Wyzwania dla integracji systemów bezpieczeństwa w budynku

Renata Żybura – Specjalista ds. Marketingu,
artykuł firmy ela-compil sp. z o. o.

Wymagania stawiane budynkom i obiektom są coraz wyższe, zarówno w przypadku nowo budowanych, jak i już funkcjonujących. Budynki pełnią bardzo zróżnicowane funkcje – poczynając od obiektów o wąsko zdefiniowanym przeznaczeniu, jak np. biurowce po rozproszone na rozległych przestrzeniach obszary przemysłowo-magazynowe lub obiekty wielofunkcyjne, jak hale widowiskowo-sportowe czy centra komunikacyjne. Niezależnie od przeznaczenia, różnic funkcjonalnych i stopnia skomplikowania struktury tych obiektów muszą być one łatwe w zarządzaniu, gwarantować bezpieczeństwo życia i mienia oraz generować możliwie niskie koszty związane z utrzymaniem. Aby spełnić te warunki nowoczesne systemy bezpieczeństwa, rozbudowane instalacje i automatyka budynkowa muszą być sterowane i zarządzane z jednego miejsca, w sposób, który umożliwi wysoką skuteczność i łatwość zarządzania.

Najistotniejsze zagadnienia

Systemy zainstalowane w budynku, jak BAS (ang. *Building Automation System*), SMS (ang. *Security Management System*) dla dowolnie dużego obiektu powinny być ze sobą zintegrowane w jeden system kontroli i zarządzania budynkiem **BMS** (ang. *Building Management System*). Założenie takie oznacza w praktyce stosowanie nowoczesnych technologii, zarówno komputerów, sterowników, urządzeń peryferyjnych, jak i samych sieci komunikacyjnych wraz z protokołami komunikacyjnymi.

BMS jest systemem zarządzania budynkiem, który znajduje zastosowanie w budynkach biurowych, hotelowych, użyteczności publicznej, galeriach handlowych, centrach komunikacyjnych, takich jak dworce czy lotniska, a także w obiektach przemysłowych oraz wielu innych. Zwykle na BMS składa się kilka systemów. Główny podział wyodrębnia: BAS odpowiedzialny za integrację i zarządzanie podsystemami i urządzeniami odpowiadającymi za komfort w budynku oraz SMS, któremu przyporządkowane są systemy i instalacje odpowiedzialne za bezpieczeństwo. Podział pomiędzy podsystemami BAS i SMS jest umowny, bowiem część sygnałów alarmowych z urządzeń automatyki budynkowej powinna docierać na obsługiwane 24 godz./dobę stanowiska SMS. Do zadań BMS należą: integracja, kontrola, monitorowanie, optymalizacja i raportowanie wszystkich elementów infrastruktury.

BAS jest natomiast systemem zarządzania automatyką budynkową, który integruje takie podsystemy i urządzenia, jak np.:

- oświetlenie wewnętrzne i zewnętrzne,
- ogrzewanie,
- wentylacja i klimatyzacja,
- system zasilania UPS,
- system pogodowy,
- obsługa urządzeń audio-wideo i innych urządzeń codziennego użytku,
- sterowniki wind i ruchomych schodów.

SMS – to system integrujący i zarządzający systemami i urządzeniami odpowiedzialnymi za bezpieczeństwo. SMS integruje, wizualizuje i nadzoruje zintegrowane podsystemy i urządzenia. Wyposażony jest w jedno- lub wielostanowiskowe centrum obsługujące alarmy i komunikaty o awariach z takich systemów, jak:

- system sygnalizacji włamania i napadu (SSWiN),
- system telewizji dozorowej (CCTV),
- system sygnalizacji pożaru (SSP),
- system kontroli dostępu,
- system sterowania oddymianiem pożarowym,
- sterowanie i monitorowanie klap przeciwpożarowych,
- depozytory kluczy,
- instalacje stałych urządzeń gaszących,
- instalacje automatycznego wydzielenia przeciwpożarowego i dymowe,
- system wykrywania gazów,
- system łączności,
- dźwiękowy system ostrzegawczy (DSO).

Stanowisko systemu integrującego i wizualizującego systemy bezpieczeństwa w budynku

Systemy bezpieczeństwa w nowoczesnym budynku nie tylko czuwają nad bezpieczeństwem użytkowników, ale podnoszą też jego wartość. **Integracja systemów bezpieczeństwa przyczynia się do polepszenia ergonomii użytkowania obiektu i znacząco wpływa na obniżenie kosztów jego eksploatacji.** Systemy zainstalowane w budynku powinny być zintegrowane już na etapie jego projektowania i powstawania, wtedy osiąga się największy efekt. *Integrację można również wprowadzić w obiektach już istniejących, rozbudowywanych czy modernizowanych*. System nadrzędny, odpowiadający za monitorowanie

i nadzór stanów zintegrowanych podsystemów, a także za ich integrację i wizualizację, powinien być systemem otwartym, elastycznym i skalowalnym, ponieważ tylko wówczas będzie możliwe zintegrowanie wszystkich systemów i urządzeń w celu zapewnienia bezpieczeństwa i sprawności zarządzania obiektem. Takie właściwości systemu integrującego są nieodzowne ze względu na heterogeniczność, czyli różnorodność podsystemów i urządzeń zainstalowanych w budynku. Praktycznie w każdym obiekcie znajdują się systemy heterogeniczne ze względu na przeznaczenie, np. system sygnalizacji pożaru, system kontroli dostępu, system CCTV itp. Heterogeniczność dotyczy również pochodzenia poszczególnych systemów od różnych producentów, co skutkuje innym standardem komunikacji i obsługi.

Integracja systemów bezpieczeństwa polega na skomunikowaniu wielu systemów i urządzeń heterogenicznych w taki sposób, aby możliwa była wymiana danych pomiędzy nimi. **Integracja pozwala na interakcję pomiędzy poszczególnymi systemami, a tym samym na zautomatyzowanie wielu zadań oraz osiągnięcie efektu synergii.** Integracja odbywa się poprzez odpowiednią platformę zapewniającą interfejsy komunikacyjne oraz oprogramowanie pozwalające na wymianę informacji i formułowanie różnych funkcji logicznych.

Jednym ze sposobów bezpośredniego komunikowania się z danym urządzeniem lub systemem jest **interfejs dedykowany**, który składa się ze styku elektrycznego (RS 232, RS 485, USB, Ethernet itp.) oraz protokołu wymiany danych. Wymianę danych narzuca w tym przypadku producent danego urządzenia lub systemu. Komunikacja poprzez interfejs dedykowany odbywa się szybko i pewnie, bowiem realizowana jest na najniższym poziomie bez dodatkowych translacji. W przypadku systemów odpowiedzialnych za bezpieczeństwo, kryterium czasu jest bardzo istotne. Realizacja interfejsu dedykowanego w przypadku systemów bezpieczeństwa wiąże się zwykle z uzyskaniem odpowiednich, często poufnych informacji od producenta.

Inny sposób komunikowania się z danym urządzeniem lub systemem może odbywać się za pomocą **uniwersalnego standardu komunikacyjnego**. Przykładem jest serwer OPC (ang. *open connectivity*). W procesie komunikacji potrzebne jest dodatkowe ogniwo w postaci serwera OPC, który komunikuje się z systemem integrowanym. Odczytane dane są następnie udostępniane w postaci drzewka zmiennych. System integrujący może połączyć się z takim serwerem i dokonywać odczytu, jak również zapisu wartości. Dodatkowej pracy wymaga jednak zinterpretowanie tych danych. Przykładowo, odczytana wartość 25 może oznaczać kąt otwarcia klapy przeciwpożarowej lub temperaturę w kanale wentylacyjnym. Inne standardy otwartych interfejsów to BacNet, LON czy ModBus.

W rozbudowanych systemach zarządzających bardzo duża ilość danych napływa w czasie rzeczywistym. Zadaniem obsługi jest stała analiza tych danych i podejmowanie odpowiednich decyzji. Kluczowym elementem w analizie informacji i w procesie decyzyjnym jest czytelne i zrozumiałe przedstawienie tego rodzaju danych obsłudze.

Wizualizacja wykorzystywana jest do prezentacji stanów i procesów zachodzących w systemach zainstalowanych w obiekcie. Odbywa się na ekranie lub ekranach komputera i może dotyczyć pojedynczego systemu lub całej zintegrowanej grupy systemów. W przypadku systemów zintegrowanych, wizualizacja wprowadza uporządkowany, ustandaryzowany sposób prezentowania stanów, niezależnie od rodzaju zintegrowanego systemu.

Optymalne rozwiązania dla budynków

Integracja systemów bezpieczeństwa ma na celu ułatwienie zarządzania budynkiem, zwiększenie poziomu bezpieczeństwa i zmniejszenie poziomu kosztów związanych z obsługą poszczególnych systemów.

Dzięki integracji z systemem CCTV, system nadrzędny wspiera obsługę podglądem wideo aktualnej sytuacji w obiekcie, prezentowanym w czasie rzeczywistym. Umożliwia także nawigowanie po planie sytuacyjnym i prezentowanie na żywo obrazu z wybranej kamery. Obraz może być wkomponowany w ekran komputera. System nadrzędny może również zarządzać ekspozycją obrazów na „ścianie" monitorów. Nawigacja odbywa się za pomocą myszki komputerowej lub za pomocą ekranu dotykowego. W przypadku sytuacji alarmowej system, w ramach procedury alarmowej, automatycznie wybiera kamery i monitory, na których ma być pokazany obraz. Jeśli zintegrowany jest również system kontroli dostępu obraz z kamer prezentowany na monitorze komputera pozwala na weryfikację wizualną wchodzących i wychodzących osób, co w sposób znaczący wspiera i optymalizuje zarządzanie dostępem do obiektu.

Integracja z systemem kontroli dostępu oraz sygnalizacji włamania i napadu pozwala na ich pełną wizualizację na planach sytuacyjnych, wspomaganie sterowania uzbrajania i rozbrajania stref oraz zwalnianie drzwi ewakuacyjnych z kontrolą dostępu w przypadku alarmu. Zintegrowanie systemu kontroli dostępu usprawnia zarządzanie dostępem użytkowników do poszczególnych stref obiektu. Jest to możliwe m.in. dzięki wizualizacji stanów przejść, spływającym do operatora informacjom o pró-

bach nieuprawnionego użycia identyfikatora czy zastosowaniu ręcznej blokady drzwi.

Zarządzanie obiegiem kluczy to obszar powiązany z kontrolą dostępu. Sprawną realizację tej funkcji umożliwiają depozytory kluczy – zintegrowane z nadrzędnym systemem szafki z kluczami, wyposażone w czytnik i klawiaturę. Dostęp do klucza określony jest zgodnie z uprawnieniami użytkownika i harmonogramem czasowym. Warto tutaj zwrócić uwagę na fakt, że integracja kontroli dostępu wraz z depozytorami kluczy umożliwia optymalizację organizacji obiegu kluczy i kosztów z tym związanych, zwłaszcza w przypadku biurowców czy obiektów uczelnianych. System nadzorujący poinformuje bowiem obsługę np. o próbie nieuprawnionego użycia klucza, przekroczenia czasu lub braku zwrotu – w zależności od zdefiniowanych uprzednio uprawnień.

Dzięki zintegrowaniu interkomów możliwa jest wizualizacja stanu rozmów, tworzenie zestawień połączeń, a przede wszystkim alarmowe wywołanie operatora systemu nadrzędnego w celu poinformowania go o zdarzeniu lub potrzebie pomocy. W sytuacjach alarmowych w momencie nadejścia komunikatu o zdarzeniu system może wyświetlić widok z kamery, która rejestruje zgłoszone zdarzenie, co ułatwia podjęcie dalszych działań.

System integrujący pozwala także oddzielić część detekcyjną od wykonawczej systemu sygnalizacji alarmu pożarowego i wspomaga proces sterowania i monitorowania jego przebiegu. Centrale systemu sygnalizacji pożaru (SSP) spełniają tym samym dokładnie taką rolę, do jakiej zostały stworzone – powiadamiają system nadrzędny o wykrytym pożarze. Rejestracja alarmów na centralnym serwerze umożliwia późniejszą ich analizę w powiązaniu z innymi systemami bezpieczeństwa i automatyki budynkowej.

Integracja systemów bezpieczeństwa optymalizuje także proces związany z serwisowaniem i dokonywaniem okresowych przeglądów. Dzięki możliwości prowadzenia dzienników konserwacji i gromadzeniu protokołów z przeglądów w postaci formularzy, system integrujący zapewnia utrzymanie wysokiego stanu technicznego infrastruktury w budynku, jak również usprawnia przeprowadzanie napraw i konserwacji, zgodnie z przyjętym harmonogramem.

Optymalne wykorzystanie integracji systemów bezpieczeństwa polega zatem na takim sprzężeniu różnorodnych funkcji, jakie pełnią poszczególne systemy, aby uzyskać synergiczne efekty ułatwiające zarządzanie funkcjonowaniem budynku.

Proces budowania koncepcji integracji systemów bezpieczeństwa

Aby właściciele i użytkownicy budynków mogli w pełni korzystać z osiągnięć i funkcjonalności integracji systemów bezpieczeństwa konieczna jest jasno sprecyzowana koncepcja systemu zarządzania budynkiem. Dobrze przemyślana koncepcja umożliwia dopasowanie systemu zgodnie z indywidualnymi potrzebami użytkownika oraz optymalizację funkcjonalności, wygody, bezpieczeństwa i kosztów eksploatacji obiektu. W tym celu konieczne jest postępowanie według określonego porządku, który odzwierciedla się w następujących krokach:

Przykład centrum zarządzania bezpieczeństwem w obiekcie

1. Dokonanie audytu potrzeb i wymagań inwestora/użytkownika.
2. Uzgodnienie z inwestorem/użytkownikiem przyjętych założeń.
3. Sprawdzenie informacji dotyczących możliwości współpracy zastosowanego rozwiązania z urządzeniami pochodzącymi od różnych producentów.
4. Sprawdzenie uniwersalności systemu pod kątem obsługi protokołów komunikacyjnych.
5. Stworzenie projektu systemu na bazie powyższych ustaleń.
6. Sprawdzenie skalowalności przyjętego rozwiązania.
7. Sprawdzenie, czy system jest w pełni sieciowy i pozwala na dowolne rozmieszczenie stacji roboczych w dowolnym miejscu.
8. Określenie poziomu i stopnia integracji poszczególnych systemów oraz relacji pomiędzy systemami bezpieczeństwa a pozostałymi systemami teletechnicznymi zainstalowanymi w budynku.
9. Określenie wykorzystanego protokołu komunikacyjnego oraz możliwości pracy autonomicznej poszczególnych systemów, niezależnie od systemu integrującego.
10. Określenie struktury sieci oraz liczby stacji operatorskich dla systemu integrującego.
11. Określenie wymagań technicznych wobec urządzeń oraz oprogramowania.
12. Stworzenie struktury zintegrowanego systemu, opisującej funkcje i zadania poszczególnych elementów.

Zarówno nowo powstające jak i już funkcjonujące budynki muszą dostosowywać się do zmieniających się potrzeb organizacji i kształtować środowisko pracy w zależności od rodzaju i stopnia złożoności zadań jakie mają rozwiązywać. Elastyczność i skalowalność systemu integrującego nabiera w tym kontekście szczególnego znaczenia – musi się on bowiem zmieniać i dostosowywać do zmieniających się potrzeb użytkowników obiektu.

W najbliższej przyszłości integracja systemów bezpieczeństwa będzie musiała zmierzyć się z nowymi wyzwaniami i podołać realizacji jeszcze bardziej zaawansowanym zadaniom. Jednym z nich jest integrowanie coraz większej liczby różnych systemów bezpieczeństwa i urządzeń – systemy powinny zatem stawać się coraz bardziej otwarte. Stopień otwartości systemów stwarza dla integratorów i użytkowników większą możliwość wyboru różnych rozwiązań.

Kolejnym zjawiskiem jest wprowadzenie standardów branżowych, dzięki którym będzie łatwiejsza nie tylko integracja systemów, ale również umożliwią one bardziej harmonijny i szybszy wzrost całej branży. Innym wyzwaniem jest transformacja systemów integrujących od modeli bazujących na dostarczaniu sprzętu do modeli bazujących na opracowywaniu i dostarczaniu oprogramowania i świadczenia usług.

ela-compil sp. z o. o.
ul. Słoneczna 15A, 60-286 Poznań
www.ela-compil.pl