Integracja systemów bezpieczeństwa w obiekcie

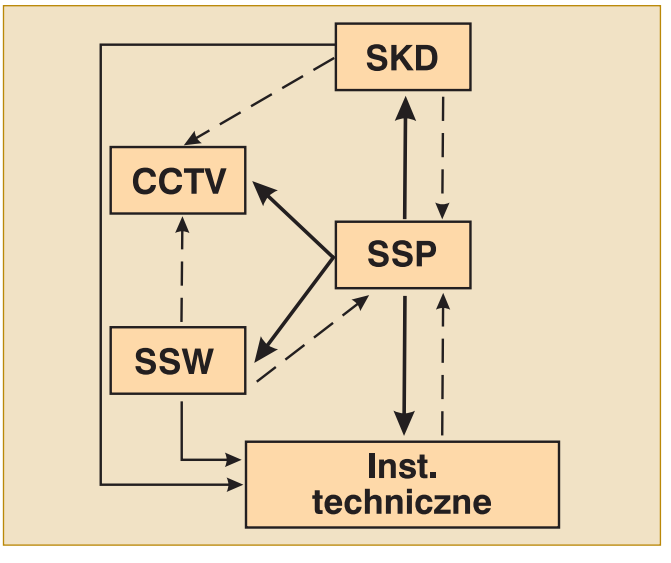
REMIGIUSZ STANISŁAWEK – *„Emax"*

Artykuł opisuje rozwiązania w zakresie integracji systemów bezpieczeństwa w obiekcie. Przedstawiono rozwiązania realizowane zarówno od strony sprzętowej, jak i software'owej. Na przykładzie zintegrowanego systemu zarządzania instalacjami technicznymi ZEUS 2000 wykazano przewagę integracji software'owej nad sprzętową.

Bezpieczeństwa obiektu nie gwarantuje tylko odpowiednia liczba oraz wielkość systemów zabezpieczeń. Ważne jest także poprawne ich zaprojektowanie, skonfigurowanie oraz umożliwienie komunikacji z innymi urządzeniami technicznymi i komputerowymi systemami nadzoru.
Praktycznie wszystkie systemy pozwalają na bezpośrednie przesyłanie informacji pomiędzy zainstalowanymi w obiekcie centralkami, co zwiększa poziom bezpieczeństwa budynku. Ale tylko zintegrowane systemy umożliwiają rozwiązywanie nietypowych problemów technicznych, takich, jak np. nadzorowanie obiektów o strategicznym dla użytkownika znaczeniu, rozproszonych na dużym obszarze.
Integrację można rozpatrywać zarówno w aspekcie połączeń sprzętowych (integracja bezpośrednia), jak i centralnego zarządzania poprzez komputerowy system nadzoru (integracja przez system zarządzający).

Integracja bezpośrednia

Czasy, w których poszczególne systemy bezpieczeństwa działały niezależnie od siebie, bezpowrotnie minęły. Obecnie wszystkie systemy w obiekcie muszą ze sobą współpracować. Zależności między nimi są obwarowane przepisami, a także podyktowane szeroko rozumianym bezpieczeństwem i komfortem użytkowania.
Poszczególne systemy bezpieczeństwa stosują najczęściej określone procedury funkcjonowania:
- W przypadku **systemu telewizji dozorowej** stosuje się wejście alarmowe uaktywniające np. nagrywanie. Doprowadzony sygnał może pochodzić z centralki dowolnego systemu, np. sygnalizacji pożaru.
- Od **systemu kontroli dostępu** wymaga się realizacji funkcji odryglowywania drzwi na drogach ewakuacyjnych w przypadku pożaru. Możliwe jest otwarcie drzwi pojedynczo, w całym budynku bądź tylko w strefie, w której wystąpił pożar. Możliwa jest także integracja z instalacją interkomową oraz systemem obsługi parkingu.
- **System detekcji CO** powinien przesłać informację o alarmie do centralki pożaru, która wysyła polecenie otwarcia określonych klap dymowych lub uruchamia wentylację wywiewną. Możliwe jest również przesłanie takiego sygnału bezpośrednio do wymienionych urządzeń.
- **System sygnalizacji włamania** w sposób jawny bądź dyskretny powiadamia ochronę budynku uruchamiając sygnalizatory optyczne i akustyczne, a także przesyłając sygnały na zewnątrz np. do stacji monitorowania.
- **System wczesnej detekcji dymu** w przypadku wykrycia alarmu przesyła informacje do centrali sygnalizacji pożaru.
- Nadrzędnym systemem w każdym obiekcie jest **system sygnalizacji pożaru**. Jest to najważniejszy system bezpie-



Rys. 1. Schemat bezpośredniej integracji systemów zabezpieczeń. Linią ciągłą zaznaczono bezpośrednie sterowania systemami, linią przerywaną informacje przesyłane do innych instalacji, które mogą być przez dany podsystem wykorzystane

czeństwa, często również największy, dlatego musi mieć zaprogramowaną złożoną mapę sterowań. Mapa ta opisuje, które sygnały z czujników pożarowych, grup czujników bądź sygnałów pochodzących z innych urządzeń będą zawierały polecenia do innych instalacji. Ze względu na liczbę czujników pożarowych nie jest możliwe stworzenie zależności w oparciu o stan pojedynczego czujnika. Stosowane są dodatkowo zależności liniowe (linii dozorowych), dwuczujnikowe, grupowe i międzygrupowe. Definiują one warunki wymagane do wysłania przez centralkę sygnału sterującego. Dla przykładu, zależność międzygrupowa wymaga, aby przynajmniej jedna czujka z każdej grupy czujek podanej w tej zależności została wprowadzona w stan alarmu. Bardzo ważne jest poprawne zaprojektowanie podziału instalacji pożarowej na linie dozorowe i grupy czujek.
System sygnalizacji pożaru w sytuacjach alarmowych wykonuje dodatkowo następujące zadania:
– otwiera klapy dymowe w celu usunięcia gromadzącego się dymu
– zamyka klapy pożarowe oraz drzwi pożarowe, aby uniemożliwić rozprzestrzenianie się pożaru
– sprowadza windy i blokuje je na parterze (lub na innym, wybranym piętrze)
– uruchamia system tryskaczowy (pompy, zawory piętrowe, hydranty)
– wysyła polecenia odczytania stosownych komunikatów do systemu nagłaśniającego
– uruchamia sygnalizatory optyczne i akustyczne
– przesyła sygnał do straży pożarnej bądź do oddalonej firmy monitorującej
– przesyła sygnał o pożarze do wybranych instalacji zabezpieczeń (SKD) oraz do instalacji technicznych budynku.
Centralki pożaru mają praktycznie nieograniczone możliwości przyłączania dodatkowych modułów I\O. Dlatego najczęściej do nich doprowadzane są, oprócz sygnałów alarmowych, także sygnały techniczne z urządzeń.

Integracja przez system zarządzający

Integracja na poziomie sprzętowym, realizowana poprzez łączenie wyjść sterujących z wejściami sygnałowymi centralek poszczególnych systemów, daje jedynie niezbędne i podstawowe możliwości przekazywania sygnałów. Interesującym rozwiązaniem jest jednak objęcie wszystkich systemów nadrzędnym komputerowym systemem zarządzającym.

Inteligentne sterowanie

System komputerowy sprawuje dwustopniowy nadzór nad obiektem. Po pierwsze, możliwa jest kontrola podsystemów przez operatora (dotyczy to sterowania określonymi podsystemami w ramach uprawnień przypisanych danemu użytkownikowi). W takim przypadku system zapewnia kontrolę elementów wykonawczych. Drugim rodzajem kontroli jest samodzielne podejmowanie działań przez komputer nadzorujący budynek. Scenariusze tych działań są opracowywane przez użytkowników systemu i w reakcji na kombinację sygnałów z wybranych podsystemów wykonują określone sterowania w innych.

Jeżeli system komputerowy posiada dodatkowo możliwości przesyłania informacji przez modem w postaci faksu, głosu, e-maila lub wiadomości SMS, otrzymujemy narzędzie znacznie zwiększające bezpieczeństwo obiektu.

Mogą być różne scenariusze inteligentnego sterowania, np.:

Scenariusz 1.
Wymagania: W przypadku wystąpienia alarmu pożarowego lub alarmu włamaniowego należy obraz z najbliższej kamery wyświetlić na monitorze nr 3 oraz załączyć nagrywanie sygnału z tej kamery na magnetowidzie w sposób ciągły. Informacja o alarmie, z dokładnością do pomieszczenia, powinna zostać dodatkowo przesłana do administratora budynku jako wiadomość SMS.

Scenariusz 2.
Wymagania: W obiekcie bankowym droga do skarbca zabezpieczona jest kilkoma strefami kontroli dostępu, systemem alarmowym oraz monitorowana. W pomieszczeniu ochrony na monitorze nr 1 należy automatycznie załączać sygnał wizyjny z kamer na korytarzu skarbcowym w momencie przemieszczania się tam osoby. Ponieważ dostęp do skarbca ograniczono tylko do kilku osób, można założyć, że w danej chwili w tej części budynku znajduje się jedna osoba.

Scenariusz 3.
Wymagania: Zazbrojenie systemem alarmowym piętra 3 powinno automatycznie zaryglować wszystkie drzwi chronione systemem kontroli dostępu.

Korzyści z integracji

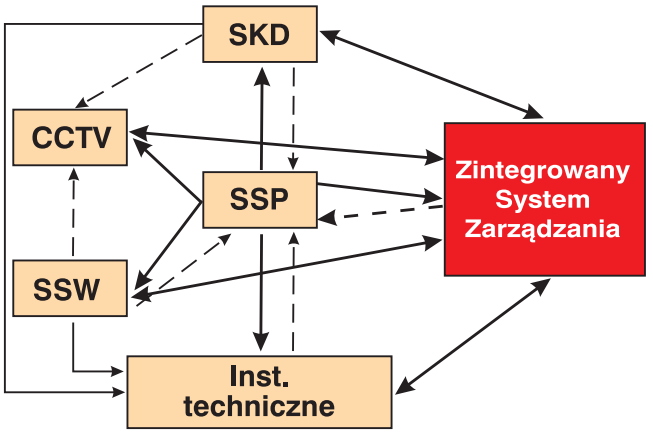
Integracja na poziomie oprogramowania daje oczywiste korzyści. Dla operatora systemu jest to wizualizacja wszystkich instalacji na planach pięter oraz na ekranach synoptycznych, natychmiastowe powiadamianie o alarmach, uszkodzeniach oraz przeglądanie danych historycznych. Tworzenie złożonych raportów umożliwia natomiast sprawdzenie poprawności obsługi scenariuszy oraz map sterowań w obiekcie.
Obsługa wszystkich instalacji z poziomu jednego, spójnego interfejsu graficznego jest znacznie prostsza od odczytu danych z wielu centralek bądź sterujących nimi systemów komputerowych.

Problemy integracji

W przeszłości wybudowano wiele obiektów, które wyposażono w najróżniejsze systemy, bez specjalnego zwracania uwagi na kompatybilność instalacji z systemami zarządzającymi i na obowiązujące standardy. Efektem tego jest bardzo duża liczba nietypowych instalacji technicznych. Ich użytkownicy sygnalizują obecnie konieczność integracji tych instalacji z nowymi systemami oraz możliwość ich monitorowania czy zarządzania. Dlatego zastosowanie centralnego systemu komputerowego należy przewidzieć już na etapie wyboru producentów systemów zabezpieczeń, co ułatwi ich integrację przez wybrany system zarządzający.
Pomimo „otwartości" systemów zarządzających, przy integracji systemów należy liczyć się z problemem udostępnienia protokołu komunikacyjnego przez producenta sprzętu. Jest to o tyle istotne, iż dotychczas nie dopracowano się żadnego standardowego protokołu dla systemów zabezpieczeń budynku.

Otwartość systemu integrującego

Prawdziwie „otwarty" system komputerowy powinien przychodzące sygnały przekonwertować do spójnego formatu komunikacji. Powinien też umożliwiać sterowanie podsystemami w maksymalnym zakresie, dopuszczalnym przez protokół.
Na *rysunku 2* przedstawiono schematycznie ideę integracji systemów zabezpieczeń przy użyciu systemu komputerowego.



Rys. 2. Schemat integracji systemów zabezpieczeń z wykorzystaniem centralnego systemu zarządzającego. Ponieważ sterowanie systemem sygnalizacji pożaru nie jest zalecane, oznaczono je linią przerywaną

Przykładem w pełni otwartego systemu zarządzania zabezpieczeniami budynków jest system ZEUS 2000 firmy EMAX. Integruje on poszczególne instalacje poprzez tworzenie kolejnych modułów dopasowujących, które „tłumaczą" sygnały na drodze urządzenie – komputer, przy użyciu translatora komunikatów.

Język tworzenia scenariuszy działania

Spójny sposób obsługi dowolnych sygnałów umożliwił opracowanie języka tworzenia scenariuszy działania, które pozwalają na obsługę zaawansowanych zależności pomiędzy poszczególnymi systemami, czego nie da się uzyskać poprzez integrację sprzętową.

W systemie ZEUS 2000 operuje się dwoma podstawowymi pojęciami, niezależnie od rodzaju instalacji:
- adresem zmiennej – zmienna jest to odpowiednik fizycznego obiektu (elementu) świata zewnętrznego (np. czujnik, kamera), adres zmiennej jednoznacznie identyfikuje zmienną w systemie. Zmienne posiadają adresy techniczne w postaci trzyczłonowej (np. 2500.100.1) oraz tzw. aliasy – czyli unikatowe nazwy nadawane przez użytkownika systemu (np. czujka_ochrona_strop_lewa)
- wartością zmiennej – każda zmienna w danym momencie czasu posiada określony stan, opisujący aktualne zachowanie się monitorowanego elementu. Wartości opisane są liczbami bądź słownie (np. 15 określa Alarm, 9 określa Alarm techniczny etc.)

Przykładowy sformalizowany opis realizujący fragment Scenariusza 1 z pierwszej części artykułu wyglądać może następująco:

```
    // Alarmy – parter – sekretariat
JEŻELI
    ssp_czujka_1/5      ALARM
    ssp_czujka_1/6      ALARM
    ssp_czujka_1/7      ALARM
    ssp_rop_41/1        ALARM
    ssw_linia_2501
WYKONAJ
    cctv_kam_7          3
    cctv_sterowanie_1   START
    SEND „Alarm – Sekretariat (Parter)" #NUM_1 #NUM_2 MD_SMS

    // Alarmy – parter – kiosk
JEŻELI
    2500.16.1           15
    2500.17.1           15
    2505.2501.1         15
WYKONAJ
    2700.5.1            3
    2700.1001.1         START
    SEND „Alarm – Kiosk (Parter)" #NUM_1 #NUM_2   2901
```

Rozbudowane możliwości powiadamiania

Przy projektowaniu scenariuszy działania można nakazać, aby system „sam zadzwonił" po straż pożarną i „przesłał faksem" plan dojazdu do obiektu. Możliwe jest sprawdzenie aktualnego stanu systemu z dowolnego miejsca za pomocą telefonu, modemu, sieci Internet itp. Możliwości systemu ZEUS 2000 w tym zakresie są następujące:
- Telefon alarmowy – w sytuacjach awaryjnych system „dzwoni" pod wskazane numery i przekazuje określone wiadomości.
- Fax alarmowy – możliwe jest automatyczne przekazywanie informacji faxem, np. z planem dojazdu do obiektu.
- SMS – możliwe jest wysyłanie (system informuje użytkownika o alarmach i uszkodzeniach) oraz odbiór (użytkownik steruje systemem) wiadomości tekstowych.
- Telefon informacyjny – możliwe jest uzyskanie informacji o aktualnym stanie systemu z dowolnego miejsca za pomocą zwykłego telefonu oraz zdalne wykonywanie sterowań.
- Modem, sieci komputerowe, WWW – dostęp do informacji jest możliwy także za pomocą wszelkich sieci komputerowych.
- Odczyt i rejestracja poleceń – w sytuacjach alarmowych możliwe jest odczytywanie informacji przez komputer i/lub rejestracja dźwięku w centrum sterowania.

Uwagi końcowe

Integracja technicznych systemów zabezpieczeń przy użyciu otwartego systemu zarządzającego pozwala na elastyczne zarządzanie tymi systemami. Modyfikacje scenariuszy postępowania umożliwiają szybsze i bardziej rozbudowane modelowanie sterowań pomiędzy integrowanymi podsystemami. Niezaprzeczalną zaletą graficznego przedstawienia instalacji jest możliwość szybkiej reakcji w sytuacjach alarmowych. Inaczej przemawia do użytkownika np. plan lewego skrzydła piętra z migającym czujnikiem pożarowym, inaczej zaś lakoniczna informacja na czytniku centralki z napisem „pokoj 1627 – adm. komp. – pozar". ■