów). **Centrala Concept 4000 jest wykonywana w 3. stopniu zabezpieczenia zgodnie z PN-EN 50131-1, bank więc mógł realizować systemy w 2. stopniu (minimalny wymóg rozporządzenia MSWiA) lub w stopniu 3.**

Bardzo ważną cechą nowo projektowanego systemu SSWiN była integracja z systemem kontroli dostępu (KD) umożliwiającym zdalne zarządzanie uprawnieniami użytkowników. Wymienione systemy KD były programowane lokalnie, każda zmiana uprawnień (co przy rotacji pracowników w oddziałach jest nieuniknione) wymagała każdorazowo przyjazdu do konkretnej placówki banku.

W nowym systemie zastosowano zarządzanie zdalne z obiektu centrali w Warszawie. Dzięki temu zrealizowano zarówno bezpośredni nadzór, jak i zdalną obsługę systemów. Było to ważne również z tego powodu, że w niektórych



Rys. 3. Schemat podłączania central alarmowych innych producentów, zainstalowanych wcześniej w placówkach banku w celu umożliwienia zarządzania wszystkich obiektów z tego samego oprogramowania Insight Professional oraz widok wnętrza centrali IP firmy Inner Range wykorzystywanej do tego celu

placówkach systemy KD mogły nie spełniać wymogów zapisanych w 18 punkcie załącznika 1 do wspomnianego rozporządzenia, że systemy KD muszą gwarantować zapamiętanie zdarzeń przynajmniej z 30 dni. **Ten wymóg dla systemu KD może być trudny do zrealizowania w ruchliwych obiektach, kiedy system nie jest podłączony do komputera, gdzie mogą być przechowywane zdarzenia archiwalne.**

Przygotowanie tak masowej logistycznie operacji w krótkim czasie wymagało opracowania precyzyjnych założeń wymiany systemów w placówkach rozproszonych po całym kraju. Nie zdradzając szczegółów, w operacji brało udział wiele firm instalacyjnych, które zgodnie z przygotowaną dokumentacją i wytycznymi instalacyjnymi wykonywały swoje prace. Poszczególne obiekty były uruchamiane z centrali banku, bez konieczności obecności specjalistów od programowania systemów w poszczególnych oddziałach. Aby uruchomienie i dalsze działanie systemu przebiegało bez problemów, dział IT banku perfekcyjnie przygotował środowisko komunikacji po TCP/IP w sieci WAN. Dzięki temu centrala banku ma dostęp online do każdego z podłączonych oddziałów. Zarządzanie odbywa się za pomocą oprogramowania Insight Professional dostarczonego w trakcie realizacji projektu.

Ponieważ bank posiada wiele oddziałów, których systemy wypełniały wymogi cytowanego rozporządzenia, została przygotowana wersja uproszczona podłączania takich systemów do wspólnego oprogramowania *(rys. 3)*. **Centrala IP** Concept 4000 przejmuje na siebie sterowanie przejściami KD w podłączanej placówce, wyjścia istniejącej centrali SSWiN natomiast są podłączane do wejść alarmowych Centrali IP. Dzięki temu możliwe jest zdalne nadawanie uprawnień w systemie KD oraz nadzór nad centralami SSWiN innego producenta. System powstał w 2011 r. i jest systematycznie rozwijany.

SYSTEM ROZPROSZONY OBSŁUGUJĄCY WIELE DUŻYCH OBIEKTÓW

Od kilku lat system Concept 4000 zabezpiecza obiekty zlokalizowane w całym kraju jednej z czołowych grup medialnych. Rozwiązanie jest odmiennie od opisanego poprzednio. W systemie bankowym podłączono wiele małych obiektów rozproszonych w całej Polsce, a w omawianym – kilkanaście dużych i bardzo dużych obiektów. Wymogiem inwestora było uporządkowanie systemów KD zainstalowanych w obiektach rozrzuconych po całym kraju. Istniejące już systemy pochodziły od różnych producentów, a osoby korzystające z obiektów posiadały w portfelach wiele kart – Cotaga, HID-a, karty magnetyczne do stołówki itp. Pracownik często miał przy sobie po kilka kart dostępu do tego samego obiektu, administrowanie wydawaniem kart i nadawanie uprawnień było więc niezwykłym wyzwaniem. Konieczne było przygotowanie całej operacji tak, by użytkownicy nie odczuli dyskomfortu wymiany systemu, a koszty były rozłożone w czasie i do tego akceptowalne dla inwestora, który zarządzał kilkuset przejściami i tysiącami wydanych kart.

Po prawie półrocznych testach kart i czytników ustalono, że docelową będzie najnowocześniejsza, cienka, bezstykowa elektroniczna karta wielosektorowa Legic Advant. Podjęto decyzję, że przechodzenie z systemu na system będzie ewolucyjne. Ponieważ pracownicy nie mieli do tej pory identyfikatorów ze zdjęciem, zastosowano sprytny trik. Oprogramowanie systemowe Insight Professional umożliwia wykonywanie identyfikatorów na cienkich kartach ISO i podkładach samoprzylepnych. Każdy pracownik otrzymał więc identyfikator ze zdjęciem, który należało dokleić do aktualnie używanej karty dostępu. Podkłady samoprzylepne, z naniesionym zdjęciem pracownika, były pełnoprawnymi kartami Legic Advant! Po tej operacji każdy pracownik miał dwie karty: aktualnie działającą kartę HID-a czy Cotaga i naklejony na nią dodatkowy identyfikator Legica. Założono, że w przyszłości działać będzie karta „smart", poprzednio zaś używana karta zostanie usztywniającą podkładką. W czasie testów wybrano te czytniki, które radziły sobie z odczytem w sytuacji, gdy dwie karty (obie posiadające anteny) były sklejone ze sobą.

Mając przygotowaną strategię „skoku w przyszłość", rozpoczęto przygotowanie rozwiązania pozwalającego na podmianę wielu różnych systemów rozrzuconych po całej Polsce i doprowadzenie do scentralizowania bazy danych. W tym przypadku przydała się uniwersalność systemu Inner Range. Ponieważ bezproblemowo współpracuje on z czytnikami różnych producentów (różnymi formatami Wiegand), prawie niezauważalnie dla pracowników wymieniano to, czego użytkownik nie widzi. Na ścianach wisiały stare czytniki różnych systemów, a „za ścianą" urządzenia firmy Inner Range zarządzały coraz większą liczbą przejść. Nowo powstające systemy wyposażano w czytniki Legic, a czytniki w systemach zastanych systematycznie wymieniano. I tak Concept 4000 z czytnikami Legic znalazł się we wszystkich obiektach i zastąpił „stare" systemy.

Oprócz KD karty identyfikacyjne służą również do innych celów. Stołówki są np. rozliczane za pomocą tej samej, wielofunkcyjnej karty Legic Advant. Wykorzystywana jest także w magazynach do wypożyczania sprzętu, wydawania kluczy samochodów służbowych i odbierania wydruków z drukarek sieciowych (czytniki Legic, zaprogramowane w naszej firmie, zaimplementowano do wielofunkcyjnych urządzeń sieciowych firmy Xerox). Serce rozproszonego systemu znajduje się w serwerowni w Warszawie i stąd po TCP/IP są zarządzane wszystkie obiekty w Polsce. System powstał w 2007 r. i jest systematycznie rozwijany.